



PŘIJATÉ TEXTY

P10_TA(2026)0286

Zjištění a doporučení zvláštního výboru pro Evropský štít pro demokracii

Usnesení Evropského parlamentu ze dne 15. září 2026 o zjištěních a doporučeních zvláštního výboru pro Evropský štít pro demokracii (2025/2069(INI))

Evropský parlament,

- s ohledem na své rozhodnutí ze dne 18. prosince 2024 o zřízení zvláštního výboru pro Evropský štít pro demokracii a stanovení jeho působnosti, početního složení a funkčního období¹,
- s ohledem na společné sdělení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 12. listopadu 2025 nazvané „Evropský štít pro demokracii: podpora silných a odolných demokracií“ (JOIN(2025)0791),
- s ohledem na Smlouvu o Evropské unii (SEU), a zejména na její článek 2 o základních hodnotách EU, článek 5 o pravomocích EU, článek 10 o demokratickém životě a článek 21 o vnější činnosti,
- s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 o mezinárodním trhu a článek 222 o solidaritě,
- s ohledem na Chartu Organizace spojených národů,
- s ohledem na ustanovení o svobodě projevu stanovená v článku 19 Všeobecné deklarace lidských práv, článek 19 Mezinárodního paktu o občanských a politických právech, článek 11 Evropské úmluvy o lidských právech (EÚLP) a článek 10 Listiny základních práv Evropské unie,
- s ohledem na Listinu základních práv Evropské unie,

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

- s ohledem na nařízení Evropského parlamentu a Rady (EU, Euratom) 2025/2445 ze dne 26. listopadu 2025 o statusu a financování evropských politických stran a evropských politických nadací²,
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci)³,
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2024/1624 ze dne 31. května 2024 o předcházení využívání finančního systému k praní peněz nebo financování terorismu⁴,
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2024/1083 ze dne 11. dubna 2024, kterým se stanoví společný rámec pro mediální služby na vnitřním trhu a mění směrnice 2010/13/EU (evropský akt o svobodě médií)⁵,
- s ohledem na směrnici Evropského parlamentu a Rady (EU) 2024/1069 ze dne 11. dubna 2024 o ochraně osob zapojených do účasti veřejnosti, před zjevně neopodstatněnými žalobními návrhy nebo zneužívajícími soudními řízeními („strategická soudní řízení proti účasti veřejnosti“)⁶ (směrnice proti strategickým soudním řízením proti účasti veřejnosti),
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy⁷ (nařízení o transparentnosti a cílení politické reklamy),
- s ohledem na nařízení Evropského parlamentu a Rady (EU, Euratom) 2023/2841 ze dne 13. prosince 2023, kterým se stanoví opatření k zajištění vysoké společné úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie⁸ (nařízení o kybernetické bezpečnosti),

² Úř. věst. L, 2025/2445, 8.12.2025, ELI:
<http://data.europa.eu/eli/reg/2025/2445/oj>.

³ Úř. věst. L, 2024/1689, 12.7.2024, ELI:
<http://data.europa.eu/eli/reg/2024/1689/oj>.

⁴ Úř. věst. L, 2024/1624, 19.6.2024, ELI:
<http://data.europa.eu/eli/reg/2024/1624/oj>.

⁵ Úř. věst. L, 2024/1083, 17.4.2024, ELI:
<http://data.europa.eu/eli/reg/2024/1083/oj>.

⁶ Úř. věst. L, 2024/1069, 16.4.2024, ELI:
<http://data.europa.eu/eli/dir/2024/1069/oj>.

⁷ Úř. věst. L, 2024/900, 20.3.2024, ELI:
<http://data.europa.eu/eli/reg/2024/900/oj>.

⁸ Úř. věst. L, 2023/2841, 18.12.2023, ELI:
<http://data.europa.eu/eli/reg/2023/2841/oj>.

- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2023/1114 ze dne 31. května 2023 o trzích kryptoaktiv a o změně nařízení (EU) 1093/2010 a (EU) 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937⁹ (nařízení o trzích kryptoaktiv),
- s ohledem na směrnici Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES¹⁰ (směrnice o odolnosti kritických subjektů),
- s ohledem na směrnici Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)¹¹,
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách)¹² a nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích)¹³,
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2024/1252 ze dne 11. dubna 2024, kterým se stanoví rámec pro zajištění bezpečných a udržitelných dodávek kritických surovin a mění nařízení (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1724 a (EU) 2019/1020¹⁴ (evropský akt o kritických surovinách),
- s ohledem na společné sdělení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 3. prosince 2025 nazvané „Posílení hospodářské bezpečnosti EU“ (JOIN(2025)0977),
- s ohledem na nařízení Evropského parlamentu a Rady (EU) 2021/692 ze dne 28. dubna 2021, kterým se zavádí program Občané, rovnost,

⁹ Úř. věst. L 150, 9.6.2023, s. 40, ELI: <http://data.europa.eu/eli/reg/2023/1114/oj>.

¹⁰ Úř. věst. L 333, 27.12.2022, s. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>.

¹¹ Úř. věst. L 333, 27.12.2022, s. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>.

¹² Úř. věst. L 277, 27.10.2022, s. 1, ELI: <http://data.europa.eu/eli/reg/2022/2065/oj>.

¹³ Úř. věst. L 265, 12.10.2022, s. 1, ELI: <http://data.europa.eu/eli/reg/2022/1925/oj>.

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

práva a hodnoty a zrušují nařízení Evropského parlamentu a Rady (EU) č. 1381/2013 a nařízení Rady (EU) č. 390/2014¹⁵,

- s ohledem na směrnici Evropského parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie¹⁶,
- s ohledem na směrnici Evropského parlamentu a Rady 2010/13/EU ze dne 10. března 2010 o koordinaci některých právních a správních předpisů členských států upravujících poskytování audiovizuálních mediálních služeb (směrnice o audiovizuálních mediálních službách)¹⁷,
- s ohledem na rozhodnutí Rady 2014/145/SZBP ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny¹⁸ a nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014 o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny¹⁹,
- s ohledem na rozhodnutí Rady 2014/119/SZBP ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině²⁰ a nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014 o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině²¹,
- s ohledem na rozhodnutí Rady 2014/512/SZBP ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině²² a nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině²³,

15 Úř. věst. L 156, 5.5.2021, s. 1, ELI:
<http://data.europa.eu/eli/reg/2021/692/oj>.

16 Úř. věst. L 305, 26.11.2019, s. 17, ELI:
<http://data.europa.eu/eli/dir/2019/1937/oj>.

17 Úř. věst. L 95, 15.4.2010, s. 1, ELI:
<http://data.europa.eu/eli/dir/2010/13/oj>.

18 Úř. věst. L 78, 17.3.2014, s. 16, ELI:
[http://data.europa.eu/eli/dec/2014/145\(1\)/oj](http://data.europa.eu/eli/dec/2014/145(1)/oj).

19 Úř. věst. L 78, 17.3.2014, s. 6, ELI:
<http://data.europa.eu/eli/reg/2014/269/oj>.

20 Úř. věst. L 66, 6.3.2014, s. 26, ELI:
[http://data.europa.eu/eli/dec/2014/119\(1\)/oj](http://data.europa.eu/eli/dec/2014/119(1)/oj).

21 Úř. věst. L 66, 6.3.2014, s. 1, ELI:
<http://data.europa.eu/eli/reg/2014/208/oj>.

22 Úř. věst. L 229, 31.7.2014, s. 13, ELI:
<http://data.europa.eu/eli/dec/2014/512/oj>.

23 Úř. věst. L 229, 31.7.2014, s. 1, ELI:
<http://data.europa.eu/eli/reg/2014/833/oj>.

- s ohledem na rozhodnutí Rady (SZBP) 2022/266 ze dne 23. února 2022 o omezujících opatřeních v reakci na uznání nezávislosti území Doněcké a Luhanské oblasti Ukrajiny, která nejsou pod kontrolou vlády, a vyslání ruských ozbrojených sil na tato území²⁴ a na nařízení Rady (EU) 2022/263 ze dne 23. února 2022 o omezujících opatřeních v reakci na uznání nezávislosti území Doněcké a Luhanské oblasti Ukrajiny, která nejsou pod kontrolou vlády, a vyslání ruských ozbrojených sil na tato území²⁵,
- s ohledem na rozhodnutí Rady 2014/2643 ze dne 8. října 2024 o omezujících opatřeních vzhledem k destabilizujícím činnostem Ruska²⁶ a nařízení Rady (EU) č. 2024/2014 ze dne 8. října 2024 o omezujících opatřeních vzhledem k destabilizujícím činnostem Ruska²⁷,
- s ohledem na rozhodnutí Rady 2012/642/SZBP ze dne 15. října 2012 o omezujících opatřeních vůči Bělorusku²⁸ a na nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska²⁹,
- s ohledem na rozhodnutí Rady (SZBP) 2023/1532 ze dne 20. července 2023 o omezujících opatřeních vzhledem k vojenské podpoře útočné války Ruska proti Ukrajině³⁰ ze strany Íránu a nařízení Rady (EU) 2023/1529 ze dne 20. července 2023 o omezujících opatřeních vzhledem k vojenské podpoře útočné války Ruska proti Ukrajině ze strany Íránu³¹,
- s ohledem na rozhodnutí Rady (SZBP) 2024/1603 ze dne 31. května 2024, kterým se mění rozhodnutí (SZBP) 2016/849 o omezujících opatřeních vůči Korejské lidově demokratické republice³², a na prováděcí nařízení Rady (EU) 2024/1602 ze dne 31. května 2024,

²⁴ Úř. věst. L 42 I, 23.2.2022, s. 109, ELI:
<http://data.europa.eu/eli/dec/2022/266/oj>.

²⁵ Úř. věst. L 42 I, 23.2.2022, s. 7, ELI:
<http://data.europa.eu/eli/reg/2022/263/oj>.

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

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

²⁸ Úř. věst. L 285, 17.10.2012, s. 1, ELI:
<http://data.europa.eu/eli/dec/2012/642/oj>.

²⁹ Úř. věst. L 134, 20.5.2006, s. 1, ELI:
<http://data.europa.eu/eli/reg/2006/765/oj>.

³⁰ Úř. věst. L 186, 25.7.2023, s. 20, ELI:
<http://data.europa.eu/eli/dec/2023/1532/oj>.

³¹ Úř. věst. L 186, 25.7.2023, s. 1, ELI:
<http://data.europa.eu/eli/reg/2023/1529/oj>.

³² Úř. věst. L, 2024/1603, 31.5.2024, ELI:
<http://data.europa.eu/eli/dec/2024/1603/oj>.

kterým se provádí nařízení (EU) 2017/1509 o omezujících opatřeních vůči Korejské lidově demokratické republice³³,

- s ohledem na návrh nařízení Rady, kterým se stanoví víceletý finanční rámec na období 2028-2034, který dne 16. července 2025 předložila Komise (COM(2025)0571),
- s ohledem na návrh nařízení Evropského parlamentu a Rady o digitálních sítích, kterým se mění nařízení (EU) 2015/2120, směrnice 2002/58/ES a rozhodnutí č. 676/2002/ES a zrušuje nařízení (EU) 2018/1971, směrnice (EU) 2018/1972 a rozhodnutí č. 243/2012/EU (akt o digitálních sítích) (COM(2026)0016), který dne 21. ledna 2026 předložila Komise,
- s ohledem na návrh nařízení Evropského parlamentu a Rady o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA), evropském rámci pro certifikaci kybernetické bezpečnosti a bezpečnosti dodavatelských řetězců IKT a o zrušení nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti 2) (COM(2026)0011), který dne 20. ledna 2026 předložila Komise (revidovaný akt o kybernetické bezpečnosti),
- s ohledem na návrh nařízení Evropského parlamentu a Rady ze dne 3. června 2026 o rámci opatření pro posílení unijního ekosystému polovodičů a o zrušení nařízení (EU) 2023/1781 (akt o čipech 2.0) (COM(2026)0504),
- s ohledem na návrh nařízení Evropského parlamentu a Rady ze dne 3. června 2026, kterým se zřizuje rámec opatření pro posílení ekosystému cloudových služeb a ekosystému AI (akt pro rozvoj cloudu a AI) (COM(2026)0502),
- s ohledem na pozměňující návrhy přijaté Evropským parlamentem dne 27. listopadu 2025 k návrhu směrnice Evropského parlamentu a Rady, kterou se stanoví harmonizované požadavky na transparentnost zastupování zájmů jménem třetích zemí na vnitřním trhu a kterou se mění směrnice (EU) 2019/1937 (COM(2023)0637 – C9-0464/2023 – 2023/0463(COD))³⁴,
- s ohledem na svá předchozí usnesení o Ruské federaci a její agresi vůči Ukrajině, jakož i na její nepřátelské akce proti členským státům, včetně usnesení ze dne 9. října 2025 o společné reakci na nedávné narušení vzdušného prostoru a kritické infrastruktury členských států EU Ruskem³⁵,

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

³⁴ Přijaté texty, P10_TA(2025)0306.

³⁵ Přijaté texty, P10_TA(2025)0230.

- s ohledem na své usnesení ze dne 29. dubna 2026 o zprávě Komise o právním státu za rok 2025³⁶,
- s ohledem na své usnesení ze dne 7. května 2025 o přepracovaném dlouhodobém rozpočtu Unie v měnícím se světě³⁷,
- s ohledem na své usnesení ze dne 23. ledna 2025 o dezinformacích a falšování historie ze strany Ruska v zájmu ospravedlnění jeho válečné agrese proti Ukrajině³⁸ a s ohledem na své usnesení ze dne 22. října 2025 o postoji Rady k návrhu souhrnného rozpočtu Evropské unie na rozpočtový rok 2026³⁹, v němž je zmíněn projekt památníku v Bruselu,
- s ohledem na své usnesení ze dne 13. července 2023 o doporučení k reformě pravidel Evropského parlamentu týkajících se transparentnosti, bezúhonnosti, odpovědnosti a boje proti korupci⁴⁰,
- s ohledem na své usnesení ze dne 13. listopadu 2025 o řešení nadnárodních represí vůči obráncům lidských práv⁴¹,
- s ohledem na své usnesení ze dne 21. ledna 2026 o řešení beztrestnosti prostřednictvím sankcí EU, včetně globálního režimu sankcí EU v oblasti lidských práv (tzv. „Magnitského akt EU“)⁴²,
- s ohledem na své usnesení ze dne 1. června 2023 o zahraničním vměšování do všech demokratických procesů v Evropské unii, včetně dezinformací⁴³,
- s ohledem na své usnesení ze dne 15. prosince 2022 o podezření na korupci ze strany Kataru a širší potřebě transparentnosti a odpovědnosti v evropských orgánech a institucích⁴⁴,
- s ohledem na své usnesení ze dne 23. listopadu 2022 o uznání Ruské federace za stát, který podporuje terorismus⁴⁵,

³⁶ Přijaté texty, P10_TA(2026)0147.

³⁷ Přijaté texty, P10_TA(2025)0090.

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

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

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

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

⁴² Přijaté texty, P10_TA(2026)0015.

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

⁴⁴ Úř. věst. C 177, 17.5.2023, s. 109.

⁴⁵ Úř. věst. C 167, 11.5.2023, s. 18.

- s ohledem na své usnesení ze dne 9. března 2022 o zahraničním vměšování do všech demokratických procesů v Evropské unii, včetně dezinformací⁴⁶,
- s ohledem na své usnesení ze dne 8. března 2022 o zmenšujícím se prostoru pro občanskou společnost v Evropě⁴⁷,
- s ohledem na své usnesení ze dne 20. října 2021 o evropských médiích v digitální dekádě – akční plán na podporu oživení a transformace⁴⁸,
- s ohledem na své usnesení ze dne 23. listopadu 2016 o strategické komunikaci EU s cílem bojovat proti propagandě, kterou proti ní vedou třetí strany⁴⁹,
- s ohledem na své doporučení Radě a Komisi ze dne 15. června 2023 v návaznosti na vyšetřování údajných porušení a správních pochybení v oblasti provádění právních předpisů Unie týkajících se používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru⁵⁰,
- s ohledem na své doporučení ze dne 23. listopadu 2022 Radě, Komisi a místopředsedovi Komise, vysokému představiteli Unie pro zahraniční věci a bezpečnostní politiku týkající se nové strategie EU v oblasti rozšíření⁵¹,
- s ohledem na své doporučení ze dne 13. března 2019 adresované Radě a místopředsedkyni Komise, vysoké představitelce Unie pro zahraniční věci a bezpečnostní politiku a týkající se hodnocení následných kroků ESVČ dva roky po zprávě Evropského parlamentu o strategické komunikaci EU s cílem bojovat proti propagandě, kterou proti ní vedou třetí strany⁵²,
- s ohledem na kroky, které Komise učinila v návaznosti na doporučení Parlamentu uvedená v jeho usneseních,
- s ohledem na sdělení Komise ze dne 12. listopadu 2025 s názvem „Strategie EU pro občanskou společnost“ (COM(2025)0790),
- s ohledem na sdělení Komise ze dne 3. června 2026 o evropské technologické svrchovanosti, k němuž je přiložena Strategie EU pro otevřený zdrojový kód (COM(2026)0503),

⁴⁶ Úř. věst. C 347, 9.9.2022, s. 61.

⁴⁷ Úř. věst. C 347, 9.9.2022, s. 2.

⁴⁸ Úř. věst. C 184, 5.5.2022, s. 71.

⁴⁹ Úř. věst. C 224, 27.6.2018, s. 58.

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

⁵¹ Úř. věst. C 167, 11.5.2023, s. 105.

⁵² Úř. věst. C 23, 21.1.2021, s. 152.

- s ohledem na sdělení Komise ze dne 3. června 2026 nazvané „Strategický plán pro digitalizaci a umělou inteligenci v odvětví energetiky“ (COM(2026)0501),
- s ohledem na sdělení Komise ze dne 1. dubna 2025 nazvané „ProtectEU: Evropská strategie vnitřní bezpečnosti“ (COM(2025)0148),
- s ohledem na sdělení Komise ze dne 24. července 2024 nazvané „Zpráva o právním státu 2024 – Stav právního státu v Evropské unii“ (COM(2024)0800),
- s ohledem na sdělení Komise ze dne 8. července 2025 nazvané „Zpráva o právním státu 2025 – Stav právního státu v Evropské unii“ (COM(2025)0900),
- s ohledem na sdělení Komise ze dne 12. prosince 2023 o obraně demokracie (COM(2023)0630),
- s ohledem na sdělení Komise ze dne 3. prosince 2020 o evropském akčním plánu pro demokracii (COM(2020)0790),
- s ohledem na společná sdělení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku ze dne 5. prosince 2018 s názvem „Akční plán proti dezinformacím“ (JOIN(2018)0036) a ze dne 14. června 2019 s názvem „Zpráva o provádění akčního plánu proti dezinformacím“ (JOIN(2019)0012),
- s ohledem na partnerství mezi Evropskou unií a Spojeným královstvím Velké Británie a Severního Irska v oblasti bezpečnosti a obrany uzavřené dne 19. května 2025,
- s ohledem na národní bezpečnostní strategii Spojených států amerických z listopadu 2025 a na národní obrannou strategii z ledna 2026,
- s ohledem na politické směry na funkční období Komise 2024–2029, které předsedkyně Komise Ursula von der Leyenová předložila dne 18. července 2024, nazvané „Volba Evropy“,
- s ohledem na prováděcí rozhodnutí Komise ze dne 28. března 2025 o financování programu Digitální Evropa a přijetí víceletého pracovního programu na období 2025–2027 (C(2025)1839),
- s ohledem na předběžná zjištění Komise oznámená dne 6. února 2026 týkající se nedodržování nařízení o digitálních službách ze strany společnosti TikTok, pokud jde o posuzování rizik v souvislosti s jejími doporučovacími systémy a návykovými prvky designu,
- s ohledem na kodex chování v oblasti dezinformací (zřízený jako kodex zásad boje proti dezinformacím v roce 2018 a posílený v roce

2022), který Evropská komise a Evropský sbor pro digitální služby schválily dne 13. února 2025 jako kodex chování podle článku nařízení o digitálních službách s účinností od 1. července 2025,

- s ohledem na zprávu skupiny pro spolupráci v oblasti sítí a informačních systémů ze dne 23. ledna 2020 nazvanou „Kybernetická bezpečnost sítí 5G – soubor opatření EU ke zmírnění rizik“,
- s ohledem na zprávu bývalého prezidenta Finské republiky Sauliho Niinistöa ze dne 30. října 2024 jako zvláštního poradce předsedkyně Evropské komise nazvanou „Společně bezpečnější – posílení evropské civilní a vojenské připravenosti a pohotovosti“,
- s ohledem na doporučení Komise (EU) 2023/2829 ze dne 12. prosince 2023 o inkluzivních a odolných volebních procesech v Unii a o posílení evropského charakteru a efektivního průběhu voleb do Evropského parlamentu⁵³,
- s ohledem na doporučení Komise (EU) 2023/2836 ze dne 12. prosince 2023 o podpoře zapojení a účinné účasti občanů a organizací občanské společnosti v procesech tvorby veřejných politik⁵⁴,
- s ohledem na skutečnost, že Komise v roce 2019 zřídila Evropskou síť pro volební spolupráci (ECNE),
- s ohledem na tiskovou zprávu Komise ze dne 13. listopadu 2025 o zahájení vyšetřování možného porušení nařízení o digitálních trzích ze strany společnosti Google při odstraňování obsahu vydavatelů sdělovacích prostředků ve výsledcích vyhledávání,
- s ohledem na závěry Rady ze dne 21. května 2024 „Budoucnost kybernetické bezpečnosti: společné provádění a ochrana“,
- s ohledem na závěry Rady ze dne 17. října 2022 o bezpečnosti dodavatelského řetězce informačních a komunikačních technologií,
- s ohledem na doporučení Rady ze dne 8. prosince 2022 o celounijním koordinovaném přístupu za účelem posílení odolnosti kritické infrastruktury⁵⁵,

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

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

⁵⁵ Úř. věst. C 20, 20.1.2023, s. 1.

- s ohledem na rozhodnutí Rady (SZBP) 2023/855 ze dne 24. dubna 2023 o partnerské misi Evropské unie v Moldavsku (EUPM Moldova)⁵⁶,
- s ohledem na akční plán nazvaný „Strategický kompas pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti“, který schválila Rada dne 21. března 2022 a potvrdila Evropská rada dne 25. března 2022,
- s ohledem na informace Litvy, Dánska, Estonska, Finska, Lotyšska, Německa, Slovinska a Španělska pro zasedání Rady pro dopravu, telekomunikace a energetiku dne 6. června 2025, které vyzývají ke společným opatřením v reakci na hrozby rušení a spoofingu globálních družicových navigačních systémů (GNSS),
- s ohledem na interinstitucionální dohodu (IID) ze dne 20. května 2021 mezi Evropským parlamentem, Radou Evropské unie a Evropskou komisí o povinném rejstříku transparentnosti⁵⁷,
- s ohledem na zvláštní zprávu Evropského účetního dvora č. 5/2022 ze dne 29. března 2022 nazvanou „Kybernetická bezpečnost orgánů, institucí a jiných subjektů EU: úroveň připravenosti obecně není úměrná hrozbám“,
- s ohledem na globální zásady OSN pro integritu informací – doporučení pro opatření zahrnující více zúčastněných stran, které byly zveřejněny dne 24. června 2024,
- s ohledem na Mezinárodní pakt o občanských a politických právech, zejména na jeho článek 20,
- s ohledem na Úmluvu OSN o mořském právu ze dne 10. prosince 1982, která vstoupila v platnost dne 16. listopadu 1994,
- s ohledem na Články o odpovědnosti států za mezinárodně protiprávní chování přijaté v listopadu 2001,
- s ohledem na prohlášení z Reykjavíku přijaté na 4. summitu hlav států a předsedů vlád Rady Evropy, který se konal ve dnech 16.–17. května 2023,
- s ohledem na mechanismus rychlé reakce skupiny G7 zřízený na summitu skupiny G7 v Charlevoix, který se konal ve dnech 8. až 9. června 2018,

⁵⁶ Úř. věst. L 110, 25.4.2023, s. 30, ELI:
<http://data.europa.eu/eli/dec/2023/855/oj>.

⁵⁷ Úř. věst. L 207, 11.6.2021, s. 1, ELI:
http://data.europa.eu/eli/agree_interinstit/2021/611/oj.

- s ohledem na pracovní dokument o opakujícím se vysokofrekvenčním rušení GNSS v pobaltských, východoevropských a severoevropských regionech a jeho důsledcích pro bezpečnost a ochranu mezinárodního civilního letectví, který Estonsko, Finsko, Lotyšsko, Litva, Polsko a Švédsko předložilo dne 13. června 2025 Mezinárodní organizaci pro civilní letectví,
- s ohledem na zprávu o konečném výsledku Konference o budoucnosti Evropy zveřejněnou dne 9. května 2022, a zejména na návrhy 27 a 37 této zprávy,
- s ohledem na studii s názvem „Posílení odolnosti – směrem k Evropskému štítu pro demokracii“, kterou si vyžádal zvláštní výbor Parlamentu pro Evropský štít pro demokracii a kterou zveřejnilo generální ředitelství pro občanská práva, spravedlnost a institucionální záležitosti v říjnu 2025⁵⁸,
- s ohledem na průzkum Eurobarometru Parlamentu z podzimu 2025, který byl zveřejněn v únoru 2026 a v němž jsou uvedeny obavy veřejnosti ohledně bezpečnostních rizik,
- s ohledem na zvláštní Eurobarometr Komise 568: Ochrana a podpora demokracie, zveřejněný v květnu 2025,
- s ohledem na první, druhou a třetí zprávu Evropské služby pro vnější činnost (ESVČ) o hrozbách zahraniční manipulace s informacemi a vměšování,
- s ohledem na zprávu Rady Evropy z roku 2024 nazvanou „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“ (Svoboda tisku v Evropě: čas zvrátit trend – výroční posouzení svobody tisku v Evropě partnerskými organizacemi platformy pro bezpečnost novinářů),
- s ohledem na zprávu Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) ze dne 1. října 2025 nazvanou „ENISA Hrozby v roce 2025“,
- s ohledem na zprávu Agentury Evropské unie pro spolupráci v oblasti prosazování práva (Europol) nazvanou „Posouzení hrozeb závažné a organizované trestné činnosti v EU – měnící se DNA závažné a organizované trestné činnosti“ (zpráva EU-SOCTA), která byla zveřejněna v roce 2025,

⁵⁸ Studie – „Posílení odolnosti – směrem k Evropskému štítu pro demokracii“, Evropský parlament, Generální ředitelství pro občanská práva, spravedlnost a institucionální záležitosti, tematická sekce Spravedlnost, občanské svobody a institucionální záležitosti, říjen 2025.

- s ohledem na zprávu odboru pro koordinaci algoritmického dohledu nizozemského úřadu pro ochranu údajů z října 2025 nazvanou „AI chatbots as voting aid“ (Chatboty umělé inteligence jako pomůcka pro hlasování),
- s ohledem na opatření týkající se influencerů, která přijal italský regulační orgán pro komunikace (AGCOM) dne 3. září 2025,
- s ohledem na Kodex chování pro reklamu realizovanou influencery, který přijala organizace AUTOCONTROL ve Španělsku dne 7. července 2025,
- s ohledem na varování českého Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) ze dne 3. září 2025 týkající se hrozeb v oblasti kybernetické bezpečnosti spočívajících v předávání systémových a uživatelských dat do Čínské lidové republiky a ve vzdálené správě technických aktiv vykonávané z území Čínské lidové republiky,
- s ohledem na zprávu nazvanou „Manipulation d’algorithmes et instrumentalisation d’influenceurs: enseignements de l’élection Présidentielle en Roumanie & risques pour la France“ (Manipulace algoritmů a instrumentalizace influencerů: poučení z prezidentských voleb v Rumunsku a rizika pro Francii), kterou v únoru 2025 zveřejnila služba francouzské vlády pro dohled nad zahraničním digitálním vměšováním a ochranu před ním (VIGINUM),
- s ohledem na příručku pro influencery, kterou v roce 2020 vypracovala finská organizace Mediapooli,
- s ohledem na zprávu ministerstva zahraničí USA ze srpna 2020 nazvanou „Pillars of Russia’s Disinformation and Propaganda Ecosystem“ (Piliře ruského dezinformačního ekosystému a propagandy),
- s ohledem na společné varování v oblasti kybernetické bezpečnosti vydané Agenturou USA pro kybernetickou bezpečnost a bezpečnost infrastruktury, Národní bezpečnostní agenturou USA, Federálním úřadem pro vyšetřování (FBI) a mezinárodními partnery v srpnu 2025 s názvem „Countering Chinese state-sponsored actors compromise of networks worldwide to Feed global espionage systems“ (Boj proti čínským státem sponzorovaným aktérům, kteří ohrožují sítě po celém světě s cílem vytvořit globální špiónážní systémy),
- s ohledem na zprávu Reportérů bez hranic ze dne 25. září 2025 nazvanou „The Propaganda Monitor: The Russian Edition“ (Monitor propagandy: Ruské vydání),
- s ohledem na článek, který zveřejnilo Centrum pro pluralitu a svobodu sdělovacích prostředků při Evropském univerzitním

institutu dne 1. listopadu 2025 pod názvem „Influencers as news creators: Implications for media regulation“ (Influenceri jako tvůrci zpráv: důsledky pro regulaci sdělovacích prostředků),

- s ohledem na článek zveřejněný konsorciem AlgoSoc dne 28. října 2025 s názvem „1 in 10 Dutch citizens are likely to ask AI for election advice. This is why they shouldn't“ (Každý desátý nizozemský občan se pravděpodobně obrací o radu ohledně voleb na umělou inteligenci. Důvody proč to nedělat),
- s ohledem na zprávu organizace What to Fix z června 2025 nazvanou „Bankrolling Sanctioned Entities: How Meta Platforms Ireland Ltd. May Have Violated EU Sanctions and channeled Money To RT, Sputnik and Other EU-Saned Entities through Facebook's Revenue Redistribution Programs“ (Financování subjektů, na něž se vztahují sankce: Jak mohla společnost Meta Platforms Ireland Ltd. porušovat sankce EU a přesměrovávat peníze do RT, Sputniku a dalších subjektů podléhajících sankcím EU prostřednictvím programů na přerozdělování příjmů z Facebooku),
- s ohledem na zvláštní zprávu organizace NewsGuard ze dne 6. března 2025 nazvanou „A Well-funded Moscow-based Global “News” Network has Infected Western Artificial Intelligence with Russian Propaganda“ (Dobře financovaná moskevská globální zpravodajská síť infikovala západní umělou inteligenci ruskou propagandou),
- s ohledem na zprávu organizace Media Freedom Rapid Response nazvanou „Mapping Media Freedom – Monitoring Report 2025“ (Mapování svobody médií – monitorovací zpráva 2024), zveřejněnou v únoru 2026,
- s ohledem na zprávu Světového ekonomického fóra z ledna 2025 nazvanou „Global Cybersecurity Outlook 2025“ (Globální výhled v oblasti kybernetické bezpečnosti do roku 2025),
- s ohledem na vyšetřovací zprávu zveřejněnou organizacemi VSquare, Delfi Estonia a partnerskými mediálními organizacemi dne 26. února 2024 s názvem „Kremlin Leaks: Secret Files Reveal How Putin Pre-Rigged his Reelection“ (Úniky z Kremlu: Tajné dokumenty odhalují, jak Putin předem zmanipuloval své znovuzvolení),
- s ohledem na Etický kodex chování pro influencery a tvůrce obsahu na sociálních médiích, který v roce 2024 zveřejnil Aspen Institute Germany,
- s ohledem na článek zveřejněný na webu Debunk.org dne 4. května 2023 s názvem „Kreml loni utratil 1,9 miliardy USD na propagandu, rozpočet překročil o čtvrtinu“,
- s ohledem na prohlášení ministerstva zahraničních věcí Ruské federace ze dne 28. prosince 2024 o opatřeních v reakci na 15.

balíček sankcí EU proti Rusku, v němž oznámilo rozšíření seznamu úředníků a občanů EU, kterým je zakázán vstup do země,

- s ohledem na článek ruské tiskové agentury TASS ze dne 28. prosince 2024 s názvem „Rusko v reakci na sankce výrazně rozšiřuje černou listinu úředníků EU – MZV“,
- s ohledem na tiskovou zprávu Komise ze dne 18. prosince 2023 o zahájení formálního řízení podle nařízení o digitálních službách proti společnosti X s cílem posoudit možná porušení jejích povinností, zejména pokud jde o zmírnění systémových rizik spojených s návrhem a fungováním jejích doporučovacích systémů, jakož i povinností souvisejících s posuzováním rizik, moderováním obsahu, transparentností reklamy a přístupem výzkumných pracovníků k údajům,
- s ohledem na řadu akademických a investigativních studií o doporučovacích systémech sociálních médií v souvislosti s německými spolkovými volbami, které naznačují algoritmickou předpojatost a zesílení polarizujícího nebo stranického obsahu, čímž se formuje politické informační prostředí uživatelů,
- s ohledem na tiskovou zprávu Komise ze dne 30. dubna 2024 o zahájení formálního řízení podle nařízení o digitálních službách proti platformám společnosti Meta, zejména pokud jde o nakládání s politickým obsahem na jejích online platformách,
- s ohledem na prohlášení společnosti TikTok z prosince 2024 o pokračující ochraně integrity platformy TikTok během rumunských voleb,
- s ohledem na prohlášení organizace European Solar Manufacturing Council ze dne 30. dubna 2025 s názvem „Omezit vzdálený přístup k fotovoltaickým střídačům od vysoce rizikových dodavatelů“, ve kterém varovala před riziky pro energetickou suverenitu Evropy v důsledku neregulovaných a dálkově ovládaných funkcí fotovoltaických střídačů od vysoce rizikových mimoevropských výrobců,
- s ohledem na bílou knihu o budoucnosti evropské obrany 2030 a nařízení Rady (EU) 2025/1106 ze dne 27. května 2025, kterým se zřizuje nástroj Bezpečnostní akce pro Evropu (SAFE) prostřednictvím posílení evropského obranného průmyslu⁵⁹,
- s ohledem na závěry předsednictví Rady ze dne 28. listopadu 2025 o přístupu ke spolehlivým zprávám v rámci Evropského štítu pro demokracii,

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

- s ohledem na články 55 a 213 jednacího řádu,
 - s ohledem na zprávu zvláštního výboru pro Evropský štít pro demokracii (A10-0199/2026),
- A. vzhledem k tomu, že dne 12. listopadu 2025 Komise a vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku předložily společné sdělení o zřízení Evropského štítu pro demokracii, v němž stanovily řadu opatření na posílení, ochranu a podporu silných a odolných demokracií v celé EU; vzhledem k tomu, že tato iniciativa je jedinečnou příležitostí vybudovat účinný celospolečenský přístup k ochraně evropské demokracie, svobody a prosperity; vzhledem k tomu, že demokratická odolnost a evropská bezpečnost jsou stále neoddělitelnější;
 - B. vzhledem k tomu, že chudoba, socioekonomická deprivace a marginalizace mohou vést k tomu, že některé segmenty společnosti budou obzvláště vystaveny vnějším zásahům a nepřátelským informačním operacím a budou vůči nim zranitelné;
 - C. vzhledem k tomu, že hrozba, kterou Rusko představuje pro bezpečnost a demokratickou integritu Evropy, zůstává na bezprecedentní úrovni; vzhledem k tomu, že významné výzvy představují i další aktéři, včetně Číny a Íránu; vzhledem k tomu, že je nezbytné přijmout zásadu informačního odstrašování a případně uplatňovat omezující opatření vůči subjektům odpovědným za zahraniční manipulaci s informacemi a vměšování;
 - D. vzhledem k tomu, že společné sdělení o Evropském štítu pro demokracii obsahuje několik pozitivních doporučení a návrhů, jako je zřízení Evropského střediska pro demokratickou odolnost, rozšíření jeho oblasti působnosti na přistupující země a sousedství EU a plné prosazování klíčových právních předpisů EU; vzhledem k tomu, že oba zvláštní výbory Parlamentu pro zahraniční vměšování do všech demokratických procesů v Evropské unii, včetně dezinformací (INGE a INGE 2), již vyzvaly k vytvoření struktury EU, podobné navrhovanému Evropskému centru pro demokratickou odolnost, pro boj proti zahraniční manipulaci s informacemi a vměšování; vzhledem k tomu, že by tato struktura neměla zdvojit stávající nástroje, schopnosti a pravomoci, ale měla by je konsolidovat do jediného subjektu s jasnou vizí a mandátem, skutečnými pravomocemi a financováním;
 - E. vzhledem k tomu, že nedávné zprávy ESVČ o útocích v rámci zahraniční manipulace s informacemi a vměšování prokazují stále podrobnější porozumění metodám, technické infrastruktuře a zamýšleným narativům zlovolných aktérů, avšak toto situační povědomí se dosud nepromítlo do trvalých operačních mechanismů, které by členskými státy a EU umožňovaly předjímat, předcházet, zjišťovat a přijímat včasné a koordinované protipatření; vzhledem

k tomu, že hlavním terčem nepřátelských informačních manipulačních kampaní a jiných forem nenávistných útoků jsou vnitrostátní a evropské volby; vzhledem k tomu, že tyto kampaně znevažují konkrétní kandidáty nebo politické strany, pokoušejí se zdiskreditovat samotný volební proces, zneužívají rozdělovací otázky a pokoušejí se zdiskreditovat tradiční sdělovací prostředky; vzhledem k tomu, že intenzivně napadány jsou rovněž orgány EU a členských států; vzhledem k tomu, že přístup EU k boji proti zahraniční manipulaci s informacemi a vměšování a dezinformacím je roztržštěn, přičemž mezi členskými státy existují značné rozdíly v kapacitách a neexistuje žádný zastřešující strategický rámec nebo fungující nadnárodní nebo evropský mechanismus spolupráce propojující operativní reakci se zpravodajskými informacemi o hrozbách;

- F. vzhledem k tomu, že cennými součástmi celkové odolnosti EU vůči zahraniční manipulaci s informacemi a vměšování a dezinformacím jsou ECNE, systém rychlého varování a Evropské středisko pro sledování digitálních médií (EDMO), jejich účinnost je však podstatně omezena tím, že dosud neexistují specializované operační struktury EU s pravomocí koordinovat činnosti zaměřené na budování odolnosti a mechanismy rychlé reakce a eskalace, které propojují národní operační kapacity s koordinací na úrovni EU;
- G. vzhledem k tomu, že hrozby představované zahraniční manipulací s informacemi a vměšování a dezinformacemi přesahují rámec jednotlivých členských států a představují útok na samotnou podstatu evropského projektu; vzhledem k tomu, že operace zahraniční manipulace s informacemi a vměšování systematicky cílí na základní demokratické hodnoty uvedené v článku 2 SEU a na zásadu otevřených a transparentních rozhodovacích procesů zakotvenou v článku 1 SEU, a to způsobem, který nepříznivě ovlivňuje zájmy EU a demokratické procesy v jejich členských státech; vzhledem k tomu, že v konečném důsledku jsou hlavními oběťmi těchto praktik evropští občané, neboť je přímo oslaben jejich přístup ke spolehlivým informacím a schopnost utvářet nezávislé názory a smysluplně se účastnit demokratického života a zároveň je ohrožena veřejná bezpečnost a společenská stabilita;
- H. vzhledem k tomu, že některé členské státy, které investovaly do specializovaných operačních struktur s jasnými stanovami a mandáty, jakož i dostatečné financování a personální vybavení dokazují, čeho lze dosáhnout, zejména v případě francouzské agentury VIGINUM a švédské Agentury pro psychologickou obranu, které přijaly na faktech založený, technický a nestranný přístup; vzhledem k tomu, že tyto instituce přispívají na žádost nebo z vlastního podnětu cennými poznatky, ale nejsou vhodně propojeny;
- I. vzhledem k tomu, že rychlý pokrok v oblasti umělé inteligence (AI) a technologií deepfake předstihuje adaptační schopnosti roztržštěných národních institucí a způsobuje, že dříve používaná

řešení, jako jsou povinnosti týkající se transparentnosti nebo maximálního úsilí, jsou již zastaralá; vzhledem k tomu, že bez koordinované reakce EU a jasných operačních a výzkumných schopností bude technologická převaha stále více nahrávat útočníkům na úkor obránců, což ohrozí samotný základ našich demokracií; vzhledem k tomu, že některé společnosti zabývající se umělou inteligencí namísto toho, aby posílily svá bezpečnostní opatření proti šíření a vytváření dezinformací prostřednictvím svých služeb, tato opatření naopak omezily; vzhledem k tomu, že umělá inteligence usnadňuje dezinformační kampaně, ale poskytuje také nástroje ke zlepšení naší schopnosti je odhalovat, analyzovat a bojovat proti nim;

- J. vzhledem k tomu, že zásada, podle níž by měla průmyslová odvětví finančně přispívat k řešení externalit souvisejících s jejich činností, je zakotvena v právu a praxi Unie; vzhledem k tomu, že podle rámce rozšířené odpovědnosti výrobce jsou někteří výrobci povinni financovat nakládání s odpady vzniklými jejich výrobky, a to v přímém souladu se zásadou „znečišťovatel platí“; vzhledem k tomu, že v rámci jednotného mechanismu pro řešení krizí platí všechny banky působící v bankovní unii roční příspěvky do Jednotného fondu pro řešení krizí, aby systémová rizika spojená s jejich činností nenesli daňoví poplatníci; vzhledem k tomu, že farmaceutické společnosti jsou povinny financovat preregistrační studie bezpečnosti na základě toho, že ti, kdo mají z uvedení výrobku na trh prospěch, musí přispívat k monitorování škod, které může dotýčný výrobek způsobit; vzhledem k tomu, že tato logika by se měla vztahovat na velké poskytovatele služeb informační společnosti, kteří mají prospěch z informačního ekosystému a zároveň vytvářejí systémová rizika pro demokratickou integritu;
- K. vzhledem k tomu, že EU se při několika příležitostech úspěšně orientovala v právně sporných a nově vznikajících oblastech politiky prostřednictvím strukturovaných přípravných nástrojů; vzhledem k tomu, že mezi významné příklady patří mimo jiné Zelená kniha o autorském právu a technologické výzvě z roku 1988, odborná skupina na vysoké úrovni pro umělou inteligenci a předlegislativní konzultační proces předcházející obecnému nařízení o ochraně osobních údajů⁶⁰; vzhledem k tomu, že zahraniční manipulace s informacemi a vměšování a dezinformace představují srovnatelnou výzvu související s technologickými, mezinárodními vztahy a obchodními modely, které se vyvíjejí společně se společenskými a právními jevy a zároveň konkurují ústavním hlediskům; vzhledem

⁶⁰ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>).

k tomu, že individuálně uzpůsobený víceoborový přípravný proces by mohl mít zásadní význam pro pevný, soudně přezkoumatelný legislativní rámec týkající se zahraniční manipulace s informacemi a vměšování a dezinformací, a to při plném respektování pravomocí členských států a pravomocí orgánů EU;

- L. vzhledem k tomu, že demokratické společnosti v EU jsou stále častěji terčem hybridních hrozeb, dezinformací a zahraniční manipulace s informacemi a vměšování, a to zejména v digitální sféře; vzhledem k tomu, že online prostor umožňuje šíření nových manipulačních technik, jež zahrnují: a) neautentické používání sociálních médií prostřednictvím automatizovaných softwarových programů, falešných účtů na sociálních médiích a využívání trollových továren, zesilování a zapojení pomocí botů, b) používání technik astroturfingu a floodingu k ovlivňování veřejné debaty online, c) personalizaci, sledování a mikrotargeting jednotlivců, d) webové stránky navržené tak, aby napodobovaly oficiální zdroje, e) umělé zesilování a monetizaci rozdělovacího obsahu, f) využívání syntetického obsahu, jako jsou deepfakes a jiný obsah generovaný umělou inteligencí, g) doporučovací systémy navržené tak, aby podněcovaly zapojení prostřednictvím polarizace, a h) manipulaci s velkými jazykovými modely a další techniky kontaminace dat, které zlovolně nahrávají předpojaté, klamavé nebo falešné narativy do systémů AI s cílem ovlivnit jejich trénink; vzhledem k tomu, že byly vyvinuty nástroje pro boj proti těmto technikám a negativním jevům, které jsou však stále velmi nedostatečné;
- M. vzhledem k tomu, že on-line platformy mají díky poznatkům o preferencích a zranitelnosti každého jednotlivého uživatele větší vliv na veřejný diskurz než tradiční vydavatelé; vzhledem k tomu, že důkazy naznačují, že algoritmy platform mohou jejich vlastníci a akcionáři manipulovat s cílem upřednostnit určitý politický obsah, čímž narušují informační prostředí a podkopávají možnost uživatelů získávat přesné a pluralitní informace; vzhledem k tomu, že velmi velké online platformy a velmi velké vyhledávače se staly de facto strážci veřejného prostoru, čímž výrazně ovlivňují, s jakými informacemi se občané setkávají, jak jsou upřednostňovány a za jakých podmínek se šíří;
- N. vzhledem k tomu, že EU a její členské státy nedávno přijaly soubor komplexních právních aktů s cílem vytvořit bezpečný a transparentní online prostor, včetně nařízení o digitálních službách, nařízení o digitálních trzích, nařízení o transparentnosti a cílení politické reklamy, evropského aktu o svobodě médií a aktu o umělé inteligenci; vzhledem k tomu, že tyto činy znamenají významný pokrok, pokud jde o pohnání online platform k odpovědnosti a ochranu demokratických procesů, zvýšení transparentnosti a ochranu svobody projevu, a tím přispívají ke komplexní obraně proti zahraniční manipulaci s informacemi a vměšování, ale jejich účinnost závisí na plném, včasném a důsledném prosazování, které je

i nadále náročné a pomalé a vytváří zranitelná místa; vzhledem k tomu, že strukturovaná podpora členských států v tomto ohledu je proto obzvláště důležitá; vzhledem k tomu, že EU a její členské státy by rovněž měly pokračovat ve vypracovávání nelegislativních opatření, společných přístupů a metodik s cílem narušit zahraniční manipulaci s informacemi a vměšování a bránit demokracii; vzhledem k tomu, že Parlament hraje významnou úlohu při kontrole a posilování právních předpisů EU v digitální oblasti a že toto úsilí by mělo být doplněno pravidelnými přezkumy pracovních metod Parlamentu, aby byla zajištěna účinnost;

- O. vzhledem k tomu, že z důkazů vyplývá, že doporučovací systémy velmi velkých online platform založené na angažovanosti, včetně platform X, TikTok a Instagram, jsou strukturálně motivovány ekonomikou založenou na pozornosti s cílem zesílit rozdělující, polarizující nebo zavádějící obsah, což představuje riziko pro občanský diskurz a integritu voleb, o čemž svědčí nárůst extremistického politického obsahu během voleb v celé EU; vzhledem k tomu, že tyto systémy oslabují viditelnost redakčně nezávislých a pluralitních sdělovacích prostředků a usnadňují rychlé šíření deepfakes vytvořených umělou inteligencí a syntetického nebo zmanipulovaného obsahu, což zhoršuje schopnost uživatelů, zejména zranitelných skupin, rozlišovat mezi pravdivými a nepravdivými informacemi; vzhledem k tomu, že akt o umělé inteligenci zavedl pravidla pro povinné označování obsahu vytvořeného umělou inteligencí; vzhledem k tomu, že články 34 a 35 nařízení o digitálních službách vyžadují, aby velmi velké online platformy posuzovaly a zmírňovaly systémová rizika; vzhledem k tomu, že nařízení o digitálních službách rovněž zavedlo nová důležitá pravidla pro zvýšení algoritmické transparentnosti a odpovědnosti, včetně možnosti uživatelů zvolit si nepersonalizované kanály, čímž se snížila závislost na neprůhledném algoritmickém kurátorství; vzhledem k tomu, že přetrvávají problémy v oblasti provádění a zkušeností uživatelů; vzhledem k tomu, že účinné prosazování nařízení o digitálních službách a aktu o umělé inteligenci, podpořené aktuálními pokyny a nezávislým dohledem, má zásadní význam pro boj proti manipulaci a ochranu demokratických procesů;
- P. vzhledem k tomu, že vláda USA uvalila cílené sankce, vyhrožuje cly, zakázala vydávat víza a uvalila osobní sankce vůči subjektům EU zapojeným do utváření a prosazování nařízení o digitálních službách a dalších právních předpisů v digitální oblasti, což narušuje integritu rozhodování EU a právní stát; vzhledem k tomu, že EU jako otevřený jednotný trh založený na pravidlech musí dodržovat své svrchované právo přijímat právní předpisy v souladu s demokratickými hodnotami, mezinárodními závazky a ochranou základních práv, včetně svobody projevu, která je základní hodnotou sdílenou se Spojenými státy a podobně smýšlejícími partnery v celém demokratickém světě; vzhledem k tomu, že nepodložená obvinění z cenzury podkopávají tyto sdílené hodnoty a odvádějí pozornost od

skutečného závažného porušování svobody projevu v zemích, jako je Rusko, Čína nebo Írán; vzhledem k tomu, že prosazování právních předpisů EU v digitální oblasti nesmí být narušováno zpožděním nebo omezením vyplývajícím z geopolitických úvah, zejména v případech zahrnujících lobbying ze strany velkých technologických platforem; vzhledem k tomu, že vnější tlak, včetně geoeconomického nátlaku, strategických akvizic a podpory extremistických hnutí veřejnými nebo podnikovými subjekty ze zemí mimo EU, dále ohrožuje rozhodovací svrchovanost a demokratickou odolnost EU; vzhledem k tomu, že prosazování digitálních pravidel EU se musí i nadále řídit výhradně právem Unie a ochranou demokratických zájmů, bez nepatřičného vlivu politických, obchodních nebo vnějších tlaků; vzhledem k tomu, že jednota mezi členskými státy EU a jejich politické sladění jsou v tomto ohledu klíčové;

- Q. vzhledem k tomu, že umělá inteligence je hnací silou inovací, přístupu ke znalostem, produktivity a nových digitálních odvětví a přináší nové příležitosti, jako je posílení řízení voleb a dohledu nad nimi prostřednictvím odhalování neobvyklé činnosti na internetu a koordinovaného manipulativního chování; vzhledem k tomu, že používání umělé inteligence, včetně generativních modelů a deepfakes, představuje rovněž významné výzvy pro integritu informací a volební procesy, a vyžaduje tak včasné a účinné demokratické záruky a regulatorní dohled; vzhledem k tomu, že důvěryhodné zprávy odhalily činnost moskevské dezinformační sítě známé jako „Pravda“, která se záměrně zaměřila na LLM a infiltrovala je prokremelskými narativy, které měly napodobovat neutrální a na faktech založené výstupy; vzhledem k tomu, že takové taktiky představují nebezpečný vývoj zahraniční manipulace s informacemi a vměšování, protože využívají neprůhlednost a škálovatelnost systémů umělé inteligence k nenápadnému šíření falešných nebo zavádějících geopolitických zpráv pod rouškou autoritativního jazyka a oslabují politický diskurz a důvěru v digitální technologie; vzhledem k tomu, že tato forma algoritmické manipulace ohrožuje důvěru veřejnosti v technologie umělé inteligence, narušuje demokratickou diskusi a zvyšuje riziko dezinformací napříč EU i na celém světě; vzhledem k tomu, že to je proto třeba zlepšit gramotnost v oblasti umělé inteligence ve vzdělávání, v práci a ve společnosti obecně, zvýšit transparentnost v souvislosti s odbornou přípravou LLM a dostatečně financovat výzkum; vzhledem k tomu, že výstupy umělé inteligence mohou odrážet předpojatost zaváděnou prostřednictvím návrhu systémů;
- R. vzhledem k tomu, že důležitou roli při posilování digitální odolnosti našich společností mohou hrát online influenceri, kteří zvyšují povědomí o mediální gramotnosti a demokratických postupech, podporují obsah založený na faktech a přispívají ke zdravé politické debatě; vzhledem k tomu, že rostoucí podíl občanů, zejména nezletilých a mladých dospělých, se zároveň ve velké míře spoléhá na tvůrce obsahu a influencers v sociálních médiích, herních službách

a službách pro sdílení videonahrávek a obsahu, a to i pokud jde o zprávy a aktuální informace, čímž se vystavuje rizikům spojeným s návykovým designem, škodlivým obsahem a manipulativními praktikami; vzhledem k tomu, že on-line osobnosti a influenceři mohou mít významnou schopnost utvářet veřejné mínění a informační toky, aniž by se na ně vždy vztahovaly standardy odpovědnosti srovnatelné s těmi, které se vztahují na sdělovací prostředky;

- S. vzhledem k tomu, že prezidentské volby v Rumunsku na podzim roku 2024 odhalily značné slabiny v prostředí online informací, přičemž důvěryhodné zprávy poukazují na rozšířené používání falešných účtů, botů a algoritmicky zesilovaného obsahu k prosazování konkrétních politických narativů a pokřívání volební soutěže; vzhledem k tomu, že TikTok, jedna z nejčastěji používaných platforem mezi mladými voliči, tvrdila, že zablokovala vytvoření více než 116 000 spamových účtů a v rámci povolebního úklidu odstranila 59 000 falešných účtů; vzhledem k tomu, že využívání influencerů, včetně nano a mikroinfluencerů, zahraničními aktéry dále poukazuje na to, že levní a málo viditelní aktéři mohou být zneužiti k tomu, aby se vyhnuli odhalení a ovlivňovali veřejné mínění, což je v rozporu s demokratickými normami; vzhledem k tomu, že důkazy poukazují na dva hlavní operační modely: koordinovanou manipulaci s doporučovacími algoritmy prostřednictvím sítí synchronizovaných účtů vytvářejících umělý provoz a zesilování trendů a skryté účelové využívání tvůrců obsahu, přičemž oba vzorce ukazují, jak lze využít dynamiku technických platforem a obcházet demokratické záruky;
- T. vzhledem k tomu, že Telegram, platforma pro zasílání zpráv s rostoucí uživatelskou základnou v EU, je stále častěji označován za prostředek šíření dezinformací, zahraničního vměšování a nezákonných činností, včetně šíření extremistického obsahu, náboru za účelem sabotáže, politické propagandy a dezinformací týkajících se unijních a vnitrostátních právních předpisů; vzhledem k tomu, že původ Telegramu v Rusku, jeho neprůhledná vlastnická struktura a nedostatečná moderace jeho obsahu vyvolávají trvalé obavy ohledně jeho role při podbývání demokratické diskuse; vzhledem k tomu, že Telegram se stal primárním kanálem pro nábor „jednorázových agentů“ a provádění hybridních operací; vzhledem k tomu, že bylo zjištěno, že zlovolní státní aktéři využívají technologické dovednosti, finanční potřeby a naivitu uživatelů Telegramu, zejména mladých lidí, k provádění špionážních a sabotážních operací s minimálními náklady, přičemž mohou vše nadále věrohodně popírat; vzhledem k tomu, že zprávy naznačují, že Telegram splňuje prahovou hodnotu počtu uživatelů, aby mohl být klasifikován jako velmi velká online platforma (VLOP) podle nařízení o digitálních službách, což jej podrobuje přísnějším regulačním povinnostem a požadavkům na zmírňování rizik; vzhledem k tomu, že zdlouhavé hodnocení Komise dosud nedospělo k žádnému závěru;

- U. vzhledem k tomu, že rostoucí vliv mimoevropských technologických společností – zejména těch se sídlem ve Spojených státech a Číně – poukázal na strategickou závislost EU v kritických oblastech, jako jsou datová infrastruktura, družicová komunikace, cloudové služby, online platformy, platební řešení a počítačový software, mimo jiné v odvětvích, jako je obrana; vzhledem k tomu, že podpora domácích inovací, zajištění spravedlivých a konkurenceschopných digitálních trhů, prosazování souboru digitálních pravidel, podpora evropských startupů a investice do suverénní digitální infrastruktury jsou základními kroky k vybudování konkurenceschopného, bezpečného, odolného a nezávislého digitálního ekosystému EU, které zároveň omezují příležitosti k nepřátelskému vměšování, manipulaci s informacemi a hospodářskému nátlaku; vzhledem k tomu, že sladění digitálních inovací s demokratickými hodnotami a základními právy nabízí EU příležitost stát se světovým lídrem v oblasti odpovědných a na člověka zaměřených technologií; vzhledem k tomu, že umělá inteligence mění a urychluje globalizaci a vytváří novou fázi strategické hospodářské soutěže; vzhledem k tomu, že digitální suverenity EU je obzvláště obtížné dosáhnout, pokud velmi velké online platformy a velmi velké internetové vyhledávače fungují ve faktickém oligopolním stavu;
- V. vzhledem k tomu, že výzkum ukazuje znepokojivý trend v programech přerozdělování příjmů online platforem a odhaluje, že mediální subjekty, na něž se vztahují sankce, jako jsou Sputnik a Russia Today, zůstaly i několik měsíců po zavedení sankcí EU proti Rusku uvedeny na Facebooku jako „partnerské vydavatelské společnosti“, což vyvolává otázky, zda nadále z této účasti těží finančně; vzhledem k tomu, že takové neprůhledné mechanismy monetizace umožňují zahraničním subjektům napojeným na stát profitovat ze šíření dezinformací a i přes regulační opatření nadále destabilizovat unijní a vnitrostátní informační prostory; vzhledem k tomu, že netransparentní povaha internetové reklamy umožňuje přesouvat velké finanční částky z legitimních značek na dezinformační stránky, financovat polarizující obsah a podkopávat kvalitní žurnalistiku; vzhledem k tomu, že společnost Meta je jedinou významnou technologickou společností, která zveřejňuje omezené údaje o svých monetizačních mechanismech, zatímco jiné online platformy zůstávají netransparentní;
- W. vzhledem k tomu, že v průzkumu provedeném v předvečer parlamentních voleb v Nizozemsku v roce 2025 jeden z deseti respondentů uvedl, že by se pravděpodobně obrátil na AI s žádostí o radu ohledně hlasování, přičemž dalších 13 % respondentů uvedlo, že by se na ni možná obrátilo; vzhledem k tomu, že v Nizozemsku více než třetina nejmladších respondentů odpověděla, že je pravděpodobné, že budou nebo by mohli využívat umělou inteligenci pro poradenství při hlasování; vzhledem k tomu, že tento trend odpovídá zjištěním ve všech členských státech i na celosvětové úrovni; vzhledem k tomu, že údaje nizozemského orgánu na ochranu

údajů prokazují, že doporučení ohledně hlasování generovaná chatboty s umělou inteligencí často představují velmi zkreslený a polarizovaný pohled na politickou scénu; vzhledem k tomu, že investice do vývoje LLM s otevřeným zdrojovým kódem jsou jedním ze způsobů, jak snížit obavy ze skrytých předsudků, z průniku do bezpečnostních systémů nebo zneužívání dat v chatbotech umělé inteligence;

- X. vzhledem k tomu, že aktéři zahraniční manipulace s informacemi a vměšování využívají technologie k organizování koordinovaných kampaní založených na nepravdivých informacích; vzhledem k tomu, že tyto technologie, zejména boty a softwarové programy založené na umělé inteligenci, jsou schopny vykazovat autonomní chování a následně narušovat a ničit skutečnou veřejnou diskusi tím, že zaplavují komunikaci skutečných osob neautentickým obsahem;
- Y. vzhledem k tomu, že základní právo na svobodu projevu a informací, zakotvené v článku 19 Všeobecné deklarace lidských práv, v článku 11 Listiny základních práv Evropské unie a v článku 10 Evropské úmluvy o lidských právech, je základním kamenem demokracie; vzhledem k tomu, že závazek EU k svobodě projevu představuje soudržnou a principiální strategii proti zahraniční manipulaci s informacemi a vměšování, která je v jasném kontrastu s omezeními, která autoritářské subjekty systematicky ukládají svým obyvatelům; vzhledem k tomu, že svoboda a pluralita sdělovacích prostředků a existence živého občanského prostoru umožňují společností odhalovat a odmítat manipulativní narativy prostřednictvím demokratické diskuse;
- Z. vzhledem k tomu, že svoboda projevu a informací je základním právem, jehož účelem je chránit lidi, nikoli stroje, algoritmy, boty nebo umělou inteligenci;
- AA. vzhledem k tomu, že autoritářské režimy využívají platformy sociálních médií k oslabování svobody projevu; vzhledem k tomu, že uživatelé očekávají transparentnost, řádný proces a ochranu svobody projevu, které musí být v souladu s požadavky nařízení o digitálních službách dodržovány; vzhledem k tomu, že k ochraně těchto zásad je proto nezbytné plné prosazování právních předpisů EU v digitální oblasti;
- AB. vzhledem k tomu, že svoboda projevu a informací a svoboda a pluralita sdělovacích prostředků, zakotvené v čl. 11 odst. 2 Listiny základních práv Evropské unie a v článku 10 Evropské úmluvy o lidských právech, jsou základním kamenem demokracie a odolných společností; vzhledem k tomu, že redakčně nezávislá, kvalitní, na faktech založená, dobře financovaná a komerčně životaschopná žurnalistika, včetně práce novinářů v exilu, je klíčovou ochranou proti zahraniční manipulaci s informacemi a vměšování

a dezinformacím a nezbytným nástrojem pro informované rozhodování;

- AC. vzhledem k tomu, že orgány EU v politických a operačních dokumentech pravidelně používají pojem „informační integrita“, vzhledem k tomu, že na úrovni EU nebyla stanovena žádná oficiální ani společně dohodnutá definice tohoto pojmu; vzhledem k tomu, že tato chybějící definice může vést k možným nejasnostem při jejím výkladu a uplatňování;
- AD. vzhledem k tomu, že Evropský akt o svobodě médií představuje milník v podpoře nezávislého a pluralitního mediálního prostředí v celé Evropě; vzhledem k tomu, že sdělovací prostředky plní demokratickou funkci odlišnou od funkce běžných obchodních subjektů; vzhledem k tomu, že k ochraně redakční nezávislosti a zajištění transparentnosti, odpovědnosti zdrojů a profesních standardů jsou nezbytné spolehlivé záruky, zejména v případech koncentrace vlastnictví, převzetí nebo změn kontroly; vzhledem k tomu, že Komise by měla usilovat o lepší zapojení kandidátských zemí do mediální politiky EU; vzhledem k tomu, že by to mělo rovněž zahrnovat odpovídající závazek samotných kandidátských zemí;
- AE. vzhledem k tomu, že ekosystém digitální reklamy sice přináší nové příležitosti pro mediální dosah, ale zároveň vede ke koncentraci trhu a nekalé hospodářské soutěži, přičemž několik velkých online platforem získává nepřiměřený podíl na příjmech z reklamy; vzhledem k tomu, že podle zprávy francouzského úřadu ARCOM a ministerstva kultury z roku 2023 získaly mediální organizace investující do zpravodajského obsahu a audiovizuální tvorby v roce 2022 pouze 40 % příjmů z reklamy, což je pokles oproti 65 % v roce 2012, a předpokládá se, že tento podíl do roku 2030 klesne na 29 %; vzhledem k tomu, že to často poškozuje profesionální evropské mediální společnosti a udržitelnost nezávislé žurnalistiky;
- AF. vzhledem k tomu, že nekalé praktiky dominantních účastníků internetového reklamního trhu, jako jsou praktiky, na jejichž základě uložila Komise společnosti Google pokutu ve výši 2,95 miliardy EUR za narušení hospodářské soutěže v oblasti internetové reklamy, poukazují na potřebu strukturálnějších opatření k zajištění spravedlivé hospodářské soutěže, větší transparentnosti, odpovědnosti a záruk na ochranu plurality sdělovacích prostředků, redakční nezávislosti a integrity demokratických procesů; vzhledem k tomu, že strukturální nedostatky na trhu s digitální reklamou mohou být zneužity nepřátelskými subjekty, jak dokazují kampaně typu „doppelpgänger“, které cílí na uživatele sociálních médií, a řada ruských online kampaní, jejichž cílem je, aby ukrajinští muži odmítali narukovat do vojska;
- AG. vzhledem k tomu, že nařízení o digitálních trzích má zásadní význam pro zajištění spravedlivých digitálních trhů a plurality sdělovacích

prostředků; vzhledem k tomu, že jeho provádění je stále provázáno problémy; vzhledem k tomu, že podle nařízení o digitálních trzích mohou vývojáři aplikací bezplatně informovat zákazníky o nabídkách mimo obchody s aplikacemi (app stores); vzhledem k tomu, že Komise vyšetřuje možné porušení nařízení o digitálních trzích ze strany společnosti Google degradací mediálního obsahu; vzhledem k tomu, že Komise zahájila první přezkum nařízení o digitálních trzích dne 3. července 2025;

- AH. vzhledem k tomu, že směrnice o audiovizuálních mediálních službách reguluje audiovizuální mediální služby, čímž zajišťuje ochranu spotřebitele a plní další cíle veřejného zájmu na audiovizuálním mediálním trhu; vzhledem k tomu, že tato směrnice vyžaduje, aby členské státy přijaly opatření pro rozvoj dovedností v oblasti mediální gramotnosti a aby o svých krocích každé tři roky podávaly zprávu; vzhledem k tomu, že Komise v současné době směrnicí vyhodnocuje, přičemž v listopadu 2025 požádala o příspěvky v rámci přípravy nového posouzení plánovaného na rok 2026;
- AI. vzhledem k tomu, že je třeba vybavit děti dovednostmi, které jim umožní rozpoznávat dezinformace; vzhledem k tomu, že nepřátelské subjekty mohou intenzivněji cílit v této souvislosti na vzdělávací systémy, aby úsilí o zvýšení digitální gramotnosti zmařily; vzhledem k tomu, že některé skupiny obyvatel jsou z různých důvodů vůči dezinformacím obzvláště zranitelné, včetně dětí a mladých lidí, a to z důvodu jejich vysoké expozice digitálním technologiím; vzhledem k tomu, že mediální gramotnost a kritické myšlení je třeba podporovat již od raného věku;
- AJ. vzhledem k tomu, že středisko EDMO hraje klíčovou úlohu při monitorování dezinformací a boji proti nim; vzhledem k tomu, že mandát střediska EDMO byl prodloužen, aby mohlo ve své důležité práci pokračovat; vzhledem k tomu, že v souvislosti s prodloužením jeho mandátu ovšem nebyly odpovídajícím způsobem navýšeny jeho finanční zdroje, což může omezit schopnost střediska plnit své cíle;
- AK. vzhledem k tomu, že dočasná povaha programu pro odolnost sdělovacích prostředků by mohla být příležitostí ke zvážení nových inovativních způsobů, jak podpořit nezávislé místní a regionální sdělovací prostředky;
- AL. vzhledem k tomu, že mechanismus rychlé reakce na porušování svobody médií zaznamenal v roce 2025 celkem 1 481 případů porušení svobody tisku, které se týkaly 2 377 osob nebo subjektů působících v mediální oblasti ve 36 evropských zemích a které zahrnovaly právní, fyzické a psychické výhrůžky a různé formy cenzury; vzhledem k tomu, že ačkoli ve srovnání s 1 548 případy, které byly zaznamenány v roce 2024, jde o mírný pokles, zůstává míra porušování svobody tisku na znepokojivě vysoké úrovni, která je mnohem vyšší než v roce 2023, což poukazuje na přetrvávající

a systémové ohrožení svobody sdělovacích prostředků v Evropě; vzhledem k tomu, že vraždy investigativních novinářů, např. Jana Kuciaka, Giorgose Karaivaze, Petera R. de Vriese a Daphne Caruanové Galiziové, vyvolaly u veřejnosti velké pobouření;

- AM. vzhledem k tomu, že vyjednávači Parlamentu a Rady dosáhli dne 11. prosince 2025 předběžné dohody o navrhovaném nařízení o prověřování zahraničních investic v EU;
- AN. vzhledem k tomu, že pro EU má strategický význam Rádio Svobodná Evropa / Rádio Svoboda; vzhledem k tomu, že v reakci na reformu politiky zahraniční pomoci Spojených států schválila EU na činnost Rádía Svobodná Evropa / Rádía Svoboda mimořádné finanční prostředky ve výši 5,5 milionu EUR; vzhledem k tomu, že pro tuto stanici i další nezávislé sdělovací prostředky, které mají zásadní význam pro posílení demokratické odolnosti v sousedních zemích, je nutno najít udržitelný způsob financování;
- AO. vzhledem k tomu, že nové technologie, jako je umělá inteligence, mohou zlepšit pracovní podmínky a postupy práce novinářů, ale zároveň mohou novináře vystavit novým rizikům vzhledem k možnosti rychle a levně falšovat produkci reálných mediálních subjektů, ke kampaním typu „doppelgänger“, masovému vytváření dezinformačních kanálů a ke koordinovaným útokům, jež jsou proti novinářům vedeny; vzhledem k tomu, že falšování produkce reálných mediálních subjektů představuje krádež identity a musí být jako takové řešeno soudními orgány; vzhledem k tomu, že modely umělé inteligence musí být v souladu s autorským právem Unie, aby byla zajištěna ochrana nositelů práv a právní jistota; vzhledem k tomu, že zpravodajská média čelí výzvám vyplývajícím z rostoucího vlivu systémů umělé inteligence, což подрývá důvěru veřejnosti, příjmy z reklamy a ochranu autorských práv; vzhledem k tomu, že situace v oblasti generativní umělé inteligence by měla být projednána v souvislosti s nadcházejícím přezkumem, který Komise provede u směrnice EU o autorském právu⁶¹, a že by měla být vydána zpráva obsahující její hlavní zjištění; vzhledem k tomu, že v souvislosti s mediální politikou je důležitá větší transparentnost ohledně trénovacích dat umělé inteligence;
- AP. vzhledem k tomu, že změny týkající se Agentury Spojených států pro mezinárodní rozvoj (USAID) postihly řadu evropských sdělovacích prostředků; vzhledem k tomu, že v této situaci je posílení vlastního evropského mediálního prostředí o to důležitější; vzhledem k tomu,

⁶¹ Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES (Úř. věst. L 130, 17.5.2019, s. 92, ELI: <http://data.europa.eu/eli/dir/2019/790/oj>).

že financování EU by se mělo zaměřit na iniciativy s největším dopadem na veřejnost a zahrnovat základní operační podporu;

- AQ. vzhledem k tomu, že kvůli opatřením přijatým předchozí maďarskou vládou strany Fidesz zahájila Komise s Maďarskem řízení o nesplnění povinnosti kvůli nedodržování Evropského aktu o svobodě sdělovacích prostředků a směrnice o audiovizuálních mediálních službách;
- AR. vzhledem k tomu, že probíhající ruská útočná válka proti Ukrajině ukazuje, jak zásadní úlohu hraje občanská společnost v krizových situacích, zejména pokud jde o poskytování humanitární pomoci, zajištění základních potřeb, každodenní život postiženého obyvatelstva a reakce na hrozby spojené se sabotážní a špionážní činností;
- AS. vzhledem k tomu, že občanská společnost rovněž zásadním způsobem přispívá k tvorbě politik, poskytování sociálních a komunitních služeb, zvyšování povědomí o důležitých sociálních otázkách, zvyšování odolnosti, zastupování různých skupin v ohrožených situacích a prosazování a ochraně základních práv občanů a při zajišťování toho, aby vlády zůstaly transparentní a odpovědné prostřednictvím veřejné kontroly a demokratického dohledu;
- AT. vzhledem k tomu, že Komise zveřejnila Strategii EU pro občanskou společnost, která má doplňovat opatření stanovená ve společném sdělení o Evropském štítu pro demokracii; vzhledem k tomu, že Strategie EU pro občanskou společnost potvrzuje, že platforma občanské společnosti, která má být zřízena jako součást provádění strategie, bude mít za cíl poskytnout řádný strukturovaný rámec pro ochranu a prosazování hodnot EU a efektivnější a intenzivnější úsilí v oblasti základních práv, demokracie, rovnosti a právního státu a bude funkční v roce 2026; vzhledem k tomu, že tato strategie zahrnuje také vytvoření online znalostního centra pro občanský prostor, které by mělo evidovat stávající iniciativy v oblasti monitorování občanského prostoru, zprávy a zdroje na ochranu na vnitrostátní, evropské a mezinárodní úrovni ve spolupráci s Agenturou Evropské unie pro základní práva;
- AU. vzhledem k tomu, že financování demokratické odolnosti by mělo být posíleno a využíváno koordinovaným a účinným způsobem s cílem dosáhnout maximálního dopadu a zároveň respektovat nezávislost dotčených subjektů; vzhledem k tomu, že program AgoraEU, který Komise navrhla pro víceletý finanční rámec (VFR) na období 2028–2034 s navrhovaným rozpočtem 9 miliard EUR, představuje důležitý krok vpřed při posilování podpory EU pro kulturu, sdělovací prostředky a občanskou společnost;

- AV. vzhledem k tomu, že společnosti, které účinně investují do lidského kapitálu a vzdělávání, patří k nejkonkurenceschopnějším, nejodolnějším a ekonomicky nejsilnějším; vzhledem k tomu, že programy, jako je Erasmus+, podporují evropské hodnoty a posilují demokratickou angažovanost mladých lidí a odolnost společnosti v celé EU;
- AW. vzhledem k tomu, že nepřátelské subjekty třetích zemí se snaží zasahovat do činnosti Parlamentu a uplatňovat na něj nepatřičný vliv, a to i prostřednictvím nezákonného lobbování a korupčních praktik, o čemž svědčí např. kauza „Qatargate“; vzhledem k tomu, že tento vývoj zdůrazňuje potřebu dále posilovat odolnost a integritu rozhodovacích procesů EU;
- AX. vzhledem k tomu, že francouzské ministerstvo vnitra zveřejnilo zprávu o Muslimském bratrstvu, která se zabývá znepokojivou skrytou vlivovou činností a infiltrací islamistů; vzhledem k tomu, že podobné obavy byly vyjádřeny i v souvislosti s dalšími náboženskými aktéry, jako je ruská pravoslavná církev (Moskevský patriarchát);
- AY. vzhledem k tomu, že hybridní útoky zaměřené na kritickou infrastrukturu v EU jsou častější než kdykoli předtím, přičemž tyto incidenty souvisejí se stejnými nepřátelskými třetími zeměmi, jako jsou Rusko, Bělorusko a Čína, ale také Írán a Severní Korea; vzhledem k tomu, že ve stále nestabilnějším geopolitickém prostředí musí být EU rovněž připravena na hybridní hrozby, které s těmito aktéry nesouvisejí; vzhledem k tomu, že častým cílem jejich útoků jsou základní systémy, sítě a zařízení, které jsou životně důležité pro fungování společnosti, a to i v souvislosti s veřejnou bezpečností, ochranou a hospodářskou stabilitou; vzhledem k tomu, že tyto útoky mají různé podoby a formy, od fyzické sabotáže, přes žhářství, špionáž, rušení signálu až po kybernetické útoky a jiné aktivity v šedé zóně, což svědčí o koordinované snaze testovat, podbíjet a oslabovat bezpečnost a společenskou odolnost EU; vzhledem k tomu, že tyto útoky upozorňují na nutnost urychleně odstranit nebezpečné mezery v systému;
- AZ. vzhledem k tomu, že útoky na železniční infrastrukturu ohrožují životy a bezpečnost občanů a narušují strategické logistické sítě, jak tomu bylo v případě bezprecedentní sabotáže polské železniční infrastruktury na strategické trase Varšava-Lublin, která měla způsobit železniční katastrofu a potenciálně způsobit úmrtí mnoha osob; vzhledem k tomu, že ruská vojenská zpravodajská služba (GRU) provádí soustavnou sabotáž ve všech členských státech EU a v minulosti stála mimo jiné za výbuchem muničních skladů ve Vrběticích (Česko) v roce 2014 a za útoky na kritickou infrastrukturu v Litvě, které provedly kubánští občané, kteří byli pro tyto sabotážní operace najati;

- BA. vzhledem k tomu, že v Baltském moři došlo k bezprecedentnímu nárůstu počtu případů poškozování podmořských kabelů, které jsou nezbytné pro zajištění internetové konektivity a dodávky elektřiny v celém baltském a severském regionu; vzhledem k tomu, že od roku 2023 bylo zaznamenáno nejméně 11 případů tohoto poškození, což naznačuje, že jde o koordinovanou sabotáž; vzhledem k tomu, že navrhovaný akt o digitálních sítích zahrnuje závazné povinnosti pro provozovatele podmořských kabelů v oblasti odolnosti na úrovni EU, včetně povinného dodržování bezpečnostních požadavků pro dodavatelské řetězce IKT podle revidovaného návrhu aktu o kybernetické bezpečnosti; vzhledem ke zřízení nového střediska námořního dohledu v Baltském moři pod vedením Finska, baltských spojenců a Komise, jehož smyslem je chránit kritickou podmořskou infrastrukturu; vzhledem k tomu, že přítomnost ruských lodí v irských vodách se od začátku ruské plošné invaze na Ukrajinu v roce 2022 výrazně zvýšila, což vyvolává obavy o bezpečnost důležitých propojovacích kabelů mezi Irskem a Spojeným královstvím;
- BB. vzhledem k tomu, že ochrana klíčových námořních míst přispívá k demokratické odolnosti, neboť hybridní útoky proti těmto uzlům mohou vést k vážným hospodářským, sociálním a bezpečnostním problémům; vzhledem k tomu, že čínské společnosti se silnými vazbami na Komunistickou stranu Číny mají nyní podíly ve více než 30 evropských námořních přístavních terminálech, často v těsné blízkosti evropských vojenských námořních základen; vzhledem k tomu, že ve společné bílé knize o budoucnosti evropské obrany 2030 se Komise a místopředsedkyně Komise, vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku zavázaly přezkoumat stávající právní předpisy EU a zavést přísnější pravidla týkající se vlastnictví a kontroly kritické dopravní infrastruktury;
- BC. vzhledem k tomu, že v posledních měsících bylo hlášeno několik případů narušení vzdušného prostoru a neoprávněného vniknutí dronů nad územím několika členských států EU a sousedních spojenců NATO, včetně Polska, pobaltských států, Rumunska, Dánska, Švédska, Německa, Belgie a Norska; vzhledem k tomu, že původci řady těchto incidentů jsou jednoznačně ruská vojenská letadla a drony, zatímco další incidenty, při nichž se objevily neurčené létající objekty, včetně pašeráckých balonů, které jsou používány pro nezákonnou přeshraniční činnost, jsou stále předmětem vyšetřování, ale všeobecně se má za to, že zapadají do stejného vzorce hybridního zastrašování a snah o destabilizaci v Evropě;
- BD. vzhledem k tomu, že několik evropských zemí, včetně Francie, Estonska, Německa, Polska, Česka a Norska, bylo v nedávné době terčem vážných kybernetických útoků a sabotáží zaměřených na vládní systémy, kritickou infrastrukturu a soukromé podniky, přičemž tyto útoky jsou připisovány nepřátelským třetím zemím,

včetně ruských vojenských zpravodajských služeb a subjektů napojených na čínskou vládu; vzhledem k tomu, že tyto útoky podtrhují naléhavou potřebu posílit kolektivní kybernetickou odolnost EU a její schopnost stanovit, který třetí stát nese za kybernetické útoky odpovědnost;

- BE. vzhledem k tomu, že závislost EU na zahraničních subjektech a technologiích zahraniční výroby v oblasti kritické infrastruktury a v rámci dodavatelských řetězců zůstává závažným problémem a představuje jednu z nejvýraznějších slabin EU; vzhledem k tomu, že tento jev je obzvláště rozšířený v technologickém a digitálním odvětví, což představuje klíčovou výzvu pro kybernetickou bezpečnost a evropskou strategickou autonomii;
- BF. vzhledem k tomu, že EU zůstává silně závislá na technologiích a finančních službách USA, což vystavuje evropská data a digitální infrastrukturu rizikům vyplývajícím z právních rámců USA, jako je zákon o cloudových službách (Cloud Act), zákon o dohledu nad zahraniční informační službou (Foreign Intelligence Surveillance Act) a vlastenecký zákon (Patriot Act), které poskytují orgánům USA široký přístup k údajům uchovávaným americkými společnostmi, a to i v případě, že jsou tyto údaje uloženy v EU; vzhledem k tomu, že Komise přijala v červenci 2023 rámec EU-USA pro ochranu údajů, který umožňuje volný pohyb osobních údajů mezi EU a Spojenými státy podle náležitých pravidel ochrany a poskytuje jednotlivcům z EU mechanismus pro přístup k nezávislému a neustrannému mechanismu nápravy v souvislosti se shromažďováním a využíváním jejich údajů zpravodajskými službami USA; vzhledem k tomu, že sama společnost Microsoft francouzskému senátu přiznala, že údaje EU před sledováním ze strany USA nemůže chránit;
- BG. vzhledem k tomu, že Španělsko zadalo společnosti Huawei zakázku na správu a ukládání dat ze soudně povolených odposlechů používaných donucovacími orgány i zpravodajskými službami; vzhledem k tomu, že Komise z bezpečnostních důvodů omezila přístup společnosti Huawei k sítím 5G v celé Evropské unii;
- BH. vzhledem k tomu, že všechny agentury federální vlády USA podléhají zásadě „Buy American“, tj. požadavku nakupovat přednostně domácí produkty; vzhledem k tomu, že rámec EU pro zadávání veřejných zakázek je odlišný a může v některých případech přispět k závislosti na produktech ze zemí mimo EU a prohloubit související rizika pro evropské podniky; vzhledem k tomu, že ačkoli jsou v mnoha případech k dispozici adekvátní evropské alternativy, Evropský parlament a další orgány EU nadále nakupují software a hardwarové produkty vyrobené mimo Evropu;
- BI. vzhledem k tomu, že Komise dne 20. ledna 2026 předložila revidovaný akt o kybernetické bezpečnosti, v němž navrhla závazné požadavky na řízení bezpečnosti dodavatelského řetězce IKT

v kritické infrastruktuře prostřednictvím systematického posuzování rizik a omezení vysoce rizikových dodavatelů ze zemí, které představují zvýšená bezpečnostní rizika; vzhledem k tomu, že tento nový rámec se od dobrovolného souboru bezpečnostních nástrojů pro síť 5G z roku 2020 posouvá k návrhu závazných povinností členských států; vzhledem k tomu, že navrhovaná revize aktu o kybernetické bezpečnosti by mohla výrazně, o více než 80 %, rozšířit operační mandát a rozpočet agentury ENISA, konkrétně pokud jde o koordinovanou reakci na kybernetické incidenty v reálném čase, systémy včasného varování a sdílení zpravodajských informací o hrozbách mezi členskými státy;

- BJ. vzhledem k tomu, že akt o digitálních sítích, který Komise navrhla dne 21. ledna 2026, zavádí dohled nad přidělováním spektra na úrovni EU, a to i ve vztahu k poskytovatelům družicových služeb, a odjímá právo poskytovat síť a služby v případech, kdy poskytovatel nesplňuje bezpečnostní požadavky návrhu revidovaného aktu o kybernetické bezpečnosti týkající se dodavatelského řetězce IKT; vzhledem k tomu, že kromě jiných kritických infrastruktur se kvůli prevenci scénáře selhání celého systému kvůli selhání jeho jediné části opírá i volební infrastruktura stále více o digitální síť a řadu různých komunikačních kanálů;
- BK. vzhledem k tomu, že bezfosilní energie je klíčovým odrazovým můstkem pro energetickou suverenitu Evropy; vzhledem k tomu, že podle analýzy zveřejněnou společností Wood Mackenzie v roce 2025 má devět z deseti největších světových dodavatelů solárních invertorů sídlo v Číně; vzhledem k tomu, že v čínských solárních invertorech používaných v Evropě a ve Spojených státech byla objevena skrytá komunikační zařízení; vzhledem k tomu, že podle českého úřadu pro kybernetickou bezpečnost je ohrožena ochrana údajů a v extrémních případech hrozí i dálková manipulace se solárními invertory; vzhledem k tomu, že solární elektrárny propojené prostřednictvím decentralizované husté sítě jsou náchylné ke kybernetickým útokům, a proto vyžadují přiměřenou kybernetickou ochranu;
- BL. vzhledem k tomu, že je hybridní útoky představují pro EU a její členské státy bezpečnostní hrozbu a mají významný dopad na demokracii; vzhledem k tomu, že záležitosti vnitřní bezpečnosti zůstávají v kompetenci členských států, avšak přeshraniční, propojená a mnohorozměrná povaha těchto útoků vyžaduje posílenou spolupráci, systematické sdílení informací a koordinovanou činnost na úrovni EU podpořenou odpovídajícím financováním; vzhledem k tomu, že Evropská strategie vnitřní bezpečnosti z dubna 2025 zdůrazňuje, že trestní právo EU se již vztahuje na určité formy zahraniční manipulace s informacemi a vměšování a dezinformačních činností a že posílená spolupráce EU může boj proti tomuto druhu jednání zefektivnit; vzhledem k tomu, že nástroje trestního práva

mohou posílit Evropský štít pro demokracii, pokud dotyčná činnost představuje podle platného právního řádu trestný čin;

- BM. vzhledem k tomu, že je třeba přizpůsobit a posílit mechanismy soudní a policejní spolupráce a nástroje pro přeshraniční výměnu informací s ohledem na rostoucí výzvy, které zahraniční vměšování pro vnitřní bezpečnost EU představuje; vzhledem k tomu, že k vedení a financování operací zahraničního vměšování jsou stále více využívány nové strategie teroristických a zločineckých organizací, což obnáší i využívání kryptoaktiv a komunikaci prostřednictvím různých digitálních kanálů, mimo jiné videoher nebo e-shopů, což umožňuje obcházet sankce a provádět nezákonné finanční transakce; vzhledem k tomu, že je proto třeba, aby orgány trestního soudnictví a donucovací orgány získaly informace o moderních vyšetřovacích metodách a technologiích a ohledně celého hodnotového řetězce manipulace a vměšování, aby mohly řádně shromažďovat, zpracovávat, uchovávat a používat důkazy v trestním řízení; vzhledem k tomu, že předávání osobních údajů do třetích zemí nebo mezinárodním organizacím, které je nezbytné pro účely spolupráce policie, trestního soudnictví nebo správy hranic, podléhá zvláštním podmínkám podle práva Unie a mělo proběhnout pouze tehdy, pokud lze zajistit integritu a bezpečnost těchto údajů;
- BN. vzhledem k tomu, že Europol ve své poslední zprávě EU-SOCTA zveřejněné v březnu 2025 varoval před zapojením zločineckých organizací do hybridních útoků, včetně dezinformačních kampaní; vzhledem k tomu, že Komise ve svém sdělení o programu ProtectEU uznává, že Europolu v plném využití jeho operačního potenciálu při podpoře činností zaměřených na boj proti přeshraniční trestné činnosti brání různé faktory, včetně toho, že mu chybí mandát pro činnost, pokud je o nové bezpečnostní hrozby, zejména sabotáž, hybridní hrozby a manipulaci s informacemi; vzhledem k tomu, že ve společném sdělení o Evropském štítu pro demokracii bylo oznámeno, že se revize mandátů Europolu i Agentury Evropské unie pro justiční spolupráci v trestních věcech (Eurojust) zaměří na způsoby, jak lze úsilí v boji proti zahraniční manipulaci s informacemi a vměšování a dezinformačním činnostem ještě zvýšit;
- BO. vzhledem k tomu, že se Komise zavázala zahájit reformu, která z Europolu učiní skutečně funkční policejní agenturu; vzhledem k tomu, že pracovníci donucovacích orgánů mají nejlepší možnost pozorovat destabilizující účinky, které mohou mít zahraniční manipulace s informacemi a vměšování a dezinformační kampaně na dotčené komunity; vzhledem k tomu, že proto může být jejich pomoc při ochraně demokratických institucí klíčová; vzhledem k tomu, že právní, profesní a etický rámec potřebný pro výkon této úlohy by měl být lépe definován a v celé EU lépe harmonizován;
- BP. vzhledem k tomu, že členské státy mohou Eurojust požádat o pomoc vnitrostátním orgánům při řešení jakéhokoli druhu protiprávního

jednání spadajícího do jejich jurisdikce; vzhledem k tomu, že soudní spolupráce může být obzvláště náročná, pokud se rozšiřuje na nové oblasti trestního práva, což vyžaduje modernizované právní nástroje;

- BQ. vzhledem k tomu, že situace na vnějších hranicích členských států s Ruskem a Běloruskem zůstává kvůli přetrvávajícím hybridním hrozbám stále znepokojivá; vzhledem k tomu, že agentury EU působící v oblasti spravedlnosti a vnitřních věcí hrají ve spolupráci s vnitrostátními orgány klíčovou úlohu, pokud jde o vytváření a udržování společného situačního povědomí o rizicích souvisejících s těmito hrozbami a pomoc příslušným členským státům na hranicích Unie, pokud se ocitnou v krizových situacích; vzhledem k tomu, že Komise zařadila posílení Evropské agentury pro pohraniční a pobřežní stráž mezi své stěžejní iniciativy pro legislativní období 2024–2029; vzhledem k tomu, že další iniciativy, jako je „Eastern Flank Watch“, mohou přispět k posílení ochrany vnějších hranic a ke zvýšení odolnosti vůči hybridním hrozbám;
- BR. vzhledem k tomu, že nadnárodní represe zahrnují systematické zastrašování a pronásledování ze strany orgánů třetích zemí nebo jejich zástupců, které se zaměřuje na novináře a aktivisty, obránce lidských práv, politické oponenty a členy diaspor žijících v EU, přičemž příkladem může být právní šikana ukrajinských novinářů ze strany Ruska, turecké a ázerbájdžánské pokusy o umlčení opozice a útoky plánované proti běloruské diaspoře v Litvě; vzhledem k tomu, že rostoucí dohled nad obránci lidských práv by měl být považován za formu nadnárodní represe; vzhledem k tomu, že tyto praktiky nejen narušují bezpečnost dotčených osob a porušují jejich základní práva, ale také podkopávají svrchovanost a bezpečnost EU a členských států, demokratické svobody a právní stát; vzhledem k tomu, že obětem nadnárodních represí v EU by měla být i nadále poskytována ochrana;
- BS. vzhledem k tomu, že kandidátské země a země v sousedství EU, zejména Ukrajina, Moldavsko, Arménie, Gruzie a země západního Balkánu, zůstávají i nadále terčem zahraniční manipulace s informacemi a vměšování a hybridních hrozeb; vzhledem k tomu, že zejména Moldavská republika neustále čelí koordinovaným dezinformačním kampaním podporovaných státem, jejichž cílem je oslabit moldavské demokratické instituce a integritu moldavských voleb a zkomplikovat cestu Moldavské republiky k přistoupení k EU; vzhledem k tomu, že tyto země vyžadují podporu EU při budování občanské a institucionální odolnosti a v boji proti zahraniční manipulaci s informacemi a vměšování a hybridním hrozbám, mimo jiné prostřednictvím mechanismů finanční podpory Nástroje pro Ukrajinu, Nástroje pro reformy a růst pro země západního Balkánu a Nástroje pro reformy a růst pro Moldavsko; vzhledem k tomu, že EU by měla zohlednit zpětnou vazbu a zkušenosti těchto zemí, které čelí ruským hybridním útokům již řadu let; vzhledem k tomu, že efektivita úsilí EU o posílení institucionální odolnosti v kandidátských

zemích závisí na jejich ochotě přijmout příslušná opatření, provést nezbytné reformy a účinně spolupracovat;

- BT. vzhledem k tomu, že ruská útočná válka proti Ukrajině a asertivní geopolitický postoj Číny jsou spojeny s intenzivnějším využíváním dezinformací, ekonomického nátlaku a strategického vlivu, přičemž terčem příslušných operací není pouze EU, ale také zranitelné regiony, jako jsou země západního Balkánu, země východního partnerství a globálního Jihu; vzhledem k tomu, že různé zdroje uvádějí, že roční rozpočet Ruska na šíření dezinformací a propagandu činí několik miliard eur; vzhledem k tomu, že na ochranu proti dezinformační válce Ruska nevynakládá EU odpovídající finanční prostředky a nemá účinnou strategii; vzhledem k tomu, že volby a politické události v celé Evropě svědčí o přetrvávající, cílené a sofistikované plnohodnotné ofenzivní hybridní válce, kterou chce Rusko destabilizovat důvěru v evropské politické systémy a instituce a vytvářet neustálý zmatek ohledně toho, co jsou fakta a co jsou nepravdivé informace; vzhledem k tomu, že taková válka vyžaduje odpovídající reakci a přechod od čistě obranné strategie do ofenzivy;
- BU. vzhledem k tomu, že manipulace s informacemi již byla odhalena u tří kandidátů pro prezidentské volby, které se mají konat ve Francii v roce 2027, a byla připsána Rusku;
- BV. vzhledem k tomu, že ruská útočná válka proti Ukrajině, jakož i v širším měřítku vedená ruská hybridní válka proti Evropě a jeho vměšování do demokratických procesů jiných zemí byly umožněny a odůvodněny nacionalistickou imperialistickou ideologií „rašismu“ (ruského fašismu) a jsou součástí širší strategie zaměřené proti Západu a jeho zájmům a hodnotám, včetně mezinárodního řádu založeného na pravidlech, právního státu, demokracie, lidských práv a společné bezpečnosti; vzhledem k tomu, že Parlament odsoudil ideologii, politiku a postupy současného ruského režimu jako neslučitelné s mezinárodním právem a hodnotami EU;
- BW. vzhledem k tomu, že Rusko zahájilo vícevrstvou hybridní kampaň vměšování s cílem narušit moldavské volby v letech 2024 a 2025, při které využívalo dezinformací, finančních manipulací, kybernetických útoků a zástupných sítí; vzhledem k tomu, že Rusko do těchto pokusů o narušení moldavských voleb masivně investovalo a že tyto pokusy nebyly úspěšné jen díky účinnosti moldavských obranných politik a podpoře poskytované EU; vzhledem k tomu, že dne 24. dubna 2023 byla zřízena partnerská mise Evropské unie v Moldavské republice (EUPM Moldova) s výslovným cílem podporovat moldavské orgány v boji proti zahraniční manipulaci s informacemi a vměšování;
- BX. vzhledem k tomu, že dne 7. června 2026 se v Arménii konaly parlamentní volby poté, co se Rusko v této zemi intenzivně pokoušelo politické dění ovlivnit prostřednictvím některých náboženských

aktérů a mezinárodní diaspory za účelem oslabení arménských demokratických institucí, maření mírových rozhovorů s Ázerbájdžánem a opětovnému potvrzení ruského vlivu; vzhledem k tomu, že podle arménské výroční zprávy z roku 2026 o vnějších bezpečnostních rizicích aktivovaly zahraniční mocnosti v Arménii své agenty;

- BY. vzhledem k tomu, že Srbsko se stalo klíčovým dezinformačním centrem a zprostředkovatelem ruských a v menší míře čínských vlivových operací; vzhledem k tomu, že podle výnosů moldavského soudu se v Srbsku v roce 2024 konal za podpory Ruska vojenský výcvikový tábor, který rekrutoval a vycvičil agenty, kteří měli vyvolat masové nepokoje během moldavských voleb a referenda; vzhledem k tomu, že srbská kybernetická infrastruktura byla využita k zahájení sofistikovaných cílených phishingových útoků na Bělehradskou bezpečnostní konferenci, jejichž terčem se stali úředníci a diplomaté EU a NATO; vzhledem k tomu, že Srbsko se stalo bezpečným útočištěm pro ruské tajné agenty a oligarchy, kteří sledují představitele ruské opozice a hledají způsoby, jak se vyhnout sankcím; vzhledem k tomu, že srbští občané s údajným napojením na Rusko byli zatčeni za nenávistné činy ve Francii a v Německu, které zahrnovaly hanobení židovských památek a vyvolávání etnických a náboženských neshod;
- BZ. vzhledem k tomu, že znepokojivé snížení podpory na ochranu mezinárodní demokracie ze strany USA, které odstoupily od klíčových mnohostranných a mezinárodních rámců, způsobilo značný globální deficit ve financování boje proti dezinformacím a autoritářskému vlivu;
- CA. vzhledem k tomu, že strategie národní bezpečnosti USA a strategie národní obrany odrážejí posun v dlouhodobé zahraniční politice USA, který se mimo jiné vyznačuje jasným zaměřením zájmů USA na západní polokouli a zlehčováním hrozby, kterou představuje Rusko a Čína; vzhledem k tomu, že národní bezpečnostní strategie USA se rovněž kriticky vyjadřuje ke stavu demokracie v některých členských státech EU a oznamuje opatření podobná zahraničnímu vměšování; vzhledem k tomu, že národní bezpečnostní strategie USA nahlíží globální vývoj do značné míry z hlediska hospodářského nacionalismu a strategických zájmů a zaujímá vůči tradičním spojencům přístup podle transakční logiky, čímž zpochybňuje zásady, na nichž je zahraniční politika USA po desetiletí založena;
- CB. vzhledem k tomu, že Čína používá ve srovnání s jinými aktéry sofistikovanější metody k získání vlivu v EU, mimo jiné prostřednictvím spolupráce s politickými elitami, získáváním bývalých úředníků na svou stranu nabídkou lukrativních pracovních míst a budováním rozsáhlé sítě studentů, výzkumných pracovníků a podnikatelů, jejichž úkolem je šířit pročínské narativy a politiku; vzhledem k tomu, že tyto metody jsou využívány i ke koordinované

manipulaci s informacemi a k dezinformační činnosti ve třetích zemích, jak dokládají zprávy dvoustranné americké komise, které upozorňují na čínskou dezinformační kampaň, jejímž cílem bylo poškodit pověst francouzských stíhacích letadel Rafale používaných Indií proti čínským zbraním v konfliktu mezi Indií a Pákistánem v roce 2025;

- CC. vzhledem k tomu, že mezinárodní iniciativy, včetně iniciativ OSN, Organizace pro hospodářskou spolupráci a rozvoj, Rady Evropy, podobně smýšlejících zemí ve východní Asii, včetně Japonska, Jižní Koreje a Tchaj-wanu, a skupiny G7, začaly vytyčovat zásady a rámce pro ochranu integrity informací, zakotvené v demokratických hodnotách, pluralitě sdělovacích prostředků a lidských právech;
- CD. vzhledem k tomu, že kampaně zahraniční manipulace s informacemi a vměšování a související aktivity mohou být také prováděny subjekty EU, včetně členských států; vzhledem k tomu, že důvěryhodnost demokratických institucí závisí také na tom, zda vlády nebudou šířit nepřesné, zavádějící nebo politicky účelové informace, zejména během přírodních katastrof, mimořádných situací v oblasti zdraví a humanitárních krizí; vzhledem k tomu, že přijímání placených funkcí nebo poradních funkcí bývalými vysoce postavenými úředníky členských států EU a orgánů EU nebo přijímání jiných forem spolupráce s autoritářskými režimy třetích zemí nebo jejich vládou kontrolovanými podniky může ohrozit důvěryhodnost EU a nezávislost jejího rozhodovacího procesu;
- CE. vzhledem k tomu, že fenomén manipulace s informacemi a vměšování v domácím kontextu a jeho dopad by měl být dále zkoumán a analyzován, zejména v souvislosti s jeho interakcí se zahraniční manipulací s informacemi a vměšováním; vzhledem k tomu, že opatření boje proti zahraniční manipulaci s informacemi a vměšování rovněž přispívají ke zvýšení celkové odolnosti společností v domácím kontextu, zejména pokud jde o zlepšení situačního povědomí, zvýšení transparentnosti a pluralismu a posílení úrovně mediální a digitální gramotnosti a gramotnosti v oblasti používání umělé inteligence u všech věkových skupin; vzhledem k tomu, že účinné narušování manipulace s informacemi a boj proti nim vyžaduje celospolečenský přístup napříč odvětvími;
- CF. vzhledem k tomu, že doporučení Komise týkající se inkluzivních a odolných volebních procesů v Unii, zveřejněná v prosinci 2023, dosud nebyla plně provedena ve všech členských státech, včetně ustanovení zaměřených na posílení spolupráce mezi vnitrostátními orgány během volebních procesů a před nimi prostřednictvím zřízení vnitrostátních volebních sítí;
- CG. vzhledem k tomu, že zahraniční manipulace s informacemi a vměšování se ve volebním kontextu často řídí opakujícími se vzorci, jejichž součástí je snaha diskreditovat kandidáty nebo politické

aktéry, narušit důvěru ve volební procesy a čerpat prospěch z názorového rozdělení společnosti; vzhledem k tomu, že na zajištění integrity voleb je třeba pracovat holisticky;

- CH. vzhledem k tomu, že v posledních letech hraje Evropská síť pro volební spolupráci (ECNE) stále důležitější úlohu, avšak v současnosti jí chybí zdroje a kapacity, aby posunula svou činnost na další úroveň;
- CI. vzhledem k tomu, že k účasti na schůzích ECNE byly přizvány kandidátské země; vzhledem k tomu, že existuje ještě mnoho dalších možností, jak spolupráci s těmito zeměmi v rámci činnosti ECNE dále prohloubit a vzájemně sdílet zkušenosti na poli zvládání hrozeb a osvědčené postupy při jejich potírání;
- CJ. vzhledem k tomu, že je jednoznačně zapotřebí posílit ochranu volební infrastruktury a vnitrostátních politických stran, které byly rovněž cílem kybernetických útoků a dalších forem zahraniční manipulace s informacemi a vměšováním, v neposlední řadě s ohledem na rozsáhlé kybernetické útoky na rumunské volební orgány na podzim 2024; vzhledem k tomu, že zpráva o činnosti agentury ENISA z roku 2019 již doporučila klasifikovat volební systémy, procesy a infrastruktury jako kritickou infrastrukturu, aby byla zavedena nezbytná opatření v oblasti kybernetické bezpečnosti;
- CK. vzhledem k tomu, že řada zpráv a vyšetřování, která odhalila mimo jiné kampaně typu „doppelpgänger“ zcizující identitu zavedených sdělovacích prostředků, naznačuje, že Rusko pravděpodobně zasáhlo do německých federálních voleb v roce 2025, přičemž jeho terčem se staly proevropské politické strany; vzhledem k tomu, že je rovněž možné, že do vměšováním do stejného volebního procesu se zúčastnili i další aktéři ze třetích zemí, a to v rámci širšího vzorce vměšováním zaznamenaného v několika evropských zemích;
- CL. vzhledem k tomu, že skryté financování politických stran a hnutí v EU třetími zeměmi, o němž svědčí v současnosti doložené případy zahraničního vměšováním autoritářských režimů prostřednictvím přímého nebo nepřímého financování politických stran, nadací nebo přidružených mediálních organizací, představuje hrozbu pro demokratickou odolnost, integritu voleb a legitimitu demokratického procesu;
- CM. vzhledem k tomu, že Parlament byl terčem špionáže a zahraničního vměšováním, s čímž souvisí odsouzení asistenta bývalého poslance Evropského parlamentu Maximiliana Kraha, člena strany Alternative für Deutschland (AfD), za špionážní činnost ve prospěch Číny; vzhledem k tomu, že poslanci a jejich zaměstnanci mají přístup k citlivým informacím a dokumentům uvnitř Parlamentu;
- CN. vzhledem k tomu, že nepostradatelnou strukturální složkou integrity voleb je nezávislost soudnictví; vzhledem k tomu, že integrita voleb

závisí na existenci dostupných a účinných opravných prostředků pro případ porušování volebních práv a volebních postupů, které musí být izolovány od tlaku politické a výkonné moci;

- CO. vzhledem k tomu, že od roku 2022 uvalila EU v reakci na vojenskou agresi Ruska vůči Ukrajině celkem 21 balíčků rozsáhlých a bezprecedentních sankcí; vzhledem k tomu, že cílem těchto sankcí je výrazně zvýšit tlak na ruskou válečnou ekonomiku, především na klíčová odvětví, jako je energetický, finanční a obranný průmysl, a zvláštní ekonomické zóny a subjekty, které útočnou válku umožňují nebo z ní mají prospěch, a zbavit se závislosti na dovozu fosilních paliv z Ruska; vzhledem k tomu, že EU také přijala sankce vůči Bělorusku, Íránu a Severní Koreji, které Rusko při útočné válce proti Ukrajině podporují; vzhledem k tomu, že účinnost těchto opatření by měla být posílena a mezery umožňující jejich obcházení by měly být odstraněny;
- CP. vzhledem k tomu, že od 8. října 2024 je sankční rámec EU rozšířen tak, aby umožnil se zaměřit na širokou škálu hybridních činností prováděných Ruskem, včetně narušování volebních procesů a fungování demokratických institucí, ohrožování a sabotáže hospodářských činností, služeb veřejného zájmu a kritické infrastruktury, využívání koordinovaných dezinformací a zahraniční manipulace s informacemi a vměšování, nepřátelských kybernetických činností, účelového využívání migrace a dalších destabilizujících činností; vzhledem k tomu, že na základě tohoto rámce již byly za šíření prokremelských narativů, provádění sabotáže a narušování demokratických procesů uvaleny sankce na desítky osob a subjektů, včetně ruských oligarchů, propagandistů, vojenských zpravodajských pracovníků, sdělovacích prostředků a společností; vzhledem k tomu, že tento sankční režim umožňuje EU mimo jiné přikročit ke zmrazení majetku, zákazu cestování a pozastavení vysílacích licencí či zákazu finančních transakcí a transakcí s kryptoaktivy spojených s hybridními činnostmi;
- CQ. vzhledem k tomu, že moskevský režim běžně používá odvetná opatření, včetně zatýkacích rozkazů a řízení *in absentia*, proti cizím státním příslušníkům, kteří se nacházejí v zahraničí a kritizují jeho politiku nebo odolávají jeho vlivu; vzhledem k tomu, že dne 28. prosince 2024 ruská vláda oznámila, že „výrazně rozšířila“ svou černou listinu občanů a úředníků EU poté, co do ní zahrnula zástupce orgánů EU, vlád členských států, donucovacích orgánů a obchodních organizací; vzhledem k tomu, že účelem této černé listiny, na níž figurují ti, kteří prosazují demokratické hodnoty a odmítají ruskou agresi vůči Ukrajině, je zastrašit a umlčet hlasy prostřednictvím nejasně formulovaných a svévolných omezení a falešných právních obvinění, často bez jakéhokoli formálního oznámení, odůvodnění nebo práva na odvolání; vzhledem k tomu, že tento nátlak má vzestupnou intenzitu, začíná administrativními kroky k exkluzi, pokračuje internetovou šikanou a vrcholí v podobě

fyzických hrozeb, sledování, zastrašování rodinných příslušníků nebo dokonce násilných útoků; vzhledem k tomu, že samotná hrozba zařazení na černou listinu může vést úředníky EU k autocenzuře a vyvolat u nich strach zaujímat politické postoje; vzhledem k tomu, že moskevský režim vede paralelně seznamy ruských občanů žijících mimo Rusko jako prostředek nadnárodní represe;

- CR. vzhledem k tomu, že ruská černá listina by měla být uznána jako nástroj hybridní války a zahraničního nátlaku; vzhledem k tomu, že odpovídající reakce EU by měla zahrnovat lepší sdílení zpravodajských informací, jakož i cílené sankce, jako je zmrazení majetku a zákaz cestování zahraničních úředníků, agentů a finančních zprostředkovatelů, kteří jsou odpovědní za nátlakové praktiky, a narušení finančních a logistických sítí umožňujících tyto operace, včetně kanálů pro kryptoměny;
- CS. vzhledem k tomu, že EU přijala protinátlakový nástroj s cílem chránit EU a její členské státy před hospodářským nátlakem třetích zemí;
- CT. vzhledem k tomu, že hybridní hrozby, zahraniční vměšování a dezinformační kampaně vyústily v komplexní rozsáhlé krizi, jež ovlivňují řadu oblastí a negativně dopadají na bezpečnost, poklidný život občanů a fungování společnosti, institucí a hospodářství jako celku, což již od počátku ruské agrese proti Ukrajině představuje zásadní problém v oblasti vnitřních záležitostí EU a destabilizuje demokratické instituce ve všech členských státech a ohrožuje budoucnost Evropy jako celku;
- CU. vzhledem k tomu, že účinná civilní a obranná připravenost vyžaduje komplexní, celospolečenský a mezirezortní přístup, který zohledňuje všechna rizika a usnadňuje spolupráci a integraci vnitrostátních orgánů členských států s orgány, institucemi a jinými subjekty EU, s podniky, akademickou obcí, občanskou společností a jednotlivými občany; vzhledem k tomu, že Evropský štít pro demokracii představuje jedinečnou příležitost k zavedení tohoto přístupu; vzhledem k tomu, že v rámci tohoto úsilí je třeba zajistit dlouhodobé investice, které budou realisticky odpovídat rozsahu problému, účinně koordinovat využívání finančních prostředků, vypracovat strategický výhled a začlenit hledisko odolnosti do tvorby politik, rozvoje infrastruktury, vzdělávacích systémů a dodavatelských řetězců; vzhledem k tomu, že iniciativy EU v oblasti obrany a připravenosti by měly být sladěny a fungovat v součinnosti;
- CV. vzhledem k tomu, že posílení občanské emancipace prostřednictvím zajišťování znalostí, vzdělávání, mediální a digitální gramotnosti, schopnosti kritického myšlení a přístupu ke spolehlivým informacím je klíčem ke společenské odolnosti a zajišťuje, aby všichni občané mohli předvídat rizika, rozpoznat manipulaci, vhodně reagovat během mimořádných událostí a aktivně přispívat ke kolektivní odolnosti demokratických společností; vzhledem k tomu, že zemské

radiové vysílání je k dispozici v celé EU a poskytuje spolehlivé a stabilní prostředky pro informování občanů v případě katastrof způsobených člověkem nebo přírodních katastrof, zejména v případě výpadku internetu a dalších komunikačních nástrojů; vzhledem k tomu, že připravenost musí zahrnovat praktické nástroje, jako je celoevropská aplikace pro varování před krizemi, brožura, jež přispěje k připravenosti domácností, a rozsáhlé osvětové kampaně na podporu soběstačnosti a připravenosti na krizi ve všech věkových skupinách a sociálních vrstvách;

- CW. vzhledem k tomu, že zásadní význam pro zvýšení obranné připravenosti mají civilně-vojenská spolupráce, kapacity dvojího užití a začlenění hlediska připravenosti do vzdělávacích programů spolu s praktickými dovednostmi a znalostmi v oblasti civilní obrany, a to prostřednictvím cílené odborné přípravy nejen pracovníků v kritických odvětvích, jako jsou hasiči, zdravotničtí pracovníci a státní zaměstnanci, ale také subjektů občanské společnosti a široké veřejnosti; vzhledem k tomu, že je třeba podporovat občanskou odpovědnost, povědomí o hrozbách a pochopení úlohy občanů při zajišťování bezpečnosti;
- CX. vzhledem k tomu, že klíčový význam pro zachování kontroly nad základními komunikačními kanály a posílení kritické infrastruktury mají technologická suverenita a bezpečné digitální ekosystémy, včetně projektů, jako je IRIS² nebo evropský kritický komunikační systém; vzhledem k tomu, že evropské telekomunikační společnosti jsou terčem kybernetické špionáže, jak potvrzují nedávné operace připisované skupině Salt Typhoon napojené na Čínu; vzhledem k tomu, že má-li odvětví telekomunikací, které je základním kamenem těchto ekosystémů, zůstat bezpečné a funkční, vyžaduje důkladná opatření v oblasti kybernetické bezpečnosti a odolnosti;
- CY. vzhledem k tomu, že připravenost závisí na hladké spolupráci mezi orgány, agenturami, členskými státy a podobně smýšlejícími mezinárodními partnery EU, která musí být podpořena společnými cvičeními a odbornou přípravou, sdílenými platformami pro získávání poznatků o situaci a rychlou výměnou informací; vzhledem k tomu, že Tchaj-wan, hlavní partner, pokud jde o informovanost o situaci, pořádá rozsáhlá cvičení v oblasti civilní obrany a odolnosti jako doplněk vojenských cvičení, aby byl schopen vzdorovat stále častějším válečným praktikám, které Čína používá v šedé zóně; vzhledem k tomu, že celospolečenský přístup Tchaj-wanu a osvědčené postupy mohou přispět k rozvoji připravenosti v EU a posílení společného situačního povědomí, kapacit včasného varování a celkové účinnosti Evropského štítu pro demokracii;
- CZ. vzhledem k tomu, že budování skutečné odolnosti a dosažení dostatečné úrovně civilní a obranné připravenosti vyžaduje obrovské investice, posílení evropské technologické a průmyslové základny a snížení strategických závislostí, zejména v digitální oblasti;

vzhledem k tomu, že pro tyto účely je nutné zvážit nové, cílené mechanismy financování;

Úvod

1. vítá společné sdělení o zřízení Evropského štítu pro demokracii a úsilí pokračovat v práci, která již byla vykonána v rámci Akčního plánu pro evropskou demokracii a balíčku opatření na obranu demokracie; zastává názor, že hlavním posláním Evropského štítu pro demokracii by mělo být chránit evropskou demokracii v nestabilním bezpečnostním prostředí, a přispívat tak k ochraně evropského způsobu života, právního státu a hodnot zakotvených v článku 2 SEU; zastává názor, že opatření uvedená ve výše uvedeném sdělení nemají potřebnou úroveň z hlediska cílů, obezřetnosti a kapacit a měla by být v průběhu času dále rozvíjena a postupně posilována s cílem zajistit účinné zavedení důrazných a závazných opatření na ochranu demokracie v souladu s rozsahem zjištěných výzev při současném respektování rozdělení pravomocí EU podle Smlouvy; zdůrazňuje, že opatření „měkké“ politiky jsou často nedostatečná tam, kde jsou záměrně podkopávány demokratické hodnoty, a že boj proti zahraničnímu vměšování, hybridním hrozbám a dezinformacím vyžaduje cílevědomý přístup a důrazná opatření; zastává názor, že důvěryhodnost Evropského štítu pro demokracii závisí také na vůli a odhodlání prosazovat stávající právní předpisy EU, které jsou důležité pro obranu demokracie; dále připomíná, že roztržitost EU zůstává slabinou při obraně demokracie;
2. se znepokojením bere na vědomí stále složitější a neustále se vyvíjející hrozby, které narušují demokratické procesy a instituce v EU a jejích členských státech, především zahraniční manipulaci s informacemi a vměšování, hybridní útoky a dezinformační kampaně vedené nepřátelskými aktéry ze třetích zemí a jejich spojenci v EU; zdůrazňuje, že hybridní válka přesahuje rámec samotných kybernetických nebo informačních útoků a že strategická konfrontace má nyní hospodářský, technologický a společenský rozměr; zdůrazňuje, že v této situaci se nachází mnoho podobně smýšlejících partnerů EU v jejím sousedství i na celém světě;
3. zdůrazňuje, že sociální soudržnost a důvěra ve veřejné instituce jsou základními kameny demokratické odolnosti; upozorňuje, že nedostatky v oblasti právního státu, zejména v oblastech, jako je nezávislost soudnictví, pluralita sdělovacích prostředků a účinnost protikorupčních rámců, mohou oslabit důvěru veřejnosti a být zneužívány jak vnitřními, tak vnějšími aktéry s cílem oslabit demokratický konsensus a prohloubit polarizaci společnosti; vyzdvihuje potřebu komplexního přístupu k řešení otázek ohledně stavu právního státu a k posílení sociální soudržnosti, demokratické legitimacy a společenské důvěry v celé EU a jejích členských státech; dále připomíná, že posílení právního státu v kandidátských zemích je

klíčem k podpoře jejich souladu s hodnotami EU a ke zvýšení celkové evropské demokratické odolnosti;

4. domnívá se, že Rusko je hlavní vnější hrozbou pro bezpečnost a demokratickou integritu Evropy, a opakuje, že Rusko je státem podporujícím terorismus; poukazuje na potřebu komplexní a na budoucnost zaměřené strategie pro ochranu evropské demokracie;
5. opakuje, že klíčové politické priority uvedené v iniciativě Evropský štít pro demokracii – včetně boje proti zahraniční manipulaci s informacemi a vměšování a hybridním hrozbám a včetně zvýšení odolnosti volebních procesů, posílení kybernetické bezpečnosti a podpory občanské společnosti a nezávislých médií a nezávislé investigativní žurnalistiky – musí být dostatečně financovány v nadcházejícím VFR; zdůrazňuje, že investice do demokratické odolnosti mají zásadní význam pro bezpečnost, svrchovanost a prosperitu EU; vyjadřuje svou podporu závazku Komise začlenit demokratickou odolnost do všech programů financování EU; v této souvislosti zdůrazňuje, že je třeba do obranných iniciativ EU začlenit jednotlivé aspekty hybridní obrany; zdůrazňuje však, že pro účinné využívání unijních a vnitrostátních zdrojů a prevenci plýtvání nebo roztržtosti financování je třeba v této souvislosti zavést jasné cíle, které přinesou měřitelné kroky a výsledky;
6. odsuzuje zásahy třetích zemí v některých nejvzdálenějších regionech a zámořských zemích a územích, jejichž dopad může být zhoršen jejich izolací a zeměpisnou odlehlostí od evropského kontinentu;

Evropské středisko pro odolnost demokracie

7. vítá návrh Komise na zřízení Evropského střediska pro odolnost demokracie (dále jen „středisko“) jako nezbytný a logický krok k účinnější koordinaci úsilí čelit vyvíjejícím se společným hrozbám, zejména zahraniční manipulaci s informacemi a vměšování a dezinformacím; bere na vědomí, že jeho funkce a operace mají být zaváděny postupně, za postupného zvyšování účasti členských států; vítá ujištění Komise, že na zřízení střediska již pracuje pod vedením komisaře pro demokracii, spravedlnost, právní stát a ochranu spotřebitele a že počítá s tím, že středisko zahájí svou činnost v plném rozsahu v průběhu roku 2026; konstatuje, že není zcela jasné, jaký bude harmonogram a konkrétní milníky pro postupný rozvoj činnosti střediska, neboť výraz „postupné“ provádění na základě dobrovolné účasti členských států neposkytuje dostatečnou předvídatelnost, odpovědnost ani provozní jistotu; vítá závazek Komise, že bude Parlament o vytváření Evropského štítu pro demokracii a střediska pravidelně informovat a že jej do tohoto procesu zapojí;
8. vyjadřuje však politování nad tím, že v návrhu středisko postrádá jasný mandát a zmocnění prostřednictvím právního aktu, jakož

i vyčleněné rozpočtové zdroje a personál, uzpůsobenou strukturu řízení a harmonogram; konstatuje, že společné sdělení o Evropském štítu pro demokracii středisko výslovně nespojuje s žádným z opatření v něm uvedených – ta zůstávají v různých správních rámcích Komise a ESVČ; zdůrazňuje, že středisko by mělo přinést přidanou hodnotu nad rámec stávajících struktur a nemělo by být pouze dalším z center, sítí, platforem nebo rámců, jelikož kvůli zdvojování práce, zvyšování institucionální nejednoznačnosti, prohlubování roztržitosti a napjatým rozpočtům se jen snižuje schopnost EU účinně využívat celé spektrum nástrojů, které jsou v současné době k dispozici; je pevně přesvědčen, že středisko by mělo sloužit k agregaci a konsolidaci stávajících opatření na úrovni EU tím, že bude podporovat vnitrostátní opatření, rozšiřovat je, doplňovat a pokud možno koordinovat;

9. vítá skutečnost, že společné sdělení podrobně mapuje stávající rámce, struktury, nástroje, iniciativy a programy pro boj proti zahraniční manipulaci s informacemi a vměšování a proti dezinformacím a pro zvyšování odolnosti a uvádí seznam opatření, k jejichž provedení se Komise a ESVČ zavázaly; vyzývá Komisi a ESVČ, aby navrhly jasný harmonogram jejich postupného zavádění a integrace v rámci střediska, přičemž jako lhůta pro jejich integraci by měl být stanoven rok 2026; vyzývá k tomu, aby tato integrace zahrnovala provozní odpovědnost za posílený systém včasného varování, který bude schopen řešit manipulaci s informacemi v reálném čase, zavedení a provoz jednotné zpravodajské databáze zahraniční manipulace s informacemi a vměšování, čímž se rozšíří zdroje pro činnost iniciativy EUvsDisinfo, mimo jiné na základě mapování platforem používaných pro účely zahraniční manipulace s informacemi a vměšování a dezinformací, a podpoří činnost sítě ECNE a pracovní skupiny Komise pro dezinformace a strategickou komunikaci; vyzývá Komisi, aby zajistila, že středisko bude schopno vyhodnocovat koordinované útoky na integritu informací; zdůrazňuje, že středisko musí být vybaveno tak, aby mohlo sledovat operace zahraničního vměšování a hybridní hrozby, monitorovat je a reagovat na ně, přičemž musí být zajištěno, aby všechny přidružené organizace zůstaly nezávislé, zejména na velkých technologických společnostech;
10. vítá skutečnost, že Komise uznala nutnost spolupracovat s členskými státy a Parlamentem v otázkách mandátu, struktury a pracovních metod střediska, a vyzývá Komisi, aby dále navrhla právní akt pro zřízení střediska jakožto strukturálně autonomního subjektu EU s jasným institucionálním statutem a postavením, správní strukturou a mechanismy parlamentního dohledu; zdůrazňuje, že jasné institucionální vymezení má zásadní význam pro to, aby středisko mohlo činit rozhodné kroky a zároveň nést odpovědnost; domnívá se, že zřízení střediska jakožto stálé struktury na základě právního aktu by představovalo kvalitativní posun od roztržité koordinace k integrovanější, operativnější a strategičtější kapacitě na úrovni EU;

zdůrazňuje, že v zájmu zajištění soudržných a včasných opatření v celé EU v rychle se měnícím prostředí by měl být stanoven ambiciózní harmonogram pro zřízení střediska prostřednictvím právního aktu;

11. vyzývá k tomu, aby do řízení střediska byli zapojeni zástupci všech členských států; konstatuje, že dobrovolná povaha účasti členských států, jak ji navrhuje ve svém sdělení Komise, s sebou nese riziko, že bude zachována neúčinná a roztržitá struktura s různou úrovní ochrany a reakce na společné hrozby, kterým čelí celá EU; konstatuje, že pokud se na řízení nebudou podílet všechny členské státy, vzniká riziko, že tato struktura bude fungovat na základě nižšího společného jmenovatele;
12. zdůrazňuje, že posílená opatření na úrovni Unie na ochranu demokracie musí být doprovázena silným demokratickým dohledem; vyzývá Komisi, aby Parlament o činnosti střediska pravidelně informovala, a to i pokud jde o jeho rozpočtové, provozní a strategické záležitosti; zdůrazňuje, že do řízení střediska by měli být zapojeni zástupci Evropského parlamentu, aby se posílila jeho demokratická legitimita;
13. vyzývá Komisi, aby středisku stanovila jasný mandát, rozhodovací mechanismy a pravomoc jednat, a umožnila mu tak fungovat jako nezávislé centrum excelence pro odhalování, analýzu a boj proti zahraniční manipulaci s informacemi a vměšováním a dezinformacím, jako platforma pro budování kapacit, která přispívá k vytváření společných definic a norem a k poskytování odborné přípravy a technických nástrojů v celé EU, a jako páteří struktura, která převádí analýzy hrozeb a včasná varování do konkrétních, včasných a fakticky podložených operativních výstupů a zajišťuje koordinaci technické podpory v boji proti aktivním kampaním manipulace s informacemi v reálném čase, a to v úzké spolupráci s vnitrostátními orgány a příslušnými orgány EU; zdůrazňuje, že je třeba, aby středisko bylo schopno rychle jednat v krizových situacích, zejména před volbami a v jejich průběhu, a aktuální informace transformovat do účinných opatření; konstatuje, že taktika vměšování nepřátelských aktérů se bude v průběhu času vyvíjet spolu s technologickým pokrokem a mandát střediska by měl umožňovat flexibilitu pro řešení nových výzev. zdůrazňuje, že středisko musí mít stabilní, multidisciplinární personál, včetně analytiků zahraničních manipulací s informacemi a vměšováním, odborníků na zpravodajské informace z otevřených zdrojů (OSINT), specialistů na kybernetickou bezpečnost a sledování finančních toků, a musí být oprávněno koordinovat přeshraniční pracovní skupiny s příslušnými orgány členských států;
14. vyzývá Komisi, aby zajistila, aby analytická a monitorovací kapacita střediska byla formálně strukturována jako zdroj nezávislých odborných vstupů pro procesy posuzování systémových rizik

zavedené podle nařízení o digitálních službách, včetně koordinátorů digitálních služeb v každém členském státě, a podle evropského aktu o svobodě médií, nařízení o transparentnosti a cílení politické reklamy a aktu o umělé inteligenci, mimo jiné prostřednictvím spolupráce při shromažďování, uchovávání a analýze důkazů souvisejících se zahraniční manipulací s informacemi a vměšováním a dezinformacemi, přičemž zjištění povedou přímo k donucovacím opatřením, a prostřednictvím poskytování včasných zpráv o hrozbách, analýz modelu zahraniční manipulace s informacemi a vměšováním a ukazatelů rizik pro demokracii; poukazuje na to, že úloha střediska v těchto procesech musí zůstat poradní a analytická, aby byla zachována nezávislost regulačního rozhodování; zdůrazňuje, že pokud zahraniční manipulace s informacemi a vměšováním a dezinformační činnosti podkopávají právo EU, měla by koordinační úloha střediska zajistit přímou vazbu na orgány příslušné k zahájení vyšetřování a soudních řízení; vyzývá k tomu, aby byla příslušná zjištění o systémových nedostacích nebo opakujících se zranitelných místech řádně zvážena a zohledněna ve výroční zprávě Komise o právním státu ve zvláštních pododdílech zabývajících se dezinformacemi a integritou sdělovacích prostředků v rámci pilíře plurality a svobody médií a integritou voleb a zárukami proti nepřipustnému ovlivňování v rámci pilíře brzd a protivah; konstatuje, že středisko by mohlo rovněž přispívat k odborné přípravě koordinátorů digitálních služeb a zaměstnanců vnitrostátních regulačních orgánů pro sdělovací prostředky v oblasti zahraniční manipulace s informacemi a vměšováním a dezinformací;

15. vítá koncepci platformy zúčastněných stran; konstatuje však, že její účel, struktura a přidaná hodnota stále nejsou dostatečně definovány, mimo jiné ve vztahu ke stávajícím sítím a iniciativám; uznává přidanou hodnotu příspěvku občanské společnosti k rozvoji mandátu střediska; vyzývá Komisi, aby zajistila, aby koordinace střediska zahrnovala stávající úsilí občanské společnosti a akademické obce prostřednictvím navrhované platformy; trvá na tom, že středisko musí rovněž poskytovat příležitosti pro přeshraniční kontakty a předávání vědomostí mezi vládami a různými zúčastněnými stranami;
16. vyzývá Komisi, aby zajistila, aby mandát střediska zahrnoval odpovědnost za ochranu integrity demokratických procesů na úrovni EU; znovu opakuje, že první obrannou linii představují operační struktury členských států; zdůrazňuje však, že jejich primární odpovědnost se nekryje s oprávněnými zájmy, jež má EU v oblasti boje proti zahraniční manipulaci s informacemi a vměšováním a proti dezinformacím a posilování integrity voleb; konstatuje, že koordinované kampaně manipulace s informacemi se často zaměřují na informační prostor celé EU, což odůvodňuje specializovanou operační kapacitu na úrovni EU na ochranu demokratických procesů nad rámec čistě vnitrostátních souvislostí; vyzývá Komisi, aby upřesnila, že středisko musí sloužit dvěma vzájemně se umocňujícím

cílům, a sice koordinaci činnosti členských států v této oblasti a posilování jejich operační kapacity na jedné straně a ochraně demokratických zájmů EU na straně druhé; klade důraz na to, že pracovní metody a využívání údajů musí být plně interoperabilní se stávajícími strukturami EU a členských států; zdůrazňuje, že v tomto ohledu jsou potřebné společné metodiky s otevřeným zdrojovým kódem a účinná spolupráce mezi sítěmi aktérů, včetně výzkumných pracovníků v oblasti OSINT, novinářů, komunikátorů a tvůrců politik;

17. vyzývá ty členské státy, které nemají specializované operační struktury, aby s podporou střediska zřídily nebo podstatně posílily specializované vnitrostátní instituce pro boj proti zahraniční manipulaci s informacemi a vměšování a pro odhalování dezinformací a reakci na ně; žádá Komisi, aby vypracovala plán rozvoje a proces hodnocení kapacit členských států; zdůrazňuje, že takový proces by poskytl základ pro postupné zvyšování úrovně ambicí střediska;
18. vyzývá Komisi, aby posoudila proveditelnost zmocnění střediska ke správě účelového financování EU v rámci stávajícího a nadcházejícího VFR a příslušných programů EU, kdykoli se týkají boje proti zahraniční manipulaci s informacemi a vměšování, posílení demokratické odolnosti a podpory informační integrity; žádá Komisi, aby se vyvarovala programování, které rozptyluje a tříští úsilí nebo vytváří neudržitelné dočasné iniciativy malého rozsahu, ale aby se zaměřila na koordinované strategické rozšiřitelné úsilí, které je udržitelné pro všechny zapojené subjekty;
19. požaduje, aby Komise poskytla středisku a jeho činnostem dostatečné a předvídatelné financování, včetně dostatečného počtu zaměstnanců a finančních zdrojů v rámci příštího VFR, a zvláštní rozpočtovou položku EU pro provoz střediska s jasným oddělením provozního financování a obecných nákladů na koordinaci; dále Komisi vyzývá, aby zajistila dostatečné lidské zdroje a překlenula financování ze stávajících rozpočtů, aby se před zahájením uplatňování VFR na období 2028-2034 mohly uskutečnit přípravné činnosti;
20. vyzývá Komisi, aby posoudila proveditelnost vytvoření mechanismu financování, který by doplnil zvláštní rozpočtovou položku na činnost střediska; zastává názor, že do tohoto mechanismu by měli přispívat také velcí poskytovatelé služeb informační společnosti, jejichž činnost představuje systémové riziko pro demokratickou integritu; zdůrazňuje, že každý takový mechanismus musí doprovázet co nejsilnější záruky nezávislosti a naprosté vyloučení střetu zájmů;

Digitální odolnost

21. vyzývá k plnému provádění a účinnému prosazování celého *conquista* EU souvisejícího s digitální oblastí, včetně klíčové legislativy, jako je nařízení o digitálních službách, nařízení o digitálních trzích, nařízení o transparentnosti a cílení politické reklamy, akt o umělé inteligenci

a evropský akt o svobodě médií, ve všech členských státech a při plném dodržování základních práv; zdůrazňuje, že důsledné, soudržné, systematické a včasné prosazování je základním pilířem evropské digitální suverenity a odrazování a musí být podmínkou pro působení na jednotném trhu; naléhavě Komisi žádá, aby pravidelně podávala zprávy o prosazování a uplatňování práva EU, zejména nařízení o digitálních službách, zabránila nadměrným prodlevám při vyšetřování a ukládala přísné sankce za přetrvávající porušování ze strany velmi velkých online platforem a velmi velkých internetových vyhledávačů; zastává názor, že další provádění legislativy v digitální oblasti by se mělo více zaměřit na boj proti zahraniční manipulaci s informacemi a vměšování a dezinformacím na internetu, zajištění informační integrity a ochranu demokratického diskurzu během období voleb a mimo něj;

22. vyjadřuje vážné znepokojení nad tím, že doporučovací systémy některých velmi velkých online platforem založené na interakci často představují systémové riziko pro občanský diskurz a volební procesy, neboť zesilují rozdělující, polarizující nebo zavádějící obsah, často podněcují dezinformace od zahraničních a domácích aktérů, a zároveň neúměrně upřednostňují senzační materiály před obsahem založeným na faktech; připomíná, že články 34 a 35 nařízení o digitálních službách vyžadují, aby velmi velké online platformy tato rizika posuzovaly a zmírňovaly; trvá na tom, že účinná opatření ke zmírnění rizik by měla rovněž zajistit, aby syntetický nebo zmanipulovaný obsah, jako jsou deepfakes, mohl být jasně odlišen od autentických materiálů a aby byly náležitě upřednostňovány redakčně nezávislé a pluralitní sdělovací prostředky a ověřené zdroje; vyzývá Komisi, aby v tomto ohledu prošetřila dodržování povinností vyplývajících z nařízení o digitálních službách a přijala vhodná opatření, včetně uložení předběžných opatření; navrhuje, aby tato předběžná opatření v případě potřeby zahrnovala omezení doporučovacích systémů založených na interakci, které představují systémové riziko; dále vyzývá Komisi, aby podporovala větší transparentnost a odpovědnost při navrhování algoritmických doporučovacích a reklamních systémů, zejména společně s dalšími algoritmickými systémy, s cílem posílit výběr uživatelů a zajistit nemanipulativní výchozí nastavení, a to při podpoře svobody projevu a informací; v této souvislosti připomíná velmi velkým online platformám jejich povinnost zmírňovat systémová rizika v souladu s čl. 35 odst. 1 písm. d) a článkem 38 nařízení o digitálních službách, což může zahrnovat testování a úpravu jejich algoritmických systémů, včetně jejich doporučovacích systémů, a povinnost poskytnout pro každý jejich doporučovací systém alespoň jednu možnost, která není založena na profilování; dále vyzývá Komisi, aby ve spolupráci s koordinátory digitálních služeb a se zapojením nezávislých třetích stran prostřednictvím veřejných konzultací zajistila, aby existovaly aktuální pokyny pro zmírňování systémových rizik, a aby zajistila důsledné prosazování a vysokou úroveň ochrany před rozsáhlou manipulací;

23. odsuzuje cílené sankce a pokusy vlády USA o nátlak na subjekty EU zapojené do utváření a prosazování nařízení o digitálních službách a dalších nařízeních v digitální oblasti, zejména nátlak vůči bývalému komisaři; požaduje okamžité zrušení těchto opatření; naléhavě vyzývá Komisi a členské státy, aby tomuto tlaku odolávaly, dodržovaly právní předpisy EU a hájily právo na samosprávu a digitální suverenitu; zdůrazňuje, že svoboda projevu je v EU základním právem a základní hodnotou sdílenou se Spojenými státy a podobně smýšlejícími partnery v celém demokratickém světě; poukazuje na to, že politické a obchodní aspekty, jakož i tlak ze strany třetích zemí nebo velkých technologických společností by neměly nepatřičně ovlivňovat prosazování právních předpisů EU v digitální oblasti; klade důraz na to, že rozhodnutí týkající se uplatňování pravidel EU v digitální oblasti se musí řídit výhradně právem EU a ochranou demokratických zájmů a že EU si jako otevřený jednotný trh založený na pravidlech zachovává svrchované právo regulovat svou hospodářskou činnost v souladu s demokratickými hodnotami a mezinárodními závazky; vyzývá Komisi a členské státy, aby zajistily, že ochranné a nápravné mechanismy právních předpisů EU v digitální oblasti budou chráněny před jakýmkoli vměšováním, které by mohlo ohrozit jejich nezávislost nebo účinnost, a aby zavedly spolehlivé záruky proti těmto rizikům;
24. vyzývá Komisi, aby zvýšila úsilí o podporu nařízení o digitálních službách a dalších klíčových legislativních aktů EU v digitální oblasti v kandidátských a potenciálních kandidátských zemích a sladění jejich legislativy s těmito akty a aby zajistila, aby tyto země měly podporu, nástroje a pokyny potřebné k provádění těchto zákonů, které ve vhodných případech umožní postupné začlenění do příslušných mechanismů EU pro prosazování a spolupráci; zdůrazňuje, že úsilí o demonetizaci dezinformací by mělo výslovně zahrnovat kandidátské a potenciální kandidátské země, aby se zabránilo mezerám v právních předpisech a přeshraničním dopadům; zdůrazňuje, že je třeba věnovat zvláštní pozornost trendům pozorovaným v kandidátských a potenciálních kandidátských zemích při provádění činností souvisejících s volbami podle kodexu chování v oblasti dezinformací;
25. bere na vědomí oficiální začlenění dobrovolného kodexu zásad boje proti dezinformacím do rámce nařízení o digitálních službách jako kodexu chování v oblasti dezinformací, který se stane relevantním měřítkem pro určování souladu s uvedeným nařízením, pokud jde o rizika dezinformací, s cílem doplnit další účinná zmírňující opatření velmi velkých online platforem a velmi velkých internetových vyhledávačů k řešení systémových rizik pro demokratické procesy; konstatuje, že by mohly být dále vyjasněny důsledky možného nedodržování kodexu pro dodržování a prosazování nařízení o digitálních službách; zdůrazňuje, že kodex by měl zůstat dynamickým nástrojem, který sleduje nejnovější trendy, a že Komise by měla i nadále dohlížet na jeho účinné uplatňování signatáři; je

toho názoru, že provádění nařízení o digitálních službách by mělo řešit koordinované neautentické využívání online platform, např. prostřednictvím botů, falešných účtů, polarizačních algoritmů a umělé interakce a amplifikace, což vytváří iluzi veřejné podpory; domnívá se, že tyto jevy patří k nejzávažnějším rizikům pro svobodný, autentický a otevřený diskurz na internetu, zejména v období voleb; poukazuje na to, že zahraniční autoritářské subjekty, zejména Rusko, vypracovaly dezinformační protokoly, jejichž účinky byly během nedávných voleb v celé Evropě stále viditelnější; naléhavě vyzývá všechny velmi velké online platformy a velmi velké internetové vyhledávače působící v EU, aby kodex plně dodržovaly, a naléhavě vyzývá platformu X, aby se znovu zavázala k jeho dodržování;

26. vítá příslib Komise, že vypracuje protokol k nařízení o digitálních službách pro případ krizí a incidentů, včetně jasných postupů pro koordinaci příslušných orgánů, s cílem podrobněji upravit řešení závažných incidentů a vměšování v informačním prostředí; domnívá se, že tento protokol by měl podporovat účast online platform a online vyhledávačů a měl by mimo jiné řešit zasahování do voleb prostřednictvím koordinovaného neautentického chování v online prostoru, zejména prostřednictvím amplifikace a interakce pomocí botů, jež reálně narušují skutečný veřejný diskurz; zdůrazňuje, že je třeba, aby platformy reagovaly rychle a účinně prostřednictvím preventivních a nápravných opatření proti těmto zásahům a aby orgány v případě nesouladu rychle reagovaly, místo aby se spoléhaly na opatření ex post a pozdní vymáhání; v této souvislosti vítá, že společnost Google v roce 2025 aktivně odstranila téměř 11 000 kanálů a účtů na YouTube spojených se státem podporovanou propagandou z Číny, Ruska a dalších nepřátelských aktérů, a naléhavě vyzývá všechny platformy, aby se těmito hrozbami systematicky zabývaly;
27. vítá skutečnost, že Komise dokončila vyšetřování porušení povinnosti transparentnosti podle nařízení o digitálních službách platformou X a uložila pokutu ve výši 120 milionů EUR, jakož i rozhodnutí Komise zahájit vyšetřování začlenění chatbotu Grok AI do platformy X; a rozšířit stávající vyšetřování na doporučovací systémy platformy X; naléhavě vyzývá Komisi, aby urychlila zbývající vyšetřování, včetně vyšetřování společnosti Meta, zejména s ohledem na předběžná zjištění o porušení povinností v oblasti transparentnosti a ochrany uživatelů a na zprávy poukazující na přetrvávající problémy související s podvodnou reklamou a obcházením regulace; zdůrazňuje, že je třeba přijmout donucovací opatření v případech zasahování do voleb, přetrvávající neprůhlednosti algoritmů a rozsáhlého šíření falešných účtů a sítí botů, které narušují veřejný diskurz; žádá v této souvislosti Komisi, aby urychleně dokončila vyšetřování toho, jak TikTok dodržuje nařízení o digitálních službách v souvislosti se zahraničním vměšováním do rumunských prezidentských voleb v roce 2024, které upozornilo na znepokojivé možnosti využívání doporučovacích systémů a sítí botů, a

v souvislosti s povinností TikToku zmírnit systémová rizika pro demokratické procesy a zajistit odstrašování během volebních období; dále bere na vědomí předběžné hodnocení Komise, z něhož vyplývá, že TikTok porušuje nařízení o digitálních službách svým návykovým designem;

28. klade důraz na to, že je třeba zvýšit transparentnost, pokud jde o subjekty stojící za online obsahem a účty, zejména pro reklamní účely; poukazuje na to, že opatření pro boj proti koordinovanému neautentickému chování bez zrušení anonymity na internetu mají zásadní význam pro předcházení zahraniční manipulaci s informacemi a vměšování, využívání farem botů a zabránění skrytým politickým kampaním; žádá Komisi, aby prozkoumala možná opatření, která by podpořila online platformy při přijímání přiměřených kroků k ověření toho, zda za účtem stojí člověk, čímž by se zabránilo činnosti botů; vyzývá platformy, aby upřednostňovaly rozvoj účinných mechanismů pro identifikaci, kontrolu a v případě potřeby pozastavení neautentických účtů, zejména těch, které se podílejí na koordinovaných vlivových operacích; zdůrazňuje, že opatření zaměřená na neautentické účty nesmí oslabovat schopnost zachovat si na internetu anonymitu což má zásadní význam pro ochranu novinářů, aktivistů, marginalizovaných komunit a osob ve zranitelném postavení (jako jsou oznamovatelé, disidenti a političtí oponenti autokratických režimů), a měla by i nadále poskytovat prostor pro satirické a humorné účty;
29. vyzývá Komisi a příslušné regulační orgány, aby systematicky vyšetřovaly skryté dezinformační kampaně zaměřené na využívání systémů generativní AI, včetně koordinované propagandy a sítí pro praní informací, jako jsou činnosti moskevské sítě „Pravda“ a explicitní manipulace Groku (xAI), a aby tyto kampaně zveřejňovaly způsobem, který nepodporuje jejich šíření; zdůrazňuje, že je důležité vyjasnit přesné povinnosti poskytovatelů a provozovatelů v souvislosti s požadavky na označování obsahu vytvořeného umělou inteligencí stanovenými v článku 50 aktu o umělé inteligenci a kodexu zásad boje proti dezinformacím a upřesnit, do jaké míry se tento rámec vztahuje na koncové uživatele a platformy; naléhavě žádá poskytovatele systémů umělé inteligence, aby prostřednictvím svých systémů řízení rizik AI tento jev řádně řešili a zmírňovali; dále vyzývá úřad pro AI, aby zvýšil své úsilí o monitorování bezpečnostního prostředí modelů AI a pomohl rozvíjet metodiky pro AI, včetně velkých jazykových modelů, a zajistil tak větší transparentnost a dodržování osobní integrity při trénování zdrojů údajů;
30. vyzývá Komisi, aby v úzké spolupráci s belgickým regulačním orgánem urychleně dokončila posouzení uživatelské základny a funkčnosti platformy Telegram z hlediska její klasifikace jako velmi velké online platformy podle nařízení o digitálních službách, jak již učinila v případě aplikace WhatsApp, a aby vzala v úvahu případné

nové důkazy nebo změny způsobů využívání; naléhavě žádá Komisi a příslušné orgány, aby prošetřily potenciální úlohu Telegramu při usnadňování trestné činnosti, zasahování do voleb a šíření dezinformací, extremismu a teroristického obsahu v EU a aby vyjasnily jeho možné vazby na ruské zpravodajské služby a bezpečnost jeho serverů a postupů při nakládání s údaji; zdůrazňuje, že je třeba přijmout veškerá dostupná donucovací opatření k zajištění toho, aby platforma Telegram plně dodržovala požadavky EU na transparentnost, moderování obsahu a přístup k údajům s cílem zajistit rovné podmínky a zachovat důvěru občanů v digitální informační prostor; dále důrazně vybízí Telegram, aby se připojil k dobrovolnému kodexu zásad boje proti dezinformacím;

31. doporučuje dále prověřit úlohu influencerů, včetně nanoinfluencerů a mikroinfluencerů, v utváření veřejného diskurzu a ovlivňování voleb, a to jak těch, kteří bojují proti zahraničním dezinformačním kampaním, tak těch, kteří k nim přispívají, ať již vědomě, nebo nevědomě; vítá závazek Komise posoudit úlohu online influencerů v nadcházejícím hodnocení směrnice o audiovizuálních mediálních službách nebo v rámci připravovaného aktu o digitální spravedlnosti; v této souvislosti zdůrazňuje, že je třeba zavést pokyny a přísné normy týkající se transparentnosti, včetně financování prostřednictvím platform, odměňování a dohod o sponzorství a dále rozlišování mezi reklamou a organickým obsahem a v oblasti informační integrity pro tvůrce politického obsahu na internetu, zejména influencersy působící v šedé zóně mezi obchodní propagací a politickými sděleními; vítá stávající kodexy chování a vzdělávací a další iniciativy zaměřené na zvýšení odpovědnosti a transparentnosti sociálních médií a influencerů; navrhuje, aby etické normy a povinnosti novinářů sloužily jako inspirace pro přípravu norem pro influencers; dále vyzývá Komisi, aby pokračovala v prosazování nařízení o transparentnosti a cílení politické reklamy, zejména ve vztahu k online platformám, a aby influencerům usnadnila dodržování předpisů prostřednictvím plánované sítě influencerů EU;
32. naléhavě vyzývá k tomu, aby s cílem snížit strategické závislosti byla na základě spravedlivého odměňování vytvářena regulační pískoviště a mechanismy financování na podporu technologických startupů v EU a evropské alternativy založené na hodnotách, jako jsou ty, které vznikají v Nizozemsku; vítá strategii Komise pro otevřený zdrojový kód; dále podporuje dlouhodobou vizi platform sociálních médií EU koncipovaných v souladu s hodnotami EU v oblasti transparentnosti, ochrany údajů, základních práv, svobody projevu a demokratické odpovědnosti;
33. zdůrazňuje, že reklamní praktiky a praktiky sdílení příjmů mohou motivovat k šíření manipulativního nebo škodlivého obsahu, narušovat integritu voleb a vést ke vzniku nových dezinformačních aktérů a sítí; připomíná, že dezinformace nelze demonetizovat bez

dostatečně transparentních stávajících postupů zpeněžování; vyzývá Komisi, regulační orgány EU v digitální oblasti, příslušné vnitrostátní orgány a online platformy, aby spolupracovaly s cílem odhalovat nezákonné financování a předcházet mu a zajistit transparentnost programů přerozdělování příjmů, reklamních politik a dalších zpeněžovacích služeb, které by aktérům zahraniční manipulace s informacemi a vměšování nebo dokonce sankcionovaným subjektům umožňovaly získat příjem nebo jiné výhody; vyzývá platformy, aby alespoň jednou ročně zveřejňovaly toky odměn a jejich příjemce; domnívá se, že zpeněžení činností zahraniční manipulace s informacemi a vměšování v těchto programech by mělo být řešeno v rámci povinnosti posuzování a zmírňování rizik podle nařízení o digitálních službách; považuje zpeněžení obsahu od sankcionovaných subjektů za systémové riziko, které vyžaduje rychlá nápravná opatření, jako je pozastavení sdílení příjmů; zdůrazňuje, že skuteční tvůrci a mediální tituly by měli být odškodněni za své ztráty v případě chybné nebo nespravedlivé demonetizace; je znepokojen postupným rušením závazků společností k iniciativám v oblasti svobody internetu;

34. je znepokojen zjištěními nizozemského orgánu pro ochranu údajů, která svědčí o obavách rozšířených v celé EU, z nichž vyplývá, že chatboti využívající umělou inteligenci mohou poskytovat neobjektivní a nespolehlivá doporučení, koho volit, což představuje riziko pro integritu voleb; vyzývá úřad pro AI, aby prošetřil, zda jsou tyto praktiky v rozporu s platnou legislativou, zejména s aktem o umělé inteligenci, a aby splnil svůj závazek vypracovat pokyny pro využívání umělé inteligence ve volebních procesech s cílem zajistit, aby byla umělá inteligence využívána odpovědně;

Svoboda slova

35. zdůrazňuje, že Evropský štít pro demokracii musí chránit a prosazovat svobodu projevu a informací jako základní právo platné v offline i online prostoru; klade důraz na skutečnost, že ochrana lidských práv v EU patří k nejlepším na světě a že za jejich ochranu a dodržování nesou odpovědnost i společnosti, které chtějí působit v EU a získat evropské zákazníky; zdůrazňuje proto, že velmi velké online platformy a velmi velké internetové vyhledávače musí uznat a účinně řešit širší společenské a demokratické důsledky svých služeb, mimo jiné prostřednictvím důkladného posouzení systémových rizik a zmírňujících opatření v souladu s právem Unie; v této souvislosti konstatuje, že šíření určitého obsahu nebo názorů a umlčování jiných může představovat systémové riziko pro občanský diskurz a volební procesy nebo porušení svobody projevu, zejména svobody svobodně přijímat a sdělovat informace a myšlenky; vyzývá Komisi, aby zajistila, aby platformy nesly v tomto ohledu odpovědnost podle nařízení o digitálních službách; zdůrazňuje v této souvislosti, že EU musí i nadále aktivně bojovat proti nepravdivým narativům, které tvrdí, že její digitální a demokratická legislativa podkopává

svobodu projevu; zdůrazňuje, že svoboda projevu a informací má chránit lidské bytosti, nikoli stroje nebo software, které vykazují neautentické chování, jako je umělá inteligence a amplifikace a interakce prostřednictvím botů, či automatizované softwarové programy, jež na síti provádějí opakované úkony napodobující skutečné uživatele; dále zdůrazňuje, že závazek ke svobodě projevu nesmí být využíván jako záminka pro tolerování nezákonného obsahu nebo hybridních operací autoritářských režimů, jejichž cílem je destabilizovat EU a její demokratické procesy;

36. připomíná, že online platformy hrají zásadní úlohu v podpoře otevřené veřejné diskuse, novinářské činnosti a politického pluralismu; uznává proto význam účinných záruk pro uživatele při výkonu jejich demokratických práv, včetně možnosti napadnout rozhodnutí platform o moderování a zpeněžení obsahu, a to i před správními a soudními orgány, a vymáhat povinnosti online platform informovat uživatele, pokud je jejich obsah odstraněn nebo omezen; zdůrazňuje v této souvislosti, že je důležité zajistit přístup k vysoce kvalitnímu moderování obsahu ve všech jazycích EU; připomíná, že podle nařízení o digitálních službách mají online platformy povinnost zaručit pro tento účel plnou transparentnost a samostatný mechanismus pro vyřizování stížností a zajistit, aby oznamování, podávání zpráv a možnost nápravy byly i nadále snadno dostupné a uživatelsky vstřícné; konstatuje, že ne všechny online platformy zavedly tyto mechanismy v souladu s ustanoveními nařízení o digitálních službách, a naléhavě vyzývá Komisi a členské státy, aby dotáhly donucovací opatření do konce; poukazuje na to, že ochrana základních práv jednotlivých uživatelů zahrnuje rovněž provádění důkladných posouzení a zmírňování systémových rizik ovlivňujících integritu informačního prostoru;

Integrita médií a informací

37. zastává názor, že nedílnou součástí dosažení cílů stanovených Evropským štítem pro demokracii jsou opatření na podporu svobodných, důvěryhodných a redakčně nezávislých médií, včetně médií na místní a regionální úrovni; dále zdůrazňuje, že ochrana mediálního odvětví před politickým, hospodářským nebo strukturálním ovládnutím je předpokladem pro zajištění demokratické odolnosti; konstatuje, že ochrana nezávislých médií má zásadní význam pro boj proti hybridním hrozbám ze strany nepřátelských aktérů; dále uvádí, že v této souvislosti současné digitální informační prostředí často znevýhodňuje mediální subjekty, které přebírají redakční odpovědnost a povinnosti ve veřejném zájmu, ve prospěch zprostředkovatelů, kteří nenesou srovnatelné povinnosti; vítá průlomové společné minimální normy pro svobodu a pluralitu médií stanovené v nedávno přijatém evropském aktu o svobodě médií; připomíná členským státům povinnosti stanovené v nařízení, pokud jde o ochranu médií před nepatřičnou koncentrací mediálního trhu; zdůrazňuje však, že význam aktu o svobodě médií

lze posoudit pouze na základě jeho praktického uplatňování; vyzývá členské státy, aby urychleně provedly evropský akt o svobodě médií, a Komisi, aby zajistila důsledné prosazování jeho ustanovení, včetně přijetí opatření v případě nedodržení povinností, zejména povinností velmi velkých online platforem, jejichž cílem je chránit redakční obsah před nepatřičným odstraněním nebo omezením viditelnosti; vítá nové závazky v oblasti podpory médií prostřednictvím Programu pro odolnost médií a vyzývá k harmonizaci dlouhodobých závazků v nadcházejícím VFR; dále poukazuje na to, že finanční krize, které čelí evropská média, ukazuje, že je třeba prozkoumat nová řešení v oblasti financování;

38. poukazuje na to, že je třeba pečlivě posuzovat možný dopad iniciativ EU na žurnalistiku a redakční média, zejména s ohledem na zajištění plurality médií a životaschopnosti obchodních modelů mediálních společností; vyzývá k posouzení dopadů založenému na důkazech a k náležitým konzultacím se zúčastněnými stranami v oblasti médií, předtím než se přistoupí k iniciativám, které mohou ovlivnit životaschopnost evropských mediálních společností; v této souvislosti zdůrazňuje, že je důležité sledovat vývoj ovlivňující svobodu a pluralitu médií v celé EU, a považuje výroční zprávu o právním státu se svou kapitolou o svobodě a pluralitě sdělovacích prostředků za ústřední nástroj v tomto úsilí; vyzývá Komisi, aby tento pilíř zprávy dále rozvíjela s cílem lépe zachytit nové výzvy;
39. v souvislosti s mediálními společnostmi, které nabízejí předplatné prostřednictvím aplikací, zdůrazňuje, že je důležité plně provést nařízení o digitálních trzích a účinně jej uplatňovat; bere na vědomí rozhodnutí Komise ze dne 23. dubna 2025 o porušení předpisů společnostmi Apple a Meta a její pokračující šetření ve věci možného porušení nařízení o digitálních trzích společností Google z důvodu odsouvání obsahu vydavatelů sdělovacích prostředků ve výsledcích vyhledávání na nižší pozice; poukazuje na to, že důsledné a včasné prosazování aktu o digitálních trzích má zásadní význam pro zajištění spravedlnosti, hospodářské soutěže a plurality v digitálním prostředí EU a pro řešení strukturálních závislostí a koncentrace trhu, a to i v souvislosti se službami založenými na umělé inteligenci;
40. vítá skutečnost, že společné sdělení obsahuje nová podpůrná opatření na prohloubení digitální a mediální gramotnosti, jako je Program pro odolnost médií, Program na podporu základních dovedností pro školy a posílení expertní skupiny pro mediální gramotnost, včetně zřízení nové sítě odborníků na mediální gramotnost, a aktualizované pokyny pro učitele a vzdělavatele; poukazuje na to, že stávající iniciativy v oblasti mediální gramotnosti jsou v EU i nadále roztržštěné; vyzývá k soudržnějším celounijním přístupům a k prozkoumání doplňkových opatření, včetně vytvoření digitálních nástrojů a platforem na úrovni EU; vybízí k systematické výměně osvědčených postupů mezi vnitrostátními orgány, mimo jiné prostřednictvím posílené skupiny odborníků pro mediální gramotnost

a střediska EDMO; dále poukazuje na úlohu kulturního vzdělávání při posilování demokratické gramotnosti a odolnosti vůči dezinformacím; zdůrazňuje, že nadcházející revize směrnice o audiovizuálních mediálních službách by měla posílit ustanovení o minimálních požadavcích na činnost členských států v oblasti mediální gramotnosti; klade důraz na to, že je důležité podporovat kritické chápání obsahu vytvořeného umělou inteligencí v rámci širšího úsilí v oblasti mediální a digitální gramotnosti;

41. vítá ohlášenou aktualizaci doporučení Komise o bezpečnosti novinářů⁶² a nadcházející přezkum doporučení, jež se týká strategických žalob proti účasti veřejnosti⁶³; zdůrazňuje, že tyto aktualizace a přezkumy musí zohledňovat vyvíjející se a opakující se povahu hrozeb, násilí, sabotáží a dalších opatření, jejichž cílem je zabránit novinářům v práci, včetně nových výzev, jako jsou krádeže identity a koordinované kampaně deepfake, které mohou ohrozit bezpečnost a nezávislost novinářů; zdůrazňuje, že je třeba věnovat zvláštní pozornost odrazujícím účinkům vyvolaným přetrvávající atmosférou strachu, politického tlaku nebo nepatřičného vměšování veřejných či soukromých subjektů; vyzývá členské státy, aby v souladu se svými vnitrostátními právními rámci a zavedenými postupy zvážily zavedení zvláštních přitěžujících okolností do trestního práva u trestných činů spáchaných proti novinářům, pokud jsou tyto činy motivovány jejich profesní činností nebo s ní souvisejí; dále bere na vědomí potenciální význam vypracování podpůrných opatření na pomoc novinářům při řešení nových problémů, jako je vydávání se za jinou osobu založené na AI a deepfake obsah;
42. zdůrazňuje, že je důležité chránit novináře před zneužívajícími soudními řízeními; vítá v tomto ohledu přijetí směrnice proti strategickým soudním řízením proti účasti veřejnosti a ohlášenou aktualizaci mandátu a složení skupiny odborníků proti zneužívajícím soudním řízením proti účasti veřejnosti; vyzývá členské státy, aby byly v probíhajícím procesu provádění ambiciózní, a Komisi, aby i nadále poskytovala podporu a přednostně zajistila úplné a včasné uplatňování směrnice; žádá Komisi, aby vypracovala komplexní hodnotící zprávu o účinnosti provádění; dále vyzývá EU a členské státy, aby zvážily další opatření k doplnění směrnice s cílem chránit novináře zapojené do investigativní práce, zejména v přeshraničním nebo citlivém kontextu; v této souvislosti

⁶² Doporučení Komise (EU) 2021/1534 ze dne 16. září 2021 o zajištění ochrany, bezpečnosti a posílení postavení novinářů a dalších pracovníků sdělovacích prostředků v Evropské unii (Úř. věst. L 331, 20.9.2021, s. 8, ELI: <http://data.europa.eu/eli/reco/2021/1534/oj>).

⁶³ Doporučení Komise (EU) 2022/758 ze dne 27. dubna 2022 o ochraně novinářů a obránců lidských práv, kteří se podílejí na účasti veřejnosti, před zjevně neopodstatněnými nebo zneužívajícími soudními řízeními („strategické žaloby proti účasti veřejnosti“) (Úř. věst. L 138, 17.5.2022, s. 30, ELI: <http://data.europa.eu/eli/reco/2022/758/oj>).

zdůrazňuje probíhající diskusi o zavedení evropského statusu ochrany investigativních novinářů jako možného řešení, které je třeba prozkoumat;

43. uznává zásadní úlohu veřejnoprávních médií při zajišťování toho, aby všichni občané, včetně občanů v odlehlejších a menšinových komunitách a kandidátských zemích, měli přístup ke spolehlivým, nestranným a rozmanitým zprávám na různých platformách, v různých formátech a jazycích, čímž tato média přispívají k boji proti rozšiřování oblastí bez zpravodajství; zdůrazňuje, že přístup ke kvalitním a spolehlivým informacím má zásadní význam v boji proti misinformacím a dezinformacím; znovu potvrzuje, že ochrana veřejnoprávních médií před politickým vměšováním a ovládnutím má zásadní význam pro zachování demokratické odpovědnosti a právního státu; zdůrazňuje, že důvěryhodnost veřejnoprávních médií závisí na plné redakční a organizační autonomii v souladu s článkem 5 aktu o svobodě médií, a vyzývá Komisi, aby aktivně sledovala hrozby pro nezávislost veřejnoprávních médií a přijala účinná opatření proti praktikám, které ohrožují jejich svobodu; v této souvislosti konstatuje, že pokusy o oslabení nezávislosti veřejnoprávních sdělovacích prostředků mohou být prvními ukazateli úpadku demokracie;
44. důrazně poukazuje na to, že je třeba zajistit co nejvyšší úroveň ochrany pro novináře a jiné mediální aktéry před špiónážním softwarem, invazivními sledovacími technologiemi a dalšími formami digitálních hrozeb; připomíná, že evropský akt o svobodě médií důrazně zakazuje členským státům, aby používaly invazivní sledovací software na jakýkoli materiál, digitální zařízení, stroj nebo nástroj používaný poskytovateli mediálních služeb nebo jejich redakčními pracovníky, s výjimkou případů týkajících se národní bezpečnosti; dále zdůrazňuje, že sledování novinářů představuje porušení práv, která zaručují články 7, 8 a 11 Listiny základních práv Evropské unie; konstatuje, že používání špiónážního softwaru oslabuje práci novinářů tím, že narušuje důvěru jejich zdrojů vůči nim, a že neschopnost účinně prosazovat legislativu EU je vážným ohrožením svobody informací;
45. znovu potvrzuje význam transparentnosti, spravedlivé hospodářské soutěže a udržitelnosti evropských redakčních médií v rámci stávajícího právního rámce, včetně nařízení o digitálních službách, nařízení o digitálních trzích, evropského aktu o svobodě médií a nařízení o transparentnosti a cílení politické reklamy; konstatuje, že tyto nástroje řeší manipulaci, zahraniční vměšování a protisoutěžní praktiky a zároveň chrání redakční odpovědnost a svobodu projevu; žádá Komisi, aby posoudila, jak lze tyto nástroje pro uvedené účely nejlépe využít; vyzývá velmi velké online platformy a velmi velké internetové vyhledávače, aby neodůvodněně neodstraňovaly a neodsouvaly zákonný evropský redakční mediální obsah, ani jinak neovlivňovaly jeho viditelnost a spravedlivé pořadí

a také aby zajistily transparentní a nediskriminační systémy určování pořadí;

46. vyzývá Komisi, aby dále zkoumala a případně zvážila opatření ke zlepšení konkurenceschopnosti, dostupnosti a spravedlnosti internetové reklamy pro všechny subjekty hodnotového řetězce, včetně redakčních médií; konstatuje, že redakčně nezávislá, kvalitní a na faktech založená žurnalistika čelí výzvám vyplývajícím z doporučovací systémů založených na interakci a z vyhledávacích funkcí velmi velkých online platforem založených na AI, které snižují viditelnost kvalitního obsahu a omezují návštěvnost internetových stránek médií; se znepokojením konstatuje, že v souvislosti se zavedením shrnutí obsahu umělou inteligencí ve vyhledávači Google klesla v jednom měřeném případě návštěvnost až o 70 % ; vybízí k pobídkám pro inzerenty, aby podporovali důvěryhodná evropská média, využívání kontextové reklamy namísto behaviorálního cílení a větší sledovatelnost a transparentnost v dodavatelském řetězci internetové reklamy s cílem řešit narušení trhu a zabránit nepřátelským subjektům zpeněžovat dezinformační obsah a záměrně destabilizovat společnost v EU; vyzývá v této souvislosti Komisi, aby posoudila možná opatření na podporu rozvoje a využívání evropské infrastruktury pro kontextovou reklamu na internetu;
47. vítá nedávné přijetí nařízení o přímých zahraničních investicích⁶⁴, zejména ustanovení, která zahrnují mediální odvětví jako faktor, který je třeba vzít v úvahu při určování, zda investice může negativně ovlivnit bezpečnost nebo veřejný pořádek; vyjadřuje nicméně politování nad tím, že mediální odvětví není uvedeno v povinné oblasti působnosti v příloze nařízení; v této souvislosti zdůrazňuje, že je třeba zvýšit transparentnost investic do evropských zpravodajských médií; dále poukazuje na to, že audiovizuální média se sídlem v EU podléhají přísnějším požadavkům než média se sídlem mimo EU, která jsou k dispozici publiku v EU prostřednictvím jiných způsobů distribuce; klade důraz na to, že je důležité zajistit, aby média, která jsou přístupná publiku EU, dodržovala spravedlivé a pluralitní informační standardy;
48. vyzývá Komisi a členské státy, aby pečlivě analyzovaly důsledky změny politiky pomoci ze strany vlády USA v souvislosti s pluralitou sdělovacích prostředků a nezávislou žurnalistikou a aby v případě potřeby podnikly kroky k zaplnění mezery, která zůstala na mediálních trzích v EU i v příhraničních regionech, a to i prostřednictvím nástroje Globální Evropa; vítá mimořádné financování EU poskytnuté rozhlasové organizaci Svobodná Evropa (RFE/RL); vyzývá k vypracování řešení, které by RFE/RL poskytlo

⁶⁴ Nařízení Evropského parlamentu a Rady (EU) 2019/452 ze dne 19. března 2019, kterým se stanoví rámec pro prověřování přímých zahraničních investic směřujících do Unie (Úř. věst. L 79I, 21.3.2019, s. 1, ELI: <http://data.europa.eu/eli/reg/2019/452/oj>).

stabilní a dlouhodobé financování; žádá Komisi, aby prozkoumala nové způsoby podpory svobodných a redakčně nezávislých médií v sousedství EU, zejména v regionech, které jsou neúměrně zasaženy ruskými dezinformacemi a propagandou, jako je západní Balkán;

49. poukazuje na to, že nezávislé společenské sítě pro ověřování faktů mohou hrát úlohu při odhalování dezinformačních kampaní a boji proti nim a poskytnout cenné poznatky pro posuzování a zmírňování rizik podle nařízení o digitálních službách; konstatuje, že nezávislé organizace pro ověřování faktů potřebují technickou podporu a stabilní podmínky pro svou činnost; domnívá se, že cenným nástrojem k dosažení tohoto cíle by mohla být evropská síť ověřovatelů faktů, jejíž zřízení Komise oznámila v roce 2025; zdůrazňuje, že aby byly organizace ověřující fakta důvěryhodné a efektivní, musí dodržovat přísné normy politické neutrality, nezávislosti na poskytovatelích online platforem a metodické objektivitě; klade důraz na význam spolupráce mezi ověřovateli faktů, výzkumnými pracovníky v oblasti OSINT, novináři, komunikátory a tvůrci politik; dále zdůrazňuje, že je důležité podporovat síť ověřovatelů faktů v kandidátských a potenciálních kandidátských zemích;

Občanská společnost, akademická obec, kultura a občanská angažovanost

50. zdůrazňuje klíčovou úlohu aktivní, živé a nezávislé občanské společnosti jako jednoho z hlavních pilířů při obraně naší demokracie, a to nejen tím, že působí jako strážce a odhaluje zlovolné zasahování do demokratických procesů a aktivně proti nim bojuje, ale také tím, že je základní silou v dlouhodobém úsilí o budování silnějších a odolnějších společností; poukazuje zejména na důležitou úlohu občanské společnosti při prosazování hodnot zakotvených v článku 2 SEU;
51. vítá strategii EU pro občanskou společnost, kterou zveřejnila Komise spolu se společným sdělením o Evropském štítu pro demokracii; vítá přístup Komise, který propojuje tuto strategii – jako nástroj k dalšímu posílení občanské angažovanosti – s činností týkající se Evropského štítu pro demokracii; považuje strategii za důležitý první krok, neboť představuje první komplexní přístup EU k občanské společnosti, přičemž konstatuje, že je třeba, aby další kroky byly ambicióznější a zahrnovaly opatření k účinné ochraně úlohy občanské společnosti v demokratických procesech; poukazuje na to, že budoucí iniciativy v této oblasti by se měly zabývat zmenšujícím se občanským prostorem a zároveň uznat, že organizace občanské společnosti a obránci lidských práv jsou obzvláště zranitelní, což platí zejména pro organizace zabývající se konkrétními tématy, jako jsou LGBTIQ+ osoby, rovnost žen a mužů a boj proti rasismu;

52. vyzývá Komisi, aby posílila svou činnost v oblasti občanského dialogu a vytvořila za tímto účelem nové nástroje; vítá v této souvislosti závazek Komise zřídit do roku 2026 funkční platformu občanské společnosti s cílem podpořit systematictější přístup, který bude využíván k posílení dialogu v souladu s hodnotami EU; domnívá se, že ohlášené online znalostní centrum pro občanský prostor může přispět ke koordinaci činností organizací občanské společnosti v oblasti ochrany demokracie a boje proti hybridním hrozbám, zahraniční manipulaci s informacemi a vměšování a nadnárodní represi a zlepšit informovanost o situaci; v této souvislosti zdůrazňuje význam občanské angažovanosti zaměřené na diasporu; dále připomíná, že části občanské společnosti mají rozsáhlé zkušenosti se zahraničním vměšováním a měly by být v rámci občanského dialogu zapojeny do utváření politiky pro jeho řešení;
53. zdůrazňuje úlohu a odpovědnost občanské společnosti v demokratických procesech v kandidátských zemích; vyzývá Komisi, aby v rámci možností v tomto dialogu spolupracovala s organizacemi občanské společnosti z kandidátských a potenciálních kandidátských zemí na stávajících a budoucích iniciativách Strategie EU pro občanskou společnost, zejména s těmi, které soustavně podporují soulad v digitální oblasti, informační integritu a demokratickou odolnost;
54. vyzývá členské státy, aby zajistily udržitelné a diverzifikované financování organizací občanské společnosti, včetně stabilní provozní podpory a opatření na budování kapacit, uznaly jejich zásadní úlohu při prosazování demokratických hodnot a umožnily jejich účinné a nezávislé fungování; zdůrazňuje význam konkrétních programů financování EU, které toto úsilí doplní, jako je program Občané, rovnost, práva a hodnoty (CERV); vítá úmysl Komise zachovat program CERV a začlenit jej do nového programu AgoraEU na období 2028–2034; vyzývá spolunormotvůrce, aby zajistili ambiciózní a předvídatelné financování této složky programu AgoraEU, které odpovídá potřebám organizací občanské společnosti a bude prováděno pod přímým řízením Komise;
55. klade důraz na to, že kultura je strategickým pilířem evropského projektu, neboť kulturní svoboda, dědictví a tvořivost podporují demokratickou účast, kritické myšlení a důvěru v instituce; poukazuje na skutečnost, že programy, jako je AgoraEU, mohou hrát klíčovou úlohu při převádění těchto hodnot do hmatatelné podpory; se znepokojením konstatuje, že útoky na liberální demokracii se stále častěji zaměřují na kulturní subjekty a instituce, zejména prostřednictvím různých forem politického nátlaku; zdůrazňuje proto, že ochrana umělecké svobody a kulturních institucí má zásadní význam pro obranu demokracie v EU;
56. poukazuje na to, že je důležité zachovat evropskou kulturní historii a kolektivní paměť a bojovat proti manipulaci a falšování historických

skutečností s cílem posílit demokratickou odolnost; v této souvislosti zdůrazňuje, že je třeba posílit společnou evropskou kulturu historického povědomí, a opakuje, že podporuje celoevropský památník obětem totalitních režimů 20. století, jakož i vypracování zprávy Komise o evropském historickém povědomí do začátku roku 2027; odsuzuje historický revizionismus ruského režimu a jeho používání zkreslených narativů k popírání svrchovanosti dříve podmaněných národů a k ospravedlnění zahraničního vměšování;

57. připomíná, že různí zástupci zájmových skupin, včetně organizací občanské společnosti, think tanků a zastřešujících organizací mohou být a jsou využíváni nepřátelskými subjekty ze třetích zemí jako nástroje k nezákonnému ovlivňování demokratických procesů v EU a jejích členských státech; zdůrazňuje, že opatření v oblasti finanční transparentnosti, jsou-li vhodně navržena a obsahují-li záruky zohledňující velikost organizací, mohou pomoci zmírnit riziko budoucího nepatřičného vlivu autoritářských států; klade důraz na to, že Parlament jako orgán nese zvláštní odpovědnost za posílení standardů integrity, transparentnosti a odpovědnosti s ohledem na zkušenosti získané z minulých případů korupce a zahraničního vměšování; poukazuje však na to, že opatření k řešení této otázky by měla být koncipována tak, aby nemohla být zneužita ke stigmatizaci legitimních aktivit občanské společnosti a jejich rozhodující úlohy při posilování našich demokracií;
58. zdůrazňuje důležitost návrhu směrnice o zastupování zájmů jménem třetích zemí, který předložila Komise, jako důležité součásti balíčku opatření na obranu demokracie, jehož cílem je stanovit harmonizované požadavky na hospodářské činnosti související se zastupováním zájmů prováděným jménem subjektů ze třetích zemí; zdůrazňuje, že společná pravidla v tomto ohledu mohou přispět k odpovědnosti a důvěře v rozhodování EU tím, že zavedou transparentnost, pokud jde o vliv třetích zemí; vyzývá spolunormotvůrce, aby legislativní proces neprodleně dokončili; klade důraz na to, že členské státy by měly zajistit, aby dodržování této směrnice nevedlo k omezování základních práv;
59. zdůrazňuje význam zapojení občanů do demokratických procesů; naléhavě vyzývá Komisi, aby ve spolupráci s členskými státy zajistila jasnou a účinnou komunikaci o iniciativách, které vyvíjí na podporu a širší využívání nástrojů pro zapojení občanů, které jsou dostupné, uživatelsky vstřícné, mnohojazyčné a schopné proniknout k občanům ve velkém rozsahu; vítá posílení těchto nástrojů, zejména evropské občanské iniciativy, evropských panelových diskusí občanů a Platformy aktivního občanství, ze strany Komise a návrh na posílení sítě vnitrostátních orgánů pro účast občanů; v této souvislosti poukazuje na to, že je důležité aktivně zapojovat mladé lidi do demokratického života, a uznává, že jsou klíčovými aktéry při posilování občanské a politické účasti, mimo jiné prostřednictvím rozvoje participativních digitálních platforem a rad mládeže s cílem

zajistit smysluplné zapojení do rozhodovacích procesů na místní, vnitrostátní a unijní úrovni;

60. poukazuje na to, že akademická svoboda, včetně svobody výzkumu, výuky a akademického projevu, představuje základní pilíř demokratických společností; odsuzuje útoky na akademickou svobodu a zdůrazňuje, že je třeba posílit nezávislost evropského výzkumu a jeho odolnost vůči zahraničnímu vměšování; varuje zejména před manipulací s historií ze strany zahraničních aktérů; znovu vyzývá Komisi, aby předložila legislativní návrh na ochranu základní svobody vědeckého výzkumu, včetně minimálních norem pro práva výzkumných pracovníků, etické chování, integritu a institucionální nezávislost, která bude podpořena účinnými monitorovacími mechanismy;

Ochrana kritické infrastruktury

61. zastává názor, že ochrana EU a jejích členských států před fyzickými i kybernetickými akty sabotáže zaměřenými na kritickou infrastrukturu má zásadní význam pro zajištění demokratické odolnosti; vyzývá k přijetí aktivní odrazovací strategie, důrazných preventivních opatření, posílení přeshraniční spolupráce a posílení schopnosti EU odhalovat tyto nepřátelské činnosti, odrazovat od nich a reagovat na ně; zdůrazňuje, že skutečnost, že kritickou infrastrukturu vlastní zahraniční subjekty propojené se státem, zvyšuje expozici vůči bezpečnostním rizikům a vyžaduje zvýšenou kontrolu, zejména pokud jde o komunikační infrastrukturu, digitální infrastrukturu, podmořské kabely, energetickou infrastrukturu, dopravní uzly, nemocnice a infrastrukturu veřejných služeb;
62. důrazně odsuzuje eskalující průniky dronů a další zásahy ze vzduchu, zejména ze strany Ruska a Běloruska, které cílí na kritickou infrastrukturu, včetně civilních letišť, přístavů, vojenských základen, průmyslových center, infrastruktury pro správu hranic a energetických zařízení v celé EU, a mají ji narušit; vyzývá členské státy, aby koordinovaně, jednotně a vhodným způsobem reagovaly na jakékoli narušení svého vzdušného prostoru, a to i sestřelením letadel, dronů a dalších hrozeb ze vzduchu; naléhavě žádá Komisi a členské státy, aby pracovaly na programech předávání znalostí s Ukrajinou a na společném výcviku a certifikaci pilotů dronů s ohledem na znalosti získané na Ukrajině o vedení moderní války;
63. klade důraz na strategickou úlohu agentur EU při zajišťování ochrany přeshraniční kritické infrastruktury v EU a jejích členských státech, jakož i potřebu posílit spolupráci v oblasti námořních přístavů, letišť a pozemních hraničních přechodů, a to i prostřednictvím společných posouzení zranitelnosti; upozorňuje zejména na hrozby rušení a spoofingu GPS ze strany Ruska a Běloruska a na jejich potenciál narušit provoz kritické

infrastruktury, ohrožit bezpečnost plavby a oslabit kontinuitu a odolnost základních přeshraničních služeb;

64. zdůrazňuje, že řada hybridních činností, které Rusko podniklo proti EU, představuje státem podporovaný terorismus, i když tyto aktivity nepřekročily hranici ozbrojeného útoku; upozorňuje, že na nepřátelské aktivity Ruska, které porušují územní svrchovanost členských států EU, narušují integritu jejich institucí a přímo ohrožují bezpečnost civilního obyvatelstva, je třeba uplatňovat všechny dostupné právní rámce pro boj proti terorismu; poukazuje na to, že EU musí urychleně přejít od režimu obrany k aktivnímu odstrašování; naléhavě vyzývá členské státy, aby vyhodnotily právní a operační rámce pro přiměřená ofenzivní opatření zaměřená na logistickou a digitální infrastrukturu, která stojí za destabilizačními činnostmi Moskvy; konstatuje, že Rusko je zranitelné vůči kybernetickým operacím, jak prokázalo narušení činnosti ruské společnosti Aeroflot skupinou Cyber Partisans; vyzdvihuje rozsáhlé zkušenosti Ukrajiny s poškozováním ruských kapacit a potřebu urychlit poskytování podpory Ukrajině pro posílení jejich útočných kybernetických schopností;
65. poukazuje na to, že by měla být dále posílena přeshraniční koordinace v boji proti hybridním hrozbám v námořních oblastech, a to na základě vyčleněných a odpovídajících finančních prostředků EU, a že EU musí zintenzivnit svou operativní reakci, zejména na hrozby spojené s ruskou stínovou flotilou; vyzývá v této souvislosti Komisi a členské státy, aby vypracovaly koordinovaný a celounijní výklad Úmluvy OSN o mořském právu (UNCLOS) s cílem zajistit soudržný postup proti hybridním činnostem, sabotážím, nehlášenému, nezákonnému a neregulovanému rybolovu a porušování svrchovaných práv v námořních oblastech EU, zejména v Baltském moři, a zároveň připomíná cíl úmluvy UNCLOS, kterým je zajistit mírové využívání moří; vítá dále doporučení Komise o bezpečných a odolných podmořských kabelových infrastrukturách⁶⁵ a akční plán EU pro bezpečnost kabelů; naléhavě vyzývá Komisi a členské státy, aby urychlily provádění těchto iniciativ zmapováním kabelové infrastruktury, vypracováním koordinovaného posouzení rizik a zátěžových testů, zavedením zmírňujících opatření a posílením schopnosti reakce na incidenty a schopnosti nápravy, mimo jiné podporou modulárního opravárenského vybavení a udržováním strategických zásob základních náhradních dílů;
66. vyzývá k účinné kriminalizaci a odrazování od hybridních činností a sabotáží, včetně útoku na podmořské kabely a konektory; vybízí Komisi a členské státy, aby se poučily z australského příkladu zřízení

⁶⁵ Doporučení Komise (EU) 2024/779 ze dne 26. února 2024 o bezpečných a odolných podmořských kabelových infrastrukturách (Úř. věst. L, 2024/779, 8.3.2024, ELI: <http://data.europa.eu/eli/reco/2024/779/oj>).

tzv. zón ochrany kabelů, které poskytují právní záruky a kriminalizují poškození podmořských kabelů za hranicí teritoriálního moře 12 námořních mil a které doplňuje aktivní sledování, dohled a reakce ve spolupráci s příslušnými partnery ze třetích zemí;

67. vybízí členské státy, aby prozkoumaly možnost využití mandátu bezpečnostní iniciativy proti šíření zbraní hromadného ničení (PSI) ke vstupu na palubu plavidel napojených na tyto stínové flotily, a vyzývá Finanční akční výbor, aby v rámci svých postupů vzájemného hodnocení a zařazování jurisdikcí na šedou listinu hrál aktivnější úlohu při kontrole správy rejstříku vlajek;
68. opět vyzývá k tomu, aby byla v reakci na útočnou válku Ruska proti Ukrajině v Černém moři, Severním moři a Baltském moři zřízena evropská centra pro námořní bezpečnost, a zdůrazňuje, že tato centra by měla zlepšit informovanost o situaci na moři, umožnit monitorování situace v reálném čase z vesmíru až po mořské dno, a posílit kapacity včasného varování a reakce na zvýšené hrozby ruské stínové flotily a zároveň zohledňovat environmentální hledisko a zajistit bezpečnost obchodních tras; vyzývá Komisi a členské státy, aby zabránily tomu, aby lodě stínové flotily vplouvaly do evropských vod, a aby prováděly časté a důkladné inspekce těchto plavidel, aby se zajistilo, že tyto lodě neporušují žádné zákony a nepředstavují žádné nebezpečí;
69. důrazně poukazuje na to, že stávající strukturální závislosti, které vyplývají z koncentrace trhu a zahraniční kontroly – včetně dominantního postavení velkých amerických technologických společností – v oblasti digitální infrastruktury EU, operačních systémů, datových center, výroby polovodičů, umělé inteligence, nástrojů pro rozhodování založené na datech, platební infrastruktury, kybernetické bezpečnosti, cloud computingu a různých online platform a služeb, představují vysoké riziko pro demokracii, svobodu, bezpečnost a konkurenceschopnost v rámci EU; vyjadřuje politování nad nedávnými incidenty, při nichž společnosti Microsoft, Visa a Mastercard pozastavily služby a zastavily transakce se zaměstnanci Mezinárodního trestního soudu, na něž se vztahují sankce USA; v této souvislosti zdůrazňuje zranitelnost EU vůči podobným vnějším rozhodnutím, která by mohla narušit veřejné služby a hospodářské činnosti; vyzývá Komisi, aby do Evropského štítu pro demokracii systematicky začleňovala cíle v oblasti snižování závislosti a budování evropských průmyslových kapacit;
70. považuje odolnou a konkurenceschopnou digitální infrastrukturu EU – včetně bezpečných místních datových center, suverénního cloudu EU, kapacit pro edge computing a gigabitových sítí – za strategický pilíř digitální odolnosti, který zajišťuje otevřenost, hospodářskou soutěž a globální interoperabilitu; zdůrazňuje, že tato infrastruktura by měla pomoci chránit citlivé údaje občanů EU před riziky spojenými s ukládáním v zahraničí a vystavením se právním

předpisům zemí mimo EU a řešit složité otázky týkající se zahraničního vlastnictví a investic do základních infrastruktur, mimo jiné prostřednictvím zátěžových testů digitální autonomie s cílem zmapovat závislost na velkých komerčních technologických společnostech, pokud jde o základní veřejné služby; vyjadřuje politování nad tím, že po šesti letech přípravy evropského systému certifikace kybernetické bezpečnosti pro cloudové služby (EUCS) stále chybí úroveň záruky certifikace, která by evropským poskytovatelům cloudových služeb umožnila zaručit nejvyšší ochranu strategických údajů před mimoevropskými jurisdikcemi, a zdůrazňuje, že spolehlivá certifikace kybernetické bezpečnosti má zásadní význam pro integritu a odolnost digitálních služeb, na nichž jsou založeny demokratické procesy; zdůrazňuje, že prostřednictvím aktu pro rozvoj cloudu a umělé inteligence a revidovaného aktu o kybernetické bezpečnosti by měla být obnovena práce na systému EUCS; vítá zavedení odstupňovaných úrovní záruky EU v návrhu aktu pro rozvoj cloudu a umělé inteligence a vyzývá k tomu, aby nejvyšší úroveň záruky zajistila účinnou ochranu nejcitlivějších a strategických údajů před přístupem v jurisdikcích mimo EU a zároveň nevytvářela zbytečné překážky pro inovace a investice;

71. zdůrazňuje, že je třeba řešit rizika spojená se strategickými a citlivými hardwarovými a softwarovými součástmi a službami připojenými k síti, které umožňují dálkový přístup, přenos dat nebo kontrolu systému a jež pocházejí z vysoce rizikových třetích zemí včetně Číny; se znepokojením bere na vědomí rizika spojená s dominantním postavením čínských solárních střídačů a dalších komponent, které jsou v některých případech uváděny na trh EU za uměle nízké ceny prostřednictvím státem podporovaných netržních postupů; v této souvislosti vítá, že revidovaný akt o kybernetické bezpečnosti, tak jak je navržen, má za cíl vytvořit rámec pro zákaz komponent připojených k síti, které umožňují vzdálený přístup, jako jsou například střídače, od dodavatelů představujících vysoké riziko, a že strategický plán pro digitalizaci a umělou inteligenci v energetickém odvětví počítá s posouzením rizik solárních zařízení a s přezkoumáním rámce pro bezpečnost dodávek energie; vyzývá k urychlenému přijetí těchto opatření na ochranu kritické energetické infrastruktury před manipulací na dálku, výpadky a riziky spojenými s dodavatelským řetězcem; vyzývá Komisi a členské státy, aby podporovaly bezpečné alternativy se sídlem v EU a vyráběné v EU, přezkoumaly stávající pravidla pro zadávání veřejných zakázek s cílem posoudit, zda brání digitální suverenitě, a usilovaly o komplexní agendu technologické suverenity EU s jasnými normami odolnosti a kritérii pro vývoj nebo pořízování technologií nebo digitální infrastruktury a zajistily, aby regulační rámce, obchodní politiky a politiky hospodářské soutěže účinně předcházely nekalým tržním praktikám a snižovaly závislost na poskytovatelích ze zemí mimo EU; zdůrazňuje, že klíčem k úspěchu v digitální oblasti je hospodářská soutěž, otevřenost a technologická excelence a že EU by měla mít strategii zaměřenou na přilákání,

udržení a zachování klíčových technologií, přičemž by měla náležitě zohledňovat faktory související se zahraničními akvizicemi; opětovně zdůrazňuje, že je třeba se v oblasti kritické infrastruktury řídit politikou „nakupovat evropské“, která by měla být koncipována a prováděna vyváženým a přiměřeným způsobem; podporuje svrchovanou digitální infrastrukturu EU s technologiemi zvyšujícími soukromí a ekosystém rozhraní EU pro programování aplikací (API), který využívá energii bez fosilních paliv pro datová centra a cloudovou infrastrukturu, a to i prostřednictvím tržně orientovaných iniciativ a iniciativ veřejného a soukromého sektoru, jako jsou společné podniky nebo sdružené sítě v oblastech, jako je umělá inteligence, gigatovárný a cloudové služby;

72. vítá cíle stanovené v evropském nařízení o kritických surovinách (CRMA) v oblasti těžby, zpracování, recyklace a snižování spotřeby kritických surovin a zdůrazňuje, že v době náhlé krize se závislost na čínských vzácných zeminách může ukázat jako stejně škodlivá jako závislost na ruských zdrojích uhlíku; opětovně zdůrazňuje nutnost plného provádění nařízení o kritických surovinách, vytváření zásob, recyklace a nahrazování kritických surovin, urychlení diverzifikace zdrojů kritických surovin z Číny směrem k spolehlivějším partnerům, zvýšení vlastní těžby a zpracování v EU a efektivnějšího využívání zdrojů;
73. vyzývá k formálnímu uznání hackerských útoků na objednávku jako samostatné hrozby pro demokratické instituce a procesy, proti níž by bylo možné účinněji zasáhnout aktualizací definic v trestním právu; vybízí Komisi a členské státy, aby zahájily koordinovanou mezinárodní iniciativu zaměřenou na boj proti tzv. „neprůstřelným“ poskytovatelům hostingu, kteří vědomě pronajímají infrastrukturu pachatelům kybernetické kriminality, a to i prostřednictvím blokování a filtrování podvodných čísel autonomních systémů, s cílem účinně omezit jurisdikce, z nichž mohou tyto poskytovatelé působit; zdůrazňuje přetrvávající riziko obchodování se zranitelností podniků na darknetu, které vystavuje digitální komunikační systémy a zařízení zahraničnímu vměšování;
74. poukazuje na to, že je třeba zajistit větší integraci a strategickou koordinaci mezi zaváděním digitální infrastruktury, opatřeními proti zahraniční manipulaci s informacemi a vměšování a opatřeními proti dezinformacím a kybernetickou bezpečností a obrannou politikou s cílem posílit strategickou autonomii EU; zdůrazňuje, že je třeba využít infrastrukturu dvojího užití, jako jsou odolná datová centra rozptýlená v celé EU, aby byla zajištěna provozní kontinuita tváří v tvář přírodním katastrofám a hybridním nebo válečným hrozbám; dále poukazuje na to, že je třeba zvýšit investice do vojenské mobility a bezpečné komunikace, včetně bezodkladného a přednostního zavádění gigabitových sítí a vesmírných kapacit, jako je IRIS², s cílem poskytovat šifrované služby pro veřejné a obranné použití; vyzývá

k tomu, aby tyto kritické komunikační kapacity byly zpřístupněny Ukrajině a Tchaj-wanu;

75. zdůrazňuje, že je třeba zvýšit investice do bezpečných, interoperabilních a odolných systémů sdílení informací a místních datových center, na něž se nevztahují extraterritoriální právní předpisy; zdůrazňuje, že tyto investice mají zásadní význam pro zajištění rychlejší a spolehlivější komunikace mezi příslušnými orgány na vnitrostátní úrovni a na úrovni EU, pro posílení ochrany před kybernetickými útoky a narušením bezpečnosti údajů a pro zaručení integrity, dostupnosti a důvěrnosti citlivých údajů, mimo jiné prostřednictvím posílených schopností v oblasti kybernetické bezpečnosti a moderní digitální infrastruktury EU; zdůrazňuje, že redundance mají klíčový význam pro zajištění provozní bezpečnosti a bezpečnosti komunikace, jako jsou pozemní zabezpečené komunikační systémy nebo inerciální navigační systémy;
76. zdůrazňuje, že rámce kybernetické bezpečnosti, jako je směrnice NIS 2, akt o kybernetické odolnosti⁶⁶ a nařízení o kybernetické solidaritě⁶⁷, musí fungovat v souladu s cílem podpořit normy bezpečné již od fáze návrhu a zabránit roztržitosti právních předpisů; v této souvislosti bere na vědomí cílenou revizi směrnice NIS 2; vítá návrh Komise výrazně posílit a rozšířit operační mandát a zdroje agentury ENISA prostřednictvím revidovaného aktu o kybernetické bezpečnosti; vyzývá k tomu, aby revize výslovně zahrнула odborníky na zahraniční manipulace s informacemi a vměšování mezi zúčastněné strany zastoupené v poradní skupině agentury ENISA; vyzývá Komisi, aby zajistila dostatečné financování z VFR na období 2028–2034 s cílem zabezpečit, aby si podniky, zejména v odvětví IKT, mohly dovolit dodatečné investice vyplývající z revize aktu o kybernetické bezpečnosti; dále zdůrazňuje, že malé a střední podniky potřebují podporu při plnění předpisů, a to vedle výjimek, které by měly zajistit, aby nedošlo k oslabení jejich bezpečnosti a v důsledku toho ani celkové kybernetické bezpečnosti;
77. připomíná nízkou míru provedení směrnice NIS 2 ve vnitrostátním právu; vyjadřuje politování nad tím, že po uplynutí lhůty dne 17. října 2024 musela Komise zaslat formální upozornění nezvykle vysokému

⁶⁶ Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti) (Úř. věst. L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

⁶⁷ Nařízení Evropského parlamentu a Rady (EU) 2025/38 ze dne 19. prosince 2024, kterým se stanovují opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických hrozeb a incidentů a pro připravenost a reakci na ně a mění nařízení (EU) 2021/694 (nařízení o kybernetické solidaritě) (Úř. věst. L, 2025/38, 15.1.2025, ELI: <http://data.europa.eu/eli/reg/2025/38/oj>).

počtu 23 členských států, které tuto směrnici neprovedly v plném rozsahu; naléhavě vyzývá členské státy, aby co nejdříve dokončily provedení směrnice ve vnitrostátním právu, vzhledem k tomu, že na konci roku 2025, tedy více než rok po uplynutí lhůty, nebyla směrnice dosud provedena 10 členskými státy; vítá v tomto ohledu závazek Komise úzce spolupracovat s členskými státy na zajištění rychlého a soudržného provádění horizontálního rámce kybernetické bezpečnosti stanoveného ve směrnici NIS 2, jakož i aktu o kybernetické odolnosti a nařízení o kybernetické solidaritě, jak je stanoveno ve strategii vnitřní bezpečnosti ProtectEU; vyzývá Komisi a členské státy, aby podporovaly překlenutí nedostatků týkajících se informovanosti o situaci, zmírňování rizik a koordinovaných opatření pokrývajících kybernetická, hybridní a informační rizika současně;

Spolupráce v oblasti spravedlnosti a vnitřních věcí

78. zastává názor, že by měly být uplatňovány a případně dále rozvíjeny všechny trestněprávní nástroje dostupné na úrovni členských států a EU s cílem předcházet nezákonnému jednání, jehož cílem je podkopávat demokratické instituce a procesy, a bojovat proti takovému jednání; zdůrazňuje, že je třeba, aby příslušné vnitrostátní orgány byly vybaveny vhodnými nástroji a kanály spolupráce pro prevenci, vyšetřování, odhalování a stíhání trestných činů souvisejících se zahraničním vměšováním; domnívá se, že korupce a zastrasování volených a veřejných činitelů zločineckými sítěmi by měly být řešeny v rámci reakce EU na hybridní hrozby prostřednictvím posílené spolupráce mezi specializovanými protikorupčními agenturami, donucovacími orgány a příslušnými orgány Unie; žádá Komisi, aby posoudila přidanou hodnotu zavedení minimálních pravidel v právu Unie týkajících se definice trestného činu vědomé účasti na organizované činnosti vměšováním jménem zahraničních mocností a sankcí za tento trestný čin; konstatuje, že nadcházející revize mandátů rady orgánů EU v oblasti spravedlnosti a vnitřních věcí by mohla představovat příležitost k posílení operačního rozměru Evropského štítu pro demokracii; podporuje zejména závazek Komise k ambiciózní revizi mandátu Europolu, který by umožnil přeměnit jej ve skutečně operativní policejní agenturu, která bude lépe podporovat členské státy;
79. vítá skutečnost, že společné sdělení uznává pozitivní přínos spolupráce v oblasti trestního soudnictví a prosazování práva v boji proti zahraniční manipulaci s informacemi a vměšováním a dezinformačním činnostem; vyzývá spolutvůrce právních předpisů, aby v rámci přípravy plánované revize mandátů Europolu a Eurojustu pečlivě posoudili právní mezery a omezení, které v současné době těmto agenturám brání poskytovat plnou pomoc členským státům čelícím hybridním hrozbám, a aby prozkoumali, jakým způsobem je možné překonat tato omezení a současně respektovat základní práva a pravomoci založené na Smlouvách; domnívá se, že doplnění

hybridních hrozeb do přílohy I nařízení o Europolu⁶⁸ by vyjasnilo právní rámec a usnadnilo práci Europolu v této oblasti; dále zdůrazňuje, že je třeba zajistit, aby Europolu a Eurojustu byly poskytnuty odpovídající finanční a lidské zdroje k tomu, aby mohly účinně provádět posílení svých mandátů, k němuž má dojít;

80. považuje nadnárodní represe za rostoucí a vážnou hrozbu pro demokracii a vnitřní bezpečnost v EU; zdůrazňuje, že nadnárodní represe mohou být páčány online prostřednictvím nenávistných a pomlouvačných kampaní a šíření nezákonného obsahu, ale mohou také vést k fyzickým útokům a vraždám; se znepokojením zaznamenává rostoucí počet příkladů toho, jak nepřátelské subjekty ze zemí mimo EU využívají trestnou činnost jako službu a zločinecké organizace jako prostředníky v rámci EU k útokům na jednotlivce a subjekty označené za politické protivníky; zdůrazňuje, že tyto praktiky představují nepřijatelný akt zahraničního vměšování s potenciálně destabilizujícími účinky na naši společnost; v této souvislosti zdůrazňuje, že je třeba odstranit zbývající mezery v právu Unie a dále posílit koordinaci na úrovni EU v oblasti trestního soudnictví a prosazování práva prostřednictvím rámce policejní a justiční spolupráce zaměřeného na nadnárodní represe v rámci Evropského štítu pro demokracii a zároveň zapojit jednotlivce a skupiny, proti nimž jsou namířeny, a zajistit jejich ochranu; upozorňuje na to, že je naléhavě nutné řešit zneužívání červeného oběžníku Interpolu k politicky motivovaným účelům;
81. důrazně odsuzuje účelové využívání migrace třetími zeměmi nebo nepřátelskými nestátními subjekty s cílem destabilizovat členský stát nebo EU; zastává stanovisko, že tento jev představuje nepřijatelný pokus o vyvíjení politického tlaku na členské státy stojící v první linii a na EU; zdůrazňuje, že tyto praktiky rovněž představují závažné zneužívání zranitelných osob, které mohou mít nárok na mezinárodní ochranu, a neměly by mít nepříznivý dopad na právo žádat o azyl; bere na vědomí zvláštní ustanovení o účelovém využívání migrace, která byla nedávno zahrnuta do klíčových právních předpisů EU; dále vítá nedávnou revizi právního rámce EU s cílem zahrnout hybridní hrozby mezi důvody pro spuštění mechanismu EU pro pozastavení zrušení vízové povinnosti; zdůrazňuje, že důvěryhodná a účinná reakce EU musí být rovněž založena na úzké koordinaci a loajální spolupráci mezi sousedními členskými státy a mezi nimi a orgány EU v duchu loajality a vzájemné solidarity a na posílených technologických a operačních kapacitách v oblasti správy hranic při

⁶⁸ Nařízení Evropského parlamentu a Rady (EU) 2016/794 ze dne 11. května 2016 o Agentuře Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a o zrušení a nahrazení rozhodnutí 2009/371/SVV, 2009/934/SVV, 2009/935/SVV, 2009/936/SVV a 2009/968/SVV (Úř. věst. L 135, 24.5.2016, s. 53. ELI: <http://data.europa.eu/eli/reg/2016/794/oj>).

současném zachování integrity schengenského prostoru a zajištění plného dodržování základních hodnot EU;

82. bere na vědomí, že Komise oznámila revizi mandátu agentury Frontex; zdůrazňuje, že revize by měla poskytnout nezbytný právní základ, analytické kapacity a odpovídající lidské, finanční a technické zdroje, které umožní účinnou pomoc členským státům při správě a ochraně vnějších hranic v souladu s příslušnými právními předpisy Unie, včetně základních práv; v této souvislosti zdůrazňuje, že je třeba dále posílit schopnost EU podporovat členské státy v záležitostech souvisejících s vnitřními věcmi v rámci VFR na období 2028–2034, a to i v reakci na hrozby hybridní povahy;

Vnější rozměr

83. zdůrazňuje, že je třeba, aby měl Evropský štít pro demokracii silný vnější rozměr, a vítá opatření, která podporují země mimo EU, zejména prostřednictvím budování kapacit s cílem posílit odolnost kandidátských a potenciálních kandidátských zemí vůči zahraniční manipulaci s informacemi a vměšování, hybridnímu vměšování a nadnárodním represím, prostřednictvím podpory nezávislých sdělovacích prostředků a žurnalistiky a lepší schopnosti odhalovat dezinformace a bojovat proti nim před volbami a v jejich průběhu; zdůrazňuje potřebu adekvátního financování, včetně základního financování prostřednictvím nástroje „Globální Evropa“, pro nezávislá média v sousedních zemích; konstatuje, že kapacity a závazky kandidátských zemí se liší, což vyžaduje diferencované citlivé provádění Evropského štítu pro demokracii v závislosti na příslušném kontextu a při plném respektování hodnot EU; zdůrazňuje, že posílení demokratické odolnosti je klíčové jak pro důvěryhodnost rozšíření, tak pro bezpečnost a stabilitu EU; vyzývá k systematickému zapojení kandidátských zemí do příslušných opatření, podpůrných mechanismů a sítí odborníků v rámci vnějšího rozměru;
84. vyzývá k tomu, aby Evropský štít pro demokracii sloužil jako obousměrný mechanismus předávání odborných znalostí, v jehož rámci by Unie integrovala úspěšné modely rychlé reakce, rámce civilně-vojenské spolupráce a detekční techniky v reálném čase, a připomíná odborné znalosti partnerů v první linii, kteří čelí ruské agresi a vměšování; zdůrazňuje, že EU by si měla odnést značné ponaučení z posilování odolnosti v Moldavsku a na Ukrajině;
85. konstatuje, že Tchaj-wan má vedoucí úlohu ve vývoji špičkových technologií a má bohaté zkušenosti s obranou proti hybridním útokům Číny a zahraniční manipulaci s informacemi a vměšování; vyzývá k pravidelným výměnám informací o příslušných bezpečnostních otázkách, jakož i k užší spolupráci v boji proti zahraniční manipulaci s informacemi a vměšování a sabotáži

podmořských kabelů s podobně smýšlejícími partnery ve východní Asii, včetně Tchaj-wanu, Japonska a Jižní Koreje;

86. vyzývá k vypracování komplexní strategie v prioritních regionech, v jejímž rámci by byly v úzké koordinaci s diplomatickými misemi členských států EU mobilizovány delegace EU a mise a operace společné bezpečnostní a obranné politiky (SBOP) s cílem lépe porozumět místním okolnostem, které mohou vést k zahraničnímu vměšování, a zajistit vhodnou reakci; bere na vědomí, že delegace EU a velvyslanectví členských států mohou podporovat pořádání osvětových kampaní v hostitelských zemích; domnívá se, že posílení kapacit v oblasti strategické komunikace a veřejné diplomacie v rámci delegací EU – se zaměřením na podporu narativů založených na faktech, občanské angažovanosti a budování důvěry, zejména mezi mladými lidmi a pedagogy – má zásadní význam; je proto znepokojen zprávami o možném snížení počtu delegací EU a jejich zaměstnanců, zejména v souvislosti s rostoucími mezinárodními výzvami a geopolitickým napětím;
87. poukazuje na to, že delegace EU a mise a operace SBOP mohou v úzké koordinaci s diplomatickými misemi členských států EU účinněji sloužit jako první linie obrany proti hybridním útokům, včetně kybernetických operací a operací zahraniční manipulace s informacemi a vměšování; vyzývá k posílení informovanosti a strategické komunikace o přínosech, přítomnosti a úloze misí a operací v rámci společné bezpečnostní a obranné politiky (SBOP) po celém světě, zejména v bezprostředním sousedství EU a v kandidátských a potenciálních kandidátských zemích; vyzývá místopředsedkyni Komise, vysokou představitelku Unie pro zahraniční věci a bezpečnostní politiku a Radu, aby do misí SBOP začlenily týmy pro sledování zahraniční manipulace s informací a vměšování a reakci na ně, zajistily odbornou přípravu všech relevantních současných a budoucích misí a operací v oblasti zahraniční manipulace s informacemi a vměšování a posílily koordinaci civilních a vojenských operací s cílem bojovat proti hybridnímu vlivu;
88. zdůrazňuje význam společných cvičení, budování kapacit a technické pomoci partnerským zemím, které čelí soustavnému hybridnímu tlaku; vyzývá členské státy a ESVČ, aby do mandátů jednotlivých misí a operací začlenily činnost v oblasti budování kapacit a odbornou přípravu v oblasti hybridních hrozeb s cílem zvýšit připravenost partnerských zemí; vítá nasazení týmů EU pro hybridní rychlou reakci a týmů rychlé kybernetické reakce jako užitečných nástrojů při budování kapacit a odolnosti v zemích, na něž jsou zaměřeny kybernetické útoky a hybridní útoky a útoky zahraniční manipulace s informacemi a vměšování, jak dokládá nedávný příklad Moldavska; v této souvislosti bere na vědomí přítomnost agentury Frontex v několika příslušných třetích zemích a potenciální přidanou hodnotu jejích kapacit v tomto ohledu;

89. zdůrazňuje, že opakované pokusy o normalizaci vztahů s Ruskem, aniž byla zohledněna bytostná povaha ruského státu a jeho imperiální strategické cíle, přispěly ke zvýšené nestabilitě a k oslabení odrazujícího účinku a evropské a celosvětové bezpečnosti; zdůrazňuje, že budoucí politiky EU a členských států musí být založeny na realistickém posouzení této historické kontinuity a musí upřednostňovat odstrašování, odolnost a bezpečnost zemí v sousedství Ruska před krátkodobými hospodářskými nebo politickými hledisky; vítá úsilí, které bylo v posledních letech vynaloženo s cílem oddělit hospodářství EU od závislosti na ruských fosilních palivech; dále zdůrazňuje, že úplné a nezvratné ukončení této závislosti by mělo být pro EU a její členské státy strategickou prioritou;
90. vítá posílený závazek vyjádřený ve společném sdělení k rozvoji kapacit pro ofenzivní informační operace; konstatuje, že pro tento závazek, který vyžaduje dlouhodobé plánování, je třeba vyčlenit zdroje; zdůrazňuje, že mezi cíle by mělo patřit posílení proaktivních a intenzivnějších informačních opatření ze strany EU v jejím sousedství s cílem čelit destabilizačním snahám, jakož i dalším nepřátelským státům a státem podporovaným koordinovaným manipulacím s informacemi, operacím kognitivní války a nepřátelským kampaním zaměřeným na ovlivňování ze strany autoritářských či zlovolných aktérů; poukazuje na to, že mezi obyvatelstvem žijícím v autoritářských režimech, zejména v Rusku a Bělorusku, je třeba šířit věcné a důvěryhodné informace, s cílem odhalit destruktivní postupy vlády, které ohrožují svobodu a mír nejen v sousedních zemích, ale především v jejich vlastní zemi; vyzývá k maximálnímu možnému využití digitálního a kybernetického prostoru a jeho bezhraniční povahy k dosažení tohoto cíle;
91. s vážným znepokojením konstatuje, že v některých členských státech vládní opatření a strategická rozhodnutí opakovaně sloužila ruským zájmům; připomíná případ bývalé vlády strany Fidesz v Maďarsku jako obzvláště jasný příklad, který mimo jiné zahrnoval neschopnost řádně informovat a prošetřit pronikání ruských státních kybernetických aktérů, uzavírání dlouhodobých smluv s Ruskem o plynu za ceny vyšší než tržní, systematické bránění pomoci EU Ukrajině a sbližování s ruskými postoji v klíčových rozhodnutích EU v oblasti zahraniční a bezpečnostní politiky; vyzývá k řádnému podávání zpráv a vyšetřování činností a kampaní, které mohou souviset se zahraničním vlivem a vměšováním; vyzývá k větší ostražitosti, posílenému monitorování a plnému využívání unijních nástrojů k ochraně EU před vnitřními nástroji zahraničního vlivu a vměšováním;
92. konstatuje, že kandidátské země, potenciální kandidátské země a země sousedící s EU, zejména západní Balkán, Moldavsko, Ukrajina, Arménie a Gruzie jsou jasným terčem ruských operací zahraniční manipulace s informacemi a vměšováním, přičemž jedním

z cílů je zdiskreditovat EU a oslabit vnímaný přínos vstupu do ní; vyzývá Komisi a ESVČ, aby prohloubily spolupráci s příslušnými subjekty v těchto zemích v oblasti odolnosti informačních systémů, kybernetické bezpečnosti a hybridních hrozeb a aby přešly od podpory ad hoc k systematické a dlouhodobé pomoci zaměřené na budování institucionální, právní a občanské odolnosti; vyzývá k tomu, aby EU financovala regionální koordinační centra pro boj proti hrozbám pro integritu informací na internetu a zahraniční manipulaci s informacemi a vměšování v příslušných částech sousedství EU a aby byla posílena podpora investigativní žurnalistiky a regulačních orgánů pro sdělovací prostředky; zdůrazňuje, že je třeba se zvláště zaměřit na pomoc při zajištění integrity voleb v kandidátských nebo potenciálních kandidátských zemích, a to i v souvislosti se stažením finančních prostředků USAID, což má dopad zejména na západní Balkán;

93. zdůrazňuje, že podpora, kterou EU poskytuje kandidátským zemím při posilování odolnosti vůči zahraničnímu vměšování, by měla být doprovázena prokázaným prováděním příslušných reforem v těchto zemích a jejich hmatatelnými výsledky; vyzývá Komisi, aby i nadále uplatňovala přísný přístup při posuzování pokroku kandidátských zemí v rámci přístupových kapitol; zdůrazňuje, že nedostatky v řešení klíčových otázek, jako je korupce, chybějící nezávislé sdělovací prostředky, porušování lidských práv a nedostatky v demokratických procesech, podkopávají důvěru občanů ve vnitrostátní orgány a orgány EU, čímž vytvářejí euroskeptické narativy, které mohou být zneužity třetími zeměmi a subjekty zapojenými do zahraniční manipulace s informacemi a vměšování;
94. vyzývá Komisi, aby zřídila regionální centra EDMO, která by po vzoru stávajícího centra pro Moldavsko pokrývala příslušné kandidátské, potenciální kandidátské a sousední země EU;
95. vyzývá Komisi, aby z programů mediální gramotnosti učinila trvalou součást předvstupní pomoci a evropského nástroje sousedství; zdůrazňuje, že nedílnou součástí těchto nástrojů by měla být kulturní spolupráce, která posílí společenskou soudržnost, sdílené hodnoty a mezilidskou angažovanost v kandidátských a sousedních zemích; zdůrazňuje, že zrušení tematických programů a souvisejících finančních prostředků určených na lidská práva a demokracii a na organizace občanské společnosti, jak je stanoveno v návrhu Komise týkajícího se víceletého finančního rámce na období 2028–2034 a v návrhu nového programu „Globální Evropa“, vyvolává značnou nejistotu ohledně toho, jak budou tyto závazky vyplývající ze Smlouvy o EU účinně začleněny do všech oblastí politiky, uváděny do praxe a monitorovány; znovu vyzývá Komisi, aby posílila programy zaměřené na rozsáhlé zapojení a podporu občanské společnosti, obránců lidských práv, novinářů a investigativních sdělovacích prostředků ve třetích zemích; trvá na tom, aby nový VFR poskytoval

předvídatelné financování, které umožní rychlou reakci na hrozby proti základním svobodám a podpoří místní iniciativy;

96. naléhavě vyzývá k úsilí EU o podporu partnerských zemí v jejím východním a jižním sousedství, jakož i v prioritních zemích subsaharské Afriky, asijsko-tichomořského regionu a Latinské Ameriky při budování odolnosti vůči zahraniční manipulaci s informacemi a vměšování, posilování demokratických procesů a zajišťování integrity voleb, mimo jiné i prostřednictvím vyhrazeného financování v kontextu příštího VFR; zdůrazňuje zejména, že transformace probíhající v severní Africe a oblasti Sahelu mají přímý dopad na bezpečnost a demokratickou odolnost EU, a konstatuje, že tyto regiony jsou vůči zahraničním manipulacím s informacemi a vměšování obzvláště zranitelné, zejména v důsledku politické nestability a křehkých informačních ekosystémů; zdůrazňuje, že Rusko a Čína stále více spolupracují na posílení revizionistických narativů o údajném úpadku Západu a „neokolonialismu“ v těchto regionech, což odhaluje strategickou komunikační mezeru, která podkopává důvěryhodnost a vliv EU; zdůrazňuje zejména, že je třeba nadále rozvíjet cílená opatření zaměřená na odolnost vůči zahraniční manipulaci s informacemi a vměšování pro tyto regiony, včetně podpory nezávislých sdělovacích prostředků, občanské společnosti, digitální gramotnosti a gramotnosti v oblasti umělé inteligence, strategické komunikace v místních jazycích a posílených mechanismů monitorování a reakce, jako je stěžejní projekt EUvsDisinfo, kromě mechanismů finanční podpory;
97. uznává zřízení partnerské mise Evropské unie v Moldavsku jako úspěšný příklad toho, jak může EU hrát rozhodující úlohu při podpoře struktur partnerské země pro řešení krizí a posilování její odolnosti vůči kybernetickým hrozbám, hybridním hrozbám a hrozbám zahraniční manipulace s informacemi a vměšování; domnívá se, že partnerská mise Evropské unie v Moldavsku by měla sloužit jako vzor pro začlenění boje proti hybridním hrozbám do mandátu stávajících misí nebo pro zřízení podobných misí v jiných partnerských zemích; domnívá se, že takové dohody by měly být upřednostňovány se zeměmi, jejichž vnitřní nestabilita přímo ovlivňuje bezpečnost EU; bere na vědomí parlamentní volby, které se v Moldavsku konaly dne 28. září 2025, jakož i prezidentské volby konané dne 3. listopadu 2024 a výrazné vítězství proevropských sil, a to navzdory značnému úsilí a zdrojům, které Rusko vynaložilo na destabilizaci situace v Moldavsku a jeho odklon od evropské a euroatlantické cesty;
98. se znepokojením konstatuje, že Arménie čelila zintenzivnění hybridních hrozeb spojených s Ruskem, jejichž cílem bylo ovlivnit výsledek jejích voleb v červnu 2026 a oslabit její demokratické procesy, sociální soudržnost a úsilí o budování míru, včetně nepřátelských kybernetických činností, koordinované manipulace

s informacemi, zasahování do voleb, hospodářského nátlaku a zjevných a skrytých hrozeb ze strany vysokých ruských představitelů, jakož i aktivace vlivových sítí; připomíná, že arménská zahraniční zpravodajská služba informovala o využívání otevřených i skrytých informačních operací, zkreslujících narativů a snah o manipulaci veřejného diskurzu způsobem, který poškozuje národní zájmy Arménie, a zdůrazňuje, že na takovém hybridním nátlaku se mohou podílet jak státní, tak nestátní aktéři, včetně domácích zprostředkovatelů, jako jsou například někteří náboženští představitelé a oligarchické sítě napojené na širší ruské strategie ovlivňování v regionu; vítá zřízení mise EUPM Armenia, která má arménským orgánům poskytovat strategické poradenství a budovat kapacity v oblasti boje proti zahraniční manipulaci s informacemi a vměšování, kybernetickým útokům a nezákonným finančním tokům; vybízí misi EU v Arménii (EUMA), aby v rámci svého příspěvku k demokratické odolnosti posílila svou komunikaci s místními demokratickými aktéry, komunitními organizacemi a nezávislými sdělovacími prostředky; připomíná, že Arménie je stále členem Ruskem řízené Organizace Smlouvy o kolektivní bezpečnosti, a vyzývá Arménii, aby ji zcela opustila;

99. vyjadřuje hluboké politování nad rozhodnutím prezidenta USA ze dne 7. ledna 2026 odstoupit od významného počtu mezinárodních organizací, včetně řady orgánů OSN, pozastavit účast v nich nebo s nimi ukončit spolupráci; vyjadřuje vážné znepokojení nad tím, že takový krok ohrozí finanční udržitelnost systému OSN, oslabí mnohostrannou spolupráci v době, kdy je to nejvíce zapotřebí, a podpoří autoritářské a revizionistické aktéry, kteří se historicky snažili využít jakéhokoli odstoupení západních mocností od mezinárodních organizací nebo ukončení spolupráce s nimi; zdůrazňuje proto, že je třeba, aby EU posílila své vedoucí postavení při podpoře a posilování mnohostranných organizací a aby prosazovala demokratické instituce; vybízí vládu USA, aby zvážila své rozhodnutí a znovu potvrdila svůj závazek vůči OSN a mnohostranné spolupráci;
100. vyjadřuje svůj důrazný nesouhlas s nedávno zveřejněnou strategií národní bezpečnosti USA, zejména s negativním popisem EU, jejích výzev a rizik, jakož i s pojetím mezinárodních vztahů založeným na sférách vlivu; odsuzuje veškeré pokusy o ovlivňování nebo podkopávání demokratických procesů v EU; zdůrazňuje, že je důležité chránit integritu orgánů EU a rozhodovací proces Unie; vyjadřuje znepokojení nad tím, že některé prvky této strategie zjevně neřeší dostatečně hrozbu, kterou představuje Rusko, zejména pro evropskou, a tedy i americkou bezpečnost; dále vyjadřuje politování tím, že strategie obsahuje nesprávné hodnocení politického systému EU a že zaujímá bezdůvodně nepřátelský postoj vůči ní; domnívá se, že uvedená strategie dále posiluje nutnost, aby EU pokročila ve své strategické autonomii, snížila závislost a diverzifikovala partnerství;

101. zdůrazňuje, že v mezinárodní spolupráci s podobně smýšlejícími partnery, mimo jiné s G7, NATO, OSN, Organizací pro bezpečnost a spolupráci v Evropě a Radou Evropy, je důležité přednostně se zaměřit na zásady a cíle Evropského štítu pro demokracii; podporuje další rozvoj společných standardů s otevřeným zdrojovým kódem, průkopnických rámců pro bezpečnost umělé inteligence, datových modelů, metodik a taxonomií mezi partnery se stejným smýšlením, aby byla umožněna účinnější spolupráce; potvrzuje klíčovou úlohu NATO v boji proti hybridní válce namířené proti demokratickým institucím a připomíná v tomto ohledu jeho specializované nástroje a strategie, zejména uplatňované prostřednictvím jeho Střediska excelence pro strategickou komunikaci; zdůrazňuje skutečnost, že po přistoupení Finska a Švédska je 23 z 27 členských států EU rovněž spojenci NATO, a zdůrazňuje potřebu silné synergie mezi strategiemi EU a NATO; vítá kroky, které již byly přijaty ve dvoustranných a mnohostranných rámcích, včetně Kodexu chování OSN pro integritu informací na digitálních platformách, závazků přijatých v prohlášení Rady Evropy z Reykjavíku k ochraně volebních systémů před zahraničním vměšováním, pokračujícího úsilí mechanismu rychlé reakce skupiny G7 a vytvoření partnerství v oblasti bezpečnosti a obrany, zejména těch, která se zaměřují na boj proti kybernetickým útokům, hybridním hrozbám a zahraniční manipulaci s informacemi a vměšováním a na ochranu kritické infrastruktury; v této souvislosti znovu upřímně oceňuje pokračující angažovanost Spojeného království v oblasti evropské bezpečnosti;

Volební systémy a odolnost voličů

102. zdůrazňuje, že hlavním cílem Evropského štítu pro demokracii by mělo být chránit integritu voleb na místní, regionální a celostátní úrovni a na úrovni EU a v kandidátských zemích; vyzývá Komisi a členské státy, aby při plném dodržování zásady subsidiarity a v rozsahu stanoveném ve Smlouvách spolupracovaly na provádění reforem zaměřených na posílení odolnosti volebních procesů v Evropě se zvláštním zaměřením na opatření, která mají zabránit zahraničnímu vměšováním; konstatuje, že útoky na integritu voleb jsou mnohostranné, komplexní a dlouhodobé a jsou součástí ekosystému hrozeb, které je třeba řešit celospolečenským přístupem; navrhuje, aby iniciativa Evropský štít pro demokracii podporovala koordinaci úsilí online i off-line o zachování integrity evropských voleb, včetně úsilí o řešení hybridních hrozeb, kybernetických hrozeb, financování vměšováním a manipulací s informacemi;

103. vyzývá členské státy, aby zvýšily úsilí o provádění doporučení Komise týkajících se inkluzivních, spolehlivých a odolných volebních procesů v EU; zdůrazňuje zejména, že je důležité zřídit vnitrostátní volební síť, které by vnitrostátním orgánům a odborným subjektům pomáhaly pracovat v součinnosti; vyzývá Komisi a členské státy, aby usilovaly o systematický rozvoj a rozšiřování zátěžových testů zaměřených na volby jak na vnitrostátní, tak na přeshraniční úrovni,

a to s využitím praktických zkušeností a poznatků získaných z předchozích volebních cyklů, s cílem lépe předvídat, simulovat a zmírňovat rizika spojená s manipulací s informacemi, kybernetickým vměšováním a zesilováním vlivu prostřednictvím platform;

104. vyzývá členské státy, aby zajistily, aby volební orgány nebo rovnocenné orgány odpovědné za funkční, svobodné a spravedlivé volby byly dostatečně financovány a vybaveny vhodnými nástroji, které jim umožní plnit jejich funkce, ať už jde o poskytování odborné přípravy personálu a nezbytných digitálních nástrojů, nebo o zajištění dostatečných investic do volebních orgánů a volební infrastruktury;
105. domnívá se, že nenávistné kampaně, zastrašování a násilí, které kandidátům ztěžují účast ve veřejné debatě nebo interakci s voliči, představují hrozbu pro demokracii. zdůrazňuje, že tyto hrozby mohou být podněcovány pokusy zemí mimo EU destabilizovat EU, a to i prostřednictvím dezinformačních taktik, jako jsou deepfakes, které nepravdivě zobrazují skutečné politické kandidáty a jsou záměrně navrženy tak, aby uváděly voliče v omyl; vítá v tomto ohledu závazek Komise předložit doporučení týkající se bezpečnosti v politice; vyzývá členské státy, aby zvýšily své úsilí o ochranu kandidátů ve volbách a zvolených zástupců;
106. zdůrazňuje, že bezpečnost a ochrana žen v politickém životě jsou nezbytnými předpoklady pro rovné zastoupení a odolnou demokracii; odsuzuje dezinformační kampaně, a to i prostřednictvím deepfakes a sexuálního obsahu bez souhlasu, které jsou využívány k obtěžování, vyhrožování a zastrašování kandidátek a často se spoléhají na narativy zpochybňující jejich kompetentnost, důvěryhodnost a morální integritu, čímž odrážejí ženy od politické účasti a podkopávají důvěru v demokratické instituce; vítá cílený zákaz „svlékacích“ aplikací stanovený v aktu o umělé inteligenci a připomíná, že akt o digitálních službách označuje genderově podmíněné násilí a ochranu nezletilých osob za systémové riziko; vyzývá Komisi, aby do nadcházejících doporučení týkajících se bezpečnosti v politice zahrnula zvláštní ustanovení týkající se monitorování a prevence dezinformačních kampaní zaměřených konkrétně na kandidátky a boje proti těmto kampaním;
107. odsuzuje podvodnou reklamu, která napodobuje a zneužívá identitu politiků, politických kandidátů a dalších veřejných činitelů; varuje, že ačkoli hlavním cílem těchto podvodů je často finanční zisk, neoprávněné použití obrazu a podoby veřejně známé osobnosti s cílem falešně navodit dojem autentičnosti či podpory může způsobit poškození dobré pověsti, přispívat k rozostření hranice mezi autentickými informacemi a smyšleným obsahem a dále podkopávat důvěru veřejnosti v demokratické procesy a politické aktéry; vyzývá Komisi a členské státy, aby prověřily, zda online platformy dodržují

předpisy, pokud jde o jejich postupy při odstraňování nelegálních reklam;

108. zdůrazňuje klíčovou úlohu Evropské sítě pro volební spolupráci (ECNE) při podpoře výměny osvědčených postupů v oblasti volební odolnosti v celé EU a jejích členských státech, přičemž bere na vědomí stávající omezení ECNE a vítá závazek Komise k jejímu posílení; vyzývá k ambiciózní reformě ECNE, včetně přezkumu jejích zdrojů a personálního obsazení, dalšího rozvoje společného mechanismu volební odolnosti a většího zapojení kandidátských zemí; vyzývá Komisi, aby v rámci ECNE zřídila stálou monitorovací skupinu odpovědnou za dohled nad prováděním doporučení Komise týkajících se inkluzivních a odolných volebních procesů v EU a nadcházejících doporučení týkajících se bezpečnosti politických aktérů; domnívá se, že tato monitorovací skupina by měla být rovněž pověřena vypracováním návrhů na budoucí aktualizace těchto doporučení; dále vyzývá k tomu, aby Parlament a Úřad pro evropské politické strany a evropské politické nadace (APPF) byly zapojeny jako stálí partneři do všech schůzí ECNE;
109. zdůrazňuje, že volební infrastruktura je základním prvkem demokratické odolnosti EU a musí být účinně chráněna před rostoucími fyzickými a kybernetickými hrozbami; vítá záměr Komise posílit ochranu infrastruktury související s volbami prostřednictvím stávajících právních předpisů a nástrojů; vyzývá Komisi, aby toto úsilí doplnila cílenou revizí směrnice o odolnosti kritických subjektů s cílem zahrnout volební infrastrukturu do seznamu základních služeb veřejné správy uvedeného v této směrnici; žádá Komisi, aby zajistila, že toto začlenění bude následně zohledněno ve směrnici NIS 2 a v pokynech agentury ENISA;
110. vyzývá Komisi a členské státy, aby se zabývaly problémem vměšování zahraničních aktérů do stranické politické scény v Evropě; se znepokojením bere na vědomí různé příklady financování extremistických hnutí v EU zeměmi mimo EU; domnívá se, že důležitým nástrojem k objasnění tohoto problému je finanční transparentnost, a v této souvislosti vyzývá k rozsáhlejší výměně názorů mezi soukromými a veřejnými subjekty; je znepokojen přetrvávajícími nedostatky ve fungování registrů skutečných majitelů v členských státech, včetně kvality údajů nebo rizika příliš omezeného přístupu pro osoby s oprávněným zájmem, jako jsou novináři nebo organizace občanské společnosti; naléhavě vyzývá členské státy, aby plně a důsledně provedly směrnici o boji proti

praní peněz⁶⁹, která harmonizuje pravidla pro přístup k registrům skutečných majitelů; dále zdůrazňuje, že politická reklama a politická komunikace v online prostředí musí být plně transparentní, pokud jde o totožnost zadavatele a zdroj financování, v souladu s pravidly EU pro transparentnost; vyzývá k důslednému prosazování stávajících opatření, která mají zabránit využívání zástupného financování v politice; zdůrazňuje význam účinného monitorování a spolupráce mezi orgány v celé EU s cílem zajistit dodržování povinností týkajících se transparentnosti; v tomto smyslu vyzývá Komisi a členské státy, aby prozkoumaly možnosti zlepšení spolupráce mezi orgány pro boj proti korupci a nezávislými volebními komisemi v členských státech;

111. se znepokojením bere na vědomí rostoucí důkazy o zahraničním vměšování a špionáži namířené proti politickým institucím a procesům na úrovni EU i členských států; vítá vyšetřování v několika členských státech, která vedla k odsouzením, a probíhající případy týkající se úplatkářství, špionáže a aktivit zahraničních vlivových skupin; zdůrazňuje vážná rizika, která představují nedostatečná bezpečnostní opatření při náboru zaměstnanců a společníků s úzkými vazbami na autoritářské režimy; zdůrazňuje, že ochrana integrity a fungování orgánů EU vyžaduje důrazná opatření proti špionáži a infiltraci; dále zdůrazňuje nutnost prošetřit závažná a stále se rozvíjející obvinění, že maďarští úředníci působící v rámci předchozí maďarské vlády vedené stranou Fidesz prováděli špionážní činnosti zaměřené na orgány EU, včetně zpráv o tom, že citlivé informace z jednání EU byly sdíleny s ruskými protějšky, což vyvolává obavy ohledně porušení důvěrnosti, úniku zpravodajských informací a integrity rozhodovacích procesů EU;
112. vítá nedávno přijaté revidované znění nařízení o statutu a financování evropských politických stran a evropských politických nadací; bere na vědomí ustanovení týkající se financování a účasti stran ze zemí mimo EU, zejména pokud jde o skutečnost, že strany ze zemí mimo EU by neměly mít žádné právo veta ani kontrolu nad evropskými stranami; vyzývá spolunormotvůrce k zajištění plného a účinného provedení nařízení;
113. opětovně vyzývá Komisi, aby posílila výroční zprávu o právním státu a posílila demokracie proti zahraničnímu vměšování, mimo jiné tím, že se zaměří na svobodné a spravedlivé volby, pevné právní záruky,

⁶⁹ Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice 2006/70/ES (Úř. věst. L 141, 05.06.2015, s. 73, ELI: <https://eur-lex.europa.eu/eli/dir/2015/849/oj>).

system brzd a protivah a fungování demokratických institucí, s cílem poskytnout ucelenější obraz o standardech právního státu v celé EU;

114. konstatuje, že rychlý rozvoj kryptoměn, včetně platform nebo poskytovatelů služeb působících mimo Unii, vytváří potenciální zranitelnost, pokud jde o nedostatek transparentnosti a schopnosti kontrolovat financování politických stran a hnutí v Evropě; zdůrazňuje, že vzhledem ke své pseudonymní povaze a globálnímu dosahu a možnosti využívat anonymizační techniky a služby představují kryptoměny výzvu, pokud jde o zjištění skutečného zdroje politických darů a zmírnění zahraničního vlivu na demokratické procesy; zdůrazňuje, že politické dary zahrnující kryptoměny by měly podléhat zásadě „poznej svého dárce“ a splňovat stejné standardy transparentnosti a odpovědnosti jako tradiční finanční příspěvky; oceňuje závazek Komise spojit národní odborníky pod záštitou ECNE a v úzké spolupráci s dalšími sítěmi EU a zúčastněnými stranami v oblasti výměny osvědčených postupů, přípravy možných pokynů a podpory společných opatření; vyzývá Komisi v tomto ohledu, aby nadále sledovala provádění balíčku opatření proti praní peněz a nařízení o trzích kryptoaktiv (MiCA) pro zajištění účinného a soudržného prosazování a aby se zabývala veškerými možnými mezerami v právních předpisech, které bude případně nutné odstranit; v této souvislosti konstatuje, že balíček opatření pro integraci trhu a dohled zahrnuje navrhovanou revizi nařízení MiCA;
115. vyzývá členské státy, aby si vyměňovaly osvědčené postupy v oblasti dohledu nad financováním politických stran; vyjadřuje znepokojení nad tím, že některé finanční zpravodajské jednotky nemají potřebný mandát k tomu, aby příslušným vnitrostátním a evropským orgánům předkládaly informace týkající se zasahování do voleb; vyzývá Komisi, aby posoudila přidanou hodnotu rozšíření úlohy, mandátu a zdrojů úřadu APPF s cílem dále posílit koordinaci vnitrostátních orgánů a orgánů EU odpovědných za dohled nad financováním politických stran; v této souvislosti zdůrazňuje, že je třeba posílit spolupráci mezi APPF a ECNE;

Úloha sankcí při ochraně demokracie

116. považuje sankce vůči jednotlivcům a státním i nestátním subjektům, které se podílejí na činnostech zaměřených na podkopání demokratické integrity EU nebo jejích členských států, za zásadní součást nástrojů Evropského štítu pro demokracii; dále zdůrazňuje, že je třeba přijmout účinné sankce založené na objektivních a jednotných kritériích, které musí zahrnovat komplexní soubor opatření, včetně zmrazení a konfiskace majetku, jasného přiřazení odpovědnosti a veřejného odhalení, zvýšení nákladů a snížení příjmů, zákazů dovozu a vývozu, zákazů cestování, odepření přístupu na trhy EU a do finančních systémů EU a dalších účinných, důrazných a razantních omezujících opatření; opětovně vyzývá Radu, aby postupně přešla na hlasování kvalifikovanou většinou při přijímání

rozhodnutí v oblastech společné zahraniční a bezpečnostní politiky, jako jsou sankce;

117. vyzývá k posílení účinnosti a dopadu sankcí EU přijatých v návaznosti na ruskou invazi na Ukrajinu, aby byla definitivně oslabena schopnost Ruska pokračovat ve vedení své brutální agresivní války a ohrožovat bezpečnost dalších sousedních zemí; vyzývá Komisi a členské státy, aby pravidelně a pečlivě posuzovaly uložené sankce z hlediska optimální účinnosti a možného dalšího rozšíření, včetně sankcí zaměřených na jednotlivce a subjekty, kteří se podílejí na aktivním obcházení sankcí EU vůči Rusku; domnívá se, že by EU měla dále rozšířit svůj sankční režim, zejména v oblasti hybridních hrozeb a destabilizujících aktivit Ruska, a to zaměřením se na finanční a technické struktury, které podporují dezinformace, kybernetické útoky a vměšování do voleb, jako jsou operace s kryptoměnami, reklamní sítě a poskytovatelé hostingu, a zároveň by měla narušit ruské zástupné sítě v zemích mimo EU, zejména v Africe, na Blízkém východě a v Latinské Americe, a uvalit sankce na média, logistická centra a skupiny spojené s wagnerovci, které šíří protiujiční narativy; domnívá se, že za účelem dalšího zvýšení nákladů na hybridní agresi by EU měla rozšířit sankce zaměřené na osoby a subjekty ze zemí mimo EU (zejména čínské) jež jsou odpovědné za aktivní obcházení sankcí a usnadňují ruské operace, a že by měla ruským kybernetickým žoldnéřům zakázat využívání služeb se sídlem v EU, jako jsou hostingové, doménové a cloudové služby, a veřejně odhalovat politiky EU nebo lobbisty tajně financované Moskvou a uvalovat na ně sankce;
118. domnívá se, že důležitým krokem k uznání problému jasně systematického, mnohostranného a často státem sponzorovaného vměšování, které v Evropě provádějí země, jako je Rusko nebo Írán, by mohla být identifikace a pojmenovávání zemí původu, kromě připsání odpovědnosti jednotlivcům nebo společnostem; vítá rozhodnutí Komise zařadit Rusko na seznam vysoce rizikových třetích zemí v rámci EU pro boj proti praní peněz a financování terorismu s cílem udržet integritu finančního systému EU; vyzývá Komisi, aby posoudila, zda by bylo vhodné zařadit Bělorusko na další seznam vzhledem k jeho rizikovému profilu a vazbám na ruské politické a hospodářské struktury; připomíná, že nové nařízení o boji proti praní peněz poskytne rozšířené možnosti pro identifikaci vysoce rizikových třetích zemí a jejich zařazení na seznam; vyzývá Komisi, aby s pomocí Orgánu pro boj proti praní peněz plně využila svých pravomocí, pokud jde o zajištění uplatňování cílených finančních sankcí;
119. zdůrazňuje, že účinnost a důvěryhodnost sankcí EU závisí na jejich přísném a důsledném prosazování; vyzývá proto členské státy, aby vytvořily mechanismus pro účinné monitorování činností v oblasti prosazování práva, a to i prostřednictvím spolupráce s občanskou společností a akademickou obcí, s cílem zlepšit koordinaci

a spolupracovat na odstranění mezer a harmonizaci postupů; vítá, že ohlášená revize mandátu Úřadu evropského veřejného žalobce (EPPO) nabízí příležitost k posílení jeho úlohy tak, aby zahrnovala vyšetřování a stíhání porušení sankcí; zdůrazňuje, že tato reforma by měla být doprovázena odpovídajícím financováním, aby Úřad evropského veřejného žalobce mohl účinně plnit posílené povinnosti;

120. připomíná, že protinátlačový nástroj EU, který je v platnosti od roku 2023, stanoví širokou škálu opatření EU pro boj proti pokusům třetích zemí o hospodářský nátlak na EU nebo některý členský stát; zdůrazňuje, že protinátlačový nástroj by měl být součástí proaktivní strategie eskalace s cílem reagovat na hrozby zaměřené na evropskou územní celistvost a digitální, regulační, finanční nebo hospodářskou suverenitu; připomíná, že přístup hospodářských subjektů ze zemí mimo EU na vnitřní trh je podmíněn dodržováním práva EU;
121. odsuzuje politicky motivované využívání černých listin, vízových zákazů a dalších omezujících či odvetných opatření ze strany zahraničních vlád, zejména Ruska, namířených proti občanům EU, zástupcům státních orgánů a obchodních organizací, novinářům, aktérům občanské společnosti, humanitárním organizacím a politickým představitelům, včetně demokraticky zvolených poslanců Evropského parlamentu; je znepokojen tím, že tyto praktiky, jejichž cílem je vyvíjet nepřiměřený politický tlak na regulační autonomii EU a rámec základních práv, podkopávají diplomatické normy a zásadu vzájemného respektu mezi jurisdikcemi; požaduje koordinovanější a rozhodnější reakci EU na tato svévolná opatření spolu se stálým diplomatickým úsilím, s cílem zajistit ochranu a bezpečnost osob na černé listině a nabídnout jim solidaritu a nezbytnou pomoc; vyjadřuje plnou podporu všem dotčeným osobám; zdůrazňuje, že je třeba vytvořit systém pro průběžné posuzování a informování cílových osob, zejména v souvislosti s ruskou černou listinou, včetně poslanců EP a jejich zaměstnanců a úředníků EU, s cílem zajistit transparentnost a ochranu;

Připravenost EU

122. vítá Strategii EU pro unii připravenosti a zdůrazňuje, že cíle stanovené v této strategii jsou úzce propojeny s cíli Evropského štítu pro demokracii; dále zdůrazňuje, že demokratická odolnost vyžaduje, aby společnosti byly schopny fungovat za výjimečných nebo rušivých podmínek, a že reformy zaměřené na posílení připravenosti by proto měly tvořit nedílnou součást Evropského štítu pro demokracii; vítá iniciativy členských států, jako jsou iniciativy ve Švédsku a Finsku, jejichž cílem je posílit společenskou připravenost, spolupráci a jasnou komunikaci o povinnostech občanů; zdůrazňuje, že účinná politika připravenosti musí být založena na začleňování ve všech věkových skupinách, komunitách a sociálních a hospodářských skupinách;

v této souvislosti zdůrazňuje úlohu společností, sdružení a kvalifikovaných osob při podpoře základních služeb a péče; zdůrazňuje, že účinná civilní odolnost vyžaduje, aby byli občané zapojeni a vzděláni o tom, jak a kdy přispět;

123. vyzývá k vypracování výroční veřejně přístupné zprávy o činnosti EU týkající se celkového stavu připravenosti v celé EU s komplexním strukturovaným přehledem pro každý členský stát; zdůrazňuje, že tato zpráva by mohla mimo jiné stanovit institucionální připravenost, stav civilně-vojenské spolupráce, strategické schopnosti, preventivní opatření, mechanismy reakce, zranitelná místa a klíčové trendy a zároveň respektovat aspekty národní bezpečnosti; zdůrazňuje, že zpráva by mohla přispět k výměně osvědčených postupů a sloužit jako vodítko a poradenský nástroj pro provádění strategií připravenosti členských států; konstatuje, že by se mělo zvážit, zda by při přípravě této zprávy mohlo hrát koordinační úlohu Evropské středisko pro odolnost demokracie;
124. požaduje urychlený vývoj a zavedení celounijní interoperabilní aplikace pro varování před krizí, která by rezidentům během mimořádných událostí poskytovala spolehlivé a vícejazyčné informace v reálném čase; doporučuje, aby byla tato aplikace začleněna do vnitrostátních a unijních systémů včasného varování a byla přístupná všem osobám, přičemž by měl být kladen zvláštní důraz na její dostupnost pro zranitelné skupiny, a aby byla pravidelně aktualizována s ohledem na technologický pokrok a v souladu s osvědčenými postupy v oblasti krizového řízení;
125. vítá iniciativy v několika členských státech týkající se distribuce brožury o připravenosti domácností, která nabízí jasné a praktické pokyny přizpůsobené rozmanité sociální a zeměpisné realitě Evropy s cílem pomoci občanům připravit se na mimořádné události; vyzývá Komisi, aby vypracovala brožuru na úrovni EU, která by odrážela přeshraniční a nadnárodní kontext a zahrnovala by doporučené nouzové zásoby, pokyny pro praktickou soběstačnost na dobu nejméně 72 hodin, základní rady ohledně první pomoci a zvláštní pokyny pro zranitelné skupiny, včetně starších osob, osob se zdravotním postižením a rodin s dětmi;
126. vyzývá k pořádání pravidelných rozsáhlých cvičení připravenosti koordinovaných na úrovni EU, do nichž by byly zapojeny orgány a agentury EU, členské státy, regionální a místní orgány, soukromý sektor a občanská společnost; domnívá se, že příprava na různé scénáře, sahající od povodní, lesních požárů, zemětřesení a mimořádných zdravotních událostí až po chemické, biologické, radiologické a jaderné incidenty, může rovněž přispět k posílení schopnosti Evropy, pokud jde o předcházení hrozbám, jako jsou ty, jež se projevily při ruské útočné válce proti Ukrajině a hybridních útocích proti Evropě jako celku, odolávat jim a reagovat na ně; doporučuje, aby tato cvičení simulovala složité a realistické scénáře,

včetně kybernetických útoků, narušení kritické infrastruktury, koordinovaných dezinformačních kampaní a hybridních krizí, s cílem posoudit schopnosti reakce, zlepšit interoperabilitu mezi úrovněmi správy, sdílet osvědčené postupy a podpořit kulturu připravenosti na všech úrovních; v této souvislosti zdůrazňuje, že iniciativy EU v oblasti vojenské mobility jsou rovněž velmi důležité, pokud jde o civilní připravenost a schopnost přepravovat dodávky humanitární pomoci v mimořádných situacích; dále vyzývá k zavedení Evropského dne připravenosti; domnívá se, že jeho datem by měl být 24. únor, což je datum nevyprovokované plošné vojenské invaze Ruska na Ukrajinu v roce 2022, jako symbol solidarity EU s Ukrajinou a důrazná připomínka nutnosti posílit civilní a obrannou připravenost na rostoucí hrozby ze strany autoritářských režimů;

127. vyzývá Komisi, aby zvážila možnost rozšíření programu Erasmus+ nebo podobných programů o přeshraniční iniciativy zaměřené na školení v oblasti připravenosti pro pracovníky v kritických odvětvích, jako jsou hasiči, zdravotničtí pracovníci, dobrovolníci civilní ochrany, státní úředníci a zástupci organizací občanské společnosti a široká veřejnost; doporučuje, aby tyto programy podporovaly přeshraniční a meziodvětvovou výměnu znalostí, společná cvičení a školení v oblasti hybridních hrozeb a mimořádných událostí a posilovaly místní kapacity připravenosti ve všech členských státech se zvláštním zaměřením na zranitelné regiony;
128. požaduje urychlené zavedení bezpečných komunikačních systémů, jako je IRIS² a evropský kritický komunikační systém, s tím, že se bude vycházet z již existujících systémů na úrovni členských států; zdůrazňuje, že tyto iniciativy zajišťují odolnost telekomunikací, kontinuitu základních služeb během krizí, snižují vnější závislosti ve strategických odvětvích a posilují kybernetickou bezpečnost této infrastruktury prostřednictvím harmonizovaného povolování spektra, certifikace kybernetické bezpečnosti a opatření v oblasti bezpečnosti dodavatelského řetězce IKT v souladu s návrhy Komise DNA a CSA;
129. požaduje větší koordinaci mezi orgány, institucemi a jinými subjekty EU, členskými státy a podobně smýšlejícími mezinárodními partnery prostřednictvím sdílených platforem pro získávání poznatků o situaci, společných metodik a mechanismů pro rychlou a bezpečnou výměnu informací; zdůrazňuje, že tyto nástroje umožňují soudržnou, pružnou a koordinovanou reakci na hybridní hrozby, zlepšují předvídaní rizik a posilují kolektivní připravenost a odolnost EU; v této souvislosti zdůrazňuje, že připravenost a odolnost jsou záležitostmi kolektivní odpovědnosti, jež vyžadují zapojení společnosti;
130. zdůrazňuje potřebu začlenit připravenost do VFR na období 2028–2034 s cílem vybudovat důvěryhodnou odolnost a dosáhnout dostatečné úrovně civilní a obranné připravenosti; naléhavě vyzývá Komisi, aby vytvořila cílené finanční nástroje kombinující příslušné nástroje v oblasti obrany a civilní bezpečnosti, jako je nástroj

na obranu Evropy a nástroj pro zabezpečení Evropy, s cílem zajistit dostatečné a stabilní financování projektů budování odolnosti, technologických inovací a schopností dvojího užití, iniciativ v oblasti civilní připravenosti, ochrany kritické infrastruktury a úsilí o posílení průmyslové a technologické suverenity EU; konstatuje, že vyhrazené finanční zdroje by měly upřednostňovat také místní úsilí o připravenost, zejména na územích, která jsou nejvíce vystavena zranitelným místům a hybridním hrozbám, zejména informační válce;

131. doporučuje, aby rozhodovací orgány EU přezkoumaly a optimalizovaly strategie a pohotovostní plány, jež by použily v případě otevřeného vojenského konfliktu proti jednomu nebo více členským státům a podobných krizových scénářů, včetně případů aktivace čl. 42 odst. 7 SEU; dále zdůrazňuje, že ve všech orgánech, institucích a jiných subjektech EU je třeba zajistit nejvyšší úroveň bezpečnosti a zabezpečení, a to i v oblasti kybernetické bezpečnosti a bezpečnosti a integrity informací, a vytvořit v tomto ohledu nezbytné podmínky, včetně zajištění akreditovaných bezpečných komunikačních kanálů a odpovídajících zasedacích místností pro neveřejné schůze; zdůrazňuje, že je třeba přísně prosazovat pravidla týkající se narušení bezpečnosti a důvěrnosti informací, zejména v souvislosti se zvýšeným rizikem špionáže a sabotáže, a to i prostřednictvím účinného vyšetřování a stíhání těchto případů; vyzývá v této souvislosti k pravidelným auditům zranitelných míst a závislostí, zejména v digitálním prostoru, ve všech orgánech, institucích a jiných subjektech EU; zdůrazňuje, že i bez otevřeného vojenského konfliktu představují hybridní hrozby stále větší riziko pro každodenní fungování EU;
132. vítá úsilí Komise o posílení fyzické a informační bezpečnosti v orgánech EU, jak je uvedeno ve sdělení řídící rady z října 2025, včetně plánů na zabezpečené zasedací místnosti, posílených postupů pro bezpečnostní prověrky zaměstnanců, kteří nakládají s utajovanými informacemi, a zřízení Bezpečnostní akademie s cílem zajistit pravidelné aktuální informace o vývoji hrozeb; konstatuje, že tato opatření reagují na zvýšená rizika špionáže, zahraničního vměšování a hybridních hrozeb namířených proti rozhodovacím procesům EU; zdůrazňuje však, že zlepšení fyzické bezpečnosti musí být doplněno spolehlivými protokoly kybernetické bezpečnosti a schopnostmi kontrašpionáže, aby bylo možné řešit celé spektrum rizik infiltrace; požaduje urychlené přijetí návrhu nařízení o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie, který předložila Komise⁷⁰; připomíná, že nařízení o kybernetické bezpečnosti pro orgány, instituce a jiné subjekty EU doporučuje rozpočet na kybernetickou bezpečnost ve výši 10 % celkového rozpočtu na informační a komunikační technologie pro

⁷⁰ Návrh nařízení Evropského parlamentu a Rady o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie, který dne 23. března 2022 předložila Komise (COM(2022)0119).

subjekty EU; vítá činnost Služby kybernetické bezpečnosti pro orgány, instituce a jiné subjekty Unie (CERT-EU) a trvá na tom, že je třeba zajistit, aby tato služba měla dostatečný rozpočet a řádné personální obsazení;

133. doporučuje další opatření k posílení bezpečnosti Parlamentu, jeho odolnosti vůči zahraničnímu vměšování a schopnosti účinně fungovat v krizích, včetně posílené podpory poslanců a zaměstnanců prostřednictvím kontrol IT a bezpečnostních kontrol, cílené odborné přípravy, brífinků před pracovními cestami a interdisciplinárních činností zaměřených na budování odolnosti, které zahrnují fyzickou bezpečnost, bezpečnost informací a kybernetickou bezpečnost; zdůrazňuje, že v souladu s nařízením o kybernetické bezpečnosti je třeba dále posílit jeho rámec kybernetické bezpečnosti, zlepšit provozní vyspělost a posílit schopnosti odhalování hrozeb v měnícím se technologickém prostředí a prostředí hrozeb a zároveň zajistit cílenější odbornou přípravu zaměstnanců pro boj proti manipulaci s informacemi a uplatňovat pro citlivé schůze a cesty přísnější bezpečnostní prověrky; konstatuje, že používání soukromých mobilních zařízení a notebooků pro parlamentní práci představuje potenciální zranitelnost, a zdůrazňuje, že poslanci a zaměstnanci by měli být vybaveni zabezpečenými zařízeními od EP; vítá stávající dobrovolné prověřování na špionážní software a vyzývá k jeho systematickému rozšíření na všechna zařízení používaná pro parlamentní činnost; dále vyzývá Komisi a ESVČ, aby systematicky zapojovaly Parlament do svých činností a cvičení v oblasti připravenosti, jako je cvičení „EU Integrated Resolve“;

◦

◦ ◦

134. pověřuje svou předsedkyni, aby předala toto usnesení Radě, Komisi, místopředsedkyni Komise, vysoké představitele Unie pro zahraniční věci a bezpečnostní politiku a vládám a parlamentům členských států.