Evropský parlament
2024-2029

Zvláštní výbor pro Evropský štít pro demokracii

2025/2069(INI)

18.12.2025

NÁVRH ZPRÁVY

o zjištěních a doporučeních zvláštního výboru pro Evropský štít pro demokracii (2025/2069(INI))

Zvláštní výbor pro Evropský štít pro demokracii

Zpravodaj: Tomas Tobé

OBSAH

Strana

NÁVRH USNESENÍ EVROPSKÉHO PARLAMENTU 3

VYSVĚTLUJÍCÍ PROHLÁŠENÍ.....39

PŘÍLOHA: ZVEŘEJŇOVÁNÍ PODNĚTŮ 41

NÁVRH USNESENÍ EVROPSKÉHO PARLAMENTU

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 období[1],

– 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 10 o demokratickém životě a článek 21 o vnější činnosti,

– s ohledem na Smlouvu o fungování Evropské unie, a zejména na čl. 114 o mezinárodním trhu a článek 222 o solidaritě,

– s ohledem na Listinu základních práv Evropské unie,

– 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 nadací[2],

– 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 terorismu[4],

– 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],

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

– 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],

– s ohledem na nařízení Evropského parlamentu a Rady (EU) 2024/900 ze dne 13. března 2024 o transparentnosti a cílení politické reklamy[7],

– 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 Unie[8].

– 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) 2019/1937[9] (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/ES[10],

– 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) 2021/692 ze dne 28. dubna 2021, kterým se zavádí program Občané, rovnost, práva a hodnoty a zrušují nařízení Evropského parlamentu a Rady (EU) č. 1381/2013 a nařízení Rady (EU) č. 390/2014[14],

– s ohledem na směrnici Evropského parlamentu a Rady (EU) 2019/1937 ze dne 23. října 2019 o ochraně osob, které oznamují porušení práva Unie[15],

– 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

---

[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.
[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 156, 5.5.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/692/oj.
[15] Úř. věst. L 305, 26.11.2019, s. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj.

upravujících poskytování audiovizuálních mediálních služeb (směrnice o audiovizuálních mediálních službách)[16],

– 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 Ukrajiny[17] 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 Ukrajiny[18],

– 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 Ukrajině[19] 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 Ukrajině[20].

– s ohledem na rozhodnutí Rady 2014/512/SZBP ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině[21] a nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014 o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině[22],

– 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 území[23] 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 území[24],

– s ohledem na rozhodnutí Rady 2012/642/SZBP ze dne 15. října 2012 o omezujících opatřeních vůči Bělorusku[25] a na nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních vůči prezidentu Lukašenkovi a některým představitelům Běloruska[26],

– s ohledem na rozhodnutí Rady (SZBP) 2023/1532 ze dne 20. července 2023 o omezujících opatřeních vzhledem k vojenské podpoře útočné války Ruska proti Ukrajině ze strany Íránu[27] a nařízení Rady (EU) 2023/1529 ze dne 20. července 2023 o

[16] Úř. věst. L 95, 15.4.2010, s. 1, ELI: http://data.europa.eu/eli/dir/2010/13/oj.
[17] Úř. věst. L 78, 17.3.2014, s. 16, ELI: http://data.europa.eu/eli/dec/2014/145(1)/oj.
[18] Úř. věst. L 78, 17.3.2014, s. 6, ELI: http://data.europa.eu/eli/reg/2014/269/oj.
[19] Úř. věst. L 66, 6.3.2014, s. 26, ELI: http://data.europa.eu/eli/dec/2014/119(1)/oj.
[20] Úř. věst. L 66, 6.3.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/208/oj.
[21] Úř. věst. L 229, 31.7.2014, s. 13, ELI: http://data.europa.eu/eli/dec/2014/512/oj.
[22] Úř. věst. L 229, 31.7.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/833/oj.
[23] Úř. věst. L 42 I, 23.2.2022, s. 109, ELI: http://data.europa.eu/eli/dec/2022/266/oj.
[24] Úř. věst. L 42 I, 23.2.2022, s. 77, ELI: http://data.europa.eu/eli/reg/2022/263/oj.
[25] Úř. věst. L 285, 17.10.2012, s. 1, ELI: http://data.europa.eu/eli/dec/2012/642/oj.
[26] Úř. věst. L 134, 20.5.2006, s. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj.
[27] Úř. věst. L 186, 25.7.2023, s. 20, ELI: http://data.europa.eu/eli/dec/2023/1532/oj.

omezujících opatřeních vzhledem k vojenské podpoře útočné války Ruska proti Ukrajině ze strany Íránu[28],

– 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 republice[29], a na prováděcí nařízení Rady (EU) 2024/1602 ze dne 31. května 2024, kterým se provádí nařízení (EU) 2017/1509 o omezujících opatřeních vůči Korejské lidově demokratické republice[30],

– 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 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))[31],

– s ohledem na své usnesení ze dne 9. října 2025 o společné reakci na nedávné narušení vzdušného prostoru a kritické infrastruktury členských států EU Ruskem[32],

– s ohledem na své usnesení ze dne 18. června 2025 o zprávě Komise o právním státu za rok 2024[33],

– s ohledem na své usnesení ze dne 7. května 2025 o přepracovaném dlouhodobém rozpočtu Unie v měnícím se světě[34],

– 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 korupci[35],

– s ohledem na své usnesení ze dne 1. června 2023 o zahraničním vměšování do všech demokratických procesů v Evropské unii, včetně dezinformací[36],

– 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 institucích[37],

– s ohledem na své usnesení ze dne 23. listopadu 2022 o uznání Ruské federace za stát, který podporuje terorismus[38],

---

[28] Úř. věst. L 186, 25.7.2023, s. 1, ELI: http://data.europa.eu/eli/reg/2023/1529/oj.
[29] Úř. věst. L, 2024/1603, 31.5.2024, ELI: http://data.europa.eu/eli/dec/2024/1603/oj.
[30] Úř. věst. L, 2024/1602, 31.5.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/1602/oj.
[31] Přijaté texty, P10_TA(2025)0306.
[32] Přijaté texty, P10_TA(2025)0230.
[33] Úř. věst. C, C/2025/6259, 19.12.2025, ELI: http://data.europa.eu/eli/C/2025/6259/oj.
[34] Přijaté texty, P10_TA(2025)0090.
[35] Úř. věst. C, C/2024/4011, 17.7.2024, ELI: http://data.europa.eu/eli/C/2024/4011/oj.
[36] Úř. věst. C, C/2023/1226, 21.12.2023, ELI: http://data.europa.eu/eli/C/2023/1226/oj.
[37] Úř. věst. C 177, 17.5.2023, s. 109.
[38] 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 dezinformací[39],

– s ohledem na své usnesení ze dne 8. března 2022 o zmenšujícím se prostoru pro občanskou společnost v Evropě[40],

– s ohledem na své usnesení ze dne 20. října 2021 o evropských médiích v digitální dekádě – akční plán na podporu oživení a transformace[41],

– s ohledem na své usnesení ze dne 23. listopadu 2016 o strategické komunikaci EU s cílem bojovat proti propagandě, kterou proti ní vedou třetí strany[42],

– 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 softwaru[43],

– 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 rozšíření[44],

– 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 strany[45],

– 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 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),

[39] Úř. věst. C 347, 9.9.2022, s. 61.
[40] Úř. věst. C 347, 9.9.2022, s. 2.
[41] Úř. věst. C 184, 5.5.2022, s. 71.
[42] Úř. věst. C 224, 27.6.2018, s. 58.
[43] Úř. věst. C, C/2024/494, 23.1.2024, ELI: http://data.europa.eu/eli/C/2024/494/oj.
[44] Úř. věst. C 167, 11.5.2023, s. 105.
[45] Úř. věst. C 23, 21.1.2021, s. 152.

– 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 nazvaná „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 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 kodex chování v oblasti dezinformací,

– 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 parlamentu[46],

– 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 politik[47].

– 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,

[46] Úř. věst. L, 2023/2829, 20.12.2023, ELI: http://data.europa.eu/eli/reco/2023/2829/oj.
[47] Úř. věst. L, 2023/2836, 20.12.2023, ELI: http://data.europa.eu/eli/reco/2023/2836/oj.

– 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 infrastruktury[48],

– s ohledem na rozhodnutí Rady (SZBP) 2023/855 ze dne 24. dubna 2023 o partnerské misi Evropské unie v Moldavsku (EUPM Moldova)[49],

– 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 transparentnosti[50],

– 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,

---

[48] Úř. věst. C 20, 20.1.2023, s. 1.
[49] Úř. věst. L 110, 25.4.2023, s. 30, ELI: http://data.europa.eu/eli/dec/2023/855/oj.
[50] 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 2025[51],

– 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 Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) ze dne 1. října 2025 nazvanou „ENISA Hrozby v roce 2025“,

– s ohledem na zprávu Europolu nazvanou „Posouzení hrozeb závažné a organizované trestné činnosti v EU – měnící se DNA závažné a organizované trestné činnosti“, která byla zveřejněna v roce 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 influencer reklamu, 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),

[51] 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 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“ (Pilíře 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, 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 špionážní 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“ (Influenceři 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 2024“ (Mapování svobody médií – monitorovací zpráva 2024), zveřejněnou v únoru 2025,

– 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 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 článek 55 jednacího řádu,

– s ohledem na zprávu zvláštního výboru pro Evropský štít pro demokracii (A10-0000/2025),

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 stanovili řadu opatření na posílení, ochranu a podporu silných a odolných demokracií v celé EU;

B. vzhledem k tomu, že Evropské středisko pro odolnost demokracie představuje jádro Evropského štítu pro demokracii; vzhledem k tomu, že obě 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 pro boj proti zahraniční manipulaci s informacemi a zahraničnímu vměšování (FIMI);

C. vzhledem k tomu, že nedávné zprávy ESVČ o hrozbách 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 EU umožňovaly přijímat včasná a koordinovaná protiopatření; vzhledem k tomu, že institucionální propojení EU je hlavním terčem nepřátelských informačních manipulačních kampaní; vzhledem k tomu, že EU trpí roztříštěným přístupem k boji proti zahraniční manipulaci s informacemi a vměšování a dezinformacím, přičemž mezi členskými státy existují značné rozdíly v kapacitách a neexistuje žádný zastřešující strategický rámec propojující operativní reakci se zpravodajskými informacemi o hrozbách;

D. vzhledem k tomu, že cennými součástmi celkové odolnosti EU vůči zahraniční manipulaci s informacemi a vměšování a dezinformacím jsou ECNE, systém rychlého varování (RAS) 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 propojující národní operační kapacity s koordinací na úrovni EU;

E. vzhledem k tomu, že hrozby představované zahraniční manipulací s informacemi a vměšováním 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 Smlouvy o EU a na zásadu otevřených a transparentních rozhodovacích procesů zakotvenou v článku 1 Smlouvy o EU, a to způsobem, který nepříznivě ovlivňuje zájmy EU;

F. vzhledem k tomu, že jednotlivé členské státy, které investovaly do specializovaných operačních struktur s jasnými stanovami a mandáty, jakož i dostatečným financováním a personálním vybavením, dokazují, čeho lze dosáhnout, zejména v případě francouzské agentury VIGINUM a švédské Agentury pro psychologickou obranu;

G. vzhledem k tomu, že rychlý pokrok v oblasti umělé inteligence (AI) a technologií deepfake předstihuje adaptační schopnosti roztříštěných národních institucí; vzhledem k tomu, že bez koordinované reakce EU a jasných operačních schopností bude technologická převaha stále více nahrávat útočníkům na úkor obránců;

H. vzhledem k tomu, že souběh raných fází provádění nařízení o digitálních službách (DSA), nařízení o digitálních trzích (DMA), aktu o umělé inteligenci (AI Act) a evropského aktu o svobodě médií (EMFA) vytváří příležitost k vybudování komplexní obrany proti zahraniční manipulaci s informacemi a vměšování;

I. 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) personalizace, sledování a mikrotargetingu jednotlivců, d) webových stránek navržených tak, aby napodobovaly oficiální zdroje, e) umělého zesilování rozdělujícího obsahu,f) využívání syntetického obsahu, jako jsou deepfakes a jiný obsah generovaný umělou inteligencí, a g) doporučovacích systémů záměrně navržených tak, aby podněcovaly zapojení prostřednictvím polarizace;

J. vzhledem k tomu, že online platformy při rozhodování o tom, zda propagovat obsah ve feedu uživatele, využívají své poznatky o preferencích a zranitelných místech každého jednotlivého uživatele, díky čemž jsou vlivnější než tradiční vydavatelé;

K. vzhledem k tomu, že EU nedávno přijala soubor komplexních právních aktů s cílem vytvořit bezpečný a transparentní online prostor, včetně nařízení o digitálních službách, nařízení o transparentnosti a cílení politické reklamy a aktu o umělé inteligenci;

vzhledem k tomu, že tyto právní akty představují významný pokrok v oblasti odpovědnosti digitálních platforem a ochrany demokratických procesů, zvyšování transparentnosti a zajištění svobody projevu; vzhledem k tomu, že jejich prosazování zůstává i nadále výzvou;

L. vzhledem k tomu, že využití umělé inteligence přináší nové příležitosti pro posílení správy voleb a dohledu nad nimi, například prostřednictvím odhalování neobvyklé online aktivity 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; vzhledem k tomu, že důvěryhodné zprávy odhalily činnost moskevské dezinformační sítě známé jako „Pravda“, která se záměrně zaměřila na velké jazykové modely (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; 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 podtrhuje potřebu posílit gramotnost v oblasti umělé inteligence ve vzdělávání, v práci a ve společnosti obecně;

M. vzhledem k tomu, že důležitou roli při posilování digitální odolnosti našich společností mohou hrát online influenceři, když zvyšují povědomí o mediální gramotnosti, demokratických postupech nebo přispívají ke zdravé politické debatě;

N. 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; 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;

O. 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 a nevystopovatelné politické propagandy; vzhledem k tomu, že jeho původ v Rusku a nedostatečná moderace obsahu vyvolávají trvalé obavy ohledně jeho role při podrývání 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 DSA, což jej podrobuje přísnějším regulačním povinnostem a požadavkům na zmírňování rizik;

P. 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, cloudové služby a platformy sociálních médií; vzhledem k tomu, že nezbytnými kroky k vybudování konkurenceschopného, bezpečného a odolného digitálního ekosystému EU jsou posílení domácích inovací, podpora evropských startupů a investice do suverénní digitální infrastruktury ; 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;

Q. vzhledem k tomu, že výzkum ukazuje znepokojivý trend v programech přerozdělování příjmů online platforem, který odhaluje, že mediální subjekty, na než 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 informační prostory EU;

R. 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, dalších 13 % respondentů uvedlo, že by ji možná využilo; vzhledem k tomu, že v Nizozemsku představuje kombinovaný podíl nejmladších voličů více než jednu třetinu voličů; vzhledem k tomu, že tento trend je v souladu se zjištěními ve všech členských státech i na celosvětové úrovni; vzhledem k tomu, že údaje nizozemského orgánu na ochranu údajů prokazují, že doporučení týkající se hlasování generovaná chatboty s umělou inteligencí často představují velmi zkreslený a polarizovaný pohled na politickou scénu;

S. vzhledem k tomu, že základní právo na svobodu projevu a informací, zakotvené 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 společnostem odhalovat, odkrývat a odmítat manipulativní narativy prostřednictvím demokratické diskuse;

T. vzhledem k tomu, že svoboda projevu a informací je základním právem, jehož účelem je chránit lidi, nikoli stroje, boty a umělou inteligenci;

U. 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 boti a softwarové programy založené na umělé inteligenci, jsou schopny vykazovat autonomní chování a

následně narušovat a ničit skutečnou veřejnou diskusi tím, že zaplavují projevy skutečných osob neautentickým obsahem;

V. vzhledem k tomu, že svoboda a pluralita sdělovacích prostředků jsou základními kameny evropského způsobu života, zakotvenými v čl. 11 odst. 2 Listiny základních práv Evropské unie; vzhledem k tomu, že redakčně nezávislá, vysoce kvalitní žurnalistika je účinným protijedem proti zahraniční manipulaci s informacemi a vměšování a dezinformacím;

W. vzhledem k tomu, že podle nařízení o digitálních trzích by vývojáři aplikací, kteří distribuují své aplikace prostřednictvím obchodů s aplikacemi, měli mít možnost bezplatně informovat zákazníky o alternativních nabídkách mimo obchod s aplikacemi; vzhledem k tomu, že Komise zahájila vyšetřování možného porušení nařízení o digitálních trzích ze strany společnosti Google, která ve výsledcích vyhledávání snižuje hodnocení obsahu vydavatelů médií; vzhledem k tomu, že Komise zahájila první přezkum nařízení o digitálních trzích dne 3. července 2025;

X. vzhledem k tomu, že směrnice o audiovizuálních mediálních službách vyžaduje, aby členské státy přijaly opatření pro rozvoj dovedností v oblasti mediální gramotnosti a každé tři roky podávaly zprávu o svém úsilí v této oblasti;

Y. vzhledem k tomu, že organizace Media Freedom Rapid Response zaznamenala v roce 2024 celkem 1 548 případů porušení svobody tisku, od právních, fyzických a psychických hrozeb až po různé formy cenzury, které se týkaly 2 567 osob nebo subjektů působících v oblasti médií v 35 evropských zemích, což představuje alarmující nárůst oproti 1 153 případům porušení zaznamenaným v roce 2023;

Z. vzhledem k tomu, že vyjednavači Parlamentu a Rady dosáhli dne 11. prosince 2025 předběžné dohody o navrhovaném nařízení o prověřování zahraničních investic v Unii;

AA. vzhledem k tomu, že pro EU má strategický význam činnost Rádia Svobodná Evropa/Rádia Svoboda (RFE/RL); vzhledem k tomu, že EU schválila na tuto činnost nouzové financování ve výši 5,5 milionu EUR v návaznosti na reformu politiky zahraniční pomoci Spojených států; vzhledem k tomu, že je třeba vypracovat udržitelné řešení financování RFE/RL;

AB. vzhledem k tomu, že nové technologie, jako je umělá inteligence, mohou zlepšit pracovní podmínky a metody novinářů, ale mohou také novináře vystavit novým hrozbám, jako je rychlé a levné napodobování stávajících médií, masové vytváření dezinformačních kanálů a koordinované útoky proti novinářům;

AC. vzhledem k tomu, že probíhající ruská útočná válka proti Ukrajině ilustruje zásadní úlohu, kterou hraje občanská společnost v krizových situacích, zejména pokud jde o poskytování humanitární pomoci, zajištění základních potřeb a pokračování každodenního života postiženého obyvatelstva;

AD. vzhledem k tomu, že občanská společnost rovněž hraje zásadní úlohu při přispívání k tvorbě politik, poskytování sociálních a komunitních služeb, zvyšování povědomí o důležitých sociálních otázkách, zastupování různých skupin v ohrožených situacích a prosazování a ochraně základních práv občanů;

AE. 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, jejíž zřízení Komise oznámila jako součást provádění strategie, bude mít za cíl poskytnout pravidelný a strukturovaný rámec pro ochranu a prosazování hodnot EU a zefektivnění a posílení zapojení v oblasti základních práv, demokracie, rovnosti a právního státu a bude funkční v roce 2026; vzhledem k tomu, že strategie zahrnuje také vytvoření online centra znalostí o občanském prostoru, které by mělo dokumentovat stávající iniciativy v oblasti monitorování občanského prostoru, zprávy a zdroje ochrany na vnitrostátní, evropské a mezinárodní úrovni ve spolupráci s Agenturou Evropské unie pro základní práva;

AF. vzhledem k tomu, že program AgoraEU, který Komise navrhla pro víceletý finanční rámec (VFR) na období 2028–2034, představuje významný pokrok v posilování podpory EU pro kulturu, média a občanskou společnost, s předpokládaným rozpočtem ve výši 9 miliard EUR;

AG. vzhledem k tomu, že hybridní útoky zaměřené na kritickou infrastrukturu v EU jsou častější než kdykoli předtím, přičemž tyto incidenty souvisejí se stejnými zlovolnými aktéry, jako jsou Rusko a Čína, ale také Írán a Severní Korea; vzhledem k tomu, že častým cílem těchto útoků jsou základní systémy, sítě a zařízení, které jsou životně důležité pro fungování společnosti, včetně veřejné bezpečnosti, ochrany a hospodářské stability; vzhledem k tomu, že tyto útoky mají různé podoby a formy, jako je fyzická sabotáž, žhářské útoky, špionáž a rušení signálu, jakož i kybernetické útoky a jiné aktivity v šedé zóně, které všechny svědčí o koordinovaném úsilí o testování, narušení a oslabení bezpečnosti a společenské odolnosti EU;

AH. vzhledem k tomu, že v Baltském moři došlo k bezprecedentnímu nárůstu počtu poruch podmořských kabelů, které jsou nezbytné pro připojení k internetu a dodávky elektřiny v celém baltském a severském regionu; vzhledem k tomu, že od roku 2023 bylo zaznamenáno nejméně 11 případů poškození kabelů, což naznačuje koordinovanou sabotáž;

AI. vzhledem k tomu, že v posledních měsících bylo hlášeno několik narušení vzdušného prostoru a neoprávněných 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 řada těchto incidentů byla jednoznačně přičítána ruským vojenským letadlům a dronům, zatímco jiné incidenty, při nichž se objevily neidentifikované létající objekty, jsou stále předmětem vyšetřování, ale všeobecně se má za to, že jsou součástí stejného vzorce hybridního zastrašování a destabilizace namířených proti Evropě;

AJ. vzhledem k tomu, že několik evropských zemí, včetně Francie, Estonska, Německa, Česka a Norska, čelilo v poslední době závažným kybernetickým útokům zaměřeným na vládní systémy, kritickou infrastrukturu a soukromé podniky, které jsou připisovány ruským vojenským zpravodajským službám a čínským subjektům napojeným na stát, což vše podtrhuje naléhavou potřebu posílit kolektivní kybernetickou odolnost EU a její schopnosti v oblasti přičtení odpovědnosti třetímu státu za kybernetické útoky;

AK. vzhledem k tomu, že závislost EU na zahraničních subjektech a technologiích zahraniční výroby v oblasti kritické infrastruktury a dodavatelských řetězců zůstává závažným problémem a představuje jednu z nejvýznamnějších slabých stránek EU; vzhledem k tomu, že tento jev je obzvláště rozšířený v technologickém a digitálním odvětví, což představuje klíčovou výzvu pro kybernetickou bezpečnost;

AL. vzhledem k tomu, že nástroje trestního práva mohou přispět k Evropskému štítu pro demokracii v rozsahu, v jakém dotyčné činnosti představují trestné činy;

AM. 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 pro vnitřní bezpečnost EU představuje zahraniční vměšování;

AN. vzhledem k tomu, že Agentura Evropské unie pro spolupráci v oblasti prosazování práva (Europol) ve své nejnovější zprávě o hodnocení hrozeb závažné a organizované trestné činnosti v EU (EU-SOCTA), zveřejněné v březnu 2025, varovala před zapojením zločineckých organizací do hybridních kampaní; vzhledem k tomu, že sdělení Komise 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 mezer v mandátu agentury, pokud jde o nové bezpečnostní hrozby, zejména sabotáž, hybridní hrozby a manipulaci s informacemi;

AO. vzhledem k tomu, že se Komise zavázala zahájit reformu, která z Europolu učiní skutečně funkční policejní agenturu; vzhledem k tomu, že policisté jsou klíčovými partnery při ochraně demokratických institucí; vzhledem k tomu, že by to mělo být jasněji uznáno v příslušných politikách;

AP. vzhledem k tomu, že členské státy mohou požádat Agenturu Evropské unie pro justiční spolupráci v trestních věcech (Eurojust) o pomoc vnitrostátním orgánům při řešení jakéhokoli druhu protiprávního jednání spadajícího do jejich jurisdikce; vzhledem k tomu, že soudní spolupráce může být obzvláště náročná při rozšiřování do nových oblastí trestního práva, což vyžaduje modernizované právní nástroje;

AQ. vzhledem k tomu, že agentury EU odpovědné za správu hranic, migraci a azyl, tj. Evropská agentura pro pohraniční a pobřežní stráž (Frontex) a Agentura Evropské unie pro otázky azylu, hrají v oblasti spolupráci s vnitrostátními orgány klíčovou úlohu, pokud jde o vytváření a udržování společného situačního povědomí o rizicích spojených se zneužíváním migračních toků pro politické účely a pokud jde o poskytování krizové pomoci členským státům, které se nacházejí v „první linii“; vzhledem k tomu, že Komise zařadila posílení agentury Frontex do svých stěžejních iniciativ pro volební období 2024–2029;

AR. vzhledem k tomu, že kandidátské země a sousedé EU, zejména Ukrajina, Moldavsko a země západního Balkánu, zůstávají i nadále terčem zahraniční manipulace s informacemi a vměšování a hybridních hrozeb a potřebují podporu EU k budování občanské a institucionální odolnosti;

AS. vzhledem k tomu, že ruská útočná válka proti Ukrajině a asertivní geopolitický postoj Číny vedly k intenzivnějšímu využívání dezinformací, ekonomického nátlaku a strategického vlivu, které se zaměřují nejen na EU, ale také na zranitelné regiony, jako je západní Balkán, země východního partnerství a globální Jih; vzhledem k tomu, že

různé zdroje uvádějí, že rozpočet Ruska na šíření dezinformací a propagandy činí mezi 1 a 2 miliardami USD ročně; vzhledem k tomu, že volby a politické události v celé Evropě svědčí o přetrvávající, cílené a sofistikované plnohodnotné ofenzivní hybridní válce vedené Ruskem, jejímž cílem je destabilizovat důvěru v naše politické systémy a instituce a vytvářet neustálý zmatek mezi tím, co jsou fakta a co jsou nepravdivé informace; vzhledem k tomu, že taková válka vyžaduje odpovídající reakci a přechod od čistě obranné strategie k ofenzivní;

AT. 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;

AU. vzhledem k tomu, že snížení podpory USA pro mezinárodní demokracii vytvořilo značnou globální mezeru ve financování boje proti dezinformacím a autoritářskému vlivu;

AV. vzhledem k tomu, že mezinárodní iniciativy, včetně iniciativ OSN, Organizace pro hospodářskou spolupráci a rozvoj a skupiny G7, začaly vytyčovat zásady a rámce pro ochranu integrity informací, zakotvené v demokratických hodnotách, pluralitě sdělovacích prostředků a lidských právech;

AW. vzhledem k tomu, že manipulace s informacemi a vměšování představují rostoucí výzvu pro demokratickou odolnost EU; vzhledem k tomu, že určité formy manipulativních informačních aktivit mohou také pocházet od subjektů působících v rámci EU; vzhledem k tomu, že fenomén manipulace s informacemi a vměšování v domácím kontextu by měl být dále zkoumán a prozkoumán, zejména v souvislosti s jeho interakcí se zahraniční manipulaci s informacemi a zahraničním vměšování; vzhledem k tomu, že opatření předložená v boji proti 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 ve všech věkových skupinách;

AX. 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;

AY. vzhledem k tomu, že v posledních letech hraje ECNE stále důležitější úlohu, avšak v současnosti jí chybí zdroje a kapacity, aby posunula svou činnost na další úroveň;

AZ. vzhledem k tomu, že k účasti na schůzích ECNE byly přizvány kandidátské země; vzhledem k tomu, že kromě jejich účasti stále existuje značný potenciál pro další prohloubení spolupráce s těmito zeměmi v rámci činnosti sítě, pro sdílení zkušeností, jak přistupovat k hrozbám, a pro výměnu osvědčených postupů při jejich potírání;

BA. vzhledem k tomu, že je zřetelně zapotřebí posílit ochranu volební infrastruktury a vnitrostátních politických stran, které byly rovněž cílem kybernetických útoků, v neposlední řadě s ohledem na rozsáhlé kybernetické útoky na rumunské volební orgány na podzim 2024;

BB. vzhledem k tomu, že skryté financování politických stran a hnutí v EU třetími zeměmi ohrožuje legitimitu demokratického procesu;

BC. 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 jsou izolovány od tlaku politické a výkonné moci;

BD. vzhledem k tomu, že v letech 2022 až 2025 zavedla EU v reakci na vojenskou agresi Ruska vůči Ukrajině celkem 19 balíčků rozsáhlých, bezprecedentních sankcí, čímž výrazně zvýšila tlak na ruskou válečnou ekonomiku, především v klíčových odvětvích, jako je energetika, finance a obranný průmysl, zvláštní ekonomické zóny a subjekty, které útočnou válku umožňují nebo z ní mají prospěch, a zbavila 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;

BE. vzhledem k tomu, že od 8. října 2024 sankční rámec EU umožňuje zaměřit se 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 migrantů 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 EU má nyní možnost přikročit také ke zmrazení majetku, zákazu cestování a pozastavení vysílacích licencí či zákazu finančních transakcí a transakcí s kryptoaktivy spojených s hybridními činnostmi;

BF. vzhledem k tomu, že 28. prosince 2024 ruská vláda oznámila, že „výrazně rozšířila“ svou černou listinu občanů a úředníků EU, včetně zástupců 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 neprůhledných a svévolných omezení, často bez jakéhokoli formálního oznámení, odůvodnění nebo práva na odvolání;

BG. vzhledem k tomu, že hybridní hrozby, zahraniční vměšování a dezinformační kampaně se vyvinuly v komplexní a rozsáhlé meziodvětvové krize, jež negativně dopadají na bezpečnost a ochranu, blahobyt občanů a fungování společnosti a hospodářství jako celku, což představuje zásadní problém v oblasti vnitřních záležitostí EU a destabilizuje demokratické instituce ve všech členských státech, jak je patrné již od počátku ruské agrese proti Ukrajině;

BH. vzhledem k tomu, že účinná civilní a obranná připravenost vyžaduje komplexní, celospolečenský a mezirezortní přístup zohledňující všechna rizika a založený na spolupráci vnitrostátních orgánů členských států s orgány, institucemi a jinými subjekty EU, s podniky, akademickou obcí, občanskou společností a jednotlivými občany; vzhledem k tomu, že toto úsilí musí být doplněno dlouhodobými investicemi,

strategickým výhledem a začleněním hlediska odolnosti do tvorby politik, rozvoje infrastruktury, vzdělávacích systémů a dodavatelských řetězců;

BI. vzhledem k tomu, že klíčem k odolnosti společnosti je posílení postavení občanů a 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 krize;

BJ. vzhledem k tomu, že zásadní význam pro zvýšení obranné připravenosti mají civilně-vojenská spolupráce, kapacity dvojího užití a začlenění hlediska připravenosti do vzdělávacích programů 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;

BK. 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;

BL. vzhledem k tomu, že připravenost závisí na hladké spolupráci mezi orgány, agenturami, členskými státy a mezinárodními partnery EU, která musí být podpořena společnými cvičeními a odbornou přípravou, sdílenými platformami pro získávání poznatků o situaci a rychlou výměnou informací;

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

Úvod

1. vítá společné sdělení Komise a vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku 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 před vnějšími hrozbami a přispívat tak k ochraně evropského způsobu života, právního státu a hodnot zakotvených v článku 2 SEU;

2. se znepokojením bere na vědomí stále složitější a neustále se vyvíjející hrozby pro EU a její členské státy, mezi něž patří především zahraniční manipulace s informacemi a vměšování, hybridní útoky a dezinformační kampaně vedené nepřátelskými aktéry ze třetích zemí; zdůrazňuje, že tyto nepřátelské akce podkopávají demokratické základy EU, neboť způsobují rozkol, snižují důvěru veřejnosti v instituce, míří na citlivá místa ve společnosti a často využívají pokročilé digitální technologie;

3. považuje Rusko za hlavní vnější hrozbu pro demokratickou integritu Evropy; znovu opakuje, že Rusko pokládá za stát, který podporuje terorismus; poukazuje na naléhavou potřebu komplexní, soudržné a na budoucnost zaměřené strategie pro účinné řešení těchto výzev a ochranu evropské demokracie;

4. znovu vyjadřuje své přesvědčení, že klíčové politické priority uvedené v iniciativě Evropský štít pro demokracii – včetně boje proti zahraniční manipulaci s informacemi a vměšování a hybridním hrozbám, zvýšení odolnosti volebních procesů, posílení kybernetické bezpečnosti, podpory občanské společnosti a prosazování nezávislé a investigativní žurnalistiky – musí být pevně zakotveny a dostatečně financovány v nadcházejícím VFR;

Evropské středisko pro odolnost demokracie

5. vítá návrh Komise na zřízení Evropského střediska pro odolnost demokracie („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 průběhu roku 2026; vítá závazek Komise, že bude Parlament o vytváření Evropského štítu pro demokracii a střediska pravidelně informovat a že jej do tohoto procesu zapojí;

6. připomíná však, že návrh postrádá dostatečně podrobné provozní informace, jasné rozpočtové příděly, zvláštní strukturu řízení, konkrétní mandát a harmonogram; konstatuje, že společné sdělení o Evropském štítu pro demokracii výslovně nespojuje centrum s žádným z opatření v něm uvedených – ta zůstávají v různých správních rámcích Komise a ESVČ; vyjadřuje znepokojení nad tím, že bude-li středisko pouze dalším centrem, sítí, platformou nebo rámcem, mohlo by to dále oslabit schopnost EU účinně využívat celé spektrum nástrojů, které jsou v současné době k dispozici, a prohloubit nedostatky zjištěné ve společném sdělení, včetně snížené reaktivity, roztříštěnosti a napjatých rozpočtů;

7. 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; žádá, aby integrace zahrnovala příslušné mechanismy dohledu a prosazování podle nařízení o digitálních službách, zejména s cílem určit a minimalizovat systémová rizika, koordinovat úsilí v boji proti manipulacím s informacemi, zajistit provozní odpovědnost za posílený systém včasného varování a údržbu a provoz jednotné zpravodajské databáze s údaji o zahraniční manipulaci s informacemi a vměšování a rozvíjet mimo jiné iniciativu EUvsDisinfo, ECNE a pracovní skupinu Komise pro dezinformace a strategickou komunikaci;

8. vítá skutečnost, že Komise uznala nutnost spolupracovat s členskými státy a Parlamentem na mandátu, struktuře a pracovních metodách střediska, a vyzývá Komisi, aby tento proces zahájila tím, že do prvního čtvrtletí roku 2027 navrhne právní základ pro zřízení střediska jako 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 podnikat rozhodné kroky a zároveň nést odpovědnost;

9. vyzývá Komisi, aby středisku poskytla jasný mandát a rozhodovací mechanismy, které mu umožní fungovat jako nezávislé centrum excelence pro odhalování a analýzu zahraniční manipulace s informacemi a vměšování a dezinformací, jako platforma pro budování kapacit, která zavede společné definice, normy, odbornou přípravu a technické nástroje v celé EU, a jako operační páteř zajišťující v reálném čase koordinaci technické podpory v boji proti aktivním dezinformačním kampaním;

10. vyzývá Komisi, aby zajistila, že středisku bude svěřena 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 v oblasti boje proti zahraniční manipulaci s informacemi a vměšování a dezinformacím EU; 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;

11. vyzývá členské státy, které nemají specializované operační struktury, aby za podpory střediska zřídily nebo podstatně posílily specializované vnitrostátní instituce pro boj proti zahraniční manipulaci s informacemi a vměšování a odhalování dezinformací a reakci na ně; vyzývá Komisi, aby vypracovala plán rozvoje kapacit členských států;

12. vyzývá Komisi, aby posoudila proveditelnost zmocnění střediska ke správě a k přidělování specializovaných grantů EU v rámci příslušných programů EU, včetně programu Digitální Evropa, Nástroje pro propojení Evropy, programu Horizont Evropa, programu Občané, rovnost, práva a hodnoty (CERV) a navrhovaného programu AgoraEU, a aby středisko pověřila vydáváním výzev k podávání návrhů a výběrem, kontrolou a hodnocením projektů v oblastech spadajících do jeho oblasti působnosti, zejména pokud jde o Evropské středisko pro sledování digitálních médií, iniciativy v oblasti mediální gramotnosti a další příslušné evropské, regionální a přeshraniční iniciativy zaměřené na boj proti zahraniční manipulaci s informacemi a vměšování, posílení demokratické odolnosti a podporu integrity informací;

13. vyzývá Komisi, aby pro činnost střediska vyčlenila v rozpočtu EU zvláštní položku s jasným oddělením provozního financování a obecných nákladů na koordinaci; rovněž 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;

14. vyzývá Komisi, aby posoudila proveditelnost vytvoření mechanismu financování z příspěvků velmi velkých online platforem, který by doplnil zvláštní rozpočtovou položku na činnost střediska; připomíná, že bankovní sektor financuje mechanismy řešení problémů bank, farmaceutické společnosti přispívají na monitorování bezpečnosti a znečišťující odvětví nesou environmentální náklady; žádá vytvoření mechanismu, v jehož rámci by platformy sociálních médií přispívaly úměrně tomu, jaká infrastruktura je třeba k eliminaci negativních vnějších vlivů a systémových rizik spojených s jejich službami, a to jak v souvislosti se zahraniční manipulací s informacemi a vměšováním a s dezinformacemi, tak v souvislosti s budováním odolnosti; zdůrazňuje, že tyto příspěvky by nejen byly v souladu se zavedenými evropskými zásadami odpovědnosti, ale rovněž by zajistily, aby náklady na ochranu demokratického diskurzu hradili ti, kteří mají z digitálního informačního ekosystému největší prospěch;

Digitální odolnost

15. vyzývá k plnému provedení klíčových právních předpisů v digitálním prostoru, jako je nařízení o digitálních službách, nařízení o transparentnosti a cílení politické reklamy a akt o umělé inteligenci, ve všech členských státech; zastává názor, že provádění právních předpisů v digitální oblasti by se do budoucna mělo více zaměřit na boj proti dezinformacím na internetu, zajištění integrity informací a ochranu demokratického diskurzu v období voleb; v této souvislosti vyjadřuje znepokojení nad tím, že opožděné pokyny a technické normy představují překážku pro včasné provedení aktu o umělé inteligenci; vítá skutečnost, že Komise se ve svém návrhu souhrnného balíčku pro digitální oblast, jehož cílem je zjednodušit právní předpisy v oblasti umělé inteligence, snaží tento problém řešit propojením harmonogramu provádění pravidel pro vysoce rizikové systémy umělé inteligence s dostupností norem nebo jiných podpůrných nástrojů;

16. vítá oficiální začlenění dobrovolného kodexu zásad boje proti dezinformacím do rámce nařízení o digitálních službách; domnívá se, že neautentické používání sociálních médií, např. prostřednictvím botů, falešných účtů, polarizačních algoritmů a umělého zapojování uživatelů a vyostřování obsahu, patří k nejzávažnějším rizikům pro svobodný a otevřený diskurz na internetu, zejména v období voleb; 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;

17. vítá příslib Komise, že vypracuje protokol pro případ krizí a incidentů k nařízení o digitálních službách s cílem podrobněji upravit řešení závažných incidentů a vměšování v informačním prostředí; domnívá se, že tento protokol by měl mimo jiné řešit zasahování do voleb prostřednictvím koordinovaného neautentického chování v online prostoru, zejména prostřednictvím botového vyostřování obsahu a zapojování uživatelů, jež reálně narušují skutečný veřejný diskurz;

18. bere na vědomí, že Komise dokončila vyšetřování porušení povinnosti transparentnosti podle nařízení o digitálních službách ze strany platformy X a uložila pokutu ve výši 120 milionů EUR; naléhavě vyzývá Komisi, aby urychlila ostatní probíhající vyšetřování možných porušení právních předpisů EU v digitální oblasti, včetně těch, která se týkají zasahování do voleb, algoritmické netransparentnosti nebo šíření falešných účtů a botů; zejména Komisi žádá, aby urychleně dokončila vyšetřování dodržování nařízení o digitálních službách ze strany platformy TikTok v souvislosti s rumunskými prezidentskými volbami v roce 2024, včetně povinnosti omezit systémová rizika pro demokratické procesy;

19. vyzývá Komisi a příslušné regulační orgány, aby vyšetřily a veřejně odhalily skryté dezinformační kampaně zaměřené na využívání generativních systémů umělé inteligence, jako jsou činnosti moskevské sítě „Pravda“; naléhavě vyzývá poskytovatele systémů umělé inteligence, aby tento jev řádně řešili a potlačovali prostřednictvím svých systémů řízení rizik umělé inteligence; dále vyzývá ke koordinaci bezpečnostních norem pro poskytovatele velkých jazykových modelů na mezinárodní úrovni, což zajistí větší transparentnost, pokud jde o trénování z různých zdrojů údajů;

20. vyzývá Komisi, aby urychleně dokončila posouzení uživatelské základny a funkčnosti platformy Telegram z hlediska její klasifikace jako velmi velké online platformy podle nařízení o digitálních službách; naléhavě vyzývá Komisi a příslušné orgány, aby prošetřily možnou úlohu sítě Telegram v usnadňování trestné činnosti, zasahování do voleb a šíření dezinformací v rámci EU; dále důrazně vybízí tuto platformu, aby se připojila k dobrovolnému kodexu zásad boje proti dezinformacím a 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;

21. 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; v této souvislosti zdůrazňuje, že je třeba zavést přísné normy transparentnosti a integrity informací pro tvůrce politického obsahu na internetu, zejména influencery působící v šedé zóně mezi obchodní propagací a politickými sděleními; vítá kodexy chování a vzdělávací a další iniciativy zaměřené na zvýšení odpovědnosti a transparentnosti sociálních médií a influencerů;

22. domnívá se, že digitální infrastruktura EU, včetně zabezpečených místních datových center a svrchovaných kapacit EU v oblasti cloud computingu a edge computingu, je strategickým pilířem digitální odolnosti, která zajišťuje, aby citlivé údaje Evropanů nebyly uchovávány v zahraničních datových centrech; vyzývá Komisi, aby v rámci plánovaného aktu o vývoji cloudových služeb a umělé inteligence navrhla definici svrchovaného cloudu a jeho oblast působnosti; vyzývá Komisi, aby se zamyslela nad neúspěšnou diskusí o systému certifikace kybernetické bezpečnosti EU pro cloudové služby a aby v revizi aktu o kybernetické bezpečnosti navrhla praktické řešení, které bude reagovat na obavy ohledně kybernetické bezpečnosti a svrchovanosti v souvislosti s koncentrací moci; důrazně žádá vytvoření regulačních pískovišť a mechanismů financování na podporu inovací, jež přinášejí technologické startupy EU, zejména v odvětvích s kritickou závislostí; dále podporuje dlouhodobou vizi platforem sociálních médií EU koncipovaných v souladu s hodnotami EU v oblasti transparentnosti, ochrany údajů, svobody projevu a demokratické odpovědnosti;

23. vyzývá Komisi, digitální regulační orgány EU a online platformy, aby zajistily transparentnost programů přerozdělování příjmů, neboť z nich mohou plynout příjmy původcům zahraniční manipulace s informacemi a vměšování, či dokonce subjektům uvedeným na sankčních seznamech; domnívá se, že zpeněžení činností zahraniční manipulace s informacemi a vměšování v těchto programech by mělo být řešeno v rámci povinnosti posuzovat a omezovat rizika podle nařízení o digitálních službách;

24. je znepokojen zjištěními nizozemského orgánu pro ochranu údajů, z nichž vyplývá, že chatboti využívající umělou inteligenci mohou poskytovat neobjektivní a nespolehlivá doporučení, koho volit, což představuje riziko pro integritu voleb; vyzývá Komisi, aby splnila svůj závazek k vypracování pokynů pro využívání umělé inteligence ve volebních procesech, jež zajistí, aby byla umělá inteligence využívána odpovědně;

Svoboda projevu

25. zdůrazňuje, že Evropský štít pro demokracii musí chránit a prosazovat svobodu projevu a informací jako základní právo platné v offline i online prostoru; zdůrazňuje, že

ochrana lidských práv v EU patří k nejlepším na světě a že za jejich ochranu nesou odpovědnost i společnosti, které chtějí působit v prostředí EU a získat evropské zákazníky; zdůrazňuje však, že svoboda projevu a informací má chránit lidské bytosti, a nikoli stroje nebo software, které vykazují neautentické chování, jako je umělá inteligence a umělé vyostřování obsahu a zapojování uživatelů prostřednictvím botů, či automatizované softwarové programy, jež na síti provádějí opakované úkony napodobující skutečné uživatele;

26. uznává význam účinných záruk pro uživatele při výkonu jejich demokratických práv, včetně možnosti napadnout rozhodnutí platforem o moderování obsahu a povinnosti platforem informovat uživatele, jakmile je jejich obsah odstraněn nebo omezen; připomíná, že podle nařízení o digitálních službách mají platformy povinnost mít pro tyto účely k dispozici samostatný mechanismus pro vyřizování stížností; zdůrazňuje, že ochrana základních práv jednotlivých uživatelů zahrnuje rovněž provádění důkladných posouzení a omezování systémových rizik ovlivňujících integritu informačního prostoru;

Integrita médií a informací

27. zastává názor, že nedílnou součástí dosažení cílů stanovených Evropským štítem pro demokracii jsou opatření na podporu svobodných a redakčně nezávislých médií; vítá v tomto ohledu průlomové společné minimální normy pro svobodu a pluralitu médií stanovené v nedávno přijatém evropském aktu o svobodě médií; zdůrazňuje však, že význam uvedeného aktu lze posoudit pouze na základě jeho praktického uplatňování, a proto vyzdvihuje důležitost jeho důsledného prosazování; vítá nové závazky v oblasti podpory médií prostřednictvím Programu pro odolnost médií a vyzývá k harmonizaci dlouhodobých závazků v nadcházejícím VFR;

28. zdůrazňuje, že je třeba důkladně posuzovat možný dopad právních předpisů EU na žurnalistiku a redakční sdělovací prostředky, se zvláštním ohledem na zajištění udržitelnosti a životaschopnosti obchodních modelů mediálních společností;

29. v souvislosti s mediálními společnostmi, které prodávají předplatné prostřednictvím aplikací, zdůrazňuje, že je důležité plně provést nařízení o digitálních trzích; v této souvislosti bere na vědomí rozhodnutí Komise o nesplnění povinností ze strany společností Apple a Meta ze dne 23. dubna 2025; bere na vědomí šetření Komise ve věci možného porušení nařízení o digitálních trzích společností Google z důvodu odsouvání obsahu vydavatelů sdělovacích prostředků ve výsledcích vyhledávání na nižší pozice;

30. vítá skutečnost, že společné sdělení obsahuje nová podpůrná opatření na podporu 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; zdůrazňuje, že nadcházející revize směrnice o audiovizuálních mediálních službách by měla posílit ustanovení o minimálních požadavcích na činnost členských států v oblasti mediální gramotnosti;

31. vítá ohlášenou aktualizaci doporučení Komise o bezpečnosti novinářů[52] a nadcházející přezkum doporučení, jež se týká strategických žalob proti účasti veřejnosti[53]; zdůrazňuje, že tyto aktualizace a přezkumy musí zohledňovat dopad hrozeb, násilí, sabotáže a dalších způsobů maření novinářské práce na ochranu, bezpečnost a postavení novinářů a dalších pracovníků médií v EU;

32. zdůrazňuje, že je důležité chránit novináře před zneužívajícími soudními řízeními; vítá v tomto ohledu přijetí směrnice proti strategickým soudním řízením proti účasti veřejnosti[54] 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; žádá Komisi, aby vypracovala komplexní hodnotící zprávu o účinnosti provádění;

33. vítá předběžnou dohodu o nařízení o přímých zahraničních investicích[55], 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;

34. vyzývá Komisi a členské státy, aby v souvislosti s pluralitou sdělovacích prostředků a nezávislou žurnalistikou pečlivě analyzovaly důsledky změny politiky pomoci ze strany vlády USA a aby v případě potřeby přijaly opatření k zaplnění mezery na mediálních trzích jak v EU, tak v příhraničních regionech; vítá mimořádné financování EU poskytnuté rozhlasové organizaci Svobodná Evropa (RFE/RL); vyzývá k vypracování řešení, které by RFE/RL poskytlo stabilní a dlouhodobé financování;

35. zdůrazňuje, že sítě pro ověřování faktů podporované občanskou společností mohou hrát úlohu při odhalování dezinformačních kampaní a boji proti nim a poskytovat cenné poznatky pro posouzení rizik v souladu s aktem o digitálních službách; konstatuje, že nezávislé organizace pro ověřování faktů potřebují pro svou činnost stabilní podmínky; domnívá se, že 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 a metodické objektivity;

---

[52] 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).

[53] 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).

[54] Směrnice 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“) (Úř. věst. L, 2024/1069, 16.4.2024, ELI: http://data.europa.eu/eli/dir/2024/1069/oj).

[55] 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).

Občanská společnost

36. zdůrazňuje klíčovou úlohu občanské společnosti při obraně naší demokracie, a to nejen tím, že působí jako strážce a odhaluje zahraniční pokusy zasahovat 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;

37. vítá strategii EU pro občanskou společnost, kterou zveřejnila Komise spolu se sdělením o Evropském štítu pro demokracii; vítá přístup Komise, který propojuje tuto strategii s činností týkající se štítu jako nástroj k dalšímu posílení občanské angažovanosti;

38. 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 systematičtější přístup, který bude využíván k posílení dialogu v souladu s hodnotami EU; domnívá se, že ohlášené on-line znalostní centrum pro občanský prostor může přispět ke koordinaci činností organizací občanské společnosti v oblasti ochrany demokracie a boje proti hybridním hrozbám a zahraniční manipulaci s informacemi a vměšování a zlepšit informovanost o situaci;

39. zdůrazňuje význam konkrétních programů financování, jako je program Občané, rovnost, práva a hodnoty (CERV); vítá myšlenku Komise zachovat program CERV a začlenit jej do nového programu AgoraEU na období 2028–2034; vyzývá Komisi, aby zajistila, aby financování této složky programu AgoraEU odpovídalo potřebám organizací občanské společnosti a bylo prováděno pod přímým řízením Komise;

40. zdůrazňuje, že je třeba zvýšit finanční transparentnost, pokud jde o financování organizací občanské společnosti obecně, a zejména v souvislosti s podporou ze strany třetích zemí; připomíná, že organizace občanské společnosti mohou být a byly využívány nepřátelskými subjekty ze zemí mimo EU jako nástroje k nezákonnému ovlivňování demokratických procesů v EU a jejích členských státech; zdůrazňuje, že Parlament má jako orgán zvláštní odpovědnost přispívat k reformám v této oblasti s ohledem na tzv. skandál Qatargate; 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 jako takové;

41. vítá návrh směrnice o zastupování zájmů jménem třetích zemí, který předložila Komise, jako důležitou součást balíčku opatření na obranu demokracie a jehož cílem je stanovit harmonizované požadavky na hospodářské činnosti související se zastupováním zájmů prováděným jménem subjektu ze třetí země; zdůrazňuje, že společná pravidla v tomto ohledu by představovala důležitou součást transparentnosti, pokud jde o vliv třetích zemí; vyzývá spolunormotvůrce, aby legislativní proces neprodleně dokončili;

42. 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 svých nástrojů pro zapojení občanů; 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;

Ochrana kritické infrastruktury

43. zastává názor, že ochrana EU a jejích členských států před fyzickými i digitálními akty sabotáže zaměřenými na kritickou infrastrukturu má zásadní význam pro zajištění demokratické odolnosti; vyzývá k přijetí důrazných preventivních opatření, posílení přeshraniční spolupráce a posílení schopnosti EU odhalovat tyto nepřátelské činnosti, odrazovat od nich a reagovat na ně;

44. důrazně odsuzuje eskalující zásahy bezpilotních letounů a další zásahy ze vzduchu zaměřené na kritickou infrastrukturu, včetně civilních letišť, vojenských základen a energetických zařízení v celé EU, a na její narušení, kterých se dopouštějí zejména Rusko a Bělorusko; 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;

45. zdůrazňuje, že škála hybridních aktivit, které Rusko vyvíjí proti EU, se v podstatě rovná státem podporovanému terorismu, 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; zdůrazňuje, 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;

46. vyzývá Komisi a členské státy, aby vypracovaly společný výklad Úmluvy Organizace spojených národů o mořském právu (UNCLOS) ze strany EU s cílem zajistit koordinovaný postup proti hybridním činnostem a sabotáži v námořních oblastech EU, zejména v Baltském moři; domnívá se, že přeshraniční koordinaci lze dále zlepšit jak na provozní, tak na finanční úrovni; zdůrazňuje, že je třeba, aby EU zintenzivnila svou reakci na hybridní hrozby v námořních oblastech, včetně hrozeb, které představuje ruská „stínová flotila“; poukazuje na to, že řešení těchto výzev vyžaduje vyčlenění dostatečných finančních prostředků EU;

47. se znepokojením bere na vědomí stávající strukturální závislosti v digitální infrastruktuře EU, včetně operačních systémů, datových center, polovodičů, umělé inteligence, kybernetické bezpečnosti, cloud computingu a různých digitálních platforem a služeb, které jsou důsledkem koncentrace trhu a zahraniční kontroly a všechny představují vysoké riziko pro demokracii, svobodu a bezpečnost v EU a pro konkurenceschopnost EU; vyzývá Komisi a členské státy, aby prostřednictvím ambiciózních a cílených politik, které zvýší investice do společností v EU a jejich podíl na trhu, vytvořily jako základní vrstvu svrchovanou digitální infrastrukturu EU s technologiemi na ochranu soukromí a ekosystém rozhraní EU pro programování aplikací (API), přičemž využijí evropské dodávky čisté energie při rozvoji datových center a cloudové infrastruktury, a to i prostřednictvím tržně orientovaných iniciativ, např. společné podniky nebo federované sítě v oblastech, jako jsou gigatovárny na umělou inteligenci nebo cloudové služby;

48. zdůrazňuje, že je třeba zajistit větší integraci mezi digitální infrastrukturou, kybernetickou bezpečností a obrannou politikou s cílem posílit strategickou autonomii

EU a že je třeba využít infrastrukturu dvojího užití, jako jsou odolná datová centra rozptýlená v celé EU, s cílem zajistit provozní kontinuitu tváří v tvář hybridním nebo válečným hrozbám; dále poukazuje na to, že je třeba zvýšit investice do vojenské mobility a bezpečné komunikace, včetně bezodkladného a přednostního zavádění vesmírných kapacit, jako je IRIS², s cílem poskytovat šifrované služby pro veřejné a obranné použití;

49. zdůrazňuje, že rámce kybernetické bezpečnosti, jako je směrnice NIS 2, akt o kybernetické odolnosti[56] a akt o kybernetické solidaritě[57], musí fungovat v souladu s cílem podpořit normy bezpečné již od fáze návrhu a zabránit roztříštěnosti právních předpisů; v této souvislosti vyzývá k revizi příslušných právních předpisů v oblasti kybernetické bezpečnosti a poukazuje na to, že je třeba posílit stávající struktury, jako je ENISA a Evropské centrum kompetencí pro kybernetickou bezpečnost;

50. 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 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 aktu o kybernetické solidaritě, jak je stanoveno ve strategii vnitřní bezpečnosti ProtectEU;

Spolupráce v oblasti spravedlnosti a vnitřních věcí

51. 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; 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;

52. vítá skutečnost, že společné sdělení uznává pozitivní přínos spolupráce v oblasti trestního soudnictví a prosazování práva v boji proti zahraniční manipulaci s informacemi a vměšování a dezinformačním činnostem; vyzývá Komisi, aby při přípravě plánované revize mandátů Europolu a Eurojustu pečlivě posoudila právní mezery, které v současné době těmto agenturám brání poskytovat plnou pomoc členským státům čelícím hybridním hrozbám, a aby prozkoumala, jakým způsobem je překonat;

---

[56] 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).

[57] 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).

53. se znepokojením bere na vědomí 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, což představuje vážnou hrozbu pro vnitřní bezpečnost EU; zdůrazňuje, že tyto praktiky představují neúnosný akt zahraničního vměšování s potenciálně destabilizujícími účinky na naši společnost; v této souvislosti poukazuje na to, že je třeba dále na úrovni EU posilovat koordinaci v oblasti trestního soudnictví a prosazování práva;

54. důrazně odsuzuje účelové využívání migrace jako zbraně proti EU; zastává názor, že tento jev představuje nepřijatelný pokus nepřátelských třetích zemí vyvíjet politický tlak na členské státy v přední linii a na EU; vítá zvláštní ustanovení o účelovém využívání migrace, která byla nedávno začleněna do klíčových právních předpisů EU týkajících se správy hranic a migrace; zdůrazňuje, že členské státy postižené těmito hrozbami by měly mít možnost počítat s podporou specializovaných agentur EU; vyzývá k posílení mandátu agentury Frontex, aby měla právní základ a lidské, finanční a technické zdroje, které potřebuje k náležité pomoci členským státům při řešení těchto hybridních hrozeb; v této souvislosti zdůrazňuje, že je třeba dále posílit schopnost EU přispívat k úsilí členských států v oblasti ochrany hranic dostatečnými investicemi v souladu s VFR na období 2028–2034;

Vnější rozměr

55. zdůrazňuje, že je třeba, aby Evropský štít pro demokracii měl silný vnější rozměr; vítá, že do společného sdělení byla zahrnuta konkrétní opatření zaměřená na podporu zemí za hranicemi EU, zejména prostřednictvím budování kapacit s cílem zlepšit odolnost kandidátských a potenciálních kandidátských zemí vůči zahraniční manipulaci s informacemi a vměšování a hybridnímu vměšování, podpory nezávislých sdělovacích prostředků a žurnalistiky a zvýšení jejich schopnosti monitorovat dezinformace v sociálních médiích před volbami a během voleb;

56. podporuje myšlenku využít diplomatické cesty k posílení kapacit v prioritních regionech; domnívá se, že úloha delegací EU a velvyslanectví členských států EU je klíčová, pokud jde o lepší pochopení místních podmínek, které mohou vést k zahraničnímu vměšování, a zajištění odpovídající reakce; bere na vědomí, že delegace EU a velvyslanectví členských států mohou podporovat pořádání osvětových kampaní v hostitelských zemích; zdůrazňuje, že je důležité zapojit mise a operace společné bezpečnostní a obranné politiky (SBOP) do činností plánovaných ve společném sdělení; vyzývá členské státy a ESVČ, aby do jednotlivých mandátů misí a operací začlenily činnost v oblasti budování kapacit a odbornou přípravu v oblasti hybridních hrozeb s cílem zvýšit připravenost vnitrostátních protějšků;

57. vyzývá k vypracování komplexní strategie, na jejímž základě by delegace EU a mise a operace SBOP mohly 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; 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; vyzývá místopředsedkyni Komise, vysokou představitelku Unie pro

zahraniční věci a bezpečnostní politiku a Radu, aby do misí SBOP začlenily týmy pro sledování dezinformací a reakci na ně, zajistily odbornou přípravu všech pracovníků misí v oblasti zahraniční manipulace s informacemi a vměšování a posílily koordinaci civilních a vojenských operací s cílem bojovat proti hybridnímu vlivu;

58. vítá skutečnost, že ve společném sdělení byl posílen závazek rozvíjet kapacitu ofenzivních informačních operací; konstatuje, že pro tento závazek, který vyžaduje dlouhodobé plánování, je třeba vyčlenit zdroje; zdůrazňuje, že cílem by mělo být, aby EU ve svém sousedství posílila proaktivní informační opatření proti destabilizujícímu úsilí Ruska; poukazuje na to, že mezi obyvatelstvem žijícím v autoritářských režimech, zejména v Rusku, 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;

59. uznává, že bezprostřední sousedé EU, včetně západního Balkánu, Moldavska a Ukrajiny, čelí závažnému zahraničnímu vměšování; vyzývá k financování regionálních koordinačních center pro boj proti zahraniční manipulaci s informacemi a vměšování, k intenzivnější podpoře investigativní žurnalistiky a regulačních orgánů pro sdělovací prostředky a k rozšíření strategické komunikace založené na faktech prostřednictvím delegací EU s cílem bojovat proti dezinformacím namířeným proti EU; zdůrazňuje, že je třeba se konkrétně zaměřit na pomoc v oblasti integrity voleb v zemích, které jsou kandidáty na členství v EU;

60. vyzývá Komisi, aby z programů mediální gramotnosti učinila trvalou součást předvstupní pomoci a evropského nástroje sousedství se zvláštními granty EU na podporu investigativní žurnalistiky ve zranitelných regionech;

61. vyzývá k posílení stávajícího úsilí EU o podporu partnerských zemí v jejím 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; zdůrazňuje zejména, že je třeba nadále rozvíjet stěžejní projekt EUvsDisinfo;

62. uznává zřízení 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 hybridním a kybernetickým hrozbám a hrozbám zahraniční manipulace s informacemi a vměšování; domnívá se, že 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; bere na vědomí parlamentní volby, které se v Moldavsku konaly dne 28. září 2025, a výrazné vítězství proevropské Strany akce a solidarity (PAS);

63. vítá nasazení týmů rychlé reakce EU na hybridní hrozby, jak dokládá nedávný příklad Moldavska, jako užitečný nástroj při budování kapacit a odolnosti v zemích, na něž se zaměřují hybridní a kybernetické útoky a útoky zahraniční manipulace s informacemi a vměšování, a to na základě specifického know-how a odborných znalostí EU a jejích členských států;

64. zdůrazňuje, že v mezinárodní spolupráci s podobně smýšlejícími partnery, jako jsou G7, NATO, OSN, Organizace pro bezpečnost a spolupráci v Evropě a Rada Evropy, je

důležité přednostně se zaměřit na zásady a cíle Evropského štítu pro demokracii; vítá kroky, které již byly učiněny v rámci dvoustranného a mnohostranného zapojení, zejména Kodex chování OSN pro informační integritu na digitálních platformách, závazek členských států Rady Evropy v Reykjavícké deklaraci chránit volební systémy před zahraničním vměšováním, partnerství v oblasti bezpečnosti a obrany a pokračující úsilí mechanismu rychlé reakce skupiny G7 předvídat a rozvíjet kolektivní reakce na zahraniční manipulace s informacemi a vměšování;

65. vítá vytvoření partnerství v oblasti bezpečnosti a obrany mezi EU a Spojeným královstvím v květnu 2025; vítá jeho zaměření mimo jiné na spolupráci v boji proti kybernetickým problémům, hybridním hrozbám a zahraniční manipulaci s informacemi a vměšování a na ochranu kritické infrastruktury;

Volební systémy a odolnost voličů

66. zdůrazňuje, že hlavním cílem Evropského štítu pro demokracii by mělo být chránit integritu voleb na místní, regionální, celostátní a evropské úrovni; vyzývá Komisi a členské státy, aby při plném dodržování zásady subsidiarity spolupracovaly na provádění reforem zaměřených na posílení odolnosti volebních procesů v Evropě se zvláštním zaměřením na opatření, která mají zabránit zahraničnímu vměšování;

67. 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 sítě, které by vnitrostátním orgánům a odborným subjektům pomáhaly pracovat v součinnosti;

68. 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;

69. domnívá se, že nenávistné kampaně 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 třetích zemí o destabilizaci EU; 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;

70. zdůrazňuje klíčovou úlohu Evropské sítě pro volební spolupráci (ECNE) při zajišťování výměny osvědčených postupů, pokud jde o volební odolnost v EU a jejích členských státech; bere však na vědomí stávající omezení její činnosti; vítá závazek Komise posílit ECNE, včetně reforem, jako je zavedení registru společných referencí a norem pro volební procesy;

71. vyzývá Komisi, aby zvýšila svou úroveň ambicí, pokud jde o reformu ECNE, mimo jiné přezkumem jejích zdrojů a stálých zaměstnanců a dalším rozvíjením společného mechanismu volební odolnosti; zdůrazňuje, že je důležité provádět konkrétní opatření k intenzivnějšímu zapojení kandidátských zemí do činnosti ECNE; 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;

72. vyzývá Komisi, aby do všech zasedání ECNE zapojila Parlament a Úřad pro evropské politické strany a evropské politické nadace (APPF) jako stálé partnery;

73. 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;

74. 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; zdůrazňuje zejména, že je třeba bojovat proti skryté politické komunikaci, včetně neprůhledných struktur financování a skrytých sponzorů, s cílem chránit demokratickou integritu a zajistit transparentnost pro občany;

75. se znepokojením bere na vědomí rostoucí důkazy o zahraničním vměšování a špionáži v evropském politickém systému; vítá vyšetřovací úsilí ve všech členských státech, které vedlo k odsouzení a probíhajícím řízením týkajícím se úplatkářství, špionáže a prosazování zájmů cizích států; zdůrazňuje vážná rizika, která představují nedostatečná bezpečnostní opatření při náboru zaměstnanců a společníků s úzkými vazbami na autoritářské režimy;

76. 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; vyzývá spolunormotvůrce k zajištění jeho účinného a urychleného provedení;

77. konstatuje, že vývoj v oblasti kryptoměn vytváří potenciální zranitelnost jak z hlediska nedostatečné transparentnosti, tak z hlediska možnosti kontrolovat financování politických stran a hnutí v Evropě; oceňuje závazek Komise spojit národní odborníky pod záštitou ECNE a další sítě EU a zúčastněné strany za účelem úzké spolupráce v oblasti výměny osvědčených postupů, přípravy možných pokynů a podpory společných opatření v této souvislosti; vyzývá Komisi, aby nadále sledovala provádění balíčku opatření proti praní peněz a nařízení o trzích s kryptoaktivy a aby se zabývala veškerými případnými mezerami v právních předpisech, které bude případně nutné odstranit;

Úloha sankcí při ochraně demokracie

78. považuje sankce vůči zahraničním subjektům, zemím nebo jednotlivcům, podílejícím se na jednání, jehož záměrem je narušit demokratickou integritu EU nebo jejích členských států, za důležitý prvek cílů Evropského štítu pro demokracii; dále zdůrazňuje, že účinné sankce musí zahrnovat komplexní soubor opatření, včetně zmrazení a konfiskace majetku, přiřazení a odhalení odpovědnosti, zvyšování nákladů a snižování příjmů, zákazů dovozu a vývozu, odepření přístupu a dalších příslušných omezujících opatření;

79. vyzývá Komisi a členské státy, aby pravidelně a pečlivě posuzovaly uložené sankce z hlediska optimální účinnosti a možného dalšího rozšíření, včetně sekundárních sankcí zaměřených na subjekty, které se podílejí na obcházení sankcí; 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 kryptoměny, reklamní sítě a poskytovatelé hostingu, a zároveň by měla narušit ruské zástupné sítě v zemích mimo EU, zejména v Africe a na Blízkém východě, a uvalit sankce na média, logistická centra a skupiny spojené s Wagnerem, které šíří protiunijní narativy; domnívá se, že za účelem dalšího zvýšení nákladů na hybridní agresi by EU měla rozšířit sekundární sankce na firmy ze zemí mimo EU, a zejména na čínské firmy, které 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;

80. domnívá se, že důležitým krokem k uznání problému jasného systematického a mnohostranného vměšování, které v Evropě provádějí země, jako je Rusko nebo Írán, by mohla být identifikace a pojmenovávání zemí původu, nikoliv jednotlivců nebo společností; 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; připomíná, že nové nařízení o boji proti praní peněz poskytne další právní základ pro identifikaci nebezpečných zemí, včetně těch, které se podílejí na šíření zbraní hromadného ničení;

81. zdůrazňuje, že účinnost a důvěryhodnost sankcí EU závisí na jejich přísném a důsledném prosazování; zdůrazňuje, že ohlášená revize mandátu Úřadu evropského veřejného žalobce (EPPO) nabízí příležitost k posílení jeho úlohy tak, aby zahrnovala vyšetřování a stíhání porušení sankcí;

82. odsuzuje politicky motivované používání „černých listin“ ze strany Ruska namířené proti občanům EU, zástupcům státních orgánů a obchodních organizací, novinářům, aktérům občanské společnosti a politickým činitelům, včetně demokraticky zvolených poslanců Evropského parlamentu; požaduje koordinovanější a rozhodnější reakci EU na tato svévolná opatření s cílem zajistit ochranu a bezpečnost osob na černé listině a nabídnout jim solidaritu a nezbytnou podporu; vyjadřuje plnou podporu všem dotčeným osobám;

Připravenost EU

83. 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;

84. požaduje urychlený vývoj a zavedení celounijní interoperabilní aplikace pro varování před krizí, která by občanům během mimořádných událostí poskytovala spolehlivé a vícejazyčné informace v reálném čase; doporučuje, aby byla tato aplikace začleněna do vnitrostátních a unijních systémů včasného varování, byla přístupná zranitelným

skupinám a byla pravidelně aktualizována v souladu s technologickým pokrokem a osvědčenými postupy v oblasti krizového řízení;

85. 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, praktické pokyny pro 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;

86. vyzývá k pořádání pravidelných rozsáhlých cvičení připravenosti koordinovaných na úrovni EU, do nichž by byly zapojeny orgány EU, členské státy, regionální a místní orgány, soukromý sektor a občanská společnost; doporučuje, aby tato cvičení simulovala složité a realistické scénáře, včetně kybernetických útoků, narušení kritické infrastruktury, koordinovaných dezinformací a hybridních krizí, s cílem posoudit schopnosti reakce, zlepšit interoperabilitu mezi úrovněmi správy a podpořit kulturu připravenosti na všech úrovních; za tímto účelem 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;

87. 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;

88. požaduje urychlené zavedení bezpečných komunikačních systémů, jako je IRIS² a evropský kritický komunikační systém; zdůrazňuje, že tyto iniciativy zajišťují odolnost telekomunikací, kontinuitu základních služeb během krizí, snižují vnější závislosti ve strategických odvětvích a posilují kybernetickou bezpečnost těchto infrastruktur;

89. požaduje větší koordinaci mezi orgány, institucemi a jinými subjekty EU, členskými státy a 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 předvídání rizik a posilují kolektivní připravenost a odolnost EU;

90. 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 zranitelná a vystavena hybridním hrozbám;

91. doporučuje, aby rozhodovací orgány EU přezkoumaly a optimalizovaly své strategie a pohotovostní plány v případě otevřeného vojenského konfliktu proti jednomu nebo více členským státům a podobných krizových scénářů; 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; zdůrazňuje, že i bez otevřeného vojenského konfliktu představují hybridní hrozby stále větší riziko pro každodenní fungování EU;

92. 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 Komise (COM/2022/0119); 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 subjekty EU;

93. doporučuje, aby byla přijata další opatření ke zvýšení bezpečnosti a odolnosti Parlamentu vůči zahraničnímu vměšování a jeho připravenosti a schopnosti fungovat během krizí; vyzývá v této souvislosti k větší podpoře poslanců, včetně kontrol IT a bezpečnostních kontrol, školení a zvláštních brífinků před pracovními cestami, a k posílení interdisciplinárního školení a dalších aktivit zaměřených na budování odolnosti, které by spojovaly fyzickou a informační bezpečnost, zabezpečení a kybernetickou bezpečnost; vyzývá k dalšímu cílenému školení zaměstnanců Parlamentu s cílem zabránit manipulaci s informacemi; doporučuje posílit prostředí kybernetické bezpečnosti v souladu s nařízením o kybernetické bezpečnosti a zvýšit jeho provozní vyspělost s cílem dále posílit jeho odolnost v oblasti kybernetické bezpečnosti a zlepšit jeho schopnosti odhalovat hrozby v kontextu dynamického prostředí kybernetických bezpečnostních hrozeb a rychle se měnícího technologického prostředí;

94. v souvislosti s vnitřní bezpečností Parlamentu konstatuje, že používání soukromých mobilních telefonů a dalších zařízení, jako jsou notebooky, poslanci a zaměstnanci pro pracovní účely představuje zranitelnost, která by mohla být zneužita k útoku na Parlament; zdůrazňuje, že poslanci a zaměstnanci by měli být k plnění svých úkolů

vybaveni potřebnými zařízeními IT, jako jsou mobilní telefony a notebooky; vítá v této souvislosti bezpečnostní prověrky nabízené poslancům a zaměstnancům na požádání s cílem odhalit potenciální špionážní software na soukromých zařízeních; vyzývá správu, aby tyto prověrky systematizovala a rozšířila na všechna zařízení používaná pro práci související s Parlamentem; požaduje jasnější pravidla a systematické a vhodné pokyny pro poslance a zaměstnance a ochranná opatření ke zmírnění těchto rizik, zejména během pracovních cest;

95. vyzývá Komisi a ESVČ, aby systematicky zapojovaly Parlament do svých činností a cvičení v oblasti připravenosti, jako je cvičení „EU Integrated Resolve“;

°

° °

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

VYSVĚTLUJÍCÍ PROHLÁŠENÍ

Evropská unie je založena na hodnotách demokracie, právního státu a základních práv, které tvoří základ jejího politického řádu, institucionální legitimity a společenské soudržnosti. V posledních letech se tyto základy stále častěji stávají terčem rychle se stupňujících nepřátelských aktivit. Zahraniční manipulace s informacemi a vměšování, hybridní operace, koordinované dezinformační kampaně a další formy zlomyslného ovlivňování nabývají na rozsahu, sofistikovanosti a dopadu.

Tyto taktiky záměrně využívají společenské rozpory, manipulují veřejnou diskusi a snaží se oslabit důvěru občanů v orgány a demokratické procesy Unie a jejích členských států. Vzhledem k jejich stále více digitální povaze – posílené neprůhlednými online platformami a sítěmi pro přeshraniční šíření – se situace s hrozbami stává složitější a její zvládání pro jednotlivé členské státy obtížnější. V této souvislosti Unie uznala potřebu strategičtější, koordinovanější a předvídavější reakce. V návaznosti na práci svých předchozích zvláštních výborů zabývajících se zahraničním vměšováním do demokratických procesů (INGE a INGE2) se Evropský parlament v prosinci 2024 rozhodl zřídit zvláštní výbor pro Evropský štít pro demokracii (EUDS), jehož úkolem je zkoumat, jak může Unie lépe bránit své demokratické základy.

Významným příspěvkem k tomuto úsilí je společné sdělení o Evropském štítu pro demokracii, které předložila Komise spolu s místopředsedkyní Komise, vysokou představitelkou Unie pro zahraniční věci a bezpečnostní politiku. Poskytuje strukturovaný přehled současného prostředí hrozeb a určuje několik oblastí, v nichž je třeba přijmout další opatření na ochranu Unie před zahraniční manipulací s informacemi a vměšováním a dezinformacemi a na posílení odolnosti společnosti. Zpravodaj tuto iniciativu vítá a je si vědom její přidané hodnoty při upevňování porozumění Unie budoucím výzvám.

I když sdělení udává správný směr, úroveň jeho ambicí zůstává vzhledem k rozsahu hrozeb příliš omezená. Je zapotřebí nejen rámec pro reflexi, ale také konkrétní program reforem schopný zajistit operační kapacitu, odpovědnost a dlouhodobou připravenost.

Unie vytváří rostoucí ekosystém struktur, nástrojů a programů zaměřených na boj proti zahraniční manipulaci s informacemi a dezinformacím. Toto úsilí – včetně práce příslušných pracovních skupin, sítí spolupráce a mechanismů včasného varování – je významné. Aby se tato práce posunula na další úroveň, je však nutné provést i reformy. Návrh na zřízení Evropského střediska pro odolnost demokracie je vítanou a slibnou iniciativou. Ve formě uvedené ve sdělení však tato iniciativa postrádá nezbytnou operační jasnost, bez níž se středisko nemůže stát efektivním centrem odborných znalostí a činnosti. V návrhu zprávy byla předložena konkrétní doporučení pro dosažení tohoto cíle.

Pokud jde o digitální sféru, kterou v mnoha ohledech využívají nepřátelské subjekty ze třetích zemí k provádění svých operací, se zpravodaj domnívá, že je třeba dodržovat příslušné právní předpisy EU a že Komise musí zintenzivnit svá donucovací opatření, zejména v případech, kdy existují náznaky manipulace související s volbami, systémové algoritmické neprůhlednosti, koordinovaného neautentického chování nebo rozsáhlého zneužívání funkcí platforem.

Vyvíjející se prostředí hrozeb rovněž vyžaduje, aby členské státy efektivněji spolupracovaly na úrovni Unie při konání voleb. Integrita volebních procesů je jádrem demokratické

odolnosti. V této souvislosti návrh zprávy zdůrazňuje, že je třeba výrazně posílit Evropskou síť pro volební spolupráci, a vybízí ke komplexní reformě, která by tuto síť učinila ambicióznější a operativně relevantnější. Infrastruktura související s volbami by navíc měla být uznána za součást kritické infrastruktury Unie a odpovídajícím způsobem chráněna.

Zpravodaj rovněž vítá, že společné sdělení o Evropském štítu pro demokracii zahrnuje vnější rozměr. Cílů štítu pro demokracii nelze dosáhnout bez úzké spolupráce s partnery v sousedství Unie, zejména s kandidátskými zeměmi, které jsou stále více vystaveny intenzivnímu zahraničnímu vměšování. Podpora jejich odolnosti – mimo jiné prostřednictvím budování kapacit, školení a poskytování odborných znalostí – je nezbytná pro ochranu širšího demokratického prostoru Evropy. Návrh zprávy vyzývá ESVČ, aby do mandátů misí a operací SBOP systematicky začleňovala opatření v oblasti připravenosti na hybridní hrozby, a posílila tak schopnost protějšků v členských státech odhalovat nepřátelské ovlivňování a bojovat proti němu. V rámci vnějšího rozměru štítu by měl být rovněž proveden přezkum příslušných sankčních nástrojů, aby se zajistilo, že budou optimálně nastaveny tak, aby se zaměřovaly na aktéry narušující demokratickou integritu Evropy. Spojení s podobně smýšlejícími partnery je důležité i pro zajištění účinných kolektivních reakcí; zpravodaj vítá využívání mnohostranných a dvoustranných kanálů spolupráce, včetně stávajících partnerství EU v oblasti bezpečnosti a obrany.

V návrhu zprávy se dále zdůrazňuje potřeba ambiciózního programu pro zvýšení odolnosti společnosti. Důležitou součástí jsou reformy na podporu mediálního odvětví spolu s opatřeními na posílení mediální gramotnosti. Dalším klíčovým aspektem je občanská společnost a strategie EU pro občanskou společnost: silná a nezávislá občanská společnost je pro demokratickou odolnost nezbytná. Zpravodaj se zasazuje o to, aby v příštím víceletém finančním rámci na období 2028–2034 byly podpořeny spolehlivé programy k provádění politických priorit uvedených v iniciativě Evropský štít pro demokracii.

Posilování společenské odolnosti vyžaduje také lepší ochranu kritické infrastruktury, která by měla být přehodnocena s ohledem na cíle Štítu pro demokracii. To následně vyžaduje reformy, které zvýší evropskou suverenitu v oblasti digitální infrastruktury, operačních systémů, datových center, polovodičů, umělé inteligence, kybernetické bezpečnosti, cloud computingu a různých digitálních platforem a služeb. Revize mandátů příslušných agentur EU, jako je Europol a Frontex, může rovněž hrát významnou úlohu při zlepšování odolnosti a ochrany před hybridními hrozbami.

V neposlední řadě návrh zprávy zdůrazňuje, že předpokladem budování demokratické odolnosti je také to, aby společnosti byly schopny dále fungovat i za mimořádných nebo rušivých podmínek. Nedílnou součástí Evropského štítu pro demokracii proto musí být reformy zaměřené na posílení připravenosti – od kapacit krizového řízení až po kontinuitu demokratických institucí. Závěrem návrhu zprávy je, že ochrana a posilování evropských demokratických systémů vyžaduje nejen ostražitost a odolnost na všech úrovních společnosti, ale také koordinovanou a prozíravou strategii Unie podpořenou dostatečnými zdroji a politickým závazkem.

PŘÍLOHA: ZVEŘEJŇOVÁNÍ PODNĚTŮ

Zpravodaj v souladu s článkem 8 přílohy I jednacího řádu prohlašuje, že do své zprávy zahrnul podněty k záležitostem týkajícím se předmětu spisu, které při vypracovávání návrhu zprávy obdržel od zástupců zájmových skupin spadajících do oblasti působnosti interinstitucionální dohody o povinném rejstříku[1] transparentnosti nebo představitelů orgánů třetích zemí, včetně jejich diplomatických misí a velvyslanectví:

1. Zástupci zájmových skupin spadající do oblasti působnosti interinstitucionální dohody o povinném rejstříku transparentnosti
European Partnership for Democracy
EU DisinfoLab
Schibsted ASA
European Confederation of Police
Reporters sans frontières
TikTok Technology Ltd
Europe MédiaLab
Psychological Defence Research Institute
Civil Society Europe (CSE)
European Fact-Checking Standards Network
Stiftung Mercator
The Foundation for European Progressive Studies (FEPS)
Konrad Adenauer Foundation
Association of Commercial Television in Europe (ACT)
European Association for Local Democracy (ALDA)
Martens Center
2. Představitelé orgánů třetích zemí, včetně jejich diplomatických misí a velvyslanectví
n.a.

Výše uvedený seznam je sestaven na výhradní odpovědnost zpravodaje.

Pokud jsou na seznamu uvedena jména, funkce, případně jména i funkce fyzických osob, zpravodaj prohlašuje, že příslušné fyzické osoby byly seznámeny s prohlášením Evropského parlamentu o ochraně osobních údajů č. 484 (https://www.europarl.europa.eu/data-protect/index.do), které stanoví podmínky platné pro zpracování jejich osobních údajů a práva související s tímto zpracováním.

[1] Interinstitucionální dohoda z května 2021 mezi Evropským parlamentem, Radou Evropské unie a Evropskou komisí o povinném rejstříku transparentnosti (Úř. věst. L 207, 11.6.2021, s. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2021/611/oj).