Parlamento europeo
2024-2029

Commissione speciale sullo scudo europeo per la democrazia

2025/2069(INI)

18.12.2025

PROGETTO DI RELAZIONE

sulle conclusioni e raccomandazioni della commissione speciale sullo scudo europeo per la democrazia
(2025/2069(INI))

Commissione speciale sullo scudo europeo per la democrazia

Relatore: Tomas Tobé

INDICE

Pagina

PROPOSTA DI RISOLUZIONE DEL PARLAMENTO EUROPEO 3

MOTIVAZIONE.....41

ALLEGATO: DICHIARAZIONE DEI CONTRIBUTI.....44

PROPOSTA DI RISOLUZIONE DEL PARLAMENTO EUROPEO

sulle conclusioni e raccomandazioni della commissione speciale sullo scudo europeo per la democrazia

(2025/2069(INI))

Il Parlamento europeo,

– vista la sua decisione, del 18 dicembre 2024, sulla costituzione, le attribuzioni, la composizione numerica e la durata del mandato della commissione speciale sullo scudo europeo per la democrazia[1],

– vista la comunicazione congiunta della Commissione europea e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 12 novembre 2025, dal titolo: "Scudo europeo per la democrazia a puntello di democrazie solide e resilienti" (JOIN(2025)0791),

– visto il trattato sull'Unione europea (TUE), in particolare l'articolo 2 sui valori fondanti dell'UE, l'articolo 10 sulla vita democratica e l'articolo 21 sull'azione esterna,

– visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114 sul mercato interno e l'articolo 222 sulla solidarietà,

– vista la Carta dei diritti fondamentali dell'Unione europea,

– visto il regolamento (UE, Euratom) n. 2025/2445 del Parlamento europeo e del Consiglio del 26 novembre 2025, relativo allo statuto e al finanziamento dei partiti politici europei e delle fondazioni politiche europee[2],

– visto il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)[3],

– visto il regolamento (UE) 2024/1624 del Parlamento europeo e del Consiglio, del 31 maggio 2024, relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo[4],

– visto il regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla

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

libertà dei media)[5],

– vista la direttiva (UE) 2024/1069 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, sulla protezione delle persone attive nella partecipazione pubblica da domande manifestamente infondate o procedimenti giudiziari abusivi ("azioni legali strategiche tese a bloccare la partecipazione pubblica")[6],

– visto il regolamento (UE) 2024/900 del Parlamento europeo e del Consiglio, del 13 marzo 2024, relativo alla trasparenza e al targeting della pubblicità politica[7],

– visto il regolamento (UE, Euratom) 2023/2841 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione[8],

– visto il regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937[9] (regolamento sui mercati delle cripto-attività),

– vista la direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio[10],

– vista la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)[11],

– visti il regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)[12] e il regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali)[13],

– visto il regolamento (UE) 2021/692 del Parlamento europeo e del Consiglio, del 28 aprile 2021, che istituisce il programma Cittadini, uguaglianza, diritti e valori e abroga il regolamento (UE) n. 1381/2013 del Parlamento europeo e del Consiglio e il regolamento (UE) n. 390/2014 del Consiglio[14],

---

[5] GU L, 2024/1083, 17.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1083/oj.
[6] GU L, 2024/1069, 16.4.2024, ELI: http://data.europa.eu/eli/dir/2024/1069/oj.
[7] GU L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj.
[8] GU L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj.
[9] GU L 150 del 9.6.2023, pag. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.
[10] GU L 333 del 27.12.2022, pag. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj.
[11] GU L 333 del 27.12.2022, pag. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.
[12] GU L 277 del 27.10.2022, pag. 1, ELI: http://data.europa.eu/eli/reg/2022/2065/oj.
[13] GU L 265 del 12.10.2022, pag. 1, ELI: http://data.europa.eu/eli/reg/2022/1925/oj.
[14] GU L 156 del 5.5.2021, pag. 1, ELI: http://data.europa.eu/eli/reg/2021/692/oj.

– vista la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione[15],

– vista la direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi)[16],

– visti la decisione 2014/145/PESC del Consiglio concernente misure restrittive relative ad azioni che compromettono o minacciano l'integrità territoriale, la sovranità e l'indipendenza dell'Ucraina[17] e il regolamento (UE) n. 269/2014, del 17 marzo 2014, concernente misure restrittive relative ad azioni che compromettono o minacciano l'integrità territoriale, la sovranità e l'indipendenza dell'Ucraina[18],

– visti la decisione 2014/119/PESC del Consiglio, del 5 marzo 2014, concernente misure restrittive nei confronti di determinate persone, entità e organismi in considerazione della situazione in Ucraina[19] e il regolamento (UE) n. 208/2014, del 5 marzo 2014, concernente misure restrittive nei confronti di determinate persone, entità e organismi in considerazione della situazione in Ucraina[20],

– visti la decisione 2014/512/PESC del Consiglio, del 31 luglio 2014, concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina[21] e il regolamento (UE) n. 833/2014 del Consiglio, del 31 luglio 2014, concernente misure restrittive in considerazione delle azioni della Russia che destabilizzano la situazione in Ucraina[22],

– visti la decisione (PESC) 2022/266 del Consiglio, del 23 febbraio 2022, concernente misure restrittive in risposta al riconoscimento delle zone non controllate dal governo delle regioni ucraine di Donetsk e Luhansk dell'Ucraina e la conseguente decisione di inviare truppe russe in tali zone[23] e il regolamento (UE) 2022/263 del Consiglio, del 23 febbraio 2022, concernente misure restrittive in risposta al riconoscimento delle zone delle oblast di Donetsk e Luhansk dell'Ucraina non controllate dal governo e all'invio di forze armate russe in tali zone[24],

– visti la decisione 2012/642/PESC del Consiglio, del 15 ottobre 2012, relativa a misure restrittive nei confronti della Bielorussia[25] e il regolamento (CE) n. 765/2006 del

---

[15] GU L 305 del 26.11.2019, pag. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj.
[16] GU L 95 del 15.4.2010, pag. 1, ELI: http://data.europa.eu/eli/dir/2010/13/oj.
[17] GU L 78 del 17.3.2014, pag. 16, ELI: http://data.europa.eu/eli/dec/2014/145(1)/oj.
[18] GU L 78 del 17.3.2014, pag. 6, ELI: http://data.europa.eu/eli/reg/2014/269/oj.
[19] GU L 66 del 6.3.2014, pag. 26, ELI: http://data.europa.eu/eli/dec/2014/119(1)/oj.
[20] GU L 66 del 6.3.2014, pag. 1, ELI: http://data.europa.eu/eli/reg/2014/208/oj.
[21] GU L 229 del 31.7.2014, pag. 13, ELI: http://data.europa.eu/eli/dec/2014/512/oj.
[22] GU L 229 del 31.7.2014, pag. 1, ELI: http://data.europa.eu/eli/reg/2014/833/oj.
[23] GU L 42 I del 23.2.2022, pag. 109, ELI: http://data.europa.eu/eli/dec/2022/266/oj.
[24] GU L 42 I del 23.2.2022, pag. 77, ELI: http://data.europa.eu/eli/reg/2022/263/oj.
[25] GU L 285 del 17.10.2012, pag. 1, ELI: http://data.europa.eu/eli/dec/2012/642/oj.

Consiglio, del 18 maggio 2006, concernente misure restrittive nei confronti del presidente Lukashenko e di determinati funzionari della Bielorussia[26],

– visti la decisione (PESC) 2023/1532 del Consiglio, del 20 luglio 2023, concernente misure restrittive in considerazione del sostegno militare dell'Iran alla guerra di aggressione della Russia nei confronti dell'Ucraina[27] e il regolamento (UE) 2023/1529 del Consiglio, del 20 luglio 2023, concernente misure restrittive in considerazione del sostegno militare dell'Iran alla guerra di aggressione della Russia nei confronti dell'Ucraina[28],

– visti la decisione (PESC) 2024/1603 del Consiglio, del 31 maggio 2024, che modifica la decisione (PESC) 2016/849 relativa a misure restrittive nei confronti della Repubblica popolare democratica di Corea[29] e il regolamento di esecuzione (UE) 2024/1602 del Consiglio, del 31 maggio 2024, che attua il regolamento (UE) 2017/1509 relativo a misure restrittive nei confronti della Repubblica popolare democratica di Corea[30],

– vista la proposta di regolamento del Consiglio che stabilisce il quadro finanziario pluriennale per il periodo 2028-2034, presentata dalla Commissione il 16 luglio 2025 (COM(2025)0571),

– viste le modifiche adottate dal Parlamento europeo il 27 novembre 2025 relative alla proposta di una direttiva del Parlamento europeo e del Consiglio che stabilisce requisiti armonizzati nel mercato interno sulla trasparenza della rappresentanza d'interessi esercitata per conto di paesi terzi e che modifica la direttiva (UE) 2019/1937 (COM(2023)0637 – C9-0464/2023 – 2023/0463(COD))[31],

– vista la sua risoluzione del 9 ottobre 2025 su una risposta congiunta alle recenti violazioni dello spazio aereo e delle infrastrutture critiche degli Stati membri dell'UE da parte della Russia[32],

– vista la sua risoluzione del 18 giugno 2025 sulla relazione sullo Stato di diritto 2024 della Commissione[33],

– vista la sua risoluzione del 7 maggio 2025 su un rinnovato bilancio a lungo termine per l'Unione in un mondo che cambia[34],

– vista la sua risoluzione del 13 luglio 2023 sulle raccomandazioni per una riforma delle norme del Parlamento europeo in materia di trasparenza, integrità, responsabilità e lotta alla corruzione[35],

---

[26] GU L 134 del 20.5.2006, pag. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj.
[27] GU L 186 del 25.7.2023, pag. 20, ELI: http://data.europa.eu/eli/dec/2023/1532/oj.
[28] GU L 186 del 25.7.2023, pag. 1, ELI: http://data.europa.eu/eli/reg/2023/1529/oj.
[29] GU L, 2024/1603, 31.5.2024, ELI: http://data.europa.eu/eli/dec/2024/1603/oj.
[30] GU L, 2024/1602, 31.5.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/1602/oj.
[31] Testi approvati, P10_TA(2025)0306.
[32] Testi approvati, P10_TA(2025)0230.
[33] GU C, C/2025/6259, 19.12.2025, ELI: http://data.europa.eu/eli/C/2025/6259/oj.
[34] Testi approvati, P10_TA(2025)0090.
[35] GU C, C/2024/4011, 17.7.2024, ELI: http://data.europa.eu/eli/C/2024/4011/oj.

– vista la sua risoluzione del 1° giugno 2023 sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione[36],

– vista la sua risoluzione del 15 dicembre 2022 sulla sospetta corruzione da parte del Qatar e, più in generale, sulla necessità di trasparenza e responsabilità nelle istituzioni europee[37],

– vista la sua risoluzione del 23 novembre 2022 sul riconoscimento della Federazione russa come Stato sostenitore del terrorismo[38],

– vista la sua risoluzione del 9 marzo 2022 sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, inclusa la disinformazione[39],

– vista la sua risoluzione dell'8 marzo 2022 sulla riduzione degli spazi per la società civile in Europa[40],

– vista la sua risoluzione del 20 ottobre 2021 sui media europei nel decennio digitale: un piano d'azione per sostenere la ripresa e la trasformazione[41],

– vista la sua risoluzione del 23 novembre 2016 sulla comunicazione strategica dell'UE per contrastare la propaganda nei suoi confronti da parte di terzi[42],

– vista la sua raccomandazione del 15 giugno 2023 destinata al Consiglio e alla Commissione in seguito all'esame delle denunce di infrazione e di cattiva amministrazione nell'applicazione del diritto dell'Unione in relazione all'uso di Pegasus e di spyware di sorveglianza equivalenti[43],

– vista la sua raccomandazione del 23 novembre 2022 sulla raccomandazione del Parlamento europeo al Consiglio, alla Commissione e al vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza concernente la nuova strategia dell'UE in materia di allargamento[44],

– vista la sua raccomandazione al Consiglio e alla vicepresidente della Commissione/alta rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 13 marzo 2019, sul bilancio del seguito dato dal SEAE a due anni dalla relazione del Parlamento europeo sulla comunicazione strategica dell'UE per contrastare la propaganda nei suoi confronti da parte di terzi[45],

– visto il seguito dato dalla Commissione alle raccomandazioni formulate dal Parlamento europeo nelle sue risoluzioni,

---

[36] GU C, C/2023/1226, 21.12.2023, ELI: http://data.europa.eu/eli/C/2023/1226/oj.
[37] GU C 177 del 17.5.2023, pag. 109.
[38] GU C 167 dell'11.5.2023, pag. 18.
[39] GU C 347 del 9.9.2022, pag. 61.
[40] GU C 347 del 9.9.2022, pag. 2.
[41] GU C 184 del 5.5.2022, pag. 71.
[42] GU C 224 del 27.6.2018, pag. 58.
[43] GU C, C/2024/494, 23.1.2024, ELI: http://data.europa.eu/eli/C/2024/494/oj.
[44] GU C 167 dell'11.5.2023, pag. 105.
[45] GU C 23 del 21.1.2021, pag. 152.

– vista la comunicazione della Commissione del 12 novembre 2025 dal titolo "Strategia dell'UE per la società civile" (COM(2025)0790),

– vista la comunicazione della Commissione del 1° aprile 2025 su ProtectEU: strategia europea di sicurezza interna (COM(2025)0148),

– vista la comunicazione della Commissione del 24 luglio 2024, dal titolo "Relazione sullo Stato di diritto 2024 – La situazione dello Stato di diritto nell'Unione europea" (COM(2024)0800),

– vista la comunicazione della Commissione dell'8 luglio 2025, dal titolo "Relazione sullo Stato di diritto 2025 – La situazione dello Stato di diritto nell'Unione europea" (COM(2025)0900),

– vista la comunicazione della Commissione del 12 dicembre 2023 dal titolo "Difesa della democrazia" (COM(2023)0630),

– vista la comunicazione della Commissione del 3 dicembre 2020 sul piano d'azione per la democrazia europea (COM(2020)0790),

– viste le comunicazioni congiunte della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 5 dicembre 2018, dal titolo "Piano d'azione contro la disinformazione" (JOIN(2018)0036) e del 14 giugno 2019 dal titolo "Relazione sull'attuazione del piano d'azione contro la disinformazione" (JOIN(2019)0012),

– visto il partenariato in materia di sicurezza e difesa tra l'Unione europea e il Regno Unito di Gran Bretagna e Irlanda del Nord, adottato il 19 maggio 2025,

– visti gli orientamenti politici per la legislatura 2024-2029 della Commissione, presentati dalla presidente della Commissione Ursula von der Leyen il 18 luglio 2024, dal titolo "La scelta dell'Europa",

– vista la decisione di esecuzione della Commissione, del 28 marzo 2025, relativa al finanziamento del programma Europa digitale e all'adozione del programma di lavoro pluriennale 2025-2027 (C(2025)1839),

– visto il codice di condotta sulla disinformazione,

– vista la relazione del gruppo di cooperazione in materia di reti e sistemi informativi del 23 gennaio 2020 dal titolo "Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures" (Cibersicurezza delle reti 5G – Pacchetto di strumenti dell'UE per misure di attenuazione dei rischi),

– vista la relazione del 30 ottobre 2024 di Sauli Niinistö, ex presidente della Repubblica di Finlandia, in qualità di consigliere speciale della presidente della Commissione europea, dal titolo "Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness" (Più sicuri insieme – Rafforzare la preparazione e la prontezza civili e militari dell'Europa),

– vista la raccomandazione (UE) 2023/2829 della Commissione, del 12 dicembre 2023, relativa a processi elettorali inclusivi e resilienti nell'Unione e al rafforzamento della natura europea e dell'efficienza nello svolgimento delle elezioni del Parlamento europeo[46],

– vista la raccomandazione (UE) 2023/2836 della Commissione, del 12 dicembre 2023, sulla promozione del coinvolgimento e della partecipazione effettiva dei cittadini e delle organizzazioni della società civile ai processi di elaborazione delle politiche pubbliche[47],

– vista l'istituzione da parte della Commissione, nel 2019, della rete europea di cooperazione in materia elettorale (ECNE),

– visto il comunicato stampa della Commissione del 13 novembre 2025 relativo all'avvio di un'indagine su una potenziale violazione della legge sui mercati digitali da parte di Google nella retrocessione dei contenuti degli editori di media nei risultati di ricerca,

– viste le conclusioni del Consiglio del 21 maggio 2024 sul futuro della cibersicurezza: attuare e proteggere insieme,

– viste le conclusioni del Consiglio del 17 ottobre 2022 sulla sicurezza della catena di approvvigionamento delle TIC,

– vista la raccomandazione del Consiglio dell'8 dicembre 2022 su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche[48],

– vista la decisione (PESC) 2023/855 del Consiglio del 24 aprile 2023, relativa a una missione di partenariato dell'Unione europea in Moldova (EUPM Moldova)[49],

– visto il piano d'azione dal titolo "Una bussola strategica per la sicurezza e la difesa – Per un'Unione europea che protegge i suoi cittadini, i suoi valori e i suoi interessi e contribuisce alla pace e alla sicurezza internazionali", approvato dal Consiglio il 21 marzo 2022 e dal Consiglio europeo il 25 marzo 2022,

– viste le informazioni fornite da Lituania, Danimarca, Estonia, Finlandia, Germania, Lettonia, Slovenia e Spagna in vista della riunione del Consiglio "Trasporti, telecomunicazioni e energia" del 6 giugno 2025, che chiede azioni comuni in risposta alle minacce di interferenza e falsificazione nei sistemi globali di navigazione satellitare (GNSS),

– visto l'accordo interistituzionale del 20 maggio 2021 tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea su un registro per la trasparenza obbligatorio[50],

---

[46] GU L, 2023/2829, 20.12.2023, ELI: http://data.europa.eu/eli/reco/2023/2829/oj.
[47] GU L, 2023/2836, 20.12.2023, ELI: http://data.europa.eu/eli/reco/2023/2836/oj.
[48] GU C 20 del 20.1.2023, pag. 1.
[49] GU L 110 del 25.4.2023, pag. 30, ELI: http://data.europa.eu/eli/dec/2023/855/oj.
[50] GU L 207 dell'11.6.2021, pag. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2021/611/oj.

– vista la relazione speciale n. 05/2022 della Corte dei conti europea del 29 marzo 2022 dal titolo "Cibersicurezza delle istituzioni, degli organi e delle agenzie dell'UE: il livello complessivo di preparazione non è commisurato alle minacce",

– visti i principi globali delle Nazioni Unite per l'integrità delle informazioni – Raccomandazioni per un'azione multilaterale, pubblicati il 24 giugno 2024,

– visto il Patto internazionale relativo ai diritti civili e politici, in particolare l'articolo 20,

– vista la convenzione delle Nazioni Unite sul diritto del mare del 10 dicembre 1982, entrata in vigore il 16 novembre 1994,

– visti gli articoli sulla responsabilità degli Stati per atti illeciti internazionali, adottati nel novembre 2001,

– vista la dichiarazione di Reykjavik, adottata in occasione del 4° vertice dei capi di Stato e di governo del Consiglio d'Europa, tenutosi dal 16 al 17 maggio 2023,

– visto il meccanismo di risposta rapida del G7, istituito in occasione del vertice del G7 a Charlevoix, tenutosi dall'8 al 9 giugno 2018,

– visto il documento di lavoro presentato il 13 giugno 2025 all'Organizzazione per l'aviazione civile internazionale da Estonia, Finlandia, Lettonia, Lituania, Polonia e Svezia sulle ricorrenti interferenze in radiofrequenza sui GNSS nelle regioni del Baltico, dell'Europa orientale e settentrionale e sulle loro implicazioni per la sicurezza dell'aviazione civile internazionale,

– vista la relazione sull'esito finale della Conferenza sul futuro dell'Europa, pubblicata il 9 maggio 2022, in particolare le sue proposte 27 e 37,

– visto lo studio richiesto dalla commissione speciale sullo scudo europeo per la democrazia del Parlamento dal titolo "Strengthening Resilience – Towards the European Democracy Shield" (Rafforzare la resilienza: verso lo scudo europeo per la democrazia), pubblicato dalla sua direzione generale dei diritti dei cittadini, della giustizia e degli affari istituzionali nell'ottobre 2025[51],

– viste la prima, la seconda e la terza relazione del servizio europeo per l'azione esterna (SEAE) sulla manipolazione delle informazioni e le minacce di interferenza da parte di attori stranieri,

– vista la relazione dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) del 1° ottobre 2025 dal titolo "ENISA Threat Landscape 2025" (ENISA: panorama delle minacce 2025),

– vista la relazione di Europol dal titolo "EU Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime" (Valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità

[51] Studio dal titolo "Strengthening Resilience – Towards the European Democracy Shield" (Rafforzare la resilienza: verso lo scudo europeo per la democrazia), Parlamento europeo, direzione generale dei Diritti dei cittadini, della giustizia e degli affari istituzionali, dipartimento tematico Giustizia, libertà civili e affari istituzionali, ottobre 2025.

nell'UE – Il DNA in evoluzione della criminalità organizzata e delle forme gravi di criminalità), pubblicata nel 2025,

– vista la relazione del dipartimento per il coordinamento della sorveglianza algoritmica dell'autorità olandese per la protezione dei dati, dell'ottobre 2025, dal titolo "AI chatbots as voting aid" (I chatbot di IA come aiuto al voto),

– viste le misure adottate dall'autorità italiana per le garanzie nelle comunicazioni (AGCOM) il 3 settembre 2025 in merito agli influencer,

– visto il codice di condotta per la pubblicità degli influencer, adottato da AUTOCONTROL in Spagna il 7 luglio 2025,

– visto l'avviso emesso il 3 settembre 2025 dall'agenzia nazionale per la sicurezza informatica e dell'informazione (NÚKIB) della Repubblica ceca in merito alle minacce alla cibersicurezza associate al trasferimento di dati verso la Repubblica popolare cinese e le sue regioni amministrative speciali e alla loro amministrazione a distanza,

– vista la relazione dal titolo "Manipulation d'algorithmes et instrumentalisation d'influenceurs: enseignements de l'élection présidentielle en Roumanie & risques pour la France", pubblicata dal servizio di vigilanza e protezione contro le ingerenze digitali straniere (VIGINUM) del governo francese nel febbraio 2025,

– visto l'Influencer Handbook, prodotto dalla finlandese Mediapooli nel 2020,

– vista la relazione del dipartimento di Stato degli Stati Uniti dell'agosto 2020 dal titolo "Pillars of Russia's Disinformation and Propaganda Ecosystem" (Pilastri dell'ecosistema russo di disinformazione e propaganda),

– visto l'avviso congiunto sulla cibersicurezza dell'Agenzia statunitense per la sicurezza informatica e delle infrastrutture, dell'Agenzia per la sicurezza nazionale statunitense, dell'FBI e dei partner internazionali pubblicato nell'agosto 2025 e dal titolo "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems" (Contrastare il compromesso tra gli attori cinesi sponsorizzati dallo Stato e le reti mondiali che alimentano i sistemi di spionaggio globali),

– vista la relazione di Reporter senza frontiere del 25 settembre 2025 dal titolo "The Propaganda Monitor: The Russian Edition" (Osservatorio della propaganda: edizione russa),

– visto l'articolo pubblicato dal Centro per il pluralismo e la libertà dei media in occasione dell'articolo pubblicato dallo stesso Centro presso l'Istituto universitario europeo il 1° novembre 2025 dal titolo "Influencers as news creators: implications for media regulation" (Influencer come creatori di notizie: implicazioni per la regolamentazione dei mezzi di comunicazione),

– visto l'articolo pubblicato dal consorzio AlgoSoc il 28 ottobre 2025 dal titolo "1 in 10 Dutch citizens are likely to ask AI for election advice. This is why they shouldn't" (1 cittadino olandese su 10 potrebbe chiedere consiglio elettorale all'IA. Ecco perché non dovrebbe),

– vista la relazione di What to Fix del giugno 2025 dal titolo "Bankrolling Sanctioned Entities: How Meta Platforms Ireland Ltd. May Have Violated EU Sanctions and Channeled Money To RT, Sputnik and Other EU-Sanctioned Entities via Facebook's Revenue Redistribution Programs" (Finanziamento delle entità sanzionate: in che modo Meta Platforms Ireland Ltd. potrebbe aver violato le sanzioni dell'UE e incanalato denaro verso RT, Sputnik e altre entità sanzionate dall'UE attraverso i programmi di ridistribuzione delle entrate di Facebook"),

– vista la relazione speciale di NewsGuard del 6 marzo 2025 dal titolo "A Well-funded Moscow-based Global "News" Network has Infected Western Artificial Intelligence with Russian Propaganda" (Una rete globale di notizie ben finanziata e con sede a Mosca ha contaminato l'intelligenza artificiale occidentale con la propaganda russa),

– vista la relazione di Media Freedom Rapid Response dal titolo "Mapping Media Freedom – Monitoring Report 2024" (Mappatura della libertà dei media: relazione di monitoraggio 2024), pubblicata nel febbraio 2025,

– vista la relazione del Forum economico mondiale del gennaio 2025 dal titolo "Global Cybersecurity Outlook 2025" (Prospettive globali sulla cibersicurezza 2025),

– vista la relazione investigativa pubblicata da VSquare, Delfi Estonia e dalle organizzazioni dei media partner il 26 febbraio 2024 dal titolo "Kremlin Leaks: Secret Files Reveal How Putin Pre-Rigged his Reelection" (Kremlin Leaks: file segreti rivelano come Putin si è avvalso di elezioni truccate per la sua rielezione),

– visto il codice di condotta etico per gli influencer dei social media e i creatori di contenuti, pubblicato dall'Aspen Institute Germany nel 2024,

– visto l'articolo pubblicato da Debunk.org il 4 maggio 2023 dal titolo "Kremlin spent 1.9 billion USD on propaganda last year, the budget exceeded by a quarter" (Lo scorso anno il Cremlino ha speso 1,9 miliardi di USD in propaganda, bilancio superato di un quarto),

– vista la dichiarazione del ministero degli Affari esteri della Federazione russa, del 28 dicembre 2024, sulle misure in risposta al 15° pacchetto di sanzioni dell'UE nei confronti della Russia, in cui ha annunciato l'ampliamento dell'elenco dei funzionari e dei cittadini dell'UE cui è vietato l'ingresso nel paese,

– visto l'articolo dell'agenzia di stampa russa TASS del 28 dicembre 2024 dal titolo "Russia substantially expands blacklist of EU officials in response to sanctions – MFA" (La Russia amplia in modo sostanziale la lista nera dei funzionari dell'UE in risposta alle sanzioni – AMF),

– vista la dichiarazione di TikTok del dicembre 2024 sul continuare a proteggere l'integrità di TikTok durante le elezioni rumene,

– vista la dichiarazione rilasciata dal Consiglio europeo per la produzione solare il 30 aprile 2025 dal titolo "Restrict Remote Access of PV Inverters from High-Risk Vendors" (Limitare l'accesso remoto degli inverter fotovoltaici da fornitori ad alto rischio), che mette in guardia dai rischi per la sovranità energetica dell'Europa derivanti dalle capacità non regolamentate e di controllo remoto degli inverter fotovoltaici di produttori non europei ad alto rischio,

– visto l'articolo 55 del suo regolamento,

– vista la relazione della commissione speciale sullo scudo europeo per la democrazia (A10-0000/2025),

A. considerando che il 12 novembre 2025 la Commissione e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato una comunicazione congiunta sull'istituzione dello scudo europeo per la democrazia, che definisce una serie di misure per responsabilizzare, proteggere e promuovere democrazie forti e resilienti in tutta l'UE;

B. considerando che il Centro europeo per la resilienza democratica costituisce il fulcro dello scudo europeo per la democrazia; che entrambe le commissioni speciali del Parlamento sulle ingerenze straniere in tutti i processi democratici nell'Unione europea, compresa la disinformazione (INGE e INGE 2), avevano già chiesto l'istituzione di una struttura dell'UE volta a contrastare la manipolazione delle informazioni e le ingerenze da parte di attori stranieri (FIMI);

C. considerando che le recenti relazioni del SEAE sulle minacce relative alla manipolazione delle informazioni e le ingerenze da parte di attori stranieri dimostrano una comprensione sempre più granulare delle metodologie degli attori malevoli, delle infrastrutture tecniche e delle narrazioni previste, ma che tale consapevolezza situazionale non si è tradotta in meccanismi operativi sostenuti che consentano all'UE di adottare contromisure tempestive e coordinate; che il nesso istituzionale dell'UE è al centro di campagne ostili di manipolazione delle informazioni; che l'UE risente di un approccio frammentato al contrasto alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri, con notevoli variazioni nelle capacità degli Stati membri e senza un quadro strategico generale che colleghi la risposta operativa all'analisi delle minacce;

D. considerando che l'ECNE, il sistema di allarme rapido (RAS) e l'Osservatorio europeo dei media digitali (EDMO) sono componenti preziose della resilienza complessiva dell'UE alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri, ma la loro efficacia è sostanzialmente limitata dall'assenza di una struttura operativa specifica dell'UE dotata dell'autorità di coordinare le attività di sviluppo della resilienza e i meccanismi di risposta rapida e di escalation che colleghino le capacità operative nazionali al coordinamento a livello dell'UE;

E. considerando che le minacce poste dalla manipolazione delle informazioni e dalle ingerenze da parte di attori stranieri si estendono oltre i singoli Stati membri, fino a rappresentare un attacco all'essenza stessa del progetto europeo; che le operazioni di manipolazione delle informazioni e le ingerenze da parte di attori stranieri mirano sistematicamente ai valori democratici fondamentali di cui all'articolo 2 TUE e al principio di processi decisionali aperti e trasparenti sancito dall'articolo 1 TUE, in modo da ledere gli interessi dell'UE;

F. considerando che i singoli Stati membri che hanno investito in strutture operative dedicate, con statuti e mandati chiari, nonché finanziamenti e personale sufficienti, dimostrano ciò che è realizzabile, in particolare nei casi del VIGINUM francese e dell'Agenzia svedese per la difesa psicologica;

G. considerando che il rapido progresso dell'intelligenza artificiale (IA) e delle tecnologie deepfake sta superando la capacità di adattamento di istituzioni nazionali frammentate; che, in assenza di risposte coordinate dell'UE e di chiare capacità operative, il vantaggio tecnologico favorirà sempre più gli aggressori rispetto ai difensori;

H. considerando che la concomitanza delle prime fasi di attuazione del regolamento sui servizi digitali (DSA), del regolamenti sui mercati digitali (DMA), del regolamento sull'intelligenza artificiale (regolamento sull'IA) e del regolamento europeo sulla libertà dei media (EMFA) costituisce una finestra di opportunità per costruire difese globali contro la manipolazione delle informazioni e le ingerenze da parte di attori stranieri;

I. considerando che le società democratiche nell'UE sono sempre più prese di mira dalle minacce ibride, dalla disinformazione e dalla manipolazione delle informazioni e dalle ingerenze da parte di attori stranieri, con una particolare intensità nella sfera digitale; che lo spazio online consente la proliferazione di nuove tecniche di manipolazione, tra cui: a) l'uso non autentico dei social media attraverso programmi software automatizzati, falsi account sui social media e l'uso di troll farm, l'amplificazione e l'engagement basati su bot, b) l'uso di tecniche di astroturfing e flooding per influenzare il dibattito pubblico online, c) la personalizzazione, il tracciamento e il microtargeting degli individui, d) siti web progettati per imitare le fonti ufficiali, e) l'amplificazione artificiale di contenuti divisivi, f) l'uso di contenuti sintetici, come i deepfake e altri contenuti generati dall'IA e g) sistemi di raccomandazione appositamente progettati per indirizzare l'engagement attraverso la polarizzazione;

J. considerando che le piattaforme online, al momento di decidere se promuovere o meno contenuti nel feed di un utente, utilizzano le loro conoscenze sulle preferenze e le vulnerabilità di ogni singolo utente, il che le rende più influenti degli editori tradizionali;

K. considerando che l'UE ha recentemente adottato una serie di atti legislativi globali per istituire uno spazio online sicuro e trasparente, tra cui il regolamento sui servizi digitali, il regolamento sulla trasparenza e il targeting della pubblicità politica e il regolamento sull'IA; che tali atti legislativi rappresentano un passo avanti importante nel responsabilizzare le piattaforme digitali e proteggere i processi democratici, aumentando la trasparenza e tutelando la libertà di espressione; che, allo stesso tempo, la loro adozione rimane una sfida;

L. considerando che l'uso dell'IA presenta nuove opportunità per rafforzare la gestione e il controllo delle elezioni, ad esempio individuando attività online insolite e comportamenti manipolativi coordinati; che l'uso dell'IA, compresi i modelli generativi e i deepfake, presenta altresì sfide significative per l'integrità delle informazioni e i processi elettorali; che relazioni credibili hanno messo in luce le operazioni di una rete di disinformazione con sede a Mosca nota come "Pravda", che ha deliberatamente preso di mira e si è infiltrata in modelli linguistici di grandi dimensioni con narrazioni pro-Cremlino progettate per imitare risultati neutri e basati sui fatti; che tali tattiche rappresentano una pericolosa evoluzione della manipolazione delle informazioni e delle ingerenze da parte di attori stranieri, in quanto sfruttano l'opacità e la scalabilità dei sistemi di IA per diffondere sottilmente messaggi geopolitici falsi o fuorvianti con il pretesto di un linguaggio autorevole; che tale forma di manipolazione algoritmica minaccia di erodere la fiducia del pubblico nelle tecnologie di IA, distorcere il discorso

democratico ed esacerbare i rischi di disinformazione in tutta l'UE e a livello globale; che ciò sottolinea la necessità di rafforzare l'alfabetizzazione in materia di IA nell'istruzione, nel lavoro e nella società in generale;

M. considerando che gli influencer online possono svolgere un ruolo importante nel rafforzare la resilienza digitale delle nostre società, nel sensibilizzare in merito all'alfabetizzazione mediatica e alle procedure democratiche o nel contribuire a un sano dibattito politico;

N. considerando che le elezioni presidenziali dell'autunno 2024 in Romania hanno messo in luce vulnerabilità significative nell'ambiente dell'informazione online, con relazioni credibili che indicano l'uso diffuso di account falsi, bot e contenuti amplificati algoritmicamente per promuovere narrazioni politiche specifiche; che TikTok, una delle piattaforme più utilizzate dai giovani elettori, ha affermato di aver bloccato la creazione di oltre 116 000 account di spam e di aver rimosso 59 000 account falsi in una pulizia post-elettorale; che l'uso di influencer, compresi i nano e i micro influencer, da parte di attori stranieri evidenzia ulteriormente il fatto che gli influencer a basso costo e a bassa visibilità possono essere utilizzati come arma per eludere l'individuazione e influenzare l'opinione pubblica, in violazione delle norme democratiche;

O. considerando che Telegram, una piattaforma di messaggistica con una crescente base di utenti nell'UE, è sempre più di frequente segnalata come canale di disinformazione, ingerenze straniere e attività illecite, compresa la diffusione di contenuti estremisti e propaganda politica non rintracciabile; che le sue origini russe e la mancanza di una significativa moderazione dei contenuti hanno sollevato persistenti preoccupazioni in merito al suo ruolo nel minare il discorso democratico; che Telegram è divenuto un canale primario per l'assunzione di "agenti monouso" e la conduzione di operazioni ibride; che è stato riscontrato come attori statali malintenzionati sfruttino le competenze tecnologiche, le esigenze finanziarie e l'ingenuità degli utenti di Telegram, in particolare i giovani, per condurre operazioni di spionaggio e sabotaggio a costi minimi, mantenendo nel contempo una negabilità plausibile; che le relazioni suggeriscono che Telegram raggiunge la soglia di utenza per essere classificata come piattaforma online di dimensioni molto grandi (VLOP) a norma del regolamento sui servizi digitali, il che la rende soggetta a obblighi normativi e requisiti di attenuazione dei rischi più rigorosi;

P. considerando che la crescente influenza delle imprese tecnologiche non europee, in particolare quelle con sede negli Stati Uniti e in Cina, ha messo in evidenza le dipendenze strategiche dell'UE in settori critici quali l'infrastruttura dei dati, i servizi cloud e le piattaforme di social media; che la promozione dell'innovazione locale, il sostegno alle start-up europee e gli investimenti nelle infrastrutture digitali sovrane sono passi essenziali verso la costruzione di un ecosistema digitale dell'UE competitivo, sicuro e resiliente; che l'allineamento dell'innovazione digitale ai valori democratici e ai diritti fondamentali offre all'UE l'opportunità di diventare un leader mondiale nella tecnologia responsabile e incentrata sull'uomo;

Q. considerando che le ricerche indicano una tendenza preoccupante nei programmi di ridistribuzione delle entrate delle piattaforme online, rivelando che i media soggetti a sanzioni, come Sputnik e Russia Today, erano ancora elencati tra gli "editori partner" su Facebook mesi dopo l'introduzione delle sanzioni dell'UE nei confronti della Russia, sollevando dubbi sul fatto che abbiano continuato a beneficiare finanziariamente; che

tali meccanismi di monetizzazione opachi consentono agli attori stranieri affiliati allo Stato di trarre profitto dalla condivisione della disinformazione e continuano a destabilizzare gli spazi di informazione dell'UE nonostante le misure normative;

R. considerando che, in un'indagine svolta in vista delle elezioni parlamentari del 2025 nei Paesi Bassi, 1 intervistato su 10 ha dichiarato che probabilmente chiederà consigli di voto all'IA e un altro 13 % ha dichiarato che farà buon uso di tali consigli; che nei Paesi Bassi il rapporto combinato per gli elettori più giovani è superiore a un terzo degli elettori; che tale tendenza è coerente con i risultati in tutti gli Stati membri e a livello mondiale; che un recente studio dell'autorità olandese per la protezione dei dati dimostra che le raccomandazioni di voto generate dai chatbot IA presentano spesso una visione altamente distorta e polarizzata del panorama politico;

S. considerando che il diritto fondamentale alla libertà di espressione e di informazione, sancito dall'articolo 11 della Carta dei diritti fondamentali dell'Unione europea e dall'articolo 10 della Convenzione europea dei diritti dell'uomo, è un fondamento della democrazia; che l'impegno dell'UE a favore della libertà di espressione rappresenta una strategia di contrasto alle manipolazioni delle informazioni e alle ingerenze da parte di attori stranieri coerente e basata su principi, in netto contrasto con le restrizioni che i contesti autoritari impongono sistematicamente alle loro popolazioni; che la libertà e il pluralismo dei media e l'esistenza di uno spazio civico dinamico consentono alle società di individuare, esporre e respingere le narrazioni manipolative attraverso la deliberazione democratica;

T. considerando che la libertà di espressione e di informazione è un diritto fondamentale pensato per proteggere le persone, non le macchine, i bot e l'IA;

U. considerando che gli autori delle manipolazioni delle informazioni e delle ingerenze da parte di attori stranieri sfruttano le tecnologie per orchestrare campagne di disinformazione non autentiche coordinate; che tali tecnologie, in particolare i bot e i programmi software basati sull'IA, sono in grado di mostrare un comportamento autonomo e successivamente distorcono e distruggono il discorso pubblico autentico, inviando a grande velocità contenuti non autentici in espressioni di persone reali;

V. considerando che la libertà e il pluralismo dei media sono pietre angolari dello stile di vita europeo, sanciti dall'articolo 11, paragrafo 2, della Carta dei diritti fondamentali dell'Unione europea; che il giornalismo editoriale indipendente e di alta qualità è un potente antidoto alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri;

W. considerando che, a norma del regolamento sui mercati digitali, gli sviluppatori di app che distribuiscono le loro app tramite gli app store dovrebbero essere in grado di informare gratuitamente i clienti in merito a offerte alternative al di fuori dell'app store; che la Commissione ha avviato un'indagine su una potenziale violazione del regolamento sui mercati digitali da parte di Google nella retrocessione dei contenuti degli editori di media nei risultati di ricerca; che la Commissione ha avviato il suo primo riesame del regolamento sui mercati digitali il 3 luglio 2025;

X. considerando che la direttiva sui servizi di media audiovisivi impone agli Stati membri di adottare misure per sviluppare le competenze in materia di alfabetizzazione mediatica e di riferire ogni tre anni in merito ai loro sforzi;

Y. considerando che Media Freedom Rapid Response nel 2024 ha documentato 1 548 violazioni della libertà di stampa, da minacce legali, fisiche e psicologiche a forme di censura, nei confronti di 2 567 persone o entità legate ai media in 35 paesi europei, un aumento allarmante rispetto alle 1 153 violazioni registrate nel 2023;

Z. considerando che l'11 dicembre 2025 i negoziatori del Parlamento e del Consiglio hanno raggiunto un accordo provvisorio sulla proposta di regolamento relativo al controllo degli investimenti esteri nell'Unione;

AA. considerando che il lavoro di Radio Free Europe/Radio Liberty (RFE/RL) è di interesse strategico per l'UE; che l'UE ha approvato un finanziamento di emergenza di 5,5 milioni di EUR per questo lavoro, all'indomani della riforma della politica di aiuti esteri degli Stati Uniti; che occorre sviluppare una soluzione di finanziamento sostenibile per RFE/RL;

AB. considerando che le nuove tecnologie, come l'IA, possono migliorare le condizioni e i metodi di lavoro dei giornalisti, ma possono altresì esporli a nuove minacce, come l'impersonificazione rapida ed economica dei media esistenti, la creazione di massa di organi di disinformazione e gli attacchi coordinati contro i giornalisti;

AC. considerando che la guerra di aggressione russa in corso contro l'Ucraina illustra il ruolo fondamentale che la società civile svolge quando le comunità si trovano in situazioni di crisi, in particolare quando si tratta di fornire aiuti umanitari, garantire i bisogni di base e garantire il proseguimento della vita quotidiana delle popolazioni colpite;

AD. considerando che la società civile svolge anche un ruolo essenziale nel contribuire all'elaborazione delle politiche, nell'erogazione di servizi sociali e comunitari, nella sensibilizzazione su importanti questioni sociali, nella rappresentanza di diversi gruppi in situazioni di vulnerabilità e nella promozione e tutela dei diritti fondamentali dei cittadini;

AE. considerando che la Commissione ha pubblicato la strategia dell'UE per la società civile, che integrerebbe le azioni definite nella comunicazione congiunta sullo scudo europeo per la democrazia; che la strategia dell'UE per la società civile conferma che la piattaforma della società civile, annunciata dalla Commissione nell'ambito dell'attuazione della strategia, mirerà a fornire un quadro regolare e strutturato per la protezione e la promozione dei valori dell'UE e la razionalizzazione e il rafforzamento dell'impegno in materia di diritti fondamentali, democrazia, uguaglianza e Stato di diritto, e diventerà operativa nel 2026; che la strategia prevede anche la creazione di un polo di conoscenze online sullo spazio civico, che dovrebbe documentare le iniziative, le relazioni e le risorse di protezione esistenti in materia di monitoraggio dello spazio civico, a livello nazionale, europeo e internazionale, in cooperazione con l'Agenzia dell'Unione europea per i diritti fondamentali;

AF. considerando che il programma AgoraEU, proposto dalla Commissione per il quadro finanziario pluriennale (QFP) 2028-2034, costituisce un importante passo avanti nel rafforzamento del sostegno dell'UE alla cultura, ai media e alla società civile, con un bilancio previsto di 9 miliardi di EUR;

AG. considerando che gli attacchi ibridi contro le infrastrutture critiche nell'Unione europea sono diventati estremamente frequenti, con incidenti legati agli stessi attori malevoli

quali la Russia, la Cina, ma anche l'Iran e la Corea del Nord; che tali attacchi spesso prendono di mira sistemi, reti e strutture essenziali che sono vitali per il funzionamento di una società, tra cui la sicurezza pubblica, l'incolumità pubblica e la stabilità economica; che tali attacchi assumono varie forme, come il sabotaggio fisico, gli attacchi incendiari, lo spionaggio e il blocco dei segnali, nonché gli attacchi informatici e altre attività nelle zone grigie, che dimostrano uno sforzo coordinato per testare, perturbare e minare la sicurezza e la resilienza della società dell'UE;

AH. considerando che il Mar Baltico ha registrato un inedito aumento nel numero di perturbazioni dei cavi sottomarini, vitali per la connettività di Internet e l'alimentazione elettrica in tutta la regione baltica e nordica; che dal 2023 sono stati registrati almeno 11 episodi di danni ai cavi, il che suggerisce un sabotaggio coordinato;

AI. considerando che negli ultimi mesi sono state segnalate molteplici violazioni dello spazio aereo e incursioni non autorizzate di droni in diversi Stati membri dell'UE e nei vicini alleati della NATO, tra cui Polonia, Stati baltici, Romania, Danimarca, Svezia, Germania, Belgio e Norvegia; che alcuni di questi incidenti sono stati chiaramente attribuiti ad aeromobili e droni militari russi, mentre altri, che coinvolgono oggetti aerei non identificati, restano oggetto di inchiesta, per quanto si sospetti ampiamente che condividano lo stesso modello di intimidazione e destabilizzazione ibrida diretta contro l'Europa;

AJ. considerando che diversi paesi europei, tra cui Francia, Estonia, Germania, Repubblica ceca e Norvegia, hanno recentemente subito gravi attacchi informatici diretti contro i sistemi governativi, le infrastrutture critiche e le imprese private attribuiti ai servizi di intelligence militare russi e agli attori cinesi legati allo Stato, i quali sottolineano l'urgente necessità di rafforzare le capacità collettive di ciberresilienza e di attribuzione informatica dell'UE;

AK. considerando che la dipendenza dell'UE dagli attori stranieri e dalle tecnologie di produzione estera nelle infrastrutture critiche e nelle catene di approvvigionamento continua a destare grande preoccupazione ed è una delle vulnerabilità più significative dell'UE; che questa situazione è particolarmente diffusa nei settori tecnologico e digitale, il che rappresenta una sfida fondamentale per la cibersicurezza;

AL. considerando che gli strumenti di diritto penale possono contribuire allo scudo europeo per la democrazia nella misura in cui le attività in questione costituiscono reati;

AM. considerando che i meccanismi di cooperazione giudiziaria e di polizia e gli strumenti per lo scambio transfrontaliero di informazioni devono essere adeguati e rafforzati, alla luce delle crescenti sfide poste dalle ingerenze straniere alla sicurezza interna dell'UE;

AN. considerando che l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) ha messo in guardia, nella sua ultima relazione dell'UE sulla valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità (EU-SOCTA), pubblicata nel marzo 2025, sul coinvolgimento delle organizzazioni criminali in campagne ibride; che la comunicazione della Commissione su ProtectEU riconosce che vari fattori impediscono a Europol di raggiungere pienamente il suo potenziale operativo nel sostenere le attività di lotta alla criminalità transfrontaliera, comprese le lacune nel mandato dell'Agenzia circa le nuove minacce

alla sicurezza, in particolare il sabotaggio, le minacce ibride e la manipolazione delle informazioni;

AO. considerando che la Commissione si è impegnata ad avviare una riforma che renderà Europol un'agenzia di polizia realmente operativa; che gli agenti di polizia sono partner fondamentali nella salvaguardia delle istituzioni democratiche; che ciò dovrebbe essere riconosciuto più chiaramente nelle politiche pertinenti;

AP. considerando che gli Stati membri possono chiedere all'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) di assistere le autorità nazionali nella gestione di qualsiasi tipo di condotta illegale soggetta alla loro giurisdizione; che la cooperazione giudiziaria può rivelarsi particolarmente difficile quando si estende a nuovi settori in materia penale, il che richiede un pacchetto di strumenti giuridici modernizzato;

AQ. considerando che le agenzie dell'UE aventi responsabilità nel settore della gestione delle frontiere, della migrazione e dell'asilo, ossia l'Agenzia europea della guardia di frontiera e costiera (Frontex) e l'Agenzia dell'Unione europea per l'asilo, hanno un altro ruolo fondamentale da svolgere, in cooperazione con le autorità nazionali, nel creare e mantenere una conoscenza situazionale comune sui rischi connessi allo sfruttamento dei flussi migratori a fini politici e nell'assistere gli Stati membri in prima linea in situazioni di crisi; che la Commissione ha incluso il rafforzamento di Frontex nelle sue iniziative faro per la legislatura 2024-2029;

AR. considerando che i paesi candidati e i vicini dell'UE, in particolare l'Ucraina, la Moldova e i Balcani occidentali, rimangono fortemente colpiti dalla manipolazione delle informazioni e ingerenze da parte di attori stranieri nonché dalle minacce ibride e richiedono il sostegno dell'UE per sviluppare la resilienza civica e istituzionale;

AS. considerando che la guerra di aggressione della Russia contro l'Ucraina e la postura geopolitica assertiva della Cina hanno intensificato il ricorso alla disinformazione, alla coercizione economica e all'influenza strategica, prendendo di mira non solo l'UE, ma anche regioni vulnerabili come i Balcani occidentali, i paesi partner orientali e il Sud del mondo; che varie fonti rivelano che il bilancio della Russia per la diffusione della disinformazione e della propaganda è compreso tra 1 e 2 miliardi di USD all'anno; che le elezioni e gli eventi politici in tutta Europa dimostrano una guerra ibrida offensiva su vasta scala persistente, mirata e sofisticata perpetrata dalla Russia, volta a destabilizzare la fiducia nei nostri sistemi politici e nelle nostre istituzioni e a creare una confusione costante tra fatti e informazioni false; che tale guerra richiede una risposta adeguata e il passaggio da una mera strategia difensiva a una strategia offensiva;

AT. considerando che la missione di partenariato dell'UE nella Repubblica di Moldova (EUPM Moldova) è stata istituita il 24 aprile 2023 con l'esplicito scopo di sostenere le autorità moldove nella lotta contro la manipolazione delle informazioni e le ingerenze da parte di attori stranieri;

AU. considerando che la riduzione del sostegno degli Stati Uniti alla democrazia internazionale ha creato un notevole divario globale nei finanziamenti per contrastare la disinformazione e l'influenza autoritaria;

AV. considerando che le iniziative internazionali, comprese quelle delle Nazioni Unite, dell'Organizzazione per la cooperazione e lo sviluppo economici e del G7, hanno iniziato a delineare principi e quadri per la salvaguardia dell'integrità dell'informazione, ancorati ai valori democratici, al pluralismo dei media e ai diritti umani;

AW. considerando che la manipolazione delle informazioni e ingerenze da parte di attori stranieri costituiscono una sfida crescente per la resilienza democratica dell'UE; che alcune forme di attività di informazione manipolativa possono essere perpetrate anche da attori che operano all'interno dell'UE; che il fenomeno della manipolazione delle informazioni e delle ingerenze nel contesto nazionale dovrebbe essere ulteriormente esaminato e compreso, in particolare nella sua interazione con la manipolazione delle informazioni e ingerenze da parte di attori stranieri; che le misure presentate per combattere la manipolazione delle informazioni e le ingerenze da parte di attori stranieri contribuiscono anche ad aumentare la resilienza complessiva delle società nel contesto nazionale, in particolare per quanto riguarda il miglioramento della consapevolezza situazionale, l'aumento della trasparenza e del pluralismo e il rafforzamento dei livelli di alfabetizzazione mediatica e digitale in tutte le fasce d'età;

AX. considerando che le raccomandazioni della Commissione sui processi elettorali inclusivi e resilienti nell'Unione, pubblicate nel dicembre 2023, devono ancora essere pienamente attuate in tutti gli Stati membri, comprese le disposizioni volte a rafforzare la cooperazione tra le autorità nazionali durante e prima dei processi elettorali attraverso la creazione di reti elettorali nazionali;

AY. considerando che negli ultimi anni l'ECNE ha svolto un ruolo di crescente importanza ma attualmente non dispone delle risorse e delle capacità necessarie per elevare le sue attività al livello successivo;

AZ. considerando che i paesi candidati sono stati invitati a partecipare alle riunioni dell'ECNE; che, oltre a tale partecipazione, esiste ancora un potenziale significativo per rafforzare ulteriormente la cooperazione con tali paesi nel contesto delle attività della rete, per trarre insegnamenti dalle reciproche esperienze in caso di minacce e per scambiare le migliori prassi nella lotta alle minacce di questo tipo;

BA. considerando che vi è una chiara necessità di rafforzare la protezione dell'infrastruttura elettorale e dei partiti politici nazionali, anch'essi oggetto di attacchi informatici, non da ultimo alla luce degli attacchi informatici su larga scala contro le autorità elettorali rumene nell'autunno 2024;

BB. considerando che il finanziamento occulto dei partiti e dei movimenti politici nell'UE da parte di paesi terzi rappresenta una minaccia per la legittimità del processo democratico;

BC. considerando che l'indipendenza della magistratura è una componente strutturale indispensabile dell'integrità elettorale; che l'integrità elettorale dipende dall'esistenza di misure correttive accessibili ed efficaci contro le violazioni dei diritti di voto e delle procedure elettorali, isolati dalle pressioni politiche ed esecutive;

BD. considerando che, tra il 2022 e il 2025, l'UE ha imposto un totale di 19 pacchetti di sanzioni, estese e senza precedenti, in risposta all'aggressione militare della Russia nei confronti dell'Ucraina, aumentando in modo sostanziale la pressione sull'economia di guerra russa, prendendo di mira settori chiave come l'energia, la finanza e il settore della

difesa, le zone economiche speciali, i facilitatori e gli speculatori della sua guerra di aggressione, ponendo fine alla dipendenza dell'UE dalle importazioni di combustibili fossili dalla Russia; che l'UE ha adottato inoltre sanzioni nei confronti di Bielorussia, Iran e Corea del Nord in risposta al loro sostegno alla Russia nell'aggressione militare nei confronti dell'Ucraina;

BE. considerando che, dall'8 ottobre 2024, il quadro sanzionatorio dell'UE ha consentito di prendere di mira un'ampia gamma di attività ibride svolte dalla Russia, tra cui l'indebolimento dei processi elettorali e del funzionamento delle istituzioni democratiche, le minacce e il sabotaggio delle attività economiche, i servizi di interesse pubblico e le infrastrutture critiche, l'uso della disinformazione coordinata e della manipolazione delle informazioni e ingerenze da parte di attori stranieri, le attività informatiche dolose, la strumentalizzazione dei migranti e altre attività destabilizzanti; che tale quadro ha già portato a sanzionare decine di individui ed entità, tra cui oligarchi, propagandisti, agenti dell'intelligence militare, organi di informazione e società russi, per aver diffuso narrazioni pro-Cremlino, condotto sabotaggi e compromesso i processi democratici; che le misure correlate consentono ora all'UE di includere il congelamento dei beni, i divieti di viaggio e la sospensione delle licenze di radiodiffusione e di vietare le transazioni finanziarie e di cripto-attività legate ad attività ibride;

BF. considerando che il 28 dicembre 2024 il governo russo ha annunciato di aver "ampliato in modo significativo" la sua lista nera di cittadini e funzionari dell'UE, compresi i rappresentanti delle istituzioni dell'UE, dei governi nazionali, delle agenzie di contrasto e delle organizzazioni commerciali; che tale lista nera, rivolta a coloro che promuovono i valori democratici e si oppongono all'aggressione russa in Ucraina, cerca di intimidire e mettere a tacere le voci attraverso restrizioni opache e arbitrarie, spesso senza alcuna notifica formale, giustificazione o diritto di ricorso;

BG. considerando che le minacce ibride, le ingerenze straniere e le campagne di disinformazione si sono trasformate in crisi complesse, su vasta scala e intersettoriali con effetti negativi sulla sicurezza, sul benessere dei cittadini e sul funzionamento della società e dell'economia nel suo complesso, costituendo una sfida fondamentale per gli affari interni dell'UE e destabilizzando le istituzioni democratiche in tutti gli Stati membri, come si è visto durante l'aggressione russa nei confronti dell'Ucraina;

BH. considerando che un livello elevato di preparazione civile e in materia di difesa richiede un approccio globale, esteso a tutta la società, a tutta l'amministrazione e a tutti i rischi, che integri le autorità nazionali degli Stati membri con le istituzioni, gli organi e gli organismi dell'UE, nonché le imprese, il mondo accademico, la società civile e i singoli cittadini; che tale sforzo deve essere accompagnato da investimenti a lungo termine, previsione strategica e integrazione della resilienza nell'elaborazione delle politiche, nello sviluppo delle infrastrutture, nei sistemi di istruzione e nelle catene di approvvigionamento;

BI. considerando che l'emancipazione dei cittadini è fondamentale per la resilienza della società e che la preparazione deve includere strumenti pratici quali un'app di allerta in caso di crisi a livello dell'UE, un opuscolo sulla preparazione delle famiglie e campagne di sensibilizzazione di ampia portata che promuovano l'autosufficienza e la prontezza in caso di crisi;

BJ. considerando che la cooperazione civile-militare, le capacità a duplice uso e l'integrazione della preparazione nei programmi educativi sono essenziali per migliorare la preparazione alla difesa attraverso una formazione mirata non solo per i lavoratori in settori critici, come i vigili del fuoco, gli operatori sanitari e i funzionari pubblici, ma anche per gli attori della società civile e il pubblico in generale;

BK. considerando che la sovranità tecnologica e la sicurezza degli ecosistemi digitali, compresi progetti come IRIS^2 e il sistema europeo di comunicazione critica, sono fondamentali per mantenere il controllo sui canali di comunicazione essenziali e rafforzare le infrastrutture critiche;

BL. considerando che la preparazione dipende da una costante cooperazione tra le istituzioni, le agenzie, gli Stati membri e i partner internazionali dell'UE, sostenuta da esercitazioni e formazione congiunte, piattaforme condivise di conoscenza situazionale e da un rapido scambio di informazioni;

BM. considerando che lo sviluppo di una resilienza credibile e il conseguimento di un livello sufficiente di preparazione civile e di difesa richiedono ingenti investimenti, la promozione della base tecnologica e industriale dell'Europa e la riduzione delle dipendenze strategiche; che tale sforzo richiede l'esplorazione di nuovi meccanismi di finanziamento mirati;

Introduzione

1. accoglie con favore la comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza sull'istituzione di uno scudo europeo per la democrazia e i continui sforzi per sviluppare il lavoro già intrapreso nell'ambito del piano d'azione per la democrazia europea e del pacchetto per la difesa della democrazia; è del parere che la missione principale dello scudo europeo per la democrazia dovrebbe essere quella di proteggere la democrazia europea dalle minacce esterne e, in ultima analisi, contribuire a salvaguardare lo stile di vita europeo, lo Stato di diritto e i valori sanciti dall'articolo 2 TUE;

2. prende atto con preoccupazione del panorama di minacce, sempre più complesso e in evoluzione, cui devono far fronte l'UE e i suoi Stati membri, caratterizzato da manipolazione delle informazioni e ingerenze da parte di attori stranieri, attacchi ibridi e campagne di disinformazione condotte da attori malintenzionati di paesi terzi; sottolinea che si tratta di azioni ostili che compromettono le fondamenta democratiche dell'UE fomentando la divisione, diminuendo la fiducia dei cittadini nelle istituzioni e sfruttando le vulnerabilità della società, spesso attraverso tecnologie digitali avanzate;

3. ritiene che la Russia sia la principale minaccia esterna all'integrità democratica dell'Europa; ribadisce che la Russia è uno Stato sostenitore del terrorismo; sottolinea l'urgente necessità di una strategia globale, coerente e lungimirante per affrontare efficacemente tali sfide e salvaguardare la democrazia europea;

4. ribadisce la propria convinzione che le principali priorità politiche delineate nell'iniziativa relativa allo scudo europeo per la democrazia, tra cui la lotta contro la manipolazione delle informazioni e le ingerenze da parte di attori stranieri e le minacce ibride, il rafforzamento della resilienza elettorale, il rafforzamento della cibersicurezza, il sostegno alla società civile e la promozione del giornalismo indipendente e

investigativo, debbano essere saldamente integrate e sufficientemente finanziate nell'ambito del prossimo QFP;

Centro europeo per la resilienza democratica

5. accoglie con favore la proposta della Commissione relativa a un centro europeo per la resilienza democratica (il Centro) quale passo necessario e logico verso un maggiore coordinamento degli sforzi per resistere all'evoluzione delle minacce comuni, in particolare la manipolazione delle informazioni e le ingerenze da parte di attori stranieri e la disinformazione; prende atto del suo approccio di introduzione graduale di funzioni e operazioni, che prevede anche un graduale aumento della partecipazione degli Stati membri; accoglie con favore l'assicurazione della Commissione che sta già lavorando alla creazione del Centro sotto la guida del commissario per la Democrazia, la giustizia, lo Stato di diritto e la protezione dei consumatori, con l'obiettivo esplicito di garantirne l'operatività nel corso del 2026; accoglie con favore l'impegno della Commissione ad aggiornare e coinvolgere regolarmente il Parlamento nel processo di attuazione dello scudo europeo per la democrazia e del Centro;

6. ricorda tuttavia che la proposta manca di dettagli operativi sufficienti, di stanziamenti di bilancio chiari, di una struttura di governance specifica, di un mandato concreto e di un calendario; osserva che la comunicazione congiunta sullo scudo europeo per la democrazia non collega esplicitamente il Centro ad alcuna delle azioni ivi delineate, che restano in diversi quadri amministrativi all'interno della Commissione e del SEAE; esprime preoccupazione per il fatto che, se il Centro si configurasse solo come un altro polo, una rete, una piattaforma o un quadro, potrebbe ridurre ulteriormente la capacità dell'UE di utilizzare in modo efficiente l'intera gamma di strumenti attualmente disponibili e aggravare le carenze individuate nella comunicazione congiunta, tra cui la ridotta reattività, la frammentazione e l'insufficienza dei bilanci;

7. accoglie con favore il fatto che la comunicazione congiunta fornisca un'ampia mappatura dei quadri, delle strutture, degli strumenti, delle iniziative e dei programmi esistenti in materia di lotta alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri e di disinformazione e resilienza, nonché un elenco delle azioni che la Commissione e il SEAE si sono impegnati a intraprendere; invita la Commissione e il SEAE a proporre un calendario chiaro per la loro graduale introduzione e integrazione all'interno del Centro, fissando al 2026 il termine ultimo per tale integrazione; chiede che tale integrazione includa i pertinenti meccanismi di supervisione e applicazione del regolamento sui servizi digitali, in particolare al fine di individuare e ridurre al minimo il rischio sistemico, coordinare gli sforzi per contrastare le campagne di manipolazione delle informazioni, garantire la responsabilità operativa di un sistema di allarme rapido (RAS) rafforzato e la manutenzione e il funzionamento di una banca dati unificata di intelligence in materia di manipolazione delle informazioni e ingerenze da parte di attori stranieri, nonché sviluppare, tra l'altro, la risorsa EUvsDisinfo, l'ECNE e la task force della Commissione sulla disinformazione e la comunicazione strategica;

8. accoglie con favore il riconoscimento da parte della Commissione della necessità di impegnarsi con gli Stati membri e il Parlamento sul mandato, la struttura e i metodi di lavoro del Centro e invita la Commissione ad avviare il processo proponendo, entro il primo trimestre del 2027, una base giuridica per l'istituzione del Centro come entità

dell'UE con uno statuto e un posizionamento istituzionali chiari, una struttura di governance e meccanismi di controllo parlamentare; sottolinea che la chiarezza istituzionale è essenziale per consentire al Centro di agire con decisione pur rimanendo responsabile;

9. invita la Commissione a dotare il Centro di un mandato e di meccanismi decisionali chiari, che gli consentano di funzionare come centro indipendente di eccellenza per l'individuazione e l'analisi delle operazioni di manipolazione delle informazioni e ingerenze da parte di attori stranieri e di disinformazione, come piattaforma di sviluppo delle capacità che stabilisce definizioni, norme, formazione e strumenti tecnici comuni in tutta l'UE nonché come spina dorsale operativa in grado di coordinare in tempo reale il sostegno tecnico per contrastare le campagne attive di manipolazione delle informazioni;

10. invita la Commissione a garantire che al Centro sia affidata la responsabilità di salvaguardare l'integrità dei processi democratici a livello dell'UE; ribadisce che le strutture operative degli Stati membri costituiscono una prima linea di difesa; sottolinea, tuttavia, che la loro responsabilità primaria non esaurisce gli interessi legittimi dell'UE in termini di lotta alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri; invita la Commissione a chiarire che il Centro deve perseguire due obiettivi che si rafforzano reciprocamente, vale a dire coordinare le attività degli Stati membri in questo settore e rafforzare la loro capacità operativa, nonché tutelare gli interessi democratici dell'UE;

11. invita gli Stati membri che non dispongono di strutture operative dedicate a istituire o rafforzare in modo sostanziale istituzioni nazionali dedicate alla rilevazione e alla risposta alla manipolazione delle informazioni e ingerenze da parte di attori stranieri e alla disinformazione, con il sostegno del Centro; invita la Commissione a stabilire una tabella di marcia per lo sviluppo delle capacità degli Stati membri;

12. invita la Commissione a valutare se è fattibile conferire al Centro il potere di amministrare e assegnare sovvenzioni specifiche dell'UE nell'ambito dei pertinenti programmi dell'Unione, tra cui il programma Europa digitale, il meccanismo per collegare l'Europa, Orizzonte Europa, il programma Cittadini, uguaglianza, diritti e valori (CERV) e il programma AgoraEU proposto, e ad autorizzarlo a pubblicare inviti a presentare proposte e a selezionare, supervisionare e valutare progetti nei settori che rientrano nel suo mandato, in particolare l'EDMO, le iniziative di alfabetizzazione mediatica e altre iniziative europee, regionali e transfrontaliere pertinenti, dedicate alla lotta contro la manipolazione delle informazioni e le ingerenze da parte di attori stranieri, al rafforzamento della resilienza democratica e alla promozione dell'integrità delle informazioni;

13. invita la Commissione a prevedere un'apposita linea di bilancio dell'UE per le operazioni del Centro, con una chiara separazione tra i finanziamenti operativi e i costi generali di coordinamento; invita la Commissione a garantire risorse umane sufficienti e finanziamenti ponte dai bilanci esistenti per consentire i lavori preparatori prima del QFP 2028-2034;

14. invita la Commissione a valutare la fattibilità dell'istituzione di un meccanismo di finanziamento a integrazione della linea di bilancio specifica per le operazioni del

Centro, sulla base dei contributi delle piattaforme online di dimensioni molto grandi; ricorda che il settore bancario finanzia meccanismi di risoluzione bancaria, le aziende farmaceutiche sostengono il monitoraggio della sicurezza e i settori inquinanti sostengono i costi ambientali; chiede un meccanismo in base al quale le piattaforme di social media contribuiscano in modo proporzionale all'infrastruttura necessaria per contrastare le influenze esterne negative e i rischi sistemici connessi ai loro servizi, sia per quanto riguarda la manipolazione delle informazioni e le ingerenze da parte di attori stranieri e la disinformazione che per rafforzare la resilienza; sottolinea che tali contributi non solo risulterebbero in linea con i principi europei consolidati di responsabilità e rendicontabilità, ma garantirebbero anche la condivisione dei costi relativi alla protezione del discorso democratico tra coloro che traggono i maggiori profitti dall'ecosistema dell'informazione digitale;

Resilienza digitale

15. chiede la piena attuazione della legislazione chiave nello spazio digitale, ad esempio il regolamento sui servizi digitali, il regolamento sulla trasparenza e il targeting della pubblicità politica e il regolamento sull'IA, in tutti gli Stati membri; ritiene che il proseguimento dell'attuazione della legislazione digitale dovrebbe concentrarsi maggiormente sulla lotta alla disinformazione online, sulla garanzia dell'integrità delle informazioni e sulla protezione del discorso democratico nei periodi elettorali; esprime preoccupazione, a tale proposito, per il fatto che i ritardi negli orientamenti e nelle norme tecniche costituiscano un ostacolo alla tempestiva attuazione del regolamento sull'IA; accoglie con favore il fatto che, nella sua proposta Omnibus digitale volta a semplificare la legislazione in materia di IA, la Commissione cerchi di affrontare tale problema collegando il calendario di attuazione delle norme sui sistemi di IA ad alto rischio alla disponibilità di norme o altri strumenti di sostegno;

16. accoglie con favore l'integrazione ufficiale del codice volontario di buone pratiche sulla disinformazione nel quadro del regolamento sui servizi digitali; ritiene che l'uso non autentico dei social media, ad esempio attraverso bot, account falsi, algoritmi di polarizzazione, engagement e amplificazione artificiali, sia tra i rischi più gravi per un discorso libero e aperto online, in particolare nei periodi elettorali; invita con urgenza tutte le piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi (VLOSE) che operano nell'UE a rispettare pienamente il codice ed esorta la piattaforma X ad aderire nuovamente ad esso;

17. accoglie con favore l'impegno della Commissione a elaborare un protocollo sugli incidenti e le crisi connessi al regolamento sui servizi digitali per affrontare ulteriormente gli incidenti gravi e le interferenze nell'ambiente informativo; ritiene che tale protocollo dovrebbe affrontare, tra l'altro, le interferenze elettorali condotte mediante comportamenti non autentici coordinati nello spazio online, in particolare attraverso l'amplificazione e l'engagement basati sui bot che distorcono efficacemente il discorso pubblico autentico;

18. prende atto del completamento da parte della Commissione dell'indagine sulla violazione da parte della piattaforma X degli obblighi di trasparenza a norma del regolamento sui servizi digitali, seguita dall'imposizione di un'ammenda di 120 milioni di EUR; esorta la Commissione ad accelerare le restanti indagini sulle presunte violazioni della legislazione digitale dell'UE, comprese quelle che riguardano

interferenze elettorali, opacità algoritmica o proliferazione di account e bot falsi; invita, in particolare, la Commissione a concludere rapidamente le indagini sulla conformità di TikTok al regolamento sui servizi digitali nel contesto delle elezioni presidenziali rumene del 2024, compreso il suo obbligo di attenuare i rischi sistemici per i processi democratici;

19. invita la Commissione e le autorità di regolamentazione competenti a indagare e denunciare pubblicamente le campagne di disinformazione segrete volte a sfruttare i sistemi di IA generativa, come le attività della rete "Pravda" con sede a Mosca; esorta i fornitori di sistemi di IA ad affrontare e mitigare debitamente questo fenomeno attraverso i loro sistemi di gestione dei rischi dell'IA; chiede inoltre che la definizione di norme di sicurezza per i fornitori di modelli linguistici di grandi dimensioni sia coordinata a livello internazionale, garantendo una maggiore trasparenza per l'addestramento delle fonti di dati;

20. invita la Commissione a completare con urgenza la propria valutazione della base di utenti e delle funzionalità di Telegram al fine di determinarne la classificazione come VLOP a norma del regolamento sui servizi digitali; esorta la Commissione e le autorità competenti a indagare sul potenziale ruolo di Telegram nel facilitare le attività criminali, le ingerenze elettorali e la diffusione della disinformazione all'interno dell'UE; incoraggia inoltre vivamente la piattaforma ad aderire al codice volontario di buone pratiche sulla disinformazione e a rispettare pienamente i requisiti dell'UE in materia di trasparenza, moderazione dei contenuti e accesso ai dati per garantire condizioni di parità e mantenere la fiducia dei cittadini nello spazio digitale dell'informazione;

21. raccomanda di esaminare ulteriormente il ruolo degli influencer, compresi i nano influencer e i micro influencer, nel plasmare il discorso pubblico e nell'influenzare le elezioni, sia quelli che contrastano che quelli che contribuiscono alle campagne di disinformazione straniere, consapevolmente o inconsapevolmente; sottolinea, a tale proposito, la necessità di norme rigorose in materia di trasparenza e integrità delle informazioni per i creatori di contenuti politici online, in particolare gli influencer che operano in una zona grigia tra la promozione commerciale e i messaggi politici; accoglie con favore i codici di condotta, la formazione e altre iniziative esistenti che sono stati sviluppati per rendere i social media e gli influencer più responsabili e trasparenti;

22. ritiene che un'infrastruttura digitale dell'UE, che comprenda centri di dati locali sicuri e capacità sovrane di cloud computing e edge computing europei, sia un pilastro strategico della resilienza digitale, poiché garantirebbe che i dati sensibili degli europei non siano conservati in centri di dati stranieri; invita la Commissione a proporre una definizione di cloud sovrano e del suo ambito di applicazione nel futuro atto legislativo sullo sviluppo del cloud e dell'IA; invita la Commissione a riflettere sul fallimento del dibattito sul sistema di certificazione europeo della cibersicurezza per i servizi cloud e a proporre una soluzione tangibile nella revisione del regolamento sulla cibersicurezza, tenendo conto delle preoccupazioni in materia di cibersicurezza e sovranità connesse a una concentrazione di potere; esorta a creare spazi di sperimentazione normativa e meccanismi di finanziamento per sostenere l'innovazione da parte delle start-up tecnologiche dell'UE, in particolare nei settori con dipendenze critiche; sostiene inoltre la visione a lungo termine relativa a piattaforme di social media dell'UE, concepite in

conformità dei valori dell'UE di trasparenza, protezione dei dati, libertà di espressione e responsabilità democratica;

23. invita la Commissione, le autorità di regolamentazione digitale dell'UE e le piattaforme online a garantire la trasparenza dei programmi di ridistribuzione delle entrate che potrebbero consentire a chi mette in atto operazioni di manipolazione delle informazioni e ingerenze da parte di attori stranieri, o persino alle entità inserite nell'elenco delle sanzioni, di guadagnare; ritiene che la monetizzazione delle attività di manipolazione delle informazioni e ingerenze da parte di attori stranieri nell'ambito di tali programmi dovrebbe essere affrontata negli obblighi di valutazione e mitigazione dei rischi previsti dal regolamento sui servizi digitali;

24. prende atto con preoccupazione delle conclusioni dell'autorità olandese per la protezione dei dati, che indicano che i chatbot di IA possono fornire consigli di voto distorti e inaffidabili, ponendo in tal modo rischi per l'integrità elettorale; invita la Commissione a rispettare il suo impegno a elaborare orientamenti sull'uso dell'IA nei processi elettorali al fine di garantirne un uso responsabile;

Libertà di parola

25. sottolinea che lo scudo europeo per la democrazia deve proteggere e sostenere la libertà di espressione e di informazione quale diritto fondamentale applicabile sia agli spazi offline che a quelli online; sottolinea che la tutela dei diritti umani nell'UE è tra le più forti al mondo e che le imprese che desiderano operare nell'ambiente dell'UE e attrarre clienti europei hanno la responsabilità condivisa di salvaguardare tale tutela; sottolinea, tuttavia, che le libertà di espressione e di informazione sono state concepite per proteggere gli esseri umani, non le macchine o i software che mostrano un comportamento non autentico, come l'amplificazione e l'engagement basati su bot e IA, e i programmi software automatizzati che svolgono compiti ripetitivi su una rete con l'obiettivo di imitare gli utenti reali;

26. riconosce l'importanza di garanzie efficaci per gli utenti nell'esercizio dei propri diritti democratici, compresa la capacità di contestare le decisioni di moderazione dei contenuti delle piattaforme e l'obbligo delle piattaforme di informare gli utenti quando i loro contenuti sono rimossi o limitati; ricorda l'obbligo previsto dal regolamento sui servizi digitali per le piattaforme, ovvero di prevedere un meccanismo distinto di gestione dei reclami a tal fine; sottolinea che la salvaguardia dei diritti fondamentali dei singoli utenti comporta nondimeno lo svolgimento di valutazioni approfondite e l'attenuazione dei rischi sistemici che incidono sull'integrità dello spazio informativo;

Integrità dei media e delle informazioni

27. ritiene che le misure volte a promuovere la libertà e l'indipendenza editoriale dei media siano un elemento centrale del conseguimento degli obiettivi fissati dallo scudo europeo per la democrazia; accoglie con favore, a tale proposito, le innovative norme minime comuni in materia di libertà e pluralismo dei media stabilite attraverso l'adozione dell'EMFA; osserva, tuttavia, che l'importanza del regolamento può essere valutata solo sulla base della sua attuazione pratica e sottolinea pertanto l'importanza di una sua applicazione rigorosa; accoglie con favore i nuovi impegni annunciati in materia di sostegno ai media attraverso il programma per la resilienza dei media e invita ad allineare gli impegni a lungo termine nel prossimo QFP;

28. sottolinea la necessità di valutare attentamente il potenziale impatto della legislazione dell'UE sul giornalismo e sui media editoriali, con particolare riguardo alla salvaguardia della sostenibilità dei modelli di business delle imprese del settore dei media;

29. sottolinea, nel contesto delle società di media che vendono abbonamenti tramite app, l'importanza della piena attuazione del regolamento sui mercati digitali; prende atto, a tale proposito, della decisione di non conformità della Commissione del 23 aprile 2025 per quanto riguarda Apple e Meta; prende atto delle indagini della Commissione su una potenziale violazione del regolamento sui mercati digitali da parte di Google, a causa della retrocessione dei contenuti degli editori di media nei risultati di ricerca;

30. accoglie con favore il fatto che la comunicazione congiunta includa nuove azioni di sostegno alla promozione dell'alfabetizzazione digitale e dei media, come il programma per la resilienza dei media, il programma di sostegno alle competenze di base per le scuole e il rafforzamento del gruppo di esperti in materia di alfabetizzazione mediatica, compresa la creazione di una nuova rete di esperti per l'alfabetizzazione mediatica e orientamenti aggiornati per insegnanti ed educatori; sottolinea che la prossima revisione della direttiva sui servizi di media audiovisivi dovrebbe rafforzare le disposizioni sui requisiti minimi per il lavoro degli Stati membri in materia di alfabetizzazione mediatica;

31. accoglie con favore l'annunciato aggiornamento della raccomandazione della Commissione sulla sicurezza dei giornalisti[52] e la prossima revisione della raccomandazione anti-SLAPP[53]; sottolinea che tali aggiornamenti e revisioni devono tenere conto del modo in cui le minacce, la violenza, il sabotaggio e altre azioni volte a ostacolare il lavoro giornalistico incidono sulla tutela, la sicurezza e la responsabilizzazione dei giornalisti e di altri professionisti dei media nell'UE;

32. sottolinea l'importanza di proteggere i giornalisti da azioni legali abusive; accoglie con favore, a tale proposito, l'adozione della direttiva anti-SLAPP[54] e l'annunciato aggiornamento del mandato e della composizione del gruppo di esperti contro le SLAPP; invita gli Stati membri a essere ambiziosi nel processo di attuazione in corso e invita la Commissione a continuare a fornire sostegno; invita la Commissione a elaborare una relazione di valutazione globale sull'efficacia dell'attuazione;

33. accoglie con favore l'accordo provvisorio sul regolamento sugli investimenti esteri diretti[55], in particolare le disposizioni che includono il settore dei media come fattore di

---

[52] Raccomandazione (UE) 2021/1534 della Commissione, del 16 settembre 2021, relativa alla garanzia della protezione, della sicurezza e dell'empowerment dei giornalisti e degli altri professionisti dei media nell'Unione europea (GU L 331 del 20.9.2021, pag. 8; ELI: http://data.europa.eu/eli/reco/2021/1534/oj).
[53] Raccomandazione (UE) 2022/758 della Commissione, del 27 aprile 2022, sulla protezione dei giornalisti e dei difensori dei diritti umani attivi nella partecipazione pubblica da procedimenti giudiziari manifestamente infondati o abusivi ("azioni legali strategiche tese a bloccare la partecipazione pubblica") (GU L 138 del 17.5.2022, pag. 30, ELI: http://data.europa.eu/eli/reco/2022/758/oj).
[54] Direttiva (UE) 2024/1069 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, sulla protezione delle persone attive nella partecipazione pubblica da domande manifestamente infondate o procedimenti giudiziari abusivi ("azioni legali strategiche tese a bloccare la partecipazione pubblica") (GU L, 2024/1069, 16.4.2024, ELI: http://data.europa.eu/eli/dir/2024/1069/oj).
[55] Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, che istituisce un

cui tenere conto nel determinare se un investimento possa incidere negativamente sulla sicurezza o sull'ordine pubblico; si rammarica, tuttavia, che il settore dei media non rientri nell'ambito di applicazione obbligatorio di cui all'allegato del regolamento;

34. invita la Commissione e gli Stati membri ad analizzare attentamente le conseguenze del cambiamento della politica in materia di aiuti dell'amministrazione statunitense nel contesto del pluralismo dei media e del giornalismo indipendente e, se necessario, ad agire per colmare il vuoto lasciato nei mercati dei media sia all'interno dell'UE che nelle regioni limitrofe; accoglie con favore i finanziamenti di emergenza dell'UE destinati a RFE/RL; chiede lo sviluppo di una soluzione per fornire a RFE/RL finanziamenti stabili e a lungo termine;

35. sottolinea che le reti di verifica dei fatti basate sulla società possono svolgere un ruolo importante nell'individuazione e nella lotta alle campagne di disinformazione e fornire informazioni preziose per valutare i rischi del regolamento sui servizi digitali; osserva che le organizzazioni indipendenti di verifica dei fatti necessitano di condizioni stabili in cui operare; ritiene che la rete europea di verifica dei fatti, annunciata dalla Commissione nel 2025, potrebbe essere uno strumento per conseguire tale obiettivo; sottolinea che, per essere credibili ed efficaci, le organizzazioni di verifica dei fatti devono rispettare norme rigorose in materia di neutralità politica, indipendenza e obiettività metodologica;

Società civile

36. sottolinea il ruolo cruciale che la società civile svolge nel difendere la nostra democrazia, non solo nel fungere da custode, esponendo e combattendo attivamente i tentativi stranieri di interferire con i processi democratici, ma anche nel fungere da forza fondamentale nell'impegno a lungo termine per costruire società più forti e più resilienti; sottolinea, in particolare, l'importante ruolo della società civile nel sostenere i valori sanciti dall'articolo 2 TUE;

37. accoglie con favore la strategia dell'UE per la società civile, pubblicata dalla Commissione insieme alla comunicazione sullo scudo europeo per la democrazia; accoglie con favore l'approccio della Commissione di collegare tale strategia ai lavori sullo scudo quale strumento per rafforzare ulteriormente l'impegno civico;

38. invita la Commissione a rafforzare il proprio lavoro sul dialogo civile e a istituire nuovi strumenti a tal fine; accoglie con favore, in tale contesto, l'impegno della Commissione a istituire una piattaforma operativa della società civile entro il 2026 per sostenere un approccio più sistematico che sarà utilizzato per rafforzare il dialogo in linea con i valori dell'UE; ritiene che l'annunciato polo di conoscenze online sullo spazio civico possa contribuire a coordinare le attività delle organizzazioni della società civile nel settore della protezione della democrazia e della lotta contro le minacce ibride e la manipolazione delle informazioni e delle ingerenze da parte di attori stranieri, migliorando la conoscenza situazionale;

39. sottolinea l'importanza di programmi di finanziamento concreti come il programma CERV; accoglie con favore l'idea della Commissione di mantenere il programma CERV

---

quadro per il controllo degli investimenti esteri diretti nell'Unione (GU L 79I del 21.3.2019, pag. 1, ELI: http://data.europa.eu/eli/reg/2019/452/oj).

e di integrarlo nel nuovo programma AgoraEU per il periodo 2028-2034; invita la Commissione a garantire che i finanziamenti per questa componente di AgoraEU soddisfino le esigenze delle organizzazioni della società civile e siano attuati sotto la gestione diretta della Commissione;

40. sottolinea la necessità di una maggiore trasparenza finanziaria in materia di finanziamento delle organizzazioni della società civile in generale e, in particolare, nel contesto del sostegno da parte dei paesi terzi; ricorda che le organizzazioni della società civile possono essere e sono state utilizzate da attori malintenzionati di paesi terzi per influenzare illegittimamente i processi democratici nell'UE e nei suoi Stati membri; sottolinea che, nel suo ruolo di istituzione, il Parlamento ha una responsabilità particolare nel contribuire alle riforme in questo settore, alla luce del cosiddetto scandalo Qatargate; sottolinea, tuttavia, che le misure volte ad affrontare tale questione dovrebbero essere concepite in modo da evitare che siano utilizzate in modo improprio per stigmatizzare le attività legittime della società civile in quanto tale;

41. accoglie con favore la proposta di direttiva della Commissione sulla rappresentanza d'interessi esercitata per conto di paesi terzi quale parte importante del pacchetto per la difesa della democrazia, al fine di stabilire requisiti armonizzati per le attività economiche relative alla rappresentanza d'interessi esercitata per conto di un'entità di un paese terzo; sottolinea che, per quanto riguarda l'influenza dei paesi terzi, norme comuni a tale riguardo rappresenterebbero un importante elemento costitutivo in termini di trasparenza; invita i colegislatori a portare a termine senza indugio il processo legislativo;

42. sottolinea l'importanza del coinvolgimento dei cittadini nei processi democratici; esorta la Commissione a garantire, in cooperazione con gli Stati membri, una comunicazione chiara ed efficace delle iniziative che sviluppa, al fine di promuovere e migliorare l'uso degli strumenti di coinvolgimento dei cittadini; accoglie con favore il rafforzamento da parte della Commissione di tali strumenti, in particolare l'iniziativa dei cittadini europei, i panel europei di cittadini e la piattaforma di coinvolgimento dei cittadini, nonché la proposta di rafforzare la rete delle autorità nazionali sulla partecipazione dei cittadini;

Proteggere le infrastrutture critiche

43. ritiene che la protezione dell'UE e dei suoi Stati membri da atti di sabotaggio, sia fisico che digitale, delle infrastrutture critiche sia un elemento essenziale per salvaguardare la resilienza democratica; chiede solide misure preventive, una cooperazione transfrontaliera rafforzata e una maggiore capacità dell'UE di individuare, scoraggiare e rispondere a tali attività ostili;

44. condanna fermamente l'escalation di incursioni con droni e di altre incursioni aeree che prendono di mira e interferiscono con le infrastrutture critiche, compresi gli aeroporti civili, le basi militari e le strutture energetiche in tutta l'UE, in particolare perpetrate dalla Russia e dalla Bielorussia; invita gli Stati membri a rispondere in modo coordinato, unificato e adeguato a qualsiasi violazione del proprio spazio aereo, anche mediante l'abbattimento di aeromobili, droni e di altre minacce aeree;

45. sottolinea che una serie di attività ibride intraprese dalla Russia contro l'UE costituiscono terrorismo sponsorizzato dallo Stato, anche se non raggiungono la soglia dell'attacco armato; sottolinea pertanto la necessità di applicare tutti i quadri giuridici

antiterrorismo disponibili alle attività ostili della Russia che violano la sovranità territoriale degli Stati membri dell'UE, minano l'integrità delle loro istituzioni e minacciano direttamente la sicurezza della popolazione civile; sottolinea che l'UE deve passare con urgenza dalla modalità di difesa alla deterrenza attiva; esorta gli Stati membri a valutare i quadri giuridici e operativi per stabilire misure offensive proporzionate ai danni dell'infrastruttura logistica e digitale alla base delle attività di destabilizzazione di Mosca;

46. invita la Commissione e gli Stati membri a stabilire un'interpretazione comune europea della Convenzione delle Nazioni Unite sul diritto del mare (UNCLOS), al fine di garantire un'azione coordinata contro le attività ibride e il sabotaggio nelle zone marittime dell'UE, in particolare nel Mar Baltico; ritiene che il coordinamento transfrontaliero possa essere ulteriormente migliorato sia a livello operativo che finanziario; sottolinea la necessità che l'UE intensifichi la propria risposta alle minacce ibride nelle zone marittime, comprese quelle poste dalla "flotta ombra" russa; sottolinea che, per affrontare tali sfide, sono necessari finanziamenti specifici e sufficienti da parte dell'UE;

47. prende atto con preoccupazione delle dipendenze strutturali esistenti, attraverso la concentrazione del mercato e il controllo estero, nell'infrastruttura digitale dell'UE, compresi i sistemi operativi, i centri dati, i semiconduttori, l'IA, la cibersicurezza, il cloud computing e varie piattaforme e servizi digitali, che rappresentano tutti un rischio elevato per la democrazia, la libertà, la sicurezza e la competitività all'interno dell'UE; invita la Commissione e gli Stati membri a istituire, come livello fondamentale, un'infrastruttura digitale sovrana dell'UE con tecnologie che tutelino la vita privata e un ecosistema di interfaccia di programmazione delle applicazioni (API) europeo attraverso politiche ambiziose e mirate che rafforzino gli investimenti e la quota di mercato delle imprese dell'UE, facendo leva sull'approvvigionamento europeo di energia pulita nello sviluppo di centri dati e infrastrutture cloud, anche attraverso iniziative orientate al mercato quali joint venture o reti federate in settori quali le gigafactory di IA o i servizi cloud;

48. sottolinea la necessità di garantire una maggiore integrazione tra le infrastrutture digitali, la cibersicurezza e la politica di difesa per consentire il progresso dell'autonomia strategica dell'UE e la necessità di sfruttare le infrastrutture a duplice uso, come i centri dati resilienti sparsi in tutta l'UE, per garantire la continuità operativa di fronte alle minacce ibride o in tempo di guerra; sottolinea inoltre la necessità di aumentare gli investimenti nella mobilità militare e nelle comunicazioni sicure, compresa l'adozione urgente e prioritaria di capacità spaziali come IRIS^2, al fine di fornire servizi criptati per uso pubblico e della difesa;

49. sottolinea che i quadri sulla cibersicurezza quali la direttiva NIS2, il regolamento sulla ciberresilienza[56] e il regolamento sulla cibersolidarietà[57] devono essere allineati per

[56] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[57] Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694 (regolamento sulla cibersolidarietà) (GU L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

sostenere norme sicure fin dalla progettazione ed evitare la frammentazione normativa; chiede, in tale contesto, una revisione della legislazione pertinente nel settore della cibersicurezza e sottolinea la necessità di rafforzare le strutture esistenti, come l'ENISA e il Centro europeo di competenza per la cibersicurezza;

50. ricorda il basso livello di recepimento della direttiva NIS2; si rammarica del fatto che, dopo la scadenza del termine del 17 ottobre 2024, la Commissione abbia dovuto inviare lettere di costituzione in mora a ben 23 Stati membri che non avevano recepito pienamente la direttiva; invita con urgenza gli Stati membri a completare quanto prima il recepimento della direttiva, dato che, alla fine del 2025, oltre un anno dopo il termine, la direttiva doveva ancora essere recepita da 10 Stati membri; accoglie con favore, a tale proposito, l'impegno della Commissione a collaborare strettamente con gli Stati membri al fine di garantire un'attuazione rapida e coerente del quadro orizzontale in materia di cibersicurezza di cui alla direttiva NIS2, nonché del regolamento sulla ciberresilienza e del regolamento sulla cibersolidarietà, come stabilito nella strategia di sicurezza interna ProtectEU;

Cooperazione in materia di giustizia e affari interni

51. ritiene che tutti gli strumenti di diritto penale disponibili a livello degli Stati membri e dell'UE dovrebbero essere applicati e, se del caso, ulteriormente sviluppati per prevenire e contrastare i comportamenti illeciti volti a minare le istituzioni e i processi democratici; sostiene, in particolare, l'impegno della Commissione a favore di una revisione ambiziosa del mandato di Europol, al fine di trasformarlo in un'agenzia di polizia realmente operativa che sostenga meglio gli Stati membri;

52. accoglie con favore il fatto che la comunicazione congiunta riconosca il contributo positivo della giustizia penale e della cooperazione nell'attività di contrasto alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri e alle attività di disinformazione; invita la Commissione, in sede di preparazione della prevista revisione dei mandati di Europol ed Eurojust, a valutare attentamente le lacune giuridiche che attualmente impediscono a tali agenzie di fornire la loro piena assistenza agli Stati membri di fronte alle minacce ibride e a esplorare possibili soluzioni per superarle;

53. prende atto con preoccupazione dei crescenti casi in cui gli attori malintenzionati di paesi terzi utilizzano la criminalità come servizio e le organizzazioni criminali come rappresentanti all'interno dell'UE per colpire persone ed entità identificate come avversari politici, rappresentando una grave minaccia per la sicurezza interna dell'UE; sottolinea che tali pratiche costituiscono un atto intollerabile di ingerenza straniera, con effetti potenzialmente destabilizzanti sulle nostre società; sottolinea, in tale contesto, la necessità di rafforzare ulteriormente il coordinamento a livello dell'UE nel settore della giustizia penale e delle attività di contrasto;

54. condanna fermamente la strumentalizzazione della migrazione contro l'UE; ritiene che tale fenomeno rappresenti un tentativo inaccettabile da parte di paesi terzi malevoli di esercitare pressioni politiche sugli Stati membri in prima linea e sull'UE; accoglie con favore le disposizioni specifiche sulla strumentalizzazione della migrazione recentemente incluse nei principali atti legislativi dell'UE in materia di gestione delle

frontiere e migrazione; sottolinea che gli Stati membri colpiti da tali minacce dovrebbero poter contare sul sostegno di agenzie specializzate dell'UE; chiede che il mandato di Frontex sia rafforzato, in modo tale che l'Agenzia disponga della base giuridica e delle risorse umane, finanziarie e tecniche necessarie per assistere adeguatamente gli Stati membri nella gestione di tali minacce ibride; sottolinea, in tale contesto, la necessità di rafforzare ulteriormente la capacità dell'UE di contribuire agli sforzi degli Stati membri in materia di protezione delle frontiere attraverso investimenti sufficienti nell'ambito del QFP 2028-2034;

Dimensione esterna

55. sottolinea la necessità che lo scudo europeo per la democrazia abbia una solida dimensione esterna; accoglie con favore l'inclusione nella comunicazione congiunta di azioni specifiche volte a sostenere i paesi al di là delle frontiere dell'UE, in particolare agevolando lo sviluppo di capacità per migliorare la resilienza dei paesi candidati e potenziali candidati rispetto alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri e ibride, nonché sostenendo i media e il giornalismo indipendenti e aumentando la loro capacità di monitorare la disinformazione sui social media prima e durante le elezioni;

56. sostiene l'idea di sfruttare i canali diplomatici per rafforzare la capacità nelle regioni prioritarie; ritiene che il ruolo delle delegazioni dell'UE e delle ambasciate degli Stati membri dell'UE sia fondamentale per comprendere meglio le circostanze locali che possono portare a ingerenze straniere e fornire una risposta su misura; prende atto della possibilità per le delegazioni dell'UE e le ambasciate degli Stati membri di sostenere l'organizzazione di campagne di sensibilizzazione nei paesi ospitanti; sottolinea l'importanza di coinvolgere le missioni e le operazioni della politica di sicurezza e di difesa comune (PSDC) nelle azioni previste nella comunicazione congiunta; invita gli Stati membri e il SEAE a integrare le attività di sviluppo delle capacità e la formazione sulle minacce ibride nei mandati delle missioni e delle operazioni, al fine di aumentare la preparazione delle controparti nazionali;

57. chiede lo sviluppo di una strategia globale in base alla quale le delegazioni dell'UE e le missioni e operazioni in materia di PSDC, in stretto coordinamento con le missioni diplomatiche degli Stati membri dell'UE, possano servire in modo più efficace come prima linea di difesa contro gli attacchi ibridi, comprese le operazioni informatiche, le manipolazioni delle informazioni e le ingerenze da parte di attori stranieri; ritiene che il rafforzamento delle capacità di comunicazione strategica e di diplomazia pubblica all'interno delle delegazioni dell'UE, con particolare attenzione alla promozione di narrazioni basate sui fatti, dell'impegno civico e del rafforzamento della fiducia, in particolare tra i giovani e gli educatori, sia di vitale importanza; invita la vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza e il Consiglio a includere squadre di monitoraggio e risposta alla disinformazione nelle missioni di PSDC, a garantire la formazione in materia di manipolazione delle informazioni e di ingerenze da parte di attori stranieri per tutto il personale delle missioni e a rafforzare il coordinamento tra operazioni civili e militari per contrastare l'influenza ibrida;

58. accoglie con favore l'impegno rafforzato nella comunicazione congiunta a sviluppare la capacità di operazioni di informazione offensive; osserva che tale impegno richiede

risorse dedicate e una pianificazione a lungo termine; sottolinea che l'obiettivo dovrebbe includere il rafforzamento da parte dell'UE, nel suo vicinato, di misure di informazione proattive per contrastare gli sforzi destabilizzanti della Russia; sottolinea la necessità di diffondere informazioni fattuali e affidabili nelle popolazioni che vivono in regimi autoritari, in particolare la Russia, al fine di rivelare le pratiche di governance distruttive dei loro governanti, che rappresentano un pericolo per la libertà e la pace non solo nei paesi vicini, ma soprattutto all'interno del loro paese; chiede ogni possibile utilizzo dello spazio digitale e cibernetico e della sua natura priva di frontiere per conseguire tale obiettivo;

59. riconosce che i vicini immediati dell'UE, compresi i Balcani occidentali, la Moldova e l'Ucraina, devono affrontare gravi ingerenze straniere; chiede il finanziamento di poli di coordinamento regionali per contrastare la manipolazione delle informazioni e le ingerenze da parte di attori stranieri, rafforzare il sostegno al giornalismo investigativo e alle autorità di regolamentazione dei media e potenziare le comunicazioni strategiche basate sui fatti attraverso le delegazioni dell'UE per contrastare la disinformazione anti-UE; sottolinea la necessità di prestare particolare attenzione al sostegno per l'integrità elettorale nei paesi candidati all'adesione all'UE;

60. invita la Commissione a rendere i programmi di alfabetizzazione mediatica una parte permanente dell'assistenza preadesione e dello strumento europeo di vicinato, con sovvenzioni specifiche dell'UE a sostegno del giornalismo investigativo nelle regioni vulnerabili;

61. chiede di intensificare gli attuali sforzi dell'UE per sostenere i paesi partner del suo vicinato, nonché i paesi prioritari dell'Africa subsahariana, della regione Asia-Pacifico e dell'America latina, nello sviluppo della resilienza alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri, nel rafforzamento dei processi democratici e nella garanzia dell'integrità elettorale; sottolinea, in particolare, la necessità di continuare a sviluppare il progetto faro EUvsDisinfo;

62. riconosce l'istituzione dell'EUPM Moldova quale esempio virtuoso di come l'UE possa svolgere un ruolo decisivo nel sostenere le strutture di gestione delle crisi di un paese partner e nel rafforzare la sua resilienza alle minacce ibride, informatiche e relative alla manipolazione delle informazioni e alle ingerenze straniere; ritiene che l'EUPM Moldova dovrebbe fungere da modello per includere la lotta alle minacce ibride nel mandato delle missioni esistenti o l'istituzione di missioni analoghe in altri paesi partner; prende atto delle elezioni parlamentari tenutesi in Moldova il 28 settembre 2025 e della forte vittoria del partito filoeuropeo di azione e solidarietà (PAS);

63. accoglie con favore il dispiegamento di squadre di risposta rapida europee alle minacce ibride, come illustrato dal precedente esempio della Moldova, quale utile strumento per sviluppare capacità e resilienza nei paesi colpiti da attacchi ibridi, informatici e di manipolazione delle informazioni e ingerenze da parte di attori stranieri, sulla base del know-how e delle competenze specifici dell'UE e dei suoi Stati membri;

64. sottolinea l'importanza di dare priorità ai principi e agli obiettivi dello scudo europeo per la democrazia nella cooperazione internazionale con partner che condividono gli stessi principi, quali il G7, la NATO, le Nazioni Unite, l'Organizzazione per la sicurezza e la cooperazione in Europa e il Consiglio d'Europa; accoglie con favore le misure già

adottate nel quadro dell'impegno bilaterale e multilaterale, in particolare il codice di condotta delle Nazioni Unite per l'integrità delle informazioni sulle piattaforme digitali, l'impegno degli Stati membri del Consiglio d'Europa nella dichiarazione di Reykjavik a salvaguardare i sistemi elettorali dalle ingerenze straniere, i partenariati per la sicurezza e la difesa e i continui sforzi del meccanismo di risposta rapida del G7 per prevedere e sviluppare risposte collettive alla manipolazione delle informazioni e alle ingerenze da parte di attori stranieri;

65. accoglie con favore l'istituzione di un partenariato in materia di sicurezza e difesa tra l'UE e il Regno Unito nel maggio 2025; accoglie con favore il fatto che esso si concentri, tra l'altro, sulla cooperazione nella lotta ai problemi informatici, alle minacce ibride e alla manipolazione delle informazioni e delle ingerenze da parte di attori stranieri, nonché sulla protezione delle infrastrutture critiche;

Sistemi elettorali e resilienza elettorale

66. sottolinea che uno degli obiettivi principali dello scudo europeo per la democrazia dovrebbe essere proteggere l'integrità delle elezioni a livello locale, regionale, nazionale ed europeo; invita la Commissione e gli Stati membri a collaborare, nel pieno rispetto del principio di sussidiarietà, per attuare riforme volte a rafforzare la resilienza dei processi elettorali in Europa, con particolare attenzione alle misure volte a prevenire le ingerenze straniere;

67. invita gli Stati membri a intensificare gli sforzi per attuare le raccomandazioni della Commissione su processi elettorali inclusivi, solidi e resilienti all'interno dell'UE; sottolinea, in particolare, l'importanza di istituire reti elettorali nazionali per aiutare le autorità nazionali e gli organismi esperti a lavorare in sinergia;

68. invita gli Stati membri a garantire che le autorità elettorali o gli organismi equivalenti responsabili del buon funzionamento di elezioni libere ed eque siano sufficientemente finanziati e dotati degli strumenti necessari per consentire loro di svolgere le proprie funzioni, sia in termini di formazione del personale e degli strumenti digitali, sia in termini di garanzia di investimenti sufficienti negli organi elettorali e nelle infrastrutture elettorali;

69. ritiene che le campagne di odio e la violenza che rendono difficile per i candidati partecipare al dibattito pubblico o interagire con gli elettori costituiscono una minaccia per la democrazia; sottolinea che tali minacce possono essere alimentate dai tentativi dei paesi terzi di destabilizzare l'UE; accoglie con favore, a tale proposito, l'impegno della Commissione a presentare raccomandazioni sulla sicurezza in politica; invita gli Stati membri a intensificare gli sforzi per proteggere i candidati alle elezioni e i rappresentanti eletti;

70. sottolinea il ruolo chiave dell'ECNE nel garantire lo scambio delle migliori prassi in materia di resilienza elettorale nell'UE e nei suoi Stati membri; prende atto, tuttavia, delle attuali limitazioni delle sue attività; accoglie con favore l'impegno della Commissione di rafforzare l'ECNE, includendo riforme quali la creazione di un archivio di riferimenti e norme comuni per i processi elettorali;

71. invita la Commissione ad aumentare il proprio livello di ambizione per la riforma dell'ECNE, anche rivedendo le sue risorse e il suo personale permanente e sviluppando

ulteriormente il meccanismo congiunto per la resilienza elettorale; sottolinea l'importanza di attuare misure concrete per rafforzare la partecipazione dei paesi candidati alle operazioni dell'ECNE; invita la Commissione, nel quadro dell'ECNE, a istituire un gruppo di monitoraggio permanente incaricato di sorvegliare l'attuazione delle raccomandazioni della Commissione sui processi elettorali inclusivi e resilienti nell'UE e delle prossime raccomandazioni sulla sicurezza degli attori politici; ritiene che tale gruppo di monitoraggio dovrebbe altresì essere incaricato di elaborare proposte per futuri aggiornamenti di tali raccomandazioni;

72. invita la Commissione a includere il Parlamento e l'Autorità per i partiti politici europei e le fondazioni politiche europee (APPF) quali partner permanenti in tutte le riunioni dell'ECNE;

73. accoglie con favore l'obiettivo della Commissione di rafforzare la protezione delle infrastrutture legate alle elezioni attraverso la legislazione e gli strumenti esistenti; invita la Commissione a integrare tali sforzi con una revisione mirata della direttiva sulla resilienza dei soggetti critici, al fine di includere le infrastrutture elettorali nell'elenco dei servizi essenziali della pubblica amministrazione incluso nella direttiva;

74. invita la Commissione e gli Stati membri ad affrontare la questione del coinvolgimento degli attori stranieri nel panorama politico dei partiti in Europa; prende atto con preoccupazione di vari esempi di finanziamento di movimenti estremisti da parte di paesi terzi all'interno dell'UE; ritiene che la trasparenza finanziaria sia uno strumento importante per far luce su tale questione e chiede a tale riguardo un maggiore scambio tra enti pubblici e privati; sottolinea, in particolare, la necessità di combattere la comunicazione politica occulta, comprese le strutture di finanziamento opache e gli sponsor nascosti, al fine di salvaguardare l'integrità democratica e garantire la trasparenza per i cittadini;

75. prende atto con preoccupazione delle crescenti evidenze di ingerenze straniere e di spionaggio all'interno del sistema politico europeo; accoglie con favore gli sforzi investigativi profusi in tutti gli Stati membri, che hanno portato a condanne e procedimenti in corso per corruzione, spionaggio e promozione degli interessi di Stati stranieri; sottolinea i gravi rischi posti da garanzie inadeguate nell'assunzione di personale e collaboratori con stretti legami con regimi autoritari;

76. accoglie con favore il regolamento di recente adozione sulle norme rivedute per lo statuto e il finanziamento dei partiti politici europei e delle fondazioni politiche europee; prende atto delle disposizioni relative al finanziamento e alla partecipazione dei partiti di paesi terzi; invita i colegislatori ad assicurarne la piena ed efficace attuazione;

77. osserva che gli sviluppi delle criptovalute creano una potenziale vulnerabilità in termini di mancanza di trasparenza e di capacità di controllare il finanziamento dei partiti e dei movimenti politici in Europa; riconosce l'impegno della Commissione a riunire esperti nazionali sotto l'egida dell'ECNE, in stretta cooperazione con altre reti e parti interessate dell'UE, al fine di scambiare le migliori prassi, elaborare possibili orientamenti e promuovere azioni congiunte a tale riguardo; invita la Commissione a continuare a monitorare l'attuazione del pacchetto antiriciclaggio e del regolamento sui mercati delle cripto-attività e ad affrontare eventuali lacune nella legislazione che potrebbero dover essere colmate;

Il ruolo delle sanzioni nella protezione della democrazia

78. ritiene che le sanzioni nei confronti di entità, paesi o individui stranieri che adottano comportamenti volti a compromettere l'integrità democratica dell'UE o dei suoi Stati membri siano un elemento importante degli obiettivi dello scudo europeo per la democrazia; sottolinea inoltre che sanzioni efficaci devono includere una serie completa di attività, tra cui il congelamento e la confisca dei beni, l'attribuzione e l'esposizione, l'aumento dei costi e la riduzione delle entrate, i divieti di importazione ed esportazione, il rifiuto di accesso e altre misure restrittive pertinenti;

79. invita la Commissione e gli Stati membri a valutare regolarmente e attentamente le sanzioni imposte in termini di efficienza ottimale e di possibile ulteriore espansione, comprese le sanzioni secondarie nei confronti delle entità che si impegnano nell'elusione delle sanzioni; ritiene che, in particolare nell'ambito delle minacce ibride e delle attività destabilizzanti della Russia, l'UE dovrebbe ampliare ulteriormente il suo regime di sanzioni prendendo di mira i facilitatori finanziari e tecnici che sostengono la disinformazione, gli attacchi informatici e le interferenze elettorali, come gli scambi di criptovalute, le reti pubblicitarie e i fornitori di hosting, interrompendo nel contempo le reti di proxy della Russia nei paesi terzi, in particolare in Africa e in Medio Oriente, imponendo sanzioni agli organi di informazione, ai poli logistici e ai gruppi collegati a Wagner che diffondono narrazioni anti-UE; ritiene che, per aumentare ulteriormente il costo dell'aggressione ibrida, l'UE dovrebbe estendere le sanzioni secondarie nei confronti delle imprese non UE, in particolare cinesi, che facilitano le operazioni russe, e che dovrebbe vietare ai mercenari informatici russi di utilizzare servizi basati nell'UE, come i servizi di hosting, dominio e cloud, nonché esporre pubblicamente e imporre sanzioni ai politici o ai lobbisti dell'UE finanziati segretamente da Mosca;

80. ritiene che individuare e nominare tali paesi di origine, piuttosto che persone fisiche e imprese, rappresenterebbe un passo importante verso il riconoscimento del problema di una chiara interferenza sistematica e a più livelli, spesso sponsorizzata dallo Stato, che paesi quali la Russia o l'Iran stanno attuando in Europa; accoglie con favore la decisione della Commissione di inserire la Russia nell'elenco dei paesi terzi ad alto rischio nell'ambito del quadro dell'UE contro il riciclaggio di denaro e il finanziamento del terrorismo, al fine di preservare l'integrità del sistema finanziario dell'UE; rammenta che il nuovo regolamento antiriciclaggio fornirà ulteriori basi giuridiche per individuare i paesi pericolosi, compresi quelli coinvolti nella proliferazione delle armi di distruzione di massa;

81. sottolinea che l'efficacia e la credibilità delle sanzioni dell'UE dipendono da un'applicazione rigorosa e coerente; sottolinea che l'annunciata revisione del mandato della Procura europea (EPPO) offre l'opportunità di rafforzare il suo ruolo e di includere le indagini e il perseguimento delle violazioni delle sanzioni;

82. condanna l'uso, da parte della Russia, di "liste nere" di matrice politica rivolte ai cittadini dell'UE, ai rappresentanti delle autorità statali e delle organizzazioni commerciali, ai giornalisti, agli attori della società civile e ai funzionari politici, compresi i deputati del Parlamento europeo democraticamente eletti; chiede una risposta più coordinata e risoluta dell'UE a tali misure arbitrarie, garantendo la protezione e la sicurezza delle persone inserite nella lista nera e offrendo loro solidarietà e il sostegno necessario; esprime il pieno sostegno a tutte le persone interessate;

Preparazione dell'Unione europea

83. accoglie con favore la strategia europea per l'Unione della preparazione e sottolinea che gli obiettivi in essa stabiliti sono strettamente interconnessi con quelli dello scudo europeo per la democrazia; sottolinea inoltre che la resilienza democratica richiede che le società siano in grado di funzionare in condizioni eccezionali o perturbanti e che le riforme volte a rafforzare la preparazione dovrebbero pertanto costituire parte integrante dello scudo europeo per la democrazia;

84. chiede lo sviluppo e la diffusione rapidi di un'applicazione di allarme in caso di crisi interoperabile a livello dell'UE, che fornisca ai cittadini informazioni in tempo reale, affidabili e multilingue durante le emergenze; raccomanda che tale app sia integrata nei sistemi di allarme rapido nazionali e dell'UE, accessibile ai gruppi vulnerabili e regolarmente aggiornata con i progressi tecnologici e le migliori prassi nella gestione delle crisi;

85. accoglie con favore le iniziative di diversi Stati membri volte a distribuire un opuscolo sulla preparazione delle famiglie, con orientamenti chiari e pratici adattati alle diverse realtà sociali e geografiche dell'Europa per aiutare i cittadini a prepararsi alle emergenze; invita la Commissione a produrre un opuscolo a livello dell'UE che rispecchi il contesto transfrontaliero e multinazionale, contenente un indicazione delle forniture di emergenza raccomandate, istruzioni pratiche di autosufficienza per almeno 72 ore, consigli di primo soccorso di base e orientamenti specifici per i gruppi vulnerabili, compresi gli anziani, le persone con disabilità e le famiglie con bambini;

86. chiede l'organizzazione di regolari esercitazioni di preparazione su larga scala e coordinate dall'UE che coinvolgano le istituzioni dell'UE, gli Stati membri, le autorità regionali e locali, il settore privato e la società civile; raccomanda che tali esercitazioni simulino scenari complessi e realistici, tra cui attacchi informatici, perturbazioni delle infrastrutture critiche, disinformazione coordinata e crisi ibride, al fine di valutare le capacità di risposta, migliorare l'interoperabilità tra i livelli di governance e promuovere una cultura della preparazione a tutti i livelli; chiede, a tal fine, l'istituzione di una Giornata europea della preparazione; ritiene che la data di tale evento dovrebbe essere il 24 febbraio, data dell'invasione militare, su vasta scala e non provocata, dell'Ucraina da parte della Russia nel 2022, quale simbolo della solidarietà dell'UE nei confronti dell'Ucraina e forte promemoria della necessità di rafforzare la preparazione civile e di difesa contro le crescenti minacce dei regimi autoritari;

87. invita la Commissione a valutare la possibilità di ampliare il programma Erasmus+ o programmi analoghi per includere iniziative transfrontaliere sulla formazione in materia di preparazione per i lavoratori in settori critici, come i vigili del fuoco, gli operatori sanitari, i volontari della protezione civile, i funzionari pubblici e i rappresentanti delle organizzazioni della società civile e del pubblico in generale; raccomanda che tali programmi promuovano lo scambio di conoscenze transfrontaliero e intersettoriale, le esercitazioni congiunte e la formazione sulle minacce e le emergenze ibride e rafforzino le capacità di preparazione locale in tutti gli Stati membri, con particolare attenzione alle regioni vulnerabili;

88. chiede l'attuazione accelerata di sistemi di comunicazione sicuri come IRIS^2 e il sistema europeo di comunicazione critica; sottolinea che tali iniziative garantiscono la resilienza

delle telecomunicazioni, la continuità dei servizi essenziali durante le crisi, la riduzione delle dipendenze esterne nei settori strategici e il rafforzamento della cibersicurezza per tali infrastrutture;

89. chiede un maggiore coordinamento tra le istituzioni, gli organi e gli organismi dell'UE, gli Stati membri e i partner internazionali attraverso piattaforme condivise di conoscenza situazionale, metodologie comuni e meccanismi rapidi e sicuri di condivisione delle informazioni; sottolinea che tali strumenti consentono una risposta coerente, agile e coordinata alle minacce ibride, migliorano la previsione dei rischi e rafforzano la preparazione e la resilienza collettive dell'UE;

90. sottolinea la necessità di integrare la preparazione nell'ambito del QFP 2028-2034, al fine di costruire una resilienza credibile e conseguire un livello sufficiente di preparazione civile e di difesa; esorta la Commissione a sviluppare strumenti finanziari mirati che combinino i pertinenti strumenti di difesa e di sicurezza civile, come il meccanismo per la difesa dell'Europa e il meccanismo per mettere in sicurezza l'Europa, al fine di fornire finanziamenti sufficienti e stabili per i progetti di sviluppo della resilienza, l'innovazione tecnologica e le capacità a duplice uso, le iniziative di preparazione civile, la protezione delle infrastrutture critiche e gli sforzi volti a rafforzare la sovranità industriale e tecnologica dell'UE; osserva che i finanziamenti dedicati dovrebbero inoltre dare priorità agli sforzi di preparazione a livello locale, in particolare nei territori più esposti alle vulnerabilità e alle minacce ibride;

91. raccomanda alle istituzioni europee responsabili delle decisioni di rivedere e ottimizzare le loro strategie e i loro piani di emergenza in caso di conflitto militare aperto contro uno o più Stati membri e scenari di crisi analoghi; sottolinea inoltre la necessità di garantire i massimi livelli di sicurezza in tutte le istituzioni, gli organi e gli organismi dell'UE, anche nel settore della cibersicurezza e della sicurezza e integrità delle informazioni, e di creare le condizioni necessarie a tale riguardo, anche garantendo canali di comunicazione sicuri accreditati e spazi adeguati per le riunioni a porte chiuse; sottolinea la necessità di applicare rigorosamente le norme sulle violazioni della sicurezza e della riservatezza delle informazioni, in particolare nel contesto di un maggiore rischio di spionaggio e sabotaggio; sottolinea che, anche al di fuori di un conflitto militare aperto, le minacce ibride continuano a comportare rischi sempre più elevati per il funzionamento quotidiano dell'UE;

92. accoglie con favore l'impegno della Commissione volto a rafforzare la sicurezza fisica e delle informazioni all'interno delle istituzioni dell'UE, come indicato nella nota del consiglio di amministrazione interno dell'ottobre 2025, compresi i piani per sale riunioni sicure, procedure rafforzate di nulla osta di sicurezza per il personale che tratta informazioni classificate e l'istituzione dell'Accademia per la sicurezza, al fine di garantire aggiornamenti periodici sugli sviluppi delle minacce; osserva che tali misure rispondono ai maggiori rischi derivanti dallo spionaggio, dalle ingerenze straniere e dalle minacce ibride rivolte ai processi decisionali dell'UE; sottolinea, tuttavia, che il miglioramento della sicurezza fisica deve essere integrato da solidi protocolli di cibersicurezza e capacità di controspionaggio per affrontare l'intero spettro dei rischi di infiltrazione; chiede la rapida adozione della proposta di regolamento della Commissione sulla sicurezza delle informazioni nelle istituzioni, negli organi e negli organismi dell'Unione (COM(2022)0119); ricorda che il regolamento sulla cibersicurezza per le istituzioni, gli organi e gli organismi dell'UE raccomanda di

destinare un bilancio per la cibersicurezza pari al 10 % del bilancio complessivo per le tecnologie dell'informazione e della comunicazione destinato alle entità dell'UE;

93. raccomanda di adottare ulteriori misure per aumentare la sicurezza e la resilienza del Parlamento alle ingerenze straniere, nonché la sua preparazione e la sua capacità di funzionare durante le crisi; chiede, a tale proposito, un sostegno rafforzato per i deputati, che includa controlli informatici e di sicurezza, formazione e briefing specifici prima delle missioni, nonché una formazione interdisciplinare rafforzata e altre attività di sviluppo della resilienza che combinino sicurezza fisica e informatica e cibersicurezza; chiede un'ulteriore formazione mirata per il personale del Parlamento al fine di prevenire la manipolazione delle informazioni; raccomanda di rafforzare il proprio ambiente di cibersicurezza in conformità del regolamento sulla cibersicurezza e di aumentarne la maturità operativa, per rafforzare ulteriormente la propria resilienza alla cibersicurezza e migliorare le proprie capacità di rilevamento delle minacce nel contesto di un panorama dinamico delle minacce alla cibersicurezza e di un ambiente tecnologico in rapida evoluzione;

94. osserva che, nel contesto della sicurezza interna del Parlamento, l'uso da parte dei deputati e del personale di telefoni cellulari privati e di altri dispositivi come computer portatili a fini lavorativi costituisce una vulnerabilità che potrebbe essere sfruttata per attaccare l'istituzione; sottolinea che i deputati e il personale dovrebbero essere dotati dei dispositivi informatici necessari allo svolgimento delle proprie mansioni, come telefoni cellulari e computer portatili; accoglie con favore, in tale contesto, gli screening di sicurezza offerti ai deputati e al personale, su richiesta, per rilevare potenziali spyware su dispositivi privati; invita l'amministrazione a estendere e sistematizzare tale screening al fine di coprire tutti i dispositivi utilizzati per le attività connesse al Parlamento; chiede norme più chiare e orientamenti sistematici e adeguati per i deputati e il personale, nonché garanzie per attenuare tali rischi, in particolare durante le missioni;

95. invita la Commissione e il SEAE a coinvolgere sistematicamente il Parlamento nelle sue attività ed esercitazioni di preparazione, come "Integrated Resolve" dell'UE;

°

° °

96. incarica la sua Presidente di trasmettere la presente risoluzione al Consiglio, alla Commissione, al vicepresidente della Commissione/alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza nonché ai governi e ai parlamenti degli Stati membri.

MOTIVAZIONE

L'Unione europea si fonda sui valori della democrazia, dello Stato di diritto e dei diritti fondamentali, che costituiscono la base del suo ordine politico, della sua legittimità istituzionale e della sua coesione sociale. Negli ultimi anni, questi fondamenti sono stati sempre più presi di mira da una rapida intensificazione di attività ostili. La manipolazione delle informazioni e le ingerenze da parte di attori stranieri, le operazioni ibride, le campagne coordinate di disinformazione e altre forme di influenza maligna sono cresciute in termini di portata, raffinatezza e impatto.

Tali tattiche sfruttano deliberatamente le fratture sociali, manipolano il dibattito pubblico e cercano di minare la fiducia dei cittadini nelle istituzioni e nei processi democratici dell'Unione e dei suoi Stati membri. La loro natura sempre più digitale, amplificata da piattaforme online opache e da reti di diffusione transfrontaliere, ha reso il panorama delle minacce più complesso e più difficile da affrontare individualmente per gli Stati membri. In tale contesto, l'Unione ha riconosciuto la necessità di una risposta più strategica, coordinata e preventiva. Sulla base del lavoro svolto dalle sue precedenti commissioni speciali dedicate alle ingerenze straniere nei processi democratici (INGE e INGE2), nel dicembre 2024 il Parlamento europeo ha deciso di istituire una commissione speciale sullo scudo europeo per la democrazia (EUDS), incaricata di esaminare in che modo l'Unione possa difendere meglio i propri fondamenti democratici.

La comunicazione congiunta sullo scudo europeo per la democrazia, presentata dalla Commissione insieme alla VP/AR, rappresenta un importante contributo a tale sforzo. Fornisce una panoramica strutturata dell'attuale contesto di minaccia e individua diversi settori in cui sono necessarie ulteriori azioni per proteggere l'Unione dalla manipolazione delle informazioni, dalle ingerenze da parte di attori stranieri e dalla disinformazione, per rafforzare la resilienza della società. Il relatore ha accolto con favore tale iniziativa e ne ha riconosciuto il valore aggiunto nel consolidare la comprensione da parte dell'Unione delle sfide future.

Tuttavia, sebbene la comunicazione punti nella giusta direzione, il suo livello di ambizione rimane troppo limitato alla luce della portata delle minacce. Ciò che è necessario non è solo un quadro di riflessione, ma un programma concreto di riforme in grado di fornire capacità operativa, responsabilità e preparazione a lungo termine.

L'Unione ha sviluppato un ecosistema crescente di strutture, strumenti e programmi volti a contrastare la manipolazione delle informazioni e la disinformazione da parte di attori stranieri. Tali sforzi, compreso il lavoro delle task force pertinenti, delle reti di cooperazione e dei meccanismi di allarme rapido, sono significativi. Tuttavia, per portare questo lavoro al livello successivo, occorre anche porre in atto delle riforme. La proposta di istituire un centro europeo per la resilienza democratica è un'iniziativa positiva e promettente. Tuttavia, nella forma presentata nella comunicazione, tale iniziativa manca della chiarezza operativa necessaria affinché tale centro diventi un polo efficace di competenze e azioni. Nel progetto di relazione sono state formulate raccomandazioni concrete per conseguire tale obiettivo.

Per quanto concerne la sfera digitale, che in molti modi viene sfruttata da attori malevoli di paesi terzi per svolgere le loro operazioni, il relatore è del parere che occorra rispettare la pertinente legislazione dell'UE e che la Commissione debba intensificare le sue azioni di esecuzione, in particolare laddove vi siano indicazioni di manipolazione legata alle elezioni,

opacità algoritmica sistemica, comportamenti non autentici coordinati o uso improprio su larga scala delle funzionalità delle piattaforme.

L'evoluzione del contesto di minaccia impone inoltre agli Stati membri di cooperare più efficacemente a livello dell'Unione per lo svolgimento delle elezioni. L'integrità dei processi elettorali è al centro della resilienza democratica. In tale contesto, il progetto di relazione sottolinea la necessità di rafforzare in modo significativo la rete europea di cooperazione in materia elettorale (ECNE) e incoraggia una riforma globale per rendere tale rete più ambiziosa e pertinente dal punto di vista operativo. Inoltre, le infrastrutture connesse alle elezioni dovrebbero essere riconosciute come parte dell'infrastruttura critica dell'Unione e protette di conseguenza.

Il relatore ha inoltre accolto con favore il fatto che la comunicazione congiunta sullo scudo europeo per la democrazia preveda una dimensione esterna. Gli obiettivi dello scudo per la democrazia non possono essere conseguiti senza una stretta cooperazione con i partner del vicinato dell'Unione, in particolare i paesi candidati che sono sempre più esposti a intense ingerenze straniere. Il sostegno alla loro resilienza, anche attraverso lo sviluppo di capacità, la formazione e l'offerta di competenze, è indispensabile per salvaguardare il più ampio spazio democratico dell'Europa. Il progetto di relazione invita il SEAE a integrare sistematicamente le misure di preparazione alle minacce ibride nei mandati delle missioni e operazioni della PSDC, rafforzando in tal modo la capacità delle controparti nazionali di individuare e contrastare le ingerenze malevole. Nell'ambito della dimensione esterna dello scudo, dovrebbe inoltre essere intrapreso un riesame dei pertinenti strumenti sanzionatori per garantire che siano calibrati in modo ottimale per colpire gli attori che compromettono l'integrità democratica dell'Europa. L'allineamento con i partner che condividono gli stessi principi è importante anche al fine di garantire risposte collettive efficaci; il relatore accoglie con favore il ricorso a canali di cooperazione multilaterali e bilaterali, compresi gli attuali partenariati dell'UE in materia di sicurezza e difesa.

Il progetto di relazione sottolinea inoltre la necessità di un'agenda ambiziosa per rendere la società più resiliente. Le riforme a sostegno del settore dei media sono una componente importante, insieme alle misure volte a rafforzare l'alfabetizzazione mediatica. La società civile e la strategia dell'UE per la società civile costituiscono un altro aspetto fondamentale: una società civile forte e indipendente è essenziale per la resilienza democratica. Il relatore si pronuncia a favore di programmi solidi a sostegno delle priorità politiche delineate nell'iniziativa dello scudo europeo per la democrazia nell'ambito del prossimo quadro finanziario pluriennale 2028-2034.

Per rafforzare la resilienza della società è inoltre fondamentale rafforzare la protezione delle infrastrutture critiche, che dovrebbe essere riesaminata alla luce degli obiettivi dello scudo per la democrazia. Ciò a sua volta richiede riforme volte ad aumentare la sovranità europea sulle infrastrutture digitali, sui sistemi operativi, sui centri dati, sui semiconduttori, sull'IA, sulla cibersicurezza, sul cloud computing e su varie piattaforme e servizi digitali. Anche la revisione dei mandati delle pertinenti agenzie dell'UE, come Europol e Frontex, può svolgere un ruolo significativo nel migliorare la resilienza e la protezione dalle minacce ibride.

Infine, il progetto di relazione sottolinea che lo sviluppo della resilienza democratica richiede anche società in grado di continuare a funzionare in condizioni eccezionali o instabili. Le riforme volte a rafforzare la preparazione – dalle capacità di gestione delle crisi alla continuità delle istituzioni democratiche – devono pertanto costituire parte integrante dello scudo

europeo per la democrazia. Il progetto di relazione conclude che la protezione e il rafforzamento dei sistemi democratici europei richiedono non solo vigilanza e resilienza a tutti i livelli della società, ma anche una strategia dell'Unione coordinata e lungimirante, sostenuta da risorse sufficienti e dall'impegno politico.

ALLEGATO: DICHIARAZIONE DEI CONTRIBUTI

Conformemente all'allegato I, articolo 8, del regolamento, il relatore dichiara di aver incluso nella sua relazione contributi su questioni attinenti all'oggetto del fascicolo che ha ricevuto, ai fini dell'elaborazione del progetto di relazione, dai rappresentanti di interessi che rientrano nell'ambito di applicazione dell'accordo interistituzionale su un registro per la trasparenza obbligatorio[1], o dai rappresentanti delle pubbliche autorità di paesi terzi, incluse le loro missioni diplomatiche e ambasciate, qui di seguito elencati:

1. Rappresentanti di interessi che rientrano nell'ambito di applicazione dell'accordo interistituzionale su un registro per la trasparenza obbligatorio
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. Rappresentanti delle pubbliche autorità di paesi terzi, incluse le loro missioni diplomatiche e ambasciate
non disp.

L'elenco che precede è compilato sotto l'esclusiva responsabilità del relatore.

Quando delle persone fisiche sono identificate nell'elenco con il loro nome, la loro funzione o entrambi, il relatore dichiara di aver sottoposto alle persone fisiche interessate l'informativa del Parlamento europeo sulla protezione dei dati n. 484 (https://www.europarl.europa.eu/data-protect/index.do), che definisce le condizioni applicabili al trattamento dei loro dati personali e i diritti connessi a tale trattamento.

[1] Accordo interistituzionale di maggio 2021 tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea su un registro per la trasparenza obbligatorio (GU L 207 dell'11.6.2021, pag. 1, ELI:http://data.europa.eu/eli/agree_interinstit/2021/611/oj).