Parlement européen
2024-2029

Commission spéciale sur le bouclier européen de la démocratie

2025/2069(INI)

18.12.2025

PROJET DE RAPPORT

sur les conclusions et recommandations de la commission spéciale sur le bouclier européen de la démocratie
(2025/2069(INI))

Commission spéciale sur le bouclier européen de la démocratie

Rapporteur: Tomas Tobé

SOMMAIRE

Page

PROPOSITION DE RÉSOLUTION DU PARLEMENT EUROPÉEN

sur les conclusions et recommandations de la commission spéciale sur le bouclier européen de la démocratie

(2025/2069(INI))

Le Parlement européen,

– vu sa décision du 18 décembre 2024 sur la constitution, les compétences, la composition numérique et la durée de mandat d'une commission spéciale sur le bouclier européen de la démocratie[1],

– vu la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 12 novembre 2025 intitulée «Bouclier européen de la démocratie: renforcer la position de démocraties fortes et résilientes» (JOIN(2025)0791),

– vu le traité sur l'Union européenne (traité UE), et notamment son article 2 sur les valeurs fondatrices de l'Union, son article 10 sur la vie démocratique et son article 21 sur l'action extérieure,

– vu le traité sur le fonctionnement de l'Union européenne (traité FUE), et notamment son article 114 sur le marché intérieur et son article 222 sur la solidarité,

– vu la charte des droits fondamentaux de l'Union européenne,

– vu le règlement (UE, Euratom) nº 2025/2445 du Parlement européen et du Conseil du 26 novembre 2025 relatif au statut et au financement des partis politiques européens et des fondations politiques européennes[2],

– vu le règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)[3],

– vu le règlement (UE) 2024/1624 du Parlement européen et du Conseil du 31 mai 2024 relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme[4],

– vu le règlement (UE) 2024/1083 du Parlement européen et du Conseil du 11 avril 2024 établissant un cadre commun pour les services de médias dans le marché intérieur et

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

modifiant la directive 2010/13/UE (règlement européen sur la liberté des médias)[5],

– vu la directive (UE) 2024/1069 du Parlement européen et du Conseil du 11 avril 2024 sur la protection des personnes qui participent au débat public contre les demandes en justice manifestement infondées ou les procédures judiciaires abusives («poursuites stratégiques altérant le débat public»)[6],

– vu le règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique[7],

– vu le règlement (UE/Euratom) 2023/2841 du Parlement européen et du Conseil du 13 décembre 2023 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union[8],

– vu le règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) nº 1093/2010 et (UE) nº 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937[9] (règlement sur les marchés de crypto-actifs),

– vu la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil[10],

– vu la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)[11],

– vu le règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques)[12] et le règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques)[13],

– vu le règlement (UE) 2021/692 du Parlement européen et du Conseil du 28 avril 2021 établissant le programme «Citoyens, égalité, droits et valeurs» et abrogeant le règlement

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

(UE) nº 1381/2013 du Parlement européen et du Conseil et le règlement (UE) nº 390/2014 du Conseil[14],

– vu la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union[15],

– vu la directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à la fourniture de services de médias audiovisuels (directive «Services de médias audiovisuels»)[16],

– vu la décision 2014/145/PESC du Conseil du 17 mars 2014 concernant des mesures restrictives eu égard aux actions compromettant ou menaçant l'intégrité territoriale, la souveraineté et l'indépendance de l'Ukraine[17], et le règlement (UE) nº 269/2014 du Conseil du 17 mars 2014 concernant des mesures restrictives eu égard aux actions compromettant ou menaçant l'intégrité territoriale, la souveraineté et l'indépendance de l'Ukraine[18],

– vu la décision 2014/119/PESC du Conseil du 5 mars 2014 concernant des mesures restrictives à l'encontre de certaines personnes, de certaines entités et de certains organismes au regard de la situation en Ukraine[19], et le règlement (UE) nº 208/2014 du Conseil du 5 mars 2014 concernant des mesures restrictives à l'encontre de certaines personnes, de certaines entités et de certains organismes eu égard à la situation en Ukraine[20],

– vu la décision 2014/512/PESC du Conseil du 31 juillet 2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine[21], et le règlement (UE) nº 833/2014 du Conseil du 31 juillet 2014 concernant des mesures restrictives eu égard aux actions de la Russie déstabilisant la situation en Ukraine[22],

– vu la décision (PESC) 2022/266 du Conseil du 23 février 2022 concernant des mesures restrictives en réponse à la reconnaissance des zones des oblasts ukrainiens de Donetsk et de Louhansk non contrôlées par le gouvernement et à l'ordre donné aux forces armées russes d'entrer dans ces zones[23], et le règlement (UE) 2022/263 du Conseil du 23 février 2022 concernant des mesures restrictives en réaction à la reconnaissance des zones des oblasts ukrainiens de Donetsk et de Louhansk non contrôlées par le gouvernement et à l'ordre donné aux forces armées russes d'entrer dans ces zones[24],

---

[14] JO L 156 du 5.5.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/692/oj.
[15] JO L 305 du 26.11.2019, p. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj.
[16] JO L 95 du 15.4.2010, p. 1, ELI: http://data.europa.eu/eli/dir/2010/13/oj.
[17] JO L 78 du 17.3.2014, p. 16, ELI: http://data.europa.eu/eli/dec/2014/145(1)/oj.
[18] JO L 78 du 17.3.2014, p. 6, ELI: http://data.europa.eu/eli/reg/2014/269/oj.
[19] JO L 66 du 6.3.2014, p. 26, ELI: http://data.europa.eu/eli/dec/2014/119(1)/oj.
[20] JO L 66 du 6.3.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/208/oj.
[21] JO L 229 du 31.7.2014, p. 13, ELI: http://data.europa.eu/eli/dec/2014/512/oj.
[22] JO L 229 du 31.7.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/833/oj.
[23] JO L 42 I du 23.2.2022, p. 109, ELI: http://data.europa.eu/eli/dec/2022/266/oj.
[24] JO L 42 I du 23.2.2022, p. 77, ELI: http://data.europa.eu/eli/reg/2022/263/oj.

– vu la décision 2012/642/PESC du Conseil du 15 octobre 2012 concernant des mesures restrictives à l'encontre de la Biélorussie[25], et le règlement (CE) nº 765/2006 du Conseil du 18 mai 2006 concernant des mesures restrictives à l'encontre du président Lukashenko et de certains fonctionnaires de Biélorussie[26],

– vu la décision (PESC) 2023/1532 du Conseil du 20 juillet 2023 concernant des mesures restrictives en raison du soutien militaire de l'Iran à la guerre d'agression menée par la Russie contre l'Ukraine[27], et le règlement (UE) 2023/1529 du Conseil du 20 juillet 2023 concernant des mesures restrictives en raison du soutien militaire de l'Iran à la guerre d'agression menée par la Russie contre l'Ukraine[28],

– vu la décision (PESC) 2024/1603 du Conseil du 31 mai 2024 modifiant la décision (PESC) 2016/849 concernant des mesures restrictives à l'encontre de la République populaire démocratique de Corée[29], et le règlement d'exécution (UE) 2024/1602 du Conseil du 31 mai 2024 mettant en œuvre le règlement (UE) 2017/1509 concernant des mesures restrictives à l'encontre de la République populaire démocratique de Corée[30],

– vu la proposition de règlement du Conseil fixant le cadre financier pluriannuel pour les années 2028 à 2034, présentée par la Commission le 16 juillet 2025 (COM(2025)0571),

– vu les amendements adoptés le 27 novembre 2025 par le Parlement européen concernant la proposition de directive du Parlement européen et du Conseil établissant des exigences harmonisées dans le marché intérieur en matière de transparence de la représentation d'intérêts exercée pour le compte de pays tiers et modifiant la directive (UE) 2019/1937 (COM(2023)0637 – C9-0464/2023 – 2023/0463(COD))[31],

– vu sa résolution du 9 octobre 2025 sur une réponse unie aux récentes violations par la Russie de l'espace aérien et d'infrastructures critiques d'États membres de l'Union[32],

– vu sa résolution du 18 juin 2025 sur le rapport 2024 de la Commission sur l'état de droit[33],

– vu sa résolution du 7 mai 2025 sur un budget à long terme rénové pour l'Union dans un monde en mutation[34],

– vu sa résolution du 13 juillet 2023 sur des recommandations pour la réforme des règles du Parlement européen en matière de transparence, d'intégrité, de responsabilité et de lutte contre la corruption[35],

---

[25] JO L 285 du 17.10.2012, p. 1, ELI: http://data.europa.eu/eli/dec/2012/642/oj.
[26] JO L 134 du 20.5.2006, p. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj.
[27] JO L 186 du 25.7.2023, p. 20, ELI: http://data.europa.eu/eli/dec/2023/1532/oj.
[28] JO L 186 du 25.7.2023, p. 1, ELI: http://data.europa.eu/eli/reg/2023/1529/oj.
[29] JO L, 2024/1603, 31.5.2024, ELI: http://data.europa.eu/eli/dec/2024/1603/oj.
[30] JO L, 2024/1602, 31.5.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/1602/oj.
[31] Textes adoptés de cette date, P10_TA(2025)0306.
[32] Textes adoptés de cette date, P10_TA(2025)0230.
[33] JO C, C/2025/6259, 19.12.2025, ELI: http://data.europa.eu/eli/C/2025/6259/oj.
[34] Textes adoptés de cette date, P10_TA(2025)0090.
[35] JO C, C/2024/4011, 17.7.2024, ELI: http://data.europa.eu/eli/C/2024/4011/oj.

– vu sa résolution du 1er juin 2023 sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation[36],

– vu sa résolution du 15 décembre 2022 sur les soupçons de corruption par le Qatar et, plus largement, la nécessité de transparence et de responsabilité au sein des institutions européennes[37],

– vu sa résolution du 23 novembre 2022 sur la désignation de la Fédération de Russie comme État soutenant le terrorisme[38],

– vu sa résolution du 9 mars 2022 sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation[39],

– vu sa résolution du 8 mars 2022 sur le rétrécissement de l'espace dévolu à la société civile en Europe[40],

– vu sa résolution du 20 octobre 2021 sur les médias européens dans la décennie numérique: un plan d'action pour soutenir la reprise et la transformation[41],

– vu sa résolution du 23 novembre 2016 sur la communication stratégique de l'Union visant à contrer la propagande dirigée contre elle par des tiers[42],

– vu sa recommandation du 15 juin 2023 à l'intention du Conseil et de la Commission à la suite de l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalents[43],

– vu sa recommandation du 23 novembre 2022 à l'intention du Conseil, de la Commission et du vice-président de la Commission/haut représentant de l'Union pour les affaires étrangères et la politique de sécurité concernant la nouvelle stratégie de l'Union européenne en matière d'élargissement[44],

– vu sa recommandation du 13 mars 2019 au Conseil et à la vice-présidente de la Commission/haute représentante de l'Union pour les affaires étrangères et la politique de sécurité concernant le bilan du suivi donné par le Service européen pour l'action extérieure deux ans après le rapport du Parlement européen sur la communication stratégique de l'Union visant à contrer la propagande dirigée contre elle par des tiers[45],

– vu les suites données par la Commission aux recommandations formulées par le Parlement dans ses résolutions,

---

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

– vu la communication de la Commission du 12 novembre 2025 intitulée «Une stratégie de l'Union pour la société civile» (COM(2025)0790),

– vu la communication de la Commission du 1er avril 2025 intitulée «ProtectEU: une stratégie européenne de sécurité intérieure» (COM(2025)0148),

– vu la communication de la Commission du 24 juillet 2024 intitulée «Rapport 2024 sur l'état de droit – La situation de l'état de droit dans l'Union européenne» (COM(2024)0800),

– vu la communication de la Commission du 8 juillet 2025 intitulée «Rapport 2025 sur l'état de droit – La situation de l'état de droit dans l'Union européenne» (COM(2025)0900),

– vu la communication de la Commission du 12 décembre 2023 relative à la défense de la démocratie (COM(2023)0630),

– vu la communication de la Commission du 3 décembre 2020 relative au plan d'action pour la démocratie européenne (COM(2020)0790),

– vu les communications conjointes de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité du 5 décembre 2018 intitulée «Plan d'action contre la désinformation» (JOIN(2018)0036) et du 14 juin 2019 intitulée «Rapport sur la mise en œuvre du plan d'action contre la désinformation» (JOIN(2019)0012),

– vu le partenariat en matière de sécurité et de défense entre l'Union européenne et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord adopté le 19 mai 2025,

– vu les orientations politiques pour la Commission 2024-2029, présentées par la présidente Ursula von der Leyen le 18 juillet 2024 et intitulées «Le choix de l'Europe»,

– vu la décision d'exécution de la Commission du 28 mars 2025 relative au financement du programme pour une Europe numérique et à l'adoption du programme de travail pluriannuel 2025-2027 (C(2025)1839),

– vu le code de bonnes pratiques contre la désinformation,

– vu le rapport du groupe de coopération pour la sécurité des réseaux et des systèmes d'information du 23 janvier 2020 intitulé «Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures»,

– vu le rapport du 30 octobre 2024 de Sauli Niinistö, ancien président de la République de Finlande, en sa qualité de conseiller spécial auprès de la présidente de la Commission européenne, intitulé «Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness»,

– vu la recommandation (UE) 2023/2829 de la Commission du 12 décembre 2023 relative à des processus électoraux inclusifs et résilients dans l'Union, au renforcement du caractère européen des élections au Parlement européen et à une meilleure garantie de

leur bon déroulement[46],

– vu la recommandation (UE) 2023/2836 de la Commission du 12 décembre 2023 relative à la promotion de l'implication des citoyens et des organisations de la société civile dans les processus d'élaboration des politiques publiques et de leur participation effective à ces processus[47],

– vu le réseau européen de coopération en matière d'élections mis en place par la Commission en 2019,

– vu le communiqué de presse de la Commission du 13 novembre 2025 sur l'ouverture d'une enquête sur une possible violation du règlement sur les marchés numériques par Google, qui déclasserait le contenu des éditeurs de médias dans les résultats de recherche,

– vu les conclusions du Conseil du 21 mai 2024 sur l'avenir de la cybersécurité: mettre en œuvre et protéger ensemble,

– vu les conclusions du Conseil du 17 octobre 2022 sur la sécurité de la chaîne d'approvisionnement des TIC,

– vu la recommandation du Conseil du 8 décembre 2022 relative à une approche coordonnée à l'échelle de l'Union pour renforcer la résilience des infrastructures critiques[48],

– vu la décision (PESC) 2023/855 du Conseil du 24 avril 2023 relative à une mission de partenariat de l'Union européenne en Moldavie (EUPM Moldova)[49],

– vu le plan d'action intitulé «Une boussole stratégique en matière de sécurité et de défense – Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales», approuvé par le Conseil le 21 mars 2022 et par le Conseil européen le 25 mars 2022,

– vu les informations communiquées par la Lituanie, le Danemark, l'Estonie, la Finlande, l'Allemagne, la Lettonie, la Slovénie et l'Espagne en vue de la réunion du Conseil «Transports, télécommunications et énergie» du 6 juin 2025 réclamant des actions communes en réponse aux menaces de brouillage et d'usurpation des systèmes mondiaux de navigation par satellite (GNSS),

– vu l'accord interinstitutionnel du 20 mai 2021 entre le Parlement européen, le Conseil de l'Union européenne et la Commission européenne sur un registre de transparence obligatoire[50],

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

– vu le rapport spécial nº 05/2022 de la Cour des comptes européenne du 29 mars 2022 intitulé «Cybersécurité des institutions, organes et agences de l'UE – Un niveau de préparation globalement insuffisant par rapport aux menaces»,

– vu les principes mondiaux des Nations unies pour l'intégrité de l'information – recommandations pour une action multipartite, publiés le 24 juin 2024,

– vu le pacte international relatif aux droits civils et politiques, et notamment son article 20,

– vu la convention des Nations unies sur le droit de la mer du 10 décembre 1982, entrée en vigueur le 16 novembre 1994,

– vu les articles sur la responsabilité de l'État pour fait internationalement illicite, adoptés en novembre 2001,

– vu la déclaration de Reykjavik, adoptée lors du 4e sommet des chefs d'État et de gouvernement du Conseil de l'Europe, qui s'est tenu les 16 et 17 mai 2023,

– vu le mécanisme de réaction rapide du G7, établi lors du sommet du G7 à Charlevoix, qui s'est tenu les 8 et 9 juin 2018,

– vu le document de travail présenté le 13 juin 2025 à l'Organisation de l'aviation civile internationale par l'Estonie, la Finlande, la Lettonie, la Lituanie, la Pologne et la Suède sur l'interférence récurrente des radiofréquences GNSS dans les régions de la Baltique, de l'est et du nord de l'Europe et ses implications pour la sûreté et la sécurité de l'aviation civile internationale,

– vu le rapport sur les résultats finaux de la conférence sur l'avenir de l'Europe, publié le 9 mai 2022, et notamment ses propositions 27 et 37,

– vu l'étude commandée par la commission spéciale du Parlement sur le bouclier européen de la démocratie intitulée «Renforcer la résilience – Vers le bouclier européen de la démocratie», publiée en octobre 2025 par sa direction générale des droits des citoyens, de la justice et des affaires institutionnelles[51],

– vu les 1er, 2e et 3e rapports du Service européen pour l'action extérieure (SEAE) sur les menaces de manipulation de l'information et d'ingérence depuis l'étranger,

– vu le rapport de l'Agence de l'Union européenne pour la cybersécurité (ENISA) du 1er octobre 2025 intitulé «ENISA Threat Landscape 2025»,

– vu le rapport d'Europol intitulé «EU Serious and Organised Crime Threat Assessment – The changing DNA of serious and organised crime», publié en 2025,

– vu le rapport d'octobre 2025 du département de la coordination de la supervision algorithmique de l'autorité néerlandaise chargée de la protection des données intitulé «AI chatbots as voting aid»,

[51] Étude – «Renforcer la résilience – Vers le bouclier européen de la démocratie», Parlement européen, direction générale des droits des citoyens, de la justice et des affaires institutionnelles, département thématique chargé de la justice, des libertés civiles et des affaires institutionnelles, octobre 2025.

– vu les mesures adoptées par l'autorité italienne de régulation des communications (AGCOM) le 3 septembre 2025 concernant les influenceurs,

– vu le code de conduite en matière de publicité des influenceurs, adopté par AUTOCONTROL en Espagne le 7 juillet 2025,

– vu l'avertissement émis par l'agence nationale tchèque de cybersécurité et de sécurité de l'information (NÚKIB) le 3 septembre 2025 concernant les menaces en matière de cybersécurité liées au transfert de données vers la République populaire de Chine et ses régions administratives spéciales ainsi qu'à la gestion à distance de ces données,

– vu le rapport intitulé «Manipulation d'algorithmes et instrumentalisation d'influenceurs: enseignements de l'élection présidentielle en Roumanie & risques pour la France», publié par le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM) du gouvernement français en février 2025,

– vu le manuel sur les influenceurs publié par Mediapooli en Finlande en 2020,

– vu le rapport du département d'État américain d'août 2020 intitulé «Pillars of Russia's Disinformation and Propaganda Ecosystem»,

– vu l'avis conjoint en matière de cybersécurité émis en août 2025 par l'Agence américaine de cybersécurité et de sécurité des infrastructures, l'Agence de sécurité nationale des États-Unis, le FBI et des partenaires internationaux intitulé «Countering State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems»,

– vu le rapport de Reporters sans frontières du 25 septembre 2025 intitulé «The Propaganda Monitor: The Russian Edition»,

– vu l'article publié par le Centre pour le pluralisme et la liberté des médias à l'Institut universitaire européen le 1er novembre 2025 intitulé «Influencers as news creators: implications for media regulation»,

– vu l'article publié par le consortium AlgoSoc le 28 octobre 2025 intitulé «1 in 10 Dutch citizens are likely to ask AI for election advice. This is why they shouldn't»,

– vu le rapport de What to Fix de juin 2025 intitulé «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»,

– vu le rapport spécial de NewsGuard du 6 mars 2025 intitulé «A Well-funded Moscow-based Global "News" Network has Infected Western Artificial Intelligence with Russian Propaganda»,

– vu le rapport de Media Freedom Rapid Response intitulé «Mapping Media Freedom – Monitoring Report 2024», publié en février 2025,

– vu le rapport du Forum économique mondial de janvier 2025 intitulé «Global Cybersecurity Outlook 2025»,

– vu le rapport d'enquête publié par VSquare, Delfi Estonia et les médias partenaires le 26 février 2024 intitulé «Kremlin Leaks: Secret Files Reveal How Putin Pre-Rigged his Reelection»,

– vu le code de conduite éthique pour les influenceurs et les créateurs de contenus sur les médias sociaux, publié par l'Aspen Institute Deutschland en 2024,

– vu l'article publié par Debunk.org le 4 mai 2023 intitulé «Kremlin spent 1.9 billion USD on propaganda last year, the budget exceeded by a quarter»,

– vu la déclaration du ministère des affaires étrangères de la Fédération de Russie du 28 décembre 2024 sur les mesures prises en réponse au 15e train de sanctions de l'Union à l'encontre de la Russie, le ministère ayant annoncé l'extension de la liste des fonctionnaires et citoyens de l'Union interdits d'entrée dans le pays,

– vu l'article de l'agence de presse russe TASS du 28 décembre 2024 intitulé «Russia substantially expands blacklist of EU officials in response to sanctions – MFA»,

– vu la déclaration de TikTok de décembre 2024 sur la poursuite de la protection de l'intégrité de TikTok lors des élections roumaines,

– vu la déclaration du Conseil européen de l'industrie solaire du 30 avril 2025 intitulée «Restrict Remote Access of PV Inverters from High-Risk Vendors», dans laquelle il a mis en garde contre les risques pour la souveraineté énergétique de l'Europe dus aux capacités d'accès non réglementé et de contrôle à distance des onduleurs photovoltaïques provenant de fabricants non européens à haut risque,

– vu l'article 55 de son règlement intérieur,

– vu le rapport de la commission spéciale sur le bouclier européen de la démocratie (A10-0000/2025),

A. considérant que, le 12 novembre 2025, la Commission et la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité ont présenté une communication conjointe sur la mise en place du bouclier européen de la démocratie, qui définit une série de mesures visant à renforcer la position de démocraties fortes et résilientes dans l'ensemble de l'Union, à les protéger et à les promouvoir;

B. considérant que le Centre européen pour la résilience démocratique est la pièce maîtresse du bouclier européen de la démocratie; que les deux commissions spéciales du Parlement sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (INGE et INGE 2), avaient déjà demandé la mise en place d'une structure de l'Union pour lutter contre la manipulation de l'information et l'ingérence étrangères;

C. considérant que les récents rapports du SEAE sur les menaces liées aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger témoignent d'une compréhension de plus en plus pointue des méthodes, de l'infrastructure technique et des finalités des discours des acteurs malveillants, mais que cette compréhension de la situation n'a pas abouti à la création de mécanismes opérationnels durables qui permettent à l'Union de prendre des contre-mesures coordonnées en temps

utile; que le maillage institutionnel de l'Union est l'une des principales cibles des campagnes hostiles de manipulation de l'information; que l'Union pâtit d'une approche fragmentée de la lutte contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger et la désinformation, étant donné que les capacités d'action varient considérablement entre les États membres et qu'il manque un cadre stratégique global reliant les réponses opérationnelles au renseignement sur les menaces;

D. considérant que le réseau européen de coopération en matière d'élections, le système d'alerte rapide (SAR) et l'Observatoire européen des médias numériques (EDMO) sont des composantes précieuses de la résilience globale de l'Union face aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger et à la désinformation, mais que leur efficacité est considérablement limitée par l'absence d'une structure opérationnelle spécifique de l'Union habilitée à coordonner les activités de renforcement de la résilience et les mécanismes de réaction rapide et d'escalade reliant les capacités opérationnelles nationales à une coordination au niveau de l'Union;

E. considérant que les menaces que représentent les activités de manipulation de l'information et d'ingérence menées depuis l'étranger et la désinformation ne pèsent pas que sur les États membres à titre individuel, mais sont une attaque contre l'essence même du projet européen; que les opérations de manipulation de l'information et d'ingérence menées depuis l'étranger ciblent systématiquement les valeurs démocratiques fondamentales énoncées à l'article 2 du traité UE et le principe de processus décisionnels ouverts et transparents consacré à l'article 1 du traité UE, et portent atteinte aux intérêts de l'Union;

F. considérant que les États membres qui ont investi à titre individuel dans des structures opérationnelles spécifiques, dotées de statuts et de mandats clairs et disposant de ressources humaines et financières suffisantes, montrent ce qui est réalisable, notamment dans le cas de VIGINUM en France et de l'Agence suédoise de défense psychologique;

G. considérant que l'évolution rapide de l'intelligence artificielle (IA) et des technologies des hypertrucages dépasse la capacité d'adaptation des institutions nationales fragmentées; que sans réponses coordonnées de l'Union et sans capacités opérationnelles claires, les agresseurs auront toujours plus d'avance sur les défenseurs;

H. considérant que la convergence des premières étapes de la mise en œuvre du règlement sur les services numériques, du règlement sur les marchés numériques, du règlement sur l'intelligence artificielle et du règlement européen sur la liberté des médias est l'occasion de mettre en place des moyens de défense globaux contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger;

I. considérant que les sociétés démocratiques de l'Union sont de plus en plus ciblées par les menaces hybrides, la désinformation et les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, avec une intensité particulière dans la sphère numérique; que l'espace en ligne permet la prolifération de nouvelles techniques de manipulation, notamment: a) l'utilisation non authentique de médias sociaux au moyen de programmes logiciels automatisés, de faux comptes de médias sociaux et de l'utilisation d'usines à trolls, ainsi que l'amplification et les activités orchestrées par des

robots, b) l’utilisation de techniques de contrefaçon d’opinion et d’inondation pour influencer le débat public en ligne, c) la personnalisation, le suivi et le microciblage d’individus, d) les sites internet conçus pour imiter des sources officielles, e) l’amplification artificielle de contenus clivants, f) l’utilisation de contenus synthétiques, tels que les hypertrucages et d’autres contenus générés par l’IA, et g) les systèmes de recommandation conçus à dessein pour stimuler la participation par la polarisation;

J. considérant que les plateformes en ligne, lorsqu’elles décident de promouvoir ou non des contenus dans les flux d’un utilisateur, utilisent leurs connaissances sur les préférences et les vulnérabilités de chaque utilisateur, ce qui les rend plus influentes que les éditeurs traditionnels;

K. considérant que l’Union a récemment adopté un ensemble d’actes législatifs exhaustifs visant à mettre en place un espace en ligne sûr et transparent, dont le règlement sur les services numériques, le règlement relatif à la transparence et au ciblage de la publicité à caractère politique et le règlement sur l’IA; que ces actes constituent une avancée importante pour responsabiliser les plateformes numériques et protéger les processus démocratiques, renforcer la transparence et préserver la liberté d’expression; que leur mise en application demeure toutefois complexe;

L. considérant que l’utilisation de l’IA offre de nouvelles possibilités de renforcer la gestion et le contrôle des élections, par exemple grâce à la détection des activités inhabituelles et des comportements manipulateurs coordonnés; que l’utilisation de l’IA, notamment pour la création de modèles génératifs et d’hypertrucages, pose également d’importants problèmes sur les plans de l’intégrité de l’information et des processus électoraux; qu’il ressort d’informations crédibles qu’un réseau de désinformation basé à Moscou, connu sous le nom de «Pravda», a mené des activités d’infiltration de grands modèles de langage pour les alimenter de discours pro-Kremlin conçus pour imiter des formulations neutres et fondées sur des faits; que ces tactiques sont une évolution dangereuse des activités de manipulation de l’information et d’ingérence menées depuis l’étranger, car elles exploitent l’opacité et l’évolutivité des systèmes d’IA pour diffuser subtilement des messages géopolitiques faux ou trompeurs sous couvert d’un langage faisant autorité; que cette forme de manipulation algorithmique menace d’éroder la confiance du public dans les technologies d’IA, de fausser le discours démocratique et d’exacerber les risques de désinformation dans l’ensemble de l’Union et dans le monde; que cela met en avant la nécessité de renforcer la maîtrise de l’IA dans l’éducation, le monde du travail et la société dans son ensemble;

M. considérant que les influenceurs en ligne ont un rôle important à jouer dans le renforcement de la résilience numérique de nos sociétés en sensibilisant à l’éducation aux médias, en informant sur les procédures démocratiques ou en contribuant à un débat politique sain;

N. considérant que les élections présidentielles de l’automne 2024 en Roumanie ont révélé d’importantes vulnérabilités dans l’environnement de l’information en ligne, étant donné qu’il a été établi de façon crédible que des faux comptes, des robots et des contenus amplifiés par des algorithmes ont été utilisés pour promouvoir des discours politiques spécifiques; que TikTok, l’une des plateformes les plus populaires chez les jeunes électeurs, a affirmé avoir bloqué la création de plus de 116 000 comptes envoyant des messages indésirables et supprimé 59 000 faux comptes lors d’un

nettoyage après les élections; que le recours à des influenceurs, et notamment à des nanoinfluenceurs et à des micro-influenceurs, par des agents étrangers démontre que des acteurs peu coûteux et à faible visibilité peuvent être exploités pour influencer l'opinion publique, en violation des normes démocratiques, tout en passant sous les radars;

O. considérant que Telegram, une plateforme de messagerie dont le nombre d'utilisateurs dans l'Union est en hausse, est de plus en plus souvent signalée comme un vecteur de désinformation, d'ingérence étrangère et d'activités illicites, du fait notamment qu'elle diffuse des contenus extrémistes et de la propagande politique intraçable; que ses origines russes et l'absence de modération digne de ce nom des contenus suscitent des inquiétudes persistantes quant à son rôle dans l'affaiblissement du discours démocratique; que la plateforme Telegram est devenue un canal incontournable pour le recrutement d'«agents éphémères» et la conduite d'opérations hybrides; qu'il a été constaté que des acteurs étatiques malveillants exploitent les compétences technologiques, la fragilité financière et la naïveté des utilisateurs de Telegram, en particulier des jeunes, pour mener des opérations d'espionnage et de sabotage à un coût minime, tout en se ménageant la possibilité de fournir un démenti plausible; que Telegram atteindrait un nombre d'utilisateurs la faisant entrer dans la catégorie des très grandes plateformes en ligne au titre du règlement sur les services numériques, ce qui la soumettrait à des obligations réglementaires plus strictes et à des exigences d'atténuation des risques;

P. considérant que l'influence croissante des entreprises technologiques non européennes, en particulier celles établies aux États-Unis et en Chine, met en évidence les dépendances stratégiques de l'Union dans des domaines critiques tels que les infrastructures de données, les services en nuage et les plateformes de médias sociaux; que la promotion de l'innovation européenne, le soutien aux jeunes pousses européennes et les investissements dans des infrastructures numériques souveraines sont des étapes essentielles vers la mise en place d'un écosystème numérique de l'Union compétitif, sûr et résilient; que l'alignement de l'innovation numérique sur les valeurs démocratiques et les droits fondamentaux offre à l'Union l'occasion de devenir un acteur mondial de premier plan dans le domaine des technologies responsables et centrées sur l'humain;

Q. considérant que les recherches montrent une tendance inquiétante dans les programmes de redistribution des recettes des plateformes en ligne et ont ainsi révélé que des médias faisant l'objet de sanctions, tels que Sputnik et Russia Today, sont restés inscrits sur la liste des «éditeurs partenaires» de Facebook plusieurs mois après le lancement des sanctions de l'Union à l'encontre de la Russie, ce qui fait planer des doutes quant à la question de savoir si ces médias ont continué à retirer des bénéfices financiers de leurs activités; que ces mécanismes de monétisation opaques permettent aux acteurs étrangers affiliés à un État de tirer profit de la diffusion de désinformation et de continuer à déstabiliser les espaces d'information de l'Union malgré les mesures réglementaires prises;

R. considérant que, dans une enquête menée à l'approche des élections législatives de 2025 aux Pays-Bas, 1 répondant sur 10 a déclaré qu'il demandera probablement des conseils en matière de vote à l'IA, tandis que 13 % des répondants ont déclaré qu'ils pourraient peut-être recourir à l'IA; qu'aux Pays-Bas, plus d'un tiers des jeunes électeurs interrogés déclarent qu'ils utiliseront peut-être ou probablement l'IA; que cette tendance

est cohérente avec les observations faites dans les États membres et dans le monde; qu'il ressort d'une étude récente de l'autorité néerlandaise chargée de la protection des données que les recommandations de vote générées par les dialogueurs d'IA présentent souvent une vision fortement faussée et polarisée du paysage politique;

S. considérant que le droit fondamental à la liberté d'expression et d'information, consacré à l'article 11 de la charte des droits fondamentaux de l'Union européenne et à l'article 10 de la convention européenne des droits de l'homme, est une pierre angulaire de la démocratie; que la volonté de l'Union de défendre la liberté d'expression est une stratégie cohérente et fondée sur des principes de lutte contre les activités de manipulation de l'information et d'ingérence étrangères, qui contraste clairement avec les restrictions que les acteurs autoritaires imposent systématiquement à leurs populations; que la liberté et le pluralisme des médias, ainsi que l'existence d'un espace civique dynamique, donnent aux sociétés les moyens de détecter, de dénoncer et de rejeter les discours manipulateurs par la délibération démocratique;

T. considérant que la liberté d'expression et d'information est un droit fondamental conçu pour protéger les êtres humains, et non les machines, les robots et l'IA;

U. considérant que les acteurs se livrant à des activités de manipulation de l'information et d'ingérence depuis l'étranger exploitent les technologies pour orchestrer des campagnes de désinformation coordonnées et non authentiques; que ces technologies, notamment les robots et les programmes logiciels fondés sur l'IA, sont capables d'adopter un comportement autonome et, par la suite, de fausser et de détruire un véritable discours public, en inondant ainsi les propos de personnes réelles de contenus non authentiques;

V. considérant que la liberté et le pluralisme des médias, consacrés à l'article 11, paragraphe 2, de la charte des droits fondamentaux de l'Union européenne, sont des pierres angulaires du mode de vie européen; que le journalisme de qualité, indépendant sur le plan éditorial, est un puissant antidote aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger et à la désinformation;

W. considérant qu'en vertu du règlement sur les marchés numériques, les développeurs d'applications qui distribuent leurs applications par l'intermédiaire de boutiques d'applications devraient pouvoir informer gratuitement les clients sur d'autres offres en dehors des boutiques d'applications; que la Commission a ouvert une enquête sur une possible violation du règlement sur les marchés numériques par Google, qui déclasserait le contenu des éditeurs de médias dans les résultats de recherche; que la Commission a lancé son premier réexamen du règlement sur les marchés numériques le 3 juillet 2025;

X. considérant que la directive «Services de médias audiovisuels» impose aux États membres de prendre des mesures pour développer les compétences en matière d'éducation aux médias et de rendre compte tous les trois ans des mesures prises;

Y. considérant que Media Freedom Rapid Response a recensé 1 548 violations de la liberté de la presse en 2024, allant de menaces juridiques, physiques et psychologiques à des formes de censure, visant 2 567 personnes ou entités liées aux médias dans 35 pays européens, ce qui constitue une augmentation alarmante en comparaison des 1 153 violations enregistrées en 2023;

Z. considérant que, le 11 décembre 2025, les négociateurs du Parlement et du Conseil sont parvenus à un accord provisoire sur la proposition de règlement relatif au filtrage des investissements étrangers dans l'Union;

AA. considérant que les travaux de Radio Free Europe/Radio Liberty présentent un intérêt stratégique pour l'Union; que l'Union a approuvé un financement d'urgence de 5,5 millions d'euros pour ces travaux, à la suite de la réforme de la politique d'aide étrangère des États-Unis; qu'il convient de mettre au point une solution de financement durable pour Radio Free Europe/Radio Liberty;

AB. considérant que les nouvelles technologies, telles que l'IA, peuvent améliorer les conditions et les méthodes de travail des journalistes, mais peuvent également exposer ces derniers à de nouvelles menaces, telles que l'usurpation rapide et peu coûteuse de l'identité des médias existants, la création massive de médias de désinformation et les attaques coordonnées contre les journalistes;

AC. considérant que la guerre d'agression menée actuellement par la Russie contre l'Ukraine illustre le rôle vital que joue la société civile lorsque des communautés se trouvent dans des situations de crise, en particulier lorsqu'il s'agit de fournir une aide humanitaire, de satisfaire des besoins fondamentaux et de permettre aux populations touchées de continuer à vivre au quotidien;

AD. considérant que la société civile joue également un rôle essentiel en contribuant à l'élaboration des politiques, en fournissant des services sociaux et communautaires, en informant sur des questions sociales importantes, en représentant divers groupes en situation de vulnérabilité et en promouvant et protégeant les droits fondamentaux des citoyens;

AE. considérant que la Commission a publié sa stratégie de l'Union pour la société civile, qui viendrait compléter les actions prévues dans la communication conjointe sur le bouclier européen de la démocratie; que la stratégie de l'Union pour la société civile confirme que la plateforme de la société civile, dont la Commission a annoncé la création dans le cadre de la mise en œuvre de la stratégie, visera à fournir un cadre régulier et structuré pour la protection et la promotion des valeurs de l'Union ainsi que pour la rationalisation et le renforcement de l'engagement en faveur des droits fondamentaux, de la démocratie, de l'égalité et de l'état de droit, et qu'elle sera opérationnelle en 2026; que la stratégie comprend également la création d'un pôle de connaissances en ligne sur l'espace civique, qui devrait répertorier les initiatives qui existent en matière de surveillance de l'espace civique, des rapports et des ressources de protection, aux niveaux national, européen et international, en coopération avec l'Agence des droits fondamentaux de l'Union européenne;

AF. considérant que le programme «AgoraEU», proposé par la Commission pour le cadre financier pluriannuel (CFP) 2028-2034, constitue une avancée importante pour le renforcement du soutien de l'Union à la culture, aux médias et à la société civile, avec un budget prévu de 9 milliards d'euros;

AG. considérant que les attaques hybrides visant des infrastructures critiques de l'Union sont devenues plus fréquentes que jamais, avec des incidents liés aux mêmes acteurs malveillants, à savoir la Russie et la Chine, mais aussi l'Iran et la Corée du Nord; que ces attaques ciblent souvent des systèmes, des réseaux et des installations indispensables

au fonctionnement même d'une société, notamment ceux liés à la sécurité publique, à la sûreté et à la stabilité économique; que ces attaques prennent diverses formes, telles que le sabotage physique, les incendies criminels, l'espionnage et le brouillage de signaux, ainsi que les cyberattaques et d'autres activités relevant de «zones grises», qui révèlent toutes un effort coordonné visant à tester, perturber et compromettre la sécurité et la résilience sociétale de l'Union;

AH. considérant que la mer Baltique a été le théâtre d'une augmentation sans précédent du nombre de ruptures de câbles sous-marins, indispensables aux connexions internet et à l'approvisionnement en électricité dans l'ensemble de la région de la Baltique et de la région nordique; que, depuis 2023, au moins onze cas de dégradation de câbles ont été enregistrés, ce qui suggère un sabotage coordonné;

AI. considérant qu'au cours des derniers mois, de multiples violations de l'espace aérien et incursions non autorisées de drones ont été signalées dans plusieurs États membres de l'Union et alliés voisins de l'OTAN, dont la Pologne, les États baltes, la Roumanie, le Danemark, la Suède, l'Allemagne, la Belgique et la Norvège; qu'un certain nombre de ces incidents ont été clairement attribués à des avions militaires et des drones russes, tandis que d'autres incidents, impliquant des objets aériens non identifiés, font toujours l'objet d'une enquête, mais sont largement soupçonnés de relever du même schéma d'intimidation et de déstabilisation hybrides dirigé contre l'Europe;

AJ. considérant que plusieurs pays européens, dont la France, l'Estonie, l'Allemagne, la Tchéquie et la Norvège, ont récemment été confrontés à des cyberattaques majeures ciblant des systèmes gouvernementaux, des infrastructures critiques et des entreprises privées, attribuées aux services de renseignement militaire russes et à des acteurs liés à l'État chinois, et que cela souligne l'urgence de renforcer les capacités collectives de cyberrésilience et d'imputation de cyberattaques de l'Union;

AK. considérant que la dépendance de l'Union à l'égard d'acteurs étrangers et de technologies d'origine étrangère dans les infrastructures critiques et les chaînes d'approvisionnement demeure une préoccupation majeure et constitue l'une des vulnérabilités les plus importantes de l'Union; que cette situation est particulièrement répandue dans les secteurs des technologies et du numérique, ce qui représente un défi majeur pour la cybersécurité;

AL. considérant que les outils de droit pénal peuvent contribuer au bouclier européen de la démocratie dans la mesure où les activités concernées constituent des infractions pénales;

AM. considérant que les mécanismes de coopération judiciaire et policière et les outils d'échange transfrontière d'informations doivent être adaptés et renforcés, compte tenu des défis grandissants que l'ingérence étrangère fait peser sur la sécurité intérieure de l'Union;

AN. considérant que l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) a mis en garde, dans son dernier rapport d'évaluation de la menace que représente la grande criminalité organisée dans l'Union (SOCTA UE), publié en mars 2025, contre la participation d'organisations criminelles à des campagnes hybrides; que la communication de la Commission sur ProtectEU reconnaît que divers facteurs empêchent Europol d'exploiter pleinement son potentiel opérationnel de

soutien aux activités visant à lutter contre la criminalité transfrontière, notamment les lacunes dans le mandat de l'Agence en ce qui concerne les nouvelles menaces pour la sécurité, en particulier le sabotage, les menaces hybrides et la manipulation de l'information;

AO. considérant que la Commission s'est engagée à lancer une réforme qui fera d'Europol une agence de police véritablement opérationnelle; que les agents de police sont des partenaires essentiels dans la sauvegarde des institutions démocratiques; que cet aspect devrait être plus clairement reconnu dans les politiques pertinentes;

AP. considérant que les États membres peuvent demander à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) d'aider les autorités nationales à traiter tout type de comportement illégal relevant de leur compétence; que la coopération judiciaire peut s'avérer particulièrement complexe lorsqu'elle s'étend à de nouveaux domaines d'activités criminelles, ce qui nécessite une modernisation de la boîte à outils juridique;

AQ. considérant que les agences de l'Union chargées de la gestion des frontières, de la migration et de l'asile, à savoir l'Agence européenne de garde-frontières et de garde-côtes (Frontex) et l'Agence de l'Union européenne pour l'asile, ont un rôle clé à jouer, en coopération avec les autorités nationales, pour établir et maintenir une connaissance commune de la situation en ce qui concerne les risques liés à l'exploitation des flux migratoires à des fins politiques; qu'elles doivent également aider les États membres situés en première ligne lors de situations de crise; que la Commission a inclus le renforcement de Frontex dans ses initiatives phares pour la législature 2024-2029;

AR. considérant que les pays candidats et les pays voisins de l'Union, notamment l'Ukraine, la Moldavie et les Balkans occidentaux, restent fortement exposés aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger ainsi qu'aux menaces hybrides, et qu'ils ont besoin du soutien de l'Union pour renforcer leur résilience civique et institutionnelle;

AS. considérant que la guerre d'agression menée par la Russie contre l'Ukraine et la posture géopolitique affirmée de la Chine ont intensifié le recours à la désinformation, à la coercition économique et à l'influence stratégique, ciblant non seulement l'Union, mais aussi des régions vulnérables telles que les Balkans occidentaux, les pays partenaires d'Europe orientale et le Sud global; que plusieurs sources révèlent que le budget de la Russie consacré à la diffusion de la désinformation et de la propagande s'élève à un montant compris entre 1 et 2 milliards de dollars par an; que les élections et les événements politiques à travers l'Europe témoignent de l'existence d'une guerre hybride offensive à grande échelle, persistante, ciblée et sophistiquée, menée par la Russie, visant à entamer la confiance dans nos systèmes et institutions politiques et à entretenir une confusion constante entre les faits et les fausses informations; qu'une telle guerre nécessite une réponse appropriée et un passage d'une stratégie purement défensive à une stratégie offensive;

AT. considérant que la mission de partenariat de l'Union européenne en République de Moldavie (EUPM Moldova) a été créée le 24 avril 2023 dans le but clair d'aider les autorités moldaves à lutter contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger;

AU. considérant que l’affaiblissement du soutien des États-Unis à la démocratie internationale a créé un déficit de financement important au niveau mondial pour lutter contre la désinformation et l’influence autoritaire;

AV. considérant que des initiatives internationales, notamment celles menées par les Nations unies, l’Organisation de coopération et de développement économiques et le G7, ont commencé à définir des principes et des cadres pour préserver l’intégrité de l’information, fondés sur les valeurs démocratiques, le pluralisme des médias et les droits de l’homme;

AW. considérant que les activités de manipulation de l’information et d’ingérence menées depuis l’étranger constituent un enjeu grandissant pour la résilience démocratique de l’Union; que certaines formes d’activités de manipulation de l’information peuvent également provenir d’acteurs opérant au sein de l’Union; qu’il convient d’examiner et de comprendre plus avant le phénomène de manipulation de l’information et d’ingérence dans le contexte national, en particulier dans son interaction avec les activités de manipulation de l’information et d’ingérence menées depuis l’étranger; que les mesures présentées pour lutter contre les activités de manipulation de l’information et d’ingérence menées depuis l’étranger contribuent également à accroître la résilience globale des sociétés dans le contexte national, en particulier en ce qui concerne l’amélioration de la connaissance de la situation, le renforcement de la transparence et du pluralisme, et le développement des niveaux d’éducation aux médias et d’habileté numérique au sein de toutes les catégories d’âge;

AX. considérant que les recommandations de la Commission relatives aux processus électoraux inclusifs et résilients dans l’Union, publiées en décembre 2023, doivent encore être pleinement mises en œuvre dans tous les États membres, notamment les dispositions visant à renforcer la coopération entre les autorités nationales pendant et avant les processus électoraux par la mise en place de réseaux électoraux nationaux;

AY. considérant que le réseau européen de coopération en matière d’élections a joué un rôle de plus en plus important ces dernières années, mais qu’il ne dispose actuellement pas des ressources et des capacités nécessaires pour porter ses activités à un niveau supérieur;

AZ. considérant que les pays candidats ont été invités à participer aux réunions du réseau européen de coopération en matière d’élections; qu’outre cette participation, il existe encore un potentiel considérable pour améliorer davantage la coopération avec ces pays dans le cadre des activités du réseau, pour tirer des enseignements mutuels des expériences rencontrées face aux menaces et d’échanger de bonnes pratiques en matière de lutte contre ces menaces;

BA. considérant qu’il est manifestement nécessaire de renforcer la protection des infrastructures électorales et des partis politiques nationaux, qui ont également fait l’objet de cyberattaques, notamment à la lumière des cyberattaques à grande échelle ayant visé les autorités électorales roumaines à l’automne 2024;

BB. considérant que les financements occultes de partis et de mouvements politiques dans l’Union par des pays tiers constituent une menace pour la légitimité du processus démocratique;

BC. considérant que l’indépendance de la justice est une composante structurelle indispensable de l’intégrité électorale; que l’intégrité électorale dépend de l’existence de voies de recours accessibles et efficaces contre les violations des droits de vote, ainsi que de procédures électorales, à l’abri des pressions politiques et des pressions du pouvoir exécutif;

BD. considérant qu’au total, entre 2022 et 2025, l’Union a imposé 19 trains de sanctions de grande ampleur et sans précédent en réponse à l’agression militaire menée par la Russie contre l’Ukraine, qu’elle a ainsi considérablement augmenté la pression sur l’économie de guerre russe, en ciblant des secteurs essentiels tels que l’énergie, la finance et l’industrie de la défense, des zones économiques spéciales, ainsi que des complices et des profiteurs de sa guerre d’agression, et en mettant fin à la dépendance de l’Union à l’égard des importations de combustibles fossiles en provenance de Russie; que l’Union a également adopté des sanctions à l’encontre de la Biélorussie, de l’Iran et de la Corée du Nord en réponse au soutien qu’ils ont apporté à l’agression militaire menée par la Russie contre l’Ukraine.

BE. considérant que, depuis le 8 octobre 2024, le cadre de sanctions de l’Union a permis de cibler un large éventail d’activités hybrides menées par la Russie, notamment la perturbation des processus électoraux et du fonctionnement des institutions démocratiques, les menaces contre les activités économiques, les services d’intérêt public et les infrastructures critiques, ainsi que leur sabotage, le recours à la désinformation coordonnée et aux activités de manipulation de l’information et d’ingérence menées depuis l’étranger, les actes de cybermalveillance, l’instrumentalisation des migrants et d’autres activités déstabilisatrices; que ce cadre a déjà conduit à sanctionner des dizaines de personnes et d’entités, y compris des oligarques, des propagandistes, des agents du renseignement militaire, des médias et des entreprises russes, pour avoir diffusé des discours pro-Kremlin, mené des actes de sabotage et porté atteinte aux processus démocratiques; que des mesures connexes permettent désormais à l’Union d’inclure le gel des avoirs, l’interdiction de voyager et la suspension des licences de radiodiffusion, ainsi que d’interdire les transactions financières et les transactions sur crypto-actifs liées à des activités hybrides;

BF. considérant que, le 28 décembre 2024, le gouvernement russe a annoncé avoir «considérablement élargi» sa liste noire de citoyens et de fonctionnaires de l’Union, notamment à des représentants des institutions de l’Union, des gouvernements nationaux, des services répressifs et des organisations commerciales; que cette liste noire, qui cible les personnes promouvant les valeurs démocratiques et s’opposent à l’agression russe en Ukraine, vise à intimider et à faire taire certaines voix au moyen de restrictions opaques et arbitraires, souvent sans aucune notification formelle, justification, ni droit de recours;

BG. considérant que les menaces hybrides, l’ingérence étrangère et les campagnes de désinformation se sont muées en crises complexes, à grande échelle et intersectorielles, ayant des effets néfastes sur la sûreté et la sécurité, le bien-être des citoyens et le fonctionnement de la société et de l’économie dans son ensemble; que cela constitue un défi majeur pour les affaires intérieures de l’Union et déstabilise les institutions démocratiques dans l’ensemble des États membres, comme le montre l’agression de la Russie contre l’Ukraine;

BH. considérant qu'une préparation civile et militaire efficace nécessite une approche globale, intégrant l'ensemble de la société, l'ensemble du gouvernement et tous les types de risques; que cette approche doit associer les autorités nationales des États membres, les institutions, organes et organismes de l'Union, ainsi que les entreprises, les universités, la société civile et les citoyens; que cet effort doit s'accompagner d'investissements à long terme, d'une prospective stratégique et de l'intégration de la résilience dans l'élaboration des politiques, le développement des infrastructures, les systèmes éducatifs et les chaînes d'approvisionnement;

BI. considérant que l'autonomisation des citoyens est essentielle à la résilience de la société et que la préparation doit inclure des outils concrets tels qu'une application d'alerte de crise à l'échelle de l'Union, un livret sur la préparation des ménages, ainsi que des campagnes de sensibilisation de grande envergure promouvant l'autosuffisance et la préparation aux crises;

BJ. considérant que la coopération civilo-militaire, les capacités à double usage et l'intégration de la préparation dans les programmes pédagogiques sont essentielles pour améliorer la préparation en matière de défense au moyen d'une formation ciblée, non seulement pour les travailleurs des secteurs critiques, tels que les pompiers, le personnel de santé et les fonctionnaires, mais aussi pour les acteurs de la société civile et le grand public;

BK. considérant que la souveraineté technologique et des écosystèmes numériques sécurisés, notamment des projets tels qu'IRIS² et le système de communication critique européen, sont indispensables pour maintenir le contrôle sur les canaux de communication essentiels et renforcer les infrastructures critiques;

BL. considérant que la préparation dépend de la fluidité de la coopération entre les institutions, les agences, les États membres et les partenaires internationaux de l'Union, complétée par des exercices et des formations communs, des plateformes partagées sur la compréhension de la situation et un échange rapide d'informations;

BM. considérant que, pour parvenir à une résilience crédible et à un niveau suffisant de préparation civile et de défense, il est nécessaire de recourir à des investissements massifs, de renforcer la base technologique et industrielle de l'Europe et de réduire les dépendances stratégiques; que cet effort nécessite d'explorer de nouveaux mécanismes de financement ciblés;

Introduction

1. se félicite de la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité sur la mise en place d'un bouclier européen de la démocratie, ainsi que des efforts continus visant à s'appuyer sur les travaux déjà entrepris dans le cadre du plan d'action pour la démocratie européenne et du train de mesures de défense de la démocratie; est d'avis que la mission principale du bouclier européen de la démocratie devrait être de protéger la démocratie européenne contre les menaces extérieures et, à terme, de contribuer à la sauvegarde du mode de vie européen, de l'état de droit et des valeurs consacrées à l'article 2 du traité UE;

2. constate avec inquiétude la complexité grandissante ainsi que l'évolution du panorama de menaces auquel l'Union et ses États membres sont confrontés, qui se caractérise par des activités de manipulation de l'information et d'ingérence menées depuis l'étranger, des attaques hybrides et des campagnes de désinformation orchestrées par des acteurs malveillants de pays tiers; précise qu'il s'agit d'actions hostiles qui sapent les fondements démocratiques de l'Union en semant la division, en minant la confiance du public dans les institutions et en exploitant les vulnérabilités de la société, en s'appuyant souvent sur des technologies numériques avancées;

3. considère la Russie comme la principale menace extérieure pesant sur l'intégrité démocratique de l'Europe; réitère sa position selon laquelle la Russie est un État soutenant le terrorisme; explique qu'il est urgent de mettre en place une stratégie globale, cohérente et tournée vers l'avenir pour résoudre efficacement ces difficultés et préserver la démocratie européenne;

4. réaffirme sa conviction que les principales priorités stratégiques définies dans l'initiative du bouclier européen de la démocratie, notamment la lutte contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger et les menaces hybrides, le renforcement de la résilience électorale, l'amélioration de la cybersécurité, le soutien à la société civile, ainsi que la promotion du journalisme indépendant et d'investigation, doivent être pleinement intégrées et bénéficier de financements suffisants dans le prochain CFP;

Centre européen pour la résilience démocratique

5. se félicite de la proposition de la Commission relative à un Centre européen pour la résilience démocratique (ci-après, le «Centre»), dont la création constitue une étape nécessaire et logique vers un renforcement de la coordination des efforts destinés à faire face à l'évolution des menaces communes, en particulier les activités de manipulation de l'information et d'ingérence menées depuis l'étranger et la désinformation; prend acte de son approche consistant à introduire progressivement des fonctions et des opérations, y compris en augmentant peu à peu la participation des États membres; se réjouit du fait que la Commission ait assuré qu'elle travaille déjà à la mise en place du Centre sous la direction du commissaire à la démocratie, à la justice, à l'état de droit et à la protection des consommateurs, avec l'objectif clair de garantir qu'il soit opérationnel dans le courant de l'année 2026; salue l'engagement pris par la Commission de régulièrement informer le Parlement et de l'associer au processus de mise en œuvre du bouclier européen de la démocratie et du Centre;

6. rappelle toutefois que la proposition n'inclut pas suffisamment de détails opérationnels, de dotations budgétaires claires, de structure de gouvernance spécifique, de mandat concret, ni de calendrier; note que la communication conjointe sur le bouclier européen de la démocratie ne relie explicitement le centre à aucune des actions qui y sont décrites, lesquelles demeurent réparties dans différents cadres administratifs au sein de la Commission et du SEAE; se déclare préoccupé par le fait que si le Centre ne devient qu'un pôle, un réseau, une plateforme ou cadre de plus parmi d'autres, cela pourrait encore entamer la capacité de l'Union à utiliser efficacement l'ensemble des outils disponibles à ce jour et aggraver les lacunes recensées dans la communication conjointe, notamment la réduction de la réactivité, la fragmentation et les budgets serrés;

7. se félicite que la communication conjointe fournisse une cartographie détaillée des cadres, des structures, des outils, des initiatives et des programmes existants en matière de lutte contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, de lutte contre la désinformation et de renforcement de la résilience, et qu'elle dresse une liste des actions que la Commission et le SEAE se sont engagés à entreprendre; invite la Commission et le SEAE à proposer un calendrier clair pour leur mise en place progressive et leur intégration au sein du Centre, en fixant l'année 2026 comme date limite pour cette intégration; demande que cette intégration comprenne des mécanismes pertinents de surveillance et d'application du règlement sur les services numériques (DSA), en particulier dans le but d'identifier et de réduire au minimum les risques systémiques, de coordonner les efforts de lutte contre les campagnes de manipulation de l'information, de garantir la responsabilité opérationnelle d'un système d'alerte rapide (SAR) renforcé, ainsi que la maintenance et l'exploitation d'une base de données unifiée de renseignements sur les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, et de développer, entre autres, la ressource EUvsDisinfo, le réseau européen de coopération en matière d'élections et le groupe de travail de la Commission sur la désinformation et la communication stratégique;

8. se félicite que la Commission reconnaisse la nécessité de dialoguer avec les États membres et le Parlement sur le mandat, la structure et les méthodes de travail du Centre; invite la Commission à lancer le processus en proposant, d'ici au deuxième trimestre de 2027, une base juridique pour créer le Centre en tant qu'entité de l'Union dotée d'un statut institutionnel et d'un positionnement clairs, d'une structure de gouvernance et de mécanismes de contrôle parlementaire; précise que la clarté institutionnelle est essentielle pour permettre au Centre d'agir avec détermination tout en continuant à répondre de ses actes;

9. invite la Commission à doter le Centre d'un mandat et de mécanismes décisionnels clairs, lui permettant ainsi de fonctionner comme un centre d'excellence indépendant pour la détection et l'analyse des activités de manipulation de l'information et d'ingérence menées depuis l'étranger et des opérations de désinformation, en tant que plateforme de renforcement des capacités établissant des définitions, des normes, des formations et des outils techniques communs à l'échelle de l'Union, et en tant que pilier opérationnel assurant une coordination en temps réel du soutien technique dans la lutte contre les campagnes actives de manipulation de l'information;

10. invite la Commission à garantir que le Centre soit chargé de préserver l'intégrité des processus démocratiques au niveau de l'Union; réaffirme que les structures opérationnelles des États membres constituent une première ligne de défense; souligne toutefois que leur responsabilité première ne saurait à elle seule couvrir l'ensemble des intérêts légitimes de l'Union en matière de lutte contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger et la désinformation; demande à la Commission de préciser que le Centre doit poursuivre des objectifs doubles et qui se soutiennent réciproquement, à savoir coordonner les activités des États membres dans ce domaine et renforcer leurs capacités opérationnelles, ainsi que protéger les intérêts démocratiques de l'Union;

11. demande aux États membres ne disposant pas de structures opérationnelles dédiées de mettre en place ou de renforcer considérablement, avec le soutien du Centre, des institutions nationales spécifiquement chargées de détecter et de lutter contre les

activités de manipulation de l'information et d'ingérence menées depuis l'étranger et la désinformation; invite la Commission à établir une feuille de route pour le développement des capacités des États membres;

12. demande à la Commission d'évaluer la faisabilité d'habiliter le Centre à gérer et à allouer les subventions dédiées de l'Union dans le cadre des programmes pertinents de l'Union, notamment le programme pour une Europe numérique, le mécanisme pour l'interconnexion en Europe, Horizon Europe, le programme «Citoyens, égalité, droits et valeurs» (CERV) et la proposition de programme AgoraEU, et à l'autoriser à lancer des appels à propositions, ainsi qu'à sélectionner, superviser et évaluer des projets liés à des domaines relevant de son mandat, en particulier l'EDMO, les initiatives en matière d'éducation aux médias et d'autres initiatives européennes, régionales et transfrontières pertinentes consacrées à la lutte contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, au renforcement de la résilience démocratique et à la promotion de l'intégrité de l'information;

13. invite la Commission à prévoir une ligne budgétaire spécifique de l'Union pour les opérations du Centre, avec une distinction claire entre les financements opérationnels et les coûts généraux de coordination; demande à la Commission de garantir des ressources humaines suffisantes et un financement transitoire à partir des budgets existants afin de permettre la réalisation des travaux préparatoires avant le CFP 2028-2034;

14. invite la Commission à évaluer la faisabilité de la mise en place d'un mécanisme de financement destiné à compléter la ligne budgétaire consacrée aux activités du Centre, fondé sur des contributions des très grandes plateformes en ligne; rappelle que le secteur bancaire finance des mécanismes de résolution bancaire, que les entreprises pharmaceutiques soutiennent la surveillance de la sécurité, et que les industries polluantes supportent des coûts environnementaux; demande la mise en place d'un mécanisme par lequel les plateformes de réseaux sociaux contribuent de manière proportionnelle aux infrastructures nécessaires pour lutter contre les influences extérieures négatives et les risques systémiques liés à leurs services, tant en ce qui concerne les activités de manipulation de l'information et d'ingérence menées depuis l'étranger et la désinformation que le renforcement de la résilience; précise que de telles contributions seraient non seulement conformes aux principes européens établis en matière de responsabilité et d'obligation de rendre des comptes, mais qu'elles garantiraient également que les coûts de protection du discours démocratique soient partagés entre les acteurs qui tirent le plus profit de l'écosystème de l'information numérique;

Résilience numérique

15. demande la mise en œuvre complète, dans tous les États membres, des principaux actes législatifs dans le domaine numérique, tels que le règlement sur les services numériques (DSA), le règlement relatif à la transparence et au ciblage de la publicité à caractère politique et le règlement sur l'IA; est d'avis que la mise en œuvre continue de la législation numérique devrait mettre davantage l'accent sur la lutte contre la désinformation en ligne, la garantie de l'intégrité de l'information et la protection du discours démocratique en période électorale; s'inquiète, à cet égard, du fait que les retards dans l'adoption des lignes directrices et des normes techniques constituent un

obstacle à la mise en œuvre en temps utile du règlement sur l'IA; se félicite que, dans sa proposition de train de mesures omnibus sur le numérique visant à simplifier le règlement sur l'IA, la Commission cherche à remédier à cette situation en liant le calendrier de mise en œuvre des règles relatives aux systèmes d'IA à haut risque à la disponibilité de normes ou d'autres outils de soutien;

16. se félicite que le code de bonnes pratiques contre la désinformation, à caractère non contraignant, ait été officiellement intégré dans le cadre du règlement sur les services numériques (DSA); estime que l'utilisation non authentique des réseaux sociaux, par exemple au moyen de robots, de faux comptes, d'algorithmes polarisants ainsi que d'activités et d'une amplification artificielles, constitue l'une des menaces les plus graves pour le discours libre et ouvert en ligne, en particulier en période électorale; demande instamment à toutes les très grandes plateformes en ligne et à tous les très grands moteurs de recherche en ligne opérant dans l'Union de se conformer pleinement au code, et invite instamment la plateforme X à y adhérer à nouveau;

17. se félicite de l'engagement pris par la Commission d'élaborer un protocole d'incident et de crise au titre du DSA afin de mieux faire face aux incidents majeurs et aux ingérences dans l'environnement de l'information; estime que ce protocole devrait, entre autres, s'attaquer aux ingérences électorales reposant sur des comportements non authentiques coordonnés dans l'espace en ligne, en particulier au moyen d'une amplification et d'activités orchestrées par des robots, qui altèrent effectivement le discours public authentique;

18. constate que la Commission a terminé son enquête sur le manquement de la plateforme X à ses obligations de transparence prévues par le DSA, et qu'elle s'est suivie de l'imposition d'une amende de 120 millions d'euros; prie instamment la Commission d'accélérer les enquêtes restantes sur les violations présumées de la législation numérique de l'Union, y compris celles qui comportent des ingérences électorales, une opacité algorithmique ou la prolifération de faux comptes et de robots; invite, en particulier, la Commission à achever rapidement les enquêtes sur le respect par TikTok du DSA dans le contexte des élections présidentielles roumaines de 2024, notamment de son obligation d'atténuer les risques systémiques pesant sur les processus démocratiques;

19. invite la Commission et les autorités de réglementation compétentes à enquêter sur les campagnes de désinformation dissimulées visant à exploiter les systèmes d'IA générative, comme les activités du réseau «Pravda» basé à Moscou, et à les dénoncer publiquement; demande instamment aux fournisseurs de systèmes d'IA d'enrayer et d'atténuer dûment ce phénomène à l'aide de leurs systèmes de gestion des risques liés à l'IA; demande, en outre, que l'élaboration de normes de sécurité pour les fournisseurs de grands modèles de langage soit coordonnée au niveau international, afin de garantir une plus grande transparence en ce qui concerne les sources de données d'entraînement;

20. demande à la Commission d'achever d'urgence son évaluation de la base d'utilisateurs et des fonctionnalités de Telegram en vue de trancher quant à sa classification en tant que très grande plateforme en ligne, au titre du DSA; prie instamment la Commission et les autorités compétentes d'enquêter sur la potentielle contribution de Telegram au soutien d'activités criminelles, de l'ingérence électorale et de la diffusion de la désinformation au sein de l'Union; encourage en outre vivement la plateforme à adhérer

au code de bonnes pratiques contre la désinformation, à caractère non contraignant, et à se conformer pleinement aux exigences de l'Union en matière de transparence, de modération des contenus et d'accès aux données afin de garantir des conditions de concurrence équitables et de préserver la confiance des citoyens dans l'espace de l'information numérique;

21. recommande d'examiner plus avant le rôle des influenceurs, notamment des nano-influenceurs et des micro-influenceurs, dans la construction du discours public et dans l'influence sur les élections, tant pour ceux qui luttent contre les campagnes de désinformation étrangères que pour ceux qui y contribuent, que ce soit sciemment ou non; souligne, à cet égard, la nécessité de normes solides en matière de transparence et d'intégrité de l'information pour les créateurs de contenus politiques en ligne, en particulier les influenceurs qui opèrent dans une zone grise entre la promotion commerciale et la communication politique; se félicite des codes de conduite, des formations et des autres initiatives existants, qui ont été élaborés pour accroître la responsabilité des médias sociaux et des influenceurs et améliorer la transparence en la matière;

22. estime qu'une infrastructure numérique européenne, y compris des centres de données locaux sécurisés et des capacités souveraines de l'Union en matière d'informatique en nuage et d'informatique de périphérie, constitue un pilier stratégique de la résilience numérique, garantissant que les données sensibles des Européens ne sont pas stockées dans des centres de données étrangers; invite la Commission à proposer une définition du nuage souverain et de son champ d'application dans le projet de législation sur le développement de l'informatique en nuage et de l'IA; demande à la Commission de réfléchir aux discussions infructueuses sur le système européen de certification de cybersécurité pour les services d'informatique en nuage et de proposer une solution concrète dans la révision du règlement sur la cybersécurité, en tenant compte des préoccupations en matière de cybersécurité et de souveraineté liées à une concentration du pouvoir; réclame la mise en place de sas réglementaires et de mécanismes de financement pour soutenir l'innovation des start-up technologiques de l'Union, en particulier dans les secteurs qui présentent des dépendances critiques; soutient en outre la vision à long terme des plateformes de réseaux sociaux de l'Union conçues conformément aux valeurs européennes de transparence, de protection des données, de liberté d'expression et de responsabilité démocratique;

23. invite la Commission, les régulateurs numériques de l'Union et les plateformes en ligne à garantir la transparence des programmes de redistribution des revenus qui pourraient permettre aux acteurs de la manipulation de l'information et de l'ingérence étrangères, voire aux entités figurant sur la liste des sanctions, de percevoir des revenus; estime que la monétisation des activités de manipulation de l'information et d'ingérence menées depuis l'étranger dans le cadre de tels programmes devrait être prise en compte dans les obligations d'évaluation et d'atténuation des risques prévues par le DSA;

24. prend acte avec inquiétude des conclusions de l'autorité néerlandaise de protection des données, indiquant que les agents conversationnels fondés sur l'IA peuvent fournir des conseils de vote biaisés et non fiables, ce qui présente des risques pour l'intégrité électorale; invite la Commission à tenir son engagement d'élaborer des orientations sur l'utilisation de l'IA dans les processus électoraux afin de garantir une utilisation responsable de l'IA;

Liberté d'expression

25. souligne que le bouclier européen de la démocratie doit protéger et défendre la liberté d'expression et d'information en tant que droit fondamental applicable tant aux espaces hors ligne qu'aux espaces en ligne; explique que le niveau de protection des droits de l'homme dans l'Union compte parmi les plus solides au monde, et que les entreprises qui souhaitent exercer leurs activités dans l'environnement de l'Union et attirer des clients européens ont donc la responsabilité commune de préserver ces protections; précise toutefois que les libertés d'expression et d'information ont été conçues pour protéger les êtres humains, et non les machines ou les logiciels qui présentent un comportement non authentique, comme l'amplification et les activités orchestrées par l'IA et des robots, ainsi que les logiciels automatisés qui exécutent des tâches répétitives sur un réseau dans le but d'imiter de véritables utilisateurs;

26. reconnaît l'importance d'offrir des garanties efficaces aux utilisateurs lorsqu'ils exercent leurs droits démocratiques, notamment la possibilité de contester les décisions des plateformes en matière de modération des contenus et l'obligation pour ces plateformes d'informer les utilisateurs lorsque leurs contenus sont supprimés ou restreints; rappelle l'obligation qui incombe aux plateformes, en vertu du DSA, de prévoir un mécanisme distinct pour le traitement des plaintes à cette fin; souligne que la sauvegarde des droits fondamentaux des utilisateurs individuels implique également de réaliser des évaluations approfondies et d'atténuer les risques systémiques qui affectent l'intégrité de l'espace de l'information;

Intégrité des médias et de l'information

27. estime que les mesures visant à promouvoir des médias libres et indépendants sur le plan éditorial constituent une part centrale de l'atteinte des objectifs fixés par le bouclier européen de la démocratie; se félicite, à cet égard, des normes minimales communes innovantes en matière de liberté et de pluralisme des médias établies grâce à l'adoption du règlement européen sur la liberté des médias; précise toutefois que la portée du règlement ne peut être évaluée que sur la base de sa mise en œuvre concrète et insiste donc sur l'importance d'une application rigoureuse; salue les nouveaux engagements annoncés en matière de soutien aux médias par l'intermédiaire du programme consacré à la résilience médiatique et sollicite des engagements à long terme équivalents dans le prochain CFP;

28. explique qu'il est nécessaire d'évaluer attentivement l'incidence potentielle de la législation de l'Union sur le journalisme et les médias éditoriaux, en particulier pour préserver la durabilité et la viabilité des modèles économiques des entreprises de médias;

29. souligne, dans le contexte de la vente d'abonnements par des entreprises de médias via des applications, l'importance d'une mise en œuvre complète du règlement sur les marchés numériques (DMA); constate, à cet égard, la décision de non-conformité de la Commission du 23 avril 2025 à l'encontre d'Apple et de Meta; prend acte des enquêtes de la Commission sur une possible violation du DMA par Google, qui déclasserait le contenu des éditeurs de médias dans les résultats de recherche;

30. se félicite que la communication conjointe comprenne de nouvelles actions de soutien visant à promouvoir les compétences numériques et l'éducation aux médias, telles que

le programme consacré à la résilience médiatique, le programme de soutien aux compétences de base pour les écoles et le renforcement du groupe d'experts sur l'éducation aux médias, notamment la création d'un nouveau réseau d'experts pour l'éducation aux médias, ainsi que des lignes directrices actualisées à l'intention des enseignants et des éducateurs; précise que la prochaine révision de la directive «Services de médias audiovisuels» devrait renforcer les dispositions relatives aux exigences minimales applicables aux travaux des États membres en matière d'éducation aux médias;

31. se félicite de l'annonce de la mise à jour de la recommandation de la Commission sur la sécurité des journalistes[52] et de la prochaine révision de la recommandation contre les poursuites-bâillons[53]; explique que ces mises à jour et révisions doivent tenir compte de la manière dont les menaces, la violence, le sabotage et d'autres actions visant à entraver le travail journalistique ont une incidence sur la protection, la sécurité et le renforcement des moyens d'action des journalistes et autres professionnels des médias dans l'Union;

32. insiste sur l'importance de protéger les journalistes contre les poursuites abusives; se félicite, à cet égard, de l'adoption de la directive contre les poursuites-bâillons[54] et de l'annonce de la mise à jour du mandat et de la composition du groupe d'experts contre les poursuites-bâillons; invite les États membres à faire preuve d'ambition dans le processus de mise en œuvre en cours et demande à la Commission de continuer à apporter son soutien; invite la Commission à rédiger un rapport d'évaluation complet sur l'efficacité de la mise en œuvre;

33. se félicite de l'accord provisoire sur le règlement relatif au filtrage des investissements directs étrangers[55], en particulier des dispositions qui incluent le secteur des médias comme facteur à prendre en considération pour déterminer si un investissement est susceptible d'avoir une incidence négative sur la sécurité ou l'ordre public; déplore toutefois que le secteur des médias ne figure pas dans le champ d'application obligatoire de l'annexe du règlement;

34. invite la Commission et les États membres à analyser attentivement les conséquences du changement de politique d'aide de l'administration américaine dans le contexte du pluralisme des médias et du journalisme indépendant et, si nécessaire, à agir pour combler le vide laissé sur les marchés des médias, tant au sein de l'Union que dans les

[52] Recommandation (UE) 2021/1534 de la Commission du 16 septembre 2021 concernant la protection, la sécurité et le renforcement des moyens d'action des journalistes et autres professionnels des médias dans l'Union européenne (JO L 331 du 20.9.2021, p. 8, ELI: http://data.europa.eu/eli/reco/2021/1534/oj).
[53] Recommandation (UE) 2022/758 de la Commission du 27 avril 2022 sur la protection des journalistes et des défenseurs des droits de l'homme qui participent au débat public contre les procédures judiciaires manifestement infondées ou abusives («poursuites stratégiques altérant le débat public») (JO L 138 du 17.5.2022, p. 30, ELI: http://data.europa.eu/eli/reco/2022/758/oj).
[54] Directive (UE) 2024/1069 du Parlement européen et du Conseil du 11 avril 2024 sur la protection des personnes qui participent au débat public contre les demandes en justice manifestement infondées ou les procédures judiciaires abusives («poursuites stratégiques altérant le débat public») (JO L, 2024/1069, 16.4.2024, ELI: http://data.europa.eu/eli/dir/2024/1069/oj).
[55] Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union (JO L 79I du 21.3.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/452/oj).

régions frontalières; se réjouit du financement d'urgence que l'Union a accordé à RFE/RL; demande qu'une solution soit mise au point pour fournir un financement stable et à long terme à RFE/RL;

35. explique que les réseaux de vérification des faits fondés sur la société peuvent jouer un rôle dans la détection et dans la lutte contre les campagnes de désinformation, et fournir des informations précieuses pour les évaluations des risques au titre du DSA; constate que les organisations indépendantes de vérification des faits ont besoin de conditions stables pour fonctionner; estime que le réseau européen de vérificateurs de faits, annoncé par la Commission en 2025, pourrait constituer un outil permettant d'y parvenir; souligne que, pour être crédibles et efficaces, les organisations de vérification des faits doivent respecter des normes strictes de neutralité politique, d'indépendance et d'objectivité méthodologique;

Société civile

36. insiste sur le rôle crucial que joue la société civile dans la défense de notre démocratie, non seulement en exerçant sa fonction d'observatrice qui révèle et combat activement les tentatives d'ingérence étrangères dans les processus démocratiques, mais aussi en constituant une force fondamentale dans le cadre de l'effort à long terme visant à construire des sociétés plus fortes et plus résilientes; souligne, en particulier, le rôle important de la société civile dans la défense des valeurs consacrées à l'article 2 du traité UE;

37. salue la stratégie de l'Union pour la société civile, publiée par la Commission parallèlement à la communication sur le bouclier européen de la démocratie; se félicite de l'approche de la Commission consistant à lier cette stratégie à ses travaux sur le bouclier, en tant qu'outil permettant de renforcer davantage l'engagement civique;

38. invite la Commission à renforcer ses travaux sur le dialogue civil et à mettre en place de nouveaux outils à cette fin; se félicite, dans ce contexte, de l'engagement pris par la Commission de mettre en place, d'ici à 2026, une plateforme opérationnelle de la société civile afin de soutenir une approche plus systématique destinée à renforcer le dialogue conformément aux valeurs de l'Union; estime que le pôle de connaissances en ligne annoncé sur l'espace civique pourrait contribuer à la coordination des activités des organisations de la société civile dans le domaine de la protection de la démocratie et de la lutte contre les menaces hybrides et les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, et améliorer la connaissance de la situation;

39. souligne l'importance de programmes de financement concrets tels que le programme CERV; se félicite de l'idée de la Commission de maintenir le programme CERV et de l'intégrer dans le nouveau programme AgoraEU pour la période 2028-2034; invite la Commission à veiller à ce que le financement de ce volet d'AgoraEU réponde aux besoins des organisations de la société civile et soit mis en œuvre sous la gestion directe de la Commission;

40. explique qu'il est nécessaire d'améliorer la transparence financière en ce qui concerne le financement des organisations de la société civile en général, et dans le contexte du soutien apporté par des pays tiers en particulier; rappelle que les organisations de la société civile peuvent être, et ont été, utilisées comme outils par des acteurs malveillants de pays tiers pour influencer de manière illégitime les processus démocratiques dans

l'Union et ses États membres; précise qu'en tant qu'institution, le Parlement a la responsabilité particulière de contribuer aux réformes dans ce domaine, à la lumière du scandale dit du «Qatargate»; souligne toutefois que des mesures visant à résoudre ces problèmes devraient être élaborées de manière à ne pas pouvoir être utilisées à mauvais escient pour stigmatiser les activités légitimes de la société civile en tant que telles;

41. se félicite de la proposition de directive de la Commission sur la représentation d'intérêts exercée pour le compte de pays tiers, en tant qu'élément important du paquet «Défense de la démocratie», visant à établir des exigences harmonisées pour les activités économiques liées à la représentation d'intérêts exercées pour le compte d'une entité d'un pays tiers; explique que des règles communes à cet égard constitueraient une composante importante en matière de transparence en ce qui concerne l'influence exercée par des pays tiers; invite les colégislateurs à finaliser sans délai le processus législatif;

42. met en évidence l'importance de la participation des citoyens dans les processus démocratiques; prie instamment la Commission de garantir, en coopération avec les États membres, la communication claire et efficace des initiatives qu'elle met en place pour promouvoir et renforcer l'utilisation de ses instruments de participation citoyenne; se réjouit que la Commission renforce ces outils, notamment l'initiative citoyenne européenne, les panels de citoyens européens et la plateforme de participation des citoyens, ainsi que de la proposition visant à renforcer le réseau des autorités nationales en matière de participation des citoyens;

Protéger les infrastructures critiques

43. est d'avis que la protection de l'Union et de ses États membres contre les actes de sabotage physiques et numériques ciblant des infrastructures critiques constitue un élément essentiel pour préserver la résilience démocratique; appelle de ses vœux des mesures préventives robustes, une coopération transfrontière renforcée et une capacité accrue de l'Union à détecter ces activités hostiles, à les empêcher et à y faire face;

44. condamne fermement l'intensification des incursions de drones et d'autres aéronefs qui ciblent et perturbent des infrastructures critiques, y compris des aéroports civils, des bases militaires et des installations énergétiques dans l'ensemble de l'Union, en particulier lorsqu'elles sont orchestrées par la Russie et la Biélorussie; invite les États membres à réagir de manière coordonnée, unifiée et appropriée à toute violation de leur espace aérien, y compris en abattant des aéronefs, des drones et d'autres menaces aériennes;

45. souligne qu'une série d'activités hybrides menées par la Russie contre l'Union équivalent à des actes de terrorisme financé par l'État, même si elles relèvent d'une attaque armée; insiste dès lors sur la nécessité d'appliquer tous les cadres juridiques disponibles en matière de lutte contre le terrorisme aux activités hostiles de la Russie, qui violent la souveraineté territoriale des États membres de l'Union, compromettent l'intégrité de leurs institutions et menacent directement la sécurité de la population civile; explique que l'Union doit de toute urgence passer d'un mode de défense à une posture de dissuasion active; prie instamment les États membres d'évaluer les cadres juridiques et opérationnels régissant les mesures offensives proportionnées contre les

infrastructures logistiques et numériques qui sous-tendent les activités de déstabilisation menées par Moscou;

46. invite la Commission et les États membres à établir une interprétation commune par l'Union de la convention des Nations unies sur le droit de la mer (CNUDM), afin d'assurer une action coordonnée contre les activités hybrides et le sabotage dans les zones maritimes de l'Union, notamment en mer Baltique; estime que la coordination transfrontière peut encore être améliorée tant au niveau opérationnel que financier; souligne la nécessité pour l'Union d'intensifier sa réponse aux menaces hybrides dans les zones maritimes, y compris celles posées par la «flotte fantôme» russe; souligne que pour relever ces défis, un financement spécifique et suffisant de l'Union est nécessaire;

47. constate avec inquiétude les dépendances structurelles existantes, dues à la concentration du marché et au contrôle étranger, dans l'infrastructure numérique de l'Union, y compris les systèmes d'exploitation, les centres de données, les semi-conducteurs, l'IA, la cybersécurité, l'informatique en nuage et divers services et plateformes numériques, qui présentent tous un risque élevé pour la démocratie, la liberté et la sécurité au sein de l'Union, ainsi que pour la compétitivité de l'Union; invite la Commission et les États membres à mettre en place, en tant qu'assise fondamentale, une infrastructure numérique souveraine de l'Union dotée de technologies respectueuses de la vie privée et d'un écosystème d'interfaces de programmation d'applications (API) de l'Union au moyen de politiques ambitieuses et ciblées qui renforcent les investissements et la part de marché des entreprises de l'Union, en tirant parti de l'approvisionnement européen en énergie propre pour le développement de centres de données et d'infrastructures en nuage, y compris au moyen d'initiatives axées sur le marché telles que des entreprises communes ou des réseaux fédérés dans des domaines tels que les gigafabriques d'IA ou les services en nuage;

48. souligne la nécessité d'assurer une plus grande intégration entre les infrastructures numériques, la cybersécurité et la politique de défense afin de faire progresser l'autonomie stratégique de l'Union, et la nécessité de tirer parti des infrastructures à double usage, telles que les centres de données résilients dispersés dans l'ensemble de l'Union, afin d'assurer la continuité opérationnelle face aux menaces hybrides ou en temps de guerre; souligne, en outre, qu'il est nécessaire d'accroître les investissements dans la mobilité militaire et les communications sécurisées, y compris le déploiement urgent et prioritaire de capacités spatiales telles qu'IRIS^2, afin de fournir des services cryptés à des fins publiques et de défense;

49. souligne que les cadres de cybersécurité tels que la directive SRI 2, le règlement sur la cyberrésilience[56] et le règlement sur la cybersolidarité[57] doivent s'aligner pour soutenir les normes de sécurité dès la conception et éviter la fragmentation réglementaire; demande, dans ce contexte, une révision de la législation pertinente dans le domaine de la cybersécurité et souligne la nécessité de renforcer les structures existantes, telles que

[56] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).
[57] Règlement (UE) 2025/38 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir et modifiant le règlement (UE) 2021/694 (règlement sur la cybersolidarité) (JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

l’ENISA et le Centre européen de compétences en matière de cybersécurité;

50. rappelle le faible niveau de transposition de la directive SRI 2; déplore qu’après l’échéance fixée au 17 octobre 2024, la Commission a dû adresser des lettres de mise en demeure à pas moins de 23 États membres pour transposition incomplète de la directive; invite instamment les États membres à achever la transposition de la directive dès que possible, étant donné qu’à la fin 2025, soit plus d’un an après l’échéance, la directive devait encore être transposée par 10 États membres; se félicite, à cet égard, de l’engagement pris par la Commission de collaborer étroitement avec les États membres afin de garantir une mise en œuvre rapide et cohérente du cadre horizontal en matière de cybersécurité défini dans la directive SRI 2, ainsi que du règlement sur la cyberrésilience et du règlement sur la cybersolidarité, comme le prévoit la stratégie de sécurité intérieure ProtectEU.

Coopération en matière de justice et d’affaires intérieures

51. estime que tous les instruments de droit pénal disponibles au niveau des États membres et de l’Union devraient être appliqués et, le cas échéant, développés afin de prévenir et de combattre les comportements illégaux cherchant à porter atteinte aux institutions et processus démocratiques; soutient, en particulier, l’engagement de la Commission en faveur d’une révision ambitieuse du mandat d’Europol, en vue de le transformer en une agence de police véritablement opérationnelle qui soutienne mieux les États membres;

52. se félicite que la communication conjointe reconnaisse la contribution positive de la coopération en matière de justice pénale et de répression à la lutte contre les activités de manipulation de l’information et d’ingérence menées depuis l’étranger et les activités de désinformation; invite la Commission, lors de la préparation de la révision prévue des mandats d’Europol et d’Eurojust, à recenser soigneusement les lacunes juridiques qui empêchent actuellement ces agences de fournir pleine assistance aux États membres confrontés à des menaces hybrides, et à étudier les moyens de les combler;

53. relève avec inquiétude la multiplication d’exemples de la manière dont des acteurs malveillants de pays tiers utilisent la criminalité comme un service et les organisations criminelles comme des intermédiaires au sein de l’Union pour cibler des personnes et des entités identifiées en tant qu’adversaires politiques, ce qui constitue une grave menace pour la sécurité intérieure de l’Union; souligne que de telles pratiques constituent un acte intolérable d’ingérence étrangère, avec des effets potentiellement déstabilisateurs sur nos sociétés; souligne, dans ce contexte, la nécessité de renforcer encore la coordination au niveau de l’Union dans le domaine de la justice pénale et de l’application de la loi;

54. condamne fermement l’instrumentalisation et l’utilisation comme arme de la migration contre l’Union; estime que ce phénomène représente une tentative inacceptable de la part de pays tiers malveillants d’exercer une pression politique sur les États membres de première ligne et sur l’Union; se félicite des dispositions spécifiques sur l’instrumentalisation de la migration récemment incluses dans des actes législatifs clés de l’Union sur la gestion des frontières et la migration; souligne que les États membres concernés par de telles menaces devraient pouvoir compter sur le soutien d’agences spécialisées de l’Union; demande que le mandat de Frontex soit renforcé afin que

l’agence dispose de la base juridique et des ressources humaines, financières et techniques nécessaires pour aider correctement les États membres à faire face à ces menaces hybrides; souligne, dans ce contexte, la nécessité de renforcer encore la capacité de l’Union à contribuer aux efforts de protection des frontières des États membres au moyen d’investissements suffisants au titre du CFP 2028-2034;

Dimension extérieure

55. souligne que le bouclier européen de la démocratie doit avoir une forte dimension extérieure; se félicite de l’inclusion, dans la communication conjointe, d’actions spécifiques visant à soutenir les pays au-delà des frontières de l’Union, notamment en facilitant le renforcement des capacités afin d’améliorer la résilience des pays candidats et candidats potentiels face aux activités de manipulation de l’information et d’ingérence menées depuis l’étranger et aux ingérences hybrides, ainsi qu’en soutenant les médias et le journalisme indépendants et en renforçant leur capacité à surveiller la désinformation sur les médias sociaux avant et pendant les élections;

56. soutient l’idée de tirer parti des voies diplomatiques pour renforcer les capacités dans les régions prioritaires; estime que le rôle des délégations de l’Union et des ambassades des États membres de l’Union est essentiel pour mieux comprendre les circonstances locales susceptibles de conduire à l’ingérence étrangère et pour apporter une réponse adaptée; note qu’il est possible pour les délégations de l’Union et les ambassades des États membres de soutenir l’organisation de campagnes de sensibilisation dans les pays d’accueil; souligne l’importance d’associer les missions et opérations relevant de la politique de sécurité et de défense commune (PSDC) aux actions envisagées dans la communication conjointe; invite les États membres et le SEAE à intégrer des activités de renforcement des capacités et des formations sur les menaces hybrides dans les mandats individuels des missions et des opérations, afin d’améliorer la préparation des homologues nationaux;

57. demande l’élaboration d’une stratégie globale permettant aux délégations de l’Union et aux missions et opérations de la PSDC, en étroite coordination avec les missions diplomatiques des États membres de l’Union, de servir plus efficacement de première ligne de défense contre les attaques hybrides, y compris les opérations de cybersécurité et de manipulation de l’information et d’ingérence menées depuis l’étranger; estime qu’il est crucial de renforcer les capacités de communication stratégique et de diplomatie publique au sein des délégations de l’Union, en mettant l’accent sur la promotion de récits fondés sur des faits, l’engagement civique et le renforcement de la confiance, en particulier chez les jeunes et les éducateurs; invite la vice-présidente de la Commission/haute représentante de l’Union pour les affaires étrangères et la politique de sécurité et le Conseil à inclure des équipes de surveillance et de réaction à la désinformation dans les missions PSDC, à assurer la formation de l’ensemble du personnel des missions aux activités de manipulation de l’information et d’ingérence menées depuis l’étranger et à renforcer la coordination entre les opérations civiles et militaires afin de lutter contre l’influence hybride;

58. se félicite du soutien accru, dans la communication conjointe, au développement d’une capacité d’opérations d’information offensives; note qu’un tel engagement nécessite des ressources spécifiques et une planification à long terme; souligne que l’objectif devrait inclure le renforcement par l’Union, dans son voisinage, de mesures d’information

proactives pour contrer les efforts de déstabilisation menés par la Russie; souligne la nécessité de diffuser des informations factuelles et fiables aux populations vivant dans des régimes autoritaires, notamment en Russie, afin de dévoiler les pratiques de gouvernance destructrices de leurs dirigeants, qui mettent en danger la liberté et la paix non seulement dans les pays voisins, mais aussi, en premier lieu, à l'intérieur de leur propre pays; demande de tirer parti, dans toute la mesure du possible, de l'espace numérique et du cyberespace, et de leur caractère intrinsèquement sans frontières, pour atteindre cet objectif;

59. reconnaît que les voisins immédiats de l'Union, y compris les Balkans occidentaux, la Moldavie et l'Ukraine, sont confrontés à de graves ingérences étrangères; demande le financement de pôles régionaux de coordination pour lutter contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, renforcer le soutien au journalisme d'investigation et aux régulateurs des médias et intensifier les communications stratégiques fondées sur des faits par l'intermédiaire des délégations de l'Union afin de lutter contre la désinformation anti-UE; souligne la nécessité d'accorder une attention particulière à l'assistance en matière d'intégrité des élections dans les pays candidats à l'adhésion à l'Union;

60. invite la Commission à faire des programmes d'éducation aux médias une composante permanente de l'aide de préadhésion et de l'instrument européen de voisinage, avec des subventions spécifiques de l'Union pour soutenir le journalisme d'investigation dans les régions vulnérables;

61. demande que l'Union intensifie les efforts qu'elle déploie actuellement pour aider les pays partenaires de son voisinage, ainsi que les pays prioritaires d'Afrique subsaharienne, de la région Asie-Pacifique et d'Amérique latine, à renforcer leur résilience face aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger, à consolider leurs processus démocratiques et à garantir l'intégrité électorale; souligne, en particulier, la nécessité de poursuivre le développement du projet phare EUvsDisinfo;

62. reconnaît que la mise en place de l'EUPM Moldova constitue un exemple réussi de la manière dont l'Union peut jouer un rôle décisif dans le soutien aux structures de gestion des crises d'un pays partenaire et dans le renforcement de sa résilience face aux menaces hybrides, informatiques et de manipulation de l'information et d'ingérence menées depuis l'étranger; estime que l'EUPM Moldova devrait servir de modèle pour l'inclusion de la lutte contre les menaces hybrides dans le mandat des missions existantes et la mise en place de missions similaires dans d'autres pays partenaires; prend acte des élections législatives qui se sont tenues en Moldavie le 28 septembre 2025 et de la nette victoire du parti pro-européen Action et solidarité (PAS);

63. se félicite du déploiement d'équipes d'intervention rapide de l'Union en cas de menaces hybrides, comme l'illustre l'exemple récent de la Moldavie, en tant qu'instrument utile pour renforcer les capacités et la résilience dans les pays ciblés par des attaques hybrides, des cyberattaques et des activités de manipulation de l'information et d'ingérence menées depuis l'étranger, sur la base du savoir-faire et de l'expertise spécifiques de l'Union et de ses États membres;

64. souligne qu'il importe de donner la priorité aux principes et aux objectifs du bouclier européen de la démocratie dans le cadre de la coopération internationale avec des partenaires partageant les mêmes valeurs, tels que le G7, l'OTAN, les Nations unies, l'Organisation pour la sécurité et la coopération en Europe et le Conseil de l'Europe; se félicite des mesures déjà prises dans le cadre des relations bilatérales et multilatérales, notamment le code de conduite des Nations unies pour l'intégrité de l'information sur les plateformes numériques, l'engagement pris par les États membres du Conseil de l'Europe dans la déclaration de Reykjavik de protéger les systèmes électoraux contre les ingérences étrangères, les partenariats en matière de sécurité et de défense et les efforts continus du mécanisme de réaction rapide du G7 pour prévoir et élaborer des réponses collectives aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger;

65. se félicite de la mise en place d'un partenariat de sécurité et de défense entre l'Union et le Royaume-Uni en mai 2025; se félicite de l'accent mis, entre autres, sur la coopération dans la lutte contre les cybermenaces, les menaces hybrides et les activités de manipulation de l'information et d'ingérence menées depuis l'étranger, ainsi que sur la protection des infrastructures critiques;

Systèmes électoraux et résilience électorale

66. souligne que l'un des principaux objectifs du bouclier européen de la démocratie devrait être de protéger l'intégrité des élections aux niveaux local, régional, national et européen; invite la Commission et les États membres à collaborer, dans le plein respect du principe de subsidiarité, pour mettre en œuvre des réformes visant à renforcer la résilience des processus électoraux en Europe, en mettant particulièrement l'accent sur les mesures visant à prévenir l'ingérence étrangère;

67. invite les États membres à redoubler d'efforts pour mettre en œuvre les recommandations de la Commission sur des processus électoraux inclusifs, solides et résilients au sein de l'Union; souligne, en particulier, qu'il importe de mettre en place des réseaux électoraux nationaux pour aider les autorités nationales et les organismes d'experts à travailler en synergie;

68. invite les États membres à veiller à ce que les autorités électorales ou les organes équivalents chargés du bon déroulement d'élections libres et équitables soient dotés de financements suffisants et des outils appropriés pour leur permettre d'exercer leurs fonctions, que ce soit en assurant la formation du personnel et en fournissant les outils numériques nécessaires, ou en garantissant des investissements suffisants dans les organes électoraux et les infrastructures électorales;

69. considère que les campagnes haineuses et la violence qui entravent la participation des candidats au débat public ou gênent leurs interactions avec les électeurs constituent une menace pour la démocratie; souligne que ces menaces peuvent être alimentées par les tentatives de pays tiers de déstabiliser l'Union; se félicite, à cet égard, de l'engagement pris par la Commission de présenter des recommandations sur la sécurité en politique; invite les États membres à redoubler d'efforts pour protéger les candidats aux élections et les représentants élus;

70. souligne le rôle essentiel de l'ECNE pour veiller à l'échange de bonnes pratiques en matière de résilience électorale dans l'Union et ses États membres; relève toutefois les

limites actuelles de ses activités; se félicite de l'engagement pris par la Commission de renforcer l'ECNE, y compris par des réformes telles que la mise en place d'un répertoire de références et de normes communes pour les processus électoraux;

71. invite la Commission à relever son niveau d'ambition en ce qui concerne la réforme de l'ECNE, notamment en réexaminant les ressources et le personnel permanent qui lui sont affectés et en développant davantage le mécanisme commun pour la résilience électorale; souligne qu'il importe de mettre en œuvre des mesures concrètes pour renforcer la participation des pays candidats aux activités de l'ECNE; invite la Commission, dans le cadre de l'ECNE, à mettre en place un groupe de suivi permanent chargé de superviser la mise en œuvre des recommandations de la Commission sur des processus électoraux inclusifs et résilients dans l'Union, ainsi que des recommandations à venir sur la sécurité des acteurs politiques; estime qu'un tel groupe de suivi devrait également être chargé d'élaborer des propositions de mises à jour futures de ces recommandations;

72. invite la Commission à inclure le Parlement et l'Autorité pour les partis politiques européens et les fondations politiques européennes (APPF) en tant que partenaires permanents dans toutes les réunions de l'ECNE;

73. se félicite de l'objectif de la Commission de renforcer la protection des infrastructures liées aux élections au moyen de la législation et des outils existants; invite la Commission à compléter ces efforts par une révision ciblée de la directive sur la résilience des entités critiques, en vue d'inclure les infrastructures électorales dans la liste des services essentiels de l'administration publique figurant dans la directive;

74. invite la Commission et les États membres à se pencher sur la question de l'implication d'acteurs étrangers dans le paysage politique des partis européens; relève avec inquiétude divers exemples de financement par des pays tiers de mouvements extrémistes au sein de l'Union; estime que la transparence financière est un outil important pour faire la lumière sur cette question et demande un renforcement des échanges entre les entités privées et publiques à cet égard; souligne, en particulier, la nécessité de lutter contre la communication politique dissimulée, y compris les structures de financement opaques et les commanditaires cachés, afin de préserver l'intégrité démocratique et de garantir la transparence pour les citoyens;

75. relève avec inquiétude les preuves de plus en plus nombreuses de l'ingérence étrangère et de l'espionnage dans le système politique européen; se félicite des efforts d'enquête déployés dans les États membres qui ont conduit à des condamnations et à des procédures en cours liées à la corruption, à l'espionnage et à la promotion des intérêts d'États étrangers; souligne les risques graves que pose l'insuffisance des mesures de protection lors du recrutement d'agents et d'associés entretenant des liens étroits avec des régimes autoritaires;

76. salue l'adoption récente du règlement relatif au statut et au financement des partis politiques européens et des fondations politiques européennes; prend acte des dispositions relatives au financement et à la participation de partis de pays tiers; invite les États membres à veiller à sa mise en œuvre pleine et efficace;

77. constate que l'évolution des cryptomonnaies crée une vulnérabilité potentielle liée au manque de transparence et à l'incapacité de contrôler le financement des partis et

mouvements politiques en Europe; prend acte de l'engagement pris par la Commission de réunir des experts nationaux sous l'égide de l'ECNE, en étroite coopération avec d'autres réseaux et parties prenantes de l'Union, afin d'échanger les bonnes pratiques, de préparer d'éventuelles lignes directrices et de promouvoir des actions conjointes à cet égard; invite la Commission à continuer de suivre la mise en œuvre du train de mesures contre le blanchiment de capitaux et du règlement sur les marchés de crypto-actifs et à combler toute lacune potentielle dans la législation;

Le rôle des sanctions dans la protection de la démocratie

78. estime que les sanctions à l'encontre d'entités, de pays ou de personnes étrangers qui se livrent à des comportements visant à compromettre l'intégrité démocratique de l'Union ou de ses États membres constituent un élément important des objectifs du bouclier européen de la démocratie; souligne en outre que des sanctions efficaces doivent comprendre un ensemble complet de mesures, y compris le gel et la confiscation des avoirs, l'imputation et la mise en lumière des responsabilités, l'augmentation des coûts et la réduction des revenus, l'interdiction des importations et des exportations, le refus d'accès et d'autres mesures restrictives pertinentes;

79. invite la Commission et les États membres à évaluer régulièrement et attentivement les sanctions imposées en vue d'une efficacité optimale et de leur extension éventuelle, y compris les sanctions secondaires visant les entités qui cherchent à les contourner; estime que, en particulier dans le domaine des menaces hybrides et des activités déstabilisatrices russes, l'Union devrait encore étendre son régime de sanctions en ciblant les facilitateurs financiers et techniques qui soutiennent la désinformation, les cyberattaques et l'ingérence électorale, tels que les bourses de cryptomonnaies, les réseaux publicitaires et les fournisseurs d'hébergement, tout en perturbant les réseaux agissant pour le compte de la Russie dans les pays tiers, notamment en Afrique et au Moyen-Orient, en imposant des sanctions aux médias, aux plateformes logistiques et aux entités liées au groupe Wagner qui diffusent des discours anti-UE; estime que, pour augmenter encore le coût de l'agression hybride, l'Union devrait étendre les sanctions secondaires à l'encontre des entreprises de pays tiers, en particulier chinoises, qui facilitent les opérations russes, et qu'elle devrait interdire aux cybermercenaires russes d'utiliser des services basés dans l'Union, tels que des services d'hébergement, de domaine et d'informatique en nuage, et dénoncer publiquement les responsables politiques ou les lobbyistes de l'Union financés de manière occulte par Moscou, et leur imposer des sanctions;

80. considère que le fait d'identifier et de désigner les pays d'origine, plutôt que des individus ou des entreprises, pourrait constituer une étape importante vers la reconnaissance du problème que représente l'ingérence manifeste, systématique, à plusieurs niveaux et souvent financée par des acteurs étatiques, pratiquée par des pays comme la Russie ou l'Iran à travers l'Europe; se félicite de la décision de la Commission d'inscrire la Russie sur la liste des pays tiers à haut risque au titre du cadre de l'Union en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, afin de préserver l'intégrité du système financier de l'Union; rappelle que le nouveau règlement sur la lutte contre le blanchiment de capitaux fournira une base juridique supplémentaire pour identifier les pays dangereux, notamment ceux qui participent à la prolifération des armes de destruction massive;

81. souligne que l'efficacité et la crédibilité des sanctions de l'Union dépendent d'une application stricte et cohérente; souligne que la révision annoncée du mandat du Parquet européen offre l'occasion de renforcer son rôle afin d'y inclure les enquêtes et les poursuites relatives aux violations des sanctions;

82. condamne l'utilisation par la Russie, pour des motifs politiques, de «listes noires» ciblant des citoyens de l'Union, des représentants des autorités publiques et des organisations commerciales, des journalistes, des acteurs de la société civile et des responsables politiques, y compris des députés démocratiquement élus au Parlement européen; appelle de ses vœux une réponse plus coordonnée et plus résolue de l'Union à ces mesures arbitraires, afin de veiller à la protection et à la sécurité des personnes inscrites sur la liste noire et de leur apporter la solidarité et le soutien nécessaires; exprime son soutien sans réserve à toutes les personnes touchées;

Préparation de l'Union

83. se félicite de la stratégie européenne pour une union de la préparation et souligne que les objectifs énoncés dans la stratégie sont étroitement liés à ceux du bouclier européen de la démocratie; souligne en outre que la résilience démocratique exige que les sociétés soient en mesure de fonctionner dans des conditions exceptionnelles ou perturbées et que les réformes visant à renforcer la préparation devraient donc faire partie intégrante du bouclier européen de la démocratie;

84. demande le développement et le déploiement rapides d'une application interopérable d'alerte en cas de crise à l'échelle de l'Union, fournissant aux citoyens des informations en temps réel, fiables et multilingues en cas d'urgence; recommande que cette application soit intégrée dans les systèmes d'alerte précoce nationaux et de l'Union, qu'elle soit accessible aux groupes vulnérables et qu'elle soit régulièrement mise à jour en fonction des progrès technologiques et des bonnes pratiques en matière de gestion des crises;

85. se félicite des initiatives prises dans plusieurs États membres consistant à distribuer une brochure sur la préparation des ménages, qui propose des orientations claires et pratiques adaptées aux diverses réalités sociales et géographiques de l'Europe afin d'aider les citoyens à se préparer aux situations d'urgence; invite la Commission à produire une brochure au niveau de l'Union tenant compte du contexte transfrontière et multinational et contenant des recommandations relatives au matériel d'urgence, des instructions pratiques pour permettre l'autosuffisance pendant au moins 72 heures, des conseils de base en matière de premiers secours et des orientations spécifiques pour les groupes vulnérables, y compris les personnes âgées, les personnes handicapées et les familles avec enfants;

86. demande l'organisation régulière d'exercices de préparation à grande échelle coordonnés par l'Union et associant ses institutions, les États membres, les autorités régionales et locales, ainsi que le secteur privé et la société civile; recommande que ces exercices simulent des scénarios complexes et réalistes, y compris des cyberattaques, des perturbations des infrastructures critiques, une désinformation coordonnée et des crises hybrides, afin d'évaluer les capacités de réaction, d'améliorer l'interopérabilité entre les niveaux de gouvernance et de promouvoir une culture de la préparation à tous les niveaux; demande, à cette fin, la création d'une Journée européenne de la

préparation; estime que cet événement devrait être organisé le 24 février, jour de l'invasion militaire à grande échelle non provoquée de l'Ukraine par la Russie en 2022, étant donné que cette date symbolise la solidarité de l'Union avec l'Ukraine et rappelle avec force la nécessité de renforcer la préparation civile et de défense face aux menaces croissantes émanant de régimes autoritaires;

87. invite la Commission à examiner la possibilité d'étendre Erasmus+ ou des programmes similaires afin d'y inclure des initiatives transfrontières sur la formation à la préparation des travailleurs des secteurs critiques, tels que les pompiers, les professionnels de la santé, les volontaires de la protection civile, les fonctionnaires et les représentants des organisations de la société civile, ainsi que du grand public; recommande que ces programmes favorisent l'échange transfrontière et transsectoriel de connaissances, les exercices conjoints et la formation aux menaces hybrides et aux situations d'urgence, et renforcent les capacités locales de préparation dans tous les États membres, en accordant une attention particulière aux régions vulnérables;

88. demande l'accélération de la mise en œuvre de systèmes de communication sécurisés tels qu'IRIS² et le système de communication critique de l'UE; souligne que ces initiatives garantissent la résilience des télécommunications, la continuité des services essentiels pendant les crises, la réduction des dépendances extérieures dans les secteurs stratégiques et le renforcement de la cybersécurité de ces infrastructures;

89. appelle de ses vœux une coordination renforcée entre les institutions, organes et organismes de l'Union, les États membres et les partenaires internationaux au moyen de plateformes communes d'appréciation de la situation, de méthodologies communes et de mécanismes rapides et sécurisés d'échange d'informations; souligne que ces outils permettent une réponse cohérente, agile et coordonnée aux menaces hybrides, améliorent l'anticipation des risques et renforcent la préparation et la résilience collectives de l'Union;

90. souligne la nécessité d'intégrer la préparation dans le CFP 2028-2034, afin de bâtir une résilience crédible et d'atteindre un niveau suffisant de préparation civile et de défense; prie instamment la Commission d'élaborer des instruments financiers ciblés combinant des instruments pertinents en matière de défense et de sécurité civile, tels que le mécanisme pour la défense de l'Europe et le mécanisme pour une Europe sûre, afin de fournir un financement suffisant et stable pour les projets de renforcement de la résilience, l'innovation technologique et les capacités à double usage, les initiatives de préparation civile, la protection des infrastructures critiques et les efforts visant à renforcer la souveraineté industrielle et technologique de l'Union; note que les flux de financement spécifiques devraient également donner la priorité aux efforts de préparation locaux, en particulier dans les territoires les plus exposés aux vulnérabilités et aux menaces hybrides;

91. recommande aux institutions décisionnelles de l'Union de revoir et d'optimiser leurs stratégies et leurs plans d'urgence en cas d'attaque militaire ouverte contre un ou plusieurs États membres et de scénarios de crise similaires; souligne, en outre, la nécessité de garantir les niveaux les plus élevés de sûreté et de sécurité dans l'ensemble des institutions, organes et organismes de l'Union, y compris dans le domaine de la cybersécurité ainsi que de la sécurité et de l'intégrité des informations, et de créer les conditions nécessaires à cet égard, notamment en s'assurant de disposer de canaux de

communication sécurisés accrédités et de salles de réunion adéquates pour les réunions à huis clos; souligne la nécessité d'appliquer strictement les règles relatives aux violations de la sécurité et de la confidentialité de l'information, en particulier dans le contexte d'un risque accru d'espionnage et de sabotage; souligne que, même en dehors d'un conflit militaire ouvert, les menaces hybrides continuent de faire peser des risques toujours plus élevés sur le fonctionnement quotidien de l'Union;

92. salue les efforts déployés par la Commission pour renforcer la sécurité physique et la sécurité de l'information au sein des institutions de l'Union, tels que décrits dans la note du conseil d'administration d'octobre 2025, y compris les projets de salles de réunion sécurisées, l'amélioration des procédures d'habilitation de sécurité pour le personnel traitant des informations classifiées et la mise en place du collège de sécurité afin de veiller à ce que l'évolution des menaces fasse l'objet de mises à jour régulières; note que ces mesures répondent aux risques accrus d'espionnage, d'ingérence étrangère et de menaces hybrides ciblant les processus décisionnels de l'Union; souligne toutefois que les mises à niveau de la sécurité physique doivent être complétées par des protocoles de cybersécurité et des capacités de contre-espionnage solides afin de faire face à l'ensemble des risques d'infiltration; demande l'adoption rapide de la proposition de règlement de la Commission relatif à la sécurité de l'information dans les institutions, organes et organismes de l'Union (COM(2022) 119); rappelle que le règlement établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union recommande d'allouer à la cybersécurité 10 % du budget global des technologies de l'information et de la communication pour les entités de l'Union;

93. recommande que des mesures supplémentaires soient prises pour accroître la sécurité et la résilience du Parlement face à l'ingérence étrangère, ainsi que sa préparation et sa capacité à fonctionner en cas de crise; demande, à cet égard, un soutien accru à ses députés, y compris des vérifications informatiques et de sécurité, des formations et des séances d'information spécifiques avant les missions, ainsi qu'une formation interdisciplinaire avancée et d'autres activités de renforcement de la résilience combinant la sécurité physique et la sécurité de l'information, la sûreté et la cybersécurité; demande la poursuite de la formation ciblée du personnel du Parlement afin de prévenir la manipulation de l'information; recommande de renforcer son environnement de cybersécurité conformément au règlement sur la cybersécurité et d'accroître sa maturité opérationnelle afin de renforcer encore sa résilience dans ce domaine et d'améliorer ses capacités de détection des menaces dans le contexte de l'évolution incessante du panorama des menaces en matière de cybersécurité et d'un environnement technologique en mutation rapide;

94. relève, en ce qui concerne la sécurité intérieure du Parlement, que l'utilisation par les députés et le personnel de téléphones portables personnels et d'autres appareils personnels tels que des ordinateurs portables à des fins professionnelles constitue une vulnérabilité qui pourrait être exploitée pour attaquer l'institution; souligne que les députés et le personnel devraient être équipés des dispositifs informatiques nécessaires, tels que des téléphones portables et des ordinateurs portables, pour accomplir leurs tâches; se félicite, dans ce contexte, des contrôles de sécurité proposés aux députés et au personnel, sur demande, pour détecter d'éventuels logiciels espions sur des appareils privés; invite l'administration à étendre et à systématiser ce filtrage afin qu'il couvre tous les appareils utilisés pour les travaux liés au Parlement; demande des règles plus

claires et des orientations systématiques et appropriées à l'intention des députés et du personnel, ainsi que des garanties pour atténuer ces risques, en particulier pendant les missions;

95. invite la Commission et le SEAE à associer systématiquement le Parlement à leurs activités et exercices de préparation, tels que EU Integrated Resolve;

°

° °

96. charge sa Présidente de transmettre la présente résolution au Conseil, à la Commission, à la vice-présidente de la Commission et haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, ainsi qu'aux gouvernements et aux parlements des États membres.

EXPOSÉ DES MOTIFS

L'Union européenne est fondée sur les valeurs de démocratie, d'état de droit et de droits fondamentaux, qui constituent la base de son ordre politique, de sa légitimité institutionnelle et de sa cohésion sociétale. Ces dernières années, ces fondations ont de plus en plus été la cible d'une intensification rapide d'activités hostiles. L'ampleur, la sophistication et l'impact des activités de manipulation de l'information et d'ingérence menées depuis l'étranger, des opérations hybrides, des campagnes de désinformation coordonnées et d'autres formes d'influence malveillante n'ont cessé de croître.

Ces tactiques exploitent délibérément les fractures sociales, manipulent le débat public et cherchent à saper la confiance des citoyens dans les institutions et les processus démocratiques de l'Union et de ses États membres. Leur nature de plus en plus numérique, amplifiée par des plateformes en ligne opaques et des réseaux de diffusion transfrontières, accroît la complexité du panorama des menaces, de sorte qu'il est de plus en plus difficile pour les États membres de les affronter seuls. Dans ce contexte, l'Union a reconnu la nécessité d'une réponse plus stratégique, coordonnée et anticipative. S'appuyant sur les travaux menés par ses précédentes commissions spéciales consacrées à l'ingérence étrangère dans les processus démocratiques (INGE et INGE2), le Parlement européen a décidé, en décembre 2024, de créer une commission spéciale sur le bouclier européen de la démocratie (EUDS), chargée d'examiner comment l'Union peut mieux défendre ses fondements démocratiques.

La communication conjointe sur le bouclier européen de la démocratie, présentée par la Commission en collaboration avec la VP/HR, constitue une contribution importante à cet effort. Elle fournit une vue d'ensemble structurée de l'environnement actuel des menaces et recense plusieurs domaines dans lesquels des mesures supplémentaires sont nécessaires pour protéger l'Union contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger et contre la désinformation, ainsi que pour renforcer la résilience de la société. Le rapporteur s'est félicité de cette initiative et a reconnu sa valeur ajoutée pour conforter la compréhension par l'Union des défis qui l'attendent.

Toutefois, si la communication fixe le bon cap, son niveau d'ambition reste trop limité compte tenu de l'ampleur des menaces. Ce n'est pas seulement un cadre de réflexion qui est nécessaire, mais aussi un programme concret de réformes susceptible de garantir la capacité opérationnelle, la responsabilité et la préparation à long terme.

L'Union a mis en place un écosystème en pleine expansion de structures, d'outils et de programmes visant à lutter contre la manipulation de l'information et la désinformation étrangères. Ces efforts – notamment ceux des groupes de travail concernés, des réseaux de coopération et des mécanismes d'alerte précoce – sont importants, mais pour passer à un niveau supérieur, des réformes sont indispensables. La proposition visant à créer un Centre européen pour la résilience démocratique est une initiative bienvenue et prometteuse. Toutefois, sous la forme présentée dans la communication, cette initiative manque de la clarté opérationnelle requise pour que le Centre puisse faire office de pôle d'expertise et d'action efficace. Des recommandations concrètes ont été formulées dans le projet de rapport pour atteindre cet objectif.

En ce qui concerne la sphère numérique, qui à bien des égards est exploitée par des acteurs malveillants de pays tiers pour mener leurs opérations, le rapporteur est d'avis que la

législation pertinente de l'Union doit être respectée et que la Commission doit intensifier ses mesures d'exécution, en particulier lorsqu'il existe des indices de manipulation liée aux élections, d'opacité algorithmique systémique, de comportement coordonné non authentique ou d'utilisation abusive à grande échelle des fonctionnalités des plateformes.

L'évolution du paysage des menaces exige également des États membres qu'ils coopèrent plus efficacement au niveau de l'Union en ce qui concerne la conduite des élections. L'intégrité des processus électoraux est au cœur de la résilience démocratique. Dans ce contexte, le projet de rapport souligne la nécessité de renforcer considérablement le réseau européen de coopération en matière d'élections (ECNE) et plaide pour une réforme globale afin de rendre ce réseau plus ambitieux et plus pertinent sur le plan opérationnel. En outre, les infrastructures liées aux élections devraient être reconnues comme faisant partie des infrastructures critiques de l'Union et protégées en conséquence.

Le rapporteur s'est également félicité de ce que la communication conjointe sur le bouclier européen de la démocratie comporte une dimension extérieure. Les objectifs du bouclier de la démocratie ne peuvent être atteints sans une coopération étroite avec les partenaires du voisinage de l'Union, en particulier les pays candidats qui sont de plus en plus exposés à une ingérence étrangère intense. Soutenir leur résilience, notamment par le renforcement des capacités, les formations et la fourniture d'expertise, est indispensable pour préserver l'espace démocratique plus large de l'Europe. Le projet de rapport invite le SEAE à intégrer systématiquement des mesures de préparation aux menaces hybrides dans les mandats des missions et opérations PSDC, et de renforcer ainsi la capacité des homologues nationaux à détecter et à contrer les influences malveillantes. Dans le cadre de la dimension extérieure du bouclier, un réexamen des instruments de sanctions pertinents devrait également être entrepris afin de veiller à ce qu'ils soient calibrés de manière optimale pour cibler les acteurs qui compromettent l'intégrité démocratique de l'Europe. L'alignement sur des partenaires partageant les mêmes valeurs est également important en vue de garantir des réponses collectives efficaces; le rapporteur se félicite de l'utilisation des canaux de coopération multilatéraux et bilatéraux, y compris les partenariats existants de l'Union en matière de sécurité et de défense.

Le projet de rapport souligne en outre la nécessité d'un programme ambitieux pour rendre la société plus résiliente. Les réformes visant à soutenir le secteur des médias constituent un élément important à cet égard, parallèlement aux mesures visant à renforcer l'éducation aux médias. La société civile et la stratégie de l'UE en faveur de la société civile constituent un autre aspect essentiel: une société civile forte et indépendante est essentielle à la résilience démocratique. Le rapporteur plaide pour des programmes solides en soutien aux priorités stratégiques définies dans l'initiative du bouclier européen de la démocratie dans le prochain cadre financier pluriannuel 2028-2034.

Pour renforcer la résilience de la société, une protection accrue des infrastructures critiques est également essentielle et devrait être réévaluée à la lumière des objectifs du bouclier de la démocratie. Cela nécessite à son tour des réformes visant à accroître la souveraineté européenne sur les infrastructures numériques, les systèmes d'exploitation, les centres de données, les semi-conducteurs, l'IA, la cybersécurité, l'informatique en nuage et divers services et plateformes numériques. La révision des mandats des agences compétentes de l'UE, telles qu'Europol et Frontex, peut également jouer un rôle important dans l'amélioration de la résilience et de la protection contre les menaces hybrides.

Enfin, le projet de rapport souligne que le renforcement de la résilience démocratique exige également que les sociétés soient capables de continuer à fonctionner dans des conditions exceptionnelles ou perturbées. Les réformes visant à renforcer la préparation – allant des capacités de gestion de crise à la continuité des institutions démocratiques – doivent donc faire partie intégrante du bouclier européen de la démocratie. Le projet de rapport conclut que la protection et le renforcement des systèmes démocratiques européens requièrent non seulement une vigilance et une résilience à tous les niveaux de la société, mais aussi une stratégie coordonnée et tournée vers l'avenir de l'Union, soutenue par des ressources et un engagement politique suffisants.

ANNEXE: DÉCLARATION DES CONTRIBUTIONS

Conformément à l'article 8 de l'annexe I du règlement intérieur, le rapporteur déclare avoir inclus dans son rapport des contributions sur des questions relatives à l'objet du dossier qu'il a reçues, pour l'élaboration du projet de rapport, de la part des représentants d'intérêts relevant du champ d'application de l'accord interinstitutionnel sur un registre de transparence obligatoire suivants[1], ou des représentants des autorités publiques de pays tiers, y compris leurs missions diplomatiques et ambassades, suivants:

1. Représentants d'intérêts relevant du champ d'application de l'accord interinstitutionnel sur un registre de transparence obligatoire
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. Représentants des autorités publiques de pays tiers, y compris leurs missions diplomatiques et ambassades
sans objet

La liste ci-dessus est établie sous la responsabilité exclusive du rapporteur.

Lorsque des personnes physiques sont identifiées dans la liste par leur nom, leur fonction ou les deux, le rapporteur déclare avoir soumis aux personnes physiques concernées l'avis du Parlement européen relatif à la protection des données nº 484 (https://www.europarl.europa.eu/data-protect/index.do), qui définit les conditions applicables au traitement de leurs données à caractère personnel et les droits liés à ce traitement.

[1] Accord interinstitutionnel du 20 mai 2021 entre le Parlement européen, le Conseil de l'Union européenne et la Commission européenne sur un registre de transparence obligatoire (JO L 207 du 11.6.2021, p. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2021/611/oj).