



Document de séance

A9-0022/2022

8.2.2022

RAPPORT

sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation
(2020/2268(INI))

Commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation

Rapporteuse: Sandra Kalniete

SOMMAIRE

	Page
PROPOSITION DE RÉSOLUTION DU PARLEMENT EUROPÉEN	3
EXPOSÉ DES MOTIFS	62
POSITION MINORITAIRE DE CLARE DALY, AU NOM DU GROUPE THE LEFT	72
INFORMATIONS SUR L'ADOPTION PAR LA COMMISSION COMPÉTENTE AU FOND.....	73
VOTE PAR APPEL NOMINAL	74

PROPOSITION DE RÉSOLUTION DU PARLEMENT EUROPÉEN

sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (2020/2268(INI))

Le Parlement européen,

- vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7, 8, 11, 12, 39, 40, 47 et 52,
- vu la charte des Nations unies, en particulier ses articles 1 et 2,
- vu la résolution 2131 (XX) du 21 décembre 1965 de l'Assemblée générale des Nations unies intitulée «Déclaration sur l'inadmissibilité de l'intervention dans les affaires intérieures des États et la protection de leur indépendance et de leur souveraineté»,
- vu la convention de sauvegarde des droits de l'homme et des libertés fondamentales, et notamment ses articles 8, 9, 10, 11, 12, 13, 14, 16 et 17, ainsi que son protocole, et notamment son article 3,
- vu sa résolution du 23 novembre 2016 sur la communication stratégique de l'Union visant à contrer la propagande dirigée contre elle par des tiers¹ et sa recommandation du 13 mars 2019 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 tiers²,
- vu sa résolution du 13 juin 2018 sur la cyberdéfense³,
- 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 document de travail conjoint des services du 23 juin 2021 relatif au cinquième rapport sur la mise en œuvre du cadre commun de 2016 en matière de lutte contre les menaces hybrides et de la communication conjointe de 2018 intitulée «Accroître la résilience et renforcer la capacité à répondre aux menaces hybrides» (SWD(2021)0729),
- vu le plan d'action pour la démocratie européenne (COM(2020)0790),

¹ JO C 224 du 27.6.2018, p. 58.

² JO C 23 du 21.1.2021, p. 152.

³ JO C 28 du 27.1.2020, p. 57.

- vu la communication de la Commission du 3 décembre 2020 intitulée «Les médias européens dans la décennie numérique: un plan d’action pour soutenir la reprise et la transformation» (COM(2020)0784),
- vu la législation sur les services numériques,
- vu sa résolution du 20 octobre 2021 intitulée «Les médias européens dans la décennie numérique: un plan d’action pour soutenir la reprise et la transformation»⁴,
- vu le code de bonnes pratiques contre la désinformation adopté en 2018, les orientations de 2021 visant à renforcer le code de bonnes pratiques contre la désinformation (COM(2021)0262) et les recommandations du groupe des régulateurs européens pour les services de médias audiovisuels sur le nouveau code de bonnes pratiques contre la désinformation d’octobre 2021,
- vu le rapport spécial n° 09/2021 de la Cour des comptes intitulé «La désinformation concernant l’UE: un phénomène sous surveillance mais pas sous contrôle»,
- vu la proposition de directive du Parlement européen et du Conseil, présentée par la Commission le 16 décembre 2020, sur la résilience des entités critiques (COM(2020)0829) et la proposition d’annexe à la directive,
- vu le 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’Union⁵ (règlement sur le filtrage des IDE) et les lignes directrices du règlement sur le filtrage des IDE (C(2020)1981) de mars 2020,
- vu la communication conjointe de la Commission et du haut représentant de l’Union pour les affaires étrangères et la politique de sécurité du 16 décembre 2020 sur la stratégie de cybersécurité de l’UE pour la décennie numérique (JOIN(2020)0018),
- vu les articles de la Commission du droit international sur la responsabilité de l’État pour fait internationalement illicite,
- vu la proposition de directive du Parlement européen et du Conseil, présentée par la Commission le 16 décembre 2020, concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l’ensemble de l’Union, abrogeant la directive (UE) 2016/1148 (COM(2020)0823),
- vu la boîte à outils de l’Union européenne de mars 2021 pour la mise en place de mesures d’atténuation des risques sur la cybersécurité des réseaux 5G,
- vu le règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l’ENISA (Agence de l’Union européenne pour la cybersécurité) et à la

⁴ Textes adoptés de cette date, P9_TA(2021)0428.

⁵ JO L 79 I du 21.3.2019, p. 1.

certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013⁶,

- vu les études, notes d'information et analyses approfondies commandées par la commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (INGE),
 - vu l'audition de Frances Haugen organisée, le 8 novembre 2021, par sa commission du marché intérieur et de la protection des consommateurs, en collaboration avec d'autres commissions,
 - vu sa résolution du 7 octobre 2021 sur l'état des capacités de cyberdéfense de l'Union⁷,
 - vu les objectifs de développement durable des Nations unies, et notamment l'objectif 16, qui vise à promouvoir l'avènement de sociétés pacifiques et inclusives aux fins du développement durable,
 - vu le discours et la lettre d'intention sur l'état de l'Union 2021;
 - vu le rapport du secrétaire général des Nations unies du 10 septembre 2021 intitulé «Notre programme commun»,
 - vu la communication conjointe de la Commission et du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité du 10 juin 2020 intitulée «Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux» (JOIN(2020)0008),
 - vu la décision prise par le Conseil le 15 novembre 2021 en vue de modifier son régime de sanctions contre la Biélorussie en élargissant les critères de désignation à l'encontre des personnes physiques et des entités organisant les attaques hybrides et l'instrumentalisation des êtres humains menées par le régime biélorusse ou contribuant à ces violations,
 - vu sa décision du 18 juin 2020 sur la constitution d'une commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, et sur la définition de ses attributions, de sa composition numérique et de la durée de son mandat⁸, adoptée conformément à l'article 207 de son règlement intérieur,
 - vu l'article 54 de son règlement intérieur,
 - vu le rapport de la commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (A9-0022/2022),
- A. considérant que l'ingérence étrangère constitue une grave violation des valeurs et principes universels sur lesquels l'Union a été fondée, tels que la dignité humaine, la

⁶ JO L 151 du 7.6.2019, p. 15.

⁷ Textes adoptés de cette date, P9_TA(2021)0412.

⁸ JO C 362 du 8.9.2021, p. 186.

liberté, l'égalité, la solidarité, le respect des droits de l'homme et des libertés fondamentales, la démocratie et l'état de droit;

- B. considérant que l'ingérence, la manipulation de l'information et la désinformation étrangères constituent une violation des libertés fondamentales d'expression et d'information énoncées à l'article 11 de la charte des droits fondamentaux de l'Union européenne, menacent lesdites libertés et sapent les processus démocratiques de l'Union et de ses États membres, tels que la tenue d'élections libres et régulières; considérant que l'objectif de l'ingérence étrangère est de déformer ou de représenter incorrectement la réalité, de grossir artificiellement des arguments partiels et de discréditer des informations pour dévaloriser le discours politique et miner la confiance dans le système électoral et, partant, dans le processus démocratique en soi;
- C. considérant que toute action contre l'ingérence et la manipulation de l'information étrangères doit elle-même respecter les libertés fondamentales d'expression et d'information; considérant que l'Agence des droits fondamentaux de l'Union européenne joue un rôle essentiel dans l'évaluation du respect des droits fondamentaux, y compris de l'article 11 de la charte des droits fondamentaux, afin d'éviter des actions disproportionnées; considérant que les responsables de l'ingérence et de la manipulation de l'information étrangères abusent de ces libertés à leur avantage; considérant qu'il est donc essentiel d'intensifier la lutte préventive contre l'ingérence et la manipulation de l'information étrangères, car la démocratie nécessite que la population prenne des décisions éclairées;
- D. considérant qu'il est démontré que des acteurs étrangers, malveillants et autoritaires, étatiques ou non, parmi lesquels la Russie et la Chine, utilisent la manipulation de l'information et d'autres tactiques relevant de l'ingérence pour s'immiscer dans les processus démocratiques de l'Union; considérant que ces attaques, qui s'inscrivent dans une stratégie de guerre hybride et constituent une violation du droit international, induisent les citoyens en erreur, les trompent et affectent leurs choix électoraux, amplifient les polémiques, divisent, polarisent, exploitent les vulnérabilités des sociétés, encouragent les discours de haine, aggravent la situation des groupes vulnérables qui sont plus susceptibles d'être victimes de désinformation, faussent l'intégrité des élections et des référendums démocratiques, nourrissent la méfiance à l'égard des gouvernements nationaux, des autorités publiques et de l'ordre démocratique libéral, ont pour objectif de déstabiliser la démocratie européenne et constituent donc une grave menace pour la sécurité et la souveraineté de l'Union;
- E. considérant que l'ingérence étrangère est un comportement qui menace les valeurs, les procédures démocratiques, les processus politiques, la sécurité des États et des citoyens et la capacité de faire face à des situations exceptionnelles, ou a des incidences négatives sur ces éléments; considérant que cette ingérence est manipulatrice par nature; considérant qu'elle est menée et financée de façon délibérée et coordonnée; considérant que les responsables de cette ingérence, y compris leurs représentants à l'intérieur et à l'extérieur de leur propre territoire, peuvent être étatiques ou non; considérant qu'ils sont souvent aidés dans leur ingérence étrangère par des complices politiques dans les États membres, qui tirent des avantages politiques et économiques de la promotion de stratégies étrangères; considérant que le recours par des acteurs étrangers à des

représentants locaux et leur coopération avec des alliés locaux brouillent la limite entre ingérence étrangère et nationale;

- F. considérant que les tactiques en matière d'ingérence étrangère prennent de nombreuses formes, telles que la désinformation, la suppression de l'information, la manipulation de plateformes de réseaux sociaux et de leurs algorithmes, conditions générales et systèmes publicitaires, des cyberattaques, des opérations de piratage et de divulgation (hack-and-leak) visant à accéder à des informations sur les électeurs et à perturber la légitimité du processus électoral, des menaces et du harcèlement à l'encontre de journalistes, de chercheurs, de personnalités politiques et de membres d'organisations de la société civile, des dons et prêts dissimulés à des partis politiques, à des campagnes en faveur de certains candidats, à des organisations et à des médias, la mise en place de faux médias et d'organisations ou leur opération sous couverture, le recrutement et la cooptation de personnalités haut placées, le versement d'argent sale, la mise en scène de faux personnages ou de fausses identités, des pressions exercées en vue d'une autocensure, le détournement de l'histoire, de la religion et de la culture, des pressions sur des institutions éducatives et culturelles, la mainmise sur des infrastructures critiques, des pressions sur les ressortissants étrangers vivant dans l'Union, l'instrumentalisation des migrants et l'espionnage; considérant que ces tactiques sont souvent combinées pour démultiplier leurs effets;
- G. considérant que la manipulation de l'information et la diffusion de la désinformation peuvent servir les intérêts économiques d'acteurs étatiques ou non ainsi que de leurs représentants; considérant qu'elles créent des dépendances économiques qui peuvent être exploitées à des fins politiques; considérant que, dans un monde de concurrence internationale non militaire, l'ingérence étrangère peut constituer un excellent moyen de déstabiliser et d'affaiblir certains rivaux, ou d'améliorer son avantage concurrentiel en créant des canaux d'influence ou des dépendances dans les chaînes d'approvisionnement, voire en recourant au chantage ou à la contrainte; considérant que la désinformation est la cause directe et indirecte de dommages économiques qui n'ont pas fait l'objet d'une évaluation systématique;
- H. considérant que la mésinformation peut être définie comme une information manifestement fautive qui n'a pas été conçue pour causer un préjudice, alors que la désinformation est une information manifestement fautive ou trompeuse qui a été intentionnellement créée, présentée ou diffusée dans le but de causer un préjudice ou d'avoir un effet potentiellement déstabilisateur sur la société en trompant le public, ou dans un but lucratif;
- I. considérant qu'il est nécessaire de convenir, au sein de l'Union, de définitions et de méthodes communes et précises pour améliorer la connaissance partagée des menaces et mettre au point les normes européennes nécessaires pour rendre l'imputation de responsabilité et les réponses plus efficaces; considérant que le Service européen pour l'action extérieure a accompli un travail considérable dans ce domaine; considérant que ces définitions doivent garantir l'absence de vulnérabilité à l'ingérence extérieure et le respect des droits de l'homme; considérant qu'il est crucial de coopérer avec des partenaires partageant les mêmes orientations, dans les enceintes internationales pertinentes, et de s'accorder sur des définitions communes de l'ingérence étrangère, afin d'établir des normes et des standards internationaux; considérant que l'Union devrait

montrer l'exemple en fixant des règles internationales claires pour l'imputation de responsabilité dans les cas d'ingérence étrangère;

Nécessité d'une stratégie coordonnée contre l'ingérence étrangère

- J. considérant que les tentatives d'ingérence étrangère se multiplient dans le monde et deviennent de plus en plus systémiques et sophistiquées, grâce à une utilisation généralisée de l'intelligence artificielle (IA), ce qui complique l'imputation de responsabilité;
- K. considérant qu'il est du devoir de l'Union et de ses États membres de défendre leurs citoyens, infrastructures et systèmes démocratiques contre les tentatives d'ingérence étrangère; considérant néanmoins que l'Union et ses États membres semblent ne pas disposer des moyens appropriés et suffisants pour mieux prévenir et détecter ces menaces, lutter contre elles, déterminer leurs auteurs et punir ces derniers;
- L. considérant que l'existence de ces problèmes semble globalement ignorée parmi les décideurs politiques et plus généralement dans la population, ce qui peut contribuer involontairement à créer d'autres vulnérabilités; considérant que la question des campagnes de désinformation n'a pas constitué une priorité pour les décideurs politiques européens; considérant que les auditions et les travaux de la commission spéciale INGE ont contribué à la reconnaissance publique et à la contextualisation de ces questions, et ont réussi à poser un cadre au débat européen sur l'ingérence étrangère; considérant que les campagnes incessantes de désinformation menées depuis l'étranger ont déjà conduit à l'émergence d'une désinformation d'origine interne;
- M. considérant que la surveillance transparente de l'état de l'ingérence étrangère en temps réel par des organismes institutionnels et des analystes et vérificateurs de faits indépendants, la coordination efficace de leurs actions et l'échange d'informations s'avèrent essentiels pour que les mesures appropriées soient prises, non seulement pour fournir des informations sur les attaques malveillantes en cours, mais aussi pour lutter contre elles; considérant qu'il faut également s'intéresser de près à la cartographie de la société, pour déterminer quels domaines sont les plus vulnérables et les plus sensibles à la manipulation et à la désinformation étrangères, et s'attaquer aux causes de ces vulnérabilités;
- N. considérant que la priorité de la défense européenne, à savoir la préparation et la résilience des citoyens de l'Union face à l'ingérence et à la manipulation de l'information étrangères, nécessite une approche à long terme et globale de la société, en commençant au niveau de l'enseignement et en sensibilisant, à un stade précoce, le public à ces questions;
- O. considérant qu'il est nécessaire de coopérer et de se coordonner, aux différents niveaux administratifs et dans les différents secteurs, entre États membres, au niveau de l'Union et avec les pays partageant les mêmes valeurs, ainsi qu'avec la société civile et le secteur privé, afin de repérer les vulnérabilités, de détecter les attaques et de les contrecarrer; considérant qu'il est urgent de faire correspondre le niveau de menaces perçu et la sécurité nationale;

Renforcement de la résilience par la connaissance de la situation, l'éducation et la formation aux médias et à l'information, le pluralisme des médias, le journalisme indépendant et l'éducation

- P. considérant que la connaissance de la situation, de solides systèmes démocratiques, un état de droit robuste, une société civile dynamique, des alertes rapides et l'évaluation des menaces constituent les premières étapes dans la lutte contre l'ingérence et la manipulation de l'information; considérant qu'en dépit de tous les progrès accomplis pour améliorer la connaissance de l'ingérence étrangère, de nombreuses personnes, y compris des décideurs politiques et des fonctionnaires travaillant dans les secteurs potentiellement concernés, sont encore inconscientes des risques que pourrait entraîner l'ingérence étrangère et ne savent pas comment y répondre;
- Q. considérant que la bonne qualité, l'indépendance et le financement durable et transparent des médias et des journalistes professionnels sont essentiels pour la liberté et le pluralisme des médias ainsi que l'état de droit; considérant que ces principes constituent un pilier de la démocratie et le meilleur remède à la désinformation; considérant que certains acteurs étrangers profitent de la liberté de la presse occidentale pour diffuser de la désinformation; considérant que l'ère du numérique est une époque difficile pour les médias professionnels et le journalisme traditionnel, sources d'information de qualité; considérant qu'une éducation et une formation de qualité au journalisme, à l'intérieur comme à l'extérieur de l'Union, sont nécessaires pour garantir des analyses journalistiques compétentes et des normes rédactionnelles élevées; considérant que l'Union doit continuer à soutenir le journalisme dans la sphère numérique; considérant que la communication fondée sur la science devrait jouer un rôle important;
- R. considérant que des médias publics disposant d'une indépendance éditoriale sont essentiels et irremplaçables, car ils fournissent au public des services d'information impartiaux et de qualité élevée; considérant qu'il est vital de les protéger contre toute prise de contrôle hostile et de renforcer ce pilier central de la lutte contre la désinformation;
- S. considérant que les méthodologies et définitions utilisées pour analyser l'ingérence étrangère varient selon les acteurs et les institutions et se situent à différents degrés d'intelligibilité; considérant que ces différences peuvent entraver les comparaisons de la surveillance, de l'analyse et de l'évaluation du niveau de menace, ce qui complique toute action conjointe; considérant qu'il est nécessaire de fixer une définition et une méthode au niveau de l'Union pour améliorer l'analyse commune des menaces;
- T. considérant qu'il est indispensable de compléter la terminologie qui se concentre sur des contenus comme les informations fausses, inventées ou trompeuses, la mésinformation et la désinformation par une terminologie centrée sur le comportement, afin de lutter correctement contre le problème; considérant que cette terminologie doit être harmonisée et scrupuleusement respectée;
- U. considérant qu'une formation aux médias et au numérique et un travail de sensibilisation, auprès des enfants comme des adultes, constituent des outils importants pour rendre les citoyens plus résilients face aux tentatives d'ingérence dans l'espace de

l'information ainsi que pour prévenir toute manipulation et polarisation; considérant qu'en général, les sociétés qui présentent une bonne éducation aux médias résistent mieux à l'ingérence étrangère; considérant que certaines méthodes de travail des journalistes, telles que le journalisme constructif, pourraient contribuer à renforcer la confiance des citoyens dans le journalisme;

- V. considérant que la manipulation de l'information peut prendre plusieurs formes, telles que la diffusion de désinformation et d'informations complètement fausses, la représentation déformée de faits, de récits et d'opinions, la suppression de certaines informations ou opinions, l'utilisation d'informations hors de leur contexte, la manipulation des émotions, la promotion de discours de haine ou de certaines opinions au détriment d'autres et le harcèlement de personnes pour les faire taire et les opprimer; considérant que l'un des objectifs de la manipulation de l'information est de semer la confusion afin de susciter une perte de confiance des citoyens envers les «gardiens de l'information» d'hier et d'aujourd'hui; considérant qu'il existe une frontière ténue entre la liberté d'expression et la promotion des discours de haine et de la désinformation et qu'il ne faut pas la franchir;
- W. signale que l'Azerbaïdjan, la Chine, la Turquie et la Russie, entre autres, ont pris des journalistes et des opposants pour cibles au sein de l'Union, comme le blogueur et opposant azerbaïdjanais Mahammad Mirzali à Nantes ou le journaliste turc Erk Acarer à Berlin;
- X. considérant qu'il existe des éléments concrets prouvant que les processus démocratiques de l'Union sont la cible d'attaques et d'ingérence au moyen de campagnes de désinformation mettant à mal ses idéaux démocratiques et ses droits fondamentaux; considérant que la désinformation liée à des sujets tels que, entre autres, le genre, les personnes LGBTIQ+, la santé et les droits sexuels et génésiques ainsi que les minorités menace les droits de l'homme, porte atteinte aux droits numériques et politiques ainsi qu'à la sûreté et à la sécurité de ses cibles, et sème la discorde entre les États membres; considérant que, pendant les campagnes électorales, les candidates sont beaucoup plus souvent la cible de commentaires sexistes, ce qui aboutit à décourager les femmes de participer aux processus démocratiques; considérant que les personnes à l'origine de ces campagnes de désinformation, sous l'apparence de promotion de valeurs «traditionnelles» ou «conservatrices», forment des alliances stratégiques avec des partenaires locaux afin d'avoir accès à leurs renseignements et auraient reçu, selon certaines sources, des millions d'euros de financement étranger;
- Y. considérant que les institutions, les journalistes, les faiseurs d'opinion et le secteur privé, mais aussi chaque composante de la société et chaque individu ont un rôle important à jouer pour repérer la diffusion de désinformation, y mettre un terme et avertir les personnes de leur entourage qui sont en danger; considérant que la société civile, les universitaires et les journalistes ont déjà fortement contribué à sensibiliser le public et à accroître la résilience de la société, y compris en coopération avec leurs homologues dans les pays partenaires;
- Z. considérant que les organisations de la société civile représentant les minorités et les organisations de défense des droits de l'homme à travers l'Europe souffrent d'un manque chronique de fonds, malgré le rôle crucial qu'elles jouent dans la sensibilisation

et la lutte contre la désinformation; considérant que les organisations de la société civile devraient disposer de ressources suffisantes pour pouvoir jouer leur rôle et limiter les effets de l'ingérence étrangère;

- AA. considérant qu'il est important d'accéder facilement et rapidement à des informations fondées sur les faits et issues de sources fiables lorsque la désinformation commence à se répandre;
- AB. considérant qu'il est nécessaire de détecter rapidement les opérations d'ingérence étrangère et les tentatives de manipulation de l'information si l'on veut lutter contre elles; considérant que l'analyse du renseignement de l'Union et la connaissance de la situation requièrent que les États membres acceptent de partager leurs informations; considérant que la présidente de la Commission a proposé d'envisager la création d'un centre commun de connaissance de la situation; considérant que la prévention et les mesures prises en amont, notamment la réfutation des idées fausses et l'établissement d'un écosystème de l'information sain, sont bien plus efficaces que la vérification des faits et le rétablissement de la vérité («debunking») en aval, ces derniers touchant un public moins large que la désinformation originale; considérant que l'Union et ses États membres disposent actuellement de capacités insuffisantes pour prendre de telles mesures; considérant que de nouveaux outils d'analyse fondés sur l'IA, tels que le site lituanien debunk.eu, pourraient contribuer à détecter les attaques, à partager les connaissances et à informer le public;
- AC. considérant que la désinformation prospère lorsque les discours avancés à l'échelle nationale ou européenne se révèlent faibles ou morcelés, et se nourrit de la polarisation des débats émotionnels, des points faibles et des préjugés de la société et des individus; considérant que la désinformation fausse le débat public autour des élections et des autres processus démocratiques et peut rendre difficile pour les citoyens la prise de décisions éclairées;

Ingérence étrangère qui tire parti des plateformes en ligne

- AD. considérant que les plateformes en ligne peuvent s'avérer des outils facilement accessibles et peu onéreux pour ceux qui se livrent à la manipulation de l'information et à d'autres formes d'ingérence, telles que la haine, le harcèlement, les atteintes à la santé et à la sécurité de nos communautés en ligne, la réduction au silence des opposants, l'espionnage ou la diffusion de désinformation; considérant qu'il a été prouvé que leur fonctionnement encourage l'expression d'opinions extrêmes et radicales plutôt que d'informations vérifiées; considérant que les plateformes ont également leurs propres intérêts et ne sont pas nécessairement neutres dans leur traitement de l'information; considérant que certaines plateformes en ligne tirent un profit immense du système qui propage la division, l'extrémisme et la polarisation; considérant que l'espace en ligne est devenu tout aussi important pour notre démocratie que l'espace physique et qu'il nécessite donc des règles adaptées;
- AE. considérant que les plateformes ont accéléré et amplifié la propagation de la mésinformation et de la désinformation d'une manière sans précédent, ce qui soulève des difficultés; considérant que les plateformes en ligne contrôlent le flux des informations et de la publicité en ligne, et qu'elles conçoivent et utilisent des algorithmes pour contrôler lesdits flux; considérant qu'elles ne sont pas transparentes,

ne disposent pas de procédures adéquates de vérification de l'identité, usent d'une terminologie vague et obscure et ne partagent que très peu d'informations, voire aucune, sur la conception, l'utilisation et les effets de ces algorithmes; considérant que les algorithmes des plateformes en ligne peuvent créer une certaine dépendance, qui constitue un grave problème de santé publique auquel il faut trouver une solution; considérant que les plateformes en ligne devraient être responsables des effets néfastes de leurs services, étant donné que certaines étaient conscientes des failles de leurs algorithmes, en particulier de leur rôle dans la diffusion de contenus polémiques, mais n'y ont pas remédié afin de maximiser leurs profits, comme l'ont révélé des lanceurs d'alerte;

- AF. considérant que toutes les mesures prises contre la propagation de la COVID-19, y compris la vaccination dans l'ensemble de l'Union, se sont heurtées à des campagnes d'ingérence et de manipulation de l'information; considérant que les plateformes en ligne n'ont pas réussi à coordonner leurs efforts pour endiguer ces phénomènes, voire ont peut-être contribué à leur diffusion; considérant que cette désinformation peut mettre en danger de mort lorsqu'elle dissuade les personnes de se faire vacciner ou promeut de faux traitements; considérant que la pandémie a exacerbé le combat généralisé que se livrent la démocratie et l'autoritarisme, et a poussé des États autoritaires, comme la Chine et la Russie, et des acteurs non étatiques à employer une vaste gamme d'instruments visibles ou dissimulés dans l'espoir de déstabiliser leurs adversaires démocratiques; considérant que les «Facebook Papers» ont révélé que la plateforme avait été incapable de lutter contre la désinformation liée au vaccin, y compris en anglais; considérant que, dans les autres langues, la situation est encore pire pour ce type de désinformation; considérant que ce problème concerne toutes les plateformes;
- AG. considérant que de nombreux prestataires immatriculés dans l'Union vendent de faux «likes», abonnés, commentaires et partages à tout acteur souhaitant stimuler artificiellement sa visibilité en ligne; considérant qu'aucune utilisation légitime ne justifie ces services, mais qu'ils peuvent poursuivre des objectifs préjudiciables tels que la manipulation des élections et d'autres processus démocratiques, la promotion d'escroqueries, la publication de commentaires négatifs sur les produits de la concurrence, la spoliation des annonceurs et la création d'un faux public utilisé pour orienter la conversation, lancer des attaques personnelles et donner une visibilité artificielle à certaines opinions qui n'attireraient, sans cela, aucune attention; considérant que certains régimes étrangers, tels que la Russie et la Chine, utilisent massivement ces outils en ligne pour influencer le débat public dans les pays européens; considérant que la désinformation peut déstabiliser la démocratie européenne;
- AH. considérant que les plateformes sociales, les outils numériques et les applications collectent et stockent des quantités considérables de données très détaillées à caractère personnel et souvent sensible sur chaque utilisateur; considérant que lesdites données peuvent servir à prévoir les tendances comportementales, à renforcer les biais cognitifs et à orienter la prise de décision; considérant que lesdites données sont exploitées à des fins commerciales; considérant que des fuites de données se produisent de façon répétée, au détriment de la sécurité des victimes, et que les données peuvent être vendues sur le marché noir; considérant que ces bases de données pourraient constituer des mines d'or pour des acteurs souhaitant cibler certains groupes ou individus;

- AI. considérant que les plateformes sont généralement conçues pour que choisir de ne pas partager ses données soit moins intuitif, plus fastidieux et plus chronophage que de les partager;
- AJ. considérant que les plateformes en ligne sont associées à la plupart des pans de nos existences et que la diffusion d'informations sur les plateformes peut influencer considérablement notre pensée et notre comportement, par exemple en ce qui concerne les préférences électorales, les décisions économiques et sociales ainsi que le choix de ses sources d'information; considérant que ces choix déterminants d'importance publique sont aujourd'hui soumis, en réalité, aux intérêts commerciaux d'entreprises privées;
- AK. considérant que les mécanismes de traitement des algorithmes et d'autres fonctionnalités des plateformes de réseaux sociaux sont conçus pour maximiser les interactions; considérant que l'on rapporte souvent que ces fonctionnalités mettent en valeur les contenus polarisants, discriminatoires et facilitant la radicalisation, et qu'ils maintiennent les utilisateurs dans des bulles partageant les mêmes valeurs; considérant qu'il en résulte une radicalisation progressive des utilisateurs de plateformes ainsi qu'une déformation et une dégradation des processus de discussion collective, plutôt que la protection des processus démocratiques et des individus; considérant que le manque de coordination entre les mesures prises par les plateformes a entraîné des disparités et a permis à la désinformation de se diffuser d'une plateforme à l'autre; considérant que le modèle économique consistant à monétiser la diffusion d'informations polarisantes et la conception d'algorithmes fait que les plateformes sont une cible facile de manipulation par des acteurs étrangers hostiles; considérant qu'il serait possible de revoir la conception desdites plateformes afin de faire naître un espace public en ligne plus saine;
- AL. considérant que la création d'hypertrucages de documents sonores et audiovisuels («deepfakes») est devenue de plus en plus facile grâce à l'arrivée sur le marché de technologies peu chères et faciles à utiliser; considérant que la diffusion de ce type de documents est un problème qui prend des proportions gigantesques; considérant toutefois que 90 % des recherches actuelles sur les hypertrucages sont consacrés à leur création et seulement 10 % à leur détection;
- AM. considérant que les systèmes d'autorégulation, tels que le code de bonnes pratiques contre la désinformation adopté en 2018, ont permis des améliorations; considérant toutefois que dépendre de la bonne volonté des plateformes en ligne ne fonctionne pas, n'est pas efficace et n'a produit que peu de données pertinentes sur leur impact global; considérant qu'en outre, les plateformes ont pris des mesures individuelles, à l'importance et aux effets variables, qui ont permis au contenu supprimé de continuer à se diffuser ailleurs, en passant par des portes dérobées; considérant qu'il faut fixer un ensemble de règles et de sanctions claires afin que le code de bonnes pratiques ait un effet suffisant sur l'espace en ligne;
- AN. considérant que le plan d'action pour la démocratie européenne vise à renforcer le code de bonnes pratiques de 2018; considérant que ce plan et la législation sur les services numériques s'écartent du modèle de l'autorégulation et cherchent à introduire davantage de garanties et de protections pour les utilisateurs, en renforçant l'autonomie, en

dépassant la passivité vis-à-vis des services proposés et en introduisant des mesures qui imposent une plus grande transparence et une obligation de rendre des comptes aux entreprises ainsi que de nouvelles obligations aux plateformes;

- AO. considérant que les mesures actuelles contre les campagnes de désinformation sur les plateformes en ligne ne sont ni efficaces ni dissuasives, et qu'elles permettent aux plateformes de continuer à promouvoir des contenus discriminatoires et malveillants;
- AP. considérant que les plateformes consacrent nettement plus de ressources à la gestion de contenus en anglais que dans les langues moins usitées, même celles de grande diffusion;
- AQ. considérant que les procédures de réclamation et de recours proposées par les plateformes sont généralement inadaptées;
- AR. considérant qu'au cours des derniers mois, plusieurs acteurs majeurs se sont pliés à des règles de censure, par exemple lors des élections parlementaires russes de septembre 2021, lorsque Google et Apple ont supprimé les applications de vote intelligent de leurs boutiques en Russie;
- AS. considérant que le manque de transparence en ce qui concerne les choix algorithmiques des plateformes rend impossible la vérification de leurs affirmations sur ce qu'elles font pour lutter contre l'ingérence et la manipulation de l'information, et de l'effet des mesures prises; considérant que l'effet supposé de ces mesures, tel que l'annoncent les rapports annuels publiés par les plateformes, est éloigné de leur efficacité réelle, comme les «Facebook Papers» l'ont récemment démontré;
- AT. considérant que l'opacité de la publicité ciblée fait qu'un grand nombre de publicités en ligne émanant de marques réputées, parfois même d'institutions publiques, finissent sur des sites qui appellent au terrorisme ou qui hébergent des discours haineux et de la désinformation, et financent la croissance de ce type de site, à l'insu ou sans le consentement des annonceurs;
- AU. considérant qu'un petit nombre de grandes entreprises de technologies publicitaires, en premier lieu Google et Facebook, contrôlent et se partagent le marché de la publicité en ligne; considérant que cette forte concentration du marché aux mains d'un petit nombre d'entreprises conduit à une répartition très déséquilibrée du pouvoir; considérant que l'utilisation des techniques dites de «piège à clics» et la capacité de ces quelques acteurs à déterminer quels contenus sont monétisés et lesquels ne le sont pas, et ce bien que les algorithmes qu'ils utilisent ne puissent pas faire la différence entre de la désinformation et du contenu informatif normal, constituent une menace pour la diversité des médias; considérant que le marché de la publicité ciblée est profondément opaque; considérant que les entreprises de technologies publicitaires font preuve de négligence dans le contrôle du placement des annonces publicitaires, mais forcent les marques à en payer le prix;

Infrastructures critiques et secteurs stratégiques

- AV. considérant que la gestion des menaces portant sur les infrastructures critiques, particulièrement lorsqu'elles font partie d'une stratégie hybride, synchronisée et

malveillante, nécessite des efforts conjoints et coordonnés de différents secteurs, à plusieurs niveaux – européen, national, régional et local – et à divers moments;

- AW. considérant que la Commission a proposé une nouvelle directive pour renforcer la résilience des entités critiques fournissant des services essentiels dans l'Union, qui comprend une proposition de liste de nouveaux types d'infrastructures critiques; considérant que la liste des services figurera en annexe de la directive;
- AX. considérant que la mondialisation croissante de la division du travail et des chaînes de production a entraîné des déficits de fabrication et de compétences dans des secteurs clés dans l'ensemble de l'Union; considérant que cela s'est traduit par une forte dépendance de l'Union vis-à-vis de nombreux produits essentiels et actifs principaux importés de l'étranger, qui risquent de présenter des vulnérabilités intrinsèques; considérant que la résilience des chaînes d'approvisionnement devrait figurer parmi les priorités des décideurs politiques de l'Union;
- AY. considérant que les investissements directs étrangers (IDE) — investissements de pays tiers et d'entreprises étrangères — dans des secteurs stratégiques de l'Union, mais aussi dans des régions voisines, comme les Balkans occidentaux, en particulier l'acquisition de structures critiques par la Chine, ont suscité des préoccupations croissantes ces dernières années, compte tenu de l'importance de plus en plus élevée du lien entre commerce et sécurité; considérant que ces investissements risquent de créer des dépendances économiques et d'entraîner une perte de connaissances dans des secteurs clés de la production et de l'industrie;
- AZ. considérant que l'autonomie stratégique ouverte de l'Union nécessite le contrôle des infrastructures stratégiques européennes; considérant que la Commission et les États membres se sont déclarés de plus en plus préoccupés par la sécurité et le contrôle des technologies et des infrastructures en Europe;

Ingérence étrangère dans les processus électoraux

- BA. considérant que les acteurs malveillants qui cherchent à s'immiscer dans des processus électoraux exploitent l'ouverture et le pluralisme de nos sociétés comme une vulnérabilité stratégique afin d'attaquer les processus démocratiques et la résilience de l'Union et de ses États membres; considérant que l'ingérence étrangère est plus dangereuse en période électorale, car c'est un moment où les citoyens s'intéressent de nouveau et participent plus activement aux activités politiques traditionnelles;
- BB. considérant que la nature spécifique de l'ingérence étrangère dans les processus électoraux, l'utilisation des nouvelles technologies à cet égard et les conséquences qui pourraient en découler représentent une menace particulièrement grave pour la démocratie; considérant que l'ingérence étrangère dans les processus électoraux va bien au-delà de la guerre de l'information dans les médias sociaux en faveur de candidats précis, et cherche à pirater les bases de données, à obtenir des renseignements sur les électeurs inscrits et à perturber directement le fonctionnement normal, la compétitivité et la légitimité du processus électoral; considérant que l'ingérence étrangère vise à susciter le doute, l'incertitude et la méfiance, en cherchant non seulement à modifier le résultat des élections, mais aussi à délégitimer l'ensemble du processus électoral;

Financement dissimulé des activités politiques provenant d'acteurs et de donateurs étrangers

- BC. considérant que de nombreux éléments de preuve montrent que des acteurs étrangers s'immiscent activement dans le fonctionnement démocratique de l'Union et de ses États membres, notamment en période d'élections et de référendums, au moyen d'opérations de financement dissimulées;
- BD. considérant, par exemple, que la Russie, la Chine et d'autres régimes autoritaires ont injecté plus de 300 millions de dollars américains dans 33 pays à des fins d'ingérence dans les processus démocratiques; considérant que l'Iran, le Venezuela et d'autres acteurs du Moyen-Orient et de l'extrême droite américaine ont également participé à des financements dissimulés; considérant que cette tendance s'accélère clairement; considérant que la moitié de ces affaires concernent des actions menées par la Russie en Europe; considérant que la corruption et le blanchiment de capitaux sont une source de financement politique en provenance des pays autoritaires;
- BE. considérant que les outils médiatiques créés par des donateurs étrangers d'une façon opaque sont devenus des moyens extrêmement efficaces de rassembler un grand nombre d'abonnés et de produire de l'engagement;
- BF. considérant que ces opérations financent des partis politiques extrémistes, populistes et anti-européens, et d'autres mouvements ou individus qui veulent aggraver la fragmentation de la société et nuire à la légitimité des autorités publiques nationales et européennes; considérant que cela a permis à ces partis ou mouvements d'accroître leur influence;
- BG. considérant que la Russie cherche à établir des contacts avec les partis, personnalités et mouvements afin de s'appuyer sur des acteurs des institutions de l'Union pour légitimer ses positions et les gouvernements fantoches qu'elle soutient, pour faire pression en faveur d'un allègement des sanctions et pour atténuer les conséquences de son isolement international; considérant que des partis tels que la *Freiheitliche Partei Österreichs* autrichienne, le Rassemblement national français et la *Lega Nord* italienne ont signé des accords de coopération avec le parti Russie unie du président Vladimir Poutine et sont désormais accusés dans les médias d'être disposés à accepter un financement politique de la part de la Russie; considérant que d'autres partis européens, tels que l'*Alternative für Deutschland* (AfD) allemande, le *Fidesz* et le *Jobbik* hongrois, et le *Brexit Party* britannique auraient également des contacts étroits avec le Kremlin; considérant que l'AfD et le Jobbik ont également travaillé en tant que soi-disant «observateurs électoraux» lors d'élections contrôlées par le Kremlin, par exemple à Donetsk et à Lougansk dans l'est de l'Ukraine, afin de surveiller et de légitimer des élections soutenues par la Russie; considérant que les révélations sur les contacts étroits et réguliers entre des fonctionnaires russes et les représentants d'un groupe de sécessionnistes catalans en Espagne, ainsi qu'entre des fonctionnaires russes et le plus grand donateur privé pour la campagne «Brexit Vote Leave», nécessitent une enquête approfondie et s'inscrivent dans le cadre de la stratégie plus large de la Russie visant à exploiter chaque occasion de manipulation rhétorique à des fins de déstabilisation;

- BH. considérant que le Groupe d'États contre la corruption (GRECO) du Conseil de l'Europe et la Commission de Venise ont déjà formulé des recommandations de vaste portée afin de réduire l'incidence d'une possible ingérence des acteurs étrangers au moyen du financement politique;
- BI. considérant que les lois électorales, en particulier les dispositions relatives au financement des activités politiques, ne sont pas suffisamment coordonnées au niveau de l'Union, et permettent donc des méthodes de financement opaques provenant d'acteurs étrangers; considérant que la définition juridique des dons à des partis politiques est trop étroite et autorise des contributions étrangères en nature dans l'Union européenne;
- BJ. considérant que, dans certains États membres, la publicité politique en ligne n'est pas soumise aux règles applicables à la publicité politique hors ligne; considérant que la publicité politique en ligne souffre d'un grave manque de transparence, qui empêche les autorités de réglementation de faire appliquer les plafonds de dépenses et de lutter contre les sources illicites de financement, ce qui peut avoir des conséquences désastreuses pour l'intégrité de nos systèmes électoraux;
- BK. considérant que le manque de transparence du financement crée un environnement propice à la corruption, qui accompagne souvent le financement et les investissements étrangers;
- BL. considérant que le règlement (UE, Euratom) n° 1141/2014 du 22 octobre 2014 relatif au statut et au financement des partis politiques européens et des fondations politiques européennes⁹ est en cours de révision en vue d'atteindre un plus grand niveau de transparence en matière de financement des activités politiques;
- BM. considérant que le rôle des fondations politiques s'est affirmé ces dernières années, qu'elles jouent, dans la majorité des cas, un rôle positif en politique et dans le renforcement de la démocratie, mais que certaines sont devenues des vecteurs imprévisibles de formes malveillantes de financement et d'ingérence indirecte;
- BN. considérant que les technologies modernes et les actifs numériques, tels que les cryptomonnaies, sont utilisés pour maquiller les transactions financières illicites au profit d'acteurs et de partis politiques;

Cybersécurité et résilience face aux cyberattaques

- BO. considérant que l'incidence des cyberattaques et des incidents facilités par l'internet causés par des acteurs hostiles, étatiques ou non, a connu une hausse ces dernières années; considérant que plusieurs cyberattaques, telles que les campagnes mondiales d'hameçonnage ciblant les structures stratégiques de stockage des vaccins et les cyberattaques contre l'Agence européenne des médicaments, l'Autorité bancaire européenne, le Parlement norvégien et de nombreuses autres institutions, ont été

⁹ JO L 317 du 4.11.2014, p. 1.

attribuées à des groupes de pirates informatiques soutenus par des États, principalement affiliés aux gouvernements russe et chinois;

- BP. considérant que l'Union européenne s'est engagée à appliquer le droit international existant, en particulier la charte des Nations unies, dans le cyberspace; considérant que des acteurs étrangers malveillants exploitent l'absence d'un cadre juridique international solide dans le domaine du cyberspace;
- BQ. considérant que les États membres ont renforcé leur coopération dans le domaine de la cyberdéfense, dans le cadre de la coopération structurée permanente, y compris en mettant en place des équipes d'intervention rapide en cas d'incident informatique; considérant que le programme européen de développement industriel dans le domaine de la défense inclut le renseignement, les communications sécurisées et la cyberdéfense dans ses programmes de travail; considérant que la capacité actuelle à faire face aux cybermenaces est limitée en raison du manque de ressources humaines et financières, par exemple dans des structures critiques telles que les hôpitaux; considérant que l'Union s'est engagée à investir 1,6 milliard d'euros, dans le cadre du programme pour une Europe numérique¹⁰, dans la capacité de réponse et le déploiement d'outils de cybersécurité pour les administrations publiques, les entreprises et les particuliers, ainsi qu'à renforcer la coopération entre les secteurs public et privé;
- BR. considérant que la fragmentation des capacités et des stratégies de l'Union dans le domaine cybernétique et les lacunes dans ce secteur deviennent un problème croissant, comme l'a souligné la Cour des comptes européenne¹¹; considérant que la boîte à outils cyberdiplomatique de l'Union, mise en place en mai 2019, a démontré la valeur ajoutée d'une réponse diplomatique conjointe de l'Union face aux actes de cybermalveillance; considérant que le 30 juillet 2020, le Conseil a décidé pour la première fois d'appliquer des sanctions à l'encontre de personnes, d'entités et d'organismes responsables de diverses cyberattaques ou impliqués dans celles-ci;
- BS. considérant que des programmes de surveillance illicites et à grande échelle, tels que Pegasus, ont été utilisés par des acteurs étatiques étrangers pour cibler des journalistes, des militants des droits de l'homme, des universitaires, des fonctionnaires de l'État et des responsables politiques, y compris des chefs d'État européens; considérant que des États membres ont également eu recours aux logiciels espions de surveillance;

Protection des États membres, des institutions, des agences, des délégations et des missions de l'Union européenne

- BT. considérant que le caractère décentralisé et multinational des institutions de l'Union, ainsi que de leurs missions et de leurs opérations, en fait de plus en plus souvent des cibles et est exploité par des acteurs étrangers malveillants souhaitant semer la division au sein de l'Union; considérant que les institutions européennes manquent globalement d'une culture de la sécurité, alors qu'elles constituent des cibles manifestes; considérant que le Parlement, en tant qu'institution de l'Union démocratiquement élue, est confronté

¹⁰ <https://www.consilium.europa.eu/fr/policies/cybersecurity/>

¹¹

https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_FR.pdf

à des défis particuliers; considérant que plusieurs cas ont révélé que les institutions de l'Union semblent vulnérables à l'infiltration étrangère; considérant qu'il convient d'assurer la sécurité du personnel de l'Union;

- BU. considérant qu'il est prioritaire de mettre en place des procédures de gestion de crise solides et cohérentes; considérant qu'il convient d'offrir une formation supplémentaire afin d'améliorer la préparation du personnel;
- BV. considérant que des cyberattaques ont récemment visé plusieurs institutions de l'Union, ce qui souligne la nécessité d'une forte coopération interinstitutionnelle en matière de détection, de surveillance et de partage d'informations lors des cyberattaques et/ou en vue de les prévenir, notamment durant les missions et opérations de la politique de sécurité et de défense commune de l'Union; considérant que l'Union et ses États membres devraient organiser des exercices conjoints de manière régulière, afin de déceler les points faibles et de prendre les mesures qui s'imposent;

Ingérence d'acteurs étrangers par le recrutement de personnalités haut placées, les diasporas nationales, les universités et les manifestations culturelles

- BW. considérant que, en échange de leurs connaissances et au détriment des intérêts des citoyens de l'Union et de ses États membres, un certain nombre d'acteurs politiques, y compris d'anciens dirigeants européens et hauts fonctionnaires, sont engagés ou cooptés par des entreprises privées ou nationales étrangères contrôlées par des États autoritaires;
- BX. considérant que certains pays sont particulièrement actifs dans le domaine du recrutement et de la cooptation de personnalités haut placées, en particulier la Russie et la Chine, mais également l'Arabie saoudite et d'autres pays du Golfe comme le montrent les exemples de l'ancien chancelier allemand Gerhard Schröder et de l'ancien Premier ministre finlandais Paavo Lipponen, qui se sont tous deux associés à Gazprom pour accélérer le processus d'approbation de Nord Stream 1 et 2, de l'ancienne ministre autrichienne des affaires étrangères Karin Kneissl, qui a été nommée membre du conseil d'administration de Rosneft, de l'ancien Premier ministre français François Fillon, qui a été nommé membre du conseil d'administration de Zarubejneft, de l'ancien Premier ministre français Jean-Pierre Raffarin, qui promeut activement les intérêts chinois en France, de l'ancien commissaire tchèque Štefan Füle, qui a travaillé pour CEFC China Energy, de l'ancien Premier ministre finlandais Esko Aho, qui siège désormais au conseil d'administration de la Sberbank, de l'ancien ministre français chargé des relations avec le Parlement Jean-Marie Le Guen, qui est membre du conseil d'administration de Huawei France, d'Yves Leterme, ancien Premier ministre belge et actuel coprésident du fonds d'investissement chinois ToJoy, ainsi que de nombreux autres dirigeants politiques ou hauts fonctionnaires qui exercent des fonctions similaires;
- BY. considérant que la stratégie de lobbying économique peut être combinée avec des objectifs d'ingérence étrangère; considérant que, selon le rapport de l'OCDE sur le lobbying au XXI^e siècle¹², seuls les États-Unis, l'Australie et le Canada ont mis en place

¹² Organisation de coopération et de développement économiques, «Le lobbying au XXI^e siècle: transparence, intégrité et accessibilité», 2021, éditions OCDE, Paris, disponible à l'adresse suivante:

des règles encadrant l'influence étrangère; considérant qu'il existe un manque criant de règles juridiquement contraignantes et d'application du registre du lobbying de l'Union, ce qui rend quasiment impossible le suivi du lobbying provenant de l'extérieur de l'Union; considérant qu'il n'existe actuellement aucun moyen de contrôler les efforts de lobbying dans les États membres, qui influencent la législation et la politique étrangère au sein du Conseil européen; considérant que les règles relatives au lobbying dans l'Union se concentrent principalement sur les rencontres physiques et ne tiennent pas compte des différents types de lobbying existant à Bruxelles; considérant que des pays comme la Chine, la Russie, le Qatar, les Émirats arabes unis et la Turquie ont également investi massivement dans des efforts de lobbying à Bruxelles;

- BZ. considérant que les tentatives d'instrumentalisation de groupes vulnérables, dont les minorités et diasporas nationales vivant sur le sol de l'Union, représentent un élément important des stratégies d'ingérence étrangère;
- CA. considérant que différents acteurs étatiques, tels que les gouvernements russe, chinois et, dans une moindre mesure, turc, ont tenté d'accroître leur influence en mettant en place et en utilisant des instituts culturels, éducatifs (par exemple, par l'intermédiaire de subventions et de bourses d'études) et religieux au sein des États membres, dans le but stratégique de déstabiliser la démocratie européenne et d'étendre leur contrôle sur l'Europe centrale et orientale; considérant que la situation prétendument difficile de sa minorité nationale a été utilisée par le passé par la Russie comme excuse pour intervenir directement dans des pays tiers;
- CB. considérant qu'il existe des preuves d'ingérence et de manipulation de l'information en ligne de la part de la Russie dans de nombreuses démocraties libérales dans le monde, par exemple lors du référendum sur le Brexit au Royaume-Uni et des élections présidentielles en France et aux États-Unis, ainsi que de son soutien concret apporté à des partis extrémistes, populistes et anti-européens ainsi qu'à d'autres partis et individus dans toute l'Europe, notamment, mais pas uniquement, en France, en Allemagne, en Italie et en Autriche; considérant qu'il faut consolider le soutien à la recherche et à l'éducation pour comprendre l'étendue exacte de l'influence de l'ingérence étrangère sur des événements spécifiques, tels que le Brexit et l'élection du président Trump en 2016;
- CC. considérant que les réseaux Sputnik et RT, contrôlés par l'État russe, basés en Occident, associés à des médias occidentaux et entièrement ou partiellement détenus par des personnes physiques et morales russes et chinoises, se livrent à des activités de désinformation contre les démocraties libérales; considérant que la Russie fait preuve de révisionnisme historique et cherche à réécrire l'histoire des crimes soviétiques et à promouvoir la nostalgie de l'URSS auprès de la population d'Europe centrale et orientale réceptive à cette propagande; considérant que pour les médias audiovisuels nationaux d'Europe centrale et orientale, il est difficile de concurrencer le contenu télévisuel en langue russe, financé par le gouvernement russe; considérant que la coopération entre les médias chinois et les médias étrangers risque d'être déséquilibrée,

<https://doi.org/10.1787/c6d8eff8-en>

étant donné que les premiers portent la voix du parti communiste chinois à l'intérieur du pays comme à l'étranger;

- CD. considérant que plus de 500 Centres Confucius ont été ouverts dans le monde, dont environ 200 en Europe, et que les instituts Confucius et les salles de classe Confucius sont utilisés par la Chine comme outil d'ingérence dans l'Union; considérant que la liberté académique est gravement restreinte à l'institut Confucius; considérant que des universités et des programmes éducatifs sont la cible de financements étrangers massifs, notamment en provenance de Chine ou du Qatar, comme le campus de Budapest de l'université Fudan;
- CE. considérant que l'Union ne dispose actuellement pas de la boîte à outils nécessaire pour lutter contre le recrutement de personnalités haut placées et l'établissement de canaux d'influence, y compris au sein des institutions de l'Union; considérant que les capacités de connaissance de la situation et les instruments de contre-espionnage restent rares au niveau de l'Union, avec une forte dépendance à l'égard de la volonté des acteurs nationaux de partager des informations;

Dissuasion, imputation de responsabilité et contre-mesures collectives, dont les sanctions

- CF. considérant que l'Union et ses États membres ne disposent pas actuellement d'un régime de sanctions spécifique en ce qui concerne l'ingérence étrangère et les campagnes de désinformation orchestrées par des acteurs étatiques étrangers, ce qui signifie que ces derniers n'ont pas à craindre de conséquences pour leurs campagnes de déstabilisation contre l'Union;
- CG. considérant que la garantie d'une imputation claire de la responsabilité des attaques de désinformation et de propagande, y compris la désignation publique de leurs auteurs, de leurs commanditaires et des objectifs qu'ils cherchent à atteindre, ainsi que la mesure des effets de ces attaques sur le public ciblé constituent les premières étapes d'une défense efficace contre ces actions;
- CH. considérant que l'Union devrait renforcer ses outils de dissuasion, ainsi que ses outils permettant d'imputer ces attaques à leurs responsables et de déterminer si celles-ci contreviennent ou non au droit international, dans l'objectif de bâtir un régime de sanctions efficace afin que les acteurs étrangers malveillants doivent payer le prix de leurs décisions et en assumer les conséquences; considérant que le ciblage d'individus pourrait ne pas être suffisant; considérant que d'autres outils, comme des mesures commerciales, pourraient être mobilisés pour protéger les processus démocratiques européens contre les attaques hybrides commanditées par des États; considérant que les mesures de dissuasion doivent être appliquées de manière transparente en apportant toutes les garanties requises; considérant que les attaques hybrides sont soigneusement calibrées de sorte à ne pas remplir les conditions visées à l'article 42, paragraphe 7, du traité sur l'Union européenne et à l'article 5 du traité de l'Atlantique Nord;

Coopération mondiale et multilatéralisme

- CI. considérant que les actions malveillantes orchestrées par des acteurs étrangers, étatiques ou non, affectent de nombreux partenaires démocratiques dans le monde; considérant

que les alliés démocratiques sont tributaires de leur capacité à unir leurs forces pour apporter une réponse collective;

- CJ. considérant que les pays des Balkans occidentaux candidats à l'adhésion à l'Union sont frappés par des attaques d'une intensité particulière, qui prennent la forme d'ingérence étrangère et de campagnes de désinformation venant de Russie, de Chine et de Turquie, telles que les campagnes d'ingérence de la Russie au cours du processus de ratification de l'accord de Prespa en Macédoine du Nord; considérant que la Chine et la Russie ont exploité la pandémie de COVID-19 dans les Balkans occidentaux pour déstabiliser ces pays et discréditer l'Union; considérant qu'il est prévu que les pays candidats et candidats potentiels se joignent aux initiatives de l'Union visant à lutter contre l'ingérence étrangère;
- CK. considérant le manque de compréhension commune et de définitions communes persistant parmi les partenaires et alliés partageant les mêmes idées en ce qui concerne la nature des menaces en cause; considérant que le secrétaire général des Nations unies demande l'élaboration d'un code de conduite mondial pour promouvoir l'intégrité de l'information publique; considérant que la conférence sur l'avenir de l'Europe est une plateforme importante pour les discussions relatives à cette thématique;
- CL. considérant qu'il est nécessaire d'instaurer une coopération et un soutien multilatéraux mondiaux entre les partenaires partageant les mêmes idées pour faire face à l'ingérence malveillante étrangère, considérant que d'autres démocraties, comme l'Australie et Taïwan, ont développé des compétences et des stratégies avancées; considérant que Taïwan est en première ligne dans la lutte contre la manipulation de l'information, principalement en provenance de Chine; considérant que le succès du système taïwanais repose sur la coopération entre toutes les branches du gouvernement, mais aussi avec des ONG indépendantes spécialisées dans la vérification des faits et l'éducation aux médias, ainsi qu'avec les plateformes de médias sociaux, telles que Facebook, pour la promotion de l'éducation aux médias pour toutes les générations, la lutte contre la désinformation et l'endiguement de la diffusion de messages manipulateurs; considérant que la commission spéciale INGE a effectué une mission officielle de trois jours à Taïwan pour discuter de la désinformation et de l'ingérence électorale étrangère;

Nécessité d'une stratégie coordonnée de l'Union contre l'ingérence étrangère

1. est profondément préoccupé par l'incidence croissante et la nature de plus en plus sophistiquée des tentatives d'ingérence et de manipulation de l'information étrangères, essentiellement menées par la Russie et la Chine et visant tous les aspects du fonctionnement démocratique de l'Union européenne et de ses États membres;
2. invite la Commission à proposer, et aux colégislateurs et aux États membres à soutenir, une stratégie coordonnée à plusieurs niveaux et intersectorielle ainsi que des ressources financières adéquates visant à doter l'Union et ses États membres de politiques de résilience et de prospection et d'outils de dissuasion appropriés, grâce auxquels ils pourront lutter contre toutes les menaces et attaques hybrides orchestrées par des acteurs étrangers, étatiques ou non; considère que cette stratégie devrait reposer sur:
 - a) des terminologies et des définitions communes, une méthode commune, des évaluations et des analyses d'impact ex post de la législation adoptée jusqu'à

présent, un système de renseignement partagé, ainsi que la compréhension, le suivi, y compris par des alertes précoces, et la connaissance de la situation en ce qui concerne ces enjeux;

- b) des politiques concrètes permettant de renforcer la résilience des citoyens européens, conformément aux valeurs démocratiques, y compris par un soutien à la société civile;
 - c) des capacités de perturbation et de défense adaptées;
 - d) des réponses diplomatiques et dissuasives, y compris une boîte à outils de l'Union européenne pour lutter contre les opérations d'ingérence et d'influence étrangères, y compris les opérations hybrides, par des mesures appropriées, telles que l'imputation de responsabilité, la désignation des auteurs, des sanctions et des contre-mesures, ainsi que des partenariats mondiaux en vue de l'échange de pratiques et de la promotion de normes internationales en matière de comportement responsable des États;
3. souligne que toutes les mesures visant à prévenir et à détecter l'ingérence étrangère, à l'imputer à ses responsables, à lutter contre elle et à la sanctionner doivent être élaborées de manière à défendre et à promouvoir les droits fondamentaux, notamment la capacité des citoyens de l'Union à communiquer de manière sûre, anonyme et non censurée, sans ingérence induite de la part d'acteurs étrangers;
4. estime que cette stratégie devrait reposer sur une approche fondée sur les risques, sur l'ensemble de la société et sur l'ensemble du gouvernement, couvrant notamment les domaines suivants:
- a) renforcement de la résilience par la connaissance de la situation, l'éducation aux médias et à l'information, le pluralisme des médias, le journalisme indépendant et l'éducation;
 - b) ingérence étrangère qui tire parti des plateformes en ligne;
 - c) infrastructures critiques et secteurs stratégiques;
 - d) ingérence étrangère durant les processus électoraux;
 - e) financement dissimulé des activités politiques provenant d'acteurs et de donateurs étrangers;
 - f) cybersécurité et résilience face aux cyberattaques;
 - g) protection des États membres, des institutions, des agences, des délégations et des missions de l'Union européenne;
 - h) ingérence d'acteurs étrangers par le recrutement de personnalités haut placées, les diasporas nationales, les universités et les manifestations culturelles;
 - i) dissuasion, imputation de responsabilité et contre-mesures collectives, dont les sanctions;

- j) coopération mondiale et multilatéralisme;
5. demande en particulier à l'Union et à ses États membres d'augmenter les ressources et les moyens alloués aux organismes et aux associations en Europe et dans le monde, tels que les groupes de réflexion et les vérificateurs de faits, chargés de surveiller les menaces, y compris la désinformation, et de sensibiliser à leur gravité; souligne le rôle crucial de l'Union dans un sens stratégique large; demande à l'Union et à ses États membres de renforcer leur capacité de prospective et l'interopérabilité de leurs actions, afin d'être sûr qu'ils seront prêts à prévoir, à empêcher et à atténuer l'ingérence et la manipulation de l'information étrangères, à renforcer la protection de leurs intérêts et infrastructures stratégiques, et à s'engager dans une coopération et une coordination multilatérales afin de parvenir à une compréhension commune de la question dans les enceintes internationales pertinentes; invite le Conseil «Affaires étrangères» à débattre régulièrement des questions relatives à l'ingérence étrangère;
 6. est préoccupé du manque criant de sensibilisation, y compris parmi le grand public et les représentants des pouvoirs publics, à la gravité des menaces actuelles que présentent les régimes autoritaires étrangers et d'autres acteurs malveillants et qui visent tous les niveaux et secteurs de la société européenne dans le but de nuire aux droits fondamentaux et à la légitimité des autorités publiques, d'exacerber la fragmentation politique et sociale et, dans certains cas, même de mettre en danger la vie des citoyens de l'Union;
 7. s'inquiète du manque de normes et de mesures appropriées et suffisantes pour désigner les responsables d'actes d'ingérence étrangère et pour réagir à ces actes, ce qui se traduit par un calcul intéressant pour les acteurs malveillants, à savoir de faibles coûts, de faibles risques et un bénéfice élevé, le risque de représailles auquel ils sont exposés étant actuellement très faible;
 8. demande instamment à la Commission d'inclure, le cas échéant, la dimension de la manipulation de l'information et de l'ingérence étrangères dans l'analyse d'impact ex ante réalisée avant de présenter de nouvelles propositions, en vue d'intégrer la lutte contre ces phénomènes dans le processus d'élaboration des politiques de l'Union; demande instamment au SEAE et à la Commission de procéder à des examens réguliers de la résilience et à évaluer l'évolution des menaces et leur incidence sur la législation et les politiques actuelles;
 9. invite la Commission à analyser les institutions nationales récemment instaurées, telles que le coordinateur national australien de lutte contre l'ingérence étrangère, le comité de sécurité finlandais qui assiste le gouvernement et les ministères, l'agence de sécurité civile et la nouvelle agence de défense psychologique de la Suède ainsi que le Centre national de la Chine en Suède, la nouvelle agence nationale française Viginum, le Centre national de cybersécurité de la Lituanie et le groupe de travail interagences de coordination de la désinformation de Taïwan, afin de déterminer ce que nous pouvons apprendre de ces bonnes pratiques et dans quelle mesure une idée similaire pourrait être appliquée au niveau de l'Union; invite la Commission à favoriser le partage d'informations et de bonnes pratiques entre les États membres à cet égard; souligne l'importance d'une approche et d'instruments proactifs, y compris des communications stratégiques, éléments essentiels pour traduire les politiques de l'Union et des États

membres en paroles et en actes; demande à la Commission de proposer une formation adéquate en matière de science des données et de créer un organe de contrôle unique au sein de la Commission consacré à la manipulation de l'information;

10. est préoccupé par les nombreuses lacunes et failles dans la législation et les politiques actuelles au niveau de l'Union et au niveau national qui visent à détecter et prévenir l'ingérence étrangère et à lutter contre celle-ci;
11. signale qu'un certain nombre de projets et de programmes à long terme axés sur la lutte contre la désinformation sur les plans technologique, juridique, psychologique et informationnel sont actuellement financés par l'Union; demande à la Commission d'évaluer l'incidence de ces projets et programmes, ainsi que leur applicabilité;
12. demande à la Commission de mettre en place une task force en son sein, sous la houlette de Věra Jourová, vice-présidente de la Commission chargée des valeurs et de la transparence, qui se consacrerait à l'examen de la législation et des politiques existantes afin de repérer les lacunes susceptibles d'être exploitées par des acteurs malveillants et demande instamment à la Commission de combler ces lacunes; insiste sur le fait que cette structure devrait coopérer avec les autres institutions de l'Union et les États membres aux niveaux national, régional et local et faciliter l'échange de bonnes pratiques; demande à la Commission et au SEAE d'envisager de créer un centre européen de lutte contre les menaces d'ingérence et de l'intégrité de l'information indépendant et doté de ressources suffisantes, qui aurait pour mission de repérer, d'analyser et de documenter les opérations de manipulation de l'information et les menaces d'ingérence dirigées contre l'Union dans son ensemble, d'améliorer la connaissance de la situation, de mettre au point un pôle de savoir spécialisé en devenant une plateforme de coordination avec la société civile, le secteur des affaires et les institutions de l'Union et des États membres et de sensibiliser le public au moyen, entre autres, de rapports réguliers sur les menaces systémiques; souligne que le projet de création d'un tel nouveau centre européen de lutte contre les menaces d'ingérence et de l'intégrité de l'information indépendant et doté de ressources suffisantes devrait clarifier et renforcer le rôle de la division StratCom du SEAE et de ses task forces en tant qu'organe stratégique du service diplomatique de l'Union et éviter le chevauchement des activités; souligne que le mandat de la division StratCom du SEAE devrait être axé sur l'élaboration stratégique de politiques externes visant à lutter contre les menaces communes existantes et émergentes ainsi qu'à renforcer la coopération avec les partenaires internationaux dans ce domaine; signale que la division StratCom du SEAE pourrait poursuivre ces objectifs en étroite collaboration avec le nouveau centre européen de lutte contre les menaces d'ingérence et de l'intégrité de l'information et la nouvelle task force de la Commission;
13. invite les institutions et les États membres de l'Union à donner à la société civile les moyens de jouer un rôle actif dans la lutte contre l'ingérence étrangère; invite tous les niveaux et secteurs de la société européenne à mettre en place des systèmes pour rendre les organisations et les citoyens plus résilients face à l'ingérence étrangère, pour être en mesure de détecter les attaques à temps et de les contrer aussi efficacement que possible, y compris grâce à l'éducation et à la sensibilisation, dans le respect du cadre de l'Union relatif aux droits fondamentaux et de manière transparente et démocratique; souligne, dans ce contexte, les bonnes pratiques et l'approche englobant l'ensemble de

la société adoptées par Taïwan; demande aux décideurs de fournir à la société civile les outils appropriés et des fonds spécifiques pour étudier, dénoncer et combattre l'influence étrangère;

Renforcement de la résilience de l'Union par la connaissance de la situation, l'éducation aux médias et l'éducation en général

14. insiste sur le fait que les institutions et les États membres de l'Union ont besoin de systèmes solides, robustes et interconnectés pour détecter, analyser, suivre et cartographier les incidents dans lesquels sont associés des acteurs étrangers étatiques et non étatiques qui tentent de s'ingérer dans les processus démocratiques, afin d'acquérir une connaissance de la situation et une compréhension claire du type de comportement que l'Union et ses États membres doivent décourager et combattre; demande que des recherches et des sondages sociologiques soient régulièrement menés pour suivre l'évolution de la résilience et de l'éducation aux médias ainsi que pour comprendre le soutien de l'opinion publique aux discours de désinformation les plus communs et leur perception par celle-ci;
15. souligne qu'il est tout aussi important que les informations tirées de cette analyse ne restent pas bloquées au niveau des groupes de spécialistes de l'ingérence étrangère, mais soient ouvertement partagées, dans la mesure du possible, avec un public plus large, en particulier avec les personnes exerçant des fonctions sensibles, afin que chacun ait connaissance des profils des menaces et puisse éviter les risques;
16. souligne qu'il est nécessaire d'élaborer une méthode commune pour développer la connaissance de la situation, le système d'alerte rapide et le processus d'évaluation des menaces, collecter des preuves de manière systématique et détecter la manipulation de l'environnement informationnel en temps utile, ainsi que mettre au point des normes pour l'attribution technique, par exemple en ce qui concerne l'authenticité des contenus, afin de garantir une réponse efficace;
17. insiste sur la nécessité pour l'Union, en coopération avec les États membres et en travaillant de manière multilatérale au sein des forums internationaux pertinents, d'élaborer une définition conceptuelle des menaces d'ingérence auxquelles est confrontée l'Union; souligne que cette définition doit prendre en considération les tactiques, les techniques, les procédures et les outils employés pour décrire les comportements des acteurs de la menace étatiques et non étatiques que nous observons aujourd'hui; demande instamment à la Commission d'associer l'Agence des droits fondamentaux de l'Union européenne afin de garantir qu'aucun concept ou préjugé discriminatoire ou injuste n'a été intégré dans les définitions conceptuelles;
18. souligne que la diplomatie publique et la communication stratégique sont des éléments essentiels des relations extérieures de l'Union et de la protection des valeurs démocratiques de l'Union; demande que les institutions de l'Union poursuivent et intensifient l'important travail de la division StratCom du SEAE, y compris de ses task forces, du centre de situation et du renseignement de l'Union (INTCEN) et de la cellule de fusion contre les menaces hybrides, de la direction «Renseignement» de l'État-major de l'Union, du système d'alerte rapide, de la coopération établie au niveau administratif entre le SEAE, la Commission et le Parlement, du réseau de lutte contre la

désinformation dirigé par la Commission, de la task force administrative du Parlement contre la désinformation, et de la coopération en cours avec l'OTAN, le G7, la société civile et le secteur privé en ce qui concerne la coopération en matière de renseignement, d'analyse, de partage des bonnes pratiques et de sensibilisation à la manipulation de l'information et l'ingérence étrangères; se félicite du rapport spécial n° 09/2021 de la Cour des comptes intitulé «La désinformation concernant l'UE: un phénomène sous surveillance mais pas sous contrôle»; demande au SEAE et à la Commission de fixer un calendrier détaillé pour la mise en application des recommandations de la Cour des comptes;

19. souligne la nécessité de soutenir et de renforcer les efforts de suivi permanents bien avant les élections, les référendums ou les autres processus politiques importants dans l'ensemble de l'Europe;
20. invite les États membres à utiliser pleinement ces ressources en partageant les renseignements pertinents avec l'INTCEN et en renforçant leur participation au système d'alerte rapide; est d'avis que la coopération en matière d'analyse et de renseignement au sein de l'Union et avec l'OTAN doit être davantage renforcée et dans le même temps rendue plus transparente et plus responsable sur le plan démocratique, y compris en partageant des informations avec le Parlement;
21. se félicite de l'idée de la présidente de la Commission, M^{me} von der Leyen, d'établir un centre commun de connaissance de la situation afin d'améliorer la prospective stratégique et l'autonomie stratégique ouverte de l'Union, et attend davantage de précisions sur sa création et sa mission; souligne qu'un tel centre nécessiterait une coopération active avec les services compétents de la Commission, le SEAE, le Conseil, le Parlement et les autorités nationales; rappelle cependant l'importance d'éviter les doubles emplois et les chevauchements avec les structures de l'Union existantes;
22. rappelle la nécessité de doter le SEAE d'un mandat renforcé et clairement défini et des ressources nécessaires pour que la division «Communication stratégiques et analyse de l'information» et ses task forces puissent surveiller et lutter contre la manipulation de l'information et l'ingérence au-delà des sources étrangères actuellement couvertes par les trois task forces et pour lui permettre de viser une plus large couverture géographique en appliquant une approche fondée sur les risques; demande de toute urgence que le SEAE déploie des capacités adéquates afin de lutter contre la manipulation de l'information et l'ingérence émanant de la Chine, notamment en constituant une équipe spécifique sur l'Extrême-Orient; insiste en outre sur la nécessité d'accroître considérablement l'expertise et les capacités linguistiques en ce qui concerne la Chine et d'autres régions d'importance stratégique, au sein du SEAE, dans les États membres et dans les institutions de l'Union en général, et d'avoir recours aux sources de renseignement de source ouverte qui sont actuellement sous-utilisées;
23. insiste sur l'importance de médias largement diffusés, concurrentiels et pluralistes, de journalistes, de vérificateurs de faits et de chercheurs indépendants et de médias de service public forts pour un débat démocratique animé et libre; se félicite des initiatives visant à rassembler, à former et à soutenir de toute autre manière les organisations de journalistes, de vérificateurs de faits et de chercheurs indépendants dans toute l'Europe, et en particulier dans les régions les plus exposées, telles que l'Observatoire européen

des médias numériques et le Fonds européen pour la démocratie; regrette vivement que l'Observation européen des médias numériques ne couvre pas les États baltes; salue également les initiatives visant à mettre au point des indicateurs de fiabilité du journalisme et de la vérification des faits qui sont faciles à reconnaître telles que celle lancée par Reporters sans frontières; demande à la Commission de lutter contre la propriété monopolistique des médias de masse;

24. salue les recherches indispensables et les nombreuses initiatives créatives et efficaces d'éducation et de sensibilisation aux médias et au numérique menées par des particuliers, des écoles, des universités, des organisations de médias, des institutions publiques et des organisations de la société civile;
25. demande à l'Union et aux États membres d'affecter des sources de financement public de l'Union aux vérificateurs de faits indépendants, aux chercheurs, aux médias d'investigation de qualité et aux journalistes d'investigation compétents, ainsi qu'aux ONG qui mènent des recherches et enquêtent sur la manipulation de l'information et l'ingérence, qui promeuvent l'éducation aux médias, au numérique et à l'information et d'autres moyens de responsabiliser les citoyens et qui étudient comment mesurer de manière significative l'efficacité des formations en matière d'éducation aux médias, au numérique et à l'information, de la sensibilisation, de la démystification et de la communication stratégique;
26. demande le renforcement des médias professionnels et pluralistes, en garantissant la juste rémunération des éditeurs pour l'utilisation de leurs contenus en ligne; souligne que plusieurs pays dans le monde prennent des mesures pour que les médias disposent de ressources financières adéquates; rappelle sa demande de création d'un fonds de l'Union permanent pour les médias d'information et se félicite, à cet égard, de l'initiative «News», notamment les nouvelles possibilités de financement du secteur des médias et de l'éducation aux médias et à l'information dans le programme «Europe créative» (2021-2027); souligne néanmoins que les flux de financement peuvent créer des dépendances ou avoir une incidence sur l'indépendance des médias; souligne à cet égard l'importance de la transparence du financement des médias; estime que, pour protéger le pluralisme des médias, il est nécessaire de faire savoir au public qui possède ou contrôle les médias, qui leur fait des dons ou leur fournit du contenu et qui paye pour le contenu journalistique;
27. souligne la nécessité de consolider les analyses, les rapports d'incidents et les évaluations de la menace publique fondées sur les renseignements concernant la manipulation de l'information et l'ingérence et de mettre ces informations à la disposition du public; propose dès lors de créer une base de données à l'échelle de l'Union des incidents d'ingérence étrangère signalés par les autorités de l'Union et des États membres; souligne que les informations relatives à ces incidents pourraient être partagées, le cas échéant, avec les organisations de la société civile et le public, dans toutes les langues de l'Union;
28. demande à tous les États membres d'inclure l'éducation aux médias et au numérique, ainsi qu'à la démocratie, aux droits fondamentaux, à l'histoire récente, aux affaires mondiales, à l'esprit critique et à la participation du public dans leurs programmes d'enseignement et de formation, de la petite enfance à l'âge adulte, y compris la

formation des enseignants et des chercheurs; demande à la Commission et aux États membres de renforcer leur soutien à l'enseignement de l'histoire et à la recherche sur la façon dont l'ingérence étrangère et le totalitarisme du passé ont influencé la société en général, et plus particulièrement les événements démocratiques de grande ampleur;

29. demande que les institutions de l'Union et les États membres, à tous les niveaux administratifs, repèrent les secteurs exposés à des tentatives d'ingérence et proposent régulièrement au personnel travaillant dans ces secteurs des formations et des exercices sur la manière de détecter et d'éviter les tentatives d'ingérence, et souligne que ces efforts bénéficieraient d'un format standardisé établi par l'Union; recommande que des modules de formation exhaustifs soient également proposés à tous les fonctionnaires; se félicite à cet égard de la formation offerte aux députés et au personnel par l'administration du Parlement; recommande que cette formation soit développée davantage;
30. souligne la nécessité de sensibiliser toutes les couches de la société à l'ingérence étrangère; se félicite des initiatives prises par le SEAE, la Commission et l'administration du Parlement, telles que les événements de formation et de sensibilisation destinés aux journalistes, aux enseignants, aux personnes influentes, aux étudiants, aux personnes âgées et aux visiteurs, tant hors ligne qu'en ligne, à Bruxelles et dans tous les États membres de l'Union, et recommande de les développer davantage;
31. invite les États membres, l'administration de l'Union et les organisations de la société civile à partager les bonnes pratiques en matière de formation et de sensibilisation à l'éducation aux médias et à l'information, comme le prévoit la directive «Services de médias audiovisuels»¹³; demande à la Commission d'organiser ces échanges en coopération avec le groupe d'experts sur l'éducation aux médias; souligne que la directive révisée doit être mise en application rapidement et correctement par les États membres;
32. demande instamment aux institutions de l'Union de rédiger un code d'éthique pour aider les autorités publiques et les représentants politiques à utiliser les plateformes de médias sociaux et les réseaux sociaux; estime qu'il est nécessaire d'encourager une utilisation responsable de telles plateformes et de tels réseaux afin de lutter contre la manipulation et la désinformation provenant de la sphère publique;
33. demande que l'Union et ses États membres mettent en œuvre des programmes personnalisés de sensibilisation et d'éducation aux médias et à l'information, y compris pour les diasporas et les minorités, et invite la Commission à mettre en place un système permettant de partager facilement des supports dans les langues minoritaires, afin de réduire les coûts de traduction et de toucher autant de personnes que possible; demande aux régions et aux municipalités de jouer un rôle de premier plan à cet égard, étant donné qu'il importe d'atteindre les zones rurales et l'ensemble des groupes démographiques;

¹³ 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 (JO L 95 du 15.4.2010, p. 1).

34. souligne qu'une réponse essentielle aux tentatives d'ingérence étrangère consiste à protéger les principaux groupes cibles qu'elles visent; souligne qu'il est nécessaire d'adopter des mesures ciblées, par l'intermédiaire d'un cadre juridique de l'Union harmonisé, contre la diffusion de la désinformation et de discours de haine sur les questions liées au genre, les personnes LGBTIQ+, les minorités et les réfugiés; demande à la Commission d'élaborer et de mettre en œuvre des stratégies pour empêcher le financement d'individus et de groupes qui diffusent activement des informations manipulées ou participent à la manipulation d'informations, qui concernent souvent les groupes et sujets susmentionnés, dans le but de diviser la société; demande des campagnes de communication positives sur ces questions et souligne la nécessité de formations qui tiennent compte de la dimension de genre;
35. est conscient que les attaques et les campagnes de désinformation liée au genre sont souvent utilisées dans le cadre d'une stratégie politique plus large visant à saper la participation égale aux processus démocratiques, en particulier des femmes et des personnes LGBTIQ+; souligne que la désinformation concernant les personnes LGBTIQ+ alimente la haine, tant en ligne que hors ligne, et met des vies en danger; demande que les recherches sur la désinformation en ligne soient menées dans une optique intersectionnelle et que les changements apportés par les plateformes pour répondre aux campagnes de désinformation liée au genre en ligne soient surveillés; demande qu'une attention accrue soit accordée à la désinformation fondée sur le genre par la création de systèmes d'alerte précoce permettant de signaler et de mettre en évidence les campagnes de désinformation liée au genre;
36. demande à la Commission de présenter une stratégie générale d'éducation aux médias et à l'information, en mettant l'accent sur la lutte contre la manipulation de l'information;
37. se félicite de la création du groupe d'experts sur la lutte contre la désinformation et le renforcement de l'éducation au numérique par l'éducation et la formation, qui se focalisera, entre autres tâches, sur l'esprit critique, la formation des enseignants, les efforts de prévention de la mystification, de démystification et de vérification des faits, ainsi que sur la participation des étudiants; demande à la Commission de partager les résultats des travaux de ce groupe d'experts et de mettre ses conclusions en application;
38. souligne l'importance d'une communication stratégique pour contrer les discours anti-démocratie les plus courants; préconise l'amélioration de la communication stratégique de l'Union dans le but d'étendre sa portée tant à l'égard des citoyens qu'à l'étranger; insiste sur le fait que toutes les organisations démocratiques doivent défendre la démocratie et l'état de droit et ont la responsabilité commune de dialoguer avec les citoyens, en utilisant les langues dans lesquelles et les plateformes au travers desquelles ces derniers souhaitent communiquer;
39. demande aux États membres de garantir l'organisation de campagnes de communication publiques efficaces au sujet de la pandémie de COVID-19 dans le but de diffuser des informations correctes en temps utile pour combattre la mésinformation, en particulier en ce qui concerne les vaccins;
40. est vivement préoccupé de la propagation de la propagande d'État étrangère, principalement en provenance de Moscou et de Pékin, ainsi que d'Ankara, qui est

traduite dans les langues locales, par exemple dans des contenus médiatiques sponsorisés par RT, Sputnik, Anadolu, CCTV, *Global Times*, Xinhua, TRT World ou le Parti communiste chinois présentés de manière journalistique et distribués avec les journaux; soutient que ces canaux ne sauraient être considérés comme de véritables médias et qu'ils ne devraient donc ni jouir des mêmes droits que les médias démocratiques ni bénéficier de la même protection que celle accordée à ces derniers; s'inquiète également de la manière dont ces discours ont filtrés dans de véritables produits journalistiques; souligne la nécessité d'une prise de conscience face aux campagnes de désinformation de la Russie et de la Chine, qui visent à s'attaquer aux valeurs démocratiques et à diviser l'Union, puisqu'elles constituent la principale source de désinformation en Europe; demande à la Commission d'entreprendre une étude des normes minimales devant s'appliquer aux médias comme base sur laquelle s'appuyer pour éventuellement révoquer des licences en cas de violation; invite la Commission à intégrer les conclusions de cette étude dans les législations à venir, par exemple dans une éventuelle législation sur la liberté des médias; signale qu'il se peut que des acteurs de l'ingérence étrangère se fassent passer pour des journalistes; estime que, dans de telles situations, il devrait être possible de sanctionner ces personnes ou ces organisations, par exemple en les dénonçant, en les mettant sur la liste noire des événements destinés aux médias ou en révoquant leur accréditation de presse;

41. est profondément préoccupé par les attaques, le harcèlement, la violence et les menaces dont sont la cible les journalistes, les défenseurs des droits de l'homme et d'autres personnes qui dénoncent des ingérences étrangères et craint que ces actes portent également atteinte à leur indépendance; demande à la Commission de présenter rapidement des propositions concrètes et ambitieuses sur la sécurité de toutes ces personnes, y compris un instrument contre les poursuites stratégiques altérant le débat public (poursuites-bâillons) et un soutien économique, juridique et diplomatique, comme annoncé dans le cadre du plan d'action pour la démocratie européenne; se félicite, à cet égard, de la 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 européenne¹⁴; demande aux États membres de protéger efficacement les journalistes et les autres professionnels des médias au moyen d'outils législatifs et non législatifs;
42. insiste sur la nécessité d'impliquer les décideurs locaux et régionaux responsables des décisions stratégiques dans les domaines qui relèvent de leur compétence, tels que les infrastructures, la cybersécurité, la culture et l'éducation; souligne que les autorités et les responsables politiques locaux et régionaux peuvent souvent repérer les développements préoccupants à un stade précoce et insiste sur le fait que les connaissances locales sont souvent nécessaires pour définir et mettre en œuvre des contre-mesures adéquates;
43. demande à la Commission et aux États membres de mettre en place des canaux de communication et des plateformes via lesquels les entreprises, les ONG et les particuliers, y compris les membres de diasporas, peuvent signaler des situations dans lesquelles ils sont victimes de manipulation de l'information ou d'ingérence; invite les

¹⁴ JO L 331 du 20.9.2021, p. 8.

États membres à soutenir les personnes qui sont victimes d'attaques et celles qui en ont connaissance ou qui subissent des pressions;

Ingérence étrangère qui tire parti des plateformes en ligne

44. se félicite des propositions de révision du code de bonnes pratiques contre la désinformation, de législation sur les services numériques, de législation sur les marchés numériques et des autres mesures liées au plan d'action pour la démocratie européenne, qui sont autant d'outils potentiellement efficaces pour lutter contre l'ingérence étrangère; recommande que la lecture finale de ces textes tienne compte des aspects exposés dans la suite de la présente section;
45. insiste sur le fait que la liberté d'expression ne doit pas être interprétée à tort comme une liberté de se livrer à des activités en ligne qui sont illégales hors ligne, telles que le harcèlement, les discours de haine, la discrimination raciale, le terrorisme, la violence, l'espionnage et les menaces; souligne que les plateformes doivent respecter non seulement la loi du pays dans lequel elles exercent leurs activités mais également leurs conditions générales, en particulier en ce qui concerne les contenus préjudiciables en ligne; demande aux plateformes de redoubler d'efforts pour empêcher la réapparition de contenus illicites identiques à des contenus qui ont déjà été reconnus comme tels et qui ont été retirés;
46. souligne la nécessité, avant tout, de continuer d'étudier l'augmentation de la désinformation et de l'ingérence étrangère en ligne et de disposer d'une législation à l'échelle de l'Union pour garantir une transparence, un suivi et une responsabilité bien plus grands et véritables en ce qui concerne les opérations menées par les plateformes en ligne et l'accès aux données pour les demandeurs d'accès légitimes, en particulier dans le contexte d'algorithmes et de publicités en ligne; demande aux entreprises de médias sociaux de tenir des bibliothèques de publicités,
47. préconise une réglementation et des mesures pour obliger les plateformes, en particulier celles qui présentent un risque systémique pour la société, à faire ce qui leur incombe pour réduire la manipulation de l'information et l'ingérence, par exemple en utilisant des labels qui indiquent les véritables auteurs cachés derrière les comptes, en limitant la portée de comptes qui sont régulièrement utilisés pour diffuser de la désinformation ou qui enfreignent régulièrement les conditions générales de la plateforme, en suspendant, et si nécessaire, sur la base d'une législation claire, en supprimant les comptes non authentiques utilisés pour des campagnes d'ingérence coordonnées, en démonétisant les sites de diffusion de désinformation, en mettant en place des mesures d'atténuation pour les risques d'ingérence posés par les effets de leurs algorithmes, de leurs modèles publicitaires, de leurs systèmes de recommandation et de leurs technologies d'intelligence artificielle, ainsi qu'en signalant les contenus de désinformation, tant dans les publications que dans les commentaires; rappelle qu'il convient de mettre en œuvre ces mesures de manière transparente et responsable;
48. demande à la Commission de tenir pleinement compte de la note d'orientation du Conseil de l'Europe sur les meilleures pratiques en vue de la mise en place de cadres juridiques et procéduraux efficaces pour les mécanismes d'autorégulation et de corégulation de la modération de contenu, adoptée en juin 2021;

49. demande la mise en œuvre intégrale et effective du règlement général sur la protection des données¹⁵, qui limite la quantité de données que les plateformes peuvent stocker sur les utilisateurs et la durée d'utilisation de ces données, en particulier pour les plateformes et les applications utilisant des données très privées et/ou sensibles, telles que les applications de messagerie, de santé, de finance et de rencontres et les petits groupes de discussion; préconise aux plateformes des contrôleurs d'accès de s'abstenir de combiner les données à caractère personnel avec les données à caractère personnel provenant de tout autre service proposé par le contrôleur d'accès, ou avec les données à caractère personnel provenant de services tiers, pour qu'il soit aussi facile de refuser que d'accepter le stockage et le partage de données et pour permettre aux utilisateurs de choisir d'être ciblés ou non par des publicités personnalisées en ligne; salue tous les efforts consentis pour interdire les techniques de microciblage des publicités à caractère politique, notamment, mais pas seulement, les techniques qui reposent sur des données à caractère personnel sensibles, telles que l'origine ethnique, les croyances religieuses ou l'orientation sexuelle, et demande à la Commission d'envisager d'étendre une interdiction de microciblage à la publicité engagée;
50. demande que des règles de l'Union contraignantes obligent les plateformes à coopérer avec les autorités compétentes pour tester régulièrement leurs systèmes et pour repérer, évaluer et atténuer le risque de manipulation de l'information et d'ingérence que comporte l'utilisation de leurs services ainsi que les vulnérabilités auxquelles s'exposent les utilisateurs de leurs services, y compris la manière dont la conception et la gestion de leurs services contribuent à ce risque; demande que des règles de l'Union contraignantes obligent les plateformes à mettre en place des systèmes permettant de surveiller la manière dont leurs services sont utilisés, telles qu'un suivi en temps réel des publications les plus en vue et les plus populaires pays par pays, afin de détecter la manipulation de l'information et l'ingérence et de signaler des soupçons d'ingérence aux autorités responsables, et augmentent les coûts pour les acteurs qui permettent de passer sous silence de telles actions facilitées par leurs systèmes;
51. demande aux plateformes en ligne de prévoir des ressources suffisantes pour prévenir l'ingérence étrangère préjudiciable et pour garantir de meilleures conditions de travail, un suivi psychologique et une rémunération équitable pour les modérateurs de contenu; demande aux grandes plateformes de médias sociaux de fournir des rapports détaillés, pays par pays, sur les ressources consacrées à la vérification des faits, aux activités de recherche, à la modération des contenus, y compris les capacités humaines et d'intelligence artificielle dans les différentes langues, et à la collaboration avec la société civile locale; souligne la nécessité pour ces plateformes d'intensifier leurs efforts pour lutter contre la désinformation sur les marchés plus petits et moins rentables commercialement dans l'Union;
52. invite les plateformes de médias sociaux à respecter pleinement l'égalité de tous les citoyens de l'Union, indépendamment de la langue utilisée, dans la conception de leurs services, outils et mécanismes de suivi, ainsi que dans les mesures visant à accroître la transparence et à améliorer la sécurité de l'environnement en ligne; souligne que cela

¹⁵ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, JO L 119 du 4.5.2016, p. 1.

s'applique non seulement à toutes les langues nationales et régionales officielles, mais aussi aux langues des diasporas importantes dans l'Union; souligne que ces services devraient également être accessibles aux personnes malentendantes;

53. demande un étiquetage clair et lisible des trucages vidéo ultra-réalistes («deep fakes»), tant pour les utilisateurs de la plateforme que dans les métadonnées du contenu, afin d'améliorer leur traçabilité pour les chercheurs et les vérificateurs de faits; salue à cet égard les initiatives visant à améliorer l'authenticité et la traçabilité des contenus, telles que le développement de filigranes et de normes d'authenticité, et la mise en place de normes mondiales;
54. préconise une réglementation des services offrant des outils et des services de manipulation des médias sociaux, utilisés par exemple pour gonfler la portée de comptes ou de contenus à l'aide d'une participation artificielle ou de profils non authentiques; souligne que cette réglementation doit être fondée sur une évaluation approfondie des pratiques actuelles et des risques associés et doit empêcher que des acteurs malveillants utilisent ces services à des fins d'ingérence politique;
55. insiste sur le besoin de transparence de la part des personnes qui veulent faire de la publicité en ce qui concerne la véritable personne physique ou morale qui se cache derrière les comptes et les contenus en ligne; demande aux plateformes d'introduire des mécanismes permettant de détecter et de suspendre notamment les comptes non authentiques liés à des opérations d'influence coordonnées; souligne que ces pratiques ne doivent pas porter atteinte à la possibilité d'anonymat en ligne, qui est fondamentale pour la protection des journalistes, des militants, des communautés marginalisées et des personnes en situation vulnérable (par exemple, les lanceurs d'alerte, les dissidents et les opposants politiques à des régimes autocratiques) et doivent laisser une place aux comptes satiriques et humoristiques;
56. souligne qu'une responsabilité accrue en matière de suppression de contenus ne doit pas entraîner la suppression arbitraire de contenus légaux; appelle à la prudence pour ce qui est de la suspension totale de comptes de personnes réelles ou de l'utilisation massive de filtres automatisés; observe avec inquiétude les décisions arbitraires des plateformes de supprimer les comptes de représentants élus; souligne que seule une réglementation claire fondée sur des valeurs démocratiques, qui se traduisent par une politique commerciale et dont le respect est assuré au moyen d'un contrôle démocratique indépendant, doit justifier la suppression de ces comptes et qu'un processus complètement transparent relatif au droit de recours est nécessaire;
57. demande des règles contraignantes pour obliger les plateformes à créer des canaux de communication facilement accessibles et efficaces pour les personnes ou les organisations qui souhaitent signaler des contenus illicites, une violation des conditions générales ou des cas de désinformation, d'ingérence étrangère ou de manipulation, afin de permettre, le cas échéant, aux personnes accusées de répondre avant que des mesures restrictives ne soient prises, et plaide en faveur de la mise en place de procédures de saisine et de recours impartiales, transparentes, rapides et accessibles pour les victimes de contenus mis en ligne, les personnes qui signalent des contenus et les personnes ou les organisations affectées par la décision d'étiqueter des comptes, de restreindre leur visibilité, d'en bloquer l'accès, de les suspendre ou de restreindre l'accès aux revenus

publicitaires; recommande que les plateformes de médias sociaux désignent un point de contact spécifique pour chaque État membre et constituent des task forces pour chaque élection importante dans chaque État membre;

58. préconise l'adoption de règles législatives visant à garantir la transparence vis-à-vis des utilisateurs et du grand public, par exemple en obligeant les plateformes à mettre en place des archives publiques et facilement consultables des publicités en ligne, indiquant notamment qui elles visent et qui les a financées, ainsi que des contenus modérés et supprimés, à adopter des mesures d'autorégulation et à donner un accès global et significatif aux informations sur la création, l'utilisation et l'incidence des algorithmes aux autorités nationales compétentes, aux chercheurs agréés affiliés à des institutions universitaires, aux médias, aux organisations de la société civile et aux organisations internationales représentant l'intérêt public; estime qu'il convient d'harmoniser les paramètres de ces archives pour permettre une analyse sur l'ensemble des plateformes et diminuer la charge administrative pour les plateformes;
59. invite à mettre fin aux modèles commerciaux consistant à inciter les internautes à rester plus longtemps sur les plateformes en leur proposant des contenus attrayants; demande aux législateurs et aux plateformes de veiller, en ayant recours à des modérateurs humains et à un auditeur tiers, à ce que les algorithmes ne favorisent pas les contenus illicites, extrémistes, discriminatoires ou menant à la radicalisation, mais offrent plutôt aux utilisateurs une pluralité de perspectives, donnent la priorité aux contenus basés sur des faits et sur la science et valorisent ces contenus, en particulier en ce qui concerne des enjeux sociaux importants tels que la santé publique ou le changement climatique; considère que les systèmes de classement addictifs et basés sur l'engagement constituent une menace systémique pour notre société; invite la Commission à se pencher sur le problème actuel des incitations tarifaires dans le cadre desquelles, pour un même nombre de vues, des publicités très ciblées dotées de contenus cliquants sont souvent vendues à des prix bien inférieurs à ceux des publicités moins ciblées dotées de contenus contribuant à l'intégration sociale;
60. demande que les algorithmes soient modifiés afin de cesser de mettre en avant des contenus provenant de comptes et de canaux non authentiques qui contribuent artificiellement à la propagation de la manipulation de l'information nuisible en provenance de l'étranger; demande que les algorithmes soient modifiés afin qu'ils ne favorisent pas les contenus suscitant la discorde et la colère; souligne la nécessité pour l'Union de mettre en place des mesures visant à obliger juridiquement les entreprises de médias sociaux à empêcher autant que possible l'amplification de la désinformation une fois détectée et insiste sur le fait que des sanctions doivent s'en suivre pour les plateformes qui ne respectent pas l'obligation de retirer les contenus de désinformation;
61. insiste sur la nécessité d'une amélioration de la phase d'essai et d'un examen systématique des conséquences des algorithmes, notamment la manière dont ils façonnent le débat public et influent sur les résultats politiques ainsi que la manière dont les contenus sont hiérarchisés; souligne qu'un tel examen devrait également vérifier si les plateformes sont en mesure de respecter les garanties promises dans leurs conditions générales respectives et si elles ont mis suffisamment de garde-fous en place pour empêcher des comportements non authentiques coordonnés à grande échelle de manipuler le contenu diffusé sur leurs plateformes;

62. s'inquiète vivement des 65 millions d'euros de recettes publicitaires qui alimentent en moyenne chaque année quelque 1 400 sites web de désinformation ciblant les citoyens de l'Union¹⁶; souligne que les publicités en ligne, parfois même d'institutions publiques, aboutissent sur, et donc financent, des sites malveillants diffusant des discours de haine et de la désinformation sans le consentement des annonceurs concernés ou même à leur insu; fait observer que cinq sociétés, dont Google Ads, versent 97 % de ces revenus publicitaires et sont responsables de la sélection des sites web des éditeurs figurant dans leur inventaire, et ont donc le pouvoir de choisir quel contenu sera monétisé ou non; juge inacceptable l'opacité totale pour le public des algorithmes qui distribuent les fonds publicitaires; demande à la Commission d'utiliser les outils de la politique de concurrence et du droit des ententes pour garantir le fonctionnement du marché et briser ce monopole; invite ces acteurs à empêcher que les sites de désinformation soient financés par leurs services publicitaires; félicite les organisations qui se consacrent à la sensibilisation à cette question préoccupante; souligne que les annonceurs devraient avoir le droit de savoir et de décider où leurs publicités sont placées et par quel courtier leurs données sont traitées; demande la mise en place d'un processus de médiation permettant le remboursement des annonceurs lorsque des publicités sont publiées sur des sites web qui favorisent la désinformation;
63. souligne que le code de bonnes pratiques contre la désinformation mis à jour, la législation sur les services numériques, la législation sur les marchés numériques et d'autres mesures liées au plan d'action pour la démocratie européenne nécessiteront un mécanisme efficace de surveillance, d'évaluation et de sanctions après leur adoption, afin de contrôler régulièrement leur mise en œuvre au niveau des États membres et de l'Union, de repérer et de combler les lacunes sans délai ainsi que de sanctionner la mauvaise application et la non-application des engagements; demande à cet égard la désignation, dans chaque État membre, de coordinateurs pour les services numériques ingénieux et fermes, ainsi que l'octroi de ressources suffisantes pour mettre au bras de la Commission chargée du contrôle de l'application de la législation de s'acquitter des tâches qui lui sont confiées au titre de la législation sur les services numériques; souligne en outre l'importance de veiller à ce que les plateformes en ligne soient soumises à des audits indépendants certifiés par la Commission; relève que, pour garantir l'indépendance des auditeurs, les plateformes individuelles ne peuvent les financer;
64. demande à cet égard la définition d'indicateurs clés de performance (ICP) objectifs, par l'intermédiaire de la corégulation, pour garantir le caractère vérifiable des mesures prises par les plateformes ainsi que leur efficacité; souligne que ces ICP devraient inclure des mesures spécifiques à chaque pays, telles que le public visé par la désinformation, l'engagement (taux de clics, etc.), le financement d'activités de vérification des faits ou de recherche dans le pays, ainsi que la prévalence et la force des relations avec la société civile dans le pays;
65. s'inquiète fortement du manque de transparence de la révision du code de bonnes pratiques contre la désinformation, le débat étant resté majoritairement l'apanage du secteur privé et de la Commission; regrette que le Parlement européen, en particulier la

¹⁶ https://disinformationindex.org/wp-content/uploads/2020/03/GDI_Adtech_EU.pdf

commission spéciale INGE, et d'autres parties prenantes clés n'aient pas été correctement consultés lors de la rédaction de la révision du code de bonnes pratiques;

66. déplore la persistance de la nature autorégulatrice du code de bonnes pratiques, étant donné que l'autorégulation est insuffisante lorsqu'il s'agit de protéger le public contre les tentatives d'ingérence et de manipulation; est préoccupé par la possible incapacité du code de bonnes pratiques contre la désinformation mis à jour à apporter une réponse aux défis à venir; s'inquiète du fait que les orientations visant à renforcer le code de bonnes pratiques s'appuient fortement sur la proposition de législation sur les services numériques de la Commission; demande l'adoption rapide de mesures destinées à doter le code de bonnes pratiques d'engagements contraignants pour les plateformes, afin que l'Union soit bien préparée avant les prochaines élections locales, régionales, nationales et européennes;
67. demande à l'Union européenne de protéger et d'encourager le dialogue au sein de la communauté de la technologie ainsi que l'échange d'informations sur le comportement et les stratégies des plateformes sociales; estime que seule une communauté technologique ouverte peut renforcer l'opinion publique contre les attaques, la manipulation et l'ingérence; demande d'étudier la possibilité de créer un centre public-privé d'échange et d'analyse d'informations (ISAC) dans le domaine de la désinformation, dont les membres suivraient, étiquetteraient et échangeraient des informations sur le contenu de la désinformation et sur ses agents de diffusion selon une classification des menaces; estime que ces informations pourraient être utilisées par le système d'alerte rapide de l'Union et par le mécanisme du G7 et qu'elles pourraient également être utiles aux petits acteurs disposant de moins de ressources; demande par ailleurs l'adoption d'une norme sectorielle sur la désinformation pour les services de publicité et de monétisation en ligne afin de démonétiser les contenus préjudiciables, qui devrait être contrôlée par un auditeur tiers et que les systèmes de paiement en ligne et les plateformes de commerce électronique devraient également utiliser;
68. souligne que il est nécessaire que le code puisse servir d'outil efficace jusqu'à l'entrée en vigueur de la législation sur les services numériques; estime que le code devrait anticiper certaines des obligations de la législation sur les services numériques et contraindre les signataires à mettre en œuvre un certain nombre de dispositions de ladite législation concernant l'accès aux données pour les chercheurs et les régulateurs, ainsi que la transparence de la publicité, notamment la transparence des algorithmes et des systèmes de recommandation; demande instamment aux signataires de faire appel à un auditeur indépendant pour contrôler leur conformité avec ces obligations et demande la publication de ces rapports d'audit;
69. déplore le manque de transparence du processus de contrôle du respect du code et regrette le calendrier de la révision du code, qui sera achevée avant les conclusions de la commission spéciale INGE; note qu'il convient, à tout le moins, de rendre publics l'ordre du jour des réunions, les conclusions ainsi que les listes de présence; demande instamment aux signataires de témoigner devant le Parlement de leurs engagements à l'égard du code et de la façon dont ils ont mis et mettront en œuvre ces engagements;

70. estime que les régulateurs indépendants des médias, tels que le groupe des régulateurs européens pour les services de médias audiovisuels, pourraient participer de manière décisive au suivi et à l'application du code;
71. se félicite de la proposition de création d'un groupe de travail énoncée dans les orientations de la Commission visant à renforcer le code; insiste pour que la Commission invite des représentants du Parlement, des régulateurs nationaux et d'autres parties prenantes, y compris la société civile et la communauté des chercheurs, à participer à ce groupe de travail;

Infrastructures critiques et secteurs stratégiques

72. considère que, compte tenu de leur nature interconnectée et transfrontalière, les infrastructures critiques sont de plus en plus vulnérables à l'ingérence extérieure et estime que le cadre actuellement en place doit être révisé; salue donc la proposition de la Commission concernant une nouvelle directive visant à renforcer la résilience des entités critiques fournissant des services essentiels dans l'Union;
73. recommande que les États membres conservent la prérogative d'identifier les entités critiques, mais estime qu'une coordination au niveau de l'Union est nécessaire pour:
 - a) renforcer les canaux de communication et de connexion utilisés par de multiples acteurs, y compris pour la sécurité globale des missions et opérations de l'Union;
 - b) soutenir les autorités compétentes des États membres par l'intermédiaire du groupe sur la résilience des entités critiques, en garantissant une participation diversifiée des parties prenantes, et notamment la participation effective des petites et moyennes entreprises (PME), des organisations de la société civile et des syndicats;
 - c) favoriser l'échange de bonnes pratiques non seulement entre les États membres mais aussi aux niveaux régional et local, notamment avec les Balkans occidentaux, et entre les propriétaires et les exploitants d'infrastructures critiques, y compris par la communication interservices, afin d'identifier à un stade précoce les évolutions préoccupantes et de mettre au point des contre-mesures adéquates;
 - d) mettre en œuvre une stratégie commune pour répondre aux cyberattaques visant des infrastructures critiques;
74. recommande d'étendre la liste des entités critiques aux systèmes d'éducation et aux infrastructures électorales numériques, compte tenu de leur importance cruciale pour garantir le fonctionnement et la stabilité de l'Union et de ses États membres à long terme, et de permettre une certaine souplesse en ce qui concerne les décisions d'ajout à la liste de nouveaux secteurs stratégiques à protéger;
75. invite l'Union à adopter une approche globale pour traiter les questions relatives aux menaces hybrides pesant sur les processus électoraux et à améliorer la coordination et la coopération entre les États membres; invite la Commission à évaluer de manière critique la dépendance à l'égard des plateformes et l'infrastructure de données dans le contexte des élections; estime qu'un contrôle démocratique du secteur privé fait défaut; demande

un contrôle démocratique plus poussé des plateformes, y compris un accès approprié aux données et aux algorithmes pour les autorités compétentes;

76. recommande que les obligations découlant de la directive proposée, y compris les évaluations des menaces, des risques et des vulnérabilités à l'échelle de l'Union et par pays, tiennent compte des dernières évolutions et soient réalisées par le centre commun de recherche, en collaboration avec l'INTCEN du SEAE; souligne qu'il convient de doter ces institutions de ressources suffisantes de façon à ce qu'elles puissent fournir les analyses les plus avancées, sous le sceau d'un contrôle démocratique fort, sans pour autant exclure une évaluation préalable par l'Agence des droits fondamentaux de l'Union européenne afin de garantir le respect des droits fondamentaux;
77. estime que l'Union et ses États membres doivent proposer d'autres solutions de financement aux pays candidats des Balkans occidentaux et aux autres pays candidats potentiels, où les IDE sont utilisés par les pays tiers comme outil géopolitique afin d'accroître leur influence, pour éviter que des parties importantes des infrastructures critiques de pays de l'Union et de pays candidats ne tombent entre les mains de pays tiers et d'entreprises situées en dehors de l'Union, comme dans le cas du port du Pirée en Grèce et comme cela se produit actuellement dans le cas des investissements chinois dans les câbles sous-marins dans les mers Baltique, Méditerranée et Arctique; salue dès lors le règlement sur le filtrage des IDE qui constitue un outil important pour coordonner les actions des États membres en matière d'investissements étrangers, et préconise un cadre réglementaire plus solide et une meilleure application de ce cadre, afin de garantir que les IDE portant atteinte à la sécurité de l'Union soient, comme énoncés dans le règlement, bloqués et que davantage de compétences en matière d'examen des IDE soient transférées aux institutions de l'Union; demande l'abolition du principe du moins-disant dans les décisions d'investissement gouvernementales; invite tous les États membres de l'Union qui ne possèdent pas de mécanismes de filtrage des investissements à mettre en place de telles mesures; estime que le cadre devrait être mieux articulé avec des analyses indépendantes, réalisées par des instituts nationaux et européens ou d'autres parties prenantes pertinentes telles que des groupes de réflexion, afin de cartographier et d'évaluer les flux d'IDE; considère qu'il pourrait également être approprié d'inclure d'autres secteurs stratégiques dans le cadre, tels que la 5G et d'autres technologies de l'information et de la communication, afin de limiter la dépendance de l'Union et de ses États membres à l'égard des fournisseurs à haut risque; souligne que cette approche devrait être appliquée également aux pays candidats et candidats potentiels;
78. estime que l'Union est confrontée à davantage de difficultés en raison de son manque d'investissements par le passé, qui a contribué à sa dépendance à l'égard des fournisseurs étrangers de technologies; recommande de sécuriser les chaînes de production et d'approvisionnement des infrastructures et matériaux critique dans l'Union; estime que l'évolution de l'Union dans le sens d'une autonomie stratégique ouverte et de la souveraineté numérique est importante et représente la bonne façon de procéder; souligne que l'Union devrait déployer de nouveaux outils pour renforcer sa position géostratégique, y compris un instrument anticoercitif; considère que la législation européenne sur les semi-conducteurs annoncée par la Commission, qui vise à garantir que les pièces essentielles à la production de puces soient fabriquées au sein de

l'Union, constitue une étape importante pour limiter la dépendance à l'égard de pays tiers tels que la Chine et les États-Unis; estime que les investissements dans la production de puces doivent être réalisés de manière coordonnée dans l'ensemble de l'Union et sur la base d'une analyse de la demande afin d'éviter une course aux subventions publiques nationales et la fragmentation du marché unique; invite donc la Commission à créer un fonds européen spécifique pour les semi-conducteurs, qui pourrait soutenir la constitution d'une main-d'œuvre qualifiée indispensable et compenser les coûts d'établissement plus élevés des installations de fabrication et de conception dans l'Union; considère Taïwan comme un partenaire important pour stimuler la production de semi-conducteurs dans l'Union;

79. demande de poursuivre le développement de réseaux européens de fournisseurs d'infrastructures et de services de données répondant aux normes de sécurité européennes, tels que GAIA-X, étape importante pour concevoir des solutions durables de substitution aux fournisseurs de services existants et pour parvenir à une économie numérique ouverte, transparente et sécurisée; souligne qu'il est nécessaire de renforcer les PME et d'éviter la cartellisation du marché de l'informatique en nuage; rappelle que les centres de données constituent des infrastructures critiques; s'inquiète de l'influence de pays tiers et de leurs entreprises sur le développement de GAIA-X;
80. souligne que l'intégrité, la disponibilité et la confidentialité des réseaux de communication électroniques publics, tels que les dorsales internet et les câbles de communication sous-marins, revêtent un intérêt vital sur le plan de la sécurité; invite la Commission et les États membres à empêcher le sabotage et l'espionnage de ces réseaux de communication et à promouvoir l'utilisation de normes de routage sécurisé interopérables pour garantir l'intégrité et la robustesse des réseaux et services de communication électroniques, également par l'intermédiaire de la récente stratégie «Global Gateway»;
81. demande à la Commission de proposer des actions visant à mettre en place un approvisionnement sûr, durable et équitable des matières premières utilisées pour produire des composants et technologies critiques, notamment des batteries et des équipements, des technologies de cinquième génération et des générations suivantes, ainsi que des produits chimiques et pharmaceutiques, tout en soulignant l'importance du commerce mondial, de la coopération internationale, dans le respect absolu des droits des travailleurs, et de l'environnement naturel, dans le respect des normes sociales et de durabilité internationales en ce qui concerne l'utilisation des ressources; rappelle la nécessité d'octroyer le financement nécessaire à la recherche et au développement afin de trouver des substituts appropriés en cas de perturbation de la chaîne d'approvisionnement;

Ingérence étrangère pendant les processus électoraux

82. demande que la protection du processus électoral dans son ensemble soit érigée en problème de sécurité prioritaire de l'Union et des États membres, étant donné que des élections libres et équitables constituent le fondement du processus démocratique; demande à la Commission d'élaborer un meilleur cadre d'action pour lutter contre l'ingérence étrangère dans les processus électoraux, qui devrait prévoir, entre autres mesures, des canaux de communication directe avec les citoyens;

83. insiste sur la nécessité d'encourager la résilience de la société face à la désinformation pendant les processus électoraux, y compris dans le secteur privé et les milieux universitaires, et souligne qu'il convient d'adopter une approche globale dans le cadre de laquelle cette ingérence serait combattue de manière continue, allant de programmes d'éducation scolaire à l'intégrité et à la fiabilité techniques du vote, et par des mesures structurelles pour faire face à sa nature hybride; réclame en particulier un plan de préparation des élections européennes de 2024, qui devrait comprendre une stratégie, une formation et une sensibilisation des partis politiques européens et de leur personnel, ainsi que des mesures de sécurité renforcées pour empêcher toute ingérence étrangère;
84. estime que la mésinformation et la désinformation, par l'intermédiaire des médias sociaux, mettent de plus en plus à mal l'intégrité électorale; juge que les plateformes de médias sociaux devraient garantir la mise en œuvre et le bon fonctionnement des politiques visant à préserver l'intégrité des élections; se déclare préoccupé par les récentes conclusions selon lesquelles des acteurs malveillants louent les services d'entreprises privées afin que celles-ci s'immiscent dans les élections, diffusent de fausses informations et propagent des théories conspirationnistes, principalement sur les médias sociaux; demande une enquête approfondie afin de déterminer comment lutter contre le phénomène de la «désinformation rémunérée», face à sa sophistication croissante et à sa généralisation à travers le monde;
85. souligne l'importance capitale des missions d'observation électorale pour fournir des informations utiles et formuler des recommandations spécifiques visant à rendre le système électoral plus résilient et pour contribuer à la lutte contre l'ingérence étrangère dans les processus électoraux; demande l'amélioration et le renforcement des processus électoraux et souligne que les missions d'observation électorale constituent un instrument clé pour lutter contre le recours accru aux processus électoraux injustes et truqués par les régimes illibéraux cherchant une apparence démocratique; souligne, à cet égard, la nécessité de réévaluer et de mettre à jour les outils et méthodes utilisés dans le cadre de l'observation internationale d'élections afin de faire face aux nouvelles tendances et menaces, notamment la lutte contre les faux observateurs électoraux, l'échange de bonnes pratiques avec des partenaires partageant les mêmes idées ainsi qu'une collaboration plus étroite avec les organisations internationales pertinentes, comme l'Organisation pour la sécurité et la coopération en Europe (OSCE) et le Conseil de l'Europe, et tous les acteurs concernés dans le cadre de la déclaration de principes relative à l'observation internationale d'élections et du code de conduite à l'usage des observateurs électoraux internationaux; souligne que la participation de députés au Parlement européen à des missions d'observation électorale non autorisées porte atteinte à la crédibilité et à la réputation du Parlement européen; salue la procédure du groupe de soutien à la démocratie et de coordination des élections en cas d'observation électorale non officielle par des députés au Parlement européen (adoptée le 13 décembre 2018) qui permet d'exclure des députés de délégations officielles d'observation des élections pour la durée du mandat et préconise la pleine application de cette procédure;

Financement dissimulé des activités politiques provenant de donateurs étrangers

86. souligne que, s'il est encore nécessaire de mieux comprendre les effets du financement dissimulé des activités politiques sur, par exemple, les tendances antidémocratiques en Europe, il n'en demeure pas moins que le financement étranger d'activités politiques

par des opérations secrètes constitue une atteinte grave à l'intégrité du fonctionnement démocratique de l'Union et de ses États membres, en particulier en période électorale, et viole donc le principe d'élections libres et équitables; insiste sur le fait qu'il convient donc de rendre illégale dans tous les États membres la participation à toute activité secrète financée par des acteurs étrangers qui vise à influencer le processus des politiques européennes ou nationales; relève, à cet égard, que des pays comme l'Australie ont adopté des lois qui interdisent l'ingérence étrangère en politique;

87. condamne le fait que des partis extrémistes, populistes et anti-européens et certains autres partis et individus sont liés à des tentatives d'ingérence dans les processus démocratiques de l'Union et sont explicitement complices de ces tentatives et juge alarmant que ces partis soient utilisés par des acteurs d'ingérence étrangère pour faire entendre leur voix et pour légitimer leurs gouvernements autoritaires; demande que toute la lumière soit faite sur les relations politiques et économiques entre ces partis et individus et la Russie; estime que ces relations sont tout à fait inappropriées et condamne toute complicité susceptible, à des fins politiques, d'exposer l'Union et ses États membres à des attaques de puissances étrangères;
88. demande aux États membres, lorsqu'ils harmoniseront davantage les réglementations nationales, de combler notamment toutes les failles qui suivent et d'interdire les dons étrangers;
 - a) les contributions en nature provenant d'acteurs étrangers aux partis politiques, aux fondations, aux personnes occupant une fonction publique ou aux élus, y compris les prêts financiers provenant de toute personne morale ou physique basée en dehors de l'Union et de l'espace économique européen (EEE) (à l'exception des électeurs européens), les dons anonymes dépassant un certain seuil et l'absence de limites en matière de dépenses des campagnes politiques, qui permet d'exercer une influence par des dons importants; les personnes, acteurs ou partis politiques qui se sont vu offrir et/ou ont accepté une contribution financière ou en nature d'un acteur étranger doivent être tenus de le signaler aux autorités compétentes et ces informations devraient à leur tour être communiquées au niveau de l'Union pour permettre une surveillance à l'échelle de l'Union;
 - b) les citoyens prête-noms¹⁷: la transparence concernant les donateurs en tant que personnes physiques et morales doit être appliquée au moyen de déclarations de conformité attestant du statut du donateur et en accordant des pouvoirs d'application plus importants aux commissions électorales; les dons provenant de l'Union qui dépassent un seuil minimal déterminé devraient être consignés dans un registre officiel public et liés à une personne physique et un plafond devrait être fixé pour les dons provenant de personnes physiques et morales (et les subventions) en faveur de partis politiques;
 - c) les sociétés-écrans et les filiales nationales de sociétés mères étrangères¹⁸: les sociétés-écrans devraient être interdites et des exigences plus strictes devraient

¹⁷ Personne qui donne l'argent d'un tiers à un parti politique ou à un candidat en utilisant son propre nom.

¹⁸ Cette catégorie englobe deux réalités différentes: les sociétés-écrans, qui n'exercent pas d'activités commerciales réelles et ne servent qu'à dissimuler des financements, et les filiales nationales de sociétés mères

être établies afin de révéler les origines du financement par l'intermédiaire de sociétés mères; le financement et les dons à des partis politiques supérieurs à un certain seuil doivent être consignés dans un registre public et central avec un nom et une adresse officiels pouvant être liés à une personne existante, et les États membres devraient collecter ces informations; invite la Commission à veiller à ce que les autorités des États membres aient le droit d'enquêter sur l'origine des financements afin de vérifier les informations provenant des filiales nationales et de remédier au manque de données dans les registres nationaux, en particulier dans les situations où un réseau de sociétés-écrans est utilisé;

- d) les organisations à but non lucratif et les tiers¹⁹, coordonnés par des acteurs étrangers et créés dans le but d'influencer les processus électoraux: des règles plus uniformes et une plus grande transparence devraient être envisagées dans toute l'Union pour les organisations visant à financer des activités politiques lorsqu'elles cherchent à influencer directement les processus électoraux tels que les élections et les campagnes référendaires; ces règles ne devraient pas empêcher les organisations à but non lucratif et les tiers de recevoir un financement pour des campagnes thématiques; des règles garantissant la transparence des financements ou des dons doivent également s'appliquer aux fondations politiques;
- e) les publicités politiques en ligne ne sont pas soumises aux règles relatives à la publicité télévisée, radiophonique et imprimée et ne sont généralement pas réglementées au niveau de l'Union: il est donc nécessaire d'interdire les publicités achetées par des acteurs provenant de l'extérieur de l'Union et de l'EEE et de garantir une transparence totale en ce qui concerne l'achat de publicités politiques en ligne par des acteurs de l'Union; il convient d'assurer une transparence et une responsabilité démocratique beaucoup plus grandes quant à l'utilisation des algorithmes; se félicite de l'annonce de la publication par la Commission d'une nouvelle proposition législative sur la transparence des contenus politiques sponsorisés, comme proposé dans le cadre du plan d'action pour la démocratie européenne, qui devrait viser à éviter un ensemble disparate de 27 arsenaux législatifs nationaux différents en matière de publicité politique en ligne et qui veillera à ce que les partis de l'Union puissent faire campagne en ligne avant les élections européennes, tout en limitant le risque d'ingérence étrangère et en déterminant quelles règles adoptées sur une base volontaire par les partis politiques au sein des États membres et les principales plateformes de médias sociaux pourraient être appliquées à tous dans l'Union; invite les États membres à mettre à jour leurs règles nationales en matière de publicité politique, qui sont à la traîne au regard de l'adoption rapide des médias numériques en tant que principal mode de communication politique; demande à la Commission de proposer une définition démocratique de la publicité politique engagée afin de mettre fin à une situation où des plateformes privées à but lucratif décident de ce qui est engagé et de ce qui ne l'est pas;

étrangères, utilisées pour injecter de l'argent étranger dans la politique.

¹⁹ Les organisations à but non lucratif et les tiers ne sont pas tenus de divulguer l'identité de leurs donateurs, mais sont autorisés à financer des partis politiques et des candidats dans plusieurs États membres de l'Union.

- f) des auditeurs indépendants devraient assurer le suivi des dépenses électorales et les informations sur les dépenses et les dons devraient être mises à la disposition de ces auditeurs indépendants en temps utile, afin d'atténuer les risques de conflits d'intérêts et de lobbying en rapport avec le financement politique; dans le cadre de la mise en place de la divulgation proactive d'informations, les institutions responsables de la réglementation financière devraient disposer d'un mandat clair, ainsi que des capacités, des ressources et du pouvoir juridique nécessaires pour mener des enquêtes et déférer des affaires à des fins de poursuites pénales;
89. invite donc la Commission à procéder à une analyse des financements occultes dans l'Union et à présenter des propositions concrètes visant à combler toutes les lacunes qui permettent le financement opaque des partis et des fondations politiques ou des personnes occupant une fonction publique ou élective à partir de sources de pays tiers, ainsi qu'à proposer des normes européennes communes qui s'appliqueraient aux lois électorales nationales dans tous les États membres; estime que les États membres devraient viser à introduire des obligations de transparence claires concernant le financement des partis politiques et une interdiction des dons aux partis politiques et aux acteurs politiques provenant de l'extérieur de l'Union et de l'EEE, à l'exception des électeurs européens vivant en dehors de l'Union et de l'EEE, et à définir une stratégie claire concernant le système de sanctions; demande instamment à la Commission et aux États membres d'établir une autorité de l'Union pour les contrôles financiers afin de combattre les pratiques financières illicites et les ingérences de la Russie et d'autres régimes autoritaires; insiste sur la nécessité d'interdire les dons ou les financements ayant recours à des technologies émergentes très difficiles à tracer; demande aux États membres et à la Commission d'affecter davantage de ressources et des mandats plus solides aux agences de supervision afin d'obtenir des données de meilleure qualité;
90. s'engage à veiller à ce que l'ensemble des organisations à but non lucratif, des groupes de réflexion, des instituts et des ONG contribuant, dans le cadre du travail parlementaire, à l'élaboration des actes de l'Union ou jouissant d'un rôle consultatif dans le processus législatif soient totalement transparents et indépendants et que leur financement et leur propriété n'engendrent aucun conflit d'intérêts;
91. salue la révision en cours du règlement (UE, Euratom) n° 1141/2014 relatif au statut et au financement des partis politiques européens et des fondations politiques européennes; soutient tous les efforts visant à atteindre un plus grand niveau de transparence dans le financement des activités des partis et des fondations politiques européens, en particulier dans la perspective des élections européennes de 2024, y compris l'interdiction de tous les dons provenant de l'extérieur de l'Union et de sources anonymes, à l'exception des dons issus de la diaspora des États membres de l'Union, et des dons provenant de l'extérieur de l'Union qui ne peuvent pas être documentés par des contrats, des accords de service ou des cotisations associées à l'affiliation à un parti politique européen, tout en autorisant les partis membres nationaux situés en dehors de l'Union et de l'EEE à verser des cotisations à des partis politiques européens; demande instamment aux partis politiques européens et nationaux de s'engager à lutter contre l'ingérence étrangère et à combattre la propagation de la désinformation en signant une charte contenant des engagements spécifiques à cet égard;

92. souligne que la mise en œuvre de nombreuses recommandations du GRECO et de la Commission de Venise du Conseil de l'Europe renforcerait l'immunité du système politique des États membres et de l'Union dans son ensemble contre l'influence financière étrangère;

Cybersécurité et résilience face aux cyberattaques

93. demande instamment aux institutions de l'Union et aux États membres d'augmenter rapidement les investissements dans les capacités numériques stratégiques de l'Union et ses compétences de détection et de révélation des ingérences étrangères ainsi que de lutte contre ces dernières, telles que l'intelligence artificielle, la communication sécurisée et les infrastructures de données et en nuage, afin d'améliorer la cybersécurité de l'Union, tout en veillant au respect des droits fondamentaux; invite la Commission à investir également davantage dans le renforcement des connaissances numériques et de l'expertise technique de l'Union, afin de mieux comprendre les systèmes numériques utilisés dans l'ensemble de l'Union; engage la Commission à allouer des ressources humaines, matérielles et financières supplémentaires aux capacités d'analyse des cybermenaces, c'est-à-dire à l'INTCEN du SEAE, et à la cybersécurité des institutions, organes et agences de l'Union, et donc à l'ENISA et à l'équipe d'intervention en cas d'urgence informatique pour les institutions, organes et agences de l'Union (CERT-UE), ainsi que des États membres; déplore le manque de coopération et d'harmonisation entre les États membres en matière de cybersécurité;
94. salue les propositions de la Commission relatives à une nouvelle stratégie de cybersécurité et à une nouvelle directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148²⁰ (NIS2); recommande que le résultat final des travaux en cours sur la proposition corrige les défauts de la directive NIS de 2016, notamment en renforçant les exigences de sécurité, en élargissant le champ d'application, en créant un cadre pour la coopération européenne et le partage d'informations, en renforçant les capacités de cybersécurité des États membres, en approfondissant la coopération public-privé, en introduisant des exigences de mise en œuvre plus strictes et en faisant de la cybersécurité une responsabilité au plus haut niveau de direction des entités européennes vitales pour notre société; souligne combien il importe d'atteindre un niveau commun élevé de cybersécurité dans tous les États membres afin de limiter les points faibles de la cybersécurité collective de l'Union; insiste sur le besoin impérieux de résilience des systèmes d'information et salue à cet égard le réseau européen pour la préparation et la gestion des crises cyber (CyCLONE); incite à promouvoir davantage les mesures de renforcement de la confiance en matière de cyberspace de l'OSCE;
95. se félicite de la proposition faite par la Commission dans la directive NIS2 de réaliser des évaluations des risques de sécurité coordonnées des chaînes d'approvisionnement critiques, dans la même veine que sa boîte à outils de l'Union pour la 5G, afin de mieux prendre en compte les risques liés, par exemple, à l'utilisation de logiciels et de matériels produits par des entreprises sous le contrôle d'États étrangers; engage la

²⁰ Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 (COM(2020)0823).

Commission à concevoir des normes et des règles de concurrence mondiales pour la 6G, dans le respect des valeurs démocratiques; invite la Commission à promouvoir les échanges entre les institutions de l'Union et les autorités nationales sur les défis, les meilleures pratiques et les solutions liés aux mesures de la boîte à outils; estime que l'Union devrait investir davantage dans ses capacités dans le domaine des technologies 5G et post-5G afin de réduire les dépendances vis-à-vis des fournisseurs étrangers;

96. souligne que la cybercriminalité n'a pas de frontières et prie instamment l'Union d'intensifier ses efforts internationaux visant à y remédier de manière efficace; souligne que l'Union devrait jouer un rôle moteur dans l'élaboration d'un traité international relatif à la cybersécurité qui fixerait des normes internationales en matière de cybersécurité pour lutter contre la cybercriminalité;
97. accueille favorablement l'annonce de l'élaboration d'une législation sur la cyberrésilience qui viendrait compléter une politique européenne de cyberdéfense, étant donné que la cybernétique et la défense sont interconnectées; réclame une hausse des investissements dans les capacités et la coordination de la cyberdéfense européenne; recommande de favoriser le renforcement des capacités informatiques de nos partenaires au moyen de missions de formation ou de missions civiles de cybersécurité de l'Union; insiste sur la nécessité d'harmoniser et de normaliser la formation dans le domaine du cyberspace et demande des financements structurels de l'Union dans ce domaine;
98. condamne l'utilisation massive et illicite du logiciel de surveillance Pegasus de l'entreprise NSO Group par des entités publiques de pays tels que le Maroc, l'Arabie saoudite, la Hongrie, la Pologne, Bahreïn, les Émirats arabes unis et l'Azerbaïdjan à l'encontre de journalistes, de défenseurs des droits de l'homme et de responsables politiques; rappelle que Pegasus n'est qu'un des nombreux exemples de programmes exploités par des entités étatiques à des fins de surveillance illicite à grande échelle de citoyens innocents; condamne également d'autres opérations d'espionnage d'État visant des responsables politiques européens; invite instamment la Commission à dresser une liste des logiciels de surveillance illicite et à mettre à jour en permanence cette liste; demande à l'Union et aux États membres d'utiliser cette liste aux fins de l'exercice du devoir de vigilance en matière de droits de l'homme et d'un contrôle approprié des exportations européennes de technologies de surveillance et d'assistance technique ainsi que des importations dans les États membres qui présentent un risque manifeste pour l'état de droit; demande, en outre, la création d'un laboratoire citoyen de l'Union, semblable à celui établi au Canada, composé de journalistes, d'experts en droits de l'homme et d'experts en rétro-ingénierie des logiciels malveillants, qui s'attellerait à déceler et à dénoncer toute utilisation illégale de logiciels à des fins de surveillance illicite;
99. engage l'Union à adopter un cadre réglementaire solide dans ce domaine, tant au sein de l'Union qu'au niveau international; se félicite, à cet égard, de la décision du Bureau de l'industrie et de la sécurité du ministère américain du commerce de mettre NSO Group Technologies sur liste noire afin d'empêcher la société de bénéficier de technologies américaines;

100. fait part de sa préoccupation quant au fait que l'Union coopère sur des affaires judiciaires et répressives avec des pays tiers ayant collaboré avec NSO Group et utilisé le logiciel Pegasus pour espionner des citoyens de l'Union; réclame des garanties supplémentaires et un renforcement du contrôle démocratique de cette coopération;
101. invite la Commission à examiner les investissements de l'Union dans NSO Group Technologies et à adopter des mesures ciblées à l'encontre des pays tiers qui utilisent des logiciels pour espionner des citoyens de l'Union ou des personnes bénéficiant du statut de réfugié dans des États membres;
102. s'inquiète du fait que des journalistes et des défenseurs de la démocratie puissent être illégalement maintenus sous surveillance et harcelés par les régimes autoritaires qu'ils ont cherché à fuir, même sur le sol de l'Union européenne, et considère que cela constitue une violation grave des valeurs fondamentales de l'Union et des droits fondamentaux des individus, tels que prévus par la charte des droits fondamentaux, la convention européenne des droits de l'homme (CEDH) et le pacte international relatif aux droits civils et politiques; regrette le manque de soutien juridique apporté aux victimes de ce logiciel espion;
103. souligne l'urgence nécessaire de renforcer le cadre législatif afin de tenir pour responsables ceux qui distribuent, utilisent et exploitent ces logiciels à des fins illicites et non autorisées; se réfère, en particulier, aux sanctions imposées le 21 juin 2021 à Alexander Shatrov, PDG d'une société biélorusse qui produit un logiciel de reconnaissance faciale utilisé par un régime autoritaire, par exemple dans le but d'identifier des manifestants soutenant l'opposition politique; invite la Commission à empêcher toute utilisation ou tout financement dans l'Union de technologies de surveillance illicite; engage l'Union et les États membres à coopérer avec les gouvernements des pays tiers en vue de mettre fin aux pratiques et législations répressives en matière de cybersécurité et de lutte contre le terrorisme et de renforcer le contrôle démocratique; demande qu'une enquête soit menée par les autorités compétentes de l'Union sur l'utilisation illicite du logiciel espion dans l'Union et sur l'exportation de tels logiciels depuis l'Union, et qu'il y ait des conséquences pour les États membres et les pays associés, notamment ceux participant aux programmes de l'Union, qui ont acheté et utilisé ce logiciel espion et depuis lesquels il a été exporté pour cibler illégalement des journalistes, des défenseurs des droits de l'homme, des avocats et des hommes politiques;
104. demande une révision ambitieuse de la directive vie privée et communications électroniques²¹ afin de renforcer la confidentialité des communications et des données personnelles lors de l'utilisation d'appareils électroniques, sans que ne soit abaissé le niveau de protection offert par la directive et sans préjudice de la responsabilité des États membres en matière de préservation de la sécurité nationale; souligne que les autorités publiques devraient être obligées de divulguer les vulnérabilités qu'elles détectent dans les dispositifs informatiques; engage l'Union et les États membres à coordonner davantage leurs actions sur la base de la directive relative aux attaques

²¹ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO L 201 du 31.7.2002, p. 37.

contre les systèmes d'information²² afin de veiller à ce que l'accès illégal aux systèmes d'information et l'interception illégale soient définis comme des infractions pénales et fassent l'objet de sanctions appropriées; rappelle que toute transgression de la confidentialité à des fins de sécurité nationale doit être effectuée en toute légalité et à des fins explicites et légitimes dans une société démocratique, en cas de stricte nécessité et dans le respect de la proportionnalité, comme l'exigent la CEDH et la Cour de justice de l'Union européenne;

Protection des États membres, des institutions, des agences, des délégations et des missions de l'Union européenne

105. souligne que les institutions, les organes, les agences, les délégations, les missions et réseaux d'opération, les bâtiments et le personnel de l'Union sont des cibles pour tous les types de menaces et d'attaques hybrides d'acteurs étatiques étrangers et, partant, devraient être protégés comme il se doit, et qu'il convient d'accorder une attention particulière aux biens, locaux et activités du SEAE à l'étranger et à la protection du personnel de l'Union envoyé dans des pays non démocratiques gouvernés par des régimes répressifs; demande que les missions de la PSDC réagissent de manière structurée à ces menaces et qu'elles reçoivent un soutien plus concret au moyen d'une communication stratégique; prend acte de l'augmentation constante des attaques commanditées par des États contre les institutions, les organes et les agences de l'Union, notamment contre l'EMA, ainsi que contre les institutions et les autorités publiques des États membres;
106. demande un examen approfondi et périodique de l'ensemble des services, des réseaux, des équipements et du matériel des institutions, organes, agences, délégations, missions et opérations de l'Union afin de renforcer leur résilience aux menaces en matière de cybersécurité et d'exclure les programmes et dispositifs potentiellement dangereux, tels que ceux mis au point par Kaspersky Lab; demande instamment aux institutions de l'Union et aux États membres de veiller à ce que le personnel reçoive des lignes directrices adéquates et des outils sûrs; insiste sur la nécessité de sensibiliser davantage les institutions et les administrations à l'importance de l'utilisation de services et de réseaux sécurisés, y compris lors des missions; met en avant la confiance et les avantages sur le plan de la sécurité qu'offrent les systèmes d'exploitation de réseau basés sur un code source ouvert, qui sont utilisés à grande échelle par les agences militaires et gouvernementales alliées;
107. souligne l'importance d'une coordination efficace, opportune et étroite entre les institutions, organes et agences de l'Union spécialisés dans la cybersécurité, tels que la CERT-UE, parallèlement au développement complet de ses capacités opérationnelles, ainsi que l'ENISA et la future unité conjointe de cybersécurité, qui permettra d'apporter une réponse coordonnée aux menaces de cybersécurité à grande échelle dans l'Union; salue la coopération structurée en cours entre la CERT-UE et l'ENISA; se félicite également de la mise en place, au sein de l'INTCEN, du groupe de travail de l'Union sur le cyberrenseignement en vue de renforcer la coopération stratégique en matière de renseignement; apprécie les récentes initiatives prises par les secrétaires généraux des

²² Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, JO L 218 du 14.8.2013, p. 8.

institutions de l'Union pour élaborer des règles communes en matière d'information et de cybersécurité;

108. attend avec intérêt les deux propositions de règlement de la Commission établissant un cadre normatif pour la sécurité de l'information et la cybersécurité dans l'ensemble des institutions, organes et agences de l'Union, et estime que ces règlements devraient prévoir le renforcement des capacités et de la résilience; invite la Commission et les États membres à affecter des fonds et des ressources supplémentaires à la cybersécurité des institutions de l'Union afin de résoudre les problèmes posés par un paysage de menaces en constante évolution;
109. attend avec intérêt le rapport spécial de la Cour des comptes européenne sur l'audit de cybersécurité, attendu pour le début de l'année 2022;
110. réclame une enquête approfondie sur les cas signalés d'infiltration étrangère parmi le personnel des institutions de l'Union; demande un réexamen et une éventuelle révision des procédures en matière de ressources humaines, en vue d'intégrer notamment une vérification préalable au recrutement, afin de combler les lacunes permettant une infiltration étrangère; invite les organes directeurs du Parlement à améliorer les procédures d'habilitation de sécurité pour le personnel et à renforcer les règles et les contrôles d'accès à ses locaux afin d'empêcher les personnes étroitement liées à des intérêts étrangers d'avoir accès à des réunions et informations confidentielles; engage les autorités belges à réviser et à actualiser le cadre national de lutte contre l'espionnage afin que les contrevenants soient détectés, poursuivis et sanctionnés de manière efficace; préconise des actions similaires dans les autres États membres afin de protéger les institutions et agences de l'Union sur leur territoire;
111. demande à toutes les institutions de l'Union de sensibiliser leur personnel par une formation et des conseils appropriés afin de prévenir, d'atténuer et de traiter les risques de sécurité cybernétique et non cybernétique; préconise une formation obligatoire et régulière à la sécurité et aux TIC de l'ensemble du personnel (y compris les stagiaires) et des députés européens; réclame un recensement régulier et spécifique et des évaluations des risques d'influence étrangère au sein des institutions;
112. insiste sur la nécessité de procédures de gestion de crise appropriées pour les cas de manipulation de l'information, dont des systèmes d'alerte entre les niveaux administratifs et les secteurs, afin de fournir des informations mutuelles et d'empêcher les manipulations de l'information; salue, à cet égard, le système d'alerte rapide (SAR) et la procédure d'alerte rapide établis avant les élections européennes de 2019, ainsi que les procédures en place dans les administrations de la Commission et du Parlement pour avertir d'éventuels cas touchant les institutions ou les processus démocratiques de l'Union; demande à l'administration de l'Union de renforcer sa surveillance, notamment par la création d'un registre central et d'un outil de suivi des incidents, et de mettre au point une boîte à outils partagée à activer en cas d'alerte émanant du SAR;
113. réclame des règles obligatoires en matière de transparence pour les voyages offerts par des entités et pays étrangers à des membres des institutions de l'Union, dont les députés européens, les APA et les conseillers de groupes, ainsi qu'à des fonctionnaires nationaux, concernant notamment: le nom des tiers payants, le coût des voyages et les

motifs invoqués; rappelle que de tels voyages organisés ne peuvent pas être considérés comme des délégations officielles du Parlement européen et demande que des sanctions strictes soient appliquées en cas de non-respect de cette règle; souligne que les groupes d'amitié informels peuvent entraver le travail des organes officiels du Parlement européen et nuire à sa réputation et à la cohérence de son action; demande instamment aux organes directeurs du Parlement de renforcer la transparence et la responsabilisation de ces groupes, de faire appliquer les règles en vigueur et de prendre les mesures nécessaires lorsque ces groupes d'amitié sont utilisés avec malveillance par des pays tiers; demande aux questeurs d'élaborer et de tenir à jour un registre accessible des groupes d'amitié et des déclarations;

Ingérence d'acteurs étrangers par l'accaparement des élites, les diasporas nationales, les universités et les manifestations culturelles

114. condamne tous les types d'accaparement des élites et la technique de cooptation de fonctionnaires de haut niveau et d'anciens responsables politiques de l'Union utilisés par des entreprises étrangères entretenant des relations avec des gouvernements qui se livrent activement à des actions d'ingérence contre l'Union, et déplore le manque d'outils et de dispositifs de répression nécessaires pour empêcher ces pratiques; considère que la divulgation d'informations confidentielles acquises lors de mandats publics ou dans l'exercice de fonctions de fonctionnaires au détriment des intérêts stratégiques de l'Union et de ses États membres devrait avoir des conséquences juridiques et donner lieu à des sanctions sévères, dont le licenciement immédiat ou la disqualification de tout recrutement futur par les institutions; considère que les déclarations de revenus et de patrimoine de ces personnes devraient être rendues publiques;
115. invite la Commission à encourager et à coordonner les actions visant à lutter contre l'accaparement des élites, par exemple en complétant et en faisant appliquer sans exception les délais de viduité des commissaires européens et des hauts fonctionnaires de l'Union, avec obligation de rapport à l'issue de ces délais, afin de mettre fin à la pratique des allers-retours entre le secteur public et le secteur privé, et en établissant des règles structurées pour lutter contre l'accaparement des élites au niveau de l'Union; demande à la Commission d'évaluer si les exigences actuelles en matière de délais de viduité sont toujours adaptées à la situation; souligne que les anciens responsables politiques et fonctionnaires de l'Union qui sont approchés par un État étranger devraient le signaler à un organisme de surveillance spécialisé et bénéficier de la protection des lanceurs d'alerte; invite tous les États membres à appliquer et à harmoniser les délais de viduité pour leurs dirigeants politiques et à veiller à ce qu'ils disposent de mesures et de systèmes exigeant des fonctionnaires qu'ils déclarent leurs activités extérieures, leur emploi, leurs investissements, leurs avoirs et les cadeaux ou avantages importants susceptibles de donner lieu à un conflit d'intérêts;
116. est préoccupé par les stratégies de lobbying intégrées combinant intérêts industriels et objectifs politiques étrangers, en particulier lorsqu'elles servent les intérêts d'un État autoritaire; demande par conséquent aux institutions de l'Union de réformer le registre de transparence, notamment en introduisant des règles de transparence plus strictes, en répertoriant les financements étrangers du lobbying lié à l'Union et en prévoyant une catégorie de données qui permette de reconnaître les financements provenant de

gouvernements étrangers; appelle de ses vœux une coopération efficace sur cette question entre toutes les institutions de l'Union; considère que le système australien de transparence en matière d'influence étrangère est une bonne pratique à suivre;

117. invite les États membres à envisager la mise en place d'un système d'enregistrement de l'influence étrangère et la création d'un registre tenu par les pouvoirs publics des activités déclarées entreprises pour un État étranger ou en son nom, en suivant les bonnes pratiques d'autres démocraties partageant les mêmes valeurs;
118. est préoccupé par les actions entreprises par des États autoritaires étrangers en vue de contrôler les diasporas vivant sur le sol de l'Union; souligne le rôle crucial joué par le Front uni de la Chine, qui est un département dépendant directement du Comité central du Parti communiste chinois et chargé de coordonner la stratégie d'ingérence extérieure de la Chine par un contrôle strict des individus et des entreprises chinoises à l'étranger; fait observer que l'Australie et la Nouvelle-Zélande ont de l'expérience en matière de relations avec le Front uni;
119. condamne fermement les entreprises du Kremlin visant à instrumentaliser les minorités dans les États membres en mettant en application des politiques de «soutien des compatriotes», notamment dans les États baltes et les pays du voisinage oriental, dans le cadre de la stratégie géopolitique du régime de Poutine, dont l'objectif est de diviser les sociétés de l'Union, parallèlement à la mise en œuvre du concept de «monde russe», qui vise à justifier les actions expansionnistes du régime; relève qu'un grand nombre de «fondations privées», d'«entreprises privées», d'«organisations médiatiques» et d'«ONG» russes sont soit détenues par l'État, soit ont des liens cachés avec l'État russe; souligne qu'il est primordial, dans le cadre du dialogue avec la société civile russe, de faire la distinction entre les organisations qui se tiennent à l'écart de l'influence du gouvernement russe et celles qui ont des liens avec le Kremlin; rappelle qu'il existe également des preuves d'ingérence et de manipulation russes dans de nombreuses autres démocraties libérales occidentales, ainsi que d'un soutien actif aux forces extrémistes et aux entités radicales en vue de déstabiliser l'Union; constate que le Kremlin recourt largement à la culture, notamment à la musique populaire, aux contenus audiovisuels et à la littérature, dans le cadre de son écosystème de désinformation; déplore la volonté de la Russie de ne pas reconnaître pleinement les crimes soviétiques et de réécrire l'histoire du pays;
120. est préoccupé par les tentatives du gouvernement turc d'influencer les personnes ayant des racines turques dans le but d'utiliser la diaspora comme relais pour les positions d'Ankara et de diviser les sociétés européennes, notamment par l'intermédiaire de la Présidence des Turcs à l'étranger et des communautés apparentées (YTB); condamne les tentatives flagrantes de la Turquie d'instrumentaliser sa diaspora en Europe afin de changer le cours des élections;
121. condamne les entreprises de la Russie visant à exploiter les tensions ethniques dans les Balkans occidentaux afin d'attiser les conflits et de diviser les communautés, ce qui pourrait conduire à une déstabilisation de l'ensemble de la région; s'inquiète du fait que l'Église orthodoxe, dans des pays comme la Serbie, le Monténégro et la Bosnie-Herzégovine, notamment dans sa République serbe, tente de promouvoir la Russie en tant que protectrice des valeurs familiales traditionnelles et de fortifier les relations entre

l'État et l'Église; juge alarmant que la Hongrie et la Serbie servent les objectifs géopolitiques de la Chine et de la Russie; recommande d'organiser des dialogues avec la société civile et le secteur privé des Balkans occidentaux afin de coordonner les efforts de lutte contre la désinformation dans la région, en mettant l'accent sur la recherche et l'analyse et en intégrant l'expertise régionale; invite la Commission à mettre en place les infrastructures nécessaires pour contrer avec des réponses factuelles les entreprises de désinformation à court et à long termes dans les Balkans occidentaux; engage le SEAE à adopter une attitude plus proactive, en s'attelant à rehausser la crédibilité de l'Union dans la région au lieu de simplement la défendre et en élargissant la surveillance de la task force StratCom afin de se concentrer sur les menaces de désinformation transfrontières émanant des pays des Balkans occidentaux et de leurs voisins;

122. insiste sur la nécessité pour l'Union et ses États membres de soutenir davantage les pays du partenariat oriental, notamment par une coopération visant à renforcer la résilience des États et des sociétés à la désinformation ainsi qu'à la propagande de l'État russe, afin de contrer l'affaiblissement et la fragmentation stratégiques de leurs sociétés et institutions;
123. s'inquiète vivement de l'application extraterritoriale de mesures coercitives découlant de la nouvelle loi sur la sécurité nationale à Hong Kong et de la loi chinoise sur la lutte contre les sanctions étrangères, combinée aux accords d'extradition conclus par la Chine avec d'autres pays, qui permet à la Chine de mettre en œuvre des mesures dissuasives à grande échelle à l'encontre de ressortissants non chinois critiques envers le régime, par exemple, dans une affaire récente, à l'encontre de deux députés danois, ainsi que des contre-sanctions visant cinq députés européens, la sous-commission «droits de l'homme» du Parlement, trois députés des États membres de l'Union, le Comité politique et de sécurité du Conseil de l'Union européenne, deux universitaires européens et deux groupes de réflexion européens en Allemagne et au Danemark; invite tous les États membres à résister et à refuser l'extradition et, le cas échéant, à offrir une protection appropriée aux personnes concernées afin de prévenir d'éventuelles violations des droits de l'homme;
124. est préoccupé par le nombre d'universités, d'écoles et de centres culturels européens engagés dans des partenariats avec des entités chinoises, notamment des instituts Confucius, qui permettent le vol de connaissances scientifiques et l'exercice d'un contrôle strict sur tous les sujets liés à la Chine dans le domaine de la recherche et de l'enseignement, ce qui constitue une violation de la protection constitutionnelle de la liberté et de l'autonomie académiques, et sur les choix des activités culturelles en rapport avec la Chine; craint que de telles actions puissent entraîner une perte de connaissances sur les questions liées à la Chine, privant ainsi l'Union des compétences nécessaires; est préoccupé, par exemple, par le parrainage, en 2014, de la bibliothèque chinoise du Collège d'Europe par le Bureau d'information du Conseil d'État du gouvernement chinois²³; s'inquiète vivement des pressions exercées par la Chine en vue, par exemple, de censurer l'exposition sur Gengis Khan du Musée d'histoire de

²³ <https://www.coleurope.eu/fr/events/inauguration-officielle-de-la-bibliotheque-chinoise>

Nantes initialement prévue pour 2020²⁴; invite la Commission à faciliter l'échange de bonnes pratiques entre États membres afin de lutter contre l'ingérence étrangère dans les secteurs de la culture et de l'éducation;

125. est préoccupé par les cas de financement dissimulé de recherches menées en Europe, ainsi que par les tentatives de la Chine de débaucher des talents au moyen du programme «Mille talents» et des bourses des instituts Confucius, et par la combinaison délibérée de projets scientifiques militaires et civils dans le cadre de la stratégie de fusion civilo-militaire de la Chine; met en lumière la volonté des établissements d'enseignement supérieur chinois de signer des protocoles d'accord avec des établissements partenaires en Europe qui contiennent des clauses perpétuant la propagande chinoise ou apportant un soutien aux positions ou à des initiatives politiques du Parti communiste chinois, telles que les nouvelles routes de la soie, et qui permettent ainsi de contourner et de saper les positions officielles prises par le gouvernement du pays concerné; demande aux institutions culturelles, universitaires et non gouvernementales de faire montre de plus de transparence en ce qui concerne l'influence de la Chine et les invite à rendre publics tous les échanges et engagements avec le gouvernement chinois et les organisations connexes;
126. condamne la décision prise par le gouvernement hongrois d'ouvrir une antenne de l'université chinoise Fudan et, dans le même temps, de fermer l'université d'Europe centrale à Budapest; s'inquiète de la dépendance financière croissante des universités européennes à l'égard de la Chine et d'autres États étrangers, compte tenu du risque de voir des données, des technologies et des résultats de recherche sensibles passer dans des États étrangers, ainsi que des répercussions possibles de cette dépendance sur la liberté académique; insiste sur l'importance de la liberté académique pour lutter contre la désinformation et les opérations d'influence; encourage ces institutions à procéder à des évaluations détaillées de la vulnérabilité avant de conclure de nouveaux partenariats avec des partenaires étrangers; souligne que le personnel universitaire devrait être formé pour signaler tout financement ou influence dissimulés par l'intermédiaire d'une ligne téléphonique spéciale, et que les auteurs des signalements devraient toujours bénéficier de la protection des lanceurs d'alerte; demande à la Commission et aux États membres de veiller à ce que les financements de recherches d'intérêt géopolitique menées dans les universités européennes proviennent de sources européennes; engage la Commission à proposer une législation visant à accroître la transparence du financement étranger des universités, des ONG et des groupes de réflexion, par exemple au moyen de déclarations obligatoires de dons, d'un devoir de vigilance de ces entités à l'égard de leurs sources de financement, et de la divulgation des financements, des contributions en nature et des subventions d'intervenants étrangers; exhorte les autorités des États membres à adopter des règles efficaces sur le financement étranger des établissements d'enseignement supérieur, y compris des plafonds stricts et des exigences en matière de déclaration;
127. souligne que des risques similaires en matière de sécurité et de vol de propriété intellectuelle existent dans le secteur privé, lorsque des salariés peuvent avoir accès à des technologies clés et à des secrets d'affaires; invite la Commission et les États

²⁴ <https://www.chateaunantes.fr/expositions/fils-du-ciel-et-des-steppes/>

membres à encourager tant les établissements universitaires que le secteur privé à mettre en place des programmes complets de sécurité et de conformité, notamment des contrôles de sécurité spécifiques dans le cadre des nouveaux contrats; relève que des restrictions accrues en matière d'accès aux systèmes et aux réseaux ainsi que d'habilitation de sécurité peuvent être justifiées pour certains enseignants ou salariés travaillant sur des recherches et des produits critiques;

128. fait observer que la directive «carte bleue» révisée²⁵, qui facilite l'entrée dans l'Union des migrants qualifiés de pays tiers, permet par exemple aux entreprises chinoises et russes établies en Europe de faire venir des migrants qualifiés provenant de leurs pays respectifs; estime que cette situation pourrait rendre plus difficile le contrôle par les États membres de l'afflux de tels citoyens, et entraîner ainsi des risques d'ingérence étrangère;
129. prend acte du nombre croissant d'instituts Confucius établis dans le monde, et en particulier en Europe; fait observer que le Centre pour l'enseignement et la coopération linguistiques, anciennement connu sous le nom de siège des instituts Confucius ou Hanban (Bureau du Conseil international de la langue chinoise), qui est responsable du programme des instituts Confucius dans le monde entier, est une composante du système de propagande du parti-État chinois; invite les États membres et la Commission à apporter leur soutien aux cours de langue chinoise indépendants, sans implication de l'État chinois ou d'organisations connexes; estime que le Centre national de la Chine récemment créé en Suède pourrait être un bon exemple de la manière d'accroître les compétences sur la Chine en toute indépendance en Europe;
130. considère, en outre, que les instituts Confucius servent de plateforme de lobbying pour les intérêts économiques chinois ainsi que pour le service de renseignement chinois et le recrutement d'agents et d'espions; rappelle que de nombreuses universités ont décidé de mettre fin à leur coopération avec les instituts Confucius en raison des risques d'espionnage et d'ingérence chinois, à l'image des universités de Düsseldorf en 2016, de Bruxelles (VUB et ULB) en 2019, de Hambourg en 2020, et de toutes les universités de Suède; demande que d'autres universités réfléchissent à leur coopération actuelle afin de s'assurer qu'elle n'a pas d'incidence sur leur liberté académique; engage les États membres à suivre de près l'enseignement, la recherche et les autres activités au sein des instituts Confucius et, lorsque les allégations d'espionnage ou d'ingérence sont étayées par des preuves manifestes, à prendre des mesures coercitives pour préserver la souveraineté économique et politique de l'Europe, y compris en refusant de financer les instituts associés ou en leur retirant leur licence;
131. fait observer que l'ingérence étrangère peut également se faire par une influence dans les instituts religieux et l'instrumentalisation de ces derniers, à l'image de l'influence russe dans les églises orthodoxes, en particulier en Serbie, au Monténégro, en Bosnie-Herzégovine, notamment dans sa République serbe, en Géorgie et, dans une certaine mesure, en Ukraine, qui a pour buts de semer la division parmi les populations locales, de réécrire l'histoire de façon biaisée et de promouvoir des mesures anti-Union, ainsi

²⁵ Directive (UE) 2021/1883 du Parlement européen et du Conseil du 20 octobre 2021 établissant les conditions d'entrée et de séjour des ressortissants de pays tiers aux fins d'un emploi hautement qualifié, et abrogeant la directive 2009/50/CE du Conseil, JO L 382 du 28.10.2021, p. 1.

que de l'influence du gouvernement turc, par l'intermédiaire de mosquées en France et en Allemagne, et de l'influence saoudienne exercée par le truchement de mosquées salafistes dans toute l'Europe, qui promeuvent un islam radical; invite la Commission et les États membres à assurer une meilleure coordination en matière de protection des instituts religieux contre les ingérences étrangères ainsi qu'à plafonner les financements et à en accroître la transparence; engage les États membres à suivre de près les activités des instituts religieux et, le cas échéant et sur la base d'éléments probants, à prendre des mesures, notamment en refusant de financer les instituts concernés ou en révoquant leur licence;

132. demande au SEAE de produire une étude sur la prévalence et l'influence des acteurs étatiques malveillants dans les groupes de réflexion, les universités, les organisations religieuses et les institutions médiatiques européens; invite toutes les institutions et tous les États membres de l'Union à collaborer et à engager un dialogue systématique avec les parties prenantes et les experts afin de recenser précisément et de surveiller l'influence étrangère dans les sphères culturelle, universitaire et religieuse; réclame un meilleur partage des contenus entre les radiodiffuseurs nationaux européens, ainsi que ceux des pays voisins;
133. est préoccupé par les signalements d'ingérence étrangère dans les systèmes judiciaires européens; attire particulièrement l'attention sur l'exécution de jugements russes par des tribunaux européens contre des opposants au Kremlin; invite les États membres à sensibiliser le personnel judiciaire et à collaborer avec la société civile afin d'éviter que des gouvernements étrangers n'exploitent avec malveillance la coopération judiciaire internationale ainsi que les juridictions européennes; demande au SEAE de commander une étude sur la prévalence et l'influence des ingérences étrangères dans les procédures judiciaires européennes; souligne que, sur la base de cette étude, il pourrait être nécessaire de proposer des modifications en ce qui concerne les exigences de transparence et de financement dans le contexte des procédures judiciaires;

Dissuasion, imputation de responsabilité et contre-mesures collectives, dont les sanctions

134. considère que les régimes de sanctions récemment mis en place par l'Union, tels que les mesures restrictives contre les cyberattaques qui menacent l'Union et ses États membres²⁶ et le régime mondial de sanctions de l'Union en matière de droits de l'homme²⁷ (loi Magnitsky de l'Union), adoptés respectivement le 17 mai 2019 et le 7 décembre 2020, ont démontré leur valeur ajoutée en dotant l'Union d'outils de dissuasion précieux; invite la Commission à présenter une proposition législative visant à adopter un nouveau régime de sanctions thématiques pour lutter contre les actes graves de corruption; rappelle que les régimes de sanctions en matière de cyberattaques et de droits de l'homme ont été utilisés à deux reprises, respectivement en 2020 et en 2021; demande instamment que le régime de sanctions applicable aux cyberattaques devienne permanent et invite les États membres à partager sans réserve les éléments probants et les renseignements dont ils disposent afin d'alimenter les listes de sanctions applicables aux attaques informatiques;

²⁶ <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L:2019:129I:TOC>

²⁷ <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L:2020:410I:TOC>

135. demande à l'Union et à ses États membres de prendre de nouvelles mesures contre l'ingérence étrangère, en particulier quand elle prend la forme de campagnes de désinformation à grande échelle, de menaces hybrides et de guerres hybrides, dans le strict respect des libertés d'expression et d'information, notamment en mettant en place un régime de sanctions; estime que cela devrait comprendre la mise en place d'un cadre de sanctions intersectoriel et asymétrique, ainsi que des sanctions diplomatiques, des interdictions de voyager, un gel des avoirs et le retrait des titres de séjour de l'Union des étrangers et des membres de leur famille liés à des tentatives d'ingérence étrangère, qui devrait cibler aussi précisément que possible les décideurs et les organes responsables d'actions agressives, en évitant une logique de représailles, au titre de l'article 29 du traité UE et de l'article 215 du traité sur le fonctionnement de l'Union européenne (traité FUE) (mesures restrictives), et que ce cadre devrait être pleinement intégré à la politique étrangère et de sécurité commune (PESC) de l'Union et aux piliers de la PSDC; engage les États membres à faire de l'ingérence et de la désinformation étrangères et nationales un point fixe de l'ordre du jour du Conseil des affaires étrangères; demande à l'Union de définir ce qu'est un acte internationalement illicite et d'adopter des seuils minimaux pour le déclenchement de contre-mesures à la suite de cette nouvelle définition, qui devrait être accompagnée d'une analyse d'impact à des fins de sécurité juridique; souligne que le Conseil devrait pouvoir décider par un vote à la majorité, plutôt qu'à l'unanimité, des sanctions liées à l'ingérence étrangère; estime que les pays qui se livrent à la manipulation de l'information et à l'ingérence étrangères dans le but de déstabiliser l'Union devraient payer le prix de leurs décisions et en supporter les conséquences économiques et/ou en termes de réputation et/ou de diplomatie; invite la Commission et le vice-président de la Commission/haut représentant de l'Union pour les affaires étrangères et la politique de sécurité à présenter des propositions concrètes à cet égard;
136. insiste sur le fait que, tout en visant à préserver les processus démocratiques, les droits de l'homme et les libertés tels que définis dans les traités, tout régime de sanctions doit accorder une attention particulière à l'incidence des sanctions imposées sur les droits et libertés fondamentaux, afin de faire respecter la charte des droits fondamentaux, et doit être transparent quant aux motifs sur lesquels se fonde la décision d'appliquer des sanctions; insiste sur la nécessité d'une plus grande clarté au niveau de l'Union en ce qui concerne la portée et l'incidence des sanctions sur les personnes concernées, notamment sur les ressortissants et les entreprises de l'Union;
137. considère que, si la nature de ces attaques hybrides varie, le danger qu'elles représentent pour les valeurs, les intérêts fondamentaux, la sécurité, l'indépendance et l'intégrité de l'Union européenne et de ses États membres, ainsi que pour la consolidation et le soutien de la démocratie, de l'état de droit, des droits de l'homme, des principes du droit international et des libertés fondamentales, peut être considérable en raison de l'ampleur des attaques, de leur nature ou de leur effet cumulatif; se félicite que le plan d'action pour la démocratie européenne prévoit que la Commission et le SEAE élaborent ensemble une boîte à outils pour les opérations d'ingérence et d'influence étrangères, notamment pour contrer les opérations hybrides et pour incriminer clairement les parties et pays tiers qui se livrent à des actes malveillants contre l'Union;
138. souligne que l'idée que certaines actions d'ingérence étrangère entravent gravement les processus démocratiques et influencent l'exercice de droits ou de devoirs gage du

terrain au niveau international; met en exergue, à cet égard, les amendements adoptés en 2018 concernant la loi australienne de modification de la législation sur la sécurité nationale (espionnage et ingérence étrangère), qui vise à criminaliser les activités secrètes et trompeuses des acteurs étrangers ayant l'intention d'interférer avec les processus politiques ou gouvernementaux, d'avoir une incidence sur les droits ou les devoirs, ou de soutenir les activités de renseignement d'un gouvernement étranger, en créant de nouvelles infractions telles que «l'ingérence étrangère intentionnelle»;

139. est conscient que, conformément à l'article 21, paragraphe 3, du traité UE, l'Union doit veiller à la cohérence entre les différents domaines de son action extérieure et entre ceux-ci et ses autres politiques, telles que définies dans les traités; souligne, à cet égard, que l'ingérence étrangère, telle que la menace que représentent les combattants et les groupes terroristes étrangers qui influencent les individus restant dans l'Union, a également été abordée par la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme²⁸;
140. souligne que, pour que leurs effets soient renforcés, les sanctions devraient être imposées collectivement, sur la base, si possible, d'une coordination avec des partenaires partageant les mêmes valeurs, éventuellement avec la participation d'organisations internationales, et être formalisées dans un accord international, compte devant être tenu également d'autres types de réactions aux agressions; relève que les pays candidats et candidats potentiels devraient aussi adopter ces sanctions afin de s'aligner sur la PESC de l'Union; souligne l'importance du travail accompli par l'OTAN dans le domaine des menaces hybrides et rappelle à cet égard le communiqué de la réunion de l'OTAN du 14 juin 2021, dans lequel il a été réaffirmé qu'il reviendrait au Conseil de l'Atlantique Nord de décider, au cas par cas, des circonstances d'une invocation de l'article 5 du traité de l'OTAN à la suite d'une cyberattaque, et que, dans certaines circonstances, les incidences d'actes de cybermalveillance majeurs aux effets cumulés sont telles que ces actes peuvent être considérés comme équivalant à une attaque armée²⁹; souligne que l'Union et l'OTAN devraient adopter une démarche plus prospective et stratégique à l'égard des menaces hybrides, axée sur les motivations et les objectifs des adversaires, et préciser dans quels cas l'Union est mieux équipée pour faire face à une menace, ainsi que les avantages comparatifs de leurs capacités; rappelle que plusieurs États membres de l'Union ne sont pas membres de l'OTAN, mais qu'ils coopèrent avec cette dernière, par exemple dans le cadre de son programme de Partenariat pour la paix (PPP) et de son Initiative pour l'interopérabilité avec les partenaires (PII), et souligne par conséquent que toute coopération entre l'Union et l'OTAN doit être sans préjudice de la politique de sécurité et de défense des États membres de l'Union ne faisant pas partie de l'OTAN, y compris ceux qui ont adopté une politique de neutralité; insiste sur l'importance de l'assistance mutuelle et de la solidarité, conformément à l'article 42, paragraphe 7, du traité UE et à l'article 222 du traité FUE, et demande à l'Union d'élaborer des scénarios concrets pour l'activation de ces articles en cas d'une éventuelle cyberattaque; engage l'Union et tous les États membres à relier cette question à d'autres aspects de leurs relations avec les États à

²⁸ JO L 88 du 31.3.2017, p. 6.

²⁹ https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=fr

l'origine de campagnes d'ingérence et de désinformation, en particulier la Russie et la Chine;

Coopération mondiale et multilatéralisme

141. fait observer que de nombreux pays démocratiques dans le monde entier sont confrontés à des opérations de déstabilisation similaires menées par des acteurs étrangers étatiques et non étatiques;
142. insiste sur la nécessité d'une coopération mondiale multilatérale au sein des enceintes internationales concernées entre pays partageant les mêmes valeurs sur ces questions d'importance cruciale, sous la forme d'un partenariat fondé sur une conception commune et des définitions partagées, en vue d'établir des normes et des principes internationaux; met en avant l'importance d'une coopération étroite avec les États-Unis et d'autres États partageant les mêmes valeurs aux fins de la modernisation des organisations multilatérales; se félicite, à cet égard, du sommet pour la démocratie et espère qu'il débouchera sur des propositions et des actions concrètes pour contrer, par une action collective, les plus grands périls auxquels les démocraties sont aujourd'hui confrontées;
143. estime que, sur la base d'une compréhension commune de la situation, les partenaires partageant les mêmes valeurs devraient échanger les meilleures pratiques et élaborer des réponses communes aux problèmes mondiaux et aux enjeux nationaux partagés, lesquelles réponses devraient englober des sanctions collectives ainsi que la protection des droits de l'homme et des normes démocratiques; invite l'Union à mener le débat sur les implications juridiques de l'ingérence étrangère, à promouvoir des définitions et des règles d'imputation communes au niveau international et à élaborer un cadre international pour les réponses aux ingérences dans les élections afin d'établir un code mondial de bonnes pratiques pour des processus démocratiques libres et résilients;
144. demande à l'Union et à ses États membres de réfléchir aux bons formats internationaux qui permettraient un tel partenariat et une telle coopération entre des partenaires partageant les mêmes valeurs; invite l'Union et ses États membres à engager un processus au niveau des Nations unies en vue d'adopter une convention mondiale visant à promouvoir et à défendre la démocratie qui donne une définition commune de l'ingérence étrangère; engage l'Union à proposer une boîte à outils mondiale pour la défense de la démocratie, à inclure dans la convention, comprenant des actions communes et des sanctions pour lutter contre les ingérences étrangères;
145. se félicite de la déclaration de l'OTAN du 14 juin 2021, qui met en lumière le problème toujours plus grave que représentent les menaces cybernétiques, hybrides et autres menaces asymétriques, y compris les campagnes de désinformation, et l'utilisation malveillante de technologies émergentes et perturbatrices de plus en plus sophistiquées; salue les progrès réalisés en matière de coopération entre l'Union et l'OTAN dans le domaine de la cyberdéfense; se félicite de la création par la Lituanie du centre régional de cyberdéfense associant les États-Unis et les pays du partenariat oriental; est favorable à une coopération plus étroite avec les pays partenaires dans le domaine de la cyberdéfense, sur les plans du partage d'informations et du travail opérationnel; se félicite des discussions entre les États-Unis et l'Union sur les contrôles multilatéraux

des exportations de biens de cybersurveillance dans le cadre du Conseil du commerce et des technologies;

146. salue les initiatives déjà prises, notamment au niveau administratif, pour partager en temps réel les connaissances sur l'état des attaques hybrides, y compris les opérations de désinformation, telles que le système d'alerte rapide établi par le SEAE, partiellement ouvert aux pays tiers partageant les mêmes valeurs, le mécanisme de réaction rapide mis en place par le G7 et la Division civilo-militaire Renseignement et sécurité de l'OTAN;
147. souligne que la coopération mondiale devrait se fonder sur des valeurs communes exprimées dans des projets communs, que des organisations internationales telles que l'OSCE et l'UNESCO devraient y être associées et qu'elle devrait contribuer à renforcer les capacités démocratiques et à instaurer une paix et une sécurité durables dans les pays confrontés à des menaces similaires d'ingérence étrangère; invite l'Union à créer un Fonds européen pour les médias démocratiques en vue de soutenir le journalisme indépendant dans les éventuels pays de l'élargissement et les pays du voisinage européen ainsi que dans les pays candidats et candidats potentiels; insiste sur les besoins pratiques, tels que l'obtention de moyens techniques professionnels, qui sont régulièrement exprimés par les journalistes indépendants des pays voisins;
148. souligne qu'il est urgent de lutter contre la mésinformation et la désinformation en matière de climat; salue les initiatives prises lors de la COP26 en vue d'adopter une définition universelle de la mésinformation et de la désinformation en matière de climat, ainsi que de déterminer les mesures à mettre en place pour régler ce problème; demande que l'on s'inspire de modèles tels que le groupe d'experts intergouvernemental sur l'évolution du climat afin d'élaborer un code de conduite mondial sur la désinformation, processus qui servirait de base à un accord de Paris sur la désinformation;
149. souligne qu'il importe d'offrir des perspectives claires aux pays candidats et candidats potentiels et d'épauler les pays partenaires et les pays voisins, notamment dans les Balkans occidentaux et dans les voisinages orientaux et méridionaux de l'Union, étant donné que des pays tels que la Russie, la Turquie et la Chine tentent de faire de ces pays des laboratoires de manipulation de l'information et de guerre hybride, avec pour objectif de nuire à l'Union; considère les États-Unis comme un partenaire majeur dans la lutte contre les ingérences étrangères, les campagnes de désinformation et les menaces hybrides dans ces régions; s'inquiète en particulier du rôle joué par la Serbie et la Hongrie dans la diffusion généralisée de la désinformation dans les pays voisins; souligne que l'Union devrait soutenir ces pays et dialoguer avec eux, comme le prévoit le règlement IVDCI³⁰; estime que les actions entreprises peuvent être la promotion de la valeur ajoutée et de l'impact positif de l'Union dans la région, le financement de projets visant à garantir la liberté des médias, le renforcement de la société civile et de l'état de droit, ainsi que l'approfondissement de la coopération en matière d'éducation

³⁰ Règlement (UE) 2021/947 du Parlement européen et du Conseil du 9 juin 2021 établissant l'instrument de voisinage, de coopération au développement et de coopération internationale – Europe dans le monde, modifiant et abrogeant la décision n° 466/2014/UE du Parlement européen et du Conseil et abrogeant le règlement (UE) 2017/1601 du Parlement européen et du Conseil et le règlement (CE, Euratom) n° 480/2009 du Conseil, JO L 209 du 14.6.2021, p. 1.

aux médias, au numérique et à l'information, dans le respect de la souveraineté de ces pays; demande un renforcement des capacités du SEAE à cet égard;

150. encourage l'Union et ses États membres à approfondir leur coopération avec Taïwan pour contrer les opérations d'ingérence et les campagnes de désinformation émanant de pays tiers malveillants, notamment en partageant les bonnes pratiques et en adoptant des stratégies communes visant à favoriser la liberté des médias et le journalisme, à renforcer la coopération sur la cybersécurité et les cybermenaces, à sensibiliser davantage les citoyens et à améliorer la culture numérique globale de la population afin d'accroître la résilience de nos systèmes démocratiques; est favorable à l'intensification de la coopération entre les organismes publics, les ONG et les groupes de réflexion européens et taïwanais concernés dans ce domaine;
 151. invite le Parlement à promouvoir activement le discours de l'Union, à jouer un rôle de premier plan dans la promotion de l'échange d'informations et à discuter des meilleures pratiques avec les parlements partenaires du monde entier, en utilisant son vaste réseau de délégations interparlementaires, ainsi que les initiatives et les activités de soutien à la démocratie coordonnées par son groupe de soutien à la démocratie et de coordination des élections; met en exergue l'importance que revêt une coopération étroite avec les parlementaires des pays tiers dans le cadre de projets sur mesure soutenant la perspective européenne des pays candidats et candidats potentiels;
 152. demande au SEAE de renforcer le rôle des délégations de l'Union et des missions de la PSDC de l'Union dans les pays tiers afin d'accroître leur capacité à détecter et à neutraliser les campagnes de désinformation orchestrées par des acteurs étatiques étrangers, et de financer des projets éducatifs appuyant les valeurs démocratiques et les droits fondamentaux; recommande vivement la création d'une plateforme de communication stratégique, lancée par le SEAE, afin de mettre en place une coopération structurelle en matière de lutte contre la désinformation et l'ingérence étrangère, qui devrait être basée à Taipei; invite en outre les délégations de l'Union à contribuer à la lutte de l'Union contre la désinformation en traduisant les décisions pertinentes de l'Union, telles que les résolutions d'urgence du Parlement, dans la langue de leur pays d'affectation;
 153. demande que la question de l'ingérence étrangère malveillante soit abordée dans le cadre de la future boussole stratégique de l'Union;
 154. appelle de ses vœux la création d'un dispositif institutionnel permanent au sein du Parlement européen consacré au suivi de ces recommandations, afin de contrer la désinformation et l'ingérence étrangères dans l'Union de façon systématique, au-delà du mandat actuel de la commission spéciale INGE; réclame un meilleur échange institutionnalisé entre la Commission, le SEAE et le Parlement par l'intermédiaire de ce dispositif;
-
- ◦
155. charge sa Présidente de transmettre la présente résolution au Conseil, à la Commission, au vice-président de la Commission et haut représentant 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

Contexte

Lorsque le Parlement européen a décidé, le 18 juin 2020, de créer une commission spéciale sur l'ingérence étrangère, y compris la désinformation, il lui a confié le mandat d'établir une approche à long terme pour traiter les preuves d'ingérence étrangère dans les institutions et processus démocratiques de l'Union et de ses États membres.

Un an après la réunion constitutive de la commission, le 23 septembre 2020, et sur la base d'une longue série de témoignages de divers experts et praticiens, la rapporteure peut d'ores et déjà exposer la réalité, l'étendue du champ d'action et le caractère très sophistiqué des innombrables formes que prennent les opérations d'ingérence agressives décidées et financées par des acteurs étrangers contre l'Union; la rapporteure souligne également, avec inquiétude, la rapidité de l'adaptation, la volatilité et l'accélération de ce phénomène – à travers de nouveaux acteurs, de nouveaux récits, de nouveaux outils en l'espace d'un an seulement.

Des nouvelles campagnes de désinformation à grande échelle liées à la COVID-19 aux cyberattaques contre les entités des pouvoirs publics, y compris les infrastructures de santé publique, des stratégies d'ingérence intégrant l'appropriation des ressources par les élites et le lobbying industriel au financement dissimulé des activités politiques, du contrôle des centres universitaires et culturels à l'instrumentalisation des diasporas nationales, notre commission a analysé la dimension multidimensionnelle et dynamique de ce nouveau type de guerre dont l'objectif est de saper la cohésion sociale et la confiance mutuelle de nos sociétés démocratiques européennes afin de les affaiblir.

Heureusement, la commission a également assisté à une prise de conscience de ces questions cruciales, y compris la compréhension généralement partagée selon laquelle l'Union et ses États membres devraient rapidement être dotés de politiques de résilience et d'outils de dissuasion à part entière, basés sur une approche de la société dans son ensemble, leur permettant de faire face à tous les types de menaces et d'attaques hybrides et, par conséquent, de protéger le fonctionnement durable de la démocratie.

Renforcement de la résilience par la connaissance de la situation, l'éducation et la formation aux médias et à l'information, le pluralisme des médias, le journalisme indépendant et l'éducation

Il est évident que la première condition d'une défense solide contre les ingérences étrangères est la connaissance de la situation. Pour y parvenir, nous devons suivre deux étapes importantes: tout d'abord, nous devons surveiller, cartographier et analyser les différentes attaques d'ingérence afin de bien comprendre la menace; deuxièmement, nous devons nous assurer que toutes les personnes qui doivent savoir soient au courant de cette analyse.

De nombreux chercheurs, organisations de la société civile, journalistes et membres du personnel des institutions nationales ou européennes font un excellent travail d'enquête concernant cette menace. Nous avons rencontré nombre d'entre eux au sein de la commission INGE. Au niveau européen, la rapporteure apprécie particulièrement le travail des groupes de travail StratCom du SEAE. Toutefois, nous devons développer davantage ce point. Nous ne

pouvons pas accepter qu'il n'y ait toujours pas de groupe de travail chargé de surveiller les ingérences émanant de la Chine.

Nous devons également veiller à ce que les connaissances acquises soient diffusées auprès d'un public plus large. Tant les formations ciblées pour les personnes qui remplissent des fonctions sensibles à l'ingérence étrangère que les campagnes de sensibilisation générales sont importantes. Dans ce contexte, l'éducation aux médias et à la culture numérique est essentielle pour permettre aux citoyens de mieux interpréter et évaluer les informations qu'ils rencontrent.

Les journalistes ont un rôle crucial à jouer pour garantir un climat de débat constructif. Malheureusement, ils ont subi les conséquences financières de la numérisation, en particulier le fait que les mécanismes publicitaires tendent à privilégier les contenus émotionnels, dont les opinions et la désinformation, au détriment du journalisme de qualité. Les journalistes indépendants sont aussi souvent victimes de harcèlement et de menaces organisées lorsqu'ils couvrent des sujets sensibles. S'il est important de défendre l'indépendance des médias de qualité, il est également essentiel d'étudier les moyens de soutenir les organes d'information et les journalistes, tant financièrement que contre le harcèlement.

Ingérence étrangère qui tire parti des plateformes en ligne

Il est clair que le système actuel de diffusion des informations au moyen de plateformes conduit à un climat en ligne déformé dans lequel la désinformation et d'autres types de manipulation de l'information prospèrent. Les rapports sur les fuites et la vente de données sensibles, les algorithmes favorisant les contenus menant à la radicalisation et les plateformes fermant les yeux sur des violations manifestes de la loi ou de leurs propres conditions générales sont si courants que nous nous y habituons presque et cessons de nous en émouvoir. Nous devons arrêter cela.

De nombreuses discussions avec des experts m'ont convaincue que la méthode actuelle d'autorégulation ne fonctionne pas et doit être remplacée par des règles contraignantes. Nous ne pouvons pas accepter que des acteurs étrangers puissent librement manipuler le contenu que nous recevons en ligne par l'intermédiaire des plateformes ou utiliser de manière abusive les systèmes de publicité afin que des annonceurs contribuent involontairement à les financer. Nous ne pouvons pas non plus accepter que les plateformes soient autorisées à ne rien faire sans en subir les conséquences.

Certes, de nombreuses améliorations ont été apportées, tant à l'initiative des plateformes elles-mêmes qu'à celle des mesures publiques comme le code de bonnes pratiques. Cependant, sans une véritable transparence, il est impossible de se faire une idée des répercussions de ces actions. Il est également essentiel que le code de bonnes pratiques, qui est volontaire par nature, dispose d'un mécanisme d'application efficace et soit complété par une législation forte. En outre, il est frappant de constater combien de politiques anti-ingérence ne sont utilisées que pour les contenus en langue anglaise ou dans un nombre très limité de langues. Nous ne pouvons pas accepter une situation où les Lettons, les Bulgares, les Grecs ou même les francophones ou les germanophones bénéficient d'une protection bien moindre contre la manipulation en ligne que les anglophones, simplement parce que les plateformes donnent la priorité aux contenus en anglais.

Infrastructures critiques et secteurs stratégiques

Les infrastructures critiques sont essentielles au fonctionnement de l'économie et de la société. Pour mieux protéger les secteurs critiques, des efforts coordonnés et conjoints sont nécessaires dans tous les secteurs et à différents niveaux: Union européenne, national, régional et local. La nouvelle directive de la Commission visant à renforcer la résilience des entités critiques constitue un point de départ important. Toutefois, la rapporteure estime que la liste des infrastructures critiques devrait être élargie aux médias ainsi qu'aux infrastructures électorales, étant donné leur importance cruciale respective pour garantir le fonctionnement de l'Union européenne et de ses États membres, et qu'une certaine flexibilité devrait être autorisée pour l'ajout de nouveaux secteurs stratégiques à l'avenir. Il est de la plus haute importance que la directive maintienne une approche hautement adaptable permettant des mises à jour et des modifications rapides.

En outre, la dépendance des investissements étrangers et des fournisseurs de technologie étrangers dans le domaine des infrastructures critiques crée de nombreuses menaces pour l'autonomie de fonctionnement de ces dernières. L'effort de l'Union européenne en faveur de l'autonomie stratégique et de la souveraineté numérique est donc essentiel pour lutter contre ces menaces.

Financement dissimulé des activités politiques provenant d'acteurs et de donateurs étrangers

Des preuves solides montrent que des acteurs étrangers ont activement interféré dans les élections démocratiques et les référendums des pays européens, au moyen d'opérations de financement secrètes pendant les campagnes.

Ces opérations malveillantes mettent en péril l'intégrité des élections organisées dans l'Union européenne, car elles entraînent une concurrence déloyale entre les partis et les candidats en allouant à certains partis – généralement les partis anti-Union européenne – des moyens supplémentaires qui ne sont pas comptabilisés dans les déclarations officielles de campagne électorale.

Selon le rapport 2020 de l'Alliance for Securing Democracy (Alliance pour la sécurité de la démocratie) portant sur les fonds occultes en provenance de l'étranger¹, plus de 300 millions de dollars ont déjà été déversés dans 33 pays au cours de la dernière décennie par la Russie, la Chine et d'autres régimes autoritaires pour s'ingérer dans les processus démocratiques à plus de 100 reprises, et la moitié de ces cas concernent des actions de la Russie en Europe.

Certaines de ces opérations ne sont même pas illégales: elles profitent des nombreuses failles existant entre les États membres dont les dispositions de lois électorales nationales relatives au financement des activités politiques ne sont pas harmonisées au niveau de l'Union européenne.

Cybersécurité et résilience face aux cyberattaques

La numérisation croissante des services a entraîné une dépendance accrue des infrastructures critiques envers les systèmes en ligne, augmentant ainsi la vulnérabilité aux cyberattaques et à l'exposition des données. Le nombre de cyberattaques a augmenté ces dernières années,

¹ <https://securingdemocracy.gmfus.org/covert-foreign-money/>

ciblant des secteurs stratégiques tels que l'Agence européenne des médicaments (EMA) et le Parlement norvégien.

La fragmentation des capacités et des moyens, ainsi que la faiblesse des ressources humaines et financières, montrent la vulnérabilité de l'Union européenne aux cyberattaques. Les cyberattaques ne s'arrêtent pas aux frontières. Il est donc impératif que l'Union investisse rapidement dans ses capacités et ses compétences numériques stratégiques – en allouant des ressources supplémentaires, tant humaines que financières, à la cybersécurité – tout en veillant à ce qu'un même niveau élevé de cybersécurité soit atteint dans tous les États membres. La stratégie de cybersécurité de l'Union européenne pour 2020 et la directive NIS2 sont des propositions importantes pour améliorer la cybersécurité de l'Union européenne, qui sera renforcée à l'avenir par la loi sur la cyberrésilience et la politique de cyberdéfense.

En ce qui concerne les logiciels d'espionnage, tels que Pegasus, le problème doit être rapidement résolu en renforçant le cadre législatif afin que les distributeurs, les utilisateurs et les contrevenants de ces logiciels soient tenus responsables.

Protection des États membres, des institutions, des agences, des délégations et des missions de l'Union européenne

La cybersécurité doit être améliorée non seulement entre les États membres, mais aussi entre les institutions de l'Union européenne. Les récentes cyberattaques visant les institutions de l'Union européenne ont démontré la nécessité d'une forte coopération interinstitutionnelle en matière de détection, de surveillance et de partage d'informations pendant et/ou pour prévenir les cyberattaques. Les institutions européennes ont déjà pris des mesures pour renforcer leur cybersécurité et disposent d'outils pour coordonner et détecter les cyberattaques, tels que le CERT-UE, l'ENISA et la future unité cybernétique commune.

Cependant, il faut en faire davantage. Premièrement, il convient d'augmenter les ressources humaines et financières afin de répondre aux défis d'un paysage de menaces en constante évolution. Deuxièmement, les institutions de l'Union européenne devraient procéder à un audit approfondi de leurs services et réseaux, afin d'atténuer les risques de sécurité et de s'assurer que leur sécurité ne dépend pas de technologies étrangères. Enfin, il y a lieu de sensibiliser, de former et d'orienter l'ensemble du personnel afin d'atténuer et de traiter les risques liés à la sécurité, qu'ils soient cybernétiques ou non.

Ingérence d'acteurs étrangers par l'appropriation des ressources par les élites, les diasporas nationales, les universités et les manifestations culturelles

Une autre série d'outils à la disposition des pays étrangers désireux de s'immiscer dans le fonctionnement de l'Union européenne est l'ingérence par des individus.

L'«appropriation des ressources par les élites» – ou cooptation – est malheureusement un phénomène très répandu, dont la forme la plus connue est l'embauche d'anciens acteurs politiques et fonctionnaires européens de haut niveau par des entreprises contrôlées par des États étrangers en échange des connaissances qu'ils ont acquises au cours de leurs mandats ou fonctions publics. Leurs connaissances, souvent fondées sur des informations et des contacts confidentiels, sont ensuite utilisées au détriment des intérêts stratégiques de l'Union européenne et de ses États membres. Ces opérations sont souvent associées à des stratégies de lobbying industriel, où les objectifs économiques et politiques sont fusionnés.

Une autre forme d'ingérence par des individus est l'influence croissante et, finalement, le contrôle exercé sur les universités, les écoles et les centres culturels et religieux par des agents d'États étrangers, dans des domaines pertinents pour ces pays étrangers. La manière dont les instituts Confucius – nouvellement rebaptisés «centres d'éducation et de coopération linguistiques» – cherchent à contrôler tout type de recherche, d'enseignement ou même d'exposition culturelle liée à la Chine dans nombre d'universités et de musées européens est un exemple révélateur de cette pratique. D'autres pays sont également très actifs dans ce domaine, comme la Russie à travers les églises orthodoxes.

Cette forme d'ingérence bénéficie largement des efforts visant à contrôler la diaspora nationale vivant au sein de l'Union européenne, qui représente un levier potentiel massif à travers les différentes couches des sociétés européennes. Ces efforts visent également à réduire au silence les opposants politiques vivant à l'étranger.

Dissuasion, imputations et contre-mesures collectives, dont les sanctions

L'Union européenne et ses États membres doivent mettre en place des outils de dissuasion crédibles. En effet, l'Union et ses États membres ne disposent actuellement d'aucun régime spécifique de sanctions liées à l'ingérence étrangère et aux campagnes de désinformation orchestrées par des acteurs étatiques étrangers.

La rapporteure est consciente des défis juridiques qui peuvent surgir lors de l'établissement d'un tel régime de sanctions, notamment la nécessité de définir précisément les éléments des infractions et leurs éventuels effets cumulatifs en conformité avec les lois internationales et de l'Union.

La rapporteure estime toutefois que l'Union européenne peut s'inspirer utilement des pratiques antérieures d'autres partenaires à cet égard, tels que l'Australie, qui a notamment défini ce qui constitue une «ingérence étrangère intentionnelle» et pénalisé les activités dissimulées et trompeuses des acteurs étrangers.

La rapporteure pense également que nous pouvons nous appuyer sur ce qui existe déjà au niveau de l'Union européenne, à savoir le régime de mesures restrictives contre les cyberattaques menaçant l'Union et ses États membres, qui a été utilisé deux fois l'année dernière.

Enfin et surtout, nous soulignons la nécessité de coopérer étroitement avec nos partenaires internationaux de même sensibilité sur tout régime de sanctions dans le but d'imposer des sanctions ensemble afin de renforcer l'efficacité et l'effet de dissuasion.

Les entités étrangères responsables d'opérations d'ingérence agressives à l'encontre de démocraties ne devraient plus s'imaginer que leurs campagnes de déstabilisation seront sans conséquence.

Coopération mondiale et multilatéralisme

L'Union est loin d'être le seul espace démocratique au monde à être confronté à des actes d'ingérence étrangère de plus en plus agressifs. De nombreux autres pays, qu'il s'agisse de pays développés ou en développement, sont également visés par de tels agissements de la part

de la Chine, de la Russie ou d'autres régimes autoritaires, qui poursuivent toujours les mêmes objectifs: saper le fonctionnement de la démocratie afin de gagner en influence.

Nous devons réunir des partenaires partageant les mêmes idées pour aborder ces questions de manière coordonnée, sur la base d'un partenariat de démocraties.

Premièrement, nous devons nous mettre d'accord sur des définitions communes et partager une même compréhension de ce qui est actuellement en jeu afin de convenir de normes et de standards internationaux.

Nous devons aborder les questions suivantes et y répondre de manière précise et collective: qu'est-ce qu'une ingérence étrangère agressive? Comment qualifier juridiquement les opérations de désinformation et de manipulation orchestrées depuis un pays étranger? Comment définir ces menaces et attaques comme des crimes? Quel régime de sanctions collectives pourrait-on mettre en place?

Ensuite, la coopération globale devrait être basée sur un échange de bonnes pratiques et la gestion de projets concrets. Grâce à son vaste réseau de forums interparlementaires, le Parlement européen aurait un rôle de premier plan à jouer à cet égard, de même que les délégations de l'Union dans les pays tiers.

Méthodes de travail

Quelles que soient nos opinions politiques sur les différents textes législatifs et nos couleurs sur l'échiquier politique, en tant que membres de la commission INGE, nous sommes unis dans l'idée que notre démocratie doit rester forte face aux tentatives d'ingérence étrangère. C'est la raison pour laquelle nous avons construit notre travail au sein de la commission sur une coopération approfondie entre les groupes politiques. Conjointement avec le président, les coordinateurs ont décidé des experts à inviter et des études à commander. En tant que rapporteure, j'ai régulièrement consulté les rapporteurs fictifs au cours de mon travail de rédaction.

Sur le plan thématique, nous pouvons distinguer une phase de diagnostic et une phase de recherche de solutions. Au cours de la première phase, nous avons invité des experts susceptibles de nous aider à comprendre toute la variété des menaces et des méthodes utilisées. Suivant notre mandat, nous avons tenu un certain nombre d'auditions sur l'ingérence dans la sphère publique et privée et sur l'étude des méthodes de différents acteurs étrangers. Dans la phase de recherche de solutions, la commission INGE s'est attachée à identifier les outils et stratégies possibles pour prévenir et contrer les problèmes identifiés.

La commission INGE a également commandé six études et a invité les auteurs à présenter leurs conclusions. La situation sanitaire liée à la pandémie de COVID-19 nous a empêchés d'organiser des missions au cours des deux premiers semestres d'existence de la commission INGE. Cependant, au moment où nous écrivons ces lignes, les membres de la commission INGE viennent de rentrer d'une première mission réussie à l'Agence de l'Union européenne pour la cybersécurité (ENISA) à Athènes, en Grèce. Trois autres missions sont prévues: à Taipei, à Paris et à Washington.

Pour mieux préparer nos recommandations, nous avons rédigé deux questions avec demande de réponses orales. En juillet 2021, nous avons demandé au VP/HR Josep Borrell comment il

comptait remédier au manque de ressources et de mandat des task forces Stratcom du SEAE et à l'absence de sanctions adéquates contre les acteurs étrangers qui se livrent à des ingérences. En octobre 2021, nous avons demandé à la vice-présidente de la Commission Věra Jourová comment elle comptait faire en sorte que le manque de coordination entre les secteurs et les niveaux politiques n'augmente pas l'exposition à l'ingérence étrangère et comment améliorer la transparence des algorithmes et soutenir l'éducation aux médias.

L'une de nos principales conclusions était l'importance de la coopération et du partage d'informations, tant au niveau mondial qu'entre les niveaux de gouvernance et les différents secteurs au sein de l'Union. Dès le début, nous avons donc invité à nos réunions d'autres commissions et délégations compétentes en matière d'ingérence étrangère. L'expertise de ces organes frères a enrichi les débats que nous avons eus avec eux et a permis que les idées tirées de nos auditions parviennent aux commissions ordinaires qui travaillent sur les propositions législatives correspondantes.

La réunion interparlementaire que nous accueillerons en novembre 2021 sera un événement clé. Cette rencontre entre les parlementaires des pays de l'Union et un groupe de partenaires mondiaux partageant les mêmes idées sélectionnés offrira une occasion cruciale de tirer les leçons des expériences des uns et des autres et de discuter des défis et solutions communs.

Pour élaborer ce rapport, la rapporteure a rédigé quatre documents de travail: sur la situation en matière d'ingérence étrangère dans l'Union européenne, y compris la désinformation, sur le financement dissimulé des activités politiques provenant de donateurs étrangers, sur l'ingérence étrangère qui tire parti des plateformes en ligne, et sur le renforcement de la résilience de l'Union face aux menaces hybrides.

Outre toutes les réunions formelles mentionnées ci-dessus, la rapporteure a recueilli des informations en participant à des réunions et à des conférences et en lisant des études et des articles de presse.

Coopération avec d'autres organes du Parlement européen et de l'UE

En raison de la nature intersectorielle de notre mandat, la commission INGE a invité cinq commissaires à discuter de différents aspects de l'ingérence étrangère:

- Věra Jourová, vice-présidente chargée des valeurs et de la transparence,
- Margaritis Schinas, vice-président chargé de la promotion de notre mode de vie européen,
- Josep Borrell, vice-président de la Commission européenne / haut représentant de l'Union pour les affaires étrangères et la politique de sécurité,
- Thierry Breton, commissaire chargé du marché intérieur, et
- Margrethe Vestager, vice-présidente exécutive pour une Europe adaptée à l'ère du numérique et à la concurrence.

Nous avons également mené plusieurs discussions avec les agents de la Commission et des services pour l'action extérieure et, en collaboration avec la commission CONT, une réunion

spéciale avec la Cour des comptes européenne au sujet de son rapport spécial n° 09/2021 intitulé «La désinformation concernant l'UE: un phénomène sous surveillance mais pas sous contrôle».

La commission spéciale INGE a également établi un plan de coopération avec plusieurs commissions du Parlement européen avec lesquelles elle partage certaines compétences. La commission INGE compte à ce jour onze commissions et onze délégations.

Expertise externe

La commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, a demandé une expertise externe sur les sujets suivants qui sont pertinents pour le travail en cours de la commission:

- désinformation – cartographie et solutions, y compris la réglementation des plateformes;
- financement – cartographie et solutions;
- infrastructures
- meilleures pratiques dans l'approche de l'ensemble de la société pour contrer les menaces hybrides;
- incidence des campagnes de désinformation sur les migrants, les LGBTI et les groupes minoritaires;
- leçons tirées des utilisations abusives commises par des régimes autoritaires.

Aperçu des auditions d'experts externes

Auditions thématiques

- **Menaces hybrides, désinformation et polarisation – aperçu institutionnel**, 24 septembre 2020
- **Ingérence électorale, financement des partis politiques et plateformes de médias sociaux – aperçu**, 2 octobre 2020
- **Comment l'ingérence étrangère sape la souveraineté: l'exemple de nos voisins de l'Est**, 21 octobre 2020
- **Ingérence étrangère dans la sphère publique: vérification des faits, plateformes de médias sociaux et leur utilisation dans la désinformation et l'ingérence étrangère et renforcement de la résilience**, 26 octobre 2020 et 9 novembre 2020
- **Ingérence étrangère dans la sphère politique: ingérence étrangère pendant les processus électoraux, y compris au moyen de cyberattaques, de fuites de données et de communication malveillante**, 12 novembre 2020

- **Ingérence étrangère dans la sphère politique: financements politiques provenant de formes légales ou non de sociétés-relais et de donateurs utilisant un prête-nom originaires de pays tiers**, 2 décembre 2020
- **Journalisme contre propagande**, 11 décembre 2020
- **Menaces possibles d'ingérence de pays tiers dans un contexte géopolitique**, 25 janvier 2021 et 1^{er} février 2021
- **Communication stratégique pour contrer l'ingérence étrangère**, 22 février 2021
- **Comment rendre le financement des partis politiques et des campagnes plus transparent: quelles règles l'Union européenne doit-elle adopter?**, 23 février 2021
- **Démocratie en ligne: quels sont les risques? Comment se protéger?**, 17 mars 2021
- **Ingérence étrangère en matière de financement des organisations anti-choix dans l'Union européenne**, 25 mars 2021
- **Évolutions technologiques et approches réglementaires face à la désinformation: ingérence par la publicité**, 13 avril 2021
- **Évolutions technologiques et approches réglementaires concernant la désinformation**, 15 avril 2021
- **Échange de vues avec Mikhail Khodorkovsky, fondateur du Dossier Center**, 10 mai 2021
- **Audition avec Facebook, Twitter et YouTube sur le rôle des plateformes de médias sociaux dans la diffusion et le développement de la désinformation, ainsi que dans la détection et la lutte contre celle-ci**, 10 mai 2021
- **Comment l'histoire, la culture et l'éducation peuvent contribuer à lutter contre la désinformation**, 15 juin 2021
- **Désinformation et discrimination**, 12 juillet 2021
- **Plan d'action pour la démocratie européenne, législation sur les services numériques et autres instruments de l'UE: les propositions visant à protéger les processus démocratiques de l'UE contre l'ingérence étrangère, ainsi que la voie à suivre**, 2 septembre 2021
- **Sanctions et contre-mesures collectives**, 2 septembre 2021

Échange de vues avec:

- **Le rôle de l'éducation, des médias et de la culture dans la lutte contre la désinformation et l'ingérence étrangère**, 9 septembre 2021
- **Ingérence étrangère et espionnage de personnalités politiques et d'institutions européennes**, 9 septembre 2021

- **Sécurité des institutions de l'UE: répondre à l'escalade des cyberattaques**, 9 septembre 2021
- **Domages économiques des ingérences et actions de désinformation étrangères, y compris sur le marché des données**, 14 octobre 2021

POSITION MINORITAIRE DE CLARE DALY, AU NOM DU GROUPE THE LEFT

L'ingérence étrangère a certes des répercussions sociales considérables et mérite une attention particulière, mais elle n'est ni inédite ni subie exclusivement par l'Europe. Parmi les formes d'ingérences dans les processus démocratiques dans l'Union européenne, la plus systématique et lourde de conséquences est celle de la concentration massive de capitaux, tant étrangers qu'européens, qui exercent une influence sur l'élaboration de la législation et la prise de décisions politiques.

Cet état de fait est à peine abordé par la majorité au sein de la commission spéciale INGE, qui préfère tenir un discours spécieux sur une Europe victime de la malveillance d'adversaires géopolitiques. L'enquête a été utilisée pour gonfler les menaces d'ingérence russe et chinoise, pour ignorer les principales causes de la crise de légitimité politique en Europe, pour stigmatiser les écarts par rapport à la politique étrangère officielle de l'Union et pour justifier par des motifs sécuritaires les limitations de la liberté d'expression et d'autres droits fondamentaux.

Le rapport qui en résulte manque d'équilibre et d'objectivité, au point de constituer en soi de la désinformation. La prédominance en son sein d'une «expertise» émanant de groupes de réflexion atlantistes et de l'OTAN, faisant du lobbying pour des groupes d'intérêts qui tirent profit du conflit, doit elle-même être considérée comme une forme d'ingérence étrangère. L'orientation politique que le présent rapport fait prendre à l'Union va nuire gravement et durablement au caractère démocratique des sociétés européennes. La postérité verra d'un mauvais œil ce document.

**INFORMATIONS SUR L'ADOPTION
PAR LA COMMISSION COMPÉTENTE AU FOND**

Date de l'adoption	25.1.2022
Résultat du vote final	+: 25 -: 8 0: 1
Membres présents au moment du vote final	Vladimír Bilčík, Andrea Bocskor, Ioan-Rareș Bogdan, Jorge Buxadé Villalba, Włodzimierz Cimoszewicz, Gwendoline Delbos-Corfield, Anna Júlia Donáth, Marco Dreosto, Nicolaus Fest, Sunčana Glavak, Raphaël Glucksmann, Markéta Gregorová, Bart Groothuis, Balázs Hidvéghi, Sandra Kalniete, Andrey Kovatchev, Jeroen Lenaers, Nathalie Loiseau, Juan Fernando López Aguilar, Morten Løkkegaard, Pierfrancesco Majorino, Lukas Mandl, Thierry Mariani, Dace Melbārde, Maite Pagazaurtundúa, Tonino Picula, Manu Pineda, Robert Roos, Andreas Schieder, Sabine Verheyen, Viola Von Cramon-Taubadel, Javier Zarzalejos
Suppléants présents au moment du vote final	Clare Daly, Petra Kammerevert

VOTE PAR APPEL NOMINAL

Vote final – Projet tel que modifié (vote par appel nominal)	+ 25/8/1
---	--------------------

RÉSULTATS DES VOTES PAR APPEL NOMINAL

Vote par appel nominal: vote final

25	+
ECR	Dace Melbārde
PPE	Vladimír Bilčík, Ioan-Rareș Bogdan, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Jeroen Lenaers, Lukas Mandl, Sabine Verheyen, Javier Zarzalejos
Renew	Anna Júlia Donáth, Bart Groothuis, Nathalie Loiseau, Morten Løkkegaard, Maite Pagazaurtundúa
S&D	Włodzimierz Cimoszewicz, Raphaël Glucksmann, Petra Kammerevert, Juan Fernando López Aguilar, Pierfrancesco Majorino, Tonino Picula, Andreas Schieder
Verts/ALE	Gwendoline Delbos-Corfield, Markéta Gregorová, Viola Von Cramon-Taubadel

8	-
ECR	Jorge Buxadé Villalba, Robert Roos
ID	Nicolaus Fest, Thierry Mariani
NI	Andrea Bocskor, Balázs Hidvéghi
The Left	Clare Daly, Manu Pineda

1	0
ID	Marco Dreosto