Parlement européen
2019-2024

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

2020/2268(INI)

18.10.2021

PROJET DE 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

Rapporteure: Sandra Kalniete

PR_INI

SOMMAIRE

Page

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 convention de sauvegarde des droits de l'homme et des libertés fondamentales, et notamment ses articles 8, 9, 10, 11, 13, 16 et 17, ainsi que son protocole, et notamment son article 3,

– vu les communications conjointes de la Commission et du haut représentant 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 plan d'action pour la démocratie européenne (COM(2020)0790),

– vu le paquet législatif sur les services numériques,

– vu le code de bonnes pratiques contre la désinformation adopté en 2018 et les orientations de 2021 visant à renforcer le code de bonnes pratique contre la désinformation (COM(2021)0262),

– vu le rapport spécial nº 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'Union[1] (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 la proposition de directive du Parlement européen et du Conseil, présentée par la

[1] JO L 79 I du 21.3.2019, p. 1.

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'UE 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 certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013[2],

– 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 mandat[3], 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 (A9-0000/2021),

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 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 étrangère, la manipulation de l'information et la désinformation 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 et menacent lesdites libertés ainsi que les processus démocratiques de l'Union et de ses États membres, tels que la tenue d'élections libres et régulières;

C. considérant que toute action contre l'ingérence étrangère et la manipulation de l'information doit elle-même respecter les libertés fondamentales d'expression et d'information;

D. considérant que l'expérience montre que des acteurs étrangers malveillants utilisent la manipulation de l'information et d'autres tactiques en matière d'ingérence pour interférer dans les processus démocratiques de l'Union; que ces attaques trompent et induisent en erreur les citoyens, accroissent la polarisation et divisent la société, aggravent la situation des groupes vulnérables, faussent l'intégrité des élections et référendums démocratiques, et sèment la méfiance à l'égard des pouvoirs publics et de

[2] JO L 151 du 7.6.2019, p. 15.
[3] Textes adoptés de cette date, P9_TA(2020)0161.

la démocratie;

E. considérant que les tactiques en matière d'ingérence étrangère prennent la forme de la désinformation et de la suppression de l'information, mais aussi celle de la manipulation de plateformes de réseaux sociaux et de systèmes publicitaires, de cyberattaques, d'opérations de piratage et de divulgation (hack-and-leak), de menaces et de harcèlement à l'encontre de journalistes, de chercheurs, de personnalités politiques et de membres d'organisations de la société civile, de dons et prêts dissimulés à des partis politiques, des campagnes, des organisations et des médias, de faux médias et organisations ou agissant sous couverture, de l'appropriation des ressources par les élites et de la cooptation, de faux personnages, d'une pression exercée pour une autocensure, de l'exploitation abusive des récits historiques, religieux et culturels, d'une pression sur des instituts éducatifs et culturels, de la prise de contrôle d'infrastructures critiques, d'une pression sur les ressortissants étrangers vivant dans l'Union et de l'espionnage;

F. considérant que l'ingérence étrangère est un comportement qui menace ou est susceptible d'avoir des retombées négatives sur les valeurs, les procédures et les processus politiques; que cette ingérence est manipulatrice par nature et menée de façon délibérée et coordonnée; que les responsables de cette ingérence, y compris leurs mandataires sur leur territoire comme en dehors, peuvent être des acteurs étatiques ou non; que le recours par des acteurs étrangers à des mandataires locaux et à la coopération avec des alliés locaux brouille la limite entre ingérence étrangère et nationale;

G. considérant qu'il est nécessaire de convenir, entre partenaires partageant les mêmes idées, de définitions communes de l'ingérence étrangère afin d'établir des normes et des standards internationaux;

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

H. considérant que les tentatives d'ingérence étrangère augmentent et deviennent plus sophistiquées;

I. considérant qu'il est du devoir de l'Union et de ses États membres de défendre tous les citoyens contre les tentatives d'ingérence étrangère; que, néanmoins, l'Union et ses États membres semblent manquer des moyens appropriés et suffisants pour pouvoir mieux prévenir, détecter et lutter contre ces menaces;

J. considérant qu'il existe une méconnaissance générale chez de nombreux décideurs, et parmi les citoyens en général, de la réalité de ces questions, ce qui peut contribuer involontairement à créer d'autres vulnérabilités;

K. considérant que la surveillance de l'état de l'ingérence étrangère en temps réel par des organismes institutionnels et des vérificateurs de faits indépendants s'avère essentielle 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;

L. considérant que la résilience des citoyens de l'Union contre l'ingérence étrangère et la manipulation de l'information nécessite une approche à long terme et globale de la

société;

M. considérant qu'il est nécessaire de coopérer et de se coordonner aux différents niveaux administratifs et dans les différents secteurs afin d'identifier les vulnérabilités, détecter les attaques et y remédier;

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

N. considérant que la connaissance de la situation est la première étape dans la lutte contre la manipulation de l'information et l'ingérence;

O. considérant que des médias de qualité, dotés d'un financement durable et indépendants, et un journalisme professionnel sont essentiels pour la liberté des médias, le pluralisme et l'état de droit, et constituent donc un pilier de la démocratie; que les médias professionnels et le journalisme traditionnel, en tant que sources d'information de qualité, traversent une période difficile à l'ère du numérique; qu'en dépit de tous les progrès accomplis pour améliorer la connaissance de la situation, de nombreuses personnes, y compris des décideurs et des fonctionnaires travaillant dans les secteurs potentiellement concernés, sont encore inconscientes des risques liés à l'ingérence étrangère et ne savent pas comment les éviter;

P. considérant que différentes parties prenantes et institutions utilisent différentes méthodologies et définitions pour analyser l'ingérence étrangère – toutes à différents degrés d'intelligibilité, et que ces différences peuvent empêcher une surveillance, une analyse et une évaluation comparables du niveau de menace, ce qui rend plus difficile une action conjointe;

Q. considérant qu'il est nécessaire de compléter la terminologie qui se concentre sur des contenus comme les fausses informations et la désinformation par une terminologie centrée sur le comportement afin de décrire correctement le problème;

R. considérant qu'une formation dans l'éducation aux médias et au numérique et un travail de sensibilisation constituent des outils importants pour rendre les citoyens plus résilients face aux tentatives d'ingérence dans l'espace de l'information;

S. considérant que la manipulation de l'information peut prendre plusieurs formes, telles que la diffusion de désinformation, la déformation des faits et des déclarations d'opinion, la suppression de certaines informations ou opinions, l'utilisation d'informations en dehors de leur contexte, la promotion de certaines opinions au détriment d'autres et le harcèlement de personnes pour les faire taire;

T. considérant que chaque composante de la société et chaque individu ont un rôle important à jouer pour arrêter la diffusion de la désinformation et mettre en garde les personnes de leur entourage qui sont en danger;

U. considérant qu'il est important d'accéder facilement à des informations basées sur les faits lorsque la désinformation commence à se répandre;

V. considérant qu'il est nécessaire de détecter rapidement les tentatives de manipulation de

l'information pour lutter contre elles;

W. considérant que la désinformation prospère sur les débats polarisés et émotionnels, en exploitant les points faibles et les préjugés de la société et des individus, et qu'elle fausse le débat public autour des élections et autres processus démocratiques et peut rendre difficile pour les citoyens la prise de décisions éclairées;

X. considérant que les plateformes en ligne peuvent s'avérer des outils bon marché et simples pour ceux qui se livrent à la manipulation d'information et autres ingérences, telles que la haine et le harcèlement, la réduction au silence des opposants, l'espionnage ou la diffusion de désinformation;

Ingérence étrangère qui tire parti des plateformes en ligne

Y. considérant que nous avons été témoins de la persévérance d'ingérences et de campagnes de manipulation d'information à l'encontre de toutes les mesures prises contre la propagation de la COVID-19, y compris la vaccination dans l'ensemble de l'Union, les plateformes en ligne n'ayant remporté dans leur lutte contre elles que des succès très limités;

Z. considérant que les plateformes en ligne contrôlent le flux des informations et de la publicité en ligne, qu'elles conçoivent et utilisent des algorithmes pour contrôler lesdits flux et qu'elles ne partagent que très peu d'informations, voire aucune, sur la conception, l'utilisation et les effets de ces algorithmes;

AA. considérant que de nombreux prestataires immatriculés dans l'Union vendent de faux likes, commentaires et partages à tout acteur souhaitant stimuler artificiellement sa visibilité en ligne; qu'il est pratiquement impossible d'identifier les utilisations légitimes desdits services, tandis que les utilisations préjudiciables comprennent la manipulation des élections, la promotion d'escroqueries, l'analyse négative des produits de la concurrence et la spoliation des annonceurs;

AB. 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 sensibles sur chaque utilisateur; que lesdites données sont vendues sur le marché des données; que des fuites de données se produisent de façon répétée; que ces bases de données pourraient s'avérer être des mines d'or pour des acteurs souhaitant cibler des groupes ou des individus;

AC. considérant que choisir de ne pas partager ses données plutôt que de les partager est généralement fastidieux et chronophage;

AD. considérant que les plateformes en ligne sont associées à la plupart des pans de nos existences et peuvent influencer considérablement notre pensée et notre comportement, par exemple en ce qui concerne les préférences ou les comportements en matière de vote;

AE. considérant que les mécanismes de traitement des algorithmes, conçus pour maximiser les engagements, sont régulièrement dénoncés pour favoriser la polarisation et la radicalisation des contenus;

AF. considérant que la diffusion de faux documents audio et vidéo est un problème qui peut aller en s'aggravant;

AG. considérant que les systèmes d'autorégulation, tels que le code de bonnes pratiques contre la désinformation adopté en 2018, ont permis des améliorations mais laissent trop de place aux plateformes qui ne font rien ou très peu pour lutter contre les ingérences dans leurs systèmes;

AH. considérant que les sanctions actuelles qui menacent ceux qui utilisent les plateformes pour frauder ne sont pas assez sévères pour les en dissuader;

AI. considérant que les plateformes consacrent nettement moins de ressources aux contenus dans les langues les moins parlées, et même dans les langues de grande diffusion en dehors de l'anglais, par rapport aux contenus en anglais;

AJ. considérant que l'action des plateformes, ou leur absence d'action, ne peut faire l'objet d'un recours de la part de l'organisation ou du particulier affectés;

AK. considérant qu'au cours des derniers mois, plusieurs acteurs majeurs ont respecté 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;

AL. considérant que le manque de transparence en ce qui concerne les choix algorithmiques des plateformes rend pratiquement impossible la vérification de leurs affirmations sur ce qu'elles font pour lutter contre la manipulation de l'information et l'ingérence;

AM. considérant qu'un grand nombre de publicités en ligne émanant de marques réputées finissent sur des sites qui hébergent des discours haineux et de la désinformation, à l'insu ou sans le consentement des annonceurs;

Infrastructures critiques et secteurs stratégiques

AN. considérant que la gestion des menaces portant sur les infrastructures critiques, particulièrement lorsqu'elles font partie d'une stratégie hybride, synchronisée et malveillante, nécessite les efforts conjoints et coordonnés des différents secteurs, à plusieurs niveaux – européen, national, régional et local – et à divers moments;

AO. 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; que la liste des services figurera en annexe de la directive;

AP. 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; que cela s'est traduit par une forte dépendance de l'Union à l'égard de nombreux produits essentiels et actifs principaux importés de l'étranger;

AQ. considérant que les investissements directs étrangers (IDE) – investissements réalisés

par des pays tiers - dans les secteurs stratégiques de l'Union ont constitué un motif croissant de préoccupation ces dernières années;

Financement dissimulé des activités politiques provenant de donateurs étrangers

AR. considérant que de nombreux éléments de preuve montrent que des acteurs étrangers s'ingèrent 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;

AS. considérant que, par exemple, la Russie, la Chine et d'autres régimes autoritaires ont déversé plus de 300 millions d'USD dans 33 pays pour s'ingérer dans les processus démocratiques, et que cette tendance s'accélère manifestement; que la moitié de ces affaires concernent des actions menées par la Russie en Europe;

AT. considérant que ces opérations visent à financer des partis politiques européens ou des mouvements visant à approfondir la fragmentation sociétale et à nuire à la légitimité des autorités publiques nationales et européennes;

AU. considérant que les lois électorales, en particulier les dispositions relatives au financement des activités politiques, ne sont pas harmonisées au niveau de l'Union, et permettent donc des méthodes de financement opaques provenant d'acteurs étrangers, au moyen de diverses règles créant de nombreuses failles et pratiques légales ou illégales au sein de l'Union;

AV. considérant que la publicité politique en ligne n'est pas soumise aux règles applicables à la publicité politique hors ligne;

AW. considérant que le règlement (UE, Euratom) nº 1141/2014 du 22 octobre 2014 relatif au statut et au financement des partis politiques européens et des fondations politiques européennes[4] est en cours de révision en vue d'atteindre un plus grand niveau de transparence en matière de financement des activités politiques;

Cybersécurité et résilience face aux cyberattaques

AX. considérant que l'incidence des cyberattaques a connu une hausse ces dernières années; 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 (EMA) et le Parlement norvégien, ont été attribuées à des groupes de pirates informatiques soutenus par des États, principalement affiliés aux gouvernements russe et chinois;

AY. considérant que la capacité actuelle à faire face aux cybermenaces est limitée en raison de la rareté des ressources humaines et financières;

AZ. considérant que la fragmentation des capacités et des stratégies de l'Union dans le

[4] JO L 317 du 4.11.2014, p. 1.

domaine cybernétique est un problème qui va en s'accroissant;

BA. considérant que des programmes de surveillance illicites et à grande échelle ont été utilisés par des acteurs étatiques étrangers pour cibler des journalistes, des militants des droits de l'homme et des hommes politiques, y compris des chefs d'État européens;

Protection des institutions de l'Union

BB. considérant que le caractère décentralisé et multinational des institutions de l'Union peut être exploité par des acteurs étrangers malveillants souhaitant semer la division dans celle-ci;

BC. considérant qu'il est nécessaire de mettre en place des procédures de gestion de crise adéquates avant que les crises ne surviennent;

BD. 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 leur prévention;

Ingérence par l'appropriation des ressources par les élites, les diasporas nationales et les universités

BE. considérant que, en échange de leurs connaissances et au détriment des intérêts de l'Union et de ses États membres, un certain nombre d'anciens hauts fonctionnaires et d'acteurs politiques européens sont engagés ou cooptés par des entreprises étrangères contrôlées par des États qui pratiquent une ingérence malveillante au sein de l'Union;

BF. considérant que deux pays sont particulièrement actifs dans le domaine de la cooptation et de l'appropriation des ressources par les élites, à savoir la Russie et la Chine, 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 de demande 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 Zaroubejneft, de l'ancien Premier ministre français Jean-Pierre Raffarin qui s'est activement engagé à promouvoir les intérêts chinois en France, et de l'ancien commissaire tchèque Štefan Füle qui a travaillé pour CEFC China Energy;

BG. considérant que la stratégie de lobbying économique peut être combinée avec des objectifs d'ingérence étrangère;

BH. considérant que le contrôle des diasporas nationales vivant sur le sol de l'Union représente un élément important des stratégies d'ingérence étrangère;

BI. considérant que différents acteurs étatiques, tels que le gouvernement russe et le parti communiste chinois, ont tenté d'accroître leur influence en utilisant des instituts culturels, éducatifs (par exemple, par l'intermédiaire de subventions et de bourses d'études) et religieux;

BJ. 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, notamment, mais pas uniquement, 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 l'extrême droite et à d'autres forces et acteurs radicaux dans toute l'Europe, notamment, mais pas uniquement, en France, en Allemagne, en Italie et en Autriche; que les récentes découvertes de contacts étroits et réguliers entre des fonctionnaires russes et des représentants d'un groupe de sécessionnistes catalans en Espagne demandent une enquête approfondie, étant donné les tentatives constantes de la Russie d'exploiter tout ce qu'elle peut pour favoriser la déstabilisation interne et la discorde dans l'Union;

BK. 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 un outil d'ingérence dans l'Union;

Dissuasion et sanctions collectives

BL. 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 acteurs peuvent supposer sans risque que leurs campagnes de déstabilisation contre l'Union seront sans conséquence;

BM. considérant que l'Union devrait renforcer ses outils de dissuasion afin que les acteurs étrangers malveillants soient obligés de payer le prix de leurs décisions et d'en assumer les conséquences;

Coopération mondiale et multilatéralisme

BN. considérant que les actions malveillantes orchestrées par des régimes autoritaires étrangers affectent de nombreux pays démocratiques dans le monde;

BO. considérant le manque de compréhension commune et de définitions communes persistant parmi les partenaires partageant les mêmes idées en ce qui concerne la nature des menaces en cause;

BP. considérant qu'il est nécessaire d'instaurer une coopération mondiale entre les partenaires partageant les mêmes idées pour faire face à l'ingérence malveillante étrangère,

Nécessité d'une stratégie coordonnée de l'UE 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 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 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 d'outils de dissuasion appropriés leur permettant de lutter contre toutes les menaces et attaques hybrides orchestrées par des pays étrangers; considère que cette stratégie devrait reposer sur: 1 – des définitions communes, une analyse d'impact critique et ex post de la législation adoptée jusqu'à présent, ainsi que la compréhension et la connaissance de la situation des enjeux, 2 – des politiques concrètes permettant de renforcer la résilience des citoyens de l'Union conformément aux valeurs démocratiques, 3 – des capacités de perturbation adaptées, et 4 – des réponses diplomatiques et de dissuasion dans un contexte mondial;

3. souligne que toutes les mesures visant à prévenir, détecter et lutter contre l'ingérence étrangère doivent être élaborées de manière à respecter et à promouvoir les droits fondamentaux, notamment le respect de la vie privée et les libertés de pensée, d'expression et d'information;

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) le renforcement de la résilience de l'Union par la connaissance de la situation, l'éducation et la formation aux médias,

   b) l'ingérence étrangère qui tire parti des plateformes en ligne,

   c) les infrastructures critiques et les secteurs stratégiques,

   d) le financement dissimulé des activités politiques provenant de donateurs étrangers

   e) la cybersécurité et la résilience face aux cyberattaques,

   f) la protection des institutions de l'Union,

   g) l'ingérence par l'appropriation des ressources par les élites, les diasporas nationales et les universités,

   h) la dissuasion et les sanctions collectives,

   i) la coopération mondiale et le multilatéralisme;

5. demande, en particulier, que l'Union augmente les ressources et les moyens alloués aux organes et organisations chargés de la surveillance et de la sensibilisation à la gravité des menaces, y compris la désinformation, du renforcement de la protection des intérêts stratégiques et des infrastructures de l'Union et de ses États membres, ainsi que de la mise en place d'une coopération internationale avec des partenaires partageant les mêmes idées et confrontés à des défis similaires;

6. est préoccupé du manque criant de sensibilisation à la gravité des menaces actuelles que présentent les régimes autoritaires étrangers qui ciblent tous les niveaux et secteurs de la société européenne afin de nuire à la légitimité des autorités publiques et d'intensifier la fragmentation politique et sociale;

7. est préoccupé par l'absence de mesures appropriées et suffisantes pour prévenir, détecter et lutter contre ces tentatives d'ingérence, l'ingérence devenant dès lors une tactique attrayante pour les acteurs malveillants puisque les risques d'être sanctionné, ou même remarqué, sont très faibles;

8. demande instamment à la Commission d'inclure la dimension de l'ingérence et de la manipulation de l'information étrangères dans l'analyse d'impact ex ante réalisée avant de présenter de nouvelles propositions; propose que la Commission procède également à des examens réguliers de la résilience dans lesquels elle évalue l'évolution des menaces et leur incidence sur la législation et les politiques actuelles;

9. invite la Commission à analyser les initiatives nationales récentes, 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 suédoise de sécurité civile, la nouvelle agence de défense psychologique et le centre national de la Chine, et la nouvelle agence nationale française Viginum, afin de déterminer les meilleures pratiques qui pourraient être mises en œuvre au niveau de l'Union;

10. est préoccupé par les nombreuses lacunes et failles de la législation et des politiques actuelles au niveau de l'Union et au niveau national destinées à détecter, prévenir et lutter contre l'ingérence;

11. demande à la Commission de mettre en place un mécanisme européen consacré à l'examen de la législation et des politiques existantes afin de repérer les lacunes qui pourraient être exploitées par des acteurs malveillants et de proposer rapidement des moyens 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;

12. 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;

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

13. insiste sur le fait que les institutions et les États membres de l'Union ont besoin de systèmes solides et robustes 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 dissuader et combattre;

14. souligne qu'il est tout aussi important que les informations tirées de cette analyse ne restent pas au sein de groupes de spécialistes de l'ingérence étrangère, mais soient partagées avec un public plus large, en particulier avec les personnes exerçant des fonctions sensibles, afin que chacun soit conscient des schémas de menace et puisse éviter les risques;

15. souligne qu'il est nécessaire d'élaborer une méthodologie commune pour développer la connaissance de la situation, collecter des preuves systématiques et détecter la manipulation de l'environnement informationnel, ainsi que des normes pour l'attribution technique;

16. insiste sur la nécessité pour l'Union, en coopération avec les États membres et les partenaires mondiaux, d'élaborer une définition conceptuelle de la menace d'ingérence; souligne que cette définition doit prendre en considération les tactiques, les techniques et les procédures qui décrivent les schémas comportementaux des acteurs de la menace que nous observons aujourd'hui;

17. demande que les institutions de l'Union poursuivent l'important travail de la division StratCom du Service européen pour l'action extérieure (SEAE), avec ses task forces, le centre d'analyse du renseignement de l'Union européenne (INTCEN) et la cellule de fusion contre les menaces hybrides, le système d'alerte rapide, la coopération établie au niveau administratif entre le SEAE, la Commission et le Parlement, le réseau de lutte contre la désinformation dirigé par la Commission, la task force administrative du Parlement contre la désinformation, et 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 l'ingérence et à la manipulation de l'information étrangères;

18. souligne la nécessité de renforcer les efforts de suivi bien avant les élections ou les autres processus politiques importants;

19. invite les États membres à utiliser pleinement ces ressources en partageant les renseignements pertinents et en participant activement au système d'alerte rapide; est d'avis que la coopération en matière d'analyse et de renseignement doit être davantage renforcée;

20. 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, tout en attendant davantage de précisions sur sa création et sa mission; souligne qu'un tel centre nécessiterait une coopération active avec les services de la Commission, le SEAE, le Conseil et le Parlement;

21. rappelle la nécessité de doter le SEAE d'un mandat et des ressources nécessaires pour surveiller et lutter contre l'ingérence et la manipulation de l'information au-delà des régions actuellement couvertes par les trois task forces, en appliquant une approche fondée sur les risques; demande de toute urgence que le SEAE déploie des capacités adéquates afin de lutter contre l'ingérence et la manipulation de l'information émanant de la Chine; 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, tant au sein du SEAE que des institutions de l'Union en général;

22. insiste sur l'importance des journalistes indépendants, des vérificateurs de faits et des chercheurs 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 indépendants, de vérificateurs de faits et de chercheurs dans toute l'Europe, et en particulier dans les régions les plus exposées, telles que l'Observatoire européen

des médias numériques;

23. 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;

24. préconise des sources de financement public fiables et durables pour les vérificateurs de faits indépendants, les chercheurs, les médias et les journalistes de qualité, ainsi que les ONG qui enquêtent sur l'ingérence et la manipulation d'information, qui promeuvent l'éducation aux médias et d'autres moyens de responsabiliser les citoyens, et qui recherchent des moyens mesurer de manière significative l'efficacité de la formation à l'éducation aux médias, de la sensibilisation, de la démystification et de la communication stratégique; souligne que plusieurs pays dans le monde prennent des mesures pour que les médias disposent de ressources financières adéquates; se félicite, à cet égard, des nouvelles possibilités de financement de l'éducation aux médias dans le programme Europe créative 2021-2027;

25. souligne la nécessité de mettre à la disposition du public les analyses, les rapports d'incidents et les renseignements concernant l'ingérence et la manipulation de l'information; suggère donc la création d'un dépôt public, avec des informations clés disponibles dans toutes les langues de l'Union;

26. demande à tous les États membres d'inclure dans leurs programmes l'éducation aux médias et au numérique, ainsi que l'esprit critique et la participation du public, de la petite enfance à l'éducation des adultes, y compris la formation des enseignants et des chercheurs;

27. 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 qu'une formation initiale soit également proposée 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;

28. souligne la nécessité de sensibiliser au phénomène d'ingérence et de manipulation de l'information, 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 et aux visiteurs, tant hors ligne qu'en ligne, à Bruxelles et dans d'autres capitales de l'Union, et recommande de les développer davantage;

29. 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, comme le prévoit la directive sur les services de médias audiovisuels; demande à la Commission d'organiser ces échanges en coopération avec le groupe d'experts en éducation aux médias;

30. demande que l'Union et ses États membres mettent en œuvre des programmes ciblés de sensibilisation et d'éducation aux médias destinés aux diasporas et aux 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;

31. demande à la Commission de présenter une stratégie d'éducation aux médias, en mettant l'accent sur la lutte contre la manipulation de l'information;

32. souligne l'importance d'une communication stratégique pour contrer les récits anti-démocratiques les plus courants; insiste sur le fait que toutes les organisations démocratiques doivent défendre la démocratie et ont la responsabilité commune de s'engager auprès des citoyens, en utilisant leurs langues et leurs plateformes préférées;

33. est préoccupé de la propagation de la propagande d'État étrangère en provenance de Moscou et de Pékin, qui est traduite dans les langues locales, par exemple dans des contenus médiatiques sponsorisés par RT, Sputnik ou le Parti communiste chinois déguisés en journalisme et distribués avec les journaux; s'inquiète de la manière dont ces récits ont été diffusés dans de véritables produits journalistiques;

34. est profondément préoccupé par le harcèlement et les menaces à l'encontre des journalistes et demande à la Commission de présenter rapidement des propositions concrètes et ambitieuses sur la sécurité des journalistes et des professionnels des médias, comme annoncé dans le cadre du plan d'action pour la démocratie européenne;

35. 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;

36. recommande aux États membres de mettre en place des canaux de communication vers lesquels les entreprises, les ONG et les particuliers peuvent se tourner s'ils sont victimes d'ingérence ou de manipulation d'information; invite les États membres à soutenir les personnes qui sont victimes d'attaques ou qui subissent des pressions;

Ingérence étrangère qui tire parti des plateformes en ligne

37. 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, l'espionnage et les menaces; souligne que les plateformes doivent non seulement respecter la loi, mais aussi être à la hauteur des conditions générales qu'elles promettent à leurs utilisateurs;

38. souligne la nécessité, avant tout, d'accroître considérablement la transparence en ce qui concerne les opérations menées par les plateformes en ligne;

39. préconise une réglementation pour obliger les plateformes à faire ce qui leur incombe

pour réduire l'ingérence et la manipulation de l'information, par exemple en utilisant des labels qui indiquent les véritables auteurs cachés derrière les comptes, en faisant obstacle aux comptes régulièrement utilisés pour diffuser de la désinformation ou qui enfreignent régulièrement les conditions générales de la plateforme, en suspendant les comptes non authentiques utilisés pour des campagnes d'ingérence coordonnées ou en démonétisant les sites de diffusion de désinformation;

40. 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; recommande que la lecture finale de ces textes tienne compte des aspects exposés dans la suite de la présente section;

41. demande que des règles contraignantes de l'Union limitent 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, que les différentes fonctions des plateformes soient découplées afin de réduire la quantité d'informations disponibles sur chaque individu, et qu'il soit aussi facile de refuser que d'accepter le stockage et le partage des données; préconise une interdiction européenne du microciblage pour la publicité politique ou thématique;

42. demande que des règles européennes contraignantes obligent les plateformes à repérer, évaluer et atténuer régulièrement les risques d'ingérence et de manipulation de l'information que comporte l'utilisation de leurs services, obligent les plateformes à mettre en place des systèmes permettant de surveiller la manière dont leurs services sont utilisés, au moins dans toutes les langues nationales et régionales officielles, afin de détecter l'ingérence et la manipulation de l'information 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;

43. préconise une réglementation des services offrant des outils et des services de manipulation des médias sociaux; souligne que cette réglementation doit être fondée sur une évaluation approfondie des pratiques actuelles et des risques associés;

44. insiste sur le besoin général de transparence 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 les faux comptes liés à des opérations d'influence coordonnées; souligne que les demandes de preuve doivent permettre l'anonymat des personnes vulnérables (par exemple, les dénonciateurs ou les dissidents et les opposants politiques à des régimes autocratiques) et laissent une place aux comptes satiriques et humoristiques;

45. souligne qu'une responsabilité accrue en matière de suppression des contenus illégaux et dangereux ne doit pas entraîner la suppression arbitraire de contenus légaux; appelle à la prudence en matière de suspension totale des comptes de particuliers;

46. demande des règles contraignantes pour obliger les plateformes à créer des canaux de communication facilement accessibles pour les personnes ou les organisations qui

souhaitent signaler des abus ou des soupçons d'ingérence ou de manipulation, et pour mettre en place des procédures de recours, tant pour les victimes de contenus mis en ligne que pour les personnes ou les organisations affectées par la décision d'étiqueter, de restreindre la visibilité, de désactiver l'accès ou de suspendre des comptes, ou de restreindre l'accès aux revenus publicitaires;

47. préconise l'adoption de règles visant à rendre les procédures en ligne transparentes, par exemple en obligeant les plateformes à mettre en place des archives publiques et facilement consultables des publicités en ligne et à donner un accès significatif aux informations sur la création, l'utilisation et l'incidence des algorithmes et des données au niveau individuel à des chercheurs agréés affiliés à des institutions universitaires, des journalistes, des organisations de la société civile et des organisations internationales représentant l'intérêt public;

48. invite les plateformes à corriger l'équilibre entre, d'une part, la nécessité motivée par des raisons commerciales d'inciter les internautes à rester plus longtemps sur les plateformes en leur proposant des contenus attrayants et, d'autre part, la responsabilité de promouvoir des contenus de qualité; demande instamment aux plateformes de veiller à ce que leurs algorithmes ne favorisent pas les contenus illégaux, extrémistes ou menant à la radicalisation, mais offrent plutôt aux utilisateurs une pluralité de perspectives;

49. demande que les algorithmes soient modifiés afin de démanteler les contenus provenant de comptes et de canaux non authentiques qui poussent artificiellement à la diffusion de la manipulation d'information nuisible en provenance de l'étranger;

50. insiste sur la nécessité d'un examen systématique des conséquences des algorithmes; 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 permettent à des comportements non authentiques coordonnés à grande échelle de manipuler le contenu diffusé sur leurs plateformes;

51. s'alarme du nombre massif de publicités en ligne de marques réputées qui aboutissent sur, et donc financent, des sites malveillants promouvant des discours haineux et de la désinformation sans le consentement des marques concernées et sans qu'elles en aient même connaissance; considère que les services de publicité programmatique, tels que Google Ads et d'autres bourses d'annonces, devraient être responsables de la sélection des sites web des éditeurs figurant dans leur inventaire afin d'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;

52. 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 et d'évaluation après leur adoption, afin de contrôler régulièrement leur mise en œuvre aux niveaux national et de l'Union et de repérer et de combler les lacunes sans délai;

Infrastructures critiques et secteurs stratégiques

53. considère que, compte tenu de leur nature interconnectée et transfrontalière, les infrastructures critiques sont de plus en plus vulnérables aux manipulations extérieures et estime que le cadre juridique actuellement en place doit être remanié; 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 européenne;

54. recommande que, lors de l'examen de la proposition susmentionnée, des efforts soient faits pour renforcer les réseaux de connexion et les moyens de communication déjà bien coordonnés utilisés par de multiples acteurs, le soutien aux autorités compétentes des États membres par le groupe sur la résilience des entités critiques et l'échange des meilleures pratiques non seulement entre les États membres mais aussi, aux niveaux régional et local, entre les propriétaires et les exploitants d'infrastructures critiques, y compris par la communication interinstitutionnelle, afin d'identifier à un stade précoce les évolutions préoccupantes et de mettre au point des contre-mesures adéquates;

55. est d'avis que la liste des infrastructures critiques peut être étendue aux médias, ainsi qu'aux infrastructures électorales, compte tenu de leur importance cruciale pour garantir le fonctionnement de l'Union et de ses États membres, et qu'il convient de faire preuve de flexibilité au cours de la prise de décision concernant l'ajout à la liste de nouveaux secteurs stratégiques à protéger;

56. 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 de l'infrastructure de données dans le contexte des élections; estime qu'il existe un manque de contrôle démocratique sur le secteur privé;

57. recommande d'adopter une approche très flexible permettant des mises à jour et des modifications rapides de la directive proposée, sur la base des évaluations des menaces, des risques et des vulnérabilités réalisées par le centre d'analyse du renseignement de l'Union européenne (INTCEN) du SEAE; souligne la nécessité de prévoir une approche modulaire afin de garantir une adaptabilité et une flexibilité rapides;

58. estime que l'Union et ses États membres doivent fournir d'autres solutions de financement pour éviter que des parties importantes de leurs infrastructures critiques ne tombent entre les mains de pays tiers, 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 le règlement établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union qui constitue un outil important pour coordonner les actions des États membres en matière d'investissements étrangers dans les structures critiques, et préconise un cadre réglementaire plus solide afin de garantir que davantage de compétences en matière d'examen des IDE soient transférées aux institutions de l'Union; estime que le cadre juridique devrait également être mieux relié à des analyses indépendantes, réalisées soit par des instituts nationaux et européens soit par des groupes de réflexion pertinents.

considère qu'il pourrait également être approprié d'inclure d'autres secteurs stratégiques dans le cadre juridique, tels que la 5G, afin de limiter sa dépendance à l'égard des fournisseurs à haut risque;

59. estime que l'Union est confrontée à davantage de difficultés en raison de sa dépendance à l'égard des fournisseurs étrangers de technologies; estime que le récent effort de l'Union en faveur de l'autonomie stratégique et la souveraineté numérique est donc très important et représente la bonne façon de procéder; considère que l'acte législatif européen relatif aux puces annoncé par la Commission, qui vise à garantir que les pièces essentielles à la production de puces soient fabriquées en Europe, 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 du bloc afin d'éviter une course aux subventions publiques nationales et la fragmentation du marché unique; invite donc la Commission à créer un fonds européen dédié aux semi-conducteurs;

60. salue le développement par l'Union de GAIA-X, réseau européen de fournisseurs d'infrastructures et de services de données répondant aux normes de sécurité européennes, comme une étape importante pour résister à la domination des fournisseurs américains de services en nuage;

61. demande à la Commission de proposer des actions visant à mettre en place un approvisionnement sûr et durable des matières premières utilisées pour produire des batteries et des équipements d'énergie renouvelable;

Financement dissimulé des activités politiques provenant de donateurs étrangers

62. souligne 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 des élections libres et équitables, et qu'il convient donc de rendre illégale dans l'Union toute activité secrète financée par une puissance étrangère visant à influencer le processus des politiques européennes;

63. souligne qu'une part importante du financement occulte par des acteurs étrangers n'est pas à proprement parler illégale car elle est rendue possible par les nombreuses failles résultant des différentes dispositions relatives au financement des activités politiques dans les lois électorales nationales des États membres;

64. souligne que ces failles comportent:

a) les contributions en nature des acteurs étrangers aux partis politiques, y compris les prêts financiers provenant de toute personne morale ou physique basée à l'étranger, qui devraient être interdits;

b) les citoyens prête-noms et les agents sous couverture[5]: la transparence concernant les donateurs en tant que personnes physiques et morales doit être appliquée au

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

moyen de déclarations de conformité attestant du statut du donateur, et des pouvoirs d'application plus importants doivent être accordés aux commissions électorales;

c) les sociétés-écrans et les filiales nationales de sociétés mères étrangères[6]: les sociétés-écrans devraient être interdites et des exigences plus strictes devraient être établies afin de révéler les origines du financement par l'intermédiaire de sociétés mères;

d) les organisations à but non lucratif et les tiers[7], 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;

e) les publicités politiques en ligne, qui ne sont pas soumises aux règles relatives à la publicité télévisée, radiophonique et imprimée et ne sont généralement pas réglementées du tout: il est donc nécessaire de garantir une transparence totale en ce qui concerne l'entrée et la sortie des fonds impliqués dans les publicités politiques en ligne, ainsi que d'assurer une responsabilité beaucoup plus grande quant à l'utilisation des algorithmes, conformément au principe «connaissez votre client»; la Commission devrait rapidement soumettre une proposition législative sur la transparence des contenus politiques sponsorisés, comme proposé dans le cadre du plan d'action pour la démocratie européenne, qui garantira le droit effectif des partis de l'Union de faire campagne en ligne avant les élections européennes;

65. invite donc la Commission à présenter des propositions concrètes visant à combler toutes les lacunes qui permettent le financement opaque des partis politiques à partir de sources de pays tiers et 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 une interdiction des dons aux partis politiques provenant de l'extérieur de l'Union et de l'Espace économique européen (EEE), à l'exception des électeurs vivant en dehors de l'Union et de l'EEE;

66. salue la révision en cours du règlement (UE, Euratom) nº 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 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;

---

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

[7] 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.

Cybersécurité et résilience face aux cyberattaques

67. demande instamment aux institutions de l'Union d'augmenter rapidement les investissements dans les capacités et les compétences numériques stratégiques de l'Union, telles que l'intelligence artificielle, la communication sécurisée et les infrastructures de données et de nuages, afin d'améliorer la cybersécurité de l'Union; invite la Commission à investir également davantage dans l'accroissement 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; invite la Commission à allouer des ressources supplémentaires, tant humaines que financières, à la cybersécurité des institutions de l'Union et des États membres;

68. salue les propositions de la Commission concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148[8] (NIS2); recommande que le résultat final des travaux en cours sur la proposition corrige les défauts de la directive NIS de 2018, notamment en renforçant les exigences de sécurité, en introduisant des exigences de mise en œuvre plus strictes, telles que des sanctions harmonisées, et en suggérant des réglementations horizontales et une bonne coopération public-privé au niveau opérationnel; souligne l'importance 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;

69. demande à la Commission de développer la boîte à outils de l'Union constituée de mesures d'atténuation des risques de la nouvelle génération de technologies, telles que la 5G et la 6G, afin de mieux prendre en compte les risques liés à l'utilisation de logiciels et de matériels produits par des entreprises sous le contrôle d'États autoritaires étrangers, et d'élaborer des normes mondiales et des règles de concurrence, dans le respect des valeurs démocratiques, pour cette nouvelle technologie; 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;

70. soutient l'idée de la Commission de créer une loi sur la cyberrésilience qui viendrait compléter une politique européenne de cyberdéfense, étant donné que la cybernétique et la défense sont interconnectées; appelle à une augmentation des ressources destinées aux capacités et à la coordination de la cyberdéfense européenne;

71. condamne l'utilisation massive et illicite du logiciel de surveillance Pegasus par des entités étatiques contre des journalistes, des défenseurs des droits de l'homme et des hommes politiques; rappelle que Pegasus n'est qu'un des nombreux exemples de programmes de surveillance illicites exploités par des entités étatiques contre des citoyens innocents;

[8] 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.

72. s’inquiète de ce que des journalistes et des militants 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 représente une grave violation 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;

73. souligne l’urgente nécessité de renforcer le cadre législatif afin de tenir pour responsables ceux qui distribuent, utilisent et abusent de 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;

74. demande une révision ambitieuse de la directive vie privée et communications électroniques afin de renforcer la confidentialité des communications et des données personnelles lors de l’utilisation d’appareils électroniques, sans abaisser le niveau de protection offert par le règlement 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 la directive relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données; appelle l’Union et les États membres à coordonner davantage leurs actions sur la base de la directive sur les attaques contre les systèmes d’information afin de garantir que l’accès illégal aux systèmes d’information et l’interception illégale soient définis comme des infractions pénales; rappelle que toute violation 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, sur la base de la stricte nécessité et de la proportionnalité, comme l’exigent la CEDH et la Cour de justice de l’Union européenne;

Protection des institutions de l’Union

75. souligne que les réseaux, les bâtiments et le personnel des institutions de l’Union représentent une cible pour tous les types de menaces hybrides et d’attaques d’acteurs étatiques étrangers et qu’ils devraient, par conséquent, être protégés de manière appropriée; reconnaît l’augmentation constante des attaques commanditées par des États contre les institutions, les organes et les agences de l’Union, notamment contre l’Agence européenne des médicaments (EMA), ainsi que contre les institutions des États membres et les autorités publiques nationales;

76. demande un examen approfondi des services, réseaux, équipements et matériels des institutions, organes et agences de l’Union européenne utilisés pour assurer la cybersécurité; demande instamment aux institutions de l’Union et aux États membres de veiller à ce que le personnel bénéficie d’une orientation adéquate et d’outils sûrs; souligne la nécessité de sensibiliser les institutions et les administrations à l’utilisation de services et de réseaux sécurisés;

77. souligne l’importance de la coordination entre les différentes institutions, organes et

agences de l'Union européenne spécialisés dans la cybersécurité, tels que l'équipe d'intervention en cas d'urgence informatique pour les institutions de l'Union européenne (CERT-UE), conjointement avec le développement complet de ses capacités opérationnelles, ainsi que de l'Agence de l'Union européenne de cybersécurité (ENISA) et de la future unité cybernétique commune qui garantira une réponse coordonnée aux menaces de cybersécurité à grande échelle dans l'Union; salue la coopération structurée en cours entre le CERT-UE et l'ENISA; apprécie les récentes initiatives prises par les secrétaires généraux des institutions de l'Union pour élaborer des règles communes en matière d'information et de cybersécurité;

78. 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 toutes les institutions, tous les organes et toutes les agences de l'Union, et est d'avis que ces règlements devraient inclure le renforcement des capacités; invite la Commission et les États membres à allouer des fonds et des ressources supplémentaires à la cybersécurité des institutions de l'Union afin de relever les défis d'un paysage de menaces en constante évolution;

79. attend avec intérêt le rapport spécial de la Cour des comptes européenne sur l'audit de cybersécurité, attendu pour le début de 2022;

80. demande à toutes les institutions de l'Union de sensibiliser leur personnel par une formation et des conseils appropriés afin d'atténuer et de traiter les risques de sécurité cybernétique et non cybernétique; demande une formation obligatoire et régulière à la sécurité de l'ensemble du personnel et des députés européens;

81. souligne la nécessité de procédures de gestion de crise appropriées pour les cas de manipulation de l'information, dont les systèmes d'alerte entre les niveaux administratifs et les secteurs, afin de garantir la fourniture d'informations mutuelles et d'empêcher la manipulation de l'information de se propager; 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 des procédures en place dans les administrations de la Commission et du Parlement pour avertir d'éventuels cas affectant les institutions ou les processus démocratiques de l'Union; demande à l'administration de l'Union de réfléchir davantage à une boîte à outils partagée à activer en cas d'alerte SAR;

Ingérence par l'appropriation des ressources par les élites, les diasporas nationales et les universités

82. condamne tous les types d'appropriation des ressources par les élites et la technique de cooptation de fonctionnaires de haut niveau et d'anciens responsables politiques de l'Union utilisée par des entreprises étrangères ayant des liens avec des gouvernements activement engagés dans des actions d'ingérence contre l'Union, et regrette le manque d'outils et d'application 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 être strictement interdite;

83. invite la Commission à encourager et à coordonner les actions visant à lutter contre l'appropriation des ressources par les élites, par exemple en complétant les périodes de

réflexion des commissaires européens par une obligation de rapport à l'issue de ces périodes, et en établissant des règles structurées pour lutter contre l'accaparement des élites au niveau européen;

84. est préoccupé par les stratégies de lobbying intégrées combinant intérêts industriels et objectifs politiques étrangers, en particulier lorsqu'elles favorisent 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 cartographiant le financement étranger du lobbying lié à l'Union et en garantissant une entrée qui permette d'identifier les financements provenant de gouvernements étrangers; considère que le système australien de transparence en matière d'influence étrangère est une bonne pratique à suivre;

85. 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 le gouvernement des activités déclarées entreprises pour un État étranger ou en son nom, en suivant les bonnes pratiques d'autres démocraties partageant les mêmes idées;

86. est préoccupé par les tentatives menées 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; souligne l'expérience de l'Australie et de la Nouvelle-Zélande concernant le Front uni;

87. souligne que les efforts du Kremlin pour mettre en œuvre des politiques de «soutien des compatriotes», notamment dans les États baltes et les pays du voisinage oriental, font partie 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», visant à justifier les actions expansionnistes du régime;

88. est alarmé par l'application extraterritoriale des mesures coercitives découlant de la nouvelle loi chinoise sur la sécurité nationale, combinée aux accords d'extradition dont bénéficie la Chine avec d'autres pays, ce qui permet à la Chine de mettre en œuvre des actions de dissuasion à grande échelle contre des ressortissants non chinois critiques, par exemple, dans une affaire récente, contre deux parlementaires danois;

89. est préoccupé par le nombre d'universités, d'écoles et de centres culturels européens engagés dans des partenariats avec des entités chinoises, notamment des centres 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, constituant ainsi une violation de la protection constitutionnelle de la liberté et de l'autonomie académiques, et sur les choix des activités culturelles liées à la Chine; regrette, en particulier, la décision prise par le musée de Nantes d'annuler l'exposition sur Gengis Khan en 2020, suite à de fortes pressions de la Chine qui s'opposait à une telle exposition[9];

[9] https://www.chateaunantes.fr/expositions/fils-du-ciel-et-des-steppes/

90. condamne la décision prise par le gouvernement hongrois d'ouvrir une succursale de l'université Fudan et, dans le même temps, de fermer l'université centre-européenne de Budapest; s'inquiète de la dépendance financière croissante des universités européennes à l'égard de la Chine et demande à la Commission et aux États membres de garantir des allocations budgétaires appropriées pour les universités européennes; invite la Commission à proposer une législation visant à accroître la transparence du financement des universités, par exemple au moyen de déclarations obligatoires de dons;

91. est préoccupé par le nombre croissant de centres Confucius établis dans le monde, et en particulier en Europe, qui sont étroitement liés à l'État chinois; remarque que les centres Confucius ont changé de nom en 2020 et sont désormais connus sous le nom de «Centre pour l'éducation et la coopération linguistiques»; souligne l'absence de statut juridique des centres Confucius; invite les États membres et la Commission à soutenir les cours de langue chinoise indépendants, sans implication du Parti communiste chinois et de l'État chinois; estime que le Centre national de la Chine récemment créé en Suède pourrait constituer un atout important pour replacer dans leur contexte les actions et les communications des centres Confucius;

92. considère, en outre, que les centres Confucius servent de plateforme de lobbying pour les intérêts économiques chinois et pour le service de renseignement chinois et le recrutement d'espions; rappelle que de nombreuses universités ont décidé de mettre fin à leur coopération avec les centres Confucius en raison des risques d'espionnage et d'ingérence chinois, comme l'ont fait les universités de Düsseldorf en 2016, de Bruxelles (VUB et ULB) en 2019, et de Hambourg en 2020, ainsi que toutes les universités de Suède;

93. observe que l'ingérence étrangère peut également se faire par une influence dans les instituts religieux, comme l'influence russe dans les églises orthodoxes, en particulier en Serbie et au Monténégro, notamment en semant la division parmi les populations locales, en développant une écriture biaisée de l'histoire et en promouvant un agenda anti-Union, ainsi que l'influence turque, par l'intermédiaire de mosquées en France et en Allemagne; invite la Commission et les États membres à assurer une meilleure coordination en matière de protection des instituts religieux contre les ingérences étrangères;

Dissuasion et sanctions collectives

94. considère que les régimes de sanctions récemment mis en place par l'Union, tels que les mesures restrictives contre les cyberattaques menaçant l'Union et ses États membres[10] et le régime de sanctions mondiales de l'Union en matière de droits de l'homme[11], 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; 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 2021

95. demande à l'Union et à ses États membres de prendre de nouvelles mesures contre la

[10] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ%3AL%3A2019%3A129I%3ATOC
[11] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=OJ:L:2020:410I:TOC

désinformation et les menaces hybrides, dans le strict respect des libertés d'expression et d'information, notamment en mettant en place un régime de sanctions au titre de l'article 29 du traité sur l'Union européenne (le «traité UE») et de l'article 215 du traité sur le fonctionnement de l'Union (mesures restrictives) dans le domaine de l'ingérence étrangère, y compris la désinformation, qui devrait cibler autant que possible les décideurs et les organes responsables d'actions agressives; est d'avis que les pays qui se livrent à l'ingérence étrangère et à la manipulation de l'information dans le but de déstabiliser la situation au sein de 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 Haut Représentant de l'Union pour la politique étrangère et de sécurité à présenter des propositions concrètes à cet égard;

96. 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, un 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;

97. 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, ainsi que pour la consolidation et le soutien de la démocratie, de l'état de droit, des droits de l'homme et des principes du droit international, peut être substantiel en raison de l'ampleur des attaques, de leur nature ou de leur effet cumulatif; estime qu'une analyse plus approfondie de la nature et de l'incidence des menaces et actions individuelles de désinformation et hybrides qui ne relèvent pas du régime de sanctions susmentionné déjà en place pour les cyberattaques doit être effectuée afin de classer les attaques et de définir celles qui ne méritent pas une réponse de l'Union;

98. souligne que l'idée que certaines actions d'ingérence étrangère affectent gravement les processus démocratiques et influencent l'exercice de droits ou de devoirs gagne du terrain au niveau international; souligne, à cet égard, les amendements adoptés en 2018 dans 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»;

99. est conscient que, conformément à l'article 21, paragraphe 3, du traité UE, l'Union doit assurer la cohérence entre les différents domaines de son action extérieure et entre ces politiques et d'autres, 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 terrorisme[12];

100. souligne que, pour renforcer leurs effets, les sanctions devraient être imposées collectivement sur la base d'une coordination avec des partenaires partageant les mêmes

[12] JO L 88 du 31.3.2017, p. 6.

idées, également en ce qui concerne d'autres types de réactions aux attentats, éventuellement avec la participation d'organisations internationales et formalisées dans un accord international; renvoie, en particulier, au communiqué de la réunion de l'OTAN du 14 juin 2021, dans lequel il a été réaffirmé que le Conseil de l'Atlantique Nord déciderait au cas par cas à quel moment une cyberattaque conduirait à l'invocation de l'article 5 du traité de l'OTAN, et que l'incidence d'importantes cyberactivités cumulatives malveillantes pourrait, dans certaines circonstances, être considérée comme équivalant à une attaque armée[13];

Coopération mondiale et multilatéralisme

101. reconnaît que de nombreux pays démocratiques dans le monde sont confrontés à des opérations de déstabilisation similaires menées par des États autoritaires étrangers;

102. souligne la nécessité d'une coopération mondiale entre pays partageant les mêmes idées sur ces questions d'importance cruciale, sous la forme d'un partenariat fondé sur une compréhension commune et des définitions partagées, en vue d'établir des normes et des principes internationaux;

103. estime que, sur la base d'une connaissance commune de la situation, les partenaires partageant les mêmes idées devraient échanger les meilleures pratiques et identifier des réponses communes, y compris des sanctions collectives;

104. demande à l'Union et à ses États membres d'envisager les bons arrangements internationaux qui permettraient un tel partenariat et une telle coopération entre des partenaires partageant les mêmes idées;

105. se félicite de la déclaration de l'OTAN du 14 juin 2021, qui reconnaît le défi croissant 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;

106. se félicite des 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 et partiellement ouvert aux pays tiers partageant les mêmes idées, le mécanisme de réaction rapide établi par le G7 et la Division civilo-militaire Renseignement et sécurité de l'OTAN;

107. souligne que la coopération mondiale devrait être fondée sur des projets communs, impliquant des organisations internationales telles que l'Organisation de coopération et de développement économiques et l'UNESCO, et mettant en place un renforcement des capacités démocratiques dans les pays confrontés à des menaces hybrides similaires en provenance de l'étranger; demande à l'Union de créer un Fonds européen des médias démocratiques pour soutenir le journalisme indépendant dans les pays du voisinage européen;

[13] https://www.nato.int/cps/fr/natohq/news_185000.htm

108. souligne l'importance des pays stratégiques tels que ceux des voisinages orientaux et méridionaux de l'Union et des Balkans occidentaux, car la Russie tente d'utiliser ces pays comme un laboratoire de manipulation de l'information et de guerre hybride; considère que les actions de l'Union peuvent prendre la forme d'un financement de projets visant à garantir la liberté des médias et d'une coopération en matière d'éducation aux médias; attire l'attention sur la nécessité de renforcer les capacités du SEAE à cet égard;

109. invite le Parlement 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;

110. demande au SEAE de renforcer le rôle des délégations de l'Union dans les pays tiers afin de renforcer leur capacité à neutraliser les campagnes de désinformation menaçant les valeurs démocratiques orchestrées par des acteurs étatiques étrangers;

111. demande que la question de l'ingérence étrangère malveillante soit abordée dans le cadre du nouveau guide stratégique de l'Union à venir;

°

° °

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

EXPOSÉ DES MOTIFS

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 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 de l'Union par la connaissance de la situation, l'éducation et la formation aux médias

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 tordu 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 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'étranger[1], 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, ciblant des secteurs stratégiques tels que l'Agence européenne des médicaments (EMA) et le Parlement norvégien.

[1] https://securingdemocracy.gmfus.org/covert-foreign-money/

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 institutions de l'Union

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 par l'appropriation des ressources par les élites, les diasporas nationales, les universités

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 de nombreuses universités et 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 et sanctions collectives

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 définit 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 nº 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 1er 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 M.

- **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

- **Dommages économiques des ingérences et actions de désinformation étrangères, y compris sur le marché des données**, 14 octobre 2021