Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. …
5 mars 2025

Commission des questions politiques et de la démocratie

L'ingérence étrangère : une menace pour la sécurité démocratique en Europe

Rapporteure : M^me^ Zanda KALNIŅA-LUKAŠEVICA, Lettonie, Groupe du Parti populaire européen

Projet de rapport[1]

[1] Renvoi en commission: Doc. 15605, Renvoi 4693 du 25 novembre 2022.

A. Projet de résolution[2]

1. L'ingérence intentionnelle, secrète et manipulatrice de puissances étrangères, de leurs représentants ou d'acteurs privés met en péril la sécurité, les valeurs démocratiques et la gouvernance dans toute l'Europe. Cette ingérence étrangère tend à compromettre la souveraineté, à déstabiliser les systèmes politiques, à affaiblir la confiance du citoyen et à altérer les processus démocratiques. Ces agissements orchestrés, qui sont de plus en plus fréquents et rapides, ciblent les fondements des sociétés européennes et tentent d'exploiter les principes démocratiques comme autant de vulnérabilités systémiques.

2. L'Assemblée parlementaire reconnaît que l'ingérence étrangère, sous ses nombreuses formes, constitue une menace grave et persistante pour la sécurité démocratique. L'Assemblée parlementaire condamne les manœuvres systématiques et intentionnelles d'acteurs étrangers qui cherchent à affaiblir les institutions et mécanismes démocratiques.

3. L'Assemblée constate que les ingérences hostiles provenant de la Fédération de Russie se sont intensifiées depuis le début de son invasion à grande échelle lancée contre l'Ukraine. Cette tendance est illustrée par les efforts considérables qui ont été déployés pour manipuler l'information, financer secrètement des campagnes politiques et acheter des voix lors de l'élection présidentielle et du référendum constitutionnel qui se sont tenus en République de Moldova le 20 octobre 2024. En outre, les actions qui ont perturbé l'élection présidentielle roumaine du 24 novembre 2024, dues à la manipulation de la technologie numérique et de l'intelligence artificielle orchestrée depuis l'étranger, mettent en évidence l'urgente nécessité de renforcer les processus démocratiques face aux menaces hostiles et aux comportements frauduleux coordonnés en ligne.

4. Cette activité s'inscrit dans un schéma plus large qui a inclut des tentatives d'ingérence de la Fédération de Russie dans les processus électoraux et les référendums à travers le continent au cours de la dernière décennie, avec des preuves d'ingérence secrète lors du référendum sur le Brexit de 2016 au Royaume-Uni, de l'élection présidentielle américaine de 2016, du coup d'État de 2017 des dirigeants du gouvernement régional catalan contre l'ordre constitutionnel espagnol, de l'élection présidentielle française de 2017, des élections présidentielles roumaines et moldaves de 2024, et dans la politique allemande.

5. Les démocraties doivent se défendre contre les menaces posées par l'ingérence étrangère et chercher à s'adapter à cet environnement international de plus en plus hostile où les principes de souveraineté, d'autodétermination et de démocratie sont attaqués. La résilience des institutions démocratiques est essentielle pour contrer ces dangers et faire en sorte que les valeurs des droits humains, de la démocratie et de l'état de droit soient respectées.

6. Il est également indispensable de trouver un juste équilibre dans la lutte contre l'ingérence étrangère. En effet, les mesures qui visent à contrer l'influence indue ou à renforcer la transparence doivent être conformes aux normes des droits humains, en particulier celles qui protègent la liberté d'expression, d'association, de réunion, ainsi que la liberté de pensée, de conscience et de religion. Des lois trop restrictives élaborées sans tenir compte de cet équilibre risquent d'étouffer les activités démocratiques légitimes et la liberté d'expression, d'affaiblir la mobilisation de la société civile ou d'être utilisées abusivement à des fins politiques.

7. L'Assemblée souligne que l'édification de sociétés résilientes dotées d'institutions démocratiques fortes, d'une société civile active et éclairée et d'une gouvernance transparente est le moyen le plus efficace de contrer l'ingérence étrangère et de garantir la sécurité démocratique.

8. Les initiatives qui ont pour but d'améliorer la transparence dans la vie publique pour lutter contre l'ingérence étrangère doivent être mises en œuvre de manière à respecter et à préserver les libertés et l'autonomie des organisations de la société civile. Si la sauvegarde des intérêts nationaux est cruciale, les mesures de transparence ne doivent pas servir de prétexte pour imposer des restrictions injustifiées aux acteurs de la société civile, qui jouent un rôle fondamental dans la promotion des valeurs démocratiques, de la responsabilité publique et de la cohésion sociale.

9. L'Assemblée note que le Conseil de l'Europe dispose d'un large éventail de normes et de lignes directrices internationales qui visent à renforcer la résilience démocratique et qui sont pertinentes pour lutter contre l'ingérence étrangère. Il s'agit notamment des mesures dont l'objectif est d'améliorer la transparence et de faire respecter le principe de responsabilité dans la vie publique, des normes et des lignes directrices internationales qui s'appliquent au financement des partis politiques et aux élections, ainsi que des stratégies

[2] Projet de résolution adopté par la commission le 5 mars 2025.

de lutte contre la désinformation. Ces instruments sont renforcés par la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit (STCE n° 225, « la Convention de Vilnius ») qui vise à combler les lacunes juridiques qui peuvent résulter de l'évolution rapide des technologies.

10. L'Assemblée rappelle que, lors de leur quatrième Sommet tenu à Reykjavik en 2023, les chefs d'État et de gouvernement du Conseil de l'Europe ont réaffirmé leur engagement à lutter contre la désinformation, qui constitue une menace pour la démocratie et la paix, d'une manière compatible avec le droit international et le droit à la liberté d'expression et à la liberté d'opinion, ainsi que leur engagement à prendre des mesures appropriées contre l'ingérence dans les systèmes et processus électoraux.

11. L'Assemblée souligne la nécessité de mettre en place des stratégies globales et intégrées pour lutter contre l'utilisation de tactiques d'ingérence étrangères multiformes. Elle recommande l'adoption d'une approche qui mobilise la société et inclut les parlements, les gouvernements, les organismes publics, les pouvoirs locaux, les entreprises privées, les journalistes, la société civile et les citoyens pour renforcer la résilience de la société et contrer les opérations d'ingérence étrangère.

12. Compte tenu de la menace que l'ingérence étrangère fait peser sur la sécurité démocratique, l'Assemblée invite les États membres à :

12.1. intégrer les menaces d'ingérence étrangère dans les cadres de sécurité nationale qui tiennent compte de la nature interconnectée des activités hostiles qui sont menées dans les domaines cybernétique, économique, politique et informationnel ;

12.2. protéger les institutions démocratiques, les infrastructures critiques et les systèmes électoraux contre les cybermenaces ;

12.3. renforcer la coordination entre les organismes de sécurité, tant au niveau national qu'international, afin de détecter et de contrer les activités d'ingérence étrangère ;

12.4. envisager la mise à jour des dispositions législatives et réglementaires afin d'y inclure des infractions qui sont spécifiques à l'ingérence étrangère et qui visent les actions secrètes conduites pour le compte d'acteurs étrangers à des fins de manipulation.

13. Dans le cadre d'une approche qui mobilise la société aux fins d'améliorer la résilience, de renforcer la confiance du citoyen et de protéger l'intégrité des institutions, l'Assemblée appelle les États membres à :

13.1. promouvoir les initiatives d'éducation aux médias numériques, dans le but de contrer la désinformation et de renforcer la résilience des citoyens afin de leur donner les moyens de se prémunir contre la manipulation ;

13.2. introduire l'éducation aux médias numériques dans les programmes scolaires nationaux dès le plus jeune âge afin de développer les compétences essentielles de pensée critique nécessaires pour exercer son jugement, évaluer la crédibilité des sources d'information, identifier les contenus biaisés ou trompeurs, et pour utiliser l'information en ligne de manière critique et efficace ;

13.3. conformément à sa résolution 2192 (2017) intitulée « Les jeunes contre la corruption », élaborer des stratégies d'autonomisation appropriées pour sensibiliser les jeunes à la corruption et leur faire comprendre comment elle sape les sociétés démocratiques ;

13.4. encourager et soutenir les systèmes de contrôle préalable et de vérification des faits, ainsi que les partenariats avec des organisations médiatiques indépendantes et la société civile, afin de combattre la désinformation sans entraver la liberté d'expression ;

13.5. intensifier les action pour mieux protéger les journalistes, sauvegarder la liberté de la presse ainsi que financer et promouvoir le pluralisme et l'indépendance des médias ;

13.6. conformément à la Résolution 2552 (2024) de l'Assemblée, « Renforcer la démocratie par des processus participatifs et délibératifs », encourager une participation citoyenne plus active grâce aux technologies délibératives et aux processus participatifs.

14. Compte tenu des risques posés par la désinformation en tant qu'outil stratégique d'ingérence étrangère pour déformer la réalité, diviser les sociétés et affaiblir les démocraties, l'Assemblée :

14.1. accueille favorablement les principes mondiaux des Nations Unies pour l'intégrité de l'information en ligne, qui est une initiative internationale visant à garantir des espaces d'information plus sûrs et fiables, et demande que des consultations soient tenues avec les citoyens et le secteur privé pour définir les actions nécessaires à leur mise en œuvre ;

14.2. appelle les États membres et observateurs du Conseil de l'Europe qui ne l'ont pas encore fait à signer et ratifier la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit (STCE nº 225, « la Convention de Vilnius»), et à veiller à sa mise en œuvre en tenant dûment compte de l'impact des technologies de l'intelligence artificielle sur la production et la diffusion de la désinformation et de la propagande illégale ;

14.3. invite les États membres à accroître leur expertise et leurs capacités techniques pour lutter contre la désinformation en ligne et faire face aux nouvelles menaces posées par l'intelligence artificielle ;

14.4. appelle les États membres à étudier la mise en place de systèmes de vérification des informations afin de protéger les communautés en ligne contre les contenus électoraux trompeurs générés par l'intelligence artificielle ;

14.5. demande aux plateformes en ligne de fournir des politiques claires sur la publicité politique, l'amplification algorithmique et la suppression de contenus nuisibles ou de désinformation, tout en protégeant la liberté d'expression.

15. Face aux tentatives des acteurs hostiles de s'ingérer de manière inappropriée ou illicite dans les processus démocratiques de prise de décision, l'Assemblée :

15.1. réaffirme sa condamnation du financement massif et dissimulé par la Russie de partis et de responsables politiques dans des États démocratiques, dans le but d'influencer leurs processus démocratiques ;

15.2. appelle les États membres à mettre en place des cadres législatifs et politiques afin de prévenir toute ingérence dans les systèmes électoraux et à mener des enquêtes approfondies sur les allégations d'ingérence dans les élections et les référendums ;

15.3. appelle les États membres à revoir et à renforcer les cadres nationaux qui règlementent les contributions financières aux partis politiques, la publicité et les campagnes électorales afin de réduire le risque d'ingérence financière étrangère inappropriée ou illicite ;

15.4. conformément à sa Résolution 2406 (2021) « Lutte contre la corruption - Principes généraux de la responsabilité politique », invite les gouvernements nationaux à renforcer les mesures de prévention de la corruption et, en application des recommandations du Groupe d'États contre la corruption (GRECO), à adopter et à mettre à jour des codes de conduite pour tous les titulaires d'une fonction publique ;

15.5. encourage les États membres à étudier des mesures visant à accroître la transparence et l'intégrité des activités légitimes d'influence étrangère ;

15.6. encourage les États membres à consulter, à un stade précoce, la Commission européenne pour la démocratie par le droit lors de l'élaboration d'instruments de gouvernance publique visant à renforcer la transparence et l'intégrité des activités d'influence étrangères.

16. Compte tenu de la nécessité d'une action collective pour répondre au défi mondial posé par l'ingérence étrangère, l'Assemblée :

16.1. souligne l'importance de la coopération entre les États membres du Conseil de l'Europe pour faire face à la menace commune que représente l'ingérence étrangère. À cet égard, elle préconise une collaboration plus étroite avec l'Union européenne, l'Organisation pour la sécurité et la coopération en Europe (OSCE), les organes compétents de l'OTAN et d'autres organisations internationales pour élaborer des réponses coordonnées ;

16.2. prône un soutien aux initiatives de réponse rapide multipartites pour recenser les menaces diverses et évolutives qui pèsent sur nos démocraties et y réagir, notamment en partageant des informations et des analyses, et en identifiant les possibilités de réponse coordonnée ;

16.3. est favorable au recours à des sanctions ciblées et coordonnées visant des personnes, des entités et des acteurs étatiques qui se livrent à des ingérences étrangères, notamment des ingérences dans les élections, des manipulations de médias, des financements illicites et des cyberattaques ;

16.4. appelle à un renforcement des moyens juridiques permettant de demander des comptes aux acteurs étrangers et nationaux qui facilitent l'ingérence dans les processus démocratiques ;

16.5. encourage les États membres à évaluer la possibilité d'élaborer une définition large, opérationnelle et non contraignante de l'ingérence étrangère afin d'améliorer la coordination dans la lutte contre les menaces connexes et de préciser la nature des activités d'influence légitimes des États membres ;

16.6. se félicite de la création, à son initiative, de l'Alliance parlementaire pour des élections libres et équitables, qui constitue une avancée majeure permettant de faire face aux nouveaux enjeux qui menacent l’intégrité du processus électoral, de renforcer la coopération avec les partenaires nationaux et internationaux en matière électorale et de promouvoir les normes de référence du Conseil de l'Europe en la matière.

B. Projet de recommandation[3]

1. Renvoyant à sa Résolution xxxx (2025) « L'ingérence étrangère : une menace pour la sécurité démocratique en Europe », l'Assemblée souligne que toute ingérence intentionnelle, secrète et manipulatrice exercée par des puissances étrangères ou leurs représentants constitue une menace permanente pour les principaux fondamentaux de la sécurité démocratique partagés par les États membres du Conseil de l'Europe.

2. Ces ingérences visent à saper les processus électoraux, à éroder la confiance du public dans les institutions démocratiques, l'unité nationale, et à fausser la prise de décisions politiques. L'exemple le plus flagrant de cette menace est l'escalade de l'ingérence hostile de la Fédération de Russie depuis le début de sa guerre d'agression à grande échelle contre l'Ukraine, que l'Assemblée condamne fermement.

3. L'Assemblée estime qu'une réponse coordonnée et globale est nécessaire pour contrer efficacement la menace d'ingérence étrangère, et plaide pour une collaboration plus étroite avec l'Union européenne, l'Organisation pour la sécurité et la coopération en Europe (OSCE) et d'autres organisations internationales.

4. En outre, l'Assemblée souligne que des élections libres et équitables sont la pierre angulaire des sociétés démocratiques. Des processus électoraux indépendants et transparents sont nécessaires à la fois pour la confiance des citoyens dans les institutions publiques et pour la compétitivité de l'environnement électoral. L'Assemblée se déclare gravement préoccupée par le fait que les opérations d'ingérence étrangère, par la manipulation de l'information et des opinions des électeurs, constituent une menace permanente en matière électorale pour la liberté des électeurs de se forger une opinion et pour l'égalité des chances des candidats et des partis.

5. Rappelant les Principes de Reykjavik pour la démocratie, l'Assemblée reconnaît les efforts continus déployés par le Comité des Ministres pour renforcer la résilience démocratique et remédier au recul de la démocratie, notamment ses travaux sur la lutte contre la désinformation, la prévention de la manipulation algorithmique et le renforcement de l'intégrité électorale. Elle salue l'initiative du Secrétaire Général visant à élaborer un Nouveau pacte démocratique pour lutter contre le recul de la démocratie, renforcer l'engagement des citoyens et adapter les modèles démocratiques aux défis contemporains.

6. Face au perfectionnement constant des tactiques multiformes d'ingérence étrangère dans le domaine numérique, l'Assemblée accueille avec satisfaction la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit (STCE n° 225, « la Convention de Vilnius »), qu'elle considère comme un instrument essentiel pour promouvoir la transparence, l'obligation de rendre des comptes et les garanties contre les manipulations et la désinformation induites par l'intelligence artificielle.

7. Compte tenu du rôle joué par le Conseil de l'Europe en faveur de la sécurité démocratique, l'Assemblée demande au Comité des Ministres :

7.1. développer et élaborer des instruments qui contrent l'ingérence étrangère et encouragent l'adoption d'une approche axée sur la mobilisation de la société afin d'améliorer la résilience, de renforcer la confiance du citoyen et de préserver l'intégrité des institutions ;

7.2. d'étudier la possibilité d'élaborer une définition opérationnelle large et non contraignante de l'ingérence étrangère afin d'améliorer la coordination européenne et l'harmonisation des politiques, et de préciser la nature des activités d'influence légitimes.

[3] Projet de recommandation adopté par la commission le 5 mars 2025.

C. Exposé des motifs par Mme Zanda Kalniņa-Lukaševica, rapporteure

1. Introduction

1. La guerre d'agression militaire à grande échelle menée par la Fédération de Russie contre l'Ukraine a marqué un tournant pour la sécurité européenne et a des implications profondes pour la sécurité démocratique en Europe et dans le monde. Cette agression militaire s'inscrit dans le cadre d'une tentative plus large et systématique d'affaiblir la sécurité démocratique bien au-delà de l'Ukraine.

2. Les tactiques employées par la Russie pour saper les démocraties sont bien documentées. Il s'agit des cyberattaques, des campagnes de désinformation, de la subversion politique, des menaces contre les journalistes, des actes de sabotage, de l'instrumentalisation des phénomènes migratoires, de la coercition économique, et de la corruption, qui sont autant de tactiques visant à affaiblir la cohésion interne et la résilience des États démocratiques[4].

3. Ces efforts visent le tissu même des démocraties, cherchant à corroder les institutions et les principes qui ont sous-tendu la paix, la stabilité et la prospérité en Europe depuis la fin de la Seconde Guerre mondiale.

4. Cet éventail d'ingérence étrangère est également utilisé par d'autres acteurs étatiques et non étatiques qui cherchent à remettre en cause les systèmes de gouvernance démocratique libérale. Les menaces n'ont pas seulement pris de l'ampleur en exploitant les nouvelles technologies, elles se sont aussi diversifiées, s'adaptant aux vulnérabilités uniques des différents pays, communautés et régions.

5. En réponse à ces menaces en constante évolution, les États membres du Conseil de l'Europe ont élaboré et mis en œuvre des mesures pour sauvegarder leurs démocraties. Cependant, le défi de l'ingérence étrangère continue d'évoluer, exigeant une vigilance constante, de l'innovation, de la coordination et de la coopération aux niveaux national et international.

6. Les démocraties doivent se défendre contre la menace que représente l'ingérence étrangère dans le cadre d'une adaptation à un environnement international de plus en plus hostile où les principes de souveraineté, d'autodétermination et de démocratie sont attaqués. La nécessité de se défendre contre la menace est attestée par les citoyens européens. En effet, 81% des personnes interrogées dans le cadre d'une enquête Eurobaromètre reconnaissent que l'ingérence étrangère dans le système démocratique européen est un problème grave auquel il faudrait s'attaquer, et 74% répondent que cette ingérence peut influencer le comportement électoral des citoyens[5]. La résistance des institutions démocratiques est cruciale pour contrer ces dangers et garantir que les valeurs des droits humains, de la démocratie et de l'État de droit prévalent. Il importe également que les réponses à l'ingérence étrangère soient guidées par les principes mêmes qu'elles cherchent à défendre.

7. Ce rapport décrit la menace que représente l'ingérence étrangère pour la sécurité démocratique et examine les approches adoptées pour contrer les activités d'ingérence étrangère et renforcer la résilience face à celles-ci.

2. Qu'entend-on par ingérence étrangère ?

8. L'ingérence étrangère peut être décrite comme hostile, secrète, manipulatrice et intentionnelle, le plus souvent illégitime, de la part de puissances étrangères, de leurs mandataires ou d'acteurs privés, dans le but d'avancer leurs objectifs politiques, économiques ou militaires. Elle menace ou affecte négativement la sécurité, les valeurs, les procédures démocratiques et les processus politiques d'autres États, ainsi que leur capacité à faire face à des situations exceptionnelles.

9. Cette ingérence vise les fondements de nos sociétés, en essayant de transformer les piliers démocratiques en vulnérabilités systémiques, et de retourner les démocraties contre elles-mêmes.

10. Les nations démocratiques se trouvent ainsi confrontées à un défi stratégique de taille. À une époque où l'ordre fondé sur des règles est mis à rude épreuve, les régimes autoritaires capitalisent sur les arènes numériques et non numériques avec des intentions hostiles. Leur objectif premier est d'affaiblir les démocraties de l'intérieur, en érodant l'intégrité des processus de prise de décision et en sapant la confiance du public dans les institutions.

---

[4] Voir, par exemple, United States Senate Committee Print, 115th Congress, Putin's asymmetric assault on democracy in Russian and Europe : Implications for U.S. national security, 2018.
[5] European Commission, Flash Eurobarometer 528, Citizenship and democracy, December 2023 (en anglais).

11. Ces actions malveillantes ont été accélérées par le défi systémique et sociétal que représente la transformation des médias et des écosystèmes d'information et l'affaiblissement du rôle des gardiens traditionnels de la conversation publique, la militarisation des médias sociaux pour la propagation d'opérations d'information sophistiquées constituant une menace potentiellement existentielle pour la sécurité nationale de toutes les démocraties européennes.

12. L'ingérence étrangère peut prendre différentes formes, souvent utilisées en combinaison, notamment :

- l'accaparement des élites ;
- le financement occulte de la vie politique ;
- l'ingérence électorale ;
- la désinformation et la manipulation de l'information étrangère ;
- la coercition économique ;
- le contrôle transnational, la surveillance et la répression des diasporas ;
- la corruption[6].

13. L'ingérence étrangère est une composante essentielle de l'univers plus large des menaces hybrides, qui englobent un mélange de tactiques militaires et non militaires conçues pour déstabiliser les États ciblés et exercer une influence sur eux[7].

14. Le rapport exclut de sa conception de l'ingérence étrangère les opérations cinétiques, telles que les attaques de sabotage, les assassinats et les actions terroristes.

15. Le terme « ingérence étrangère » doit être distingué de celui d'« influence étrangère », car ces deux concepts, bien que liés, impliquent des niveaux d'engagement et d'intention différents. Bien qu'il existe parfois des zones grises entre les deux, l'ingérence étrangère se distingue principalement par sa nature secrète et par son intention de nuire à l'intérêt collectif de l'État en question afin de promouvoir les intérêts d'un gouvernement étranger[8].

16. L'expression « influence étrangère » désigne généralement les efforts manifestes et souvent légitimes déployés par un gouvernement ou une entité étrangère pour influencer les opinions, les politiques ou les actions d'un autre pays. Cette influence peut prendre de nombreuses formes, telles que les engagements diplomatiques, la diplomatie publique, les échanges culturels, le lobbying, et peut également inclure le financement transparent et légal d'organisations et d'organes de presse[9]. L'influence étrangère légitime et manifeste fait naturellement partie des relations internationales, la partie influente poursuivant généralement ouvertement ses intérêts tout en s'engageant avec le pays hôte d'une manière qui respecte sa souveraineté et ses cadres juridiques.

3. Principaux acteurs de l'ingérence étrangère

17. L'attribution de l'ingérence étrangère est complexe en raison des méthodes sophistiquées utilisées pour masquer la source de l'activité, et encore plus compliquée par l'utilisation de mandataires locaux ou d'organisations de façade. Le risque politique d'une fausse attribution et les limites floues entre l'influence légitime et l'ingérence secrète ajoutent au défi posé.

18. Les plateformes en ligne ont été en mesure de repérer les sources les plus fréquentes d'ingérence étrangère, Meta signalant que la Russie était la source numéro un de ces opérations sur leur infrastructure internet depuis 2017, suivie de l'Iran et de la Chine[10].

---

[6] OCDE, Renforcer la transparence et l'intégrité des activités d'influence étrangère en France, 2024, 16.
[7] European Commission, Hybrid Centre of Excellence, The Landscape of Hybrid Threats, A Conceptual Model, 2021.
[8] OCDE, Renforcer la transparence et l'intégrité des activités d'influence étrangère en France, 2024, 11.
[9] Government of Canada, Foreign Interference Commission, Influence and interference: distinctions in the context of diplomatic relations and democratic processes, 2024.
[10] Meta, Second Quarter Adversarial Threat Report, août 2024.

19. Des études menées par des parlements et institutions en Europe, en particulier celles qui ont été réalisées en France[11], en Tchéquie[12], en Estonie[13], en Lettonie[14], et aux Pays-Bas[15], ont montré que la Russie et la Chine représentent les principales menaces d'ingérence étrangère pour les démocraties. En effet, ces deux pays emploient des tactiques qui visent à subvertir et à déstabiliser les sociétés, notamment par des campagnes de désinformation à long terme, la guerre de l'information, des cyberattaques et une série de tentatives visant à contrôler les narratifs à l'étranger, notamment en influençant la recherche universitaire et en s'infiltrant dans les entreprises.

4. L'ingérence étrangère comme menace pour la sécurité démocratique

20. La sécurité démocratique repose sur la protection et le renforcement des principes, institutions et processus essentiels à la gouvernance démocratique, tels que l'État de droit, les droits humains et les élections libres et équitables. Elle comprend la sauvegarde de l'intégrité électorale, la protection des libertés civiles et la promotion d'une citoyenneté éclairée et engagée[16].

21. Les régimes autoritaires cherchent de plus en plus, et avec une efficacité croissante, à affaiblir l'intégrité des normes et des institutions établies qui protègent les libertés fondamentales. Les moyens des acteurs de l'ingérence étrangère, tels que la corruption, la désinformation, l'accaparement des élites et l'ingérence électorale, visent à saper chacun des piliers de la sécurité démocratique.

22. Ces régimes ont activement alimenté et exploité les clivages qui existent au sein des états membres du Conseil de l'Europe en utilisant ces formes d'ingérence. Ils ont notamment apporté un soutien financier à des groupes extrémistes qui amplifient les récits clivants, radicaux et parfois violents. Ils ont également financé des mouvements et des hommes politiques afin de saboter toute forme d'opposition unie à des acteurs hostiles, tout en affaiblissant les projets et l'influence démocratiques[17].

23. Les stratégies de déstabilisation visant à éroder les normes démocratiques et à amplifier la polarisation ont pour but d'affaiblir la confiance dans le système politique, ce qui, à son tour, nuit à la capacité de répondre efficacement à des défis plus vastes.

24. Des élections libres et équitables sont la pierre angulaire des sociétés démocratiques. Des processus électoraux indépendants et transparents sont indispensables à la fois pour la confiance des citoyens dans nos institutions publiques et pour la compétitivité de l'environnement électoral. Les activités d'ingérence étrangère constituent un risque permanent car elles visent à manipuler l'information et l'opinion des électeurs, à lancer des cyberattaques sur les infrastructures, à organiser l'accès à des informations sensibles provenant de gouvernement, de partis politiques et de membres du parlement, et à faciliter la fuite de ces données.

25. Cette menace en constante évolution et adaptation reste difficile à mesurer, et l'effet cumulatif de ses manifestations sur nos démocraties n'est pas encore pleinement compris. Les progrès rapides et l'adoption généralisée de l'intelligence artificielle (IA) ont le potentiel d'exacerber de manière significative les défis auxquels sont confrontées les démocraties pour faire face à l'ingérence étrangère, et les réponses devront s'adapter en fonction de ces progrès.

5. Cibles multiples et tactiques multiformes

26. Il existe de nombreux exemples très médiatisés d'activités d'ingérence étrangère menaçant la sécurité et la stabilité démocratiques. Ces activités peuvent être regroupées en trois grandes catégories : la désinformation, les cyberattaques et le piratage, ainsi que l'ingérence financière et politique.

27. Elles sont souvent employées simultanément pour produire un effet négatif cumulatif en ciblant systématiquement les piliers de la sécurité démocratique. La désinformation sape l'intérêt général, la confiance dans la crédibilité des médias, du gouvernement et même des faits eux-mêmes. Les cyberattaques

[11] Assemblée nationale française, *Rapport fait au nom de la Commission d'enquête relative aux ingérences politiques, économiques et financières de puissances étrangères visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français*, 2023.
[12] BIS, Security Information Service, Annual report, 2023.
[13] Estonia Foreign Intelligence Service, International Security and Estonia, 2024.
[14] Republic of Latvia, Constitution Protection Services, Annual Report, 2023.
[15] AIVD, Annual Report, 2023.
[13] Voir, par exemple, Conseil de l'Europe, Secrétaire Général, Situation de la démocratie, des droits de l'homme et de l'Etat de droit en Europe, 2015.
[17] Rekawek, Kacper, Thomas Renard, and Bàrbara Molas, ed(s)., Russia and the Far-Right: Insights from Ten European Countries, International Centre for Counter-Terrorism, 2024.

compromettent les données sensibles, perturbent les services essentiels et renforcent la désinformation en provoquant la fuite sélective de documents qui alimentent des contenus clivants. L'ingérence financière et politique érode l'intégrité institutionnelle et accroît le cynisme du public à l'égard de la gouvernance.

28. L'ensemble crée une boucle de rétroaction. Les cyberattaques fournissent du matériel de désinformation et un moyen de pression sur les personnalités dont les données ont été compromises, tandis que l'ingérence financière et politique amplifie la méfiance créée par les cyberattaques et les campagnes de désinformation. L'effet cumulatif de ces éléments peut mettre en évidence des vulnérabilités systémiques et créer ainsi des brèches que les acteurs hostiles peuvent exploiter pour manipuler et déstabiliser les sociétés ciblées.

5.1. Désinformation

29. Selon le Comité des Ministres du Conseil de l'Europe, la « désinformation » désigne les informations dont on peut vérifier qu'elles sont fausses, inexactes ou trompeuses, créées et diffusées dans l'intention délibérée de causer un préjudice ou d'obtenir un avantage politique ou économique en trompant le public[18].

30. Si la désinformation n'est pas une nouveauté dans la conduite des relations internationales, l'avènement des technologies numériques en a accru la portée à des niveaux sans précédent. Les campagnes de désinformation consistent à diffuser des informations fausses ou trompeuses - généralement par le biais de médias contrôlés par l'État, de médias sociaux ou de canaux clandestins - afin de façonner l'opinion publique, d'aggraver les clivages politiques nationaux sur des sujets sensibles ou de porter atteinte à la crédibilité d'institutions, de processus ou d'individus spécifiques.

31. Les campagnes de désinformation sont devenues un phénomène courant, en particulier lors des campagnes électorales ou référendaires. Les irrégularités dans les processus électoraux dues à l'ingérence étrangère illustrent l'influence croissante des menaces numériques sur les scrutins. En décembre 2024, la Cour constitutionnelle roumaine a annulé le résultat du premier tour des élections présidentielles après avoir constaté qu'il y avait eu une violation des « principes essentiels des élections démocratiques libres ». Elle a ensuite exigé que les élections soient entièrement réorganisées par le gouvernement à une date ultérieure[19]. La Cour a rendu sa décision à la suite de la déclassification de documents des services de renseignement révélant qu'un candidat avait profité d'une vaste opération d'influence orchestrée de l'étranger. L'ingérence aurait permis de manipuler les votes et de fausser l'égalité des chances entre les candidats grâce à l'usage des technologies numériques et de l'intelligence artificielle.

32. Pour parvenir à cette décision, la Cour constitutionnelle a estimé que les États devaient faire preuve de résilience face aux défis et aux risques qui sont générés par les campagnes de désinformation organisées qui affectent l'intégrité des processus électoraux. Elle a jugé que la liberté des électeurs de se forger une opinion incluait le droit d'avoir accès à des informations exactes sur les candidats et le processus électoral, ainsi qu'une protection contre des actes ou des faits illégaux et disproportionnés qui exercent une influence injustifiée sur leur comportement électoral. La Cour a précisé que la publicité électorale en ligne doit toujours être identifiée comme telle et être transparente, tant en ce qui concerne l'identité du commanditaire qu'en ce qui concerne les moyens techniques de diffusion[20].

33. Les médias financés par l'État sont un vecteur essentiel de désinformation, comme en témoignent les chaînes russes Sputnik et RT, ainsi que le réseau chinois Global Television Network. Ces médias sont sous le contrôle permanent, direct ou indirect, d'autorités étatiques et contribuent à la propagation systématique de fausses informations.

34. Des documents internes de politique étrangère émanant d'acteurs hostiles indiquent clairement que cette désinformation est une action stratégique. Le ministère russe des Affaires étrangères, par exemple, appelle à une « campagne d'information offensive » dans les « sphères politico-militaires, économiques, commerciales et psychologiques informationnelles[21] ».

35. En 2017, un rapport commandé par le Conseil de l'Europe a considéré que l'utilisation accrue de la désinformation était l'un des éléments d'un désordre de l'information plus large[22]. Même lorsque des

[18] Recommandation CM/Rec(2022)12 du Conseil de l'Europe sur la communication électorale et la couverture médiatique des campagnes électorales, 6 avril 2022.
[19] Cour constitutionnelle de Roumanie, Décision n° 32, 6 décembre 2024.
[20] Cour constitutionnelle de Roumanie, Décision no 32, 6 décembre 2024.
[21] Résolution, Conseil du ministère des Affaires étrangères de la Fédération de Russie, 11 avril 2023.
[22] Conseil de l'Europe (2017), Les désordres de l'information : Vers un cadre interdisciplinaire pour la recherche et l'élaboration des politiques, 2017. (en anglais)

campagnes de désinformation sont révélées et démenties, l'accumulation continue de fausses informations contribue à affaiblir la confiance dans l'environnement médiatique. En effet, selon une étude de l'OCDE, seules 39 % des personnes interrogées déclarent avoir une confiance élevée ou modérée dans les médias d'information, tandis que 44 % expriment une confiance faible, voire inexistante, à leur égard[23].

36. Les réseaux de désinformation, qui ont proliféré à la suite de la guerre d'agression de grande ampleur menée par la Fédération de Russie contre l'Ukraine, ont pour but d'amplifier les récits pro-Kremlin sur les plateformes de médias sociaux, aussi bien en Europe que dans le monde.

37. Les opérations d'influence menées par la Russie reposent sur des tactiques similaires à celles qui sont observées dans l'affaire « DoppelGänger », dans laquelle des acteurs malveillants ont créé des sites internet imitant des médias reconnus ou des sites gouvernementaux de pays membres du Conseil de l'Europe. Des récits de désinformation ont ensuite été publiés sur ces sites factices afin de leur donner une apparence d'authenticité et diffusés sur les réseaux sociaux par le biais d'un réseau de faux comptes[24].

38. Entre le 24 février 2022 et octobre 2023, la surveillance menée dans six pays (Allemagne, Italie, Pologne, Tchéquie, Slovaquie et Hongrie) a permis de constater la diffusion de plus de 13 000 messages de désinformation regroupés autour de récits pro-russes importants[25].

39. Des États hostiles utilisent des bots et l'intelligence artificielle pour diffuser rapidement des récits de désinformation et les amplifier dans le but d'accroître la pression des populations locales sur les décideurs et de propager des informations erronées sur les actions illégales perpétrées par la Russie en Ukraine.

40. Des études menées par l'agence française VIGINUM ont montré qu'entre septembre et décembre 2023, un réseau de 200 portails de désinformation convertissait des informations fausses et trompeuses dans les langues du public cible[26].

41. Des données de Microsoft indiquent que la désinformation ou la propagande d'origine chinoise a été déployée à une « échelle inégalée par d'autres acteurs d'influence malveillants », grâce à l'utilisation de milliers de comptes sur un éventail de plateformes internet diffusant des mèmes, des vidéos et des articles en plusieurs langues[27].

42. Des opérations de désinformation ont également cherché à exploiter des questions sensibles dans les pays cibles pour exacerber les clivages sociaux. Qualifiées de « parasites », ces opérations exploitent de manière opportuniste des contenus existants ou des informations erronées au niveau national, en les amplifiant à l'aide de bots. Elles visent à aggraver les tensions sur certaines questions et à favoriser la propagation de points de vue extrêmes. La dynamique entre la désinformation étrangère et la mésinformation nationale peut avoir un effet catalyseur sur les groupes nationaux. Cette situation, qui a été observée pendant la pandémie de Covid-19, a contribué à l'hésitation vaccinale et aux théories du complot sur la pandémie,[28] et à accélérer les tensions internes liées aux flux migratoires ou à la sécurité du processus électoral.

43. Ces campagnes de désinformation ont parfois été menées de concert avec d'autres actions hybrides, notamment en ce qui concerne l'instrumentalisation des flux migratoires dans le but de déstabiliser les démocraties européennes. Les stratégies hybrides d'ingérence étrangère ont inclus le transport de migrants et de demandeurs d'asile par le Bélarus et la Russie jusqu'aux frontières de la Pologne, de la Lituanie, de la Lettonie et de la Finlande. Le soutien de campagnes de désinformation puis l'exploitation de migrants, de minorités et de diasporas sont autant de vecteurs pour des campagnes de désinformation malveillantes. L'objectif est d'amplifier et d'exploiter les perceptions négatives existantes à l'égard des migrations, ce qui a pour effet d'exacerber les tensions au sein des sociétés européennes.

[23] OCDE, Enquête de l'OCDE sur les déterminants de la confiance dans les institutions publiques – résultats 2024, 10 juillet 2024.
[24] EU Disinfo Lab, Doppelganger – Media Clones Serving Russian Propaganda, 27 September 2022.
[25] VoxCheck, Investigation into Russian Falsehoods in Europe, 16 November 2023.
[26] VIGINUM, Rapport Technique, Février 2024.
[27] Microsoft, Digital Defense Report, October 2023.
[28] EEAS, Special Report, Short Assessment of Narrative and Disinformation around the COVID-19 Pandemic, April 2021.

5.2. Cyberattaques et piratage

44. Les technologies numériques sont devenues omniprésentes dans tous les aspects de la vie moderne, notamment dans l'administration, la défense, les infrastructures critiques et l'économie. C'est pourquoi il existe désormais une convergence de plus en plus manifeste entre les opérations d'ingérence étrangères menées dans le cadre de campagnes de désinformation et les cyberattaques lancées ou parrainées par des États en tant que vecteur d'ingérence.

45. Les cyberattaques et les tentatives de piratage qui ciblent les institutions publiques perturbent l'accès aux sites internet publics et compromettent les comptes de courrier électronique des fonctionnaires. Outre la menace qu'elles font peser sur la fourniture de services essentiels et la sécurité publique, ces activités exposent les réseaux publics à des acteurs hostiles, compromettent les communications des responsables publics et influencent les processus démocratiques. Rien qu'en 2024, des cyber-opérations hostiles en Europe ont été publiquement attribuées à des pirates informatiques pro-Kremlin, notamment en Tchéquie, en Allemagne, en Grèce, en Pologne et en Suisse[29].

46. Les menaces qui pèsent sur les élections en raison d'ingérences étrangère comprennent le piratage des courriels des candidats, une pratique qui a été utilisée lors de l'élection présidentielle américaine de 2016[30] et de l'élection présidentielle française de 2017, ainsi que des tentatives d'affaiblir les infrastructures électorales elles-mêmes, notamment les cyberattaques en Ukraine en 2014, en Macédoine du Nord en 2019 et en République de Moldova en 2019[31].

47. En décembre 2023, le Royaume-Uni a dénoncé une tentative d'ingérence cybernétique russe dans les processus politiques. Ces opérations, qui ciblaient des parlementaires, s'appuyaient sur des campagnes d'hameçonnage ciblé, le piratage et la fuite de documents commerciaux entre le Royaume-Uni et les États-Unis, ainsi que sur des ingérences visant des groupes de réflexion britanniques sur la défense de la démocratie contre la désinformation[32].

5.3. Ingérence financière et politique

48. L'accaparement et la corruption des élites sont une autre forme insidieuse d'ingérence étrangère susceptible de porter atteinte à la sécurité démocratique. La cooptation d'élites politiques, économiques ou médiatiques clés pour promouvoir les intérêts d'un État étranger se fait au détriment de la souveraineté nationale et des normes démocratiques. Elle diminue l'efficacité et la légitimité des institutions et érode l'État de droit.

49. Les tentatives alléguées de pays étrangers tels que le Qatar d'influencer les députés, les anciens députés et le personnel du Parlement européen par des actes de corruption représenteraient une grave ingérence dans les processus démocratiques européens[33]. Le Parlement européen a également souligné, dans une Résolution de 2024, l'existence d'allégations crédibles selon lesquelles certains de ses membres auraient reçu des paiements pour relayer de la propagande russe[34].

50. Le Parlement européen, vivement préoccupé par les nouvelles allégations indiquant que la Russie financerait des partis politiques dans le but de s'ingérer dans les processus internes de certaines démocraties européennes, a décidé d'ouvrir une enquête approfondie sur un éventuel soutien étranger aux mouvements séparatistes. Cette demande fait suite à des allégations selon lesquelles des émissaires liés à la Russie auraient rencontré des dirigeants indépendantistes catalans en 2017 et leur auraient proposé une aide financière massive en échange d'une législation favorable aux cryptomonnaies[35].

51. Ces préoccupations ont également suscité des appels à une plus grande transparence sur le financement des partis politiques. Une enquête a révélé que les partis populistes, d'extrême droite et d'extrême

---

[29] Voir, par exemple, GMF, Alliance for Securing Democracy, Authoritarian Interference Tracker.
[30] U.S. Department of Justice, Special Counsel Robert S. Mueller, Report on the investigation into Russian interference in the 2016 Presidential election, 2019.
[31] Hybrid Centre of Excellence, Countering hybrid threats to elections, 2024.
[32] United Kingdom Foreign, Commonwealth & Development Office, Press release, 7 December 2023.
[33] Résolution du Parlement européen du 1er juin 2023 sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (2022/2075(INI)).
[34] Résolution du Parlement européen du 25 avril 2024 sur les nouvelles allégations d'ingérence russe au Parlement européen, dans les prochaines élections européennes et incidence sur l'Union (2024/2696(RSP); & David E. Alandete "Russian Interference in the Catalan Independence Crisis (2014-2022)".
[35] Résolution du Parlement européen du 1er juin 2023 sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (2022/2075(INI)).

gauche ont reçu un quart de l'ensemble des financements privés alloués aux partis politiques dans l'Union européenne entre 2019 et 2022[36]. Par ailleurs, des informations provenant de services de renseignement indiquent que la Russie a versé 300 millions de dollars entre 2014 et 2022 afin d'influencer des responsables politiques et officiels dans 24 pays[37].

52. En mars 2024, la Tchéquie a sanctionné le site d'information Voice of Europe, basé à Prague, après des allégations indiquant qu'il aurait payé des hommes politiques dans plusieurs pays européens afin de répandre un sentiment anti-ukrainien et d'influencer les élections du Parlement européen tenues en juin dans le cadre d'une opération d'influence russe[38].

53. Des ingérences financières étrangères ont également ciblé des électeurs avant les élections. Les autorités moldaves ont constamment tiré la sonnette d'alarme concernant les tentatives de la Fédération de Russie de s'ingérer dans la politique intérieure et les processus électoraux de la République de Moldova en 2024. Elles signalent un afflux massif d'argent russe destiné à acheter des voix et de subvertir le processus démocratique[39].

54. L'inspection générale de la police de la République de Moldova a recensé des cas de corruption impliquant 130 000 citoyens et plus de 15 millions de dollars de transferts illicites en provenance de Russie pour le seul mois de septembre 2024[40]. Des estimations indiquent que l'ampleur des programmes d'achat de votes est certainement beaucoup plus élevée dans l'ensemble. En effet, les fonds étaient ventilés dans divers programmes, notamment les allocations « sociales » pour les retraités et les « primes » salariales pour les employés des structures des pouvoirs locaux[41].

6. La réponse

55. Le Conseil de l'Europe, ses États membres et les organisations internationales ont mis au point une série d'instruments pour prévenir, détecter, contrer et sanctionner la menace multiforme que représente l'ingérence étrangère.

6.1. Mettre à jour les concepts de sécurité

56. L'agression à grande échelle de l'Ukraine par la Fédération de Russie et son caractère hybride ont montré qu'il était urgent pour les démocraties de réactualiser leurs concepts de sécurité nationale.

57. Les États membres ont donc cherché à modifier les stratégies qui intègrent des actions visant à faire face au risque posé par l'accélération des opérations d'ingérence étrangère. Ainsi, l'Allemagne a adopté sa toute première stratégie de sécurité nationale[42]. Fondé sur une conception large de la sécurité, ce document vise à apporter des réponses globales aux divers défis de notre époque en matière de sécurité. Il va bien au-delà des questions traditionnelles de politique de défense et porte sur des sujets allant du développement de la coopération à la défense contre les cyber-risques.

58. Des entités ont été mises en place pour s'adapter aux activités des acteurs hostiles, notamment l'agence nationale VIGINUM, créée en France en 2021, qui est un service de vigilance et de protection contre les ingérences numériques étrangères. Son rôle est de détecter les menaces en ligne qui cherchent à nuire aux intérêts fondamentaux de la France.

59. En 2023, la France et la Slovénie, en partenariat avec le Monténégro, ont fondé le Centre de cybercapacités des Balkans occidentaux afin de renforcer les capacités qui permettront de faire face aux cyberattaques et de contrer la désinformation en ligne menées par des acteurs étrangers qui cherchent à provoquer l'instabilité dans la région[43].

60. Un mois après le début de la guerre d'agression de la Fédération de Russie contre l'Ukraine, le Conseil de l'Union européenne a approuvé la Boussole stratégique qui définit une vision stratégique commune de la

[36] Follow the Money, Follow the Money, Transparency Gap: The funding of political parties in the EU, 2024.
[37] BBC, Russia covertly spent $300m to meddle abroad – US, 14 September 2022.
[38] Ministère des Affaires étrangères de la Tchéquie, Communiqué de presse, 28 mars 2024.
[39] Assemblée Parlementaire, Communiqué de presse, 5 juillet 2024.
[40] IPN, $15 million transferred from Russia for corrupting voters in Moldova, 3 October 2024.
[41] Atlantic Council, What to know about Russian malign influence in Moldova's upcoming election, 18 October 2024.
[42] National Security Strategy | BMVg.de.
[43] Statement, Cyber security – Signing of the treaty on the Western Balkans Cyber Capacity Centre, 16 October 2024.

politique de sécurité et de défense de l'UE au cours des cinq à dix prochaines années[44]. Son intitulé exact « Pour une Union européenne qui protège ses citoyens, ses valeurs et ses intérêts, et qui contribue à la paix et à la sécurité internationales » est assez évocateur. Ce document, qui évalue l'environnement stratégique commun, décrit les menaces complexes auxquelles l'UE est confrontée en matière de sécurité :

- des menaces hybrides dont la fréquence et l'impact augmentent ;
- l'instrumentalisation de la puissance douce, sachant que les vaccins, les données et les technologies sont utilisés comme instruments de compétition politique ;
- la multiplication des tentatives de coercition économique et énergétique.

61. Parmi les instruments prévus par la Boussole stratégique figure une boîte à outils hybride de l'UE qui rassemble différents instruments visant à détecter un large éventail de menaces hybrides et à y réagir ; celle-ci inclut une boîte à outils spécifique destinée à lutter contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger. L'Union européenne disposait déjà d'un éventail d'options pour la mise en œuvre de la boîte à outils hybride de l'Union européenne, telles que la boîte à outils de cyberdiplomatie[45], mais la valeur ajoutée de la boîte à outils hybride est de permettre une réponse rapide, cohérente et coordonnée, en rassemblant une combinaison d'instruments civils et militaires[46]. Le Conseil de l'Union européenne a approuvé en mai 2024 le cadre directeur pour la mise en place pratique d'équipes de réaction rapide de l'Union européenne dans le domaine des technologies hybrides, qui peuvent être déployées sur demande pour se préparer à faire face aux menaces hybrides et les contrer[47].

62. En juin 2022 à Madrid, l'OTAN a adopté un nouveau concept stratégique, qui rappelle que « les concurrents stratégiques mettent à l'épreuve notre résilience et cherchent à exploiter l'ouverture, l'interconnexion et la numérisation de nos pays [...] Ces acteurs sont également à l'avant-garde d'un effort délibéré visant à saper les normes et les institutions multilatérales et à promouvoir des modèles de gouvernance autoritaires »[48]. Des efforts ont été demandés pour développer la résilience face à l'ingérence étrangère et aux menaces hybrides qui pèsent sur les Alliés de l'OTAN et les pays qui aspirent à devenir membres de l'Alliance, et pour les contrer.

6.2. Développer la résilience sociétale

63. Les menaces hybrides étant appelées à continuer d'influer sur le paysage sécuritaire, le développement de la résilience de la société face aux ingérences étrangères nécessite une approche globale de l'ensemble de la société. Il a été démontré que les manœuvres visant à influencer les élections depuis l'étranger sont plus susceptibles de se produire en manipulant des électeurs sur le long terme qu'en attaquant directement le système électoral. Les mesures de protection doivent donc être résolument axées sur la résistance globale de la population à l'influence étrangère[49].

64. Il est impératif de développer la résilience de la société face à l'ingérence étrangère pour préserver les institutions démocratiques et garantir l'intégrité des processus électoraux. Cela implique des stratégies à multiples facettes englobant l'éducation, la maîtrise des médias et la culture de la pensée critique chez les citoyens pour discerner et contrer la désinformation. Il est essentiel de sensibiliser le public aux tactiques utilisées par les acteurs étrangers pour diffuser de faux récits, en particulier par le biais des plateformes de médias sociaux.

65. La Finlande a intégré l'éducation aux médias dans son programme scolaire national dès le plus jeune âge, ce qui a permis aux élèves d'acquérir des compétences essentielles pour s'orienter dans le paysage complexe de l'information d'aujourd'hui. Les écoles finlandaises apprennent aux enfants à évaluer la crédibilité des différentes sources d'information, à identifier les contenus trompeurs ou biaisés et à comprendre les motivations des campagnes de désinformation[50] L'Estonie et la Lettonie ont cherché à améliorer l'éducation aux médias en s'employant respectivement à renforcer la résistance de leurs populations russophones face à la manipulation de l'information, en offrant des alternatives aux médias russes, en interagissant avec leur

[44] Conseil de l'Union européenne, Une boussole stratégique pour renforcer la sécurité et la défense de l'UE au cours de la prochaine décennie (europa.eu).
[45] The EU Cyber Diplomacy Toolbox (cyber-diplomacy-toolbox.com).
[46] European Parliament, NATO supports Hybrid Toolbox - Sundsvall Idag.
[47] Conseil de l'UE, Communiqué de presse, Menaces hybrides, 21 mai 2024.
[48] OTAN, Communiqué de presse, Menaces hybrides: le Conseil ouvre la voie au déploiement d'équipes d'intervention rapide en cas de menaces hybrides, 29 juin 2022.
[49] https://www.hybridcoe.fi/wp-content/uploads/2023/09/20230912-Hybrid-CoE-Rapport-de-Recherche-10-PEI-WEB.pdf
[50] OCDE, Les faits sans le faux : Lutter contre la désinformation, renforcer l'intégrité de l'information, 2024, 73.

minorité russophone,[51] et en soutenant et formant le journalisme indépendant dans des instituts tels que le Centre balte pour l'excellence des médias, basé à Riga.

66. En outre, la promotion d'un paysage médiatique diversifié et indépendant qui respecte l'intégrité journalistique et les pratiques de vérification des faits peut atténuer la propagation de la désinformation. La collaboration entre les gouvernements, les organisations de la société civile et les plateformes technologiques est essentielle à la mise en œuvre de stratégies efficaces pour identifier, contrer et sensibiliser à l'ingérence étrangère. L'autonomisation des communautés, y compris des minorités et des groupes vulnérables souvent ciblés par les campagnes de désinformation, par le biais d'initiatives inclusives et informatives, contribuera de manière significative à renforcer la résilience de la société face aux manipulations extérieures et à préserver le tissu démocratique des nations.

67. Le Centre commun de recherche de la Commission européenne et le Centre d'excellence pour les technologies hybrides ont proposé une méthodologie pour un mécanisme de résilience complet, qui vise à fournir un système de détection des signaux précoces, à faciliter l'analyse des menaces hybrides et à identifier les trajectoires de réponse potentielles[52].

68. Les États nordiques et baltes appliquent le concept de « défense totale », qui prévoit d'impliquer l'ensemble de la société - forces armées et société civile - dans les actions visant à prévenir, dissuader et contrer une attaque. En 2018, l'Agence suédoise de la protection civile et de la gestion de crises (MSB) a adressé une brochure à tous les ménages, contenant des lignes directrices indiquant aux citoyens comment se protéger contre les fausses informations, les cyberattaques et bien d'autres menaces[53].

6.3. Lutte contre la désinformation

69. Le renforcement de la résilience sociétale pour lutter contre l'ingérence étrangère fait partie d'un ensemble d'outils plus large pour une capacité de lutte contre la désinformation efficace et fructueuse. Si la lutte contre la désinformation doit protéger la liberté d'expression et l'accès à l'information, les États ont intensifié leurs efforts pour contrer la désinformation en perturbant les acteurs de l'ingérence étrangère, en repérant préalablement les fausses informations et en corrigeant les contenus.

70. Dans le cadre des méthodes de perturbation, les autorités étatiques ont identifié et démantelé des fermes de robots diffusant de la désinformation, comme les réseaux de désinformation basés en Russie opérant aux États-Unis d'Amérique qui ont été fermés en juillet 2024[54], et la cyberpolice en Ukraine qui ont suspendu les activités de 13 fermes de robots avec plus de 1,5 million de faux comptes de médias sociaux qui étaient enregistrés pour diffuser de la désinformation et de la propagande[55]. Les plateformes en ligne ont également pris des mesures contre les efforts coordonnés visant à manipuler le débat public à des fins stratégiques, où les faux comptes sont au cœur de l'opération. Meta a identifié 39 opérations d'influence secrètes de la Russie entre 2017 et 2024, les autres sources les plus fréquentes d'opérations d'influence secrètes émanant de l'Iran et de la Chine[56].

71. Afin de faire face aux risques liés à l'utilisation des technologies d'intelligence artificielle pour générer de fausses informations ou amplifier la diffusion de contenus manipulatoires visant à compromettre l'intégrité de l'information, la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit (STCE n° 225, « la Convention de Vilnius ») prévoit que les signataires doivent appliquer des mesures qui garantissant que les systèmes d'intelligence artificielle ne sont pas utilisés pour saper l'intégrité, l'indépendance et l'efficacité des institutions et des processus démocratiques, et qu'ils protègent ces processus, y compris la capacité de se forger librement une opinion[57].

72. Les gouvernements ont de plus en plus utilisé les communications stratégiques pour anticiper et démystifier (pré-bunk) la désinformation en déclassifiant des renseignements. Les États-Unis ont notamment utilisé cette approche pour dévoiler le processus décisionnel russe avant l'invasion de l'Ukraine par la Russie en février 2022, et pour affaiblir de manière significative les narratifs russes.

---

[51] IFES, Building Resilience Against Election Influence Operations: Preparing for the European Elections in 2024 and Beyond, 2024.
[52] Commission européenne, Hybrid Threats: A Comprehensive Resilience Ecosystem, 2023.
[53] Countering information influence activities : A handbook for communicators (msb.se.
[54] US Department of Justice, Press release, 9 July 2024.
[52] Cyber Police of Ukraine, communiqué de presse, 20 décembre 2022.
[53] Voir, par exemple, Meta, Second Quarter Adversarial Threat Report, août 2024.
[57] Rapport explicatif de la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, 5 octobre 2024.

73. Plusieurs pays européens ont amélioré la coordination intergouvernementale. L'Allemagne a mis en place un groupe de travail interministériel dirigé par le ministère fédéral de l'Intérieur et du Territoire pour favoriser une coopération étroite sur les réponses à apporter aux menaces hybrides, en particulier la désinformation. Ce groupe de travail coordonne toutes les activités menées contre la diffusion délibérée d'informations fausses et trompeuses dans le contexte de la guerre menée contre l'Ukraine, y compris le renforcement de la communication proactive et transparente ainsi que l'amélioration de la résilience de la société face aux menaces ciblant l'espace informationnel[58].

74. Les efforts visant à contrer la désinformation par la correction de contenu ont vu se développer un réseau d'organisations indépendantes et non partisanes de vérification des faits, qui travaillent souvent en collaboration avec les médias et les plateformes numériques pour identifier et corriger les fausses informations. Ces vérificateurs de faits publient souvent les informations corrigées de manière visible et veillent à ce que les fausses informations soient non seulement démystifiées, mais aussi remplacées par des récits factuels.

75. Le Comité directeur sur les médias et la société de l'information du Conseil de l'Europe a adopté en décembre 2023 une Note d'orientation sur la lutte contre la propagation de la mésinformation et de la désinformation en ligne par des solutions de vérification des faits et de conception de plateformes dans le respect des droits humains. Cette note montre que la vérification des faits joue un rôle central dans le débat public et appelle à l'indépendance des organisations de vérification des faits à l'égard des États[59].

76. À l'échelle mondiale, les Nations Unies ont lancé en 2024 les Principes mondiaux des Nations Unies pour l'intégrité de l'information, qui visent à lutter contre la désinformation, la mésinformation et les discours de haine tout en défendant les droits humains, y compris la liberté d'expression[60]. Ces principes s'adressent à une série de parties prenantes et s'articulent autour de la confiance et de la résilience de la société, de l'autonomisation du public, de l'indépendance, de la liberté et du pluralisme des médias, ainsi que de la transparence.

77. Au niveau de l'Union européenne, une approche globale a été adoptée, dont la loi sur les services numériques qui oblige les plateformes numériques à assumer une plus grande responsabilité quant au contenu qui apparaît sur leurs services. Les obligations les plus strictes de la loi s'appliquent aux très grandes plateformes en ligne et aux moteurs de recherche, qui sont considérés comme des plateformes en ligne et des intermédiaires qui comptent plus de 45 millions d'utilisateurs par mois dans l'UE. Ces plateformes doivent identifier et traiter tous les risques systémiques qu'elles représentent, notamment ceux qui sont liés aux droits fondamentaux, à la sécurité publique et aux élections.

78. Des groupes de travail spécialisés ont été créés, tels que le groupe de travail East StratCom, afin d'exposer et de démystifier les récits de désinformation, tandis que des projets visant à améliorer l'éducation aux médias ont complété ces efforts afin de renforcer la résistance à long terme à la désinformation.

79. À l'échelle nationale, la création d'agences et d'institutions pour lutter contre la menace s'est accélérée. L'Agence suédoise de défense psychologique, créée en 2022, joue un rôle crucial dans la protection de l'environnement informationnel de la Suède et dans la résilience de sa société face aux interférences étrangères. L'Agence joue un rôle opérationnel et dispose d'un mandat pour renforcer la résilience de la société contre les ingérences étrangères. L'Agence de défense psychologique identifie, analyse et soutient la lutte contre les informations malveillantes et autres informations trompeuses dirigées contre la Suède ou ses intérêts par des puissances étrangères antagonistes. Il peut s'agir de désinformation visant à affaiblir la résilience de la Suède et la volonté de la population de se défendre, ou à influencer indûment les perceptions, les comportements et les décisions des citoyens.

80. Plusieurs pays européens ont mis en place des commissions d'enquête spéciales chargées de lutter contre l'influence russe. Par exemple, en mai 2024, la Commission d'enquête sur l'influence russe et bélarusse a été créée en Pologne sur ordre du Premier ministre. La Commission, qui relève du ministre de la Justice, enquêtera sur les cas d'influence de la Russie et du Bélarus sur la politique polonaise depuis 2004.

81. Ces dernières années, des efforts accrus ont été déployés pour établir des partenariats entre les gouvernements, les plateformes en ligne et les services répressifs. Le Code de bonnes pratiques sur la

[58] Rapport annuel 2022 du Mécanisme de réponse rapide du G7.
[59] Conseil de l'Europe, Note d'orientation sur la lutte contre la propagation de la mésinformation et de la désinformation en ligne par le biais de la vérification des faits et de la conception de plateformes dans le respect des droits humains, 2024. (en anglais)
[60] United Nations, Global Principles for information integrity: Recommendations for multi-stakeholder action, June 2024.

désinformation de 2022, élaboré par l'Union européenne en collaboration avec les principales plateformes en ligne, les plateformes émergentes et spécialisées, les acteurs de l'industrie publicitaire, les vérificateurs de faits, ainsi que des organisations de recherche et de la société civile, vise à renforcer la vérification des faits, à limiter les incitations financières à la diffusion de la désinformation et à lutter contre les comportements manipulateurs tels que les faux comptes, les bots ou les hypertrucages (deep fakes) malveillants.

82. Afin de perturber l'écosystème de désinformation russe, l'Union européenne a suspendu les activités de diffusion et les licences de plusieurs organes de désinformation soutenus par le Kremlin. Ces médias ont été utilisés par le gouvernement russe pour manipuler l'information et promouvoir la désinformation sur l'agression militaire contre l'Ukraine, y compris la propagande visant à déstabiliser les pays voisins de la Russie, l'UE et ses États membres.

83. Observant que Sputnik et Russia Today étaient sous le contrôle permanent, direct ou indirect, des autorités de la Fédération de Russie et qu'ils jouaient un rôle essentiel et déterminant dans le déclenchement et le soutien de l'agression militaire contre l'Ukraine, l'Union européenne a expliqué sa décision par le fait que « La Fédération de Russie a entrepris une campagne internationale systématique de désinformation, de manipulation de l'information et de distorsion des faits afin de renforcer sa stratégie de déstabilisation des pays voisins, de l'UE et de ses États membres. (...) Pour justifier et soutenir son agression militaire contre l'Ukraine, la Fédération de Russie a lancé des actions continues et concertées de désinformation et de manipulation de l'information à destination des membres de la société civile dans l'UE et les pays voisins, en faussant et en manipulant gravement les faits[61]. »

84. Les personnes associées à la diffusion de la propagande et de la désinformation ont également été sanctionnées. Par exemple, l'Union européenne a sanctionné la rédactrice en chef de RT, Margarita Simonyan, accusée d'être une figure centrale de la propagande gouvernementale russe responsable d'actions et de politiques compromettant l'intégrité territoriale, la souveraineté et l'indépendance de l'Ukraine.

85. L'effet de la suspension des activités de diffusion au cours des six premiers mois suivant leur annonce initiale en 2022 s'est traduit par une diminution de 100 % des visites provenant des moteurs de recherche vers les médias sanctionnés, une baisse de 70 % des consultations en provenance des réseaux sociaux et une réduction de 74 % du trafic internet en provenance de l'UE[62]. Les recours en justice contre l'interdiction de RT ont été rejetés, car la suspension était une mesure proportionnée contre le soutien actif à une politique de déstabilisation plus large susceptible de constituer une menace significative et directe pour l'ordre public et la sécurité[63].

6.4. Garantir la transparence de l'influence étrangère

86. La gestion effective des conflits d'intérêts, du lobbying et du financement politique est particulièrement importante pour faire face aux vulnérabilités aux risques d'ingérence étrangère et à son effet déstabilisateur sur la démocratie[64]. Les inquiétudes concernant l'influence étrangère sur les affaires intérieures et l'opinion publique ont conduit un certain nombre de pays à travers le monde à adopter une législation visant à garantir une plus grande transparence comme première étape de la prévention des menaces.

87. En ce qui concerne la transparence et la réglementation des dons aux partis politiques et aux campagnes électorales, le Comité des Ministres du Conseil de l'Europe a demandé en 2003 aux États membres de limiter, d'interdire ou de réglementer spécifiquement les dons provenant de donateurs étrangers[65].

88. L'Assemblée parlementaire a condamné toutes les tentatives d'ingérence inappropriée ou illicite dans les processus décisionnels démocratiques d'autres États par le biais de contributions financières aux partis politiques et aux campagnes électorales. Elle a appelé les États membres à revoir leurs réglementations

[61] L'UE impose des sanctions aux médias publics RT/Russia Today et Sputnik, qui diffusent dans l'UE - Consilium (europa.eu)..
[62] Institute for Strategic Dialogue, Effectiveness of the Sanctions on Russian State-Affiliated Media in the EU, October 2022.
[63] Voir, par exemple, CJUE, arrêt du Tribunal général, RT France contre Conseil, (T-125/22), 27 juillet 2022.
[64] OCDE, Perspectives sur la lutte contre la corruption et l'intégrité, 2024
[65] Recommandation Rec(2003)4 du Comité des Ministres sur les règles communes contre la corruption dans le financement des partis politiques et des campagnes électorales, 8 avril 2003.

régissant les contributions financières aux partis politiques et aux campagnes électorales provenant de sources étrangères afin de réduire le risque d'ingérence financière étrangère inappropriée ou illicite[66].

89. L'Assemblée a également invité les gouvernements nationaux à renforcer les mesures de prévention de la corruption et à adopter et mettre à jour des codes de déontologie pour tous les titulaires d'une fonction publique[67].

90. En 2023, le Groupe d'États contre la corruption (GRECO) du Conseil de l'Europe a lancé une procédure de suivi sur le thème de la transparence du financement des partis afin d'améliorer le cadre juridique dans ce domaine et de veiller à ce que tous ses États membres disposent désormais d'une législation en la matière. Les recommandations du GRECO issues de son 4ème cycle d'évaluation concernaient la prévention de la corruption des parlementaires, juges et procureurs. Il s'agit notamment d'établir des codes d'éthiques pour les parlementaires incluant des normes de conduite professionnelle applicables et partagées par le public, d'améliorer la transparence et de réduire la vulnérabilité des parlementaires à une influence indue.

91. Le 22 mars 2022, le Conseil de l'Union européenne est parvenu à un accord politique sur la refonte du règlement relatif au statut et au financement des partis politiques européens et des fondations politiques européennes. Cette révision vise à améliorer la transparence des partis politiques européens et à renforcer le cadre de leur financement, notamment pour contrer les risques d'ingérence et de manipulation étrangères[68].

92. Les États ont pris une série de mesures supplémentaires pour améliorer la transparence des liens entre les personnes physiques ou morales opérant dans l'espace public et menant des activités d'influence au nom d'intérêts étatiques étrangers. Ces mesures peuvent renforcer l'intégrité des activités d'influence étrangères, permettre aux décideurs et aux citoyens de savoir quels intérêts sont défendus et établir une distinction plus claire entre les activités d'influence légitimes et les tentatives d'ingérence illégitimes[69].

93. Un des premiers exemples de ces efforts est la loi sur l'enregistrement des agents étrangers (Foreign Agents Registration Act - FARA), introduite aux États-Unis en 1938 pour contrer la propagande nazie. Bien qu'elle ait subi d'importantes modifications, cette loi est toujours en vigueur. Elle a pour objectif de repérer les influences étrangères aux États-Unis et de faire face aux menaces pesant sur la sécurité nationale. La loi impose aux personnes menant des actions politiques ou quasi-politiques en tant qu'agents d'entités principales étrangères de publier régulièrement leurs liens avec l'entité concernée. Les activités qui en découlent doivent également être communiquées[70].

94. En mars 2023, le Canada a annoncé l'ouverture de consultations visant à jeter les bases d'un registre des agents étrangers, à la suite d'articles de presse faisant état d'une ingérence présumée de la Chine dans les deux dernières élections du pays[71].

95. L'Australie l'avait déjà fait en 2018, après que des rapports des services de renseignement eurent décrit les vastes opérations d'influence menées par la Chine à tous les niveaux du gouvernement au cours de la décennie précédente, y compris des millions de dollars de dons politiques et des préoccupations concernant la surveillance et la manipulation des ressortissants chinois en Australie par le Parti communiste chinois[72].

96. En 2023, le gouvernement britannique a présenté le Foreign Influence Registration Scheme (FIRS), qui vise à renforcer la résilience du système politique britannique face à l'influence étrangère secrète et à fournir une plus grande assurance quant aux activités de certaines puissances ou entités étrangères qui représentent un risque pour la sécurité nationale. Le FIRS exige l'enregistrement des accords visant à mener des activités d'influence politique au Royaume-Uni sous la direction d'une puissance étrangère. Le niveau renforcé du FIRS donne au secrétaire d'État le pouvoir d'exiger l'enregistrement d'un éventail plus large d'activités pour certains pays, parties de pays ou entités contrôlées par un gouvernement étranger, lorsque cela est nécessaire pour protéger la sécurité et les intérêts du Royaume-Uni[73].

---

[66] Résolution 15302 (2021), « Transparence et réglementation des dons de sources étrangères en faveur de partis politiques et de campagnes électorales », 31 mai 2021.
[67] Résolution 2406 (2021) Lutte contre la corruption — Principes généraux de la responsabilité politique, 26 novembre 2021.
[68] Le Conseil de l'UE avance vers un financement plus transparent des partis politiques européens - Consilium (europa.eu).
[69] OCDE, Renforcer la transparence et l'intégrité des activités d'influence étrangère en France, 2024., 2024.
[70] ; Foreign Agents Registration Act (FARA): A Legal Overview (fas.org). Foreign Agents Registration Act | Foreign Agents Registration Act (justice.gov)
[71] Canada starts setting up foreign agent registry amid reports of Chinese election meddling | Reuters.
[72] What's in Australia's New Laws on Foreign Interference in Domestic Politics - Lawfare (lawfareblog.com)..
[73] Foreign Influence Registration Scheme factsheet - GOV.UK (www.gov.uk).

97. La Commission européenne, dans le cadre de son paquet « Défense de la démocratie » a proposé une nouvelle directive sur la transparence de la représentation d'intérêts pour le compte de pays tiers en décembre 2023,[74] et a organisé des consultations publiques sur une proposition qui visait à harmoniser les exigences relatives aux activités économiques de la représentation d'intérêts exercée pour le compte d'entités de pays tiers[75]. Cette proposition viendrait renforcer le registre de transparence déjà existant[76].

98. Les normes en matière de droits humains doivent guider l'élaboration et la mise en œuvre des lois de transparence relatives à l'influence étrangère afin de protéger les libertés fondamentales, notamment la liberté d'expression, la liberté d'association et la vie privée. La Commission de Venise du Conseil de l'Europe a admis que le financement étranger d'associations « peut susciter certaines préoccupations légitimes »[77], mais les mesures restrictives en matière de financement doivent être strictement nécessaires et proportionnées à l'objectif légitime. La liberté d'association est un droit humain fondamental qui est essentiel au fonctionnement d'une démocratie, et les associations telles que les groupes d'intérêt, les syndicats et les partis politiques sont tous des éléments cruciaux d'un État démocratique.

99. Le plein respect des normes internationales dans l'élaboration des instruments de transparence est essentiel pour éviter les restrictions injustifiées à la société civile et les effets négatifs sur le débat public ouvert et informé, le pluralisme et la démocratie. Il est de la plus haute importance que ces lois soient élaborées sur la base d'un processus de consultation inclusif, qu'elles comprennent des définitions précises et qu'elles prévoient des obligations claires et des sanctions proportionnées. L'environnement général de la démocratie, des droits humains et de l'État de droit ainsi que les discours qui s'y rapportent sont également des éléments clés à prendre en considération dans le cadre de l'évaluation de ces textes législatifs.

100. L'Assemblée a rappelé que les organisations non gouvernementales sont une composante indispensable d'une société ouverte et démocratique et qu'elles apportent une contribution essentielle au développement et à la réalisation de la démocratie, de l'État de droit et des droits humains. Elle s'est déclarée préoccupée par le fait que des États membres ont eu recours à une législation imposant des obligations excessives en matière de rapports et de divulgation publique aux ONG recevant des fonds de l'étranger, afin de stigmatiser ces organisations, et a donc appelé les États membres à se conformer aux normes juridiques internationales en ce qui concerne les droits à la liberté de réunion, d'association et d'expression[78].

101. Le risque d'abus d'une telle législation a été démontré par la loi russe sur les « agents étrangers », promulguée en 2012 et élargie par la suite. Elle a été utilisée comme un outil de répression pour limiter la liberté d'expression, persécuter les personnalités de l'opposition et réprimer les organisations de défense des droits humains. Quelque 200 organisations ont été enregistrées en tant qu'agents étrangers entre 2012 et février 2021. En février 2022, 73 organisations figuraient encore sur la liste, les autres ayant soit fermé leurs portes, soit été retirées de la liste. La portée excessivement large et discriminatoire du régime juridique n'a pas été jugée nécessaire dans une société démocratique[79].

7. Coopération internationale

102. L'ingérence étrangère dépasse souvent les frontières nationales, les acteurs étatiques et non étatiques exploitant les plateformes numériques, les réseaux financiers et les alliances transnationales pour perturber les processus démocratiques. Une collaboration est nécessaire au niveau international afin de renforcer les capacités de détection, de dissuasion et de réponse à l'ingérence étrangère de manière cohérente, solide et conforme aux normes internationales. Un certain nombre d'initiatives ont été lancées entre des États partageant les mêmes idées afin de répondre à la menace et de fournir une plateforme pour cette collaboration.

7.1. Le *Centre européen d'excellence pour la lutte contre les menaces hybrides, Helsinki*[80]

[74] Commission européenne, proposition de directive du Parlement européen et du Conseil établissant des exigences harmonisées dans le marché intérieur en matière de transparence de la représentation d'intérêts exercée pour le compte de pays tiers et modifiant la directive (UE) 2019/1937.
[75] EU 'foreign agents' law spooks NGOs – POLITICO.
[76] Registre de transparence (europa.eu).
[77] CDL-AD(2014)046, Lignes directrices conjointes sur la liberté d'association, paragraphe 221.
[78] Résolution 2362, Restrictions aux activités des ONG dans les États membres du Conseil de l'Europe, 27 janvier 2021.
[76] Cour européenne des droits de l'homme, *Ecodefence et autres c. Russie*, nos 9988/13 et 60 autres, 14.06.2022 ; Commission de Venise, Avis sur la compatibilité avec les normes internationales en matière de droits de l'homme d'une série de projets de loi introduit par la Douma d'État Russe entre le 10 et 23 novembre 2020 pour modifier les lois concernant les « agents étrangers », 2-3 juillet 2021.
[80] About us - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats...

103. Le Centre d'excellence européen pour la lutte contre les menaces hybrides (CdE hybride) est une organisation internationale autonome, basée sur un réseau, qui promeut une approche de l'ensemble du gouvernement et de l'ensemble de la société pour lutter contre les menaces hybrides.

104. La participation aux activités du Centre est ouverte à tous les pays de l'Union européenne et de l'OTAN, et le nombre d'États participants est passé à 36 en novembre 2024. Le Centre a pour mission de renforcer la sécurité des États et organisations participants en leur fournissant des compétences et une formation pour contrer les menaces hybrides. La vision du Centre est celle d'un monde dans lequel nos sociétés ouvertes et démocratiques fonctionnent à l'abri de toute ingérence extérieure malveillante.

105. La tâche principale du Centre est de renforcer les capacités des États participants à prévenir et à contrer les menaces hybrides. Il y parvient en partageant les meilleures pratiques, en formulant des recommandations et en testant de nouvelles idées et approches. Le Centre développe également les capacités opérationnelles des États participants en formant des praticiens et en organisant des exercices pratiques.

106. Le CdE hybride élabore de nouveaux concepts stratégiques et contribue à leur mise en œuvre par l'intermédiaire de ses réseaux intergouvernementaux et intersectoriels, qui comptent plus de 1 500 praticiens et experts travaillant dans les États participants, l'Union européenne et l'OTAN, le secteur privé et le monde universitaire.

7.2. Centres d'excellence de l'OTAN

107. Deux centres d'excellence accrédités par l'OTAN jouent un rôle important dans la lutte contre l'ingérence étrangère. Ces centres sont soutenus par des groupes d'experts internationaux issus de l'armée, des gouvernements, des universités et des milieux intéressés.

108. Le Centre d'excellence de l'OTAN pour la cyberdéfense en coopération (CCD COE), situé à Tallinn, a été établi à la suite de la cyberattaque menée en 2007 contre l'Estonie. Il s'agit d'un pôle de connaissances accrédité par l'OTAN qui offre une approche interdisciplinaire unique des questions les plus pertinentes en matière de cyberdéfense. Il mène des recherches, des formations et des exercices dans quatre domaines essentiels : la technologie, la stratégie, les opérations et le droit.

109. Le Centre d'excellence pour les communications stratégiques de l'OTAN (Stratcom COE), situé à Riga, a été créé en 2014. Il s'est imposé comme un pôle de recherche et d'information sur le thème de la communication stratégique, qui englobe la lutte contre la désinformation, la sécurité numérique et les méthodologies des acteurs hostiles.

7.3. Le G7

110. Dans le communiqué de Capri d'avril 2024, les ministres des affaires étrangères du G7 se sont engagés à protéger l'environnement de l'information et les valeurs démocratiques contre toute tentative de manipulation étrangère. Il s'agissait notamment de renforcer la résistance et la sensibilisation du public à la manipulation de l'information venant de l'étranger[81].

111. Le mécanisme de réaction rapide du G7 (MRR) est une initiative introduite dans l'« Engagement de Charlevoix sur la défense de la démocratie contre les menaces étrangères », publié par les dirigeants du G7 - États-Unis, Canada, Japon, Royaume-Uni, France, Allemagne et Italie - en juin 2018, lors de leur sommet à Charlevoix, au Québec. Le MRR a pour mandat de renforcer la coordination des pays membres du G7 « pour identifier et répondre aux menaces diverses et évolutives qui pèsent sur nos démocraties, notamment en partageant des informations et des analyses, et en identifiant les possibilités de réponse coordonnée »[82]. Il publie un rapport annuel qui identifie les défis et tendances dans le domaine de la désinformation affectant le G7.

8. Conclusions

112. Les États membres du Conseil de l'Europe sont confrontés à un environnement sécuritaire qui se détériore et dans lequel les menaces hybrides et l'ingérence étrangère sont de plus en plus importantes. Ces menaces, qui dépassent les préoccupations traditionnelles en matière de sécurité, ont évolué au point de pouvoir exploiter les vulnérabilités de la société et de remettre en cause les valeurs fondamentales de notre mode de vie, telles que la démocratie, la primauté du droit et les droits humains. En conséquence, l'ingérence

[81] Communiqué de la réunion des ministres des Affaires étrangères du G7, Capri, 19 avril 2024.
[82] Rapport annuel 2021 du Mécanisme de réponse rapide du G7.

étrangère représente une menace directe non seulement pour la sécurité démocratique des États membres individuels, mais aussi pour la préservation de la paix et de la stabilité.

113. La lutte contre l'ingérence étrangère malveillante est une tâche intrinsèquement complexe pour plusieurs raisons. Elle est tout d'abord une menace qui évolue en adoptant des formes diverses qui dépendent des progrès technologiques. La diversité des tactiques ne permet pas de reconnaître et de définir aisément la nature de l'ingérence.

114. En outre, il est difficile d'identifier et d'attribuer précisément l'ingérence. Les tactiques secrètes et l'utilisation d'acteurs par procuration ne permettent pas de faire aisément la distinction entre les activités qui sont menées localement et celles qui sont orchestrées par des acteurs étrangers hostiles. Des acteurs nationaux contribuent à la diffusion de récits de désinformation, que ce soit de manière autonome ou en collaboration avec des entités étrangères, ce qui rend la répartition des responsabilités encore plus difficile à établir. Il n'est pas non plus aisé de mesurer le véritable impact de cette ingérence car ses effets peuvent être subtils, progressifs et difficiles à quantifier. Elle contribue néanmoins à l'érosion de la confiance du citoyen et de la cohésion sociale au fil du temps.

115. Compte tenu de ces complexités, les réponses effectives doivent être multiformes et s'appuyer sur une série de mesures visant à renforcer la résilience et à sauvegarder les valeurs démocratiques. Il est donc essentiel d'élaborer une réponse qui mobilise la société afin de renforcer la résilience citoyenne, en commençant par des campagnes d'éducation numérique et de sensibilisation à grande échelle qui aident les citoyens à identifier et à contrer la désinformation. Il est également indispensable de renforcer la protection des vérificateurs de faits, de la société civile et des journalistes d'investigation, qui jouent un rôle crucial dans la dénonciation de la désinformation et de l'influence étrangère.

116. De nombreux États ne disposent pas d'une législation sur les menaces hybrides ou la désinformation, ou d'une définition appropriée, et ne sont donc pas armés sur le plan légal ou réglementaire pour les combattre efficacement. Par conséquent, il existe un écart important entre la nature de la menace et la capacité des gouvernements à la contrer efficacement par des moyens légaux[83].

117. Le *Media Pluralism Monitor* 2022 de l'Institut universitaire européen a constaté que 15 des 32 pays analysés (y compris les 27 États membres de l'UE) disposaient d'une forme de cadre réglementaire pour lutter contre la désinformation. Cependant, seuls les cadres mis en place en Finlande, en Allemagne et en Lituanie ont été jugés efficaces[84].

118. Lors de l'élaboration de réponses politiques à l'ingérence étrangère, il est impératif que toutes les mesures prises soient conformes aux normes établies en matière de droits humains. Si la menace que représente l'ingérence étrangère est bien réelle et pressante, il est essentiel que les réponses ne portent pas atteinte aux principes mêmes qu'elles visent à protéger. Les droits humains, l'État de droit et les libertés démocratiques doivent rester au premier plan de toute stratégie de lutte contre l'ingérence. Cette approche non seulement renforce la légitimité des contre-mesures, mais elle distingue également les réponses démocratiques des tactiques secrètes, souvent répressives, utilisées par les acteurs hostiles.

119. Les mesures qui ne tiennent pas compte des droits humains risquent de produire un effet contre-productif, car elles peuvent éroder la confiance du public et lui laisser penser que le gouvernement a des pouvoirs excessifs. Par exemple, si la surveillance numérique ou les restrictions qui s'appliquent aux canaux d'information peuvent sembler efficaces à court terme, ces actions doivent être soigneusement évaluées afin d'éviter qu'elles portent atteinte à la liberté d'expression, à la vie privée et au droit d'accès à l'information. Des procédures transparentes, le respect de la légalité et le respect des droits individuels doivent guider toutes les mesures de répression prises pour contrer les activités de désinformation ou de déstabilisation.

120. En veillant à ce que ces mesures soient guidées par les normes des droits humains, les États membres du Conseil de l'Europe peuvent favoriser l'adoption d'une approche équilibrée et effective qui garantit à la fois la sécurité nationale et protège les droits démocratiques de leurs citoyens.

[83] Hybrid CoE, Research Report 10, Preventing election interference: Selected best practices and recommendations, 2023.
[84] EUI, Media Pluralism Monitor, 2022.