Conférence européenne des **Présidentes et Présidents de Parlement**
European Conference of **Presidents of Parliament**
Rome, 15-16 octobre 2026 / 15-16 October 2026

Démocraties résilientes: unies face aux menaces hybrides

Document d'information

«Des puissances étrangères instrumentalisent nos vulnérabilités en se dissimulant derrière un discours démocratique. Elles les exacerbent par la technologie et l'intelligence artificielle et les financent par les cryptomonnaies. Elles ne se contentent plus d'attaquer nos institutions, mais portent atteinte à notre souveraineté même.»
Maia Sandu, Présidente de la République de Moldova, 2025

«La sécurité commence par la démocratie»,
Alain Berset, Secrétaire Général du Conseil de l'Europe, 2026

«Aujourd'hui, la sécurité de l'Europe est mise à mal non seulement par des moyens militaires, mais aussi par des menaces hybrides – désinformation, chantage à l'énergie et cyberattaques. La défense de notre sécurité démocratique est notre responsabilité commune.»
Ruslan Stefanchuk, Président de la Verkhovna Rada, 2025

1. Introduction

1. Dans le contexte géopolitique actuel, marqué par une instabilité et une incertitude croissantes, la notion traditionnelle de **sécurité** subit une profonde transformation. Les menaces hybrides se multiplient et deviennent de plus en plus sophistiquées, amplifiées par les progrès technologiques. Les États hostiles et les acteurs non étatiques exploitent l'ouverture et les vulnérabilités des sociétés démocratiques pour semer la division, aggraver la polarisation et saper la confiance du public dans les institutions et les processus démocratiques.

2. Les menaces hybrides ne sont pas des incidents isolés. Elles s'inscrivent plutôt dans une stratégie délibérée qui vise à affaiblir la résilience démocratique et à déstabiliser les sociétés de l'intérieur. Comme le Conseil de l'Europe l'a déjà souligné, «[l'ingérence étrangère] n'est pas un phénomène marginal ou de courte durée, mais un défi structurel pour la sécurité démocratique et la sécurité nationale qui appelle des réponses institutionnelles, politiques et juridiques appropriées, fondées sur le respect des droits humains, de la démocratie et de l'État de droit»[1].

2. Une menace à plusieurs dimensions

3. **La manipulation de l'information et l'ingérence étrangères (FIMI)** constituent le type de menace hybride le plus répandu et le plus nuisible. La FIMI peut prendre la forme de **campagnes de désinformation**, c'est-à-dire la conduite d'actions coordonnées destinées à diffuser des informations fausses ou trompeuses, en particulier pendant les périodes de troubles politiques ou d'élections. La propagande, les réseaux de bots et les fausses informations sont déployés avec précision pour diviser et induire en erreur. Une autre forme de FIMI est **l'amplification sur les réseaux sociaux**, par laquelle des algorithmes et des réseaux de bots augmentent la visibilité de contenus faux ou clivants afin d'éclipser les informations objectives. Certains acteurs envoient également des messages ciblés à des groupes, à des partis ou à des communautés vulnérables, destinés à influencer leurs opinions ou à provoquer la discorde (**opérations d'influence ciblées**). Les études montrent régulièrement que les femmes engagées dans la vie publique – femmes politiques, journalistes ou responsables de la société civile – sont visées de manière disproportionnée par ce type d'opérations, qui utilisent les insultes sexistes, les contenus à caractère sexuel et les attaques contre la réputation comme moyens d'intimidation politique. Ces actes constituent non seulement une violation des droits humains, mais aussi une menace structurelle pour la participation démocratique, avec des effets dissuasifs avérés sur la volonté des femmes de se présenter aux élections ou de participer au débat public.

---

[1] Étude de faisabilité du Conseil de l'Europe sur un instrument juridique traitant de la manipulation de l'information et de l'ingérence menées depuis l'étranger (FIMI), CM/Inf(2026)18.

4. Si la FIMI n'est pas en soi un phénomène nouveau, les avancées technologiques numériques ont indéniablement introduit une nouvelle dynamique. Les fournisseurs de services en ligne, notamment les plateformes de réseaux sociaux, permettent désormais la diffusion rapide et à grande échelle de contenus manipulés, d'une manière qui était auparavant impossible. L'intelligence artificielle (IA) accroît encore la vitesse, la portée et le degré de sophistication de ces activités. Le Forum économique mondial classe la désinformation et la désinformation parmi les risques à court terme les plus graves, juste derrière l'instabilité géoéconomique[2].

5. **Les menaces hybrides** visent généralement des infrastructures critiques essentielles à la sûreté publique, à la sécurité et à la stabilité économique. Ces menaces peuvent inclure le sabotage, les cyberattaques, le brouillage de signaux, les incursions de drones et d'autres activités illicites – souvent menées par des individus ou des groupes intermédiaires locaux délibérément recrutés ou manipulés à cette fin. Ce type d'actions visent à tester, perturber ou saper la résilience des sociétés démocratiques.

6. Des expériences récentes montrent qu'un large éventail d'activités peuvent être détournées à des fins hostiles – du vol de données à caractère personnel à la perturbation des services essentiels, des flux migratoires, de l'énergie, de l'approvisionnement alimentaire ou du commerce. La liste n'est pas exhaustive.

3. Lutter contre la FIMI

7. La FIMI est un élément central de l'arsenal des menaces hybrides utilisées contre les sociétés démocratiques, mais des lacunes et des obstacles structurels entravent encore notre capacité à y faire face. L'un des principaux écueils est l'absence de compréhension commune de la FIMI. Chaque pays a des définitions et des seuils différents, et tous n'ont pas la même perception de ses liens avec des menaces hybrides plus larges. De plus, on observe d'importantes disparités dans leurs capacités institutionnelles. Si certains États disposent de structures spécialisées et de mécanismes de coordination, d'autres s'appuient sur des dispositifs fragmentés, ce qui nuit à l'apport de réponses harmonisées et efficaces.

8. Les approches politiques sont souvent réparties sur différents secteurs tels que les médias, la cybersécurité, la gouvernance et le droit pénal, ce qui limite la cohérence et la coopération intersectorielle. L'absence de méthodologies, d'indicateurs ou d'outils d'analyse comparative communs rend difficile l'évaluation de la résilience et restreint les échanges paneuropéens de bonnes pratiques.

9. La FIMI étant par nature transfrontalière, les différences entre les cadres juridiques, les perceptions des menaces, les pratiques de partage d'informations et les capacités institutionnelles peuvent compliquer la coopération internationale à cet égard. D'autres difficultés découlent des interactions avec les plateformes numériques, du développement rapide de l'IA et de la manipulation des technologies émergentes.

10. Les vulnérabilités financières et l'exposition à la corruption peuvent faciliter les activités d'ingérence. Les écarts entre les cadres de droit pénal et les définitions juridiques peuvent faire obstacle aux enquêtes et à la coopération judiciaire. Enfin, bien que les instruments juridiques internationaux en vigueur soient pertinents, ils n'ont pas été spécifiquement conçus pour la FIMI, ce qui donne lieu à une mise en œuvre et à une efficacité inégales entre les États membres.

11. Conscientes de l'omniprésence de la FIMI, de ses effets perturbateurs et de l'importance d'apporter une réponse coordonnée, les organisations européennes se sont astreintes à élaborer des stratégies solides.

12. Avec la conceptualisation de son **Nouveau Pacte Démocratique pour l'Europe**[3], le Conseil de l'Europe a adopté une approche globale qui accorde une importance notable à la défense de la démocratie contre la FIMI[4]. À la suite d'une étude de faisabilité approfondie sur l'élaboration éventuelle d'un instrument du Conseil de l'Europe pour lutter contre la FIMI, le Comité des Ministres a demandé au Secrétaire Général de présenter des propositions pour la négociation d'un instrument juridique approprié, y compris une éventuelle convention-cadre, lors de sa réunion à Chisinau en mai 2026. Un tel instrument permettrait de combattre la FIMI en s'appuyant sur l'expertise et les normes du Conseil de l'Europe[5].

[2] Rapport de 2026 sur les risques mondiaux, Forum économique mondial.
[3] Vers une Résilience Démocratique – Le Nouveau Pacte Démocratique pour l'Europe.
[4] Rapport 2026 – Secrétaire Général.
[5] Décision CM.

13. Par ailleurs, l'Union européenne a mis au point une approche globale pour lutter contre la FIMI, qui combine coordination politique, analyse opérationnelle, réglementation et protection des droits. Avec le **Bouclier européen de la démocratie**[6], l'UE cherche à améliorer l'appréciation de la situation et à renforcer les institutions démocratiques, la liberté des médias et la résilience de la société. Le Centre européen pour la résilience démocratique[7] soutient le partage d'expertise et de bonnes pratiques, tandis que la boîte à outils FIMI[8] aborde la communication stratégique, l'attribution publique, l'action diplomatique, le soutien aux médias indépendants, les initiatives d'éducation aux médias, les mécanismes d'alerte précoce, la coopération internationale et, si nécessaire, la prise de sanctions.

4. Les élections, un pilier essentiel

14. Les élections sont une infrastructure clé des systèmes démocratiques, car elles sont le moyen fondamental par lequel s'établit la légitimité des institutions et s'exercent les droits démocratiques. L'intégrité, la légitimité et la crédibilité aux yeux du public des processus électoraux sont donc indispensables à la stabilité et à la résilience de la gouvernance démocratique.

15. Depuis quelques années, les élections sont devenues la cible privilégiée des menaces hybrides. Dans certains cas, l'ingérence étrangère a été directement documentée; dans d'autres, l'environnement électoral a été touché par un écosystème plus large de désinformation, de campagnes manipulatrices en ligne, d'influence illicite, de cybermenaces et de manipulation de l'information au niveau national. Ces activités ne visent pas tant à modifier le résultat final des élections qu'à affaiblir la confiance du public dans l'équité et la légitimité du processus électoral lui-même.

16. Les récentes missions d'observation électorale de l'APCE ont fait état de niveaux sans précédent d'ingérence étrangère dans les élections. Cette ingérence s'est manifestée de diverses façons: l'exercice de pressions économiques (comme la restriction de l'accès à l'énergie et les menaces contre les chaînes d'approvisionnement), le financement politique occulte (notamment le soutien à des groupes intermédiaires et à des réseaux d'achat de voix) et la guerre de l'information (par exemple, la diffusion de désinformation et de *deepfakes* (ou hypertrucages), ainsi que la publication de messages ciblés et de discours polarisants sur les réseaux sociaux). Il convient de noter que la technologie des *deepfakes* a été utilisée de manière disproportionnée contre les candidates et les élues, notamment sous la forme d'images à caractère sexuel fabriquées de toutes pièces et de scandales mensongers. Il s'agit d'un mode d'ingérence électorale clairement lié au genre dont l'effet dissuasif sur la participation des femmes à la vie politique mérite d'être explicitement reconnu et de faire l'objet de recours juridiques ciblés.

17. Les méthodes hybrides combinent souvent cyberattaques, coercition économique, financement illicite et manipulation de campagnes. Ces tactiques visent à influencer l'opinion publique et à exercer un levier géopolitique à long terme. Les observateurs ont également signalé l'utilisation de l'intelligence artificielle pour générer des contenus manipulatoires, ce qui crée des risques d'origine tant étrangère que nationale. L'absence de réglementation des campagnes en ligne et la faiblesse de la réponse des institutions ont accru les vulnérabilités, surtout lorsqu'aucune contre-mesure rapide et coordonnée n'était prévue.

18. Plusieurs cas ont mis en évidence les problèmes liés à une coordination interinstitutionnelle tardive ou incohérente, à l'opacité du financement des campagnes par des tiers et aux difficultés à surveiller les menaces numériques. Même si les preuves directes de la manipulation des résultats sont rares, l'utilisation persistante de moyens hybrides pour manipuler l'information et la FIMI continuent de présenter un risque important, même dans les pays dotés d'institutions démocratiques solides.

5. Protéger l'intégrité des élections contre l'ingérence étrangère: quelques enseignements

19. Si l'on veut protéger les élections contre l'ingérence étrangère, il convient de combiner cybersécurité, transparence et résilience sociétale. L'expérience des pays européens montre que les approches les plus efficaces associent des garanties juridiques, une protection technique et des mesures destinées à renforcer la confiance du public.

[6] Bouclier européen de la démocratie.
[7] Centre européen pour la résilience démocratique – Commission européenne.
[8] A practical toolkit for detecting, assessing, and responding to Foreign Information Manipulation and Interference (FIMI).

20. Parmi les principaux enseignements, on peut citer la sécurisation des infrastructures électorales grâce à des mesures de **cybersécurité** solides, l'exercice d'une surveillance continue, la mise en place de plans d'urgence et l'adoption de procédures transparentes de vérification et de recomptage. La **réglementation de l'influence étrangère** par le biais d'un cadre juridique approprié et l'adoption de **normes plus strictes en matière de financement des campagnes électorales et d'exigences de transparence pour la publicité politique** contribuent à prévenir l'ingérence extérieure dissimulée. Alors que les acteurs étrangers ciblent de plus en plus les électeurs plutôt que les systèmes de vote, les gouvernements doivent également lutter contre la désinformation en fournissant des services de **vérification rapide des faits**, en assurant une communication stratégique et en coopérant avec les plateformes numériques.

21. **Les médias indépendants et les organisations de la société civile** jouent un rôle essentiel pour dénoncer les actes d'ingérence et renforcer la résilience démocratique. Des garanties supplémentaires sont nécessaires pour les technologies émergentes, en particulier l'IA, notamment en matière de transparence, de contrôle humain et de mesures d'atténuation des risques. À cet égard, la nouvelle Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit instaure l'obligation générale pour les États de protéger les processus démocratiques. Cet instrument vise, entre autres, les risques que fait peser l'IA sur la participation aux processus démocratiques par le biais d'élections libres et équitables[9].

22. La Cour européenne des droits de l'homme a considéré que les États membres pouvaient être tenus de prendre **des mesures positives pour protéger l'intégrité des processus électoraux** en cas de risque réel d'ingérence étrangère hostile. Les États ne devraient pas demeurer passifs lorsqu'ils sont saisis d'éléments qui montrent que leurs processus démocratiques sont menacés[10].

23. Plusieurs exemples européens, tels que les systèmes de vote numérique sécurisés en **Estonie** et la coopération renforcée au sein de l'UE en vue des **élections du Parlement européen de 2024**, démontrent l'importance de mener des actions coordonnées. La **République de Moldova** offre une étude de cas particulièrement intéressante, puisque ce pays a été la cible d'une manipulation de l'information et d'une ingérence étrangères durables. Les attaques ont combiné désinformation, financement illicite, cyberattaques, mobilisation d'intermédiaires et tentatives de saper la confiance du public dans les institutions électorales. Des évaluations récentes soulignent la nécessité de renforcer la coordination institutionnelle, d'accroître la transparence dans le financement des campagnes, d'assurer une surveillance effective des plateformes et de soutenir l'éducation aux médias et au journalisme indépendant.

24. Le message à retenir est clair: la sécurisation des systèmes de vote ne suffit pas à garantir l'intégrité des élections; il faut également protéger l'environnement informationnel au sens large.

6. Une approche fondée sur la mobilisation de l'ensemble de la société pour tirer parti de la force collective

25. L'efficacité de la résilience face aux menaces hybrides repose sur trois aspects interdépendants: la résilience institutionnelle, numérique et sociétale.

26. Une approche fondée sur la mobilisation de l'ensemble de la société face aux menaces hybrides part du constat que les gouvernements ne peuvent à eux seuls préserver la démocratie et la sécurité. Une résilience efficace nécessite une action coordonnée entre les institutions publiques, la société civile, le secteur privé, les médias indépendants, les institutions universitaires et les citoyens. Les organisations de la société civile promeuvent l'obligation de rendre des comptes, renforcent la résilience des communautés et améliorent l'éducation aux médias. Les entreprises privées, en particulier celles des secteurs de la technologie et de la cybersécurité, jouent un rôle essentiel dans la détection et l'atténuation des cyberattaques, de la désinformation et d'autres formes de manipulation. Les médias indépendants fournissent des informations fiables et contribuent à contrer les faux récits, tandis que les chercheurs et les institutions universitaires apportent des innovations, des analyses fondées sur des preuves et la vérification des faits. Dans un tel contexte, la place des organisations de la société civile dirigées par des femmes et des organisations féministes est tout à fait particulière. D'une part, elles sont la cible fréquente de campagnes de dénigrement et d'actes d'ingérence soutenus par des puissances étrangères. D'autre part, elles sont des spécialistes

[9] 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), article 5, paragraphe 2. Voir aussi l'Avis 303 (2024) de l'APCE.
[10] Cour européenne des droits de l'homme, *Bradshaw et autres c. Royaume-Uni*, requête nº 15653/22, 22 juillet 2025.

expérimentées de l'alerte précoce, dont l'expertise en matière de détection et de documentation des actes coordonnés de harcèlement et de désinformation reste sous-exploitée par les institutions officielles. Une approche véritablement inclusive, fondée sur la mobilisation de l'ensemble de la société, doit faire de ces organisations des partenaires à part entière, et ne pas les considérer simplement comme les bénéficiaires d'une protection.

27. Cette approche est mise en pratique par le biais d'initiatives telles que la formation des journalistes, les programmes d'éducation aux médias et au numérique, les mécanismes de partage d'informations et les réseaux intersectoriels de réponse aux crises. Ce type de coopération renforce la résilience face aux menaces hybrides tout en garantissant que les réponses apportées restent démocratiques, fondées sur les droits et adaptables.

28. La sensibilisation du public et la préparation civique sont des composantes essentielles de la résilience démocratique. Les citoyens sont souvent les principales cibles des menaces hybrides, en particulier de la désinformation et des opérations d'influence. Notons qu'il ne suffit pas de renforcer l'éducation aux médias et au numérique. Les gouvernements, les parlements, les établissements d'enseignement et la société civile devraient aussi collaborer pour mettre en place des campagnes de sensibilisation en continu qui aident les citoyens à reconnaître la manipulation, à comprendre le fonctionnement des menaces hybrides et à réagir aux informations trompeuses avec un esprit critique. Ces programmes doivent en outre tenir compte des questions de genre. Les femmes continuent de faire face à des déficits importants en matière d'accès aux compétences numériques, de connaissances des enjeux de sécurité en ligne et de confiance requise pour participer aux espaces publics numériques – des lacunes que les acteurs hostiles exploitent activement. Les initiatives en faveur de l'éducation aux médias et au numérique qui ne tiennent pas compte de ces inégalités structurelles ne peuvent toucher qu'une partie de la population à laquelle elles s'adressent.

29. **Le modèle de sécurité global de la Finlande** adopte une approche qui mobilise l'ensemble de la société. Il réunit le gouvernement, les entreprises, les ONG, le monde universitaire et les citoyens autour d'un plan de lutte coordonnée contre les menaces hybrides. Ce système met l'accent sur le partage d'informations, la planification conjointe et la formation afin d'assurer la préparation à tous les niveaux, en privilégiant la résilience psychologique des citoyens et la préparation des ménages. La coopération public-privé est particulièrement étroite en matière de sécurisation des chaînes d'approvisionnement et des infrastructures critiques. La Finlande renforce aussi la résilience par l'éducation aux médias, le soutien aux médias indépendants et la collaboration entre les autorités et les médias pour lutter contre la désinformation. La coordination des initiatives est assurée par des organes gouvernementaux centraux tels que le Comité de sécurité, tandis que l'éducation et la mise en réseau intersectorielle améliorent la réponse et la préparation aux crises.

30. L'approche adoptée par la Finlande montre que la résilience dépend à la fois **de la préparation et de la réponse**. Les démocraties doivent réagir rapidement aux menaces hybrides et investir dans des mesures préventives pour minimiser les vulnérabilités avant que les crises ne surviennent. Cette double approche repose sur une prospective stratégique, des exercices fondés sur des scénarios, des programmes de préparation de la population, des systèmes d'alerte précoce et une forte coordination institutionnelle. Ces éléments devraient s'accompagner de capacités de gestion de crise et d'intervention de manière à créer une défense complète et solide contre les menaces hybrides.

7. Le rôle des parlements nationaux

31. Les parlements nationaux jouent un rôle crucial dans la lutte contre l'ingérence étrangère et le renforcement de la résilience démocratique face aux menaces hybrides. Ces instances représentatives au cœur des systèmes démocratiques contribuent de manière déterminante à l'adoption, à l'amélioration et au contrôle des politiques qui protègent les processus et institutions démocratiques. Leur engagement actif renforce la légitimité et l'efficacité des mesures prises pour lutter contre l'influence et la manipulation étrangères. Les données disponibles indiquent que les parlements qui ont une représentation équilibrée des sexes résistent mieux aux pressions populistes et au recul de la démocratie, et que la sous-représentation des femmes au sein des commissions chargées de la sécurité et de la défense constitue une faiblesse structurelle du contrôle parlementaire à l'égard des menaces examinées dans le présent document. En outre, la Finlande – citée plus haut comme un modèle de résilience au niveau de l'ensemble de la société – figure parmi les pays européens où la représentation des femmes au parlement est la plus élevée, une corrélation qui mérite d'être prise en considération lorsqu'il s'agit d'en tirer des enseignements pour les autres États membres.

32. L'une des principales compétences des parlements est **l'activité législative**. Ils examinent et adaptent les lois existantes pour répondre à l'évolution des menaces hybrides, en veillant à ce que les nouvelles mesures restent conformes aux valeurs démocratiques, aux droits fondamentaux et à l'État de droit. Les parlements sont donc encouragés à débattre et à ratifier les initiatives législatives, y compris celles proposées par le train de mesures «Défense de la démocratie» de l'UE, ainsi que les traités internationaux élaborés sous l'égide du Conseil de l'Europe, en particulier la Convention-cadre sur l'intelligence artificielle.

33. Les parlements contribuent également à l'activité législative par le biais de **l'innovation politique**. Ils aident à mettre en place des garanties plus solides contre les ingérences extérieures en élaborant et en examinant des stratégies liées à la cybersécurité, à l'intégrité électorale et à la transparence des communications. Un autre aspect clé de leur travail consiste à promouvoir la transparence et l'obligation de rendre des comptes, en particulier dans les domaines du financement politique et de la publicité.

34. En parallèle, il est indispensable de trouver un juste équilibre dans la lutte contre l'ingérence étrangère. Les mesures qui visent à contrer **l'influence étrangère** 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 dûment 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.

35. Outre leur travail sur la législation, les parlements servent de **pont entre les citoyens et les institutions publiques**. En travaillant avec la société civile, les organes de contrôle indépendants et le grand public, ils facilitent le dialogue, contribuent à sensibiliser aux menaces hybrides et participent à renforcer la culture démocratique. Ils ont également un **rôle international** lorsqu'ils échangent leurs bonnes pratiques et coopèrent avec leurs partenaires au sein du Conseil de l'Europe, de l'Union européenne et d'autres organisations internationales.

36. En combinant action législative, contrôle, mobilisation du public et coopération internationale, les parlements nationaux peuvent favoriser l'unité, l'obligation de rendre des comptes et la confiance. Leur travail permet de faire de la résilience face à l'ingérence étrangère une **priorité transpartisane et un engagement porté collectivement par la société.**

8. Conclusions

37. Par leur nature multinationale, les menaces hybrides brouillent la frontière entre paix et conflit. Face à l'aggravation des défis sécuritaires, les démocraties européennes doivent renforcer leur capacité à détecter les attaques hybrides et à se défendre. Leur plus grande force réside dans leur unité. Le renforcement de la résilience exige l'engagement actif de tous les membres de la société, ainsi que la mise en place d'un front international uni parmi les partenaires déterminés à préserver la liberté, la justice, la démocratie et les droits humains. À une époque marquée par des tensions géopolitiques croissantes, **l'unité est le fondement de la résilience démocratique et la défense la plus efficace contre ceux qui cherchent à l'affaiblir.**

Questions à débattre

- Comment les démocraties peuvent-elles trouver un équilibre entre la lutte contre la FIMI et la protection de la liberté d'expression?
- Comment le Conseil de l'Europe peut-il coopérer avec d'autres acteurs que ses États membres pour construire une résilience politique, sociale et technique face à la FIMI?
- Comment les parlements nationaux peuvent-ils partager leur expérience en matière de législation sur l'influence étrangère?
- Quels enseignements peut-on tirer de l'expérience des États européens qui ont réussi à contrer la FIMI pour protéger l'intégrité des processus électoraux?
- Quels mécanismes peuvent renforcer la coordination entre les acteurs locaux, nationaux et internationaux pour répondre rapidement aux menaces hybrides?

- Comment la société civile et le secteur privé peuvent-ils être associés aux initiatives institutionnelles qui visent à renforcer la résilience?
- Quels indicateurs peuvent être utilisés pour mesurer la résilience démocratique face aux attaques hybrides? Les Paramètres pour l'application et la mise en œuvre des Principes de Reykjavik pour la démocratie peuvent-ils jouer un rôle?
- Comment les démocraties devraient-elles répondre à la désinformation alimentée par l'IA qui supplante les méthodes traditionnelles de vérification des faits?
- Comment l'IA peut-elle être utilisée pour contrer les menaces hybrides?
- Quels moyens les parlements nationaux peuvent-ils mettre en œuvre pour renforcer la participation citoyenne et la confiance du public en période d'instabilité et de polarisation accrues?
- Quelles initiatives peuvent être prises pour renforcer le dialogue interparlementaire contre l'ingérence étrangère?
- Comment les parlements nationaux peuvent-ils soutenir le Nouveau pacte démocratique pour l'Europe?
- Quelles initiatives peuvent être prises pour favoriser une plus grande coopération entre les organisations internationales qui partagent les mêmes valeurs dans la lutte contre les menaces hybrides?
- Comment les stratégies de lutte contre la FIMI peuvent-elles spécifiquement remédier au fait que les femmes – responsables politiques, journalistes et dirigeantes de la société civile – sont ciblées de façon disproportionnée par la désinformation sexiste, les *deepfakes* et le harcèlement en ligne? Et quelles mesures législatives ou institutionnelles sont nécessaires pour combler les lacunes actuelles en matière de protection?

Annexe: principaux documents et sites internet de référence

Assemblée parlementaire du Conseil de l'Europe

- Résolution 2593 (2025) «L'ingérence étrangère: une menace pour la sécurité démocratique en Europe»
- Résolution 2622 (2025) «Russie: nouvelles menaces pour les démocraties européennes»
- Résolution 2636 (2026) «Les élections en temps de crise»

Conseil de l'Europe

- Rapport 2026 – Secrétaire Général
- Vers une Résilience Démocratique – Le Nouveau Pacte Démocratique pour l'Europe
- Étude de faisabilité du Conseil de l'Europe sur un instrument juridique traitant de la manipulation de l'information et de l'ingérence menées depuis l'étranger (FIMI)
- Paramètres pour l'application et la mise en œuvre des Principes de Reykjavik pour la démocratie (CM(2024)48-final)
- Cour européenne des droits de l'homme, *Bradshaw et autres c. Royaume-Uni*, 22 juillet 2025
- Conférence parlementaire – Les élections en temps de crise (Berne, 9 et 10 mai 2023)

Union européenne

- Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions – Bouclier européen de la démocratie: renforcer la position de démocraties fortes et résilientes, JOIN/2025/791 final
- 3rd EEAS Report on Foreign Information Manipulation and Interference Threats

- Best Practices in the whole-of-society approach in count ring hybrid threats