

Guerre hybride et protection de l'intégrité territoriale de l'Union et des infrastructures critiques de sécurité et de défense

2026/2024(INI) - 16/09/2026 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 470 voix pour, 129 contre et 62 abstentions, une résolution sur la guerre hybride et la protection de l'intégrité territoriale de l'Union et des infrastructures critiques de sécurité et de défense.

Guerre hybride: entre guerre et paix

Le Parlement a souligné que les opérations hybrides sont des actes délibérés, combinés, fondés sur le renseignement et coordonnés par les États, y compris par l'intermédiaire d'acteurs non étatiques, d'intermédiaires et de mandataires. Elles sont conçues pour ressembler à des incidents isolés et demeurer sous le seuil des conflits armés, tout en ayant le potentiel de produire des effets comparables à ceux des agressions conventionnelles. L'objectif premier de la guerre hybride est de déstabiliser, de diviser et de saper l'Union et ses États membres en exploitant les vulnérabilités systémiques et en affaiblissant leur sécurité, leur résilience et leurs fondements démocratiques, ainsi que leur préparation à la défense.

Le Parlement affirme que **la Russie**, en agissant directement ou par l'intermédiaire de multiples intermédiaires tels que la Biélorussie, **est l'acteur étatique le plus dangereux** pour ce qui est de la menace hybride qui cible l'Union et ses États membres. Il souligne que l'Union doit adopter **une approche globale** face aux menaces hybrides, qui tient compte non seulement des activités de la Russie et de la Biélorussie, mais aussi du rôle stratégique croissant de la Chine, de l'Iran et de la Corée du Nord dans l'amplification d'actions hostiles à l'encontre des intérêts et de la sécurité de l'Europe.

La Commission et le Conseil sont invités à évaluer **l'adéquation des cadres juridiques existants de l'Union** pour lutter contre les menaces hybrides, à combler les lacunes recensées et à traiter les opérations hybrides en deçà des seuils et qui ne peuvent être gérées par les seuls services répressifs comme des **questions de sécurité collective**, nécessitant une réponse civilo-militaire combinée.

Guerre de l'information, sécurité cognitive et résilience sociétale

Le Parlement a souligné l'ampleur croissante de la guerre cognitive et des manipulations de l'information étrangères, qui érodent la confiance de la société dans les institutions démocratiques, accentuent la polarisation et sapent la prise de décision démocratique et le soutien public à la sécurité et à la défense européennes, notamment l'aide à l'Ukraine. Les outils d'IA - hypertrucages, amplification algorithmique et réseaux de comptes automatisés - rendent ces opérations d'influence plus rapides, moins coûteuses et plus difficiles à détecter.

La résolution a insisté sur le fait que les activités de manipulation de l'information et d'ingérence menées depuis l'étranger doivent être **traitées comme une menace grave pour la sécurité** nécessitant une approche opérationnelle, une meilleure coordination et une collaboration entre les États membres à tous les niveaux, comprenant une **détection précoce**, des **options de réaction** adéquates et une protection renforcée des processus démocratiques, notamment lors des périodes électorales.

Étant donné que les menaces hybrides ciblent la société dans son ensemble, le Parlement estime que la résilience face aux menaces hybrides doit aller au-delà des mesures militaires, techniques et

institutionnelles en réunissant les autorités publiques, le secteur privé, la société civile, le monde universitaire et les médias indépendants afin de renforcer la confiance démocratique, la sensibilisation du public et la préparation de la société, en favorisant ainsi une nouvelle culture européenne de la sécurité. Les députés ont souligné la nécessité de **renforcer la résilience du public** face aux activités de manipulation de l'information et d'ingérence menées depuis l'étranger et demandé que la Commission prenne de nouvelles mesures en fournissant une **cartographie des vulnérabilités cognitives** et des critères de résilience.

Cybersécurité

Les cyberattaques sont devenues un élément central des campagnes hybrides tirant parti de la numérisation croissante de secteurs critiques tels que les soins de santé, la finance et l'énergie. Le Parlement a demandé que les mécanismes de lutte contre les activités de manipulation de l'information et d'ingérence menées depuis l'étranger soient **systématiquement associés aux capacités de cybersécurité** afin de détecter les infrastructures de manipulation coordonnée, d'identifier les responsables et de les neutraliser à un stade précoce.

Les députés ont recommandé à la Commission d'étudier des propositions visant à mettre en place **un cadre plus harmonisé** afin d'aider les États membres dans la planification, la coordination opérationnelle et la mise en œuvre des cyberopérations. Ils ont demandé une meilleure harmonisation des obligations en matière de **signalement d'incidents** et des notions juridiques essentielles dans l'ensemble des cadres de l'Union relatifs à la cybersécurité. La Commission et les États membres, en coopération avec l'OTAN, devraient examiner les conditions juridiques, procédurales et opérationnelles préalables à des **cybercontre-mesures** proportionnées et conformes au droit.

Infrastructures critiques

Le Parlement a condamné les attaques hybrides ciblant les infrastructures critiques de l'Union - en particulier l'énergie, les transports, les communications et les infrastructures satellitaires, y compris celles destinées à la mobilité militaire, les infrastructures maritimes et les câbles sous-marins. Il a invité instamment la Commission et les États membres de l'Union à créer, dans le cadre du prochain cadre financier pluriannuel 2028-2034, **un cadre juridique et financier européen** garantissant une protection et une résilience suffisantes des infrastructures énergétiques critiques. D'une manière générale, il importe de stimuler les capacités de surveillance, de détection et de défense contre les menaces aériennes et maritimes.

Le Parlement a demandé la mise en œuvre rapide de la directive sur la résilience des entités critiques (CER) et de la directive SRI2, qui constituent des avancées importantes pour le renforcement de la résilience contre les attaques hybrides.

La résolution invite les États membres à mener régulièrement des **exercices de préparation et de résilience** pour les infrastructures critiques, y compris des exercices conjoints, et à fournir de toute urgence les **capacités prioritaires** identifiées dans le livre blanc sur la préparation de la défense européenne, notamment en matière de défense aérienne et antimissile, de drones et de systèmes de lutte antidrones.

Face à la dépendance structurelle de l'Union à l'égard de pays tiers à haut risque, en particulier la Chine, les députés ont invité la Commission à redoubler d'efforts pour **réduire les dépendances stratégiques** et les États membres à diversifier les chaînes d'approvisionnement et à donner la **priorité aux fournisseurs européens** et partageant les mêmes valeurs dans les secteurs stratégiques à chaque fois que des considérations de sécurité l'exigent.

La résolution invite instamment les États membres à accroître le **partage de renseignement** et insiste sur l'obligation d'intégrer systématiquement des évaluations fondées sur des données et des renseignements dans la planification et la gestion des crises. Elle affirme que la **capacité unique d'analyse du renseignement** (SIAC) devrait être la plateforme unique pour le renseignement au sein des institutions européennes.