Union interparlementaire
Pour la démocratie. Pour tous.

151e Assemblée de l'UIP

Genève
19-23 octobre 2025

#IPU151 151E ASSEMBLÉE DE L'UIP Genève (Suisse) 19–23 octobre 2025

Action parlementaire contre la criminalité transnationale organisée, la cybercriminalité et les menaces hybrides pour la démocratie et la sécurité humaine

Résolution adoptée à l'unanimité par la 151e Assemblée de l'UIP
(Genève, 23 octobre 2025)

La 151e Assemblée de l'Union interparlementaire,

rappelant les buts et principes de la Charte des Nations Unies, notamment le respect de la souveraineté nationale, de l'intégrité territoriale, de la non-ingérence dans les affaires intérieures des États et du règlement pacifique des différends, ainsi que de la Déclaration universelle des droits de l'homme, de la Convention des Nations Unies contre la criminalité transnationale organisée (CNUCT) (2000), de la Convention des Nations Unies contre la corruption (2003) et d'autres instruments internationaux pertinents,

réaffirmant l'engagement de l'UIP, aux côtés d'autres institutions et de la société civile, en faveur de la démocratie, de la paix, des droits de l'homme et de l'état de droit en tant que fondements de la gouvernance légitime, et *prenant note* de la prochaine Convention des Nations Unies contre la cybercriminalité,

alarmée par les liens croissants entre la criminalité transnationale organisée, le trafic de drogue, la cybercriminalité et les menaces hybrides, qui constituent un danger pour les institutions démocratiques, la sécurité nationale et la stabilité mondiale, sapent la démocratie, corrompent les institutions et détruisent le tissu social et économique de nos sociétés,

profondément préoccupée par les attaques, les menaces, la violence sexiste en ligne et les assassinats visant des parlementaires, des journalistes, des responsables politiques, des dirigeants locaux et des chefs d'entreprise en raison de leur rôle dans la défense de la transparence et de l'état de droit,

consciente de la nécessité de renforcer la coopération entre les parlements nationaux, l'Organisation des Nations Unies (ONU), l'Organisation internationale de police criminelle (INTERPOL) et des organisations régionales, afin d'harmoniser les cadres législatifs et de contrer ces menaces en constante évolution, en particulier la fraude en ligne, la traite des êtres humains, les drogues illicites, le blanchiment d'argent et les abus connexes qui ont une portée de plus en plus transnationale,

prenant note de la lettre d'intention signée par l'UIP et l'Office des Nations Unies contre la drogue et le crime (ONUDC) en juin 2025 et de leur engagement commun à renforcer les capacités parlementaires dans la lutte contre la criminalité organisée,

alarmée par un récent rapport de l'ONUDC[1], qui révèle la prolifération à grande échelle de centres d'escroquerie dans toute l'Asie du Sud-Est, où des centaines de milliers de victimes de plus de 70 pays du monde font l'objet de traite et sont contraintes de participer à des cyberescroqueries,

[1] ONUDC, *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia*, avril 2025.

profondément alarmée du fait que les centres d'escroquerie évoluent rapidement, se muant de pôles criminels régionaux en une économie souterraine mondialisée, qu'ils exploitent les problèmes de gouvernance dans les régions en développement sous couvert d'investissements ou de constructions d'immeubles ou de complexes de loisir, avec la complicité d'intermédiaires locaux, et du fait que ces centres génèrent désormais des recettes rivalisant avec le produit intérieur brut (PIB) de certains pays et s'étendent à l'échelle mondiale,

prenant acte des rapports de l'ONUDC (2025) et d'autres organisations, qui révèlent des niveaux alarmants d'exploitation à des fins d'escroqueries numériques, de traite des êtres humains, de désinformation et de corruption par des acteurs étatiques et non étatiques, notamment des opérations directement liées à des structures de crime organisé, des sites illégaux de vente en ligne et des systèmes bancaires souterrains, générant des recettes annuelles dépassant les 50 à 75 milliards d'USD,

profondément préoccupée par de récents cas de cyberintrusions coordonnées, de sabotage d'infrastructures essentielles, d'espionnage et de campagnes de désinformation ciblées à l'encontre de plusieurs pays sur tous les continents, menés par des acteurs étatiques et non étatiques,

rappelant que les réseaux criminels transnationaux exploitent les lacunes de gouvernance, les zones économiques spéciales, les zones touchées par les conflits et les casinos pour blanchir les produits du crime, ce qui favorise la corruption, déstabilise les populations locales, viole les droits de l'homme, sape la souveraineté, menace la stabilité régionale, entrave le développement et compromet les efforts internationaux visant à combattre le crime organisé et à préserver l'état de droit,

rappelant également des exemples frappants de l'utilisation destructrice de tactiques hybrides par des acteurs étatiques, notamment le recours aveugle à la force militaire, les cyberopérations et la guerre psychologique,

préoccupée par le fait que des victimes, notamment des femmes, des enfants et d'autres groupes vulnérables, sont contraintes de participer à des escroqueries en ligne sous la menace d'être torturées ou placées en détention et risquent souvent d'être à nouveau exploitées ou de subir d'autres atteintes à leurs droits,

saluant le rôle des parlements en matière de renforcement de la législation, du contrôle et de la coopération, qui permet d'examiner les liens entre la cybercriminalité, la traite des êtres humains, le blanchiment d'argent et la corruption tout en veillant à ce que les contre-mesures veillent pleinement au respect des principes humanitaires et des droits de l'homme,

considérant que la nature transnationale et technologiquement avancée des organisations criminelles crée un déséquilibre qui élargit leur expansion et leur influence, ce qui contraint les institutions chargées d'assurer la justice et la sécurité à recourir à des institutions supranationales et à des stratégies et des moyens technologiquement avancés, et *reconnaissant* qu'une telle menace devient encore plus grave lorsque les acteurs impliqués sont des États ou qu'ils opèrent avec le soutien d'un État,

saluant le rôle de l'UIP et les efforts qu'elle déploie pour servir de cadre mondial de dialogue multilatéral entre les parlements nationaux sur les questions de paix et de sécurité et pour contribuer à mettre en œuvre des solutions concrètes grâce à sa Stratégie 2022-2026, notamment l'Objectif stratégique 4, à savoir "favoriser l'action parlementaire collective",

1. *déclare* que la lutte contre la criminalité transnationale organisée, le trafic de drogue, la cybercriminalité et les menaces hybrides – qu'elles soient le fait d'acteurs étatiques ou non étatiques – constitue une priorité mondiale nécessitant une action parlementaire concertée et une gouvernance démocratique solide, et *exhorte* les parlements à envisager des mesures garantissant que les auteurs de tels crimes répondent de leurs actes ;

2. *condamne* toutes les formes de criminalité organisée, telles que la cybertraite, la criminalité forcée et l'esclavage moderne, qu'elles soient perpétrées par des acteurs étatiques ou non étatiques, en accordant une attention particulière à leur impact disproportionné sur les femmes et les enfants, et *exhorte* les parlements à adopter des lois et des politiques qui privilégient une approche centrée sur les victimes et garantissent la protection et la réinsertion de l'ensemble des victimes et survivants ;

3. *souligne* l'importance de s'attaquer aux causes profondes de la vulnérabilité, telles que la pauvreté, le manque d'éducation, les inégalités, la traite des personnes, les conflits et la corruption, qui alimentent le recrutement au sein des sites d'escroquerie, et *exhorte* les autorités concernées à mettre en œuvre des solutions concrètes pour y remédier ;

4. *exhorte* les Parlements membres de l'UIP à actualiser leur législation nationale conformément au droit international applicable afin de lutter contre la participation d'acteurs étatiques et non étatiques à la cybercriminalité et à renforcer les mécanismes de contrôle parlementaire des services de sécurité et de renseignement, dans le respect de l'état de droit et des droits de l'homme, tout en garantissant que les mesures de lutte contre la cybercriminalité n'entraînent ni violations des principes humanitaires ni victimisation secondaire des personnes victimes de la traite ;

5. *exhorte* les parlements à renforcer leur cadre juridique national pour :

   a) ériger en infraction pénale la contrainte exercée à des fins d'escroquerie en ligne ;
   b) alourdir les sanctions à l'encontre des entreprises de sécurité impliquées dans des actes malveillants ;
   c) combler les lacunes juridiques exploitées par les jeux d'argent illicites en ligne, le blanchiment de cryptomonnaies et les systèmes bancaires clandestins ;
   d) réviser les lois électorales, financières ainsi que celles relatives à la transparence pour prévenir l'infiltration du crime organisé et l'ingérence étrangère dans les institutions démocratiques ;
   e) renforcer le contrôle indépendant des services de sécurité de l'État et des autorités chargées de l'application de la loi afin de prévenir toute complicité dans la traite des personnes et la cybercriminalité ;
   f) renforcer les sanctions à l'encontre de tout fonctionnaire ou gouvernement impliqué dans des actes malveillants ;

6. *appelle* à la protection des parlementaires et *demande* au Comité des droits de l'homme des parlementaires de l'UIP de surveiller et de documenter les attaques dirigées contre eux ;

7. *invite* les gouvernements et les parlements à s'attaquer aux causes structurelles de la vulnérabilité – pauvreté, inégalités, faiblesses institutionnelles et corruption – au moyen de politiques inclusives et durables ;

8. *soutient* le travail des organismes régionaux, internationaux et mondiaux chargés de la sécurité et de l'application de la loi qui luttent contre la criminalité transnationale organisée dans le cadre de la CNUCT, tels que l'ONUDC, INTERPOL et les organismes régionaux de lutte contre la criminalité organisée, et *encourage* la création de nouvelles institutions chargées de lutter contre la criminalité organisée dans la sphère transnationale où elle opère, telles qu'une cour internationale de lutte contre la corruption, la Cour pénale latino-américaine et caribéenne contre la criminalité organisée transnationale (COPLA) ou une agence du MERCOSUR chargée de lutter contre la criminalité organisée transnationale ;

9. *invite* les Parlements membres de l'UIP, conformément au droit international et à la jurisprudence internationale émergente, à reconnaître que les actes de criminalité transnationale organisée — qu'ils soient commis par des acteurs non étatiques ou par un État ou ses agents agissant de manière organisée ou systématique — peuvent constituer des crimes contre l'humanité ;

10. *recommande* l'élaboration de cadres et de normes communs en matière de cybersécurité entre les Parlements membres afin de protéger les infrastructures critiques et les systèmes d'information publics, conformément à la résolution de l'UIP intitulée *Cybercriminalité : les nouveaux risques pour la sécurité mondiale*, adoptée lors de la 146e Assemblée (Manama, Bahreïn, mars 2023) ;

11. *appelle* à une réglementation plus stricte des cryptomonnaies, des plateformes en ligne et des flux financiers transfrontaliers, en vue de freiner le blanchiment d'argent illicite lié aux centres d'escroquerie, et *exhorte* les institutions financières internationales à faire preuve d'une vigilance accrue ;

12. *encourage* les parlements à collaborer avec le secteur privé et la société civile afin de favoriser l'innovation technologique, qui lutte contre la désinformation et l'exploitation numérique, tout en préservant les libertés civiles, en protégeant la vie privée et en garantissant le plein respect des droits de l'homme dans toutes les mesures visant à lutter contre les menaces numériques ;

13. *reconnaît* que les tactiques de menaces hybrides — notamment le cybersabotage, la désinformation et les attaques contre les infrastructures critiques —, lorsqu'elles sont menées ou soutenues par des acteurs étatiques ou non étatiques, peuvent constituer des violations du droit international et, dans certains cas, des actes de terrorisme; et *exhorte* donc au respect intégral du droit international humanitaire et des normes relatives aux droits de l'homme ;

14. *dénonce* le recours aux violations de l'espace aérien, aux opérations d'influence coordonnées et aux cyberintrusions ciblées comme moyens d'intimidation, d'agression et d'ingérence dans les affaires intérieures d'États souverains ;

15. *demande* à l'UIP d'utiliser ses organes existants pour faciliter la coopération législative dans la lutte contre la criminalité forcée, les crimes financiers et les violations des droits de l'homme et du droit international humanitaire, et de surveiller sa mise en œuvre ;

16. *propose* d'inscrire cette question en tant que point permanent à l'ordre du jour, sous le titre *Démocratie, gouvernance et sécurité mondiale*, et d'examiner les progrès accomplis lors des prochaines Assemblées de l'UIP.