Union interparlementaire
Pour la démocratie. Pour tous.

146e ASSEMBLÉE DE L'UIP
المنامـــة، البحريـــن
MANAMA, BAHREÏN
11-15 MARS 2023 - ١١-١٥ مـارس ٢٠٢٣

146e Assemblée de l'UIP
Manama (11-15 mars 2023)

Cybercriminalité : les nouveaux risques pour la sécurité mondiale

Résolution adoptée par consensus* par la 146e Assemblée de l'UIP (Manama, 15 mars 2023)

La 146e Assemblée de l'Union interparlementaire,

condamnant toutes les formes de cybercriminalité et *réaffirmant* la nécessité de lutter contre ces actes par la coopération internationale,

réaffirmant le cadre de l'ONU relatif au comportement responsable des États dans l'utilisation des technologies de l'information et des communications (TIC) et la nécessité de mettre en œuvre ce cadre,

considérant qu'il faut instaurer la confiance et la compréhension mutuelle entre les pays face à l'utilisation malveillante des TIC par des acteurs étatiques et non étatiques, lesquels ne connaissent ni frontières ni limites,

constatant le recours et la dépendance croissants aux TIC à travers le monde,

consciente de l'augmentation des activités de cybercriminalité liée à l'accélération de la transformation numérique, accentuée par la pandémie de COVID-19,

prenant note de la responsabilité des parlements de mettre en place un cadre réglementaire qui protège les citoyens dans le cyberespace à l'aide de nouvelles infrastructures et ressources, de la même manière que dans le monde physique,

rappelant les résolutions suivantes de l'Assemblée générale des Nations Unies : 31/72 du 10 décembre 1976 intitulée *Convention sur l'interdiction d'utiliser des techniques de modification de l'environnement à des fins militaires ou toutes autres fins hostiles*, 55/63 du 4 décembre 2000 et 56/121 du 19 décembre 2001 intitulées *Lutte contre l'exploitation des technologies de l'information à des fins criminelles*, 57/239 du 31 janvier 2003 intitulée *Création d'une culture mondiale de la cybersécurité*,

rappelant également les résolutions annuelles de l'Assemblée générale des Nations Unies sur le thème *Progrès de l'informatique et des télécommunications et sécurité internationale*, et en particulier la résolution 69/28 du 2 décembre 2014, la résolution 73/266 du 22 décembre 2018 établissant le Groupe d'experts gouvernementaux chargé de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, ainsi que la résolution 75/240 du 31 décembre 2020 établissant le Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025), et *soulignant* les normes volontaires et non contraignantes concernant le comportement responsable des États dans l'utilisation des TIC dans le contexte de la sécurité internationale, élaborées par le groupe d'experts gouvernementaux et approuvées par la résolution 70/237 de l'Assemblée générale des Nations Unies du 23 décembre 2015, qui demande aux États membres de l'ONU de s'inspirer de ces normes, ainsi que l'établissement, par la résolution 77/37 de l'Assemblée générale des Nations Unies du 7 décembre 2022, d'un programme d'action des Nations Unies visant à examiner les menaces existantes et potentielles et à soutenir les capacités et les efforts des États pour mettre en œuvre et faire progresser les engagements,

F

* La délégation de l'Inde a exprimé des réserves sur le paragraphe 25.
La délégation de la Fédération de Russie a exprimé des réserves sur l'alinéa 11 et le paragraphe 1.

rappelant en outre la *Convention des Nations Unies contre la criminalité transnationale organisée* du 15 novembre 2000 et la *Convention des Nations Unies contre la corruption* du 31 octobre 2003,

soulignant l'importance des conventions régionales sur la cybercriminalité, la criminalité transnationale organisée, l'échange d'informations et l'assistance administrative, notamment la *Convention sur la cybercriminalité* du Conseil de l'Europe du 23 novembre 2001 et son *Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques* du 28 janvier 2003, l'*Accord de coopération visant à assurer la sécurité internationale de l'information entre les États membres de l'Organisation de coopération de Shanghai* du 16 juin 2009, et la *Convention arabe sur la lutte contre les infractions liées aux technologies de l'information* du 21 décembre 2010, ainsi que les lois types du Parlement latino-américain et caribéen (PARLATINO) sur la cybercriminalité (novembre 2013) et ses versions mises à jour, la prévention sociale de la violence et de la criminalité (novembre 2015), la criminalité informatique (février 2021) et la lutte contre le commerce illicite et la criminalité transnationale (février 2021), l'*Accord de coopération entre les États membres de la Communauté d'États indépendants concernant la garantie de la sécurité de l'information* du 20 novembre 2013, et l'*Accord de coopération entre les États membres de la Communauté d'États indépendants relatif à la lutte contre la criminalité dans le domaine des technologies de l'information* du 28 septembre 2018, et la *Convention sur la cybersécurité et la protection des données personnelles* de l'Union africaine du 27 juin 2014,

soulignant également que la *Convention sur la cybercriminalité* du Conseil de l'Europe, qui est ouverte à l'adhésion de tous les pays, est devenue un instrument d'importance mondiale qui compte des États parties de toutes les régions du monde et a un impact sur ces derniers,

rappelant les travaux de l'UIP sur les différents nouveaux risques auxquels sont exposées nos sociétés de plus en plus numérisées, notamment les résolutions de l'UIP intitulées *La cyber-guerre : une grave menace pour la paix et la sécurité mondiale* (adoptée le 1er avril 2015 lors de la 132e Assemblée, à Hanoï) et *Législation dans le monde pour la lutte contre l'exploitation et les abus sexuels en ligne à l'égard des enfants* (adoptée le 30 novembre 2021 lors de la 143e Assemblée, à Madrid), laquelle rappelle également la Convention du Conseil de l'Europe intitulée *La protection des enfants contre l'exploitation et les abus sexuels* (Convention de Lanzarote) du 25 octobre 2007,

se félicitant des travaux menés par l'ONU pour promouvoir le comportement responsable des États dans le cyberespace,

saluant les efforts déployés par l'ONU pour adopter, par le biais de la résolution 74/247 de l'Assemblée générale du 27 décembre 2019, une convention internationale sur la cybercriminalité, et *saluant également* la création d'un comité spécial chargé d'élaborer cette convention,

se félicitant du fait que l'UIP participe au processus de consultation multipartite de ce comité spécial pour faire entendre la voix des parlements,

prenant note de la nécessité d'appliquer une approche mondiale au problème de la cybercriminalité et de ses graves conséquences pour les citoyens, ainsi que de la nécessité de protéger la paix, la sécurité et la stabilité économique mondiales, tout en défendant les principes fondamentaux des droits de l'homme, notamment la liberté d'expression,

considérant que les législateurs, les gouvernements et l'ensemble des parties prenantes doivent prendre d'urgence des mesures plus énergiques au niveau national pour lutter contre la cybercriminalité, compte tenu de sa multiplication et de son évolution rapide,

considérant également que toutes les mesures prises dans ce domaine doivent garantir le respect des droits de l'homme et des droits fondamentaux,

notant l'évolution inégale des capacités des pays dans le domaine des TIC et de leur aptitude à protéger l'infrastructure des TIC, et *soulignant* la nécessité d'accroître l'assistance et la collaboration techniques, notamment en faveur des pays en développement,

notant également que les États doivent agir conformément aux obligations qui leur incombent en vertu du droit international des droits de l'homme, notamment le *Pacte international relatif aux droits civils et politiques*, la *Convention relative aux droits de l'enfant*, la *Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants*, la *Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes*, ainsi que leurs protocoles additionnels et les autres instruments internationaux pertinents relatifs aux droits de l'homme,

considérant qu'une action parlementaire commune de portée internationale est nécessaire pour faire connaître et mettre en œuvre les normes volontaires et non contraignantes de comportement responsable des États en matière d'utilisation des TIC,

notant que la cybercriminalité peut constituer une grave menace pour les processus démocratiques, notamment en ce qui concerne l'ingérence dans les élections en utilisant les failles de cybersécurité ou de faux comptes sur les réseaux sociaux,

reconnaissant que les femmes, les jeunes, les enfants, les personnes âgées, les personnes en situation de handicap et les populations racisées sont particulièrement vulnérables à la cybercriminalité,

reconnaissant également la nécessité de promouvoir l'égalité des sexes et l'autonomisation des femmes et des filles dans toute leur diversité, notamment par l'intégration de la dimension de genre et lors de l'élaboration, de la mise en œuvre et de l'application des politiques, des programmes et de la législation sur ces questions,

prenant note de la nature des menaces et des risques de la cybercriminalité transnationale pour la paix et la sécurité internationale, ainsi que du développement fulgurant du cyberespace, qui fait que les méthodes utilisées par les cybercriminels sont de plus en plus sophistiquées,

prenant note également que la cybercriminalité comprend, sans s'y limiter, les attaques contre les systèmes informatiques, les atteintes à la vie privée, la création et le déploiement de logiciels malveillants et, de plus en plus, des attaques contre les infrastructures civiles stratégiques, ainsi que d'autres actes qui peuvent se produire hors ligne et être facilités par les systèmes informatiques, notamment la fraude en ligne, le commerce de drogue, le blanchiment d'argent, les crimes de haine, la traite des êtres humains et la violence sexiste facilitée par la technologie, telle que le harcèlement sexuel, les menaces, la prédation, l'intimidation, les discours de haine sexistes et l'exploitation sexuelle des femmes et des enfants via Internet, autant d'actes qui ont une incidence négative sur la sécurité mondiale et la stabilité économique,

considérant que la plupart des lois nationales ont été promulguées avant l'apparition de la cybercriminalité et ne permettent donc pas toujours de répondre efficacement à ces menaces,

1. *encourage* les parlements à prendre les mesures nécessaires pour que leur pays adhère, s'il ne l'a pas encore fait, aux instruments internationaux existants qui portent sur l'utilisation des TIC à des fins criminelles, notamment la *Convention sur la cybercriminalité* du Conseil de l'Europe, qui constitue le traité multilatéral sur la cybercriminalité le plus complet actuellement en vigueur et qui est ouverte à l'adhésion de tous les États ;

2. *demande* aux parlements de s'assurer que la législation sur la cybercriminalité est à jour et pertinente, conformément au droit international, notamment aux instruments internationaux relatifs aux droits de l'homme, d'y affecter les moyens nécessaires et de mobiliser l'ensemble des parties prenantes, notamment le secteur privé, le monde universitaire, la société civile et les milieux techniques, compte tenu de l'augmentation constante de l'ampleur, de la portée, de la rapidité, de la complexité et de la fréquence de ces activités et de leurs conséquences pour la sécurité nationale, la paix et la sécurité internationale et la stabilité économique mondiale, ainsi que de prévoir dans

ces lois une compétence extraterritoriale pour permettre la poursuite des auteurs d'actes criminels, indépendamment du lieu où ces actes ont été commis et du fait qu'ils constituent ou non une infraction dans la juridiction étrangère concernée ;

3. *exhorte* les parlements à veiller à ce que des évaluations d'impact sur les droits de l'homme soient intégrées dans l'ensemble des processus législatifs relatifs à la cybercriminalité ;

4. *demande* aux parlements de renforcer les capacités des agents de la force publique, notamment les services d'enquête, les procureurs et les juges, dans le domaine de la cybercriminalité, et de leur donner les moyens d'enquêter, de poursuivre les auteurs et de juger efficacement les affaires de cybercriminalité ;

5. *encourage* les parlements à faire pleinement usage de leur fonction de contrôle afin de s'assurer que les gouvernements disposent des outils nécessaires, notamment les ressources et les capacités appropriées, pour prévenir et combattre l'augmentation rapide de la cybercriminalité et protéger la cybersécurité, l'identité, la vie privée et les données des citoyens, tout en assurant le respect des droits de l'homme et des libertés ;

6. *recommande vivement* aux parlements de veiller à ce que les cadres législatifs nationaux relatifs à la protection des infrastructures nationales essentielles, notamment l'infrastructure d'Internet, soient à jour, ou d'établir ces cadres si nécessaire ;

7. *encourage* les parlements à promouvoir un cyberespace ouvert, libre et sûr en demandant à l'exécutif de se conformer aux normes de l'ONU relatives au comportement responsable des États dans le cyberespace, de coopérer pour lutter contre la cybercriminalité et empêcher les cybercriminels et les acteurs malveillants d'agir, de donner suite aux demandes d'assistance et de renforcement des capacités, si possible en temps réel, en conformité avec l'état de droit et en respectant pleinement le droit international des droits de l'homme et les libertés fondamentales, de sécuriser la chaîne d'approvisionnement des entreprises de leur pays, de signaler spontanément les vulnérabilités potentielles à des tiers pour les aider à prévenir de futurs incidents, et en particulier de soutenir et de protéger toutes les équipes d'intervention en cas de cyberincident à l'intérieur et à l'extérieur des frontières de leur pays ;

8. *encourage également* les parlements à élaborer des lois sensibles au genre qui promeuvent les services transversaux de cybersécurité axés sur la prévention (sensibilisation, audit et formation) et la détection des incidents (24 heures sur 24 et 7 jours sur 7) et qui permettent de réagir immédiatement et efficacement aux cybermenaces, par une approche centrée sur les victimes ;

9. *recommande* aux parlements de promouvoir la création d'institutions et d'organes adaptés – par exemple, des centres nationaux de cybersécurité, des équipes d'intervention rapide dans le domaine informatique, des équipes d'intervention en cas d'incident de sécurité informatique et des centres d'opérations de sécurité –, lorsque ceux-ci n'existent pas encore dans leur pays ;

10. *recommande également* que tous les parlements veillent à ce que ces institutions et organes disposent de ressources budgétaires suffisantes et de personnel spécialisé, y compris de femmes expertes en cybersécurité, pour pouvoir réagir de façon souple, rapide et efficace à la cybercriminalité et protéger les infrastructures civiles stratégiques, les institutions publiques, les entreprises et les citoyens sans porter atteinte à la vie privée, en tenant compte du fait que la numérisation croissante des services publics et des services collectifs peut entraîner une exposition importante aux risques numériques ;

11. *exhorte* les parlements à promouvoir la coordination internationale entre ces institutions et organismes afin de surveiller, de prévenir et de détecter les cybermenaces, d'enquêter à leur sujet et de les combattre ;

12. *invite* les parlements à encourager l'exécutif à proposer des formations spécifiques en matière de cybersécurité afin d'accroître le nombre de spécialistes de la cybersécurité et de renforcer leurs capacités ;

13. *réaffirme* qu'un environnement des TIC ouvert, sûr, stable, accessible et pacifique est essentiel pour tous et nécessite une coopération efficace entre les États afin de réduire les risques pour la paix et la sécurité internationale, et *appelle* la communauté internationale à promouvoir le plein respect des droits de l'homme et des libertés fondamentales ;

14. *demande* aux parlements d'encourager l'investissement dans la recherche et le développement, en intégrant dans les projets et propositions de loi des dispositions spécifiques en matière de cybersécurité et en prévoyant des crédits budgétaires suffisants, afin d'anticiper les éventuelles cybermenaces émergentes et de s'en protéger ;

15. *encourage* les parlements à établir des partenariats avec les entreprises, le monde universitaire et toutes les autres parties prenantes, y compris la société civile, en chargeant l'exécutif de jouer le rôle de facilitateur, afin de développer un écosystème de cybersécurité solide et collaboratif qui respecte pleinement les principes des droits de l'homme et les obligations internationales en la matière ;

16. *demande* aux parlements et aux parlementaires de s'employer activement à faire émerger, au niveau national, une compréhension commune et actualisée de la nature de la cybercriminalité telle qu'elle est vécue par les citoyens, les organisations et les institutions ;

17. *exhorte* les parlements à contribuer à développer une véritable "culture de la cybersécurité" en élaborant des programmes d'enseignement destinés à former, dès l'enfance, les générations futures à l'apprentissage numérique et au savoir-faire technologique, aussi bien en ce qui concerne les vastes possibilités offertes par les technologies que les risques importants qui y sont associés ;

18. *recommande* aux parlements de renforcer la protection des femmes, des jeunes, des enfants, des personnes âgées, des personnes en situation de handicap et des populations racisées dans le cyberespace, en veillant au respect des droits de l'homme et en prévoyant dans les politiques pédagogiques relatives à l'utilisation des réseaux sociaux des dispositifs permettant de prévenir la violence sexiste ;

19. *exhorte* les parlements à prendre les mesures nécessaires pour protéger les moments cruciaux de la démocratie, notamment les périodes où les citoyens exercent leur droit de vote, afin d'éviter les attaques et les interférences qui visent à influencer, modifier ou violer la libre formation de l'opinion des citoyens pendant les processus électoraux ;

20. *demande* à la communauté internationale de prendre des mesures pour protéger la démocratie en veillant à ce que tous les parlements du monde, en tant qu'institutions représentant la volonté du peuple, bénéficient d'une protection particulière du fait de leur inscription sur les listes d'infrastructures nationales civiles critiques et de services essentiels ;

21. *souligne* la nécessité de renforcer encore la coopération et l'assistance internationales dans le domaine de la sécurité des TIC et du renforcement des capacités, afin de réduire la fracture numérique et de renforcer la lutte contre les cybermenaces à travers le monde ;

22. *demande* aux parlements d'appréhender plus en profondeur la nature complexe et l'évolution rapide de la cybercriminalité en facilitant le libre partage des connaissances, des données d'expérience et des compétences, et en tenant des séminaires, des ateliers et des conférences spécialisés sur cette question ;

23. *invite* le Secrétariat de l'UIP, de concert avec les organisations concernées, à promouvoir cette nouvelle vision de la cybersécurité en soutenant les parlements dans leurs efforts de renforcement des capacités ;

24. *recommande* que l'UIP, en tant qu'organisation mondiale des parlements, joue un rôle prépondérant dans la prévention et la lutte contre la cybercriminalité et la promotion de la cyber-résilience en participant à tous les forums internationaux pertinents, notamment ceux organisés par les Nations Unies, pour faire entendre la voix des parlements ;

25. *préconise* de créer un groupe de travail sur la cybercriminalité, subsidiaire du Conseil directeur de l'UIP, avec pour mission de se conformer aux mandats et objectifs établis dans la présente résolution, et qui sera chargé de soutenir le processus de promotion d'une convention internationale sur la cybercriminalité dans le cadre du système des Nations Unies et de renforcer les capacités des Parlements membres de l'UIP en matière d'élaboration des lois, de contrôle et de budgétisation.

26. *recommande* que l'UIP sensibilise les parlements à la réalisation des Objectifs de développement durable en faisant valoir, en premier lieu, leurs engagements universels en matière de sécurité numérique.