Document final du segment parlementaire organisé à l'occasion du 17e Forum sur la gouvernance de l'Internet de l'ONU

Faire face aux cybermenaces : approches nationales, régionales et internationales

1er décembre 2022

Nous, parlementaires participant au segment parlementaire du 17e Forum sur la gouvernance de l'Internet de l'ONU,

réunis dans le cadre du 17e Forum sur la gouvernance de l'Internet de l'ONU (FGI) et ayant discuté de questions relatives aux approches nationales, régionales et internationales – menées par les États, multilatérales et multipartites – en matière de lutte contre les cybermenaces,

nous félicitant de la poursuite et du renforcement du segment parlementaire du FGI, et nous appuyant sur les recommandations formulées lors des éditions 2019, 2020 et 2021, qui encourageaient les parlements nationaux à coopérer et à échanger leurs bonnes pratiques en matière de politique numérique,

saluant le rôle joué par le Département des affaires économiques et sociales (DESA) de l'ONU, l'Union interparlementaire (UIP) et la Chambre des représentants du Peuple de l'Éthiopie dans l'organisation conjointe du segment parlementaire du FGI 2022, ainsi que le soutien apporté par le Secrétariat du FGI,

rappelant la résolution 74/304 de l'Assemblée générale des Nations Unies du 9 septembre 2020, qui préconise de renforcer la coopération entre l'ONU, les parlements nationaux et l'Union interparlementaire,

prenant note du *Plan d'action de coopération numérique* et du rapport *Notre programme commun* du Secrétaire général de l'ONU, qui soulignent l'importance de renforcer la coopération multipartite pour assurer la sécurité en ligne,

notant que, si Internet et les technologies numériques façonnent de plus en plus nos économies et nos sociétés, ils créent aussi des vulnérabilités pour les personnes, les entités publiques et privées, les infrastructures essentielles, et bien d'autres,

rappelant que la "cybersécurité" et la "cybercriminalité" sont des questions liées mais distinctes, la "cybersécurité" devant être améliorée et la "cybercriminalité" devant être enrayée,

soulignant l'importance des instruments internationaux tels que la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), à laquelle 68 États ont déjà adhéré, et des instruments régionaux tels que la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo), ainsi que le rôle que ces instruments peuvent jouer pour promouvoir la coopération internationale et régionale,

reconnaissant que les enjeux géopolitiques ne sont jamais absents des discussions sur la cybersécurité, tout en affirmant que tous les pays ont un intérêt commun à renforcer la cybersécurité et à lutter contre la cybercriminalité,

reconnaissant également que le panorama des cybermenaces est complexe et que les pays n'ont pas tous le même niveau de préparation face à ces menaces,

notant que les questions de cybersécurité et de cybercriminalité ont des dimensions transorganisationnelles et transfrontalières, et que s'atteler à ces questions exige :

a) des approches mobilisant l'ensemble du gouvernement et de la société, avec des partenariats solides et une action menée conjointement par les autorités et les organismes compétents, le secteur privé, les milieux techniques, le monde universitaire et la société civile,
b) une coopération régionale et internationale efficace et concrète, et qui soit à la fois intergouvernementale, multilatérale et multipartite,

1. *demandons* aux parlements, aux gouvernements et à toutes les autres parties prenantes de travailler ensemble pour mettre au point des cadres politiques, réglementaires et législatifs en vue de renforcer la cybersécurité et de lutter contre la cybercriminalité, et *recommandons* que ces cadres :

a) soient élaborés de manière ouverte et transparente, avec la participation dès le départ de tous les acteurs gouvernementaux et non gouvernementaux concernés ;
b) prévoient une approche de la sécurité axée sur les personnes et intègrent les principes de l'état de droit, du contrôle judiciaire, de la proportionnalité, de la redevabilité et de la transparence ;
c) prévoient également un financement suffisant pour que les autorités chargées de leur mise en œuvre disposent des ressources financières, techniques et humaines nécessaires pour accomplir les tâches qui leur incombent ;
d) définissent clairement les rôles et les responsabilités des acteurs publics et privés concernés, afin que ceux-ci puissent collaborer de manière concrète et efficace en faveur d'un cyberespace plus sûr ;
e) s'appuient sur des normes techniques internationalement reconnues en matière de cybersécurité ;
f) soient cohérents avec la législation existante élaborée pour le monde analogique, par exemple celle visant à lutter contre les discours de haine ou contre la fraude ;

2. *appelons* les parlements à assurer un bon équilibre entre les mesures visant à renforcer la cybersécurité et à lutter contre la cybercriminalité, d'une part, et la protection des libertés fondamentales et des droits de l'homme reconnus sur le plan international, d'autre part, et en particulier à :

a) veiller à ce que les cadres relatifs à la cybersécurité soient assortis de lois strictes en matière de protection des données ;
b) encourager une coopération efficace entre les services de renseignement et les autres services gouvernementaux, et inviter les services de renseignement chargés de la cybersécurité à faire preuve de transparence et de redevabilité ;
c) éviter l'utilisation des mesures de cybersécurité à des fins politiques, par exemple pour cibler des opposants politiques ;

3. *appelons* également les parlements à :
a) entretenir un dialogue régulier avec les ministères et organismes compétents, veiller à ce que le gouvernement accorde l'attention voulue à la lutte contre les cybermenaces, et demander aux autorités de rendre compte des progrès accomplis pour renforcer la cybersécurité et enrayer la cybercriminalité ;
b) réfléchir aux mécanismes institutionnels les plus appropriés pour aborder les enjeux liés aux cybermenaces dans les parlements, notamment en précisant le mandat des commissions parlementaires existantes ou en créant des commissions spécialisées ;
c) promouvoir une coopération efficace entre les autorités publiques et le secteur privé pour renforcer la cybersécurité, ainsi que la création d'un climat de confiance propice à cette coopération ;
d) examiner les possibilités offertes par les technologies numériques, telles que l'intelligence artificielle, dans le cadre de la lutte contre la cybercriminalité, et les mesures de protection des droits de l'homme nécessaires pour éviter une utilisation abusive de ces technologies ;

4. *appelons* les parlementaires à :
a) contribuer aux efforts déployés pour sensibiliser l'ensemble de la société, renforcer ses capacités et y instaurer une culture de la cybersécurité ;
b) traduire les questions de cybersécurité en concepts accessibles à tous, aider le public à comprendre les enjeux et renforcer la volonté politique de faire face aux cybermenaces ;
c) saisir toutes les occasions possibles d'encourager la population à pratiquer une bonne cyber-hygiène ;
d) s'efforcer d'encourager les femmes à entreprendre des carrières dans le domaine de la cybersécurité et de lutter contre les incidents de cybercriminalité qui ciblent les femmes ;
e) trouver des moyens de faire entrer la problématique des cybermenaces dans le débat politique général, d'attirer l'attention des médias et d'accroître la pression sur les gouvernements pour qu'ils agissent ;
f) étudier la possibilité d'organiser des événements spéciaux dans les parlements afin de susciter le débat sur les cybermenaces, par exemple des "journées de la cybersécurité" ou des séances de questions avec les ministères et services concernés ;

5. *encourageons* les parlements, compte tenu des possibilités offertes par les instruments régionaux et internationaux pour favoriser l'harmonisation des cadres juridiques et réglementaires en matière de cybersécurité et de cybercriminalité et pour renforcer la coopération internationale, à :
a) envisager la ratification des instruments internationaux existants tels que la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) et des instruments

régionaux tels que la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo) ;
b) veiller à ce que les conventions ratifiées soient prises en compte dans les politiques, les réglementations et les législations nationales, et soient dûment mises en œuvre au niveau national ;
c) inciter leurs gouvernements à participer à la négociation de nouveaux instruments sur la cybercriminalité au niveau de l'ONU, ainsi qu'aux processus internationaux relatifs aux normes pour un comportement responsable des États dans le cyberespace ;
d) inciter également leurs gouvernements à veiller à ce que leurs positions dans ces processus soient éclairées par un dialogue multipartite et à ce que tout nouvel instrument soit compatible avec les normes de l'état de droit et les instruments relatifs aux droits de l'homme en vigueur ;

6. *appelons* les partenaires internationaux du développement à :
a) faire participer les parlements à toutes les étapes des initiatives visant à soutenir l'élaboration de cadres politiques, réglementaires et législatifs destinés à renforcer la cybersécurité et à lutter contre la cybercriminalité ;
b) renforcer la capacité des parlementaires à travailler sur les questions liées à la cybersécurité et à la cybercriminalité ainsi que sur des sujets de politique numérique plus larges, par le biais notamment de la formation et du développement des compétences ;

7. *invitons* les parlements à renforcer le dialogue et les échanges d'expériences avec d'autres parlements et instances parlementaires, notamment en partageant des informations sur les initiatives législatives existantes et nouvelles liées à la cybersécurité et à la cybercriminalité aux niveaux national et régional ;

8. *appelons* les parlements et les parlementaires à :
a) contribuer au renforcement du dialogue national multipartite sur les questions de politique relatives à Internet ;
b) poursuivre et renforcer leur collaboration avec le FGI, prendre part aux initiatives nationales et régionales du FGI et exploiter les travaux menés dans ces forums en tant que ressources pour étayer leurs discussions et activités parlementaires ;
c) participer aux processus mondiaux visant à renforcer la coopération numérique, et notamment à l'élaboration du pacte numérique mondial proposé par le Secrétaire général de l'ONU ;

9. *accueillons* avec intérêt la publication, par le Secrétariat du FGI, du *Guide to key digital policy issues and related processes and organizations: Toolkit for parliamentarians* (guide pour les parlementaires sur les principales questions de politique numérique et les processus et organisations connexes), et :
a) encourageons les parlementaires à se servir de ce guide pour étoffer, le cas échéant, leur travail sur les questions de politique numérique ;
b) recommandons que ce guide soit actualisé en tant document vivant et évolutif ;

10. *demandons* au FGI d'institutionnaliser davantage le segment parlementaire et de faciliter des échanges réguliers entre les parlementaires et les autres parties prenantes du FGI.