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)

Commission permanente
de la paix et de la sécurité internationale

C-I/146/M
17 janvier 2023

Cyberattaques et cybercriminalité : les nouveaux risques pour la sécurité mondiale

***Mémoire explicatif* présenté par les co-rapporteurs**
Mme S. Falaknaz (Émirats arabes unis) et M. J. Cepeda (Espagne)

1. Nous vivons dans un cybermonde. Des millions de personnes échangent entre elles via Internet en utilisant toutes sortes d'appareils et en partageant avec le monde entier leurs données, leurs informations personnelles, leur identité et leur activité quotidienne. Notre quotidien, nos données personnelles, nos services de santé, nos infrastructures et notre sécurité sont régis par des réseaux situés dans le cyberespace.

2. À mesure que les technologies ont progressé et que notre dépendance à leur égard s'est accrue, la cybercriminalité et les cyberattaques contre les citoyens, les groupes vulnérables, les institutions, les gouvernements ou les États ont également augmenté, de pair avec la nécessité d'assurer notre sécurité.

3. Les nombreuses mesures de confinement prises partout dans le monde en raison de la pandémie de COVID-19 ont favorisé l'achat et l'utilisation d'appareils électroniques permettant aux citoyens de rester en contact avec le monde extérieur. Cette transformation numérique à marche forcée a entraîné une forte augmentation de la cybercriminalité.

4. Les parlements sont conscients du risque que représente cette situation pour les citoyens. C'est la raison pour laquelle les co-rapporteurs ont élaboré la présente résolution, afin de protéger les citoyens contre un cyberespace hostile et de sensibiliser la communauté internationale à la nécessité de lutter contre la cybercriminalité et les cyberattaques, en coopérant et en partageant une vision commune sur la façon d'agir efficacement contre les criminels et les pirates informatiques, qui ne connaissent ni frontières ni limites.

5. La présente résolution vise également à examiner les enjeux de la lutte contre la cybercriminalité et les cyberattaques, à renforcer le rôle des parlements face aux risques qui y sont associés et à contribuer aux efforts internationaux en la matière.

6. La lutte contre la cybercriminalité et les cyberattaques se heurte à plusieurs difficultés, notamment des désaccords sur les définitions, l'obsolescence de la législation et la forte prévalence de pratiques qui compromettent la confidentialité, l'intégrité et la disponibilité des données informatiques. Les différences de législation entre pays retardent souvent les procédures contentieuses. L'évolution rapide de ces crimes exige une plus grande coopération internationale.

7. Plusieurs initiatives en matière de cybercriminalité ont déjà été lancées aux niveaux régional et international, notamment la création par l'Assemblée générale des Nations Unies d'un comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Cette convention doit être adoptée par l'Assemblée générale lors de sa soixante-dix-huitième session, en 2024. L'UIP a également abordé la question des interactions conflictuelles dans le cyberespace dans sa résolution intitulée *La cyber-guerre : une grave menace pour la paix et la sécurité mondiale* (2015).

8. La nature de ces crimes et leur multiplication ont donné naissance à de nouveaux domaines d'action et à de nouvelles initiatives aux niveaux régional et international, par exemple :

   a) le deuxième Protocole additionnel à la Convention de Budapest sur la cybercriminalité du Conseil de l'Europe, approuvé en 2021, qui établit un bouclier juridique pour la protection des droits de l'homme, de l'état de droit et des données personnelles ;

   b) les nouvelles initiatives promues par certaines institutions pour obliger les fabricants et les fournisseurs de produits ou de services TIC qui opèrent sur leur territoire à proposer des "systèmes de certification sécurisée" ou la création de nouveaux systèmes d'identification et d'authentification électroniques sûrs et fiables, par exemple des porte-monnaie numériques personnels utilisant la technologie de la chaîne de blocs et intégrés dans les téléphones portables, qui proposent de nouvelles solutions en matière de garanties, de traçabilité et d'identité sur Internet réclamées par certaines organisations, comme INTERPOL, pour lutter contre la criminalité.

9. Aux fins de préparation du présent projet de résolution, les co-rapporteurs ont participé aux réunions suivantes :

   - la deuxième session du Comité spécial des Nations Unies susmentionné, à Vienne en mai et juin 2022 ;
   - deux réunions de consultation intersessions multipartites organisées par la Présidente du Comité spécial (juin et novembre 2022), au cours desquelles ils ont communiqué des informations sur les travaux menés par l'UIP dans le domaine de la lutte contre la cybercriminalité et les cyberattaques ;
   - l'audition d'experts sur le thème de la résolution organisée par la Commission permanente de la paix et de la sécurité internationale lors de la 145e Assemblée de l'UIP à Kigali, en octobre 2022, au cours de laquelle ils ont reçu des contributions de la part d'experts et d'homologues de différentes régions du monde, ainsi que du Forum des jeunes parlementaires ;
   - le volet parlementaire du Forum sur la gouvernance de l'Internet, organisé en Éthiopie en décembre 2022, qui visait à souligner l'importance de disposer d'une vision parlementaire pour lutter contre les futures cybermenaces auxquelles pourraient être confrontés les citoyens et créer un espace numérique plus sûr ;
   - l'audition en ligne sur le thème *Créer un cyberespace sûr pour la démocratie*, organisée en décembre 2022 par l'UIP en collaboration avec la Présidente du Comité spécial afin de favoriser la prise en compte du point de vue des parlementaires dans la préparation de la convention sur la cybercriminalité et de recueillir des contributions pour l'élaboration de la présente résolution de l'UIP.

10. Les co-rapporteurs ont également participé à des réunions bilatérales avec diverses organisations, comme le Service de la criminalité organisée et du trafic de l'Office des Nations Unies contre la drogue et le crime (ONUDC) et INTERPOL, et ont pu découvrir *in situ* les systèmes de protection mis en place pour lutter contre les cyberattaques dans différents pays comme l'Albanie, l'Argentine, le Costa Rica, les Émirats arabes unis, l'Espagne, le Mexique et la République dominicaine, où ils ont également pu découvrir le travail mené par les services de sécurité et de renseignement, ainsi que les mesures prises par les parlements et d'autres institutions.

11. Toutes ces réunions et visites ont permis d'identifier les différents niveaux où il faut agir :

    a) Les cyberattaques entre États dans le cadre de guerres hybrides. La question des conflits et de la guerre dans le cyberespace a déjà été examinée par l'UIP dans sa résolution de 2015 intitulée *La cyber-guerre : une grave menace pour la paix et la sécurité mondiale*, qui souligne que les mesures de cyberdéfense et de lutte contre la cybercriminalité sont complémentaires. Il importe de noter que les gouvernements peuvent faire appel aux services d'acteurs non étatiques pour mener des cyberattaques contre des pays tiers, ce qui peut entraîner une escalade et constituer une menace pour la paix dans le monde.

    b) Les campagnes de cyberattaques sous forme de cyberespionnage, de vol de propriété intellectuelle, d'extorsion de données et d'informations détenues par des organismes gouvernementaux, des parlements, des institutions publiques ou privées (attaques par rançongiciels), ou d'attaques menées par des cybercriminels contre les infrastructures stratégiques d'un pays. Certaines de ces campagnes peuvent être définies comme des "menaces persistantes avancées", à savoir des cyberattaques complexes menées à grande échelle, par lesquelles des intrus s'établissent de façon illicite et durable sur un réseau afin de récupérer des données hautement sensibles.

    c) Les attaques cybercriminelles, sous forme de délits en ligne, menées par des délinquants qui se livrent à des activités criminelles réalisées à l'aide d'Internet ou d'autres outils de communication numérique et qui ciblent en priorité les citoyens. Ces attaques ont divers objectifs, notamment l'usurpation d'identité, la fraude, la distribution de matériel illégal ou protégé par le droit d'auteur, la vente de drogue, le blanchiment d'argent, les crimes de haine, la propagande, l'endoctrinement extrémiste et l'exploitation sexuelle des femmes et des enfants, et utilisent différentes tactiques, techniques et méthodes comme l'hameçonnage, le piratage, l'utilisation de robots informatiques ou les attaques par déni de service, faisant du cyberespace un endroit peu sûr et hostile pour tous les citoyens à travers le monde.

12. Qu'il s'agisse de cyberattaques à grande échelle menées par des groupes organisés ou de délits en ligne perpétrées par des délinquants, la réponse à la cybercriminalité ne peut reposer que sur la coopération internationale, en amenant les pays à mutualiser leurs informations et leurs connaissances sur les tactiques, techniques et procédures utilisées par ces pirates informatiques.

13. Le projet de résolution :

- appelle les parlements à adopter de nouvelles lois et à développer la coopération internationale pour lutter contre la cybercriminalité et les cyberattaques, compte tenu de l'augmentation constante de ces activités contre les citoyens, les groupes vulnérables, les institutions, les gouvernements ou les États, de leur lien avec les libertés fondamentales telles que la vie privée et la liberté d'expression, du fait qu'elles ne doivent pas porter atteinte ou diminuer la capacité des citoyens à jouir de ces libertés, et de leurs conséquences sur la paix et la sécurité internationale et la stabilité économique mondiale ;
- encourage les parlements à soutenir les efforts déployés par l'ONU en vue d'adopter une nouvelle convention sur la cybercriminalité et à l'utiliser pour renforcer la législation nationale et accroître la coopération internationale en matière de lutte contre la cybercriminalité et les cyberattaques ;
- appelle les parlements à utiliser au mieux leurs outils de contrôle pour s'assurer que l'exécutif agit contre l'augmentation rapide de la cybercriminalité tout en respectant la vie privée des utilisateurs dans le cyberespace ;
- appelle également le Secrétariat de l'UIP à jouer un rôle déterminant pour aider les parlements à renforcer leurs capacités en organisant des conférences, des ateliers et des séminaires spécialisés qui peuvent contribuer à faire comprendre la nature complexe et l'évolution rapide de la cybercriminalité et des cyberattaques et à lutter contre ces phénomènes.