Union Interparlementaire
Pour la démocratie. Pour tous.

145e Assemblée de l'UIP

Kigali (Rwanda)
11-15 octobre 2022

145e ASSEMBLÉE DE L'UIP
2022 | Kigali, Rwanda

Commission permanente
de la paix et de la sécurité internationale

C-I/145/6-Inf.1
13 septembre 2022

Audition d'experts sur le thème *Cyberattaques et cybercrimes : les nouveaux risques pour la sécurité mondiale*

Vendredi 14 octobre 2022, 14 h 30 – 16 h 30
(Salle MH1, rez-de-chaussée, Kigali Convention Centre (KCC))

Note d'orientation

Nous vivons aujourd'hui dans un monde en proie aux conflits à grande échelle. Aucun gouvernement ni parlement du monde ne pouvait prévoir les souffrances endurées par tous les habitants de notre planète dans le contexte d'une pandémie telle que la pandémie de COVID-19.

Pour protéger les citoyens, tous les gouvernements ont pris la décision de soumettre des millions de personnes sur la planète entière à des restrictions et des confinements.

Le confinement des citoyens à leur domicile a fait augmenter les connexions aux réseaux, ainsi que l'achat d'appareils, de caméras, d'ordinateurs et de smartphones permettant de se connecter aux entreprises et aux établissements scolaires, voire tout simplement de communiquer avec les membres de la famille et les amis.

Cette numérisation forcée a permis à la population de préserver ses liens sociaux et professionnels avec son milieu de travail, avec les établissements scolaires et les universités, et tout particulièrement avec les établissements médicaux et les médias. Elle a donc pu suivre en temps réel l'évolution de la pandémie et les mesures adoptées dans les différents pays.

La numérisation à un rythme accéléré a ouvert de nouveaux espaces de communication, inconnus de beaucoup jusqu'alors. Des espaces plus dangereux, tant au niveau personnel que collectif, ont toutefois également fait leur apparition, espaces que les cybercriminels ont investis en faisant appel à de nouveaux types de cyberattaques.

Par ailleurs, le grave conflit qui fait rage en Ukraine a déclenché des hostilités comme l'Europe n'en connaissait plus depuis la Deuxième Guerre mondiale et il révèle que les cyberattaques peuvent également être utilisées, dans les périodes de grande tension, à des fins belliqueuses.

Nous devons œuvrer à l'interdiction des armes létales autonomes (également connues sous le nom de "robots tueurs"), protéger en priorité toute l'infrastructure nucléaire d'éventuelles cyberattaques extérieures et éviter une nouvelle escalade de la menace nucléaire à l'échelle mondiale.

D'énormes campagnes de désinformation et de propagande sont menées par des cyber-militants organisés qui, conscients de l'absence de cadres de coopération juridique internationaux, se servent des plateformes numériques pour corrompre et influencer des groupes, des régions ou des pays.

Les attaques directes contre les infrastructures informatiques critiques d'un pays remettent en cause les réseaux de distribution de base approvisionnant nos sociétés en biens de première nécessité.

Tout ceci devrait nous faire réfléchir pour mieux appréhender la réalité mondiale dans laquelle nous sommes plongés en notre qualité de parlementaires. De nos jours, connaître la vérité devient un luxe de plus en plus précieux.

Ce nouveau contexte numérique exige aussi, tant des parlements que de l'ONU, l'adoption de mesures destinées à mettre le mieux possible à profit les avantages et le potentiel de notre société de la connaissance, tout en limitant au minimum les risques graves qu'elle fait peser sur nous.

L'article 19 de la Déclaration universelle des droits de l'homme affirme que tout individu a le droit de recevoir et de répandre, sans considération de frontières, les informations et les idées par quelque moyen d'expression que ce soit. Nous devons donc garantir à tous les citoyens de nos sociétés un accès libre à une information objective, véridique et de qualité.

Dans l'esprit de la Déclaration universelle des droits de l'homme, nous devons veiller à la constitution d'un espace public commun qui, loin de heurter, cliver, polariser ou détruire notre capacité à vivre ensemble par des messages viraux de haine, renforce chaque jour un peu plus nos démocraties.

Nous devons avoir le droit de protéger nos données et nos informations personnelles, utilisées pour manipuler et infléchir notre comportement, nous contrôler et violer nos droits de l'homme, tout en sapant les institutions démocratiques.

Nous devons légiférer pour définir les limites des algorithmes opaques et du recours aux profils psychographiques par les grandes entreprises, afin que les organisations malveillantes et les cybercriminels ne puissent pas faire appel aux réseaux sociaux pour manipuler les électeurs et influencer leur réflexion.

Nous devons inciter le secteur public, le secteur privé et la société civile à adopter de nouveaux cadres législatifs et d'auto-régulation propices à la constitution d'un espace sûr de coopération numérique mondiale.

En notre qualité de parlementaires, nous devons créer des cadres de coopération juridique internationale nous permettant de lutter efficacement contre les cybercriminels qui, échappant à tout contrôle, peuvent se mettre au service d'intérêts obscurs fomentant des attaques contre l'infrastructure critique de nos pays.

Les cybercriminels, parfaitement conscients des limites auxquelles se heurtent les pays désireux de les poursuivre, agissent à l'échelle mondiale en attaquant en masse les utilisateurs des réseaux au moyen de techniques visant leurs mots de passe et de stratégies d'ingénierie sociale telles que l'hameçonnage, vocal ou par sms (entre autres), ou les pourriels. Ils s'attaquent aussi aux connexions des utilisateurs au moyen de réseaux wifi malveillants, programmes espions, cookies, attaques par déni de service distribuées (DDoS) et injections SQL et déclenchent en outre des attaques par le biais de logiciels malveillants tels que les virus, les logiciels publicitaires ,les logiciels espions, les chevaux de Troie, les portes dérobées (backdoors), les enregistreurs de frappes (keyloggers), les escroqueries, les logiciels de rançon (ransomware), les outils de dissimulation d'activité (rootkits), les réseaux de robots (botnets), les programmes malveillants (rogueware), le minage de cryptomonnaie par cryptojacking et autres applications malveillantes.

En 2015, les Membres de l'UIP ont adopté à l'occasion de l'Assemblée de Hanoï une résolution sur la cyber-guerre, qui portait également sur la cybercriminalité. Cette résolution appelait à la conclusion d'une convention internationale traitant de ces délits.

Nos parlements, quant à eux, doivent offrir des structures opérationnelles aptes à protéger les secteurs particulièrement vulnérables de la société (les femmes, les jeunes, les enfants, les entreprises et l'infrastructure critique) et soutenir les initiatives de nature à déceler, classer, analyser et prévenir les cyberattaques.

Concernant la Convention sur la cybercriminalité, l'UIP peut et doit apporter une contribution de premier plan, par le biais de l'ONU, aux efforts entrepris à l'échelle mondiale pour proposer dans n'importe quel pays du monde des services de prévention, d'information, de détection et de riposte adaptée en cas d'incident relatif à la cybersécurité.