Union Interparlementaire
Pour la démocratie. Pour tous.

132ème Assemblée de l'UIP

Hanoï (Viet Nam), 28 mars - 1er avril 2015

Commission permanente
de la paix et de la sécurité internationale

C-I/132/DR
15 janvier 2015

La cyber-guerre : une grave menace pour la paix et la sécurité mondiale

***Projet de résolution* présenté par les co-rapporteurs,**
MM. N. Lazrek (Maroc) et J.C. Mahia (Uruguay)

La 132ème Assemblée de l'Union interparlementaire,

1) *convaincue,* au vu des immenses avantages socio-économiques que le cyberespace apporte à l'ensemble des citoyens du monde, qu'il est essentiel d'assurer prévisibilité et stabilité dans ce domaine,

2) *pleinement consciente* que nombre de concepts, définitions et normes de la cyber-politique, en particulier en ce qui concerne la paix et la sécurité internationales, ne sont pas communément compris et n'ont pas encore été clarifiés aux niveaux national, régional et multilatéral, et que le consensus international fait encore défaut dans certains domaines,

3) *reconnaissant* que le droit international public ainsi que la jurisprudence de certains organes conventionnels et certains instruments juridiques, en particulier la Charte des Nations Unies, les Conventions de Genève et leurs protocoles additionnels, la Déclaration universelle des droits de l'homme et le Pacte international relatif aux droits civils et politiques, sont pertinents et applicables à l'utilisation par les Etats des technologies de l'information et de la communication (TIC) et sont essentiels à la réduction des risques, au maintien de la paix et de la stabilité internationale et à la promotion d'un environnement informatique ouvert, sécurisé, pacifique et accessible,

4) *considérant* que le cyberespace dépasse l'internet et inclut non seulement le matériel, les logiciels, les données et les systèmes d'information mais aussi les personnes et les interactions sociales au sein de ces réseaux et de l'infrastructure tout entière,

5) *parfaitement consciente* du fait que les différents domaines de la cyber-politique sont distincts mais inextricablement liés et que les décisions prises dans des domaines tels, entre autres, que la gouvernance de l'internet, ont un impact sur les dimensions de paix et de sécurité internationales du cyberespace,

6) *considérant* que le cyberespace peut être perçu comme une nouvelle dimension de conflit ainsi qu'un nouveau champ d'activité dans lequel nombre des composantes du cyberespace, voire la plupart d'entre elles, ont des applications à la fois civiles et militaires,

7) *consciente* de ce que le cyberespace n'est pas un lieu isolé et que des activités de déstabilisation dans le cyberespace peuvent entraîner d'autres formes d'insécurité ou de conflits traditionnels,

8) *convaincue* que, en raison de l'inter-connectivité des réseaux informatiques militaires et civils, les Etats doivent encourager le secteur privé et la société civile à jouer un rôle approprié pour améliorer la sécurité des TIC et de leur utilisation, notamment en ce qui concerne la sécurité de la chaîne d'approvisionnement des produits et des services informatiques, et *convaincue en outre* qu'une coopération régionale et internationale est nécessaire pour lutter contre les menaces résultant d'une utilisation malveillante des TIC,

9) *constatant* que l'utilisation des TIC a remodelé l'environnement sécuritaire international et que, si ces technologies ont une immense utilité économique et sociale, elles peuvent aussi être utilisées à des fins contraires à la paix et à la sécurité internationales, et *constatant par ailleurs* que le risque que les TIC soient utilisées par des acteurs étatiques et non étatiques pour mener des activités criminelles et de déstabilisation a considérablement augmenté ces dernières années,

10) *considérant* que la cyber-guerre peut comprendre, sans nécessairement s'y limiter, des opérations contre un ordinateur ou un système informatique passant par l'utilisation d'un flux de données comme moyen ou méthode de guerre pour donner la mort, blesser, causer la destruction ou des dommages pendant des conflits armés,

11) *notant* que, même si la cyber-guerre n'a heureusement pas encore eu de conséquences humanitaires dramatiques, on ne mesure pas encore complètement les réalités militaires du cyberespace et les impacts de certaines activités, et *notant par ailleurs* que de nombreuses cyber-activités sont susceptibles de déstabiliser les conditions de sécurité du cyberespace sans nécessairement constituer un "recours à la force",

12) *reconnaissant* qu'un défaut de communication stratégique entre Etats, l'absence d'attribution rapide des responsabilités et une perception limitée des priorités des alliés et des adversaires peuvent mener à des erreurs de jugement, d'appréciation et des malentendus dans le cyberespace,

13) *considérant* que le fait qu'il n'y ait pas une perception commune du comportement qui est acceptable de la part d'un Etat en matière d'utilisation des TIC augmente les risques pour la paix et la sécurité internationales et que la mise au point et la diffusion de techniques et d'outils malveillants sophistiqués par des acteurs étatiques et non étatiques peuvent engendrer des erreurs d'appréciation et une escalade involontaire,

14) *condamnant* l'usage des TIC par les groupes terroristes pour communiquer, recueillir des informations, recruter, organiser, planifier et coordonner des attaques, promouvoir leurs idées et leurs actions et solliciter des financements,

15) *considérant* qu'il est nécessaire de trouver un équilibre entre contrôle des ordinateurs et des systèmes de communication à des fins de sécurité et respect de la vie privée des individus et des secrets d'Etat,

au niveau national

1. *recommande* que les parlements renforcent leurs capacités afin de mieux appréhender la complexité de la sécurité internationale dans le cyberespace et de prendre en compte l'interconnexion entre les différents aspects de l'élaboration de la cyber-politique;

2. *encourage* les parlements à travailler avec les autres pouvoirs de l'Etat à une appréciation générale de la dépendance, ainsi que des risques et des difficultés dans le cyberespace à l'échelon national;

3. *appelle* tous les parlements à réviser le cadre juridique de leur pays afin de l'adapter au mieux aux nouvelles menaces susceptibles de découler de la nature évolutive du cyberespace;

4. *encourage* les parlements à contrôler scrupuleusement les finances publiques pour s'assurer que des ressources suffisantes sont allouées à la cyber-sécurité et à la cyber-défense et que cet argent est employé à bon escient pour atteindre les objectifs visés;

5. *encourage également* les parlements à faire usage de tous les outils de contrôle à leur disposition pour s'assurer que les activités en lien avec le cyberespace sont soumises à un examen rigoureux;

6. *recommande* aux parlements des Etats qui ne l'ont pas encore fait d'exiger de leur gouvernement qu'il déclare expressément que le droit international, notamment le droit des conflits armés, s'applique à la cyber-guerre afin de faire en sorte que des limites soient posées à l'utilisation de cyber-opérations comme moyen ou méthode de guerre, tout en notant que les modalités d'application exactes sont encore en discussion au niveau international;

7. *appelle* tous les parlements à veiller à une participation significative du secteur privé et de la société civile au traitement de ces problèmes;

8. *recommande* aux parlements de s'assurer que la législation applicable au cyberespace distingue bien le civil du militaire et de faire preuve de mesure dans l'encadrement de l'utilisation des outils informatiques par les citoyens;

au niveau international

9. *recommande* que soient envisagées, aux niveaux législatif et exécutif, des mesures de coopération de nature à favoriser la paix, la stabilité et la sécurité internationales, ainsi qu'une définition commune du droit international applicable et des normes, règles et principes qui en découlent quant au comportement à adopter par les Etats;

10. *recommande également* que les parlements poussent à la clarification et à l'adoption au niveau régional, et par la suite au niveau international, de mesures concrètes de renforcement de la confiance visant à accroître la transparence, la prévisibilité et la coopération et à réduire les malentendus, ce qui limiterait le risque de conflit;

11. *exhorte* l'UIP, ainsi que les organisations internationales compétentes, à soutenir la coopération parlementaire afin de promouvoir la mise en commun des bonnes pratiques quant aux mesures concrètes à prendre pour renforcer la confiance et, partant, favoriser la paix, la stabilité et la sécurité internationales;

12. *encourage* les parlements à jouer un rôle positif dans la création d'un environnement sécurisé à l'appui d'une utilisation pacifique du cyberespace et à veiller à établir un juste équilibre entre la liberté d'expression et l'échange d'informations, d'une part, et les moyens nécessaires pour protéger la sécurité, d'autre part.