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/M
22 January 2015

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

***Mémoire explicatif* présenté par les co-rapporteurs**
M. N. Lazrek (Maroc) et M. J.C. Mahía (Uruguay)

1. Au cours des dernières années, l'utilisation accrue de l'internet et de systèmes informatiques interconnectés a entraîné une forte augmentation du nombre des cyber-attaques. Aujourd'hui, presque chaque conflit politique, économique ou militaire comporte également une composante cybernétique. Le terme de "cyber-guerre" est régulièrement utilisé par les médias pour décrire des situations extrêmement diverses aux conséquences multiples ne relevant pas toujours de la cyber-guerre à proprement parler.

2. Afin de rédiger le projet de résolution, les co-rapporteurs de la Commission permanente de la paix et de la sécurité internationale, se sont en premier lieu chargés de distinguer la cyber-guerre des autres composantes de la cyber-sécurité que sont la cyber-criminalité, le cyber-terrorisme et le cyber-espionnage.

3. Ces dernières sont principalement le fait d'acteurs privés (individus, groupes ou entreprises), bien que les Etats puissent eux procéder à une surveillance étroite des entreprises et des citoyens. En tout état de cause, ces cyber-menaces visent tant les économies nationales que la vie privée et ont un impact direct sur l'intérêt du public et des nations. La technologie évoluant rapidement, l'approche juridique de la protection de la vie privée prend bien souvent du retard, montrant clairement le dilemme entre la nécessité de protéger la sécurité et le devoir de respecter la vie privée et les droits fondamentaux. La Commission permanente de la paix et de la sécurité internationale a débattu ce sujet en octobre dernier et le sujet choisi par la Commission permanente de la démocratie et des droits de l'homme pour sa prochaine résolution, *La démocratie à l'ère numérique et la menace pour la vie privée et les libertés individuelles*, est lui aussi lié à cette problématique.

4. Dans leur projet de résolution, les co-rapporteurs se sont tenus au sujet initial adopté par la commission, à savoir *La cyber-guerre, une grave menace pour la paix et la sécurité mondiale*. Pour ce faire, ils ont défini la cyber-guerre comme la guerre menée au travers du cyberespace et englobant principalement des activités militaires consistant à utiliser des systèmes et réseaux informatiques pour attaquer un adversaire. Ils se sont pour cela inspirés des interventions des experts et des parlementaires lors de la réunion-débat organisée à l'occasion de la 131ème Assemblée de l'UIP (Genève, octobre 2014), mais aussi des communications écrites présentées, dans les semaines qui ont suivi, par les Parlements membres de l'UIP. Les co-rapporteurs tiennent à remercier toutes les personnes concernées de leurs contributions.

5. Le projet de résolution fait ressortir que, pour l'heure, l'ensemble de la cyber-législation internationale est encore terriblement opaque et qu'il n'y a pas encore de définition communément acceptée par l'ensemble des acteurs internationaux pour déterminer ce qu'est un « acte de cyber-guerre ». Plusieurs organisations régionales et multilatérales ont pourtant commencé à se pencher sur la question et différentes initiatives ont été mises en place au niveau national, mais aussi au niveau multilatéral, notamment au sein des Nations Unies.

6. Le projet de résolution repose donc sur plusieurs partis-pris. En premier lieu, lier la cyber-guerre au droit de la guerre afin de combler les vides juridiques, et donc de sérier les cyber-attaques et de qualifier celles qui relèvent de la cyber-guerre. En effet, les cyber-attaques menées en temps de paix sans pour autant déclencher la guerre ne peuvent être qualifiées de cyber-guerre. Elles n'appellent ni à l'application du droit de la guerre, ni à une réponse militaire, mais à la mise en œuvre de mesures de coercition non militaires dans le cyberespace ou le monde réel, comme par exemple des mesures économiques, commerciales ou de boycottage. On ne peut donc parler de cyber-guerre que lorsqu'une cyber-attaque a pour effet d'entraîner une situation de guerre.

7. Les co-rapporteurs sont cependant conscients que l'application du droit international existant n'est pas une solution parfaite et, que dans un certain nombre de cas, ce nouvel enjeu pour la sécurité internationale nécessite la transformation et la réinterprétation des règles existantes, voire l'adoption de nouvelles règles.

8. Le deuxième parti-pris consiste à traiter le sujet par étapes. Comme dans le cas d'autres sujets d'ampleur internationale tels que le désarmement nucléaire, une seule résolution ne suffira pas à définir l'action à engager par les parlements à l'égard des activités relevant de la cyber-guerre. Le présent projet de résolution doit se comprendre comme un premier pas sur un sujet relativement nouveau dont la communauté parlementaire internationale prend acte. Au fur et à mesure que la question évoluera, de nouvelles résolutions permettront aux parlements d'actualiser leurs connaissances sur le sujet et de développer de nouvelles stratégies.

9. Le troisième parti-pris est celui de l'action parlementaire. Il est très clair que la plupart des actions à entreprendre pour encadrer la cyber-guerre relèvent des gouvernements. Toutefois, les représentants des peuples que sont les parlementaires sont aussi à même de jouer un rôle essentiel, notamment lorsqu'il s'agit de trouver un équilibre entre sécurité nationale, sécurité humaine et libertés individuelles. Les co-rapporteurs ont par conséquent souhaité que ce projet de résolution porte principalement sur les rôles que les parlements peuvent et doivent jouer, notamment en usant de leurs pouvoirs législatif ou de contrôle qui leur permettent de veiller à ce que les gouvernements se conforment aux engagements et obligations existants ou encore de faire pression sur ces derniers afin de les encourager à contribuer à d'autres actions concrètes.

10. Le projet de résolution reflète la communauté de vue des co-rapporteurs sur une série de questions importantes et constitue une base solide pour le débat qui aura lieu à la 132ème Assemblée de l'UIP. Le document qui sera adopté lors de l'Assemblée devrait offrir la possibilité d'apporter une contribution parlementaire énergique à la définition et à l'encadrement de la cyber-guerre, notamment au travers de mesures concrètes pouvant être prises dans un avenir immédiat.