Le rôle des parlementaires dans la promotion du désarmement dans le cyberespace : un point sur la cyberguerre et la paix

Un séminaire en ligne sur le rôle des parlementaires pour promouvoir le désarmement dans le cyberespace s'est tenu le 27 janvier 2021. Organisé par le Centre de politique de sécurité de Genève (GCSP), l'Union interparlementaire (UIP), le Conseil pour l'avenir du Monde (WFC) et les Parlementaires pour la non-prolifération et le désarmement nucléaires (PNND), il faisait suite à la publication, en novembre 2020, du manuel parlementaire *Défendre notre avenir commun*, qui traite du désarmement pour la sécurité et le développement durable. Plus de 200 personnes ont participé à l'événement, notamment des parlementaires, d'éminents spécialistes de la cybersécurité et du désarmement, des universitaires, des étudiants et des membres de la société civile. Le webinaire, qui s'est déroulé en anglais avec interprétation simultanée en français, a également été l'occasion de présenter l'édition française du manuel.

M. Marc Finaud, responsable des questions de prolifération des armes au GCSP et modérateur du webinaire, a ouvert la session en évoquant la section du manuel parlementaire sur le désarmement pour les générations futures, qui traite de la cyberguerre ainsi que de la paix et du désarmement dans le cyberespace. À des fins de clarté, M. Finaud a défini et expliqué les concepts de cyberespace, cyberguerre et cybersécurité. Il a souligné que le webinaire venait à point nommé face à la menace croissante des cyberdangers. En effet, le *Rapport sur les risques mondiaux 2021* du Forum économique mondial classe les incidents de cybersécurité parmi les risques les plus susceptibles de se concrétiser au cours des dix prochaines années. D'autre part, l'organisation *Bulletin of the Atomic Scientists* explique que les inquiétantes avancées dans l'élaboration de cyberarmes font partie des raisons ayant incité le groupe à décider, le 27 janvier 2021, de maintenir l'heure affichée sur l'"Horloge de la fin du monde" à 100 secondes avant minuit – le niveau de risque le plus élevé pour l'humanité.

Mme Anda Filip, Directrice de la Division des Parlements membres et des Relations extérieures de l'UIP, a présenté l'édition française de *Défendre notre avenir commun*. Dans son introduction, elle a insisté sur le rôle fondamental des parlementaires pour faire progresser les questions de désarmement et a souligné que les parlements représentent une composante institutionnelle clé du changement. Pour Mme Filip, le manuel est un "document communautaire", puisqu'il a été élaboré grâce aux contributions de nombreux partenaires, y compris avec le soutien du Bureau des affaires de désarmement de l'ONU. Mme Filip a également mis en avant les bonnes pratiques, les modèles de politiques et les propositions d'actions concrètes qu'il contient. Enfin, elle a souligné à quel point l'ouvrage pourrait constituer une aide précieuse pour les parlementaires, afin qu'ils deviennent des "défenseurs du désarmement", capables de faire avancer cette question.

M. Saber Chowdhury, Président honoraire de l'UIP, Vice-Président de PNND et parlementaire du Bangladesh, a rappelé la résolution de l'UIP intitulée "La cyberguerre, une grave menace pour la paix et la sécurité", adoptée à la 132e Assemblée de l'UIP, tenue à Hanoi (Viet Nam) en 2015 – sa première Assemblée de l'UIP en tant que Président. M. Chowdhury a expliqué que le rôle des parlementaires est en passe d'être redéfini, modifié et mis en question. Dans le contexte de ces problématiques mondiales, les parlements doivent adopter une approche axée sur la sécurité humaine, afin de trouver un équilibre entre la perception de leurs électeurs au niveau local et le regard mondial qui s'impose pour traiter les questions internationales. De plus, étant donné que les capacités technologiques et cybernétiques progressent plus vite que les actions gouvernementales et multilatérales, l'occasion est donnée aux législateurs de faire preuve de leadership et d'ouvrir la voie à une coopération gouvernementale en la matière. M. Chowdhury a conclu sur une note d'espoir, en rappelant les utilisations pacifiques qui pouvaient être faites du cyberespace, ainsi que la définition et la diffusion d'une vision commune à travers les partenariats et la collaboration entre les parlements et la société civile.

Un sondage a été réalisé auprès des participants sur l'applicabilité du droit international au cyberespace. Si certains se sont montrés pessimistes, la grande majorité estime que les législations internationales sont bel et bien applicables au cyberespace.

M. Tilman Rodenhauser, conseiller juridique au Comité international de la Croix-Rouge (CICR), a enchaîné sur la question clé du sondage. Il a rappelé que le mandat premier du CICR est l'application du droit international humanitaire (DIH) aux conflits armés, puis il a indiqué que le DIH s'applique au cyberespace et qu'il pose des limites à la cyberguerre. En réponse à la première question (Quel est l'usage des cybertechnologies aujourd'hui dans la guerre ?), M. Rodenhauser a expliqué que la plupart des États utilisent déjà le cyberespace dans le cadre de leurs opérations militaires et qu'ils sont nombreux à avoir déjà adopté les cyberopérations en tant que branche à part entière de l'armée, considérant qu'elles ont un rôle de plus en plus important dans les opérations offensives et défensives. Il a relevé trois types de contextes d'application possibles du cyberespace dans les guerres contemporaines : dans le cadre d'opérations défensives (plus les systèmes deviennent numérisés, plus ils devront être protégés contre les cyberattaques), en parallèle d'opérations cinétiques (par exemple pour désactiver les systèmes radar ennemis avant une attaque), et à des fins de dommages physiques.

S'agissant de la seconde question (Quelles sont les principales préoccupations humanitaires et les conséquences potentiellement néfastes ?), M. Rodenhauser a indiqué que la dépendance croissante aux systèmes numériques et leur intégration accrue multiplient les cibles potentielles des cyberattaques à tous les niveaux de la société. Après avoir donné des exemples de cyberattaques contre des installations nucléaires (par exemple, en Iran en 2010 et en Inde en 2019) et des installations électriques (par exemple, en Ukraine en 2017), il a expliqué que de telles attaques peuvent causer des dommages au sein de la population civile et qu'elles devraient être régies par les règles et les normes du DIH, même en temps de guerre. Il a précisé que les établissements médicaux étaient eux aussi exposés aux cyberattaques, dont la concrétisation constituerait une violation du DIH. Enfin, M. Rodenhauser soutient la position du CICR selon laquelle le DIH s'applique aux cyberopérations, et il précise que la Cour internationale de Justice l'a également confirmé. Il a ajouté que la Charte des Nations Unies interdit le recours à la force en temps de paix et oblige les États parties à régler pacifiquement leurs conflits. De plus, les traités relatifs aux droits de l'homme offrent également certaines protections, en particulier en temps de paix. Il a indiqué que le DIH est plutôt considéré comme une branche du droit venant ajouter une protection et compléter d'autres branches du droit international applicables aux cyberopérations. M. Rodenhauser a conclu son exposé en soulignant qu'il existe encore une grande incertitude quant à la multitude d'applications des capacités cybernétiques dans les opérations militaires. Il a insisté sur le fait que les sociétés doivent inciter les gouvernements à expliquer clairement les modalités de protection du cyberespace et que les parlementaires ont un rôle clé en la matière.

Mme Anne-Marie Buzatu, responsable des opérations à la fondation ICT4Peace, a consacré son intervention à examiner des mesures pratiques visant à neutraliser certaines menaces inhérentes aux cyberopérations (civiles ou militaires). Mme Buzatu a exposé en particulier deux propositions concrètes. La première concerne l'adoption de normes et de règles communes régissant les opérations dans le cyberespace. Une cyberattaque ciblant des infrastructures essentielles est une menace réelle à laquelle ICT4Peace accorde toute son attention. Il s'agit d'une question cruciale, puisque dans les sociétés modernes, la plupart des services courants utilisent des infrastructures numériques. En conséquence, ICT4Peace demande aux gouvernements de s'engager à ne pas mener de cyberopérations offensives contre des infrastructures essentielles. Plusieurs normes défendues par ICT4Peace ont été prises en compte et reconnues par des processus internationaux visant à réglementer la conduite dans le monde virtuel.

La seconde proposition est un mécanisme national d'évaluation par les pairs pour les cyberopérations menées par un État à l'étranger. L'objectif serait, d'une part, de pallier (en partie) l'absence de mécanisme de reddition de comptes pour les États menant des cyberopérations touchant d'autres États au moyen d'un processus coopératif pour les rapports. D'autre part, il s'agirait de faciliter la contribution d'autres parties prenantes. Mme Buzatu a souligné les retombées positives d'une telle démarche, qui instaurerait une coopération entre les gouvernements et la communauté internationale dans le but de promouvoir des normes, la transparence et la reddition de comptes. C'est un objectif que les parlementaires peuvent aussi contribuer à atteindre et qui pourrait déboucher sur des mesures concrètes en vue d'une utilisation plus sûre et plus pacifique du cyberespace.

M. Arthur Duforest, assistant de recherche au PNND et étudiant de master en relations internationales, a commencé son exposé par une définition du cyberespace, le qualifiant d'"espace performatif", c'est-à-dire qui n'est pas défini par les éléments qui le composent (ordinateurs, réseaux, Internet), car ceux-ci sont en perpétuelle mutation, mais plutôt par l'utilisation qui en est faite. Le rôle des parlementaires est de faire en sorte que cette utilisation reste pacifique. M. Duforest a résumé quelques points du manuel parlementaire, plus particulièrement le chapitre intitulé "Le désarmement pour les générations futures", en insistant sur l'utilité de plusieurs des ressources présentées dans le manuel en vue d'assurer une utilisation pacifique du cyberespace. Il a mis en avant trois aspects du Manuel de Tallinn : 1) les contre-mesures, risquées dans le cyberespace, car pouvant atteindre une cible erronée ou se propager à des objectifs non militaires ; 2) des partenariats solides entre les États et avec le secteur privé, surtout dans les domaines qui évoluent rapidement et où il est difficile de rester à la page ; 3) l'obligation de diligence, l'une des principales recommandations imposant aux États de

ne pas lancer de cyberattaques et de ne pas utiliser le territoire d'un État à cette fin. De même, s'agissant de la politique du non-recours en premier aux armes nucléaires, et pour faire écho à l'appel de ICT4Peace à la modération dans l'utilisation de la force offensive, M. Duforest a souligné que l'obligation de diligence était une composante essentielle de l'utilisation pacifique du cyberespace. Il a conclu en rappelant toutes les possibilités qu'offre le manuel en termes de changements positifs et a encouragé les parlementaires et tous les participants à utiliser cette ressource le plus largement possible.

Au cours de la séance de questions et réponses, plusieurs parlementaires ont pris la parole pour formuler des observations et poser des questions sur différents points. Certains ont mis en doute la portée de la responsabilité des États et leur capacité à faire en sorte que leurs infrastructures ne soient pas utilisées à des fins de cyberattaques. Les intervenants ont indiqué que la notion d'obligation de diligence était la norme pour les gouvernements. L'exposition des systèmes de commande et de contrôle des armes nucléaires aux cyberattaques, qui reste un sujet de préoccupation d'actualité, a été abordée. Les attaques sous forme de cheval de Troie lancées contre des centrales nucléaires iraniennes en 2015 montrent que les cyberattaques peuvent tout à fait cibler des systèmes hors Internet. Le problème de la détermination (fiable) de la responsabilité des cyberattaques a été abordé : selon les experts, le débat sur la responsabilité est encore plus limité quand il s'agit d'une cyberattaque.

L'utilisation du "dark web" pour le transfert illégal d'armes ainsi que la responsabilité des gouvernements nationaux pour prévenir cette situation ont été abordées. Plusieurs parlementaires ont évoqué la nécessité d'établir un processus multilatéral qui déboucherait sur un traité régissant les comportements et les responsabilités de l'État dans le domaine cybernétique. Il a été répondu qu'un traité régissant le cyberespace ne pouvait être élaboré qu'au niveau multilatéral, dans une optique de collaboration et d'utilisation pacifique dudit espace. Les divergences (et les consensus) entre les États sur les normes et les règles du droit international (humanitaire) applicables aux cyberopérations ont fait l'objet d'une discussion. Enfin, la question du rôle des parlementaires dans la protection de leurs électeurs contre la cybercriminalité a été soulevée. Le manuel fait la distinction entre cybersécurité, cybercriminalité et cyberguerre – autant de concepts liés entre eux mais différents. Si le manuel traite principalement de la cyberguerre, bon nombre des approches qu'il décrit pour y faire face s'appliquent également à la cybersécurité et à la cybercriminalité.