17 juillet 2018

IRSEM

INSTITUT DE RECHERCHE STRATÉGIQUE
DE L'ÉCOLE MILITAIRE

NOTE DE RECHERCHE – n° 59

CYBEROPÉRATIONS ET DROIT INTERNATIONAL

De l'opportunité de saisir la Commission du droit international des Nations unies de la question du droit international applicable aux cyberopérations

François DELERUE

Chercheur Cyberdéfense et droit international à l'IRSEM

RÉSUMÉ

Le droit international est applicable au cyberespace et la question est donc aujourd'hui de déterminer comment les normes du droit international doivent être interprétées pour être appliquées aux cyberopérations. Différentes initiatives ont eu pour objectif de traiter, au moins partiellement, cette question. Ainsi, les travaux des cinq groupes d'experts gouvernementaux successifs, chargés d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (UNGGE), et les deux éditions du Manuel de Tallinn sur le droit international applicable aux cyberopérations publiées par Cambridge University Press en 2013 (*The Tallinn Manual on the International Law Applicable to Cyber Warfare*) et 2017 (*The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*) sont les processus les plus aboutis en la matière. Cette note invite le lecteur à envisager l'opportunité de continuer les discussions et négociations internationales sur le droit international applicable aux cyberopérations dans d'autres enceintes, et plus précisément au sein de la Commission du droit international des Nations unies (CDI), et compare cette possibilité aux travaux des UNGGE et des deux éditions du Manuel de Tallinn.

SOMMAIRE

Introduction[1]

L'interconnexion mondiale des réseaux et l'avènement des technologies de l'information et de la communication offrent des opportunités majeures pour le développement économique et social de nos sociétés. Cependant, on assiste depuis plusieurs années à une multiplication des actes malveillants, aux motifs et origines divers, dans l'espace numérique. Les cyberattaques contre l'Estonie en 2007 et Stuxnet en 2011 ont confirmé que le cyberespace était devenu un espace de confrontation à part entière. Par conséquent, un des enjeux majeurs des discussions internationales a été celui de l'applicabilité du droit international au cyberespace et des modalités concrètes d'application des normes juridiques[2]. C'est dans ce contexte que l'Assemblée générale des Nations unies a adopté plusieurs résolutions et a mis en place cinq groupes d'experts gouvernementaux successifs (2004, 2009, 2012, 2014 et 2016), chargés d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (UNGGE).

Le récent échec des travaux du cinquième UNGGE en juin 2017[3] questionne l'avenir des discussions multilatérales sur la cybersécurité et la cyberdéfense, et ce principalement concernant les questions liées à l'application des normes de droit international aux cyberopérations.

Prenant acte de cet échec, la présente note suggère de dissocier les discussions et négociations sur les normes de droit international et leur applicabilité[4] des discussions diplomatiques et stratégiques, y compris celles sur les normes de comportement et les mesures de confiance engagées au sein des UNGGE successifs mais aussi d'autres enceintes internationales (notamment au sein de l'Organisation pour la sécurité et la coopération en Europe et de l'Association des nations de l'Asie du Sud-Est). Les discussions diplomatiques et stratégiques devraient rester un exercice de diplomatie interétatique, tandis que les questions liées au droit international devraient être confiées à un organe international composé d'experts juridiques plutôt que de diplomates et de représentants de l'État, à savoir la Commission du droit international (CDI) des Nations unies.

Il convient de noter que l'applicabilité du droit international avait été reconnue dans les rapports finaux adoptés par les deux précédents UNGGE, respectivement en 2013 (Document ONU A/68/98, §. 19) et en 2015 (Document ONU A/70/174, § 24), qui soulignaient que :

> Le droit international et, en particulier, la Charte des Nations unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible.

De nombreux États ont confirmé qu'ils partageaient cette approche dans leurs commentaires sur ces rapports[5]. De la même manière, un certain nombre d'États ont affirmé l'applicabilité du droit international aux cyberopérations dans leurs stratégies nationales de cyberdéfense et de cybersécurité[6]. En parallèle, celle-ci fait aujourd'hui consensus dans la littérature académique. Ainsi, la question n'est plus de savoir si le droit international est applicable aux cyberopérations, mais de déterminer comment les normes du droit international doivent être interprétées pour être appliquées aux cyberopérations. C'est dans cette perspective que la CDI pourrait être saisie.

---

1. L'argument développé dans cette note a donné lieu à une publication en anglais du même auteur : « The Codification of the International Law Applicable to Cyber Operations : A Matter for the ILC ? », *ESIL Reflections*, 7:4, juin 2018, http://esil-sedi.eu/?p=12815
2. Voir notamment : François Delerue et Aude Géry, « Les aspects juridique et stratégique de la cyberdéfense », *in* Stéphane Taillat, Amaël Cattaruzza et Didier Danet (dir.), *La Cyberdéfense : politique de l'espace numérique*, Armand Colin, juillet 2018, p. 61-70.
3. Arun M. Sukumar, « The UN GGE Failed. Is International Law in Cyberspace Doomed As Well ? », Lawfare, 4 July 2017, https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well ; Adam Segal, « The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What ?, Council of Foreign Relations », 2017, https://www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what
4. À titre liminaire, il convient de souligner que cette note pourrait être considérée comme une manifestation du *interventionist and managerial project* qui caractérise une part importante de la littérature sur ces questions, comme décrit par Jean d'Aspremont (Jean d'Aspremont, « Cyber Operations and International Law : An Interventionist Legal Thought », *Journal of Conflict and Security Law*, n° 21, 2016, p. 575). Néanmoins, l'objectif de cette note n'est pas de déterminer si le droit international est applicable ni de déterminer comment les normes de droit international devraient être interprétées dans ce contexte, mais de discuter d'une possible forme que pourrait prendre les discussions sur ces questions à l'avenir après l'échec du dernier UNGGE, les États ayant déjà convenu par le passé de l'applicabilité du droit international au cyberespace et aux cyberopérations. Sur cette base, cette note se concentre sur le format des discussions et non sur leur contenu.
5. Voir entre autres : ONU, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)*, 9 septembre 2013, document ONU A/68/156/Add.1 ; ONU, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security*, 30 juin 2014, document ONU A/69/112 ; ONU, *Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)*, 18 septembre 2014, document ONU A/69/112/Add.1.
6. Voir par exemple : France, *Revue stratégique de cyberdéfense*, février 2018, p. 82, 85 et 87, http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/ ; Australie, *Australia's Cyber Security Strategy : Enabling Innovation, Growth & Prosperity*, avril 2016, p. 7, 28, 40-41, https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf ; Russie, *Doctrine of Information Security of the Russian Federation*, décembre 2016, § 34, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 ; Royaume-Uni, *National Cyber Security Strategy*, novembre 2016, p. 63, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Soumettre la question de la codification du droit international à la CDI ne constituerait pas une panacée et ne mettrait pas un terme aux actes malveillants dans le cyberespace. Nous ne devrions pas être naïfs sur ce point. Le droit international offre de nombreuses solutions pour encadrer les comportements malveillants, mais il ne peut pas à lui seul y mettre un terme. De plus, il convient de souligner que le fonctionnement de la CDI est loin d'être exempt de critique[7], même si à la lumière des arguments développés dans cette note il offrirait une solution préférable à d'autres mécanismes. Cependant, le recours à la CDI présenterait des avantages non négligeables en comparaison des précédentes initiatives en matière de codification du droit international applicable aux cyberopérations.

En ce sens, cette note compare la possibilité de saisir la CDI à deux initiatives antérieures : d'une part, les différents UNGGE successifs, et d'autre part, les deux éditions du Manuel de Tallinn sur le droit international applicable aux cyberopérations publiées par Cambridge University Press en 2013 (*The Tallinn Manual on the International Law Applicable to Cyber Warfare*) et 2017 (*The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*)[8]. Les deux éditions du Manuel de Tallinn ont été préparées par des groupes d'experts, sous la direction du professeur Michael N. Schmitt, avec le soutien matériel du Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCDCoE), mais ne représentent pas le point de vue du CCDCoE, de l'OTAN ou de leurs États membres. Ils constituent néanmoins à ce jour la publication la plus complète en la matière. L'objectif ici n'est pas d'interroger la pertinence des UNGGE ou des deux éditions du Manuel de Tallinn, mais de les utiliser comme base pour discuter de l'opportunité de saisir la CDI sur ces questions. Le Manuel de Tallinn et, dans une certaine mesure, les UNGGE visaient à analyser les modalités d'application des normes de droit international aux cyberopérations et à les codifier. Pour ces raisons, ces documents peuvent servir de modèles expérimentaux afin de déterminer l'opportunité de saisir la CDI sur ces questions.

Succès et échec de l'UNGGE

La question des enjeux pour la sécurité et la stabilité internationale liés au développement des cybercapacités des États a été introduite à l'Assemblée générale des Nations unies sous le thème des « progrès de la téléinformatique dans le contexte de la sécurité internationale » par la Fédération de Russie en 1998, donnant lieu à l'adoption de la résolution 53/70, le 4 janvier 1999. Depuis lors, l'Assemblée générale des Nations unies a adopté plusieurs résolutions sur ce thème.

Ces différentes résolutions ont notamment conduit à la création de cinq groupes d'experts gouvernementaux chargés d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (UNGGE) successifs, en 2004, 2009, 2012, 2014 et enfin en 2016. Les participants au premier UNGGE en 2004 n'avaient pas été en mesure de parvenir à un consensus et aucun rapport final n'avait été adopté. Les trois UNGGE suivants furent concluants et adoptèrent des rapports consensuels en 2010 (document ONU A/65/201), en 2013 (document ONU A/68/98) et en 2015 (document ONU A/70/174), qui furent soumis par le secrétaire général à l'Assemblée générale. L'applicabilité du droit international et de la Charte des Nations unies a été affirmée dans le rapport final du UNGGE de 2013 et réaffirmée dans celui de 2015.

En juin 2017, les experts participant au cinquième UNGGE ne sont pas parvenus à un consensus et n'ont donc pas adopté de rapport final. Le paragraphe 34 du projet de rapport, reprenant et détaillant l'applicabilité du droit international, semble avoir cristallisé les désaccords entre les participants. En effet, plusieurs États se sont opposés à ce paragraphe, car il affirmait l'applicabilité des contre-mesures, de la légitime défense et du droit des conflits armés dans l'espace numérique.

Ce cinquième UNGGE était présidé par Karsten Geier, responsable de l'équipe en charge de la coordination de la politique de cyberdiplomatie (*Leiter des Koordinierungsstabs Cyber-Außenpolitik*) du ministère fédéral des Affaires étrangères d'Allemagne[9]. Malgré quelques commentaires de Karsten Geier, notamment lors de la Cyber Week de Tel-Aviv

7. Voir notamment : Georg Nolte (dir.), *Peace through International Law : The Role of the International Law Commission. A Colloquium at the Occasion of Its Sixtieth Anniversary*, Springer, 2009 ; Pemmaraju Sreenivasa Rao, « International Law Commission », *MPEPIL*, 2017.

8. Michael N. Schmitt (dir.), *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013 ; Michael N. Schmitt et Liis Vihul (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2e éd., Cambridge University Press, 2017.

9. *Deutscher zum Vorsitzenden von UN-Expertengruppe zu internationaler Cybersicherheit ernannt*, https://www.auswaertiges-amt.de/de/aussenpolitik/themen/cyber-aussenpolitik/160830-vorsitz-expertengruppe-/282988 ; cette page est aussi disponible en anglais : *German diplomat selected to chair UN group of experts on cybersecurity*, https://www.auswaertiges-amt.de/en/aussenpolitik/themen/160830-vorsitz-expertengruppe-/283006.

fin juin 2017[10], ni lui ni le gouvernement allemand n'ont publié de déclaration officielle exposant leur position et les raisons de l'échec du dernier UNGGE. À l'inverse, les ministères des Affaires étrangères cubain, russe et états-unien ont publié des déclarations de leurs experts gouvernementaux respectifs participant au cinquième UNGGE où ils détaillent et expliquent leurs positions et les raisons de cet échec[11]. La Chine s'est elle aussi opposée à l'adoption du rapport final en refusant d'y voir figurer l'applicabilité de la légitime défense, des contre-mesures et du droit des conflits armés[12], mais sans avoir pour autant publié de déclaration officielle expliquant sa position.

L'incapacité des participants au dernier UNGGE à s'accorder sur un rapport final ne doit pas être surestimée, et notamment, ne doit pas être perçue comme un échec marquant la fin définitive du processus de négociation. Au contraire, c'est une démonstration de la vivacité des discussions internationales sur ces questions. Sur ce point, la Cour internationale de justice a adopté une position similaire dans l'affaire *Nicaragua* concernant la question de la conséquence des violations des normes de droit international sur leur existence :

> Il ne faut pas s'attendre à ce que l'application des règles en question soit parfaite dans la pratique étatique, en ce sens que les États s'abstiendraient, avec une entière constance, de recourir à la force ou à l'intervention dans les affaires intérieures d'autres États. La Cour ne pense pas que, pour qu'une règle soit coutumièrement établie, la pratique correspondante doive être rigoureusement conforme à cette règle. Il lui paraît suffisant, pour déduire l'existence de règles coutumières, que les États y conforment leur conduite d'une manière générale et qu'ils traitent eux-mêmes les comportements non conformes à la règle en question comme des violations de celle-ci et non pas comme des manifestations de la reconnaissance d'une règle nouvelle. Si un État agit d'une manière apparemment inconciliable avec une règle reconnue, mais défend sa conduite en invoquant des exceptions ou justifications contenues dans la règle elle-même, il en résulte une confirmation plutôt qu'un affaiblissement de la règle, et cela que l'attitude de cet État puisse ou non se justifier en fait sur cette base[13].

Les blocages et les défaillances temporaires font partie du processus normal de négociation et de construction des normes. Cette situation montre également clairement que les États reconnaissent que le droit international s'applique aux cyberopérations, puisqu'ils inscrivent leurs discussions et prises de position dans le cadre du droit international.

Le rôle potentiel de la CDI dans la codification du droit international applicable aux cyberopérations

Dans l'environnement international complexe et incertain que nous venons de décrire, la saisine de la CDI des questions de droit international liées à la cyberdéfense aurait différents avantages pour la continuité et la pérennité de ces discussions, comme nous allons le voir dans la troisième partie, néanmoins il convient dans un premier temps de s'intéresser au rôle qu'aurait la CDI sur ces questions en cas de saisine, c'est l'objet de la deuxième partie de cette note.

La CDI a été créée par l'Assemblée générale des Nations unies en 1947, avec un double objectif : promouvoir le développement progressif du droit international et, d'autre part, sa codification (articles 1 et 15, Statut de la CDI[14]). C'est par le biais d'une résolution de l'Assemblée générale des Nations unies que la CDI peut être saisie d'une nouvelle question,

10. « UN GGE : Quo Vadis ? », *Geneva Digital Watch newsletter*, 30 juin 2017.

11. Voir respectivement :

Pour Cuba : *71 UNGA : Cuba at the final session of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security*, http://misiones.minrex.gob.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.

Pour la Russie : *Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere* [Ответ спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности А.В.Крутских на вопрос информагентства ТАСС о состоянии международного диалога в этой сфере], http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288.

Pour les États-Unis : *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, http://www.state.gov/s/cyberissues/releasesandremarks/272175.htm.

12. Elaine Korzak, « UN GGE on Cybersecurity : The End of an Era? », *The Diplomat*, 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ ; Michael N. Schmitt et Liis Vihul, « International Cyber Law Politicized : The UN GGE's Failure to Advance Cyber Norms », JustSecurity, 2017, https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

13. Cour internationale de justice, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique)* (fond), 1986, p. 98, § 186.

14. *Statut de la Commission du droit international*, annexé à la résolution de l'Assemblée générale des Nations unies 174(II) du 21 novembre 1947. L'article 1 du Statut de la CDI reprend l'article 13(1)(a) de la Charte des Nations unies, aux termes duquel « [l]'Assemblée générale provoque des études et fait des recommandations en vue de : […] développer la coopération internationale dans le domaine politique et encourager le développement progressif du droit international et sa codification ».

soit à l'initiative d'un État membre de l'Assemblée générale, soit à l'initiative de la CDI elle-même. Une fois saisie, la CDI aurait pour mission de préparer un projet d'article accompagné d'un commentaire explicatif pouvant notamment exposer les points de consensus et de divergence dans la pratique des États et la littérature, qui seraient alors soumis à l'Assemblée générale des Nations unies. Les États membres des Nations unies seraient invités à commenter le projet d'articles. Sur cette base, la CDI devrait préparer un projet final d'articles et un rapport explicatif, que l'Assemblée générale pourrait adopter ou renvoyer à la CDI pour révision en vue de la soumission d'une nouvelle version.

Le travail que pourrait entreprendre la CDI sur le droit international applicable aux cyberopérations s'inscrirait dans le cadre des deux objectifs de la CDI (articles 1, 15-24, Statut de la CDI). En effet, le premier objectif assigné à la CDI pourrait être d'analyser comment les normes existantes du droit international s'appliquent aux cyberopérations. Ce premier objectif pourrait permettre d'envisager deux avancées : d'un côté, cela permettrait la codification des normes existantes du droit international et de leur interprétation dans ce contexte précis ; d'un autre côté, l'identification des points précis sur lesquels le droit international existant offre une réponse imparfaite, et pour lesquels il pourrait être nécessaire d'envisager l'adoption de nouvelles normes de droit international, ce qui pourrait constituer le second objectif assigné à la CDI.

Avantages de la saisine de la CDI de la codification du droit international applicable aux cyberopérations

Les paragraphes suivants comparent la possibilité de saisir la CDI de la codification du droit international applicable aux cyberopérations par rapport aux travaux des UNGGE et des deux versions du Manuel de Tallinn.

Premièrement, en confiant ce travail à la CDI, le travail juridique préparatoire serait réalisé par des juristes internationalistes intervenant en leur capacité personnelle, comme ce fut le cas pour les travaux préparatoires du Manuel de Tallinn, mais à l'inverse des travaux du UNGGE. Cela permettrait d'avoir un travail juridique préparatoire se concentrant exclusivement sur les questions juridiques. Ce travail ne serait ainsi pas affecté par des considérations politiques ou les aléas inhérents aux négociations diplomatiques. Néanmoins, les États ne seraient pas totalement exclus du processus : ils y joueraient même un rôle actif, par le biais des commentaires qu'ils soumettraient sur les différents projets d'articles et documents soumis par la CDI à l'Assemblée générale. En outre, les États garderaient le dernier mot, puisque les projets d'articles et les rapports explicatifs doivent être soumis à l'Assemblée générale.

Deuxièmement, la CDI n'aurait pour mission, au moins dans un premier temps, que de codifier la *lex lata*, c'est-à-dire le droit international existant, dans les limites fixées par les États dans la résolution de saisine de la CDI. Un tel cadre rend improbable le risque pour les États de créer un « monstre de Frankenstein » du droit international, en d'autres termes un processus de création de normes qui leur échapperait totalement. Le cadre du travail de la CDI serait fixé par l'Assemblée générale et ne pourrait être modifié que par celle-ci.

Troisièmement, en analysant et en codifiant l'applicabilité des normes du droit international au cyberespace et aux cyberopérations, le travail de la CDI permettrait également d'identifier les limites du droit international existant et ses éventuelles lacunes. Un tel travail serait particulièrement utile afin d'identifier certains points spécifiques pour lesquels les normes existantes sont imparfaites et où il serait envisageable, voire nécessaire, de réfléchir à de nouvelles normes de droit international.

Quatrièmement, le commentaire des États sur les projets et rapports successifs de la CDI serait très précieux dans l'analyse et l'identification de la pratique des États et de leur *opinio juris*[15] sur les normes de droit international concernées et leur interprétation.

Cinquièmement, la CDI aurait la possibilité de consulter des acteurs non étatiques dans la conduite de ses travaux, permettant ainsi de prendre en compte la diversité des acteurs impliqués dans les questions de cybersécurité et de cyberdéfense. En effet, la CDI a la possibilité de consulter tous les acteurs nécessaires à ses travaux, qu'il s'agisse d'agences des Nations unies, d'organisations internationales, d'organes de l'État ou même d'acteurs non étatiques (article 26, Statut de la CDI). En ce sens, la CDI pourrait faciliter la collaboration entre les États et les acteurs non

15. L'*opinio juris* est « une pratique générale acceptée comme étant le droit » (article 38, Statut de la Cour internationale de justice), en d'autres termes, il s'agit du sentiment qu'ont les États d'être juridiquement liés par cette pratique, voir notamment : Alain Pellet, Mathias Forteau, Daniel Müller et Patrick Daillier, *Droit international public*, 8e éd., LGDJ, 2009, p. 361-362.

étatiques sur ces questions, par exemple intégrant la possibilité d'une consultation des points de vue des acteurs privés. Par exemple, la CDI pourrait dialoguer avec la société Microsoft et discuter de ses propositions de Convention de Genève numérique (*Digital Geneva Convention*) ainsi que de la création d'un mécanisme international d'attribution[16], et déterminer dans quelle mesure elles sont pertinentes pour son travail. L'association d'acteurs non étatiques aux discussions et travaux sur les questions de cybersécurité et de cyberdéfense est devenue incontournable. Il est probable que des participants aux différents UNGGE aient consulté des acteurs non étatiques et qu'ils aient été associés aux travaux du UNGGE, mais le processus est resté principalement, sinon exclusivement, centré sur les États et leurs intérêts.

Sixièmement, le manque de représentativité des UNGGE et des groupes qui ont préparé les deux éditions du Manuel de Tallinn a été fortement critiqué, du fait du nombre limité de participants pour le premier et du tropisme anglo-saxon du second. Les UNGGE successifs ont été critiqués pour leur exclusivité, puisque seulement des experts d'un nombre limité d'États ont pu y prendre part. En effet, les trois premiers UNGGE (2004, 2009 et 2012) comptaient des experts de 15 États, le quatrième UNGGE (2014) comptait des experts de 20 États et le cinquième UNGGE comptait des experts de 25 États, à savoir l'Australie, le Botswana, le Brésil, le Canada, la Chine, Cuba, l'Égypte, l'Estonie, la Finlande, la France, l'Allemagne, l'Inde, l'Indonésie, le Japon, le Kazakhstan, le Kenya, le Mexique, les Pays-Bas, la Russie, la Corée du Sud, le Sénégal, la Serbie, la Suisse, le Royaume-Uni et les États-Unis. Ainsi, seuls 38 États ont été représentés au sein d'au moins un des cinq UNGGE successifs, soit seulement 38 % des 193 États membres de l'ONU. La Biélorussie, l'Allemagne et les cinq membres permanents du Conseil de sécurité des Nations unies (Chine, États-Unis, France, Royaume-Uni et Russie) sont les seuls États à avoir participé aux cinq UNGGE successifs.

Face à ce constat, on pourrait être tenté d'augmenter la représentativité d'un potentiel futur UNGGE ou d'un autre forum où ces discussions pourraient reprendre, en permettant à chaque État membre des Nations unies d'y envoyer au moins un expert gouvernemental. L'échec du dernier UNGGE a montré les difficultés qui découlent de l'augmentation du nombre d'experts participants. Une enceinte réunissant 193 experts, c'est-à-dire un par État membre des Nations unies, serait très difficile à faire fonctionner surtout si les décisions continuent à être adoptées par voie de consensus comme c'était le cas dans les différents UNGGE. Il semble donc peu opportun de s'orienter vers ce modèle.

Une autre évolution possible serait de modifier le mode d'adoption des rapports, en laissant de côté la nécessité d'un consensus pour s'orienter vers un mode d'adoption par scrutin majoritaire. Néanmoins, ces deux modèles ne sont pas exempts de critiques et il est probable qu'une enceinte d'experts gouvernementaux ne réunissant qu'un nombre limité d'États et adoptant un mode de scrutin majoritaire serait aussi fortement critiquée pour son manque de représentativité.

Dans cette perspective, la CDI offre un double avantage en termes de représentativité : d'un côté, la CDI « se compose de trente-quatre membres, possédant une compétence reconnue en matière de droit international » (article 2, Statut de la CDI). Sa composition doit refléter la diversité de la communauté internationale en vue d'assurer « la représentation des grandes formes de civilisation et des principaux systèmes juridiques du monde » (article 8, Statut de la CDI). En ce sens, il est important de noter que chaque membre de la CDI doit être issu d'un État différent (article 2, Statut de la CDI). Les membres de la CDI siègent en leur capacité personnelle et non comme experts gouvernementaux, à l'inverse de ceux siégeant au sein des UNGGE. Ils ne représentent donc pas leurs États en fonction de leur nationalité. Pourtant, certains pourraient être tentés de critiquer le fonctionnement de la CDI, notamment les États qui ne seraient pas en mesure d'y faire siéger un expert de leur nationalité familier avec leur approche particulière des questions discutées, en soulignant son exclusivité. D'un autre côté, tous les États membres des Nations unies seraient associés aux travaux de la CDI par le biais des projets d'articles et rapports soumis par la CDI à l'Assemblée générale et des commentaires qu'ils feraient sur ces documents. Ces commentaires des États permettraient ainsi de porter à la connaissance de la CDI, mais aussi de la communauté internationale du fait de leur caractère public, l'approche et la pratique particulières de chaque État sur ces questions et de permettre ainsi à la CDI de les prendre en compte dans ses travaux.

En guise de conclusion de ce sixième point, il est important de souligner que cette discussion sur la représentativité était motivée parce que c'était une critique récurrente et importante à l'encontre des UNGGE et du Manuel de Tallinn.

16. Voir notamment : Scott Charney, Erin English, Aaron Kleiner, Nemanja Milisevic, Angela McKay, Jan Neutze et Paul Nicholas, *From Articulation to Implementation : Enabling Progress on Cybersecurity Norms*, Microsoft, 2016, p. 11-12 ; Brad Smith, *The Need for a Digital Geneva Convention*, Microsoft, 2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. Microsoft a récemment commissionné la RAND pour réaliser un rapport sur sa proposition de mécanisme international pour l'attribution, John S. Davis, Benjamin Adam Boudreaux, Jonathan William Welburn, Jair Aguirre, Cordaye Ogletree, Geoffrey McGovern et Michael S. Chase, *Stateless Attribution : Toward International Accountability in Cyberspace*, RAND, 2017, https://www.rand.org/pubs/research_reports/RR2081.html

Cette discussion ne préjuge pas de la question d'une possible corrélation entre la représentativité de l'enceinte de discussion et de travail, et le résultat atteint. Augmenter la représentativité de l'enceinte risquerait de la rendre inefficace. Cette remarque amène à s'interroger sur le résultat souhaité, opposant deux conceptions différentes du succès de ses travaux : essayer d'atteindre un niveau plus large de représentativité, et donc un consensus plus large, peut également avoir comme effet négatif de vider le résultat de tout contenu significatif. À l'inverse, un résultat significatif atteint dans une enceinte restreinte, notamment si les discussions devaient être exclusivement prolongées entre *like-minded States*, risquerait d'avoir un effet limité sur le plan international.

Septièmement, la dimension temporelle et le caractère évolutif du travail de la CDI constituent à la fois un avantage indéniable et une source potentielle de critiques. À l'inverse des travaux des UNGGE et du Manuel de Tallinn, un des grands avantages du fonctionnement de la CDI est qu'il s'agit d'un travail mené sur le long terme, avec la possibilité de le faire évoluer dans le temps au fil des différents projets d'articles et rapports soumis à l'Assemblée générale et des commentaires des États. Dans le cas du Manuel de Tallinn, certains États furent invités à commenter les travaux du groupe d'experts internationaux, notamment dans le cadre du *Hague Process*[17]. Néanmoins, le processus d'adoption des deux versions du Manuel de Tallinn était principalement un exercice d'experts non gouvernementaux. La consultation des États s'est faite en une fois et n'a pas créé les conditions nécessaires à la naissance d'un dialogue entre les experts participants et les États, ni entre les États eux-mêmes.

La temporalité du travail de la CDI pourrait aussi être perçue comme un désavantage. En effet, la préparation des différentes versions des projets d'articles et des rapports, leur soumission à l'Assemblée générale et la soumission des commentaires par les États prendraient des années, si ce n'est des décennies. Il convient cependant de ne pas surestimer les désavantages de la dimension temporelle. En effet, la lenteur et le fonctionnement du processus constitueraient un véritable avantage pour deux raisons. Premièrement, le dialogue entre la CDI et l'Assemblée générale permettrait de dynamiser sur le long terme le dialogue entre les États sur ces questions. Deuxièmement, les travaux de la CDI seront exploitables et pertinents même avant leur aboutissement et l'adoption d'un projet final d'article par l'Assemblée générale. Les projets d'articles, rapports, commentaires des États et autres documents successifs produits dans le cadre des travaux de la CDI fourniraient des éléments pertinents dans la compréhension de l'approche des États et plus généralement dans l'interprétation des normes de droit international applicables aux cyberopérations. Sur ce point, les *Articles sur la responsabilité de l'État pour fait internationalement illicite* adoptés par la CDI en 2001 offrent un bon exemple[18].

La CDI a travaillé pendant plusieurs décennies sur la question de la responsabilité de l'État pour fait internationalement illicite et a soumis plusieurs projets d'articles et rapports à l'Assemblée générale avant l'adoption de la version finale en 2001. En effet, dès 1949, la CDI avait inscrit la question de la « Responsabilité de l'État » sur la liste provisoire des matières de droit international choisies comme sujet de codification. L'Assemblée générale a donné mandat à la CDI pour la codification du droit international de la Responsabilité de l'État par la résolution 799 (VIII) du 7 décembre 1953[19]. Ces différents documents produits tout au long du travail de la CDI ont permis de faire évoluer et de dynamiser les débats sur ces questions, tant entre les États qu'entre les universitaires, et ont ainsi fortement contribué au processus d'interprétation et de codification du droit international coutumier de la responsabilité des États.

Enfin, concernant la temporalité du processus, il convient de souligner que les cyberopérations sont un phénomène récent et que le recours au droit international par les États pour les analyser et y répondre n'en est qu'à ses balbutiements. Après quelques références embryonnaires, le droit international a été utilisé pour la première fois dans ce contexte par les États-Unis en 2015 dans le cadre de l'attribution à la Corée du Nord du piratage de Sony Picture Entertainment et de la prise de mesures de rétorsion contre cet État. Cette pratique s'est développée ces dernières années. Dans cette perspective, la temporalité des travaux de la CDI, et plus précisément sa lenteur, aurait comme avantage de laisser le temps pour les États de développer leur approche et leur pratique et de permettre à la CDI d'évaluer ces approches et ces pratiques naissantes en matière de droit international applicable aux cyberopérations.

17. Michael N. Schmitt et Liis Vihul (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, p. xxv-xxvii.
18. Commission du droit international, *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite*, adopté par la CDI en 2001, annexé à la résolution de l'Assemblée générale des Nations unies 56/83 du 12 décembre 2001, et rectifié par le document A/56/49 (Vol. I)/Corr.3.
19. Pour plus d'informations, voir : http://legal.un.org/ilc/guide/9_6.shtml#ilcrep

Conclusion

Cette note invite le lecteur à envisager l'opportunité de continuer les discussions et négociations internationales sur le droit international applicable aux cyberopérations dans d'autres enceintes, et plus précisément au sein de la CDI, qui constituerait une enceinte pertinente et dont les travaux pourraient relancer et dynamiser les débats sur ces questions entre les différents acteurs concernés (États, acteurs non étatiques, etc.). La saisine de la CDI favoriserait aussi la prise en compte de la diversité des approches et des pratiques sur ces questions. Finalement, il est important de saisir les limites de ces questions : avoir recours à la CDI pour codifier le droit international applicable aux cyberopérations ne serait pas un remède miracle face à l'augmentation des menaces dans le cyberespace. En effet, le droit international permet de définir le cadre dans lequel les États peuvent mener des cyberopérations et la licéité de celles-ci, définissant notamment les modalités de réponse ouvertes aux États victimes de cyberopérations. Néanmoins, la réponse à ces cyberopérations et la lutte contre les cyberopérations malveillantes dépendent principalement de considérations politiques et techniques dépassant le cadre du droit international. En ce sens, la saisine de la CDI permettrait de clarifier les considérations juridiques que doivent prendre en compte les États, mais pas les considérations techniques et politiques qui pourraient faire l'objet de discussions et de développements dans d'autres enceintes.

François Delerue est chercheur cyberdéfense et droit international à l'IRSEM, chercheur associé à la Chaire Castex de Cyberstratégie et enseignant à Sciences Po Paris. Il mène des recherches portant sur le droit international, notamment sur l'impact des nouvelles technologies (conquête spatiale, robotique, intelligence artificielle, etc.), sur les normes et la coopération internationale, et sur les questions de cyberdéfense et de cybersécurité tant sous l'angle juridique, stratégique que politique. Il intervient régulièrement à l'Institut international de Droit humanitaire (IIDH) de Sanremo, ainsi que dans diverses autres institutions. Il a enseigné à l'IUE et à l'Université de Florence (Università degli Studi di Firenze). Il a soutenu son doctorat intitulé *State-Sponsored Cyber Operations and International Law* en novembre 2016 à l'Institut universitaire européen (IUE - Florence, Italie), sous la direction du Professeur Nehal Bhuta. Il a été chercheur invité à l'Université de Columbia à New York (2014) et auditeur de la 62e session jeune de l'IHEDN (2009) et du séminaire « International Law and Cyber Operations » de l'École de l'OTAN à Oberammergau (2013). Il est titulaire d'un Master recherche en droit international et organisations internationales de l'Université de Paris 1 Panthéon-Sorbonne (2011) et d'un *LL.M. in Comparative, European and International Laws de l'IUE* (2013).

Contact : francois.delerue@defense.gouv.fr