97º SESSION ORDINAIRE
3 - 7 aout 2020
Session virtuelle

OEA/Ser.Q
CJI/RES. 260 (XCVII-O/20)
7 aout 2020
Original: espagnol

CJI/RES. 260 (XCVII-O/20)

DROIT INTERNATIONAL ET OPÉRATIONS CYBERNÉTIQUES DE L'ÉTAT

LE COMITÉ JURIDIQUE INTERAMÉRICAIN,

PRENANT EN COMPTE que l'Assemblée générale de l'OEA a demandé au CJI, par la résolution AG/RES. 2930 (XLIX-O/19) "Droit international", au point *i* portant sur "Observations et recommandations relatives au rapport annuel du Comité juridique interaméricain", de faire rapport en permanence sur les progrès réalisés au titre des questions inscrites à son programme d'action, dont celles concernant la cybersécurité,

CONSCIENT de la nécessité d'offrir aux États membres de l'OEA des paramètres clairs sur l'application du droit international au cyberespace, limitant ainsi les risques d'escalade ou de conflit involontaire,

PRENANT EN COMPTE le document "Droit international et opérations cybernétiques de l'État : Amélioration de la transparence – Cinquième Rapport", publié sous la cote CJI/doc.615/20, présenté par M. Duncan B. Hollis, Rapporteur de cette question,

DÉCIDE :

1. De remercier M. Duncan B. Hollis pour son travail en tant que Rapporteur de cette question ainsi que pour la présentation de ce rapport.

2. Sur la base des propositions contenues dans le rapport susmentionné, de recommander à l'Assemblée générale d'appuyer l'applicabilité du droit international aux opérations étatiques dans le cyberespace par le truchement de l'approbation de la déclaration suivante :

> "*L'Assemblée générale de l'OEA affirme que le droit international, y compris la Charte des Nations Unies dans sa totalité, la Charte de l'Organisation des États Américains, le droit international humanitaire, le droit international des droits de la personne, le devoir de non-intervention, l'égalité souveraine des États et le droit de la responsabilité des États sont applicables à l'utilisation des technologies de l'information et de la communication (TIC) par les États et par les personnes ou entités responsables sur le plan international*".

3. De demander au Département du droit international de présenter au CJI, en sa qualité de Secrétariat technique du Comité juridique interaméricain, une proposition visant à appuyer ou à

entreprendre des activités de formation sur l'application du droit international au cyberespace s'adressant à divers acteurs.

4. De conserver la question à son ordre du jour en élargissant sa portée au-delà des thèmes du droit international relatifs à la paix et à la sécurité internationales afin qu'elle comprenne d'autres régimes internationaux.

La présente résolution a été adoptée à l'unanimité lors de la réunion ordinaire tenue le 7 aout 2020, par les membres suivants : mesdames et messieurs Luis García-Corrochano Moyano, Eric P. Rudge, Mariana Salazar Albornoz, José Antonio Moreno Rodríguez, Milenko Bertrand-Galindo Arriagada, Duncan B. Hollis, Alix Richard, George Rodrigo Bandeira Galindo, Miguel A. Espeche-Gil, Íñigo Salvador Crespo et Ruth Correa Palacio.

97e SESSION ORDINAIRE
3 – 7 aout 2020
Réunion virtuelle

OEA/Ser. Q
CJI/doc. 615/20 rev.1
7 aout 2020
Original: anglais

DROIT INTERNATIONAL ET OPÉRATIONS CYBERNÉTIQUES DE L'ÉTAT : AMÉLIORATION DE LA TRANSPARENCE CINQUIÈME RAPPORT

(Présenté par le Professeur Duncan B. Hollis)

1. Le présent rapport est mon cinquième et dernier sur la question de l'amélioration de la transparence en ce qui concerne la façon dont les États membres entendent l'application du droit international aux opérations cybernétiques de l'État. Ce projet a pour but de contribuer à une tendance plus large dans les relations internationales qui tentent d'obtenir une plus grande transparence sur la façon dont les États nationaux entendent l'application du droit international au cyberespace. Ce faisant, quatre objectifs sont poursuivis. Ce sont les suivants :

a) identifier des domaines de convergence sur la façon dont les États entendent quelles règles juridiques internationales s'appliquent et comment elles le font. Combiné avec des déclarations existantes d'États situés à l'extérieur de la région, une uniformité de points de vue peut apporter des renseignements supplémentaires qui aideront à établir les règles de droit international coutumier pertinentes;

b) identifier des points de vue divergents sur quelles normes internationales s'appliquent et comment elles le font. Cela peut aider à établir la base d'un dialogue supplémentaire, soit pour concilier des positions en conflit, préciser le contenu de la loi o, peut-être, même chercher des modifications à celle-ci;

c) limiter les risques d'escalade ou de conflit involontaire à cause du fait que les États ont des interprétations différentes concernant l'application du droit international et ne savent pas ou ne comprennent pas comment d'autres voient le problème; enfin,

d) donner à l'OEA et à ses États membres une voix appropriée dans les conversations mondiales sur l'application du droit international.

En même temps, il est important de répéter ce que ce projet n'est pas destiné à faire. Il n'a pas pour objectif de codifier ou d'élaborer progressivement le droit international (ni même d'identifier les meilleures pratiques ou l'orientation générale). Il ne prétend pas non plus offrir une perspective intégrée ou générale sur des questions juridiques internationales dans le contexte cybernétique.

2. Au lieu de cela, ce projet est destiné, et doit se lire, comme un modeste premier pas. Le Comité juridique (et l'OEA, en termes plus généraux) peut utiliser les matériaux qui leur sont fournis ici pour évaluer quelles activités additionnelles, le cas échéant, pourraient être effectuées pour accroitre la transparence dans la façon dont le droit international s'applique aux États de la région, à leurs opérations cybernétiques et à leurs réactions face à des menaces cybernétiques de la part d'autres États. Le Comité pourrait également envisager d'accroitre les efforts existants en matière de création de capacité pour améliorer la connaissance et l'expérience des fonctionnaires pertinents en matière d'application du droit international au cyberespace. Cela peut demander la compilation (et la publication) de points de vue nationaux additionnels et/ou la mise sur pied de plateformes ou d'autres processus permettant de partager l'information et de dialoguer sur la

relation entre le droit international et le cyberespace et les technologies de l'information et de la communication (TIC) dont il découle.

3. Mon premier rapport a souligné la visibilité limitée du droit international dans la réglementation des opérations cybernétiques de l'État, malgré le nombre croissant d'opérations de ce type et leurs conséquences économiques, humanitaires et en matière de sécurité nationale[1]. Il est vrai que de nombreux États ont confirmé l'applicabilité du droit international à leur comportement dans le cyberespace[2]. Et bien que l'OEA ne l'a pas fait, d'autres organisations internationales (l'ANASE, l'Union européenne et les Nations Unies) l'ont également fait[3]. Jusqu'à maintenant, toutefois, les efforts visant à définir comment les États entendent l'application du droit international au cyberespace ont connu un succès limité.

4. Une partie du problème, dans l'application du droit international au cyberespace, découle de l'absence de normes ou de normes personnalisées. Quand il s'agit de la paix et de la sécurité internationales, par exemple, il n'existe aucun traité spécifique sur la cybersécurité. Et les conventions qui traitent de la cybercriminalité – la Convention de Budapest et (si elle entre en vigueur un jour) la Convention de l'Union africaine – ne traitent, par définition, que du comportement des acteurs non étatiques avec l'appui d'une minorité d'États nationaux[4]. Par conséquent, l'application du droit international au cyberespace dépend de l'analogie avec des traités multilatéraux plus généraux (par exemple la Charte des Nations Unies) ou avec le droit international coutumier.

5. Cependant, comme je l'ai souligné dans mon deuxième rapport, il n'existe, au niveau mondial, aucun consensus universel entre les États sur quelles normes internationales générales en vigueur s'appliquent aux opérations cybernétiques, et encore moins sur comment elles le font[5]. Pour différents régimes juridiques internationaux (par exemple la légitime défense, le droit international

---

1 *Voir* Duncan B. Hollis, *Derecho Internacional y Operaciones Cibernéticas Estatales: Mejorando la Transparencia*, OEA/Ser.Q, CJI/doc 570/18 (9 aout 2018) ("Hollis, Premier rapport"), dans http://www.oas.org/en/sla/iajc/docs/CJI_doc_570-18.pdf.

2 *Voir* Secrétaire général de l'ONU, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶19, U.N. Doc. A/68/98 (24 juin 2013) ("le droit international, et en particulier la Charte des Nations Unies, s'applique" au cyberespace); *voir également* Secrétaire général de l'ONU, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶24, U.N. Doc. A/70/174 (22 juillet 2015)

3 *Voir* UNGA Res. 266, U.N. Doc. A/RES/73/266 (2 janvier 2019); Déclaration des chefs d'État et de gouvernement de l'ANASE-États-Unis sur la coopération en matière de cybersécurité (18 novembre 2018), à https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf ; Déclaration de l'UE : 1er Comité des Nations Unies, discussion thématique sur d'autres mesures de désarmement et de sécurité internationale (26 octobre 2018) ("Déclaration de l'UE"), à https://eeas.europa.eu/delegations/un-new-york/52894/eu-statement-%E2%80%93-united-nations-1st-committee-thematic-discussion-other-disarmament-measures-and_en. Tant le G7 que le G20 ont fait des affirmations similaires. *Voir, par exemple,* Déclaration du G7 sur la responsabilité des États pour leur conduite dans le cyberespace (11 avril 2017) à https://www.mofa.go.jp/files/000246367.pdf; G20 Communiqué des chefs d'État et de gouvernement du Sommet d'Antalya (15-16 novembre 2015) ¶26, à http://www.gpfi.org/sites/gpfi/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf.

4 Conseil de l'Europe, Convention sur la cybercriminalité, (Budapest, 23 novembre 2001) CETS No 185; Convention de l'UA sur la cybersécurité et la protection des données personnelles, 27 juin 2014, AU Doc. EX.CL/846(XXV). La Convention de Budapest compte maintenant 65 parties, bien que plusieurs autres États la voient avec une certaine hostilité. *Voir* Convention sur la cybercriminalité, à http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

5 Duncan B. Hollis, *Derecho Internacional y Operaciones Cibernéticas Estatales: Mejorando la Transparencia*, OEA/Ser.Q, CJI/doc 578/19 (21 janvier 2019) ("deuxième Rapport, Hollis"), à http://www.oas.org/en/sla/iajc/docs/CJI_doc_578-19.pdf

humanitaire, les contre-mesures, la souveraineté (en tant que règle indépendante) et la diligence appropriée) un État ou plus contestent leur application *in toto* au cyberespace, tandis que d'autres divergent (parfois considérablement) quant à la façon d'interpréter l'application de ces règles aux opérations cybernétiques étatiques et parrainées par l'État.

6. Les États semblent également réticents à invoquer le libellé du droit international lorsqu'ils font des accusations relatives aux opérations cybernétiques d'autres États[6]. Une exception remarquable a été quand, en 2018, cinq États (l'Australie, le Canada, les Pays-Bas, la Nouvelle-Zélande et le Royaume-Uni) ont accusé le GRU, le service de renseignement militaire de la Russie, d'être responsable d'une série d'opérations cybernétiques, dont celles qui visaient l'Organisation pour l'interdiction des armes chimiques (OIAC) et l'Agence mondiale antidopage (AMA). Le Secrétaire aux relations extérieures du Royaume-Uni a suggéré que la Russie avait un « désir de fonctionner sans tenir compte du droit international ou des normes établies », tandis que les Pays-Bas ont suggéré, en termes plus généraux, que ces activités russes « minaient l'État de droit international »[7]. Malheureusement, ces accusations n'ont pas précisé si toutes les opérations présumées du GRU avaient violé le droit international ou si seulement quelques-unes l'avaient fait; elles n'ont pas non plus élaboré sur quelles normes internationales les accusateurs croyaient qui avaient été violées. Cependant, la majorité des affaires sont similaires aux accusations récentes du Canada, des États-Unis et du Royaume-Uni selon lesquelles le GRU a fait porter ses efforts sur la recherche relative au vaccin contre la COVID 19; le droit international n'est pas mentionné du tout[8].

---

6 *Voir* Dan Efrony et Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber-Operations and Subsequent State Practice,* 112 AJIL 583, 586 (2018); Duncan B. Hollis & Martha Finnemore, *Beyond Naming and Shaming: Accusations and International Law in Global Cybersecurity,* 33 EURO. J. INT'L L. (prochainement en 2020).

7 Communiqué de presse, Bureau des affaires étrangères du Commonwealth, *UK exposes Russian cyber-attacks* (4 octobre 2018), à https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks; Centre national de cybersécurité (NCSC), *Reckless campaign of cyber attacks by Russian military intelligence service exposed* (4 octobre 2018), à https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed; Ministère de la défense des Pays-Bas, *Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW* (a octobre 2018), à https://english.defensie.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw. L'accusation du Canada incorporait les deux formulations. Communiqué de presse, Affaires mondiales Canada, *Le Canada attribue des cyberactivités malveillantes à la Russie* (4 octobre 2018) à https://www.canada.ca/fr/affaires-mondiales/nouvelles/2018/10/le-canada-attribue-des-cyberactivites-malveillantes-a-la-russie.html (L'activité russe "démontre un mépris pour le droit international et qui sape l'ordre international fondé sur des règles."). En contraste, l'Australie et la Nouvelle-Zélande ont accusé la Russie de "ciberactivité malicieuse" sans se référer au droit internatinal du tout. *Voir, par exemple* Communiqué de presse. Gouvernement de la Nouvelle-Zélande, Communications du Bureau de la sécurité, *Malicious cyber activity attributed to Russia* (4 octobre 2018), à https://www.gcsb.govt.nz/news/malicious-cyber-activity-attributed-to-russia/; Communiqué de presse, Premier Ministre de l'Australie, *Attribution of a Pattern of Malicious Cyber Activity to Russia* (4 octobre 2018), à https://www.pm.gov.au/media/attribution-pattern-malicious-cyber-activity-russia

8 *Voir, par exemple,* NCSC (Royaume-Uni), Communiqué de presse, *UK and allies expose Russian attacks on coronavirus vaccine development* (16 juillet 2020), à https://www.ncsc.gov.uk/news/uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development; Centre de la sécurité des télécommunications (Canada), *Déclaration du CST sur les menaces visant le développement d'un vaccin contre la COVID-19* (16 juillet 2020), à https://cse-cst.gc.ca/fr/media/2020-07-16; Service de sécurité central de l'Agence nationale de sécurité des États-Unis, *NSA Teams with NCSC, CSE, DHS CISA to Expose Russian Intelligence Services Targeting COVID-19 Researchers* (16 juillet 2020), à https://www.nsa.gov/news-features/press-room/Article/2275378/nsa-teams-with-ncsc-cse-dhs-cisa-to-expose-russian-intelligence-services-target/

7. Au cours des dernières années, plusieurs États ont commencé à offrir certaines explications sur comment ils entendent l'application du droit international au cyberespace. À partir de 2012, les États-Unis ont commencé à offrir leurs points de vue dans une série de discours et de déclarations officielles[9]. En 2018, le Procureur général du Royaume-Uni a fait une importante déclaration sur l'opinion du Royaume-Uni[10]. Au cours des années suivantes, d'autres États (en majorité européens) ont commencé à offrir leurs propres perspectives détaillées, comme l'Australie[11], l'Estonie[12], la France[13], l'Allemagne[14] et les Pays-Bas[15]. Bien que cela soit un fait

---

9 *Voir, par exemple,* Brian Egan, *Remarks on International Law and Stability in Cyberspace* (10 novembre 2016), *dans* DIGEST OF U.S. PRACTICE IN INT'L LAW 815 (2016); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (octobre 2016), *dans* DIGEST OF U.S. PRACTICE IN INT'L LAW 823 (2016) ("2016 US GGE Submission"); *U.S. Submission to Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (octobre 2014), *dans* DIGEST OF U.S. PRACTICE IN INT'L LAW 732 (2014) ("2014 US GGE Submission"); Harold Koh, *International Law in Cyberspace* (18 septembre 2012), *dans* DIGEST OF U.S. PRACTICE IN INT'L LAW 593 (2012). En 2020, le Conseiller juridique du Département de la défense des États-Unis a offert des points de vue sur diverses questions fondamentales relatives à l'application du droit international au cyberespace. Cependant, il n'est pas encore clair si ses points de vue reflètent ceux des États-Unis en général ou seulement ceux du Département de la défense des États-Unis. *Voir* Paul C. Ney, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference* (2 mars 2020), à https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/;

10 Jeremy Wright, QC, MP, *Cyber and International Law in the 21st Century* (Mayo 23, 2018), at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century ("U.K. Views"/ Puntos de Vista del Reino Unido).

11 Misión Australiana a las Naciones Unidas*, Australian Paper—Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (Sept. 2019), en https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf ("Australian Views"/Puntos de Vista de Autralia); Commonwealth de Australia, Departmento de Relaciones Exteriores y Comercio, *Annex A: Australia's position on how international law applies to State conduct in cyberspace*, en AUSTRALIA'S INT'L CYBER ENGAGEMENT STRATEGY (2017) *en*https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf.

12 Kersti Kaljulaid, Presidente de Estonia, *President of the Republic at the opening of CyCon 2019* (May 29, 2019), en https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html ("Estonian Views"/Puntos de Vista de Estonia)

13 Ministère des Armées, *Droit international appliqué aux operations dans le cyberspace* (Sept. 9, 2019), https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international ("Opinions du Ministère de la défense de la France"). Je ne les ai pas appelées "Opinions françaises" étant donné qu'au moins un expert a indiqué que ce document est écrit par le Ministère de la défense de la France et que son contenu ne peut pas être attribué à l'État français en entier. *Voir* Gary Corn, *Punching on the Edges of the Gray Zone: Iranian Cyber Threats and State Cyber Responses,* JUST SECURITY (11 février 2020) (Il importe de mentionner qu'en dépit de nombreuses affirmations contraires, le document français ne prétend pas être la position officielle du gouvernement français. Il a été écrit et publié par le Ministère des Armées (MdA) français, tout comme le *Law of War Manual*, publié par le Ministère de la défense des États-Unis, ne reflète pas nécessairement les points de vue du gouvernement des États-Unis dans son ensemble).

14 Discours de l'Ambassadeur Norbert Riedel, membre de la Commission de politique cybernétique internationale, du Ministère fédéral de relations extérieures de l'Allemagne (18 mai 2015), *dans* https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832.

15 *Letter to the parliament on the international legal order in cyberspace*, 5 juillet 2019, Appendice 1, dans https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-

positif, le nombre et la spécificité de ces déclarations n'ont pas (encore) été suffisants pour en déduire la pratique générale de l'État ou l'*opinio juris*[16].

8. Plusieurs acteurs non étatiques ont essayé de combler ce déficit d'information en offrant leurs propres points de vue sur la façon dont le droit international coutumier réglemente les opérations cybernétiques étatiques. Les deux voix qui se détachent le plus sont, sans aucun doute, celles du Comité international de la Croix-Rouge (CICR) et du Groupe indépendant d'experts qui a écrit le *Manuel de Tallinn*.[17] Il est toutefois clair que ce ne sont pas tous les États qui estiment que leur contenu reflète le droit international.[18]

9. L'an dernier, l'Assemblée générale de l'ONU a chargé un nouveau Groupe d'experts gouvernementaux de l'ONU (« GEG ») d'inviter les opinions nationales sur le droit international.[19] En outre, le nouveau GEG comprend également un Groupe de travail à composition non limitée (« Groupe de travail ») sur les progrès réalisés dans le domaine de l'Information et des Télécommunications dans le contexte de la Sécurité internationale parrainé par l'ONU, qui a donné aux participants l'occasion de faire des déclarations, dont quelques-unes font référence au droit international.[20] Cependant, le GEG ne jouit de la participation que de quatre États membres de l'OEA (Brésil, Mexique, États-Unis et Uruguay). En contraste, le Groupe de travail est ouvert à tous les États membres de l'OEA. Mais la majorité des contributions liées au droit internationalsont restées très généralisées. Aussi, à l'instar du GEG, le Groupe de travail fait porter ses efforts exclusivement sur des questions de sécurité internationale et, par conséquent, limite les opinions de l'État à l'application du droit international.

10. Par conséquent, il faut créer des tribunes supplémentaires où les États membres

---

documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace ("The Netherlands Views"/Points de vue des Pays-Bas).

16 *Voir, par exemple,* Egan, *supra* note **Error! Bookmark not defined.**, dans 817.

17 *Voir, par exemple,* CICR, *Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts* (novembre 2019); MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017) ("*Tallinn 2.0*"); *voir également* CICR, *Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflict* (novembre 2019); CICR, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* (octobre 2015) 39-44.

18 Egan, *supra* note **Error! Bookmark not defined.**, à 817 ("Les interprétations ou applications du droit international proposées par des groupes non gouvernementaux peuvent ne pas refléter la pratique ou les points de vue juridiques de bon nombre d'États ou de la majorité d'entre eux. Le silence relatif des États pourrait mener à l'imprévisibilité dans le domaine cybernétique, où les États peuvent faire des suppositions sur les opinions des autres sur le cadre juridique applicable. Dans le contexte d'un incident cybernétique spécifique, cette incertitude pourrait donner lieu à des perceptions erronées et à des erreurs de calcul de la part des États, ce qui pourrait mener à une escalade et, dans le pire des cas, à des différends.").

19 *Voir* UNGA Res. 266, *supra* note **Error! Bookmark not defined.**, ¶3 (sur le mandat du GEG).

20 *Voir* U.N. Doc. A/RES/73/27, ¶5 (5 décembre 2018). Divers États (encore majoritairement européens) ont utilisé leurs commentaires sur les projets de rapports du Groupe de travail pour élaborer des points de vue sur comment s'applique le droit international au cyberespace. *Voir, par exemple,* Autriche, *Comments on Pre-Draft Report of the OEWG - ICT* (31 mars 2020); Ministère des relations extérieures de la République tchèque, Commentaires présentés par la République tchèque en réponse au rapport « préliminaire » initial du Groupe de travail à composition non limitéesur l'évolution dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale *(Commentaires présentés par la République tchèque en réaction à l'avant-projet de rapport initial du Groupe de travail à composition non limitée sur les faits nouveaux dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale)*. Ces exposés et d'autres faits devant le Groupe de travail peuvent être consultés à l'adresse : https://www.un.org/disarmament/open-ended-working-group/.

pourraient être encouragés à exprimer leurs propres points de vue sur l'application du droit international, et des occasions de le faire pourraient leur être offertes. Ce projet marque une première tentative (et plutôt prudente) de répondre à ce besoin dans la région. Il n'est pas conçu pour se substituer aux processus en cours de l'ONU ou pour compétitionner avec eux. Il a plutôt pour objectif de compléter ces efforts en permettant à toutes les voix de notre région de participer à la panoplie complète de l'application du droit international au comportement de l'État dans le cyberespace et d'explorer cette panoplie. À cet égard, le travail du Comité est en ligne avec l'appel lancé par l'Union européenne aux États membres de l'ONU à « présenter des contributions nationales sur la question de comment le droit international s'applique à l'utilisation [de technologies de l'information et de la communicati ouon] de la part des États."[21]

11. Le projet actuel a tenté de répondre au besoin d'avoir une plus grande transparence régionale en utilisant deux méthodes différentes : (i) un questionnaire préparé conjointement avec le Département du droit international de l'OEA (avec des contributions du CICR) et diffusé pour la première fois auprès des États membres en février 2019; et (ii) une discussion informelle avec des représentants juridiques des États membres selon les règles de la "Chatham House" (c'est-à-dire que les déclarations faites pendant la réunion peuvent se répéter, mais l'identité des orateurs et autres participants demeure confidentielle). Un exemplaire du questionnaire est inclus à l'annexe A du présent rapport.

12. Mon troisième rapport a apporté une mise à jour du contenu du questionnaire et a demandé de repousser la date limite pour répondre, ce que le Comité a accepté.[22] Mon quatrième rapport concerne la compilation que j'ai faite des réponses reçues de neuf États : Bolivie, Brésil, Chili, Costa Rica, Équateur, États-Unis, Guatemala, Guyana et Pérou. [23] Sur ce nombre, sept se sont avérés substantiels, tandis que les États-Unis ont remis au Comité leurs déclarations puboiques antérieures.[24] Le Brésil a souligné les travaux qu'il lui reste à faire au sein du GEG (dont l'Ambassadeur du Brésil occupe la présidence), ce groupe étant la tribune qui devrait aborder des questions relatives à l'application du droit international.[25] Les sept réponses substantielles en entier sont jointes au présent rapport en tant qu'Annexe B.

---

21 Déclaration de l'UE, *supra* note **Error! Bookmark not defined.**.

22 Duncan B. Hollis, *Derecho Internacional y Operaciones Cibernéticas Estatales: Mejorando la Transparencia: Tercer Informe*, OEA/Ser.Q, CJI/doc 594/19 (24 juillet 2019) ("Hollis, Troisième Rapport"), dans http://www.oas.org/en/sla/iajc/docs/CJI_doc_594-19.pdf.

23 *Voir Note de l'État plurinational de Bolivie, Ministère des relations extérieures, Mission permanente près l'OEA adressée au Comité juridique interaméricain,* MPB-OEA-NV104-19 (17 juillet 2019) (contenant les réponses au Questionnaire du CJI depuis le bureau du Commandant en chef de l'État Inspecteur général des Forces armées) ("Réponse de la Bolivie"); *Réponse présentée par le Chili au Questionnaire du Comité juridique interaméricain* (14 janvier 2020) ("Réponse du Chili"); *Communication de Carole Arce Echeverria, Costa Rica, Organisations internationales, Département de la politique extérieure, Ministère des relations extérieures et du culte adressée à l'OEA* (3 avril 2019) (incluant la lettre No. 163-OCRI2019 de Yonathan Alfaro Aguero, Bureau de coopération internationale et des relations adressée à Carole Arce Echeverria, qui comprend une réponse de l'« autorité pertinente » - la Cour d'appel pénale du Costa Rica (« Réponse du Costa Rica ») *Note verbal 4-2 186/2019 de la mission permanente de l'Équateur près l'OEA* (28 juin 2019) ("Réponse de l'Équateur"); Note Of. 4VM.200-2019/GJL/lr/bm, de M. Gabriel Juárez Lucas, Quatrième Vice-ministre du Ministère de l'intérieur de la République du Guatemala adressée à M. Luis Toro Utillano, Secrétaire technique, Comité juridique interaméricain (14 juin 2019) ("Réponse du Guatemala"); *Note Nº: 105/2019 de la mission permanente du Guyana près l'OEA* (30 juillet 2019) ("Réponse du Guyana"); *Réponse présentée par le Pérou au Questionnaire sur l'application du droit international dans les États membres de l'OEA dans le contexte cybernétique* (juin 2019) ("Réponse du Pérou").

24 *Voir* la note **Error! Bookmark not defined.**.

25 Réponse du Brésil au CJI de l'OEA, Note 2.2/14/19 (1er juillet 2019).

13. Outre la compilation des réponses au questionnaire, mon quatrième rapport a catalogué des conversations informelles additionnelles à ce sujet de concert avec des consultations tenues par le Secrétariat de l'OEA du Comité interaméricain contre le terrorisme (CICTE) avec le Bureau des affaires de désarmement des Nations Unies les 15 et 16 aout 2019, et la réunion informelle entre deux sessions du Groupe de travail. J'ai également souligné trois conclusions plus générales sur l'état de la transparence dans la région en ce qui concerne le droit international dans le cyberespace :

- En premier lieu, que tous les États membres qui ont répondu ont un intérêt permanent dans l'État de droit, y compris le rôle que peut jouer le droit international dans la réglementation du comportement de l'État dans le cyberespace.
- Deuxièmement, les réponses révèlent l'inégalité des capacités juridiques de l'État dans ce domaine. Certains États ont fait preuve d'une profonde connaissance des opérations cybernétiques ainsi que des nouveaux problèmes juridiques internationaux qu'elles entrainent, tandis que d'autres ont fait preuve de beaucoup moins de familiarité avec les normes juridiques internationales sous-jacentes et les questions particulières que leur application entraine dans le contexte cybernétique. Cela suggère qu'une création accrue de capacité juridique internationale est nécessaire, au-delà de l'excellent travail réalisé jusqu'à maintenant par le CICTE ainsi que par divers États membres.[26]
- En troisième lieu, le faible pourcentage de réponses au questionnaire du Comité suggère que les États sont encore réticents à être transparents dans leurs points de vue sur l'application du droit international, même quand de nouvelles occasions de le faire leur sont offertes. Cela suggère qu'il faut encourager un plus grand nombre de réponses d'États ou tenter d'obtenir leurs contributions de façons moins formelles.

14. Avec l'approbation du Comité, la date limite pour répondre au Questionnaire a été reculée jusqu'au 1er juin 2020. Malheureusement, aucune réponse supplémentaire n'a été reçue. Ceci étant dit, plusieurs États membres ont fait des déclarations pertinentes dans leurs commentaires écrits relatifs aux projets de rapports du Groupe de travail sur la sécurité internationale.[27]

15. Avec l'aide du Département du droit international de l'OEA, nous avons mis sur pied un second véhicule pour amener une plus grande variété de points de vue de l'État sur le droit international et le cyberespace dans le domaine public : une conversation dans le genre de Chatham House sur la question. Le 23 juin 2020, le Département du droit international a organisé, animé par moi, une discussion de presque trois heures à laquelle ont participé des représentants juridiques de 16 États membres ainsi que du CICR. La conversation en profondeur a confirmé plusieurs des conclusions de mon quatrième rapport, en particulier la nécessité de créer dune capacité juridique plus importante. Aussi, plusieurs explications ont été apportées sur la réticence des États membres à consigner leurs opinions relatives à l'application du droit international au cyberespace.

---

26 Pour de plus ampoles renseignements sur les activités du CICTE, veuillez consulter : http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp. Au-delà du CICTE, plusieurs États membres ont appuyé également le renforcement de la capacité juridique. Le Canada et le Mexique, par exemple, ont co-accueilli, avec l'OEA, le 30 mai 2019, un atelier s'adressant aux États membres de l'OEA offrant une discussion sur l'application du droit international dans le cyberespace.

27 (Voir, par exemple, le deuxième « avant-projet » du rapport du Groupe de travail sur les progrès réalisés dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale (27 mai 2020) (*Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security)*, dans https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf. Les textes de diverses déclarations nationales peuvent être consultés à l'adresse https://www.un.org/disarmament/open-ended-working-group/.

16. Dans le présent rapport, je me suis arrêté sur trois points. Tout d'abord, je suis en train d'actualiser et de réviser la compilation des réponses des États au Questionnaire du Comité à la lumière de la réunion du 23 juin, de même que des déclarations pertinentes des États membres dans le processus du Groupe de travail à composition non limitée. Ce sondage révisé est joint au présent rapport, à l'Annexe B.

17. En deuxième lieu, sur la base des consultations du 23 juin, je désire souligner trois types de défis : techniques, politiques et juridiques, qui doivent être relevés si l'on veut obtenir de la part des États membres une plus grande transparence relativement à l'application du droit international au cyberespace. Techniquement, le supposé « problème d'attribution » complique la capacité des États membres à parler publiquement sur l'application du droit international. Les États peuvent savoir qu'ils ont été victimes d'une cyberattaque, mais ils ne peuvent pas discerner si l'auteur de cette attaque était un État (ou un représentant dont un État pourrait être considéré juridiquement responsable). Sans la capacité technique (ou un autre type de capacité) nécessaire pour attribuer une cyberopération à un État étranger, les États ne peuvent pas invoquer le droit international, étant donné que cette norme ne s'applique que si l'auteur est un État ou un acteur dont un État pourrait être juridiquement responsable. De même, là o les acteurs fonctionnent sous le couvert de l'anonymat, il est difficile d'identifier ce que l'État doit faire (et encore plus l'opinion de droit) étant donné que le comportement ne peut pas être attribué à un État.

18. Sur le plan politique, quelques-uns des problèmes de transparence des États membres sont internes : divers représentants juridiques ont parlé de la nécessité continue de mieux organiser la responsabilité pour aborder les problèmes liés à la cybernétique (ses cadres juridiques et de politiques nationales n'ont pas encore rejoint la réalité actuelle). Bien que plusieurs États luttent contre des problèmes de cybersécurité depuis un certain temps, pour d'autres États membres ces problèmes sont encore relativement nouveaux. Par conséquent, plusieurs États membres ont fait part du manque d'expérience des gouvernements (ou du manque de ressources) concernant des questions relatives à la cybernétique.

19. Dans d'autres cas, il s'agit de problèmes institutionnels; l'expérience existe, mais elle est distribuée d'une façon qui rend plus difficile la fusion en une vision formelle de l'État qui pourrait avoir un rayonnement. Plusieurs représentants du Ministère des relations extérieures ont souligné en particulier qu'un dialogue interne élargi est nécessaire pour garantir que les ministères des relations extérieures assument le rôle principal dans les discussions sur la cyberdiplomatie, notamment les discussions pertinentes pour l'application du droit international. En même temps, le désir de certains États de retenir la liberté de participer à des opérations cybernétiques a entrainé une réticence à prendre position sur quelles opérations le droit international pourrait interdire ou restreindre afin de ne pas limiter leur future liberté de manœuvre ou de réaction.

20. D'autres participants aux consultations du 23 juin ont mentionné des défis politiques externes à une plus grande transparence. Évidemment, certains États (par exemple les États-Unis, la Russie, la Chine) disposent actuellement d'une grande capacité pour effectuer des cyberopérations et pour se défendre contre de telles opérations, une capacité qui les a amenés à réexaminer des opinions discrètes, et souvent sujettes à controverse, sur le rôle régulateur du droit international. Quelques États membres ont affirmé avoir des réticences à faire des vagues afin de ne pas entrainer cet État dans une compétition et dans un conflit entre ces acteurs; ce sont des problèmes que les États peuvent éviter s'ils restent silencieux. Pour d'autres participants, la transparence ne devrait se produire que graduellement, avec le temps, une fois que les États membres auront eu de plus amples occasions de participer à des dialogues et des discussions diplomatiques prudents.

21. En même temps, bon nombre des participants aux consultations du 23 juin ont reconnu que certaines des raisons du silence de l'État étaient tant juridiques que politiques : plusieurs États membres n'ont pas encore suffisamment d'expérience sur les façons dont le droit internationalpeut se manifester dans le contexte cybernétique pour formuler une opinion sur quelques-unes des

questions les plus actuelles et les plus pressantes (et si un État ne peut pas formuler une opinion informée, il ne peut pas être transparent).[28] Un participant a exprimé cette pensée de façon succincte : « nous n'en sommes pas encore là », c'est-à-dire qu'ils ne sont pas prêts à appliquer le droit international au contexte cybernétique.

22. En troisième lieu, vu les résultats du questionnaire et la discussion du 23 juin, le soussigné formulerait trois propositions concrètes pour examen spécifique par le Comité et par l'OEA et ses États membres de façon plus large.

28 Évidemment, de tels États pourraient être transparents sur leur incapacité à formuler un point de vue, mais on comprend que peu d'États, sinon aucun, désirent formuler une telle concession publiquement.

Proposition 1 : Le Comité devrait recommander que l'Assemblée générale de l'OEA appuie l'applicabilité du droit international aux opérations étatiques ainsi qu'à celles qui sont appuyées par l'État

23. Comme nous l'avons indiqué, l'Assemblée générale des Nations Unies et plusieurs organisations régionales (ANASE, l'UE) ont appuyé l'applicabilité du droit international au comportement de l'État dans le cyberespace. Jusqu'à maintenant, toutefois, l'OEA ne l'a pas fait. L'appui de l'OEA enverrait un signal clair relativement à l'engagement de l'Organisation et de la région envers l'État de droit dans le cyberespace. Une formulation possible pour une déclaration de ce type serait la suivante :

> *L'Assemblée générale de l'OEA affirme que le droit international, y compris la Charte des Nations Unies dans son entièreté, la Charte de l'Organisation des États Américains, le droit international humanitaire, le droit international des droits de la personne, le devoir de non-intervention, l'égalité souveraine des États et le droit de la responsabilité des États, s'appliquent à l'utilisation des technologies de l'information et de la communication (TIC) de la part des États ainsi que des acteurs responsables internationalement.*

La région de l'OEA profite de l'acceptation par les États membres de l'application de certains systèmes judiciaires internationaux (par exemple, le droit international humanitaire) pour lesquels un consensus mondial n'a pas encore été possible. J'ai également inclus la souveraineté dans la liste, bien que certains États membres pourraient avoir des doutes sur la façon dont elle est appliquée. En tout cas, en adoptant une position claire sur quelles sont les normes du droit international qui s'appliquent, l'OEA pourrait contribuer à cette conversation mondiale et, ce faisant, promouvoir l'État de droit.

24. Comme alternative – ou en tant qu'étape intermédiaire – le Comité lui-même pourrait appuyer cette formulation dans une de ses résolutions, et l'envoyer à l'Assemblée générale pour examen.

Proposition 2 : Conserver cette question à l'ordre du jour du Comité et élargir sa portée au-delà des thèmes du droit international, vers la paix et la sécurité internationales

25. Bien que mon mandat au sein du Comité expire à la fin de l'année civile, le Comité portera sans aucun doute une plus grande attention à ce point de l'ordre du jour. Cela sera le cas que le Comité (ou l'Assemblée générale) agisse ou non relativement à ma première proposition. Les participants à la discussion du 23 juin étaient enthousiastes à la possibilité de nouveaux échanges diplomatiques. Avec l'aide du Département du droit international, le Comité pourrait continuer d'organiser périodiquement de tels échanges diplomatiques. Les faibles risques que cela comporte et les obstacles peu nombreux à la participation amèneraient des occasions d'identifier des convergences et des divergences entre les points de vue des États, lesquelles peuvent ensuite être organisées contre la menace d'opérations cybernétiques parrainées par l'État pour lesquelles il n'existerait pas de réglementation appropriée ni de restrictions, comme jusqu'à maintenant.

26. Si l'on disposait de plus de temps et que l'on pouvait y apporter plus d'efforts, il pourrait être possible d'obtenir un plus grand nombre de points de vue « officiels » des États membres, ce qui aiderait à atteindre l'objectif général d'améliorer la transparence sur comment le droit international s'applique au cyberespace. Ce faisant, en outre, le Comité pourrait envisager d'élargir la portée de l'application pour couvrir d'autres questions, outre la paix et la sécurité

internationales, qui dominent les processus actuels de l'ONU. Mon questionnaire n'abordait pas, par exemple, le devoir de non-intervention, même quand plusieurs représentants de l'État ont demandé qu'une grande attention soit portés à cette question dans mes consultations du 23 juin. De même, plusieurs participants ont demandé qu'une plus grande attention soit portée au rôle du droit international des droits de la personne dans le cyberespace; c'est une question que le Comité pourrait aborder seul ou de concert avec la Commission interaméricaine des droits de l'homme.

27. Le Comité pourrait également tenter d'améliorer la transparence sur les façons dont le droit international protège le secteur de la santé. La pandémie de COVID-19 a touché gravement la région tant sur le plan humanitaire que sur le plan économique. Malheureusement, les cybermenaces risquent de causer encore plus de donnages, comme en font foi les cyberattaques contre des hôpitaux et, plus récemment, les efforts déployés dans la recherche de vaccins. Par conséquent, le Comité pourrait centraliser son attention sur une question cruciale d'intérêt actuel, qui apporterait une aide aux États membres et à leurs ressortissants dans toute la région.[29]

29 Pour obtenir des renseignements sur un effort permanent visant à clarifier les protections du droit international dans le domaine de la santé contre les cybermenaces, veuillez consulter Dapo Akande, Duncan Hollis, Harold Hongju Koh et Jim O'Brien, *Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector,* JUST SECURITY (21 mai 2020) (envoi multiple à OPINIO JURIS et à EJILTALK!).

Proposition 3 : Appuyer ou entreprendre des efforts additionnels de création de capacité juridique

28. Le CICTE et divers États membres ont entrepris, déjà, des efforts considérables et importants en vue de créer des capacités sur des questions de cybernétique entre les États membres, tant la capacité de comprendre la nature technique des TIC que les menaces qu'elles posent, de même que la capacité de comprendre et d'évaluer les problèmes juridiques qu'entrainent ces menaces. Toutefois, tant les réponses au questionnaire que les consultations du 23 juin indiquent clairement qu'il reste beaucoup à faire, en particulier dans le contexte du développement de la capacité juridique. Les participants aux consultations du 23 juin se sont exprimés abondamment sur la nécessité de développer des capacités additionnelles dans l'application du droit international dans le contexte cybernétique. Plusieurs États membres (par exemple l'Argentine, le Canada et les États-Unis) ont exprimé des opinions similaires dans leurs récents commentaires présentés au Groupe de travail à composition non limitée[30]. Par conséquent, le Comité semblerait disposer d'un solide appui s'il choisit de se montrer disposé à offrir son expérience ou ses ressources dans le cadre des efforts de création de capacité déployés actuellement.

29. Une possibilité serait que le Comité envisage la possibilité d'appuyer les efforts de création de capacité existants ou de déployer ses propres efforts additionnels (et plus diversifiés) en ce sens. Les cours sur l'application du droit international au cyberespace pourraient être complémentés par des cours qui offriraient une « formation technique » à des experts non techniciens pour aider les diplomates des États et autres représentants à comprendre et à évaluer avec précision le fonctionnement des cybermenaces. Une autre possibilité serait que le Comité utilise ses réunions avec les conseillers juridiques du Ministère des relations extérieures pour « pratiquer, comme dans un jeu », certains scénarios dans lesquels interviennent des cybermenaces afin de fournir aux avocats du gouvernement un plus grand nombre d'occasions d'appliquer les normes juridiques pertinentes (et, ce faisant, aider à faciliter le développement d'un État en ce qui concerne sa propre vision de la façon dont s'applique la loi). Enfin, le Comité pourrait vouloir tenir régulièrement des conversations comme celles qui ont eu lieu en juin, organisant et animant des discussions sur l'application du droit internationalentre les États membres (et peut-être, à un moment donné, avec d'autres parties intéressées pertinentes de l'industrie et de la société civile).

30. En résumé, par le biais d'efforts plus soutenus de transparence et de création de capacité, le Comité pourrait apporter une contribution importante à l'amélioration de l'application (et de l'efficacité) du droit international en tant qu'outil de réglementation dans le cyberespace. En outre, il pourrait le faire seul ou de concert avec d'autres institutions de l'OEA, certains États membres ou d'autres organisations. Le CICR, par exemple, a fait part de son enthousiasme à l'idée d'appuyer des efforts plus importants de création de capacité relativement au droit international dans la région.

31. Cela a été pour moi un grand privilège que de travailler à cette question pendant mon passage au sein du Comité. Je suis convaincu que les cybermenaces, dont les opérations des États et de leurs représentants, créent des risques qui comportent d'importantes conséquences économiques, humanitaires et de sécurité nationale. Le droit international fournit un mécanisme – que le temps a

---

30 *Voir, par exemple,* Argentine, *Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security* ("Avant-projet"du rapport du Groupe de travail à composition non limitée sur l'évolution dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale); Michael Walma, *Canadian Comments on Draft OEWG Report* (6 avril 2020); États-Unis, *United States Comments on the Chair's Pre-draft of the Report of the U.N. Open Ended Working Group (OEWG)* (6 avril 2020). Ces déclarations nationales (et d'autres) peuvent être consultées sur la page Web du *Groupe de travail à composition non limitée* à l'adresse https://www.un.org/disarmament/open-ended-working-group/.

validé – pour réglementer les nouvelles menaces. Les défis techniques, politiques et juridiques ont toutefois fait que la loi en général (et la pratique de l'État et l'*opinio juris*, qui comprennent la coutume spécifiquement) soient moins visibles, et par conséquent moins effectives, jusqu'à maintenant. Avec une plus grande transparence sur la façon dont les États entendent la loi pour fonctionner, il faudrait envisager une occasion plus importante de jouer un rôle régulateur très nécessaire afin de restreindre le comportement non désiré et de faciliter une aide et une coopération accrues. Je désire que ces rapports sur les résultats du questionnaire ainsi que d'autres conversations dans la région puissent constituer un premier et modeste pas pour améliorer la visibilité de l'application du droit international au cyberespace. Ils stimuleraient également le Comité (et l'OEA) à continuer à participer à des efforts similaires à l'avenir et j'ai hâte de voir les produits et processus qui découleront de ces efforts.

ANNEXE A

OEA Plus de droits pour plus de personnes

CJI

COMITÉ JURIDIQUE INTERAMÉRICAIN

COMITÉ JURIDIQUE INTERAMÉRICAIN
Av. Marechal Floriano, 196 - 3º andar - Palácio Itamaraty - Centro - Rio de Janeiro, RJ - 20080-002 - Brésil
Tel.: (55-21) 3172-1474 -

OEA/2.2/14/19

Le Département du droit international du Secrétariat aux questions juridiques du Secrétariat général de l'Organisation des États Américains, en sa qualité de Secrétariat technique du Comité juridique interaméricain (CJI), présente ses compliments aux missions permanentes et a l'honneur de les informer que le CJI effectue une étude sur l'application du droit international dans le contexte cybernétique dans les États membres de l'OEA.

Pour ce faire, le Comité demande de bien vouloir répondre aux questions suivantes :

1. Votre Gouvernement a-t-il rendu public un quelconque document officiel, un discours ou une déclaration similaire qui résume comment il entend que le droit internatiuonal s'applique aux opérations cybernétiques? Veuillez présenter des copies ou donner le lien vers ces déclarations.
2. Les branches du droit international actuel (y compris l'interdiction de l'utilisation de la force, le droit de légitime défense, le droit international humanitaire et les droits de la personne) s'appliquent-elles au cyberespace? Existe-t-il des domaines dans lesquels la nouveauté du cyberespace exclut l'application d'un ensemble spécifique de droits ou d'obligations juridiques internationaux?
3. Une opération cybernétique peut-elle constituer en elle-même une instance d'utilisation de la force? Peut-elle constituer une attaque armée qui entrainerait un droit de légitime défense en vertu de l'article 51 de la Charte des Nations Unies? Une opération cybernétique peut-elle être qualifiée d'utilisation de la force ou d'attaque armée sans causer les effets violents qui ont été utilisés comme seuils dans des conflits cinétiques passés?
4. À part les conflits armés, quand un État serait-il responsable pour les opérations cybernétiques d'un acteur non étatique? Quel degré de contrôle ou de participation un État doit-il avoir dans les opérations de l'acteur non étatique pour entrainer la resoponsabilité juridique internationale de cet État?
5. Les normes de responsabilité de l'État sont-elles les mêmes ou non dans le contexte d'un conflit armé tel que défini aux articles 2 et 3 communs aux Conventions de Genève de 1949?
    a) Selon le droit international humanitaire, une opération cybernétique peut-elle être qualifiée d'« attaque » conformément aux normes qui régissent la conduite des

hostilités si elle ne cause pas la mort, aucune lésion ni aucun dommage physique direct au système informatique en question ou à l'infrastructure qui le soutient? Une opération cybernétique qui produirait seulement une perte de fonctionnalité, par exemple, pourrait-elle être qualifiée d'attaque? S'il en est ainsi, dans quels cas?

6. Une opération cybernétique qui attaquerait seulement des données serait-elle régie par l'obligation, dans le droit international humanitaire, de diriger des attaques seulement contre des objectifs militaires et non contre des objectifs civils?

7. La souveraineté est-elle une norme discrète du droit international qui interdit aux États de participer à des opérations cybernétiques spécifiques? S'il en est ainsi, cette interdiction couvre-t-elle les opérations cybernétiques qui se trouvent sous le seuil de l'utilisation de la force et qui, en outre, ne violent pas le principe de non-intervention?

8. La diligence appropriée est-elle une norme de droit international que les États doivent respecter dans l'exercice de leur souveraineté sur les technologies de l'information et de la communication sur leur territoire ou sous le contrôle de leurs ressortissants

9. Existe-t-il d'autres règles de droit international dont votre Gouvernement estime qu'il est important de tenir compte dans l'évaluation de la réglementation des opérations cybernétiques par les États ou acteurs et dont un État serait responsable sur le plan international?

Pour des explications supplémentaires sur le questionnaire, veuillez consulter le rapport du CJI intitulé "Le droit international et les opérations cybernétiques des États : amélioration de la transparence", présenté en annexe du document portant la cote CJI/doc. 578/19.

Les réponses doivent être envoyées avant le 28 juin 2019 au Secrétariat technique du CJI, au Département du droit international, par l'intermédiaire de Luis Toro Utillano par courriel à l'adresse ltoro@oas.org. Il est également possible de communiquer avec nous au numéro de téléphone (202) 370-0632 y al Fax (202) 458-3293.

Le Département du droit international du Secrétariat aux questions juridiques du Secrétariat général de l'Organisation des États Américains saisit cette occasion pour renouveler aux missions permanentes près l'OEA les assurances de sa très haute considération.

Washington, D. C., le 20 mars 2019

Annexe B

Réponses au questionnaire du Comité juridique interaméricain du 14 février 2019 sur l'application du droit international au sein des États membres de l'OEA dans le contexte cybernétique[1]

Question 1 : Votre gouvernement a-t-il rendu publics un quelconque document officiel, discours ou déclaration similaire qui résume la façon dont il entend que le droit international s'applique aux opérations cybernétiques? Prière de joindre des copies de ces déclarations ou des liens y menant.

1. Dans cette première question, on demandait les déclarations nationales faites sur le droit international et le cyberespace. La question avait pour but d'informer le Comité des opinions énoncées antérieurement et de faire que les États membres n'auraient pas à répondre aux questions s'ils avaient déjè adopté une position de fond pertinente. Cependant, sur les neuf réponses obtenues, seule celle des États-Unis disait qu'ils avaient fait des déclarations et des discours antérieurement

1 Sept États – la Bolivie, le Chili, le Costa Rica, l'Équateur, le Guatemala, le Guyana et le Pérou – ont répondu officiellement au questionnaire. *Voir la note de l'État plurinational de Bolivie, Ministère des relations extérieures, mission permanente de l'OEA près le Comité juridique interaméricain*, MPB-OEA-NV104-19 (17 juillet 2019) (qui contient les réponses du Bureau du Commandant en chef des Forces armées de l'État, Bureau de l'Inspecteur général des Forces armées, au questionnaire du CJI ("Réponse de la Bolivie"); *Réponse présentée par le Chili au questionnaire du Comité juridique interaméricain de l'OEA* (14 janvier 2020) ("Réponse du Chili"); *Communication de Carole Arce Echeverría, Organismes internationaux, Direction générale de la politique extérieure, Ministère des relations extérieures et du culte du Costa Rica près l'OEA* (3 avril 2019) (à laquelle est jointe la lettre 163-OCRI2019, de Yonathan Alfaro Aguero, Bureau de coopération et des relations internationales, adressée à Carole Arce Echeverría, avec la réponse de la Cour de cassation pénale, (l'"instance pertinente") ("Réponse du Costa Rica"); *Note verbale 4-2 186/2019 de la mission permanente de l'Équateur près l'OEA* (28 juin 2019) ("Réponse de l'Équateur"); Note Of. 4VM.200-2019/GJL/lr/bm, de Gabriel Juárez Lucas, Quatrième Vice-ministre, Ministère de l'Intérieur, à Luis Toro Utillano, Secrétariat technique du Comité juridique interaméricain (14 juin 2019) ("Réponse du Guatemala"); *Note No: 105/2019 de la mission permanente du Guyana près l'OEA* (30 juillet 2019) ("Réponse du Guyana"); *ponse du Pérou au questionnaire sur l'application du droit international dans les États membres de l'OEA dans le contexte cybernétique* (juin 2019) ("Réponse du Pérou").

La réponse des États-Unis envoyait le Comité à ses déclarations publiques antérieures. *Voir*, Brian Egan, *Remarques sur le droit international et la stabilité dans le cyberespace* (10 novembre 2016), dans *Digest of U.S. Practice in Int'l Law* 815 (2016); *Soumission des États-Unis au Groupe d'experts gouvernementaux sur les avancées dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale* (octobre 2016), dans *Digest of U.S. Practice in Int'l Law* 823 (2016); *Soumission des États-Unis au Groupe d'experts gouvernementaux sur les avancées dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale* (octobre 2014), dans *Digest of U.S. Practice in Int'l Law* 732 (2014); Harold Koh, *Droit international dans le cyberespace* (18 septembre 2012), dans *Digest of U.S. Practice in Int'l Law* 593 (2012). Récemment, le Conseiller juridique du Département de la défense des États-Unis a prononcé un discours qui comprenait également des opinions formelles sur l'application du droit international (bien qu'il n'est pas clair s'il parlait pour les États-Unis dans leur ensemble ou seulement pour le Département de la défense). *Voir, par exemple,* Paul C. Ney, "*Remarques du Conseiller général du Ministère de la défense à la Conférence juridique du cybercommandement des États-Unis*, 2 mars 2020, dans : https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/?dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

Le Brésil a répondu au questionnaire du Comité avec l'observation qu'il utiliserait le Groupe d'experts gouvernementaux des Nations Unies (GEG) sur "Promotion du comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale" comme tribune sur laquelle aborder ces questions. *Voir*, Réponse du Brésil au CJI, OEA, Note 2.2/14/19 (1er juillet 2019).

sur l'application du droit international au cyberespace, comme les discours de 2012 et de 2016 des conseillers juridiques de l'époque du Département d'État et les écrits présentés par les États-Unis en 2014 et 2016 lors de réunions du Groupe d'experts gouvernementaux (GEG) des Nations Unies sur les progrès réalisés en matière d'information et de télécommunications dans le contexte de la sécurité internationale.[2]

2. D'autres États qui ont répondu ont dit qu'ils n'étaient pas au courant de positions antérieures sur l'application du droit international dans le contexte cybernétique[3]. Plusieurs ont saisi l'occasion pour souligner les mesures internes qu'ils ont prises en vue de mettre sur pied des organisations pertinentes ou des ensembles de règlements dans le but d'aborder des questions liées aux technologies de l'information et de la communication (TIC)[4].

3. Plusieurs États membres ont utilisé le Groupe de travail à composition non limitée sur les progrès dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale parrainé par les Nations Unies pour faire des déclarations publiques qui ont comporté des références à l'application du droit international. Toutefois, la majorité de ces déclarations contenaient des énoncés très généraux ou ont été adaptées pour aborder diverses facettes spécifiques du texte du rapport du Groupe de travail à composition non limitée. Plusieurs de ces délégations sont d'États qui ont déjà répondu directement au questionnaire cu Comité. Toutefois, quelques États, comme l'Argentine, le Brésil, le Canada, la Colombie, le Mexique, le Nicaragua et l'Uruguay, ont fait des commentaires pertinents au questionnaire.[5] Par conséquent, nous présentons ci-dessous des références aux déclarations des pays.

---

2 En ce qui concerne les citations, voir la note 1 *supra*. Il convient toutefois d'indiquer que dans la réponse des États-Unis on disait que ce n'était que « quelques-uns » des documents dans lesquels le gouvernement exprimait ses opinions. Par conséquent, il est possible qu'il y en ait d'autres qui mériteraient notre attention. En particulier, il pourrait être utile de savoir dans quelle mesure le *Laws of War Manual*, du Département de la défense. Reflète les points de vue des États-Unis dans leur ensemble. Voir Office of General Counsel, U.S. Department of Defense, *Department of Defense Law of War Manual* (juin 2015, actualisé en décembre 2016) ("Manuel du Département de la défense").

3 Voir, par exemple, la réponse de l'Équateur, note 1 *supra*, en 1 ("On ne connait aucun document officiel du gouvernement de l'Équateur qui soit public, en ce qui concerne les opérations cybernétiques"); voir aussi la réponse du Guyana, note 1 *supra*, en 1 (idem).

4 Réponse de la Bolivie, note 1 *supra*, en 1 (où une nouvelle loi de 2015 est citée); réponse du Chili, note 1 *supra*, en 1 (où l'on mentionne la "Politique nationale en matière de cyberdéfense", du Ministère de la défense, publiée le 9 mars 2018); réponse du Guatemala, note 1 *supra*, en 1 (où on mentionne la "Stratégie nationale en matière de cybersécurité" et la nouvelle Loi contre la cybercriminalité); voir aussi la Réponse du Costa Rica, note 1 *supra*, en 1.

5 Toutes les déclarations nationales peuvent être consulter à Nations Unies, *Groupe de travail à composition non limitée*, sur le site Web : https://www.un.org/disarmament/open-ended-working-group/. *Voir, par exemple*, Argentine, *Avant-projet de rapport du Groupe de travail à composition non limitée sur les progrès dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale* ("commentaires de l'Argentine"); Brésil, *Commentaires présentés par le Brésil relativement à l'Avant-projet de rapport du Groupe de travail à composition non limitée sur les progrès dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationalel* (8 avril 2020) ("commentaires du Brésil"); Michael Walma, *Commentaires du Canada sur l'Avant-projet de rapport du Groupe de travail à composition non limitée sur les progrès dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale (6 avril 2020)* ("commentaires du Canada"); Colombie, *Commentaires de la Colombie sur l'Avant-projet de rapport du Groupe de travail à composition non limitée sur les progrès dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale* (16 avril 2020) ("commentaires de la Colombie"); Mexique, *Commentaires préliminaires du Mexique relativement à l'Avant-projet de rapport du Groupe de travail à composition non limitée sur les progrès dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale* (2020) ("commentaires du

4. Le faible nombre de déclarations officielles antérieures en combinaison avec le caractère général des déclarations faites plus récemment confirme l'hypothèse sur laquelle se base ce projet : que les États ont dit relativement peu jusqu'à maintenant sur la façon dont le droit international s'applique au comportement des États dans le cyberespace. Il confirme également que la majorité des activités internes liées à la cybersécurité ont porté principalement jusqu'à maintenant sur des stratégies ou des politiques nationales en matière de cybersécurité et de cybercriminalité interne, de même que sur d'autres facettes de la réglementation relative aux TIC.

Question 2 : Les branches du droit international actuel (y compris l'interdiction de l'utilisation de la force, le droit à la légitime défense, le droit international humanitaire et les droits de la personne) s'appliquent-elles au cyberespace? Existe-t-il des domaines dans lesquels la nouveauté du cyberespace exclut l'application d'un ensemble spécifique de droits ou d'obligations juridiques internationales?

5. Bien qu'une récente résolution de l'Assemblée générale des Nations-Unies[6] semble indiquer qu'il existe maintenant un soutien généralisé de l'application du droit internationnal au cyberespace, les premières tentatives faites par les Nations-Unies ont révélé que certains États avaient d'importantes réserves relativement à l'applicabilité de certains systèmes judiciaires internationaux. En fait, supposément à cause de ces réserves, le Groupe d'experts gouvernementaux des Nations-Unies qui s'est réuni en 2016 et en 2017 n'a pas élaboré de rapport final[7]. Par conséquent, il est toujour nécessaire de déterminer si l'existence de certains domaines du droit international relatifs au cyberespace est ou non une question controversée et, si elle l'est, quels sont ces domaines. La seconde question visait à recueillir les opinions des États sur des facettes du droit international qu'ils considéreraient inapplicables (ou dont l'application pourrait être à tout le moins problématique) dans le contexte cybernétique.

6. En général, les réponses au questionnaire reflètent un appui généralisé à l'application des domaines existants du droit international au cyberespace. Comme la réponse du Chili le résume, "le droit international en vigueur fournit le cadre juridique applicable [...], y compris les normes relatives au *jus ad bellum*, au droit international humanitaire, aux droits de la personne, ainsi que les normes qui régissent la responsabilité internationale des États"[8]. D'autres États qui ont confirmé

Mexique"); Nicaragua, *MINIC-MIS-143-04-2020* (avril 2020) ("commentaires du Nicaragua"); Uruguay, *Commentaires sur l'Avant-projet de rapport du Groupe de travail à composition non limitée sur les progrès dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale* (2020) ("commentaires de l'Uruguay").

Pour avoir des renseignements sur les commentaires d'autres États membres, voir le Chili, *Commentaires du Chili relativement au rapport préliminaire de la Présidence* (2020) ("commentaires du Chili"); l'Équateur, *Commentaires préliminaires de l'Équateur relativement au projet de rapport du Groupe de travail à composition non limitée des Nations-Unies sur les progrès réalisés dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale* (avril 2020) ("commentaires de l'Équateur"); le Venezuela (régime de Maduro) *Réflexions préliminaires du Venezuela relativement au projet de rapport du Groupe de travail à composition non limitée sur les progrès réalisés dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale* (2020) ("commentaires du Venezuela"); les États-Unis, *Commentaires des États-Unis sur le projet de rapport de la Présidence du Groupe de travail à composition non limitée sur les progrès réalisés dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale* (6 avril 2020) ("commentaires des États-Unis").

6 Voir AGNU résolution 266, UN doc. A/RES/73/266 (2 janvier 2019).

7 Voir, par exemple, Arun M. Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, dans *Lawfare* (4 juillet 2017), à l'adresse https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

8 Réponse du Chili, note 1 *supra*, en 1 (par conséquent, le Chili observe que "la planification, la conduite et l'exécution des opérations dans le cyberespace doivent se limiter strictement au respect du droit

l'application du droit international sont l'Équateur, le Pérou et les États-Unis[9]. Outre le *jus ad bellum* et le *jus in bello,* dans la réponse du Pérou on souligne la validité de plusieurs droits de la personne dans le cyberespace, dont "le droit à la vie privée et à l'intimité, la liberté d'information, la liberté d'expression, l'accès libre et égal à l'information, l'élimination du fossé numérique, les droits de propriété intellectuelle, la libre circulation de l'information, le droit au secret des communications, etc."[10]. Les États-Unis se font l'écho de l'application du droit international des droits de la personne, en même temps qu'ils envisagent l'application du droit international comme "pierre angulaire" de leur politique relative au cyberespace[11].

7. La Bolivie donne elle aussi une réponse positive, mais centrée sur le droit international "destiné à être appliqué dans les conflits armés", assortie d'opinions sur la façon de distinguer les affaires dans lesquelles le droit international humanitaire s'appliquerait et celles dans lesquelles il ne s'appliquerait pas[12]. Par conséquent, il n'est pas clair si la réponse positive de la Bolivie s'étend à l'application d'autres sous-domaines du droit international outre le *jus ad bellum* et le *jus in bello*.

8. Le Guatemala et le Guyana appuient l'application du droit international. Ils formulent toutefois tous les deux des réserves sur la portée universelle de l'application du droit existant. Sans donner d'exemples, le Guatemala fait observer qu'il pourrait y avoir des domaines dans lesquels "la nouveauté du cyberespace exclut quant à elle l'application de droits ou d'obligations déterminés à caractère international"[13]. Quant au Guyana, il indique que les opérations cybernétiques ne s'inscrivent pas dans des concepts traditionnels et qu'il existe un débat passionné sur si les domaines existants du droit international s'appliquent au cyberespace[14]. Tenant compte du travail antérieur du Groupe d'experts gouvernementaux de l'ONU (GEG), le Guyana affirme que bien qu'il reconnait que le droit international devrait s'appliquer au cyberespace, il est difficile d'appliquer des principes existants tels que l'usage de la force, qui implique traditionnellement un élément physique ainsi que des attaques avec un type d'arme quelconque[15].

---

international public, en tenant compte particulièrement du droit international des droits de la personne et du droit international humanitaire").

9 Réponse de l'Équateur, note 1 *supra*, en 1 ("les branches du droit international s'appliquent au cyberespace") ; réponse du Pérou, note 1 en 1 ("considérant le rôle essentiel qui revient à la Charte du fait de son lien avec d'autres instruments internationaux [...], on pourrait considérer qu'il n'existerait aucun domaine des relations internationales qui soit en marge des principes mentionnés. Étant donné que le cyberespace se convertit en scène quotidienne d'interaction au niveau international, les acteurs de ces relations sont obligés de respecter les obligations les plus importantes du droit international, au nombre desquelles on remarque l'interdiction de l'utilisation de la force, le droit à la légitime défense en le respect des droits de la personne et du droit international humanitaire"); Koh, note 1 en 594 (où il est indiqué que les principes du droit international s'appliquent au cyberespace, lequel n'est pas une zone "dépourvue de lois" où n'importe qui pourrait effectuer des activités hostiles sans restrictions et sans avoir à respecter des règles).

10 Réponse du Pérou, note 1 supra, en 1.

11 Écrit présenté par les États-Unis au GEG en 2014, note 1 *supra*, en 733 (l'application du droit international est la "pierre angulaire" des opinions des États-Unis, étant donné leurs caractéristiques distinctives); Egan, note 1 *supra*, en 815. Sur l'application des droits de la personne, voir Koh, note 1 *supra*, en 598; Egan, note 1 *supra*, en 820; écrit présenté par les États-Unis au GEG en 2016, note 1 *supra*, en 824.

12 Réponse de la Bolivie, note 1 *supra*, en 2 a 7. La Bolivie indique que le droit international humanitaire ne régirait pas les opérations cybernétiques reliées à la sécurité nationale, la publicité, l'espionnage, la manipulation de la structure stratégique essentielle, les opérations cybernétiques à des fins politiques ou la piraterie de systèmes privés qui mette en danger les opérations économiques et sociales de l'État. Íd. en 3 a 7.

13 Réponse du Guatemala, note 1 *supra*, en 1 et 2.

14 Réponse du Guyana, note 1 *supra*, en 1 et 2.

15 Id.

9. Par conséquent, bien que l'application générale du droit international aux opérations cybernétiques semble être fermement enracinée, les deux dernières réponses semblent indiquer qu'il faut poursuivre le dialogue. Il serait utile d'indiquer *quels domaines* particuliers d'application du droit international donnent matière à réflexion à certains États et pourquoi. Cela aiderait à comprendre le degré de convergence (ou de divergence) d'opinions sur la façon dont les systèmes judiciaires internationaux régissent les opérations cybernétiques des États ou parrainées par ces derniers.

10. Les commentaires faits par les États membres au Groupe de travail à composition non limitée sur les progrès réalisés dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale renforcent ces facettes. Ceux-ci reflètent le large consensus voulant que le droit international, y compris la Charte des Nations-Unies, s'applique au cyberespace. Le Canada, le Chili, la Colombie, le Mexique, l'Uruguay et les États-Unis ont tous exprimé explicitement cette idée.[16] Quelques États, par exemple le Nicaragua et le Venezuela (représenté par le régime de Maduro), ont remis en question la pertinence du droit international en vigueur dans le cyberespace malgré le fait qu'ils ont accepté son application dans ce contexte.[17] D'autres commentaires ont ajouté un nouveau degré de préoccupation qui n'avait pas été exprimé dans les réponses au questionnaire du Comité; par exemple, si les différences dans la capacité juridique pourraient affecter la véritable application ou l'évolution de la loi (étant donné que les États dotés d'une infrastructure avancée en matière de cybersécurité pourraient disposer de la capacité nécessaire pour influencer de façon disproportionnée le contenu et les limites des normes relatives au cyberespace sur les États qui n'ont pas cette capacité).[18]

Question 3 : Une opération cybernétique peut-elle en elle-même constituer une utilisation de la force? Peut-elle constituer une attaque armée qui crée un droit de légitime défense en vertu de l'article 51 de la Charte des Nations-Unies? Une opération cybernétique peut-elle être qualifiée d'utilisation de la force ou d'attaque armée sans causer les effets violents qui ont été utilisés pour marquer ce seuil dans des conflits cinétiques passés?

11. La majorité des États, mais pas tous, semblent accepter l'application du droit international relatif à l'utilisation de la force (par exemple le *jus ad bellum*) à leurs opérations cybernétiques. Cette question visait à déterminer quels États de la région adhèrent à cette position prédominante et lesquels adhèrent à d'autres positions. En même temps, d'autres questions ont surgi relativement à l'application entre les États qui acceptent le *jus ad bellum* dans le cyberespace, en particulier dans quelle mesure les seuils tablis pour l'"utilisation de la force" ou les "attaques armées" nécessitent la présence d'effets "violents" analogues à ceux qui étaient considérés

16 *Voir* commentaires du Canada, note **Error! Bookmark not defined.** *supra*; commentaires de la Colombie, note **Error! Bookmark not defined.** *supra*; commentaires du Chili, note **Error! Bookmark not defined.** *supra*; commentaires du Mexique, note **Error! Bookmark not defined.** *supra*; commentaires des États-Unis, note 5 *supra*; ocommentaires de l'Uruguay, note **Error! Bookmark not defined.** *supra*.

17 Commentaires du Nicaragua, note **Error! Bookmark not defined.** *supra* (il suggère que nous sommes confrontés à une "applicabilité déficiente" du droit international dans ce domaine mais ne nie pas en principe que le droit international s'applique au domaine des technologies de l'information et de la communication); commentaires du Venezuela, note 5 *supra* (il suggère qu'il faut "adapter le droit international au contexte des TIC, en tenant compte des vides juridiques existants"). Dans ses commentaires au Groupe de travail à composition non limitée sur les progrès dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, l'Argentine a demandé que les suggestions du Groupe de travail à composition non limitée soient utilisées pour clarifier l'application de l'interdiction d'utiliser la force et le droit international humanitaire. *Voir* commentaires de l'Argentine, *supra*, note 5.

18 *Voir, par exemple,* commentaires du Mexique, *supra*, note 5; commentaires de la Bolivie, *supra*, note 5; commentaires de l'Équateur, *supra*, note 5.

auparavant comme dépassant ces seuils. La question qui se pose maintenant est de savoir comment gérer les nouveautés par rapport à l'échelle ou les effets des opérations cybernétiques (c'est-à-dire les opérations qui ne sont pas similaires à des opérations cinétiques passées qui avaient dépassé le seuil de l'utilisation de la force ni à des sanctions économiques ou politiques qui n'avaient pas atteint ce seuil). Comment le droit international doit-il considérer ces opérations cybernétiques? Doivent-elles être placées automatiquement en-dessous ou au-dessus du seuil de l'utilisation de la force, ou faut-il faire plus de recherches et d'analyses pour diviser les opérations cybernétiques de cette nouvelle "zone grise" selon qu'elles sont au-delà ou en-deça des seuils correspondants?[19] Par conséquent, cette question permettait de savoir si les États considèrent les opérations cybernétiques comme des cas d'utilisation de la force (ou attaques armées) entièrement par analogie avec des cas qui se seraient produits antérieurement ou s'ils croient qu'il faut établir une nouvelle norme à cette fin.

12. La Bolivie, le Chili, le Guatemala, le Pérou et les États-Unis entendent clairement que les opérations cybernétiques pourraient par elles-mêmes entrainer l'interdiction de l'utilisation de la force et du droit inhérent d'autodéfense pour répondre à une "attaque armée"[20]. Comme l'a expliqué le Guatemala :

> Une opération cybernétique peut constituer en elle-même une utilisation de la force, étant donné que l'utilisation de la force ne se réfère pas exclusivement à la force physique, mais également aux risques ou aux atteintes à la sécurité et à la protection des tiers. [...] le droit à la ségitime défense existe face à une attaque ou à une opération cybernétique qui attente contre la souveraineté d'un pays[21].

Dans l'écrit présenté au GEG en 2014, les États-Unis ont souligné leur idée que le droit inhérent à la légitime défense pourrait s'appliquer à l'utilisation illégale de la force, ce qui semble indiquer un même seuil pour les deux normes[22]. Cela diffère de la position des États qui estiment que toutes les attaques armées constituent une utilisation de la force, mais que tous les cas d'utilisation de la force ne constituent pas des attaques armées (lesquelles comprendraient

---

19 Voir Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace,* 42 *Yale J. Int' L.* 1 (2017).

20 Réponse de la Bolivie, note 1 en 2 a 7; réponse du Chili, note 23 en 1 (le Chili s'abstiendra d'utiliser la force "a travers le cyberespace" d'une façon qui contrevienne au droit international et pourra exercer "son droit à la légitime défense face à une attaque armée perpétrée à travers le cyberespace"); réponse du Guatemala, note 23 *supra*, en 2; réponse du Pérou, note 1 *supra*, en 1 a 3; Koh, note 1 *supra*, en 595 (où on présente l'opinion des États-Unis selon laquelle *a*) les activités cybernétiques pourraient constituer une utilisation de la force dans certaines circonstances conformément à la signification établie à l'article 2.4 de la Charte des Nations Unies et dans le droit international coutumier, et *b*) les activités de réseaux informatiques qui constituent une attaque armée ou une menace imminente d'attaque armée pourraient mener à l'exercice du droit national de légitime défense d'un État, reconnu à l'article 51 de la Charte des Nations Unies); écrit présenté par les États-Unis au GEG en 2014, note 1 *supra*, en 734; Egan, note 1 *supra*, en 816 (où on indique que le GEG des Nations-Unies qui s'est réuni en 2015 a approuvé le droit à la légitime défense). L'Équateur a également répondu à la question par l'affirmative, mais il a cité la définition d'"attaque armée" utilisée à l'article 92 du manuel *Tallinn 2.0*, où cette expression est définie dans le contexte d'un conflit armé (c'est-à-dire le *jus in bello*), à la différence de la façon dont elle est utilisée à l'article 51 de la Charte des Nations Unies et dans le *jus ad bellum*. Voir la réponse de l'Équateur, note 1 *supra*, en 1.; MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2017) ("*Tallinn 2.0*"); *Voir* aussi *CICR*, *Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflict*. Dans les commentaires qu'elle a présentés au Groupe de travail à composition non limitée, la Colombie a exprimé l'idée que l'autodéfense est "essentielle pour maintenir la paix et la stabilité dans le domaine des TIC". Commentaires de la Colombie, *supra*, note 5.

21 Réponse du Guatemala, note 1 *supra*, en 2; réponse du Pérou, note 1 *supra*, en 3 (où on cite le CICR et Michael Schmitt, selon lesquels les utilisations de la force ne se limitent pas à la force cinétique).

22 Koh, note 1 *supra*, en 597.

seulement les formes "les plus graves" de l'utilisation de la force)[23]. Les États-Unis ont affirmé également qu'ils peuvent exercer leur droit inhérent de légitime défense suite à des activités cybernétiques constituant une attaque armée réelle ou imminente, indépendamment de si l'attaquant est un État ou un agent non étatique[24].

13. Par contre, le Guyana exprime des doutes dans sa réponse en ce qui concerne l'applicabilité du *jus ad bellum* aux opérations uniquement cybernétiques. En se basant sur la définition de force qui figure dans *Black's Law Dictionary* ("pouvoir considéré de façon dynamique"), le Guyana indique qu'il est possible qu'une opération cybernétique ne constitue pas en elle-même une utilisation de la force[25]. Il affirme également qu'une attaque armée implique l'utilisation d'armement et qu'une opération cybernétique, qui n'implique pas l'utilisation d'armement physique, ne peut pas être considérée comme une attaque armée qui entraine l'exercice de la légitime défense[26]. En même temps, le Guyana souligne qu'il est possible que des opérations cybernétiques soient utilisées dans des conflits armés; elles seraient alors régies par le droit international humanitaire[27].

14. En ce qui concerne la question de savoir si une opération cybernétique peut franchir le seuil de l'utilisation de la force (ou d'une attaque armée[28]) sans avoir d'effets violents, les opinions des États sont diverses. La majorité des États qui ont répondu préfèrent tracer les seuils pertinents au moyen d'analogies entre les opérations cybernétiques et des opérations passées, cinétiques ou d'un autre type, qui réunissaient ou non les conditions requises pour être considérées comme des utilisations de la force ou des attaques armée. Cependant, quelques États mentionnent la possibilité de ne pas se limiter à des analogies de ce type. Le Chili, par exemple, indique que les opérations cybernétiques analogues au seuil de gravité nécessaire pour répondre aux exigences établies en droit international pour être considérées comme des attaques armées peuvent entrainer le droit de légitime défense[29]. En même temps, la réponse du Chili laisse probablement place pour la définition des attaques armées en termes plus généraux en indiquant que les "cyberattaques dirigées contre leur souveraineté, leurs habitants, leur infrastructure physique ou de l'information" pourraient remplir les exigences pour être considérées comme des attaques armées[30].

15. Le Pérou admet plus ouvertement "la possibilité qu'une opération cybernétique dépourvue d'effets violents puisse être qualifiée d'utilisation de la force ou d'attaque armée"[31]. Toutefois, il se base sur l'idée que par le passé, un armement cinétique avait possiblement été utilisé sans causer d'effets violents et, malgré cela, aurait constitué une utilisation de la force (par exemple, le lancement d'un missile qui croiserait le territoire d'un autre État mais sans tomber dans cet État)[32]. En général, le Pérou souligne qu'il faut faire une distinction entre les "cyberattaques" (qui impliquent que "des dommages soient causés à un objectif militairement pertinent, celui-ci pouvant

---

23 Voir *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. U.S.)* [1986] ICJ Rep. 14, paragraphes 176 et 191 (27 juin) (où l'on décrit les attaques armées comme étant les formes les plus graves d'utilisation de la force).

24 Écrit présenté par les États-Unis au GEG en 2014, note 1 *supra*, en 734 et 735. Dans l'écrit, on réitère également la preuve de l'absence de volonté ou de capacité de se défendre d'un État sans son consentement dans les cas où un État territorial n'est pas disposé à arrêter ou à prévenir une attaque réelle ou imminente lancée dans le cyberespace ou au moyen de celui-ci ou s'il ne peut pas le faire. Id. en 735.

25 Réponse du Guyana, note 1 *supra*, en 2.

26 Id.

27 Voir id. en 3 et 5.

28 Cela part de la supposition qu'il pourrait y avoir deux seuils différents, contrairement à l'opinion des États-Unis. Voir les notes 23-25 *supra* et le texte qui les accompagne.

29 Réponse du Chili, note 1 *supra*, en 2.

30 Id. en 2.

31 Réponse du Pérou, note 1 *supra*, en 3.

32 Id.

être détruit totalement ou partiellement, ou même capturé ou neutralisé") et une "interruption abrupte des communications dans le cyberespace", c'est-à-dire "les opérations cybernétiques qui causent des inconvénients, y compris des inconvénients extrêmes, mais pas de lésions directes ni de morts, ni de destruction de la propriété"[33]. Par conséquent, dans sa réponse spécifique, le Pérou souligne l'établissement de la légalité des opérations cybernétiques dans le contexte de l'utilisation de la force en tenant compte de si elles peuvent "causer la mort ou des légions à des personnes ou des dommages à des biens"[34].

16. Le Guatemala adopte une approche différente dans sa réponse et exprime la volonté de repenser ce qui constitue des "effets violents" parce que les conséquences d'une opération cybernétique peuvent être "supérieures et ultérieures, menaçant des secteurs comme la santé et la sécurité, notamment"[35]. Il indique que dans le contexte cybernétique, les conséquences qui produisent "la mort, l'angoisse, la pauvreté" devraient être considérées violentes[36].

17. La Bolivie indique dans sa réponse qu'il pourrait être difficile d'appliquer le seuil dans la pratique parce que "les effets des cyberattaques ne seront pas toujours connus immédiatement", ce qui rend difficile vérifier s'il y a eu utilisation de la force. En même temps, la Bolivie indique qu'elle évaluera le seuil sur la base d'analogies avec le contexte cinétique, c'est-à-dire qu,il s'agirait d'une "attaque armée" si "l'attaque virtuelle cybernétique utilise des moyens non conventionnels mais qui ont le même impact qu'une attaque armée"[37].

18. Finalement, les États-Unis n'ont pas répondu au questionnaire en soi, mais leurs déclarations antérieures nous éclairent sur leurs opinions. Dans son important discours de 2012, Harold Koh a indiqué que les États-Unis préféraient une approche contextuelle pour identifier les cas d'utilisation de la force (avec, toutefois, l'exception susmentionnée voulant que la définition utilisée par les États-Unis comprend également les attaques armées) :

> Lorsque nous établissons si un événement constituait une utilisation de la force dans le cyberespace ou au moyen de celui-ci, nous devons évaluer des facteurs tels que le contexte dans lequel l'événement s'est produit, l'auteur de l'acte (en tenant compte des difficultés relatives à l'attribution dans le cyberespace), l'objectif et le lieu, les effets et l'intention, entre autres facettes possibles[38].

En même temps, M. Koh estime clairement que la preuve nécessite une analogie et demande si la lésion physique directe et les dommages patrimoniaux qui découlent de l'événement cybernétique semblent être ce qu'on pourrait considérer comme un cas d'utilisation de la force si des armes cinétiques les avait produits[39]. Il mentionne également des exemples concrets d'opérations cybernétiques qui constitueraient une utilisation de la force : i) la fusion du noyau du réacteur d'une centrale nucléaire causée par un acte cybernétique; ii) des opérations cybernétiques qui ouvrent un baccage en amont d'une zone peuplée et cause de la destruction, et iii) une opération cybernétique qui rend inutilisable le contrôle de la circulation aérienne et cause des accidents

---

33 Id. en 2.

34 Id. en 3.

35 Réponse du Guatemala, note 1 *supra*, en 2.

36 Id.

37 Réponse de la Bolivie, note 1 *supra*, en 2 à 7 (la Bolivie souligne que le droit de légitime défense comprend également la "légitime défense anticipée", à laquelle on peut avoir recours seulement quand la menace est imminente et la nécessité de se défendre est immédiate (au lieu d'être des représailles).

38 Koh, note 1 *supra*, en 595 ("les activités cybernétiques qui, directement ou indirectement, causent des morts, des lésions ou une destruction importante sont probablement considérées comme des utilisations de la force". Les États-Unis ont conservé ce point de vue depuis lors. Voir l'écrit présenté au GEG en 2014, note 1, en 734. Cet écrit a été annexé à celui de 2016, ce qui indique que son contenu était encore valide.

39 Koh, note 1 *supra*, en 595.

d'avion[40]. Dans la mesure où tous ces exemples impliquent une forme quelconque de "violence", il semblerait que les États-Unis favorisent un seuil pour l'utilisation de la force analogue à celui qui est utilisé dans le contexte cinétique.

Question 4 : À part les conflits armés, quand un État serait-il responsable des opérations cybernétiques d'un acteur non étatique? Quel degré de contrôle ou de participation un État doit-il avoir dans les opérations de l'acteur non étatique pour entrainer la responsabilité juridique internationale de cet État?

Question 5 : les normes en matière de responsabilité de l'État sont-elles ou non les mêmes dans le contexte d'un conflit armé, tel que ce terme est défini dans les articles 2 et 3 communs aux Conventions de Genève de 1949?

19. Les États sont responsables du comportement non seulement de leurs propres organes et services dans le cyberespace, mais aussi de tout agent non étatique qu'il appuie ou contrôle[41]. Aux questions 4 et 5 on demande qu'entendent les États de l'assignation de la responsabilité juridique internationale pour des actes commis par des agents non étatiques, en particulier le degré de "contrôle" requis par l'État. Comme chacun sait, les menaces cybernétiques peuvent être perpétrées non seulement directement par des États, mais également par divers agents non étatiques, dont des groupes hacktivistes et des organisation cybercriminelles. Dans certains cas, les États essaient d'utiliser ces agents non étatiques comme substituts pour effectuer diverses opérations cybernétiques.

20. Tracer les actes d'un substitut et les relier à un auteur principal dans le cyberespace peut être assez difficile sur le plan technique (bien que peut-être pas aussi difficile que certains le supposaient avant). En même temps, une connexion factice n'est pas suffisante et il doit y avoir également une attribution juridique, c'est-à-dire une connexion suffisante entre un État et un agent non étatique pour que le premier assume la responsabilité juridique pour les actes du second. Par exemple, un État pourrait approuver les actes d'un agent non étatique à posteriori et, ainsi, assumer la responsabilité juridique pour ceux-ci[42]. Une autre possibilité est que les États soient juridiquement responsables pour les actes des agents étatiques qui opèrent sous son contrôle, bien que le degré de contrôle n'est en général pas clair. Dans le cas du Nicaragua, la Cour internationale de justice (CIJ) a indiqué que le droit international contient une règle qui impose responsabilité à l'État pour les actes d'agents non étatiques sur lesquels il aurait un "contrôle effectif" (c'est-à-dire s'il ordonne l'acte ou dirige une opération)[43]. Toutefois, quelques années plus tard, le Tribunal pénal international pour l'ancienne Yougoslavie a adopté une norme moins stricte de "contrôle général" aux effets du droit international humanitaire. Selon le Tribunal, cette preuve nécessite quelque chose de plus que la simple fourniture d'équipement, d'entraînement militaire ou d'assistance financière, mais n'insiste pas sur l'émission d'ordres spécifiques par l'État ni sur sa conduite des opérations[44]. Par la suite, la Cour pénale internationale a approuvé la norme du "contrôle général"[45].

---

40 Id.

41 Voir Commission de droit international, *Projet d'articles sur la responsabilité de l'État pour des faits internationalement illicites*, dans *Rapport sur lre travaux réalisés lors de sa cinquante-et-unième session* (3 mai au 23 juillet 1999), UN doc. A/56/10 55 [3]; *Tallinn 2.0,* note 20 *supra*, règle 15.

42 Articles sur la responsabilité de l'État, note 41 *supra*, art. 11; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* 52 (2012).

43 *Nicaragua Case*, note 23 *supra*, par. 115.

44 *Prosecutor v. Dusko Tadić aka 'Dule'* (jugement) ICTY-94-1-A (15 juillet 1999), par. 131 à 145 et 162.

45 *Prosecutor v. Lubanga*, Affaire No. ICC-01/04-01/06, Salle de première instance, jugement (Cour pénale internationale, 14 mars 2012).

21. Toutefois, la CIJ a continué d'insister sur sa formule du "contrôle effectif" dans le contexte de l'utilisation de la force. En même temps, elle affirme que la preuve du "contrôle général" pourrait être appropriée dans le contexte du droit international humanitaire, ce qui rend possible un consensus sur le "contrôle général" dans le contexte du droit international humanitaire et le "contrôle effectif" dans d'autres contextes[46]. Par conséquent, dans le questionnaire nous avons posé des questions sur la responsabilité de l'État tant en général que dans le contexte du droit international humanitaire sur la base de l'existence d'un conflit armé dans le sens donné à cette expression dans les Conventions de Genève.

22. Dans leur réponse, plusieurs États membres soulignent la difficulté de l'attribution dans le cyberespace[47]. D'autres parlent moins de la question de la responsabilité pour des actes de substituts et parlent plus du devoir qui revient à l'État de s'assurer que son territoire ne soit pas utilisé par des agents non étatiques pour lancer des attaques[48]. À cet égard, le Pérou commente que "l'inertie d'un État face à un acteur non étatique qui pourrait causer une cyberattaque contre un autre État alors qu'il serait à même de contrôler pourrait causer que son comportement soit attribuable à l'État"[49]. La Bolivie, pour sa part, affirme que les États ne sont pas responsables s'ils ne disposent pas de l'infrastructure technologique nécessaire pour contrôler les agents non étatiques[50]. Les États-Unis indiquent que "le seul fait qu'une activité cybernétique ait été lancée depuis le territoire d'un autre État, qu'elle tire son origine autrement dans ce territoire ou qu'elle ait été lancée depuis l'infrastructure cybernétique d'un autre État est insuffisant, en l'absence d'autres éléments, pour attribuer cette activité à l'État"[51].

23. Les États qui se concentrent sur la question des agents substituts accordent une grande importance aux articles portant sur la responsabilité de l'État. Le Chili, le Guyana et le Pérou basent leur réponse sur l'article 8 :

> Un État est responsable d'une opération cybernétique illicite sur le plan international si celle-ci a été perpétrée par le truchement de l'un de ses organes, par une personne ou entité exerçant une autorité gouvernementale, ou bien par une

46 *Case concerning application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (jugement) [1997] ICJ Rep. 43, 208–09, par. 402 à 407 (où on indique que la preuve du contrôle général pourrait bien s'appliquer aux types de classifications utilisés en droit international humanitaire et être appropriée à eux).

47 Réponse du Guatemala, note 1 *supra*, en 3 (oùon indique qu'il "est extrêmement compliqué" de déterminer une claire responsabilité pour une attaque cybernétique); Réponse du Pérou, note 1 *supra*, en 4 (où on indique qu'il existe une grande "incertitude relativement à l'attribution, et aux niveaux d'attribution de la responsabilité pour les cyberattaques", ce qui rend plus difficile la possibilité de "contrôle de ceux qui utilisent le cyberespace pour déchainer des attaques par le biais d'Internet").

48 Réponse de l'Équateur, note 1 *supra*, en 1 ("Les États ne sont pas responsables d'une attaque d'un acteur non étatique, bien qu'il devrait y avoir moyen de collaborer afin de trouver les responsables de de celle-ci. Il incombe également à l'État de réglementer les services et d'établir des normes à ce sujet pour éviter qu'une attaque puisse se produire à partir du territoire appartenant à un État"); Réponse du Guatemala, note 1 *supra*, en 3 (où ce pays répond dans la perspective de la diligence appropriée de l'État hôte plutôt que du degré de contrôle exercé sur des agents substituts).

49 Réponse du Pérou, note 1 *supra*, en 4 (où on cite l'article 11 des articles portant sur la responsabilité de l'État).

50 Réponse de la Bolivie, note 1 *supra*, en 3 à 7. La réponse de la Bolivie à la question sur les substituts est indirecte, même si elle indique l'existence d'un lien entre un État et les agents non étatiques liés aux objectifs ou aux stratégies de la politique de l'État en matière de défense dans une situation de conflit armé. Id.

51 Écrit présenté par les États-Unis au GEG en 2014, note 1 *supra*, en 738.

personne ou un groupe de personnes agissant conformément aux instructions ou au contrôle de cet État[52].

Toutefois, dans les articles portant sur la responsabilité de l'État, aucune opinion n'est formulée sur le degré de "contrôle" que l'État doit exercer; cette question doit être évaluée dans chaque cas[53]. Cela concorde avec l'opinion des États-Unis, qui approuvent la responsabilité de l'État pour les activités réalisées au moyen d'"agents substituts" qui agissent en suivant des instructions de l'État ou sous sa direction ou son contrôle, bien qu'ils affiment uniquement que le degré de contrôle exercé doit être "suffisant"[54]. Les États-Unis ont également reconnu qu'un État peut reconnaitre ou adopter à postériori une opération cybernétique d'un agent non étatique comme si elle était la sienne[55].

24. Le Chili, par contre, en exposant son point de vue sur le degré de contrôle nécessaire pour qu'il y ait responsabilité juridique, mentionne les causes de *Nicaragua* et du *Genocidio* et est d'avis que "le degré de contrôle ou de participation que doit avoir un État dans les opérations d'un acteur non étatique pour qu'il soit responsable sur le plan international ou la norme en ce domaine est le contrôle effectif"[56]. Il est également d'avis que les normes relatives à la responsabilité de l'État sont les mêmes dans le contexte des conflits armés[57].

25. En ce qui concerne le droit international humanitaire, le Pérou adopte une position similaire, qui favorise une règle uniforme quant à la responsabilité de l'État tant dans des conflits armés que dans d'autres contextes. Bien qu'il reconnaisse la possibilité que les articles sur la responsabilité de l'État soient remplacés par une *lex specialis,* il indique que pour ce faire il faut disposer d'une analyse exhaustive. Dans ce cas, "[d]e la révision des Conventions de Genève, aucune altération n'est décelée concernant les normes relatives à la responsabilité internationale contenues dans le Projet d'articles sur la responsabilité de l'État pour des faits illicites sur le plan international. Par conséquent, on ne peut y apporter de changements au domaine d'application de ce projet"[58]. Toutefois, dans la norme relative à la responsabilité énoncée dans les articles portant sur la responsabilité de l'État, il est fait référence au "contrôle" uniquement de façon générale, sans distinguer s'il doit être "effectif" ou "général".

26. D'autres États ont eu plus de difficulté à répondre à la question 5. Le Guatemala indique qu'il "est nécessaire de poursuivre les discussions dans des tribunes internationales sur les facettes uniques et différentes que présenterait un conflit dans le cyberespace, en particulier des facettes comme l'attribution et la territorialité des attaques"[59]. D'autres États ont compris que la question se référait aux différences dans les normes en matière de responsabilité dans les cas de conflits armés internationaux et sans caractère international[60].

---

52 Articles sur la responsabilité de l'État, note 41 *supra*, art. 8; réponse du Chili, note 1 *supra*, en 2; réponse du Guyana, note 1 *supra*, en 3; réponse du Pérou, note 1 *supra*, en 4. Les réponses du Chili et du Pérou semblent également se baser sur l'article 5 des articles portant sur la responsabilité de l'État, dans lequel l'État est responsable du "comportement d'une personne ou entité qui [...] aurait la faculté, de par le droit de cet État d'exercer des attributions du pouvoir public, à condition que dans le cas dont il s'agit, la personne ou l'entité agisse en cette capacité". Voir la réponse du Chili, note 1 *supra*, en 2, et la réponse du Pérou, note 1 *supra*, en 4.

53 Articles portant sur la responsabilité de l'État, note 41 *supra*, en 48 (commentaire sur l'article 8).

54 Koh, note 1 *supra*, en 595; écrit présenté par les États-Unis au GEG en 2014, note 1 *supra*, en 738 (idem); Egan, note 1 *supra*, en 821; écrit présenté par les États-Unis au GEG en 2016, note 1 *supra*, en 826.

55 Egan, nota 1 *supra*, en 821; écrit présenté par les États-Unis au GEG en 2016, note 1 *supra*, en 826.

56 Réponse du Chili, note 1 *supra*, en 2.

57 Id. en 3.

58 Réponse du Pérou, note 1 *supra*, en 4 et 5.

59 Réponse du Guatemala, note 1 *supra*, en 3.

60 Voir, par exemple, la réponse de la Bolivie, note 1 *supra*, en 4 à 7, et la réponse du Guyana, note 1 *supra*, en 3. Dans la réponse de l'Équateur, on souligne simplement que "les États sont les responsables de

Question 6 : Selon le droit international humanitaire, une opération cybernétique peut-elle être qualifiée d'"attaque" conformément aux normes qui régissent la conduite des hostilités si elle ne cause pas la mort, pas de lésions ni de dommages physiques directs au système informatique en question ou à l'infrastructure qu'il appuie? Une opération cybernétique produisant uniquement une perte de fonctionnalité, par exemple, pourrait-elle être qualifiée d'attaque? Si oui, dans quels cas?

27. La sixième question est la première de deux questions abordant la façon dont le droit international humanitaire (ou *jus in bello*) s'applique aux opérations cybernétiques. Elle porte principalement sur une question qui a divisé les États et les experts jusqu'à maintenant : comment définir une "attaque" aux effets du droit international humanitaire. Une grande partie de cette branche du droit, notamment ses principes fondamentaux de distinction, de proportionnalité et de précautions, est formulée en grande partie depuis le point de vue de l'interdiction de certains types d'"attaques" (par exemple, celles dirigées contre des civils ou des objectifs civils) et de l'autorisation d'autres types (par exemple, celles qui sont dirigées contre des objectifs militaires)[61]. Comme le CICR l'a indiqué récemment, la question de l'interprétation large ou stricte du concept d'"attaque" en ce qui concerne les opérations cybernétiques est essentielle pour l'applicabilité de ces normes et pour la protection qu'elles confèrent aux civils et à l'infrastructure civile[62]. En effet, dans la mesure où une opération ne constituerait *pas* une "attaque", elle pourrait se faire dans le cadre d'un conflit armé sans tenir compte de la plupart des normes du droit international humanitaire[63].

28. Conformément au droit international humanitaire, on entend par "attaques" en droit international coutumier (codifié dans l'article 49 du Protocole additionnel I aux Conventions de Genève) "les actes de violence contre l'adversaire, qu'ils soient offensifs ou défensifs"[64]. De même, comme l'explique le *Tallinn Manual 2.0*, "les conséquences, et non la nature de celle-ci, déterminent en général la portée du terme 'attaque'; la 'violence' doit être considérée dans le sens des conséquences violentes et ne se limite pas aux actes violents"[65]. Le CICR a indiqué que "l'idée que les opérations cybernétiques pour lesquelles on prévoit des morts, des lésions ou des dommages physiques constituent des attaques conformément au droit international humanitaire est généralement acceptée"[66]. Cependant, on sait bien que quelques opérations cybernétiques (par exemple le *ransomware* ou programme de capture illicite de fichiers en échange d'une ransom) sont nouvelles parce qu'elles peuvent perturber le fonctionnement d'objets sans y faire de dommages

---

respecter les normes dans les conflits armés, même quand il existe des parties qui ne sont pas parties à la Convention" correspondante. Réponse de l'Équateur, note 1 *supra*, en 2.

61 Par exemple, le principe de distinction se pose régulièrement comme l'interdiction que la population civile fasse l'objet d'une attaque. Voir, par exemple, le Protocole additionnel aux Conventions de Genève du 12 aout 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I) (8 juin 1977), 1125 UNTS 3, art. 5.2 ("Protocole additionnel I"); le Protocole additionnel aux Conventions de Genève du 12 aout 1949 relatif à la protection des victimes des conflits armés internationaux (12 décembre 1977), 1125 UNTS 609, art. 13.2; le Statut de Rome de la Cour pénale internationale (17 juillet 1998), art. 8.2.b.f; la Convention relative aux lois et coutumes de la guerre terrestre (H.IV) et son annexe : le Règlement relatif aux lois et coutumes de la guerre terrestre (18 octobre 1907), 36 Stat. 2277, art. 8.2.b.i-ii; Jean Marie Henckaerts et Louise Doswald-Beck, *Customary International Humanitarian Law* (CICR, 2005), règles 1, 7, 9 et 10.

62 CICR, *Document de position sur Droit international humanitaire et cyberopérations pendant des conflits armés* (novembre 2019) en 7 ("Document de position du CICR").

63 Même en l'absence d'attaques, les États doivent agir avec un "soin constant" dans un conflit armé international afin de "préserver la population civile [...] et les biens à caractère civil". Protocole additionnel I, note 61 *supra*, art. 57.1; *Tallinn 2.0,* note 20 *supra*, en 476.

64 Protocole additionnel I, note 61 *supra*, art. 49.

65 *Tallinn 2.0*, note 20 supra en 415.

66 Voir le Document de position du CICR, note 62.

physiques[67]. Cela mène à la question de si les opérations cybernétiques qui ne produisent pas d'effets de ce type (par exemple l'interruption du fonctionnement d'une usine de purification d'eau sans causer nécessairement de dommages physiques) peuvent constituer une attaque. Des opinions divergentes ont été émises jusqu'à maintenant, même entre les membres du groupe indépendant d'experts qui a élaboré le *Tallinn Manual 2.0*[68].

29. La majorité des auteurs du *Tallinn Manual 2.0* sont d'avis que pour qu'il y ait violence, il doit y avoir des dommages physiques qui requièrent, par exemple, le "remplacement de composantes physiques" telles qu'un système de contrôle[69]. D'autres estiment que les dommages comprennent les cas dans lesquels il ne serait pas nécessaire de remplacer des composantes physiques et le fonctionnement pourrait être rétabli en réinstallant le système d'opération, tandis que quelques experts peu nombreux considèrent qu'une attaque pourrait consister en la "perte d'aptitude pour l'utilisation de l'infrastructure cybernétique" en soi[70]. Le CICR, quant à lui, a argumenté que dans un conflit armé, une opération visant à mettre hors service un ordinateur ou un réseau informatique constitue une attaque conformément au droit international humanitaire, indépendamment de si l'objet est mis hors service par des moyens cinétiques ou cybernétiques[71].

30. Par conséquent, la sixième question avait pour but de déterminer si les États membres considèrent aussi le seuil pour une attaque dans le contexte du droit international humanitaire en termes de violence (ou d'effets violents) ou s'ils estiment que la catégorie "attaque" pourrait s'appliquer aux opérations cybernétiques sur la base de la perte de fonctionnalité, au lieu des concepts plus traditionnels de dommages physiques ou de destruction.

31. Les réponses au questionnaires reflètent un soutien à l'applicabilité du droit international humanitaire en général et à l'idée que les opérations cybernétiques peuvent constituer une attaque dans ce contexte[72]. Cependant, il y a plus de variété dans les réponses à la question de si une opération cybernétique peut être qualifiée d'"attaque" conformément au droit international humanitaire si elle ne cause pas de morts, de lésions ou de dommages physiques directs. Le Chili, le Pérou et les États-Unis ont répondu que non[73]. Le Chili cite l'article 49 du Protocole additionnel I aux Conventions de Genève en insistant que les attaques dans le contexte du droit international humanitaire doivent impliquer "des effets ou conséquences causés par l'acte comme tel, lesquels doivent être violents"[74]. En particulier, il indique que pour que l'acte puisse être considéré comme

---

67 CICR, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* (octobre 2015) 41 ("Rapport 2015 du CICR").

68 *Tallinn 2.0*, note 20 supra en 417.

69 *Id.*

70 Rapport du CICR de 2015, note 67 *supra*, en 41. Voir aussi CICR, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (novembre 2019), en 28 ("Rapport du CICR de 2019") ("Les normes du DIH qui protègent les objets civils peuvent toutefois accorder toute la portée de la protection juridique seulement si les États reconnaissent que les opérations cybernétiques qui affectent la fonctionnalité de l'infrastructure civile sont sujettes aux normes qui réglementent les attaques en vertu du DIH ".)

71 Voir le Document de position du CICR, note 62 *supra*, en 7-8, et le Rapport du CICR de 2015, note 67 *supra*, en 43 (où on affirme que le droit international doit traiter comme des attaques les opérations cybernétiques qui désactivent des objets, étant donné que la définition d'objectif militaire comprend la neutralisation, d'où on déduit que la neutralisation d'objets est comprise dans le domaine du droit international humanitaire).

72 Voir, par exemple, la réponse de la Bolivie, note 1 *supra*, en 3 à 7; id. en 4 à 7 (où on mentionne deux points de vue concernant si une opération cybernétique peut donner lieu par elle-même à un conflit armé sujet au droit international humanitaire); la réponse du Chili, note 1 *supra*, en 3; la réponse du Guyana, note 1 *supra*, en 3; la réponse du Pérou, note 1 *supra*, en 1; Koh, note 1 *supra*, en 595 (opinion des États-Unis).

73 Réponse du Guyana, note 1 *supra*, en 4.

74 Réponse du Chili, note 1 *supra*, en 3.

une attaque, son résultat doit exiger que "l'État touché doit prendre des mesures destinées à réparer ou à récupérer l'infrastructure ou le système informatique touché, étant donné que dans ces cas les conséquences de l'attaque sont similaires à celles décrites ci-dessus, en particulier les dommages physiques à la propriété"[75]. Le Pérou répond que pour qu'il y ait une "attaque", des "dommages physiques" doivent être causés à des "personnes" ou à des "biens publics ou privés"[76]. Les États-Uni, quant à eux, ont souligné que le seuil pour une "attaque" dans le contexte du droit international humanitaire il faut établir, notamment, si une activité cybernétique produit des effets cinétiques irréversibles ou des effets non cinétiques réversibles sur la population civile, sur des objectifs à caractère civil ou sur l'infrastructure civile[77]. Cela implique que si une opération cybernétique produit des effets non cinétiques ou réversible, elle ne constitue pas une attaque armée[78], ce qui semblerait exclure, par exemple, les programmes intrus de rançongiciels (*ransomware*) qui ne seraient pas cinétiques en eux-mêmes ou les cas dans lesquels les données interrompues pourraient être rétablies.

32. Par contre, le Guatemala et l'Équateur appuient l'idée de délimiter les attaques sur la base des pertes de fonctionnalité, plutôt que des morts, des lésions ou de la destruction de biens qu'elles pourraient causer. Le Guatemala indique qu'au nombre des opérations cybernétiques qui peuvent être considérées comme une attaque, se trouvent celles "qui produisent uniquement une perte de fonctionnalité"[79]. L'Équateur est d'avis que "[u]ne opération cybernétique peut être considérée comme une attaque si elle laisse sans fonctionnalité l'infrastructure essentielle de l'État ou autre chose qui mette en danger la sécurité de l'État"[80].

33. Les réponses de la Bolivie et du Guyana sont plus ambiguës. D'une part, la Bolivie affirme que la définition d'attaques selon le droit international humanitaire comprendrait une opération cybernétique "de laquelle on s'attend à ce qu'elle puisse causer des pertes de vies humaines, des lésions aux personnes et des dommages aux biens ou leur destruction"[81]. D'autre part, ce pays dit qu'une opération cybernétique "pourrait être considérée comme une attaque quand elle a pour objectif de rendre inutilisables les services de base (eau, électricité, télécommunications ou le secteur financier) d'un État"[82]. Le Guyana observe que quand une opéfation cybernétique produit une perte de fonctionnalité, elle peut ou non constituer une attaque[83]. Tout comme le Chili, il fait référence à l'article 49 du Protocole additionnel I et relie le concept d'attaque à la nécessité qu'il y ait violence (pour ce qui a trait aux moyens ou aux conséquences) : "une opération cybernétique qui ne cause pas de morts, de lésions ou de dommages physiques ne peut pas constituer une attaque" conformément au droit international humanitaire[84]. Par ailleurs, ce pays indique que "les opérations cybernétiques qui minent le fonctionnement des systèmes et de l'infrastructure informatiques nécessaires à la fourniture de services et de ressources à la population civile constituent une attaque". Au nombre de ceux-ci, on compte "les centrales nucléaires, les

---

75 Id.

76 Cependant, la réponse du Pérou est un peu ambiguë, car elle semble être basée sur des éléments du *jus ad bellum* pour indiquer les normes applicables à une attaque dans le contexte du droit international humanitaire et mentionne l'approche contextuelle des États-Unis pour laquelle Harold Koh exprime sa préférence. La réponse du Pérou, note 1 *supra*, en 6.

77 Écrit présenté par les États-Unis au GEG en 2014, note 1 *supra*, en 736.

78 Egan, note 1 *supra*, en 818. Egan n'a pas mentionné dans son discours le critère de dommages réversibles ou irréversibles, mais il a souligné, par contre, "la nature et la portée de ces effets, de même que la nature de la relation, si elle existe, entre l'activité cybernétique et le conflit armé particulier en question". Id.

79 Réponse du Guatemala, note 1 *supra*, en 3.

80 Réponse de l'Équateur, note 1 *supra*, en 3.

81 Réponse de la Bolivie, note 1 *supra*, en 4 à 7.

82 Id.

83 Réponse du Guyana, note 1*supra*, en 3.

84 Id.

hôpitaux, les banques et les systèmes de contrôle de la circuation aérienne"[85]. Ces réponses semblent indiquer la nécessité d'approfondir le dialogue sur à quel point la mort ou la destruction doivent être immédiates après la perte de fonctionnalité. En d'autres mots, la perte de fonctionnalité d'un service essentiel constitue-t-elle en elle-même une attaque, ou s'il doit y avoir des morts, des lésions ou des dommages matériels concommitants (ou raisonnablement prévisibles) ?

Question 7 : Une opération cybernétique qui attaque seulement des données serait-elle réglementée par l'obligation, dans le droit international humanitaire, de diriger des attaques seulement contre des objectfs militaires et non contre des objectifs civils ?

34. Le droit international humanitaire requient clairement que les États "attaquants" fassent une distinction entre objectifs civils et militaires et permet les attaques contre des objectifs militaires, mais interdit les attaques contre la population civile et les objectifs à caractère civil[86]. Toutefois, quand il s'agit du cyberespace, il n'est pas toujours clair de savoir ce qui constitue un "objectif" auquel s'applique ce principe. La discussion fondamentale a porté principalement sur les "données." Cela veut-il dire que les "données", étant donné leur nature non physique, ne constituent pas un objectif et que par conséquent, les militaires n'ont pas besoin de faire une distinction et les exclure de leurs opérations cybernétiques ? Ou au moins quelques "données" devraient-elles être considérées comme un "objectif" auquel s'applique le principe de la distinction et les normes pertinentes du droit international humanitaire ?

35. La majorité des experts du groupe indépendant qui a rédigé le *Tallinn Manual 2.0* ont adopté la première position : "il ne faut pas comprendre que le concept d''objectif' dans le conflit armé comprend les données, du moins dans le droit actuel"[87]. Les experts s'entendent toutefois pour dire qu'une opération cybernétique dirigée contre des données pourrait entrainer l'application des normes du droit international humanitaire dans les cas où "on pourrait prévoir qu'elle occasionne des lésions, des morts, des dommages matériels ou la destruction d'objets physiques", étant donné que les personnes et les objets touchés seraient protégés par les règles pertinentes du droit international humanitaire, comme celles qui ont trait à la distinction[88]. Par contre, le CICR a proposé une définition plus large de données avec l'expression "données civiles essentielles" (par exemple les données médicales, biométriques et de sécurité sociale, les dossiers des impôts, les comptes bancaires, les dossiers de clients de compagnies, les listes des électeurs et les registres électoraux). Il a indiqué qu'"effacer ou altérer de façon frauduleuse des données civiles essentielles peut occasionner plus de dommages à la population civile que la destruction d'objets physiques"[89].

---

85 Id. (où on cite l'article 54.2 du Protocole additionnel I

86 Quand un objet particulier est utilisé à des fins civiles et militaires (les objets dénommés "objets à double usage"), il devient un objectif militaire (sauf les parties qui peuvent se séparer). Voir les sources dans lesquelles ce principe de "distinction" est codifié dans la note 61 *supra*.

87 *Tallinn 2.0*, note 20 *supra*, en 437.

88 Id. en 416.

89 CICR, Document de position, note 62 *supra*, en 8 ; Rapport du CICR de 2019, note 71 *supra*, en 21 (En outre, les données se sont converties en une composante essentielle du domaine numérique et en une pierre angulaire de la vie dans de nombreuses sociétés. Cependant, il existe divers points de vue concernant la question à savoir si les données civiles doivent être considérées comme des objets civils et, par conséquent, si elles doivent être protégées selon les principes et les normes du droit international humanitaire qui régissent la conduite des hostilités. Le CICR est d'avis que la conclusion voulant que ce type d'opération ne serait pas interdit par le droit international humanitaire dans le monde d'aujourd'hui, de plus en plus dépendant du domaine cybernétique, soit parce qu'éliminer ou modifier ces données ne constituerait pas une attaqueau sens du droit international humanitaire, soit parce que ces données ne seraient pas considérées comme des objets auxquels s'appliquerait l'interdiction d'attaques contre des biens à caractère civil, cela semble difficile de concilier avec l'obectif et le but de cet ordre juridique. En peu de mots, le remplacement d'archives sur consistant en papiers et documents par des archives

Bien que le CICR reconnait que la question de si les données peuvent constituer un objectif civil n'est pas encore réglée, il a indiqué qu'elle devrait être résolue dans le domaine du droit international humanitaire. Autrement, il y aura un large "fossé dans la protection" qui est incompatible avec l'objet et le but du droit international humanitaire. La septième question visait à recueillir l'opinion des États membres sur cette question importante.

36. Aucun des États qui ont répondu à cette question n'a adopté la position selon laquelle les données civiles seraiet sujettes directeent au principe de distinction dans le conflit armé. En fait, plusieurs États mentionnent le principe de distinction sans formuler d'opinion sur la condition des données en tant qu'objet[90]. Cependant, la réponse du Chili semble indiquer que le principe de distinction pourrait s'appliquer aux opérations cybernétiques visant indirectement des données sur la base de leurs répercussions. Il cite le commentaire contenu dans le Protocole additionnel I selon lequel un objet doit être "visible et tangible", ce qui signifie qu'"aux fins du droit international humanitaire en vigueur, les données mentionnées ne se qualifieraient pas comme objets, en principe, parce qu'elles sont essentiellement intangibes, sans préjudice des éléments physiques dans lesquels les données sont contenues, par exemple le matériel"[91]. En même temps, le Chili indique qu'"une attaque dirigée exclusivement contre des données informatiques pourrait parfaitement entrainer des conséquences adverses qui affecteraient la population civile". Il donne pour exemple la possibilité d'une opération cybernétique qui éliminerait la base de données relatives à la sécurité sociale d'un État[92] et conclut qu'"il faut tenir compte du principe de distinction dans le contexte des opérations cybernétiques; pour cette raison, un État devrait s'abstenir d'attaquer des données au cas où cela pourrait affecter la population civile, à moins que ces donnéesne soient utilisées à des fins militaires"[93]. Le Guyana répond selon une optique similaire. Après avoir indiqué qu'effacer, supprimer ou corrompre des données pourrait avoir des conséquences d'une grande portée, il fait porter son attention sur les effets de l'opération cybernétique, au lieu d'aborder la question de si les données qui seraient l'objectif de l'attaque peuvent être considérées comme un objet ou non[94].

37. Dans sa réponse, le Pérou n'aborde pas la possibilité que les données puissent être considérées comme un objectif civil, mais il fait porter son attention (affirmativement) sur la possibilité qu'elles puissent être considérées comme un objectif militaire. Il indique que certaines "données" (par exemple "un logiciel qui permette la communication entre les troupes d'une armée en campagne ou qui synchronise l'arsenal de missiles d'un pays ou aide à localiser un aéronef ennemi") sont des objectifs militaires légitimes, tandis que d'autres systèmes de données utilisés dans des conflits (par exemple "un système de données permettant le fonctionnement de la salle d'opérations d'un hôpital de campagne dans lequel sont soignés des blessés de guerre ou la population civile") ne peuvent pas être la cible d'attaques[95].

38. Plusieurs commentaires présentés par des États membres au Groupe de travail à composition non limitée ont affirmé l'importance d'appliquer le droit international humanitaire au contexte cybernétique. Quelques États, comme le Brésil, ont souligné, en outre, que cette

---

numériques sous forme de données ne devrait pas réduire la protection que le droit international humanitaire leur accorde") ; Rapport du CICR en 2015, note 67 *supra*, en 43.

90 Voir la réponse de la Bolivie, note 1 *supra*, en 5 à 7 ; la réponse de l'Équateur, note 1 *supra*, en 2, et la réponse du Guatemala, note 1 *supra*, en 3.

91 Réponse du Chili, note 1 *supra*, en 4.

92 Id.

93 Id.

94 Réponse du Guyana, note 1 *supra*, en 4 (où on dit qu'en ce qui a trait aux données, il faut tenir compte de si l'opération cybernétique dirigée contre les données a produit une perte de fonctionnalité telle que cela pourrait constituer une attaque).

95 Réponse du Pérou, note 1 *supra*, en 6. Le Pérou explique que dans le premier cas, les attaques causeraient "undommage militaire important aux forces de la contrepartie", tandis qu'une attaque contre les données dans l'hôpital de campagne "n'entrainerait pas un avantage militaire légitime". Id.

application doit inclure expressément les principes fondamentaux d'"humanité, besoin, proportionnalité et distinction". [96] Toutefois, aucune des contributions apportées au Groupe de travail à composition non limitée n'a abordé la définition d'une attaque ni l'idée des données en tant qu'objectif civil (ou militaire).

Question 8 : La souveraineté est-elle une norme discrète du droit international qui interdirait aux États de participer à des opérations cybernétiques spécifiques? Si c'est le cas, cette interdiction couvre-t-elle les opérations cybernétiques qui se trouvent sous le seuil de l'utilisation de la force et qui, en outre, ne violent pas le principe de non-intervention?

39. La souveraineté est sans aucun doute la caractéristique structurelle de base de l'ordre juridique international actuel, qui assigne des droits et des responsabilités aux États[97]. C'est un principe fondamental de certaines des normes juridiques internationales mentionnées (par exemple, l'interdiction de l'utilisation de la force, le droit de légitime défense, la responsabilité de l'État). Aussi, dans certains contextes, la souveraineté existe non seulement en tant que principe de base, mais en tant que norme indépendante qui réglemente le comportement de l'État (par exemple, un aéronef qui pénètre dans l'espace aérien d'un autre État sans autorisation viole sa souveraineté)[98]. Cependant, il n'est pas encore clair si la souveraineté est une norme dans le cyberespace. Dans le *Tallinn Manual 2.0* on indique que c'est une règle qui limite les opérations cybernétiques d'un État qui ne donnent pas lieu à l'utilisation de la force et ne constituent pas non plus une intervention interdite[99]. Toutefois, en 2018, le Procureur général du Royaume-Uni a émis l'opinion selon laquelle la souveraineté n'était pas une norme de droit international en soi, mais un principe qui servait de base à d'autres normes[100]. Par la suite, le Ministère de la défense de la France et le

96 Commentaires du Brésil, *supra,* note 5

97 *Island of Palmas (Netherlands v. United States of America)*, 2 R.I.A.A. 829, 839 (1928) ("La souveraineté dans les relations entre les États signifie indépendance. L'indépendance par rapport à la portion du monde qu'ils occupent est le droit d'exercer, à l'intérieur de cette zone, à l'exclusion de tout autre État, les fonctions d'un État [...]. La souveraineté territoriale, comme on l'a déjà dit, implique le droit exclusif d'effectuer les activités propres à un État. Ce droit a comme corollaire un devoir : l'obligation de protéger, à l'intérieur du territoire, les droits d'autres États, en particulier leur droit à l'intégrité et à l'inviolabilité en temps de paix et de guerre" [traduction en espagnol du CJI]).

98 Voir, par exemple, Michael N. Schmitt et Liis Vihul, *Respect for Sovereignty in Cyberspace,* 95 dans *Texas L. Rev.* 1639, 1640 (2017). Outre l'interdiction de l'utilisation de la force énoncée à l'article 2.4, il existe en droit international un accord général sur le devoir de non-intervention qui s'applique au cyberespace. Voir, par exemple, *Case Concerning Armed Activities in the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (juridiction et admissibilité) [2006] ICJ Rep. 6, [46]-[48]; *Nicaragua Case*, note 23 *supra*, par. 205; Résolution 2625 (XXV) de l'Assemblée générale des Nations Unies, du 24 octobre 1970, qui contient la Déclaration relative aux principes du droit international, lesquels se réfèrent aux relations d'amitié et à la coopération entre les États conformément à la Charte des Nations Unies. Le GEG de 2015 a approuvé ce principe au sein des normes du droit international qui s'appliquent au cyberespace. Voir Secrétaire général des Nations Unies, Rapport du *Groupe d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationnale*, U.N. Doc. A/70/174 (22 juillet 2015) par. 26 et 28.*b*. La règle 66 du manuel *Tallinn 2.0* énonce qu'"un État ne peut pas intervenir, y compris par des moyens cybernétiques, dans les questions internes ou externes d'un autre État". *Tallinn 2.0,* note 20 *supra*, en 312 (traduction en espagnol du CJI). Cependant, à l'instar de ce qui arrive avec l'utilisation de la force, des questions continuent de se poser à savoir si ce devoir existe dans l'espace cybernétique et quelles opérations cybernétiques il interdit ou règlemente.

99 *Tallinn 2.0,* note 20 *supra*, règle 4 ("Un État ne doit pas faire d'opérations cybernétiques qui violent la souveraineté d'un autre État" [traduction en espagnol du CJI]).

100 Voir, par exemple, Jeremy Wright, QC, MP. *Cyber and International Law in the 21st Century* (23 mai 2018) à https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century ("les

Gouvernement de la Hollande ont exprimé leur soutien à la souveraineté à titre de norme autonome[101].

40. La huitième question avait pour but de recueillir les opinions des États membres sur la question de la souveraineté en tant que principe en contraposition à la souveraineté en tant que norme. La question porte principalement sur la fonction limitante de la souveraineté, c'est-à-dire si elle limite la capacité d'un État d'effectuer des opérations cybernétiques à l'extérieur de son territoire et de quelle façon. Ce qui est intéressant est que bon nombre des États qui ont répondu ont pris la question comme une invitationà réaffirmer la fonction habilitatrice de la souveraineté; par exemple, en accord avec l'autorité de l'État pour réglementer les TIC à l'intérieur de leur propre juridiction territoriale. La Bolivie et le Guyana disent que la souveraineté autorise les États à exercer leur juridiction sur l'infrastructure ou sur les activités cybernétiques dans leur territoire[102]. L'Équateur, par contre, émet des doutes sur la capacité des États d'exercer leur souveraineté dans le cyberespace étant donné son "intangibilité" et, en même temps, affirme que les États ont souveraineté sur l'"infrastructure cybernétique" ainsi que sur les activités liées à cette infrastructure sur leur territoire[103]. Le Chili et les États-Unis se font également écho du pouvoir que la souveraineté confère aux États sur les TIC sur leur territoire, mais observent que ce pouvoir doit agir à l'intérieur de certaines limites. Les deux pays mentionnent qu'il faut que les États exercent la

---

opinions du Royaume-Uni"). ("Certains ont essayé de démontrer l'existence d'une norme orientée spécifiquement vers l'espace cybernétique qui s'applique à la 'violation de la souveraineté territorielle' [...]. Évidemment, la souveraineté est fondamentale pour le système international basé sur des normes, mais je ne suis pas convaincu que nous puissions dans les faits extrapoler à partir de ce principe général une norme spécifique ou une interdiction d'activités cybernétiques en plus d'une intervention interdite. Par conséquent, la position du Gouvernement du Royaume-Uni est qu'il n'y a pas une norme de ce type dans le droit international actuel".

101 Voir Ministère des Armées, *Droit international appliqué aux opérations dans le cyberespace* (9 septembre 2019), dans : https://www.defense.gouv.fr/salle-de-presse/communiques/communiques-du-ministere-des-armees/communique_la-france-s-engage-a-promouvoir-un-cyberespace-stable-fonde-sur-la-confiance-et-le-respect-du-droit-international ("Opinion fu Ministère de la défense de la France") en 6 ("Toute pénétration non autorisée de systèmes français par un État ou tout acte qui prendrait effet sur le territoire français au moyen d'un vecteur numérique pourrait constituer, à tout le moins, une violation de la souveraineté" [traduction en anglais du Rapporteur]); *Letter to the parliament on the international legal order in cyberspace,* 5 juillet 2019, appendice 1 à https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace ("Opinion des Pays-Bas") ("Selon certains pays et certains juristes, le principe de souveraineté ne constitue pas une norme indépendamment contraignante du droit international qui la sépare des autres normes dérivées de celui-ci. Les Pays-Bas ne sont pas d'accord avec ce point de vue, étant donné qu'ils croient que le respect de la souveraineté d'autres pays est une obligation en elle-même, dont la violation pourrait par ailleurs constituer un acte illicite sur le plan international" [traduction en espagnol du CJI]). Dans une analyse universitaire récente, on se demande si la France s'inscrit clairement dans le camp de la souveraineté en tant que norme. Voir Gary Corn, *Punching on the Edges of the Gray Zone: Iranian Cyber Threats and State Cyber Responses,* JUST SECURITY (11 février 2020) ("bien que le Ministère de la défense affirme que les cyberattaqes, telles qu'elle définit ce terme, contre des systèmes numériques français ou tout effet produit en territoire français par des moyens numériques pourraient constituer une violation de la souveraineté en général, en aucun moment elle ne dit sans aucun doute qu'une violation du principe de souveraineté constitue un non-respect d'une obligation internationale. Au contraire, les auteurs du document, de toute évidence conscients du débat, restent délibérément vagues à cet égard et réaffirment simplement le droit de la France à répondre aux cyberattaques avec la gamme complète d'options qu'elle a à sa portée en accord avec le droit international")

102 Réponse de la Bolivie, note 1 *supra*, en 5 à 7; réponse du Guyana, note 1 *supra*, en 5.

103 Réponse de l'Équateur, note 1 *supra*, en 2.

souveraineté conformément au droit international des droits de la personne[104]. La Colombie a appuyé ce dernier point dans ses commentaires au Groupe de travail à composition non limitée.[105]

41. En ce qui concerne la question de savoir si la souveraineté fonctionne comme une norme autonome dans le cyberespace, trois États —la Bolivie, le Guatemala et le Guyana— ont répondu que oui[106]. Le Guyana, par exemple, affirme que les protections de la souveraineté "ne se limitent pas aux activités qui constituent une utilisation injustifiée de la force, une attaque armée ou une intervention interdite"[107]. Il est d'accord que l'État "ne doit pas effectuer d'opérations cybernétiques qui violent la souveraineté d'un autre État", et l'existence d'une violation de ce type dépend "de la gravité de l'infraction et de s'il y a eu interférence dans les fonctions deu gouvernement"[108]. Le Guatemala adopte une position similaire et indique qu'"un État qui participe à des opérations cybernétiques spécifiques viole la souveraineté d'un pays si au moment d'effectuer une attaque cybernétique certains renseignements sont captés dans le cyberenvironnement d'un autre État, même si cela ne cause aucun dommage qui ait des répercussions sur du matériel ou sur les droits humains d'une ou de plusieurs personnes"[109].

42. Les réponses d'autres États sont assez ambiguës. Le Pérou dit simplement que la souveraineté "est l'un des piliers fondamentaux de la société internationale", sans exposer d'opinion sur sa condition de norme indépendante[110]. L'Équateur indique que la "norme" qui autorise les États à contrôler leur propre infrastructure cybernétique "ne défend pas à un État [...] de participer à des opérations cybernétiques", mais il ne présente pas d'opinion sur s'il serait possible de réglementer la façon dont il le fait par rapport à d'autres États souverains[111].

43. Dans sa réponse, le Chili décrit la souveraineté commu un principe dont "[l]es États qui effectuent des opérations cybernétiques doivent toujours tenir compte"[112]. Par conséquent, "chaque fois qu'un État envisage d'effectuer une opération cybernétique, il doit prendre en considération le fait qu'il ne doit pas affecter la souveraineté d'un autre État"[113]. La référence à un "principe" orienteur peut suggérer quelque chose de différent d'une règle concrète, bien que l'utilisation du verbe "doivent" crée des attentes d'un caractère plus obligatoire. Par ailleurs, le Chili affirme ce qui suit :

> chaque État est obligé de respecter l'intégrité territoriale et l'indépendance politique d'autres États et doit remplir fidèlement ses obligations internationales, y compris le principe de non-intervention. Par conséquent, les opérations cybernétiques

104 Réponse du Chili, note 1 *supra*, en 4 et 5 (où il reconnait que la souveraineté autorise l'Étatà protéger et à défendre "son infrastructure essentielle de l'information, [...] à condition que ces mesures n'aillent pas à l'encontre d'une norme de droit international, par exemple celles qui sont présentes dans le droit international des droits de la personne ou dans le droit international humanitaire"); écrit présenté par les États-Unis au GEG en 2014, note 1 *supra*, en 737 à 738 (où on indique que l'exercice de la juridiction d'un État territorial n'est pas illimité, mais qu'il doit concorder avec le droit international applicable, y compris les obligations internationales en matière de droits de la personne, et on mentionnent en particulier la liberté d'expression et la liberté d'opinion).

105 Commentaires de la Colombie, note 5 *supra.*

106 Réponse de la Bolivie, note 1 *supra*, en 5 à 7; réponse du Guatemala, note 1 *supra*, en 3; réponse du Guyana, note 1 *supra*, en 5.

107 Rponse du Guyana, note 23 *supra*, en 5

108 Id.

109 Réponse du Guatemala, note 1 *supra*, en 3.

110 Réponse du Pérou, note 1 *supra*, en 6 et 7.

111 Réponse de l'Équateur, note 1 *supra*, en 2.

112 Réponse du Chili, note 1 *supra*, en 5.

113 Id.

qui empêchent l'exercice de la souveraineté par un autre État constituent une violation de cette souveraineté et sont interdites par le droit international[114].

La dernière phrase semble indiquer que la souveraineté pourrait constituer une norme autonome sauf si la référence à l'intervention dans l'exercice de la souveraineté d'un autre État s'entend comme l'équivalent du *domaine reservé* protégé par le devoir de non-intervention[115].

44. La position des États-Unis est moins claire encore. En 2014, Harold Koh, à l'époque Conseiller juridique, a affirmé que "la souveraineté de l'État [...] doit être prise en compte dans la réalisation d'activités dans le cyberespace, y compris hors du contexte du conflit armé"[116]. Il n'est toutefois pas clair si tenir compte de la souveraineté de l'État indique la reconnaissance par les États-Unis de la souveraineté en tant que norme autonome. Dans son discours de 2016, Brian Egan, à l'époque Conseiller juridique, a précisé que "les opérations cybernétiques réalisées à distance au moyen d'ordinateurs ou d'autres dispositifs en réseau situés sur le territoire d'un autre État ne constituent pas en elles-mêmes une violation du droit international"[117]. En même temps, Il a admis que "dans certaines circonstances, les opérations cybernétiques non consensuelles d'un État dans le territoire d'un autre pourraient violer le droit international, même si elles n'atteignent pas le seuil pour l'utilisation de la force". De toute façon, M. Egan a indiqué que "le moment précis où une opération cybernétique non consensuelle viole la souveraineté d'un autre État est une question que les avocats du Gouvernement des États-Unis continuent d'évaluer minutieusement et, en dernière instance, qui sera résolue par la pratique et par l'*opinio juris*"[118]. Toutefois, plus récemment, le Conseiller juridique du Département de la défense des États-Unis a indiqué qu'"en ce qui concerne les opérations cybernétiques qui ne constitueraient pas une intervention interdite ou une utilisation de la force [c'est-à-dire celles qui pourraient être couvertes par une règle de souveraineté], le Département est d'avis qu'il n'exixte pas une pratique étatique suffisamment étendue et consistante résultant d'un sentiment d'obligation juridique de conclure que le droit international coutumier interdit en général de telles opérations cybernétiques non consensuelles dans le territoire d'un autre État[119].

45. Dans une discussion entre 16 représentants d'États membres tenue conformément aux "Règles de Chatham House" [120] le 23 juin 2020, la diversité actuelle d'opinions sur la question de la souveraineté s'est renforcée. Plusieurs participants ont demandé que l'on déclare l'opinion voulant que la souveraineté soit considérée comme une norme pour le cyberespace, ce qui entrainerait que la violation de cette norme impliquerait une responsabilité juridique internationale. D'autres, toutefois, ont fait part d'un scepticisme plus important en ce qui concerne la valeur de ce travail; un

---

114 Id.

115 Voir la note 99.

116 Koh, note 1 *supra*, en 596 (traduction en espagnol du CJI); écrit présenté par les États-Unis au GEG en 2014, note 1 *supra*, en 737; écrit présenté par les États-Unis au GEG en 2016, note 1 *supra*, en 825.

117 Egan, *supra* note 1, en 818 (traduction en espagnol du CJI). Entre autres, M. Egan a dit que les États-Unis recueillait des renseignements à l'extérieur du pays et que ces activités pourraient violer les lois internes d'autres États, mais qu'elles n'étaient pas interdites en elles-mêmes dans le droit international coutumier. Id.

118 Id. en 819

119 *Voir* Paul C. Ney, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, 2 mars 2020, dans https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/?dod-general-counsel-remarks-at-us-cyber-command-legal-conference. Toutefois, il n'est pas clair si M. Ney exprimait l'opinion des États-Unis dans leur ensemble ou s'il s'agissait seulement de la position de militaires américains, ambigüité qui existe également en ce qui concerne les opinions du Ministère de la Défense de la France. Voir la note 101 *supra*.

120 Chatham House, *La Règle de Chatham House:* https://www.chathamhouse.org/chatham-house-rule (Quand une réunion, ou une partie de la réunion, est convoquée selon la Règle de Chatham House, les participants ont le droit d'utiliser l'information qu'ils reçoivent, mais ne peuvent pas révéler l'identité ni l'affiliation de l'orateur, ni d'aucun autre participant).

participant a suggéré qu'il pourrait exister plusieurs sens au mot "souveraineté" pour lui attribuer le rang de règle. Un autre participant a estimé que "la discussion sur la souveraineté est une distraction", et un troisième participant a suggéré explicitement qu'il fallait réexaminer le sens de ce mot dans le contexte cybernétique.

Question 9 : La diligence appropriée est-elle une norme de droit international que les États doivent respecter dans l'exercice de leur souveraineté sur les technologies de l'information et de la communication sur leur territoire ou est-elle sous le contrôle des ressortissants de l'État?

46. La diligence appropriée est un principe de droit international selon lequel un État doit répondre aux activités dont il sait (ou il devrait raisonnablement savoir) qu'elles ont leur origine sur son territoire ou dans d'autres zones dont il a le contrôle et qui violent les droits d'un autre État[121]. C'est une obligation d'efforts et non de résultat : dans les cas où un État aurait connaissance de la conduite ou devrait la connaitre, il doit utiliser "tous les moyens qui sont raisonnablement à sa portée" pour la corriger[122]. En tant que principe, la diligence appropriée régit actuellemet le comportement de l'État dans divers contextes, en particulier dans le droit environnemental international, où il constitue la base de l'exigence que les États freinent sur leur territoire la pollution qui serait une source de dommages transfrontaliers pour le territoire d'autres États.

47. Tout comme dans le cas de la souveraineté, des opinions contraires existent concernant si la diligence appropriée est une exigence du droit international dans le cyberespace. Dans le rapport du GEG de 2015 elle est mentionnée au nombre des normes "volontaires" du comportement responsable des États, au lieu de l'inclure dans les principes applicables du droit international[123]. Les ministères de la Défense des Pays-Bas et de la France l'ont décrite comme une norme juridique qui s'applique au cyberespace[124]. Toutefois, les Pays-Bas observent que tous les pays ne sont pas d'accord pour dire que le principe de la diligence appropriée constitue une obligation en soi dans le cadre du droit international, et on croit que les États-Unis sont l'un des pays qui remettent en

---

121 *Voir*, par exemple, *Corfu Channel Case; Assessment of Compensation (United Kingdom v. Albania)* [1949] ICJ Rep., par. 22 (9 avril); *Trail Smelter Case (United States-Canada)*, UNRIAA, vol. III, 1905 (1938, 1941).

122 Voir *Application of the Convention on the Protection and Punishment of the Crime of Genocide (Bosnia v. Serbia)* (jugement) [2007] ICJ Rep. 1, par. 430.

123 GEG de 2015, note 1 *supra*, par. 13 et 26 à 28.

124 Opinion du Ministère de la défense de la France, note 101 *supra*, en 10 ("En accord avec l'obligation d'agir avec la diligence appropriée, les États doivent assurer que leur domaine souverain dans le cyberespace ne soit pas utilisé pour commettre des actes illicites sur le plan international. Si un État ne respecte pas cette obligation, cela n'est pas une raison de faire une exception à l'interdiction de l'utilisation de la force, contrairement à l'opinion de la plupart des membres du groupes d'experts qui ont rédigé le Manuel de Tallinn"; opinion des Pays-Bas, note 101 *supra*, appendice, en 4 ("le principe de la diligence appropriée nécessite que les États prennent des mesures relativement aux activités cybernétiques réalisées par des personnes sur leur territoire ou pour lesquelles des réseaux qui se trouvent sur leur territoire ou sous leur contrôle sont utilisés, lesquels violent un droit d'un autre État et dont les États ont connaissance ou devraient avoir connaissance" [traduction en espagnol du CJI]). Bien qu'elle ne décrive pas la diligence appropriée comme étqant une norme spécifique du droit international, l'Estonie a catalogué son contenu comme étant une exigence pour le comportement de l'État. Kersti Kaljulaid, Président de l'Estonie, Président *de la République à l'ouverture de CyCon 2019* (mai 2019), dans : https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html ("L'opinion de l'Estonie) ("les États doivent faire un effort raisonnable pour assurer que leur territoire ne soit pas utilisé dans le but de porter atteinte aux droits d'autres États. Ils doivent chercher des moyens d'offrir un soutien quand l'État lésé en fait la demande pour identifier, attribuer ou investiguer des opérations cybernétiques malicieuses. Cette expectative dépend de la capacité nationale, ainsi que de la disponibilité et de l'accessibilité de l'information." [traduction en espagnol du CJI]).

question cette classification[125]. Par conséquent, étant donné que la neuvième question visait à recueillir l'opinion des États membres sur la classification de la diligence appropriée concernant les obligations d'un État conformément au droit international dans le cyberespace.

48. Le Chili, l'Équateur, le Guatemala, le Guyana et le Pérou adoptent la position voulant que le principe de la diligence appropriée fait partie du droit international que les États doivent appliquer dans le cyberespace[126]. Comme l'explique le Chili, "du point de vue des opérations cybernétiques, un État doit exercer la diligence appropriée afin de ne pas permettre que son territoire souverain, y compris l'infrastructure cybernétique sous son contrôle, ne soit utilisé pour la réalisation d'opérations cybernétiques qui affectent les droits ou qui pourraient avoir des conséquences adverses sur un autre État"[127]. Le Guatemala adopte une position similaire et ajoute que comme "cyberespace" est un terme très large, agir avec la diligence appropriée peut être extrêmement compliqué[128]. Même à cela, dans la mesure où la diligence appropriée "découle du principe de souveraineté", le Guatemala est d'avis que "chaque État doit avoir le contrôle pour arrêter l'activité nocive qui se produit depuis son territoire, en s'obligeant à prendre des mesures préventives, établissant une équipe communautaire d'intervention d'urgence, adoptant des politiques de sécurité de l'information, et en faisant un travail de conscientalisation en matière de sécurité de l'information"[129].

49. La réponse de la Bolivie est plus ambiguë. Sans se référer au statut juridique de la diligence appropriée, ce pays est d'avis que l'on ne peut pas responsabiliser un État pour une attaque cybernétique s'il n'a pas l'infrastructure technologique nécessaire pour contrôler un agent non étatique[130]. Cette opinion pourrait être compatible avec le principe de la diligence appropriée en tant que norme juridique internationale pour les opérations cybernétiques, étant donné qu'elle exige généralement que les États "aient connaissance" des activités en question, ce qui ne serait pas possible dans le cas des États qui ne disposeraient pas de l'infrastructure technique nécessaire[131]. Par ailleurs, l'impossibilité de "contrôler" des activités cybernétiques dont elle aurait connaissance pourrait indiquer que la Bolivie n'adhère pas à la doctrine de la diligence appropriée dans le cyberespace. Sans une précision de la réponse, il est difficile d'arriver à une conclusion. De même, dans les déclarations publiques antérieures des États-Unis, le statut juridique de la diligence appropriée n'a pas été abordé directement. Il importe de signaler, cependant, que les États-Unis ont eu tendance à décrire toute obligation de répondre à des demandes d'assistance en des termes non contraignants[132]. Le fait que les États-Unis n'aient pas approuvé publiquement le principe de la diligence appropriée en tant que norme juridique au sein du GEG ni dans d'autres contextes pourrait indiquer des doutes relatifs au statut juridique de ce principe.

50. Lors de la discussion de Chatham House de juin 2020, plusieurs États membres ont fait part de leur appui à la diligence appropriée en tant que norme (importante) du droit international

---

125 Opinion des Pays-Bas, note 101 *supra*, appendice, en 4.

126 Réponse du Chili, note 1 *supra*, en 6 et 7; réponse de l'Équateur, note 1 *supra*, en 2; réponse du Guatemala, note 1 *supra*, en 4; réponse du Guyana, note 1 *supra*, en 5; réponse du Pérou, note 1 *supra*, en 7.

127 Réponse du Chili, note 1 *supra*, en 6 et 7. L'Équateur a dit simplement que "la diligence appropriée s'applique à ce qui se produit dans les ressources technologiques au sein de son territoire national". Réponse de l'Équateur, note 1 *supra*, en 2.

128 Réponse du Guatemala, note 1 *supra*, en 4.

129 Id. en 2 et 4.

130 Réponse de la Bolivie, note 1 *supra*, en 3 à 7.

131 Voir *Tallinn 2.0*, note 20 *supra*, en 40.

132 Écrit présenté par les États-Unis au GEG en 2014, note 1 *supra*, en 739 ("Un État *devrait* coopérer, d'une façon en accord avec le droit interne et avec les obligations internationales, avec les demandes d'aide provenant d'autres États pour enquêter sur des délits cybernétiques, obtenir des preuves électroniques et mitiger les activités cybernétiques malicieuses sur son territoire".

dans le contexte cybernétique. Cependant, un représentant d'un État membre a exprimé des doutes relativement à l'appui à la diligence appropriée, étant donné le risque de non-respect qui pourrait survenir pour les États qui ne peuvent pas répondre adéquatement aux attaques cybernétiques faute de capacité technique.

Question 10 : Existe-t-il d'autres règles de droit international dont votre Gouvernement estime qu'il serait important de tenir compte dans l'évaluation de la réglementation relative aux opérations cybernétiques faites par les États ou par des acteurs et dont la responsabilité reviendrait à un État dans le domaine international?

51. Dans la dixième et dernière question, on demandait aux États d'indiquer d'autres domaines du droit international sur lesquels le Comité devrait faire porter ses efforts afin d'améliorer la transparence dans le contexte cybernétique. Les réponses abordent différents sujets. La Bolivie demande que l'on accorde plus d'attention à la protection des "droits fondamentaux de ses citoyens dans toute dimension dans laquelle ils agissent", y compris dans le cyberespace[133]. Certaines réponses portent principalement sur la cybercriminalité et, en particulier, la Convention de Budapest, élaborée par le Conseil de l'Europe[134]; d'autres soulignent la contribution des Manuels de Tallinn[135].

52. Deux États, soit l'Équateur et le Guyana, indiquent qu'il pourrait être nécessaire d'élaborer un nouveau droit international dans le contexte cybernétique. L'Équateur souligne la nécessité d'établir la façon de réglementer "les attaques visant des objectifs militaires et/ou civils qui affectent massivement la population, comme c'est le cas pour les infrastructures essentielles, les hôpitaux, les moyens de transport publics et les autres infrastructures qui affectent la sécurité de l'État"[136]. Le Guyana dit qu'il serait prudent de disposer d'un ensemble de principes du droit international adaptés à la nature particulière du cyberespace et observe que les principes juridiques actuels ont été élaborés pour une époque et un contexte différents[137].

53. Lors des consultations de Chatham House de juin 2020, plusieurs États membres ont demandé que l'on porte une plus grande attention au principe de non-ingérence (et à la question de savoir quelles activités cybernétiques constituent de la coertion). Plusieurs participants se sont faits l'écho de l'appel visant à porter une plus grande attention aux questions juridiques "en dessous" du seuil de l'utilisation de la force établi par l'interdiction contenue dans l'article 2 (4) de la Charte des Nations Unies. D'autres ont suggéré de traiter moins des questions de paix et de sécurité internationale en faveur d'une plus grande attention à l'application du droit international des droits de la personne à l'espace cybernétique. D'autres questions traitées ont été le droit diplomatique, le principe de la bonne foi, les contre-mesures et les normes relatives aux preuves pour l'attribution d'opérations cybernétiques à un État.

54. Pour terminer, au moins un participant a demandé d'élaborer une perspective latinoaméricaine relativement à la gouvernance internationale et au cadre juridique de l'espace cybernétique. Le participant a indiqué que la majeure partie des idées sur le droit international dans l'espace cybernétique ont été élaborées par les États européens ou par des spécialistes des pays du Nord. Au lieu de dupliquer les efforts déployés actuellement (par exemple, le GEG des Nations Unies, le Groupe de travail à composition non limitée des Nations Unies, etc.), les pays d'Amérique latine pourraient se fonder sur ces principes pour élaborer un cadre latinoaméricain afin de comprendre le droit international dans l'espace cybernétique, en se basant sur une culture politique

133 Réponse de la Bolivie, note 1 *supra*, en 6 et 7.

134 Réponse du Guatemala, note 1 *supra*, en 4; réponse de la Bolivie, note 1 *supra*, en 6 et 7.

135 Réponse du Costa Rica, note 1 *supra*, en 2 (où le Costa Rica se dit intéressé à adhérer à la Convention de Budapest); réponse du Guatemala, note 1 *supra*, en 4 (où on cite la Convention de Budapest).

136 Réponse de l'Équateur, note 1 *supra*, en 3.

137 Réponse du Guyana, note 1 *supra*, en 5 et 6 (où on indique que l'anonymat est une difficulté particulière pour l'application du droit actuel).

commune d'institutions démocratiques et d'histoire ibéro-américaine. L'OEA a été citée comme étant l'endroit idéal pour coordonner cette vision conjointe.