Études internationales

Droit international et normes pour le cyberespace
Ambiguïtés et instrumentalisation géopolitique
International Law and Norms for Cyberspace
Ambiguities and Geopolitical Instrumentalization

François Delerue, Frédérick Douzet and Aude Géry

Volume 51, Number 2, Summer 2020

Cyberstudies
Cyberstudies

URI: https://id.erudit.org/iderudit/1084460ar
DOI: https://doi.org/10.7202/1084460ar

See table of contents

Publisher(s)

École supérieure d'études internationales

ISSN

1703-7891 (digital)

Explore this journal

Cite this article

Delerue, F., Douzet, F. & Géry, A. (2020). Droit international et normes pour le cyberespace : ambiguïtés et instrumentalisation géopolitique. *Études internationales*, *51*(2), 287–312. https://doi.org/10.7202/1084460ar

Article abstract

International law and norms of responsible behaviour play a central role in UN-led processes on Developments in the Field of icts in the Context of International Security. The purpose of this article is therefore to analyse –and provide insights on– the place of international law in the context of the UNGGE and OEWG, and to explain how international law is being instrumentalized in the present discussions. Firstly, it will explain the context in which these two processes were established and their respective mandates. Secondly, it will discuss the ambiguity –or even confusion– about the role of norms and international law in the regulation of cyberspace and the geopolitical motivations behind it.

Droit international et normes pour le cyberespace
Ambiguïtés et instrumentalisation géopolitique

François DELERUE*, Frédérick DOUZET** et Aude GÉRY***

RÉSUMÉ : *Le droit international et les normes de comportement responsable sont au cœur des discussions onusiennes sur les progrès de la téléinformatique dans le contexte de la sécurité internationale. L'objet du présent article est donc d'analyser la place du droit international, et de donner des pistes de réflexions à ce sujet, dans le cadre des deux processus en cours à l'ONU – le Groupe de travail à composition non limitée (GTCNL) et le Groupe d'experts gouvernementaux chargés d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (GEG) –, et d'expliciter la façon dont le droit international est instrumentalisé dans les présentes négociations. Dans un premier temps, il expliquera dans quel contexte sont nés ces deux processus et quels sont leurs mandats respectifs. Dans un deuxième temps, il discutera de l'ambiguïté – voire de la confusion – sur le rôle des normes et du droit international dans la régulation du cyberespace et des motivations géopolitiques qui la sous-tendent.*

MOTS CLÉS : droit international, normes de comportement responsable, ONU, GEG, UNGGE, GTCNL, OEWG, cybersécurité, téléinformatique, cyberespace

ABSTRACT : *International law and norms of responsible behaviour play a central role in UN-led processes on Developments in the Field of ICTs in the Context of International Security. The purpose of this article is therefore to analyse –and provide insights on– the place of international law in the context of the UNGGE and OEWG, and to explain how international law is being instrumentalized in the present discussions. Firstly, it will explain the context in which these two processes were established and their respective mandates. Secondly, it will discuss the ambiguity –or even confusion– about the role of norms and international law in the regulation of cyberspace and the geopolitical motivations behind it.*

KEYWORDS : International law ; Norms of responsible behavior ; UN ; OEWG ; UNGGE ; Cybersecurity ; ICT ; Cyberspace.

* François Delerue est chercheur en gouvernance de la cybersécurité à l'Université de Leyde (Universiteit Leiden) et enseignant à Sciences Po.

** Frédérick Douzet est professeure de géopolitique à l'Institut français de géopolitique (Université Paris 8) et directrice du centre de recherche et de formation GEODE.

*** Aude Géry est postdoctorante au sein du centre de recherche et de formation GEODE.

Le 12 novembre 2018, le président Emmanuel Macron lançait l'Appel de Paris pour la confiance et la sécurité dans le cyberespace à l'occasion de son discours au Forum sur la gouvernance de l'Internet à l'UNESCO. Ce texte unique en son genre est né de la rencontre des volontés de la France et du secteur privé. En effet, pour la première fois, des États et des acteurs non étatiques, notamment des entreprises privées françaises et étrangères, s'accordaient sur une déclaration commune en matière de sécurité et stabilité du cyberspace. Les soutiens à l'Appel de Paris réaffirmaient leur attachement « à un cyberespace ouvert, sûr, stable, accessible et pacifique, devenu partie intégrante de la vie sous tous ses aspects sociaux, économiques, culturels et politiques » et au fait que « le droit international, dont la Charte des Nations unies dans son intégralité, le droit international humanitaire et le droit international coutumier, s'applique à l'usage des technologies de l'information et de la communication (TIC) par les États »[1]. Références des deux citations ?

L'ambition de la France était de relancer les discussions internationales sur la régulation du cyberespace, mises à mal après l'échec en juin 2017 des travaux du cinquième Groupe d'experts gouvernementaux chargés d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale (GEG)[2]. Cet échec et les désaccords qu'il a mis en lumière ont plongé les négociations internationales dans une période d'instabilité et d'incertitude. Avec l'Appel de Paris, la France souhaitait montrer son rôle moteur sur ces questions, fédérer les États partageant des points de vue similaires (généralement qualifiés de *like-minded states*) et favoriser la reprise des discussions. Néanmoins, les rivalités de pouvoir géopolitiques n'ont cessé de prévaloir, conduisant à l'adoption de deux résolutions concurrentes par l'Assemblée générale des Nations unies (AGNU) en décembre 2018 et la mise en place deux processus de négociation concurrents. Dans ce contexte onusien, le droit international est un élément central des discussions internationales sur la paix et la stabilité dans le cyberespace. Or, le droit international fait également l'objet de représentations géopolitiques contradictoires qui compliquent les négociations, principalement pour deux raisons.

1 Appel de Paris pour la confiance et la sécurité dans le cyberespace, 12 novembre 2018 (https://pariscall.international/fr/).

2. En anglais, Group of Governmental Experts on Developments in the Field of ICTS in the Context of International Security (GGE).

La première est liée au fait que le cyberespace en soi fait l'objet de représentations contradictoires mais qui coexistent, y compris au sein d'un même État. D'un côté, le cyberespace est vu comme un espace à conquérir, impliquant qu'il n'est pas soumis à la souveraineté des États et qu'il existe donc un besoin d'élaborer de nouvelles règles pour y encadrer les comportements. Cette représentation explique donc que l'on se pose la question de savoir si le droit international s'applique ou non. D'un autre côté, le cyberespace est perçu comme un territoire sur lequel s'exerce la souveraineté des États, un nouveau moyen d'agir (Desforges 2018 ; Desforges et Douzet 2018 : 87-108). Dès lors, la seule question qui se pose est celle de savoir comment le droit international existant s'applique. Cependant, les caractéristiques du cyberespace, notamment son immédiateté et son ubiquité (Dupéré et Loiseau 2017 ; Loiseau 2017), compliquent l'application des règles du droit international. Elles entraînent donc des débats sur son interprétation, ses limites et les moyens à employer pour assurer la sécurité et la stabilité du cyberespace.

La seconde raison est liée à la nature même du droit international qui organise la coexistence des États. Tout débat sur la régulation internationale du cyberespace, et plus particulièrement sur le droit international, s'inscrit dans le cadre de rapports de force entre États. Le droit international est un outil de la diplomatie des États. Il « est donc un objet de stratégie, utilisé, voire manipulé en fonction de la perception qu'un État se fait de son intérêt national » (Fernandez 2011 : 14). La « politique juridique extérieure » (Ladreit de Lacharrière 1983) des États va donc varier en fonction de leur perception de la menace géopolitique. Or, en raison de l'exacerbation des tensions dans le cyberespace – et plus généralement dans le monde –, la question du droit international est devenue un objet de crispations. L'analyse de la position des États sur le droit international, et plus largement sur la régulation internationale du cyberespace, révèle différentes représentations de la menace. Elle traduit également en termes juridiques la stratégie des États sur ces questions. Enfin, elle dépeint des visions différentes de l'ordre juridique international.

La question du droit international a de longue date fait l'objet d'âpres débats entre États et a été utilisée par certains États pour tenter de contrer les avancées technologiques d'autres États, comme on a pu le voir en matière spatiale (Klein 1971 : 271-285). L'observateur avisé aura noté que ce sujet, dans le cadre de la régulation du cyberespace, a toujours fait l'objet de désaccords, et ce dès la première

résolution de l'AGNU en 1998. Cependant, le consensus obtenu par les GEG de 2010, 2013 et 2015 et les progrès notoires réalisés ont occulté les désaccords fondamentaux sur le droit international.

Le droit international est un sujet important et une source de tension dans les travaux des GEG depuis le début. Les deux GEG qui se sont soldés par un échec, en 2004 et en 2017, faute de consensus pour l'adoption d'un rapport final, ont échoué notamment à cause de questions liées au droit international. Or, depuis l'échec du dernier GEG en 2017, on assiste à un double phénomène : d'une part, le renforcement du rôle central du droit international comme argument dans les stratégies diplomatiques des États et, d'autre part, une instrumentalisation accrue du droit dans les discours politiques, qui suscite un clivage entre les États (voir notamment U.S. Department of State 2019). Produit des rapports de force entre États, le droit international est aussi devenu l'instrument privilégié des rivalités de pouvoir dans le cadre des nouvelles négociations sur les technologies de l'information et de la communication dans le contexte de la sécurité internationale.

En décembre 2018, deux résolutions ont en effet été adoptées à l'ONU pour relancer ces négociations : la résolution 73/27, « Progrès de l'informatique et des télécommunications et sécurité internationale », et la résolution 73/266, « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale », créant respectivement le Groupe de travail à composition non limitée (GTCNL)[3] et le sixième GEG. Or, comme nous le verrons dans cet article, le traitement de la question du droit international au sein de ces dialogues, comme au sein des GEG qui les ont précédés, révèlent de fortes oppositions. Il existe, d'une part, un désaccord sur les moyens à employer pour assurer la sécurité et la stabilité du cyberespace et, d'autre part, sur le contenu même des négociations, notamment les possibles réponses autorisées par le droit international pour des faits internationalement illicites qui feraient courir le risque d'une militarisation du cyberespace, selon certains États qui souhaiteraient plutôt négocier sur des principes protecteurs tels que la souveraineté.

3. En anglais, Open-Ended Working Group on Developments in the Field of ICTS in the Context of International Security (OEWG).

L'objet du présent article est donc d'analyser la place et l'instrumentation du droit international dans le cadre des deux processus de négociation en cours à l'ONU. Dans un premier temps, il expliquera dans quel contexte géopolitique sont nés ces deux processus et comment s'articulent et se chevauchent leurs mandats respectifs. Dans un deuxième temps, il discutera de l'ambiguïté – voire de la confusion – sur le rôle des normes et du droit international dans la régulation du cyberespace et des motivations géopolitiques qui la sous-tendent, ravivant ainsi le débat sur la nécessité d'un traité international qui divise les États.

I – Éléments de contexte sur le GEG et le GTCNL

Les deux processus mis en place à la demande de l'AGNU sont le reflet des tensions géopolitiques actuelles. Si leur composition et calendrier diffèrent, leurs mandats se recoupent très largement. Un bref rappel historique sur les précédents GEG et les discussions onusiennes sur les progrès de la téléinformatique dans le contexte de la sécurité internationale permet de mesurer à la fois les progrès accomplis et l'ampleur du chemin qu'il reste à parcourir.

A – Les GEG précédents et les discussions onusiennes sur les progrès de la téléinformatique dans le contexte de la sécurité internationale

La question des enjeux pour la sécurité et la stabilité internationale liés au développement des cyber capacités des États a été introduite à l'Assemblée générale des Nations unies sous le thème des « progrès de la téléinformatique dans le contexte de la sécurité internationale » par la Fédération de Russie en 1998, donnant lieu à l'adoption de la résolution 53/70 le 4 décembre 1998. Depuis, l'Assemblée générale adopte chaque année une résolution annuelle sur ce thème.

Ces différentes résolutions ont notamment conduit à la création de cinq GEG successifs en 2004, 2009, 2012, 2014 et enfin en 2016, mais c'est seulement à partir de 2010 que les travaux ont commencé à porter leurs fruits. Les participants au premier GEG en 2004 n'avaient en effet pas été en mesure de parvenir à un consensus. Aucun rapport final n'avait donc été adopté. Comme le soulignait un des experts de la délégation russe, « [l]a principale pierre d'achoppement était la question de savoir si le droit international humanitaire et le droit international réglementaient suffisamment les questions de sécurité dans le cadre des relations internationales en cas d'utilisation "hostile" des technologies

de l'information et de la communication à des fins politico-militaires » (Streltsov 2007 : 7). Ainsi, déjà à l'époque, le droit international était au centre des désaccords entre les experts gouvernementaux. Les trois GEG suivants furent concluants et adoptèrent des rapports consensuels en 2010 (A/65/201), en 2013 (A/68/98) et en 2015 (A/70/174), soumis par le Secrétaire général à l'Assemblée générale qui en a simplement pris note et a recommandé aux États de s'en inspirer. Ces trois rapports contiennent des recommandations sur les mesures de confiance susceptibles de favoriser la sécurité et la stabilité du cyberespace, sur les mesures de coopération et d'assistance internationales pouvant être mises en œuvre par les États et enfin, des normes de comportement responsable ayant pour objectif de mieux définir ce qui constitue un comportement responsable dans le cyberespace.

Et surtout, en 2013, l'applicabilité du droit international a pour la première fois été reconnue dans le rapport final :

> Le droit international et, en particulier, la Charte des Nations Unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible.
>
> (A/68/98 (2013) : § 19)

Le rapport de 2015 du GEG, qui pour la première fois avait explicitement comme mandat de traiter du droit international (A/RES/68/243 (2013)), est allé plus loin en consacrant au droit international sa sixième partie, dans laquelle les États membres ont listé plusieurs règles du droit international, parmi lesquelles le principe de souveraineté, de non-intervention ou encore l'interdiction du recours à la force. Depuis, de nombreux États ont confirmé qu'ils partageaient cette approche dans leurs contributions volontaires transmises au Secrétaire général des Nations unies (A/68/156/Add.1, 2013 ; A/69/112, 2014 ; A/69/112/Add.1, 2014).

Le cinquième GEG s'est soldé par un échec en juin 2017. Les experts gouvernementaux participants ne sont pas parvenus à un accord en vue de l'adoption d'un rapport final consensuel. Cet échec est notamment le fruit du refus de trois États de voir l'applicabilité de certaines branches du droit international inscrite dans le rapport final. En effet, la Chine, Cuba et la Russie s'opposaient à ce que l'applicabilité du droit de légitime défense, des contre-mesures et du droit des conflits armés soient mentionnée et développée dans le rapport du GEG. Les experts gouvernementaux cubains et russes expliquèrent qu'une telle inscription pourrait servir à justifier la militarisation du

cyberespace (République de Cuba 2017 ; The Ministry of Foreign Affairs of the Russian Federation 2017) et invoquèrent des divergences d'interprétation profondes. C'est donc dans ce contexte qu'ont été créés le groupe de travail à composition non limitée et le sixième Groupe d'experts gouvernementaux.

B – Le Groupe de travail à composition non limitée (GTCNL) et le sixième Groupe d'experts gouvernementaux (GEG)

Le GTCNL et le GEG ont été créés respectivement par les résolutions 73/27 et 73/266, adoptées à quelques jours d'intervalle les 5 et 22 décembre 2018, dans un contexte particulièrement tendu entre les États. Pour la première fois depuis le début des discussions en 1998, deux (au lieu d'une) résolutions sur les TIC dans le contexte de la sécurité internationale ont été adoptées par l'Assemblée générale, témoignant d'une rupture apparente entre les États sur ce sujet et donnant l'impression de deux blocs d'États s'opposant.

Le contexte de la création des deux processus de négociation

Les résolutions à l'origine de l'établissement du GTCNL et du GEG ont été proposées par deux groupes d'États formant en apparence des blocs opposés. La réalité est cependant plus complexe et nuancée.

La Russie, soutenue par la Chine et d'autres États (A/C.1/73/L.27/Rev.1), a proposé un premier projet de résolution en octobre 2018. Ce projet de résolution contenait un paragraphe établissant un GTCNL et listait non seulement les normes adoptées par le GEG en 2015 mais également des normes du *Code de conduite international pour la sécurité de l'information* proposé par les États membres de l'Organisation de coopération de Shanghai en 2015 qui avait été à l'époque rejeté en bloc par les États occidentaux. Les États-Unis, notamment soutenus par de nombreux États européens (A/C.1/73/L.37) ont déposé en réaction un projet concurrent de résolution, établissant un sixième GEG et recommandant aux États de mettre en œuvre les rapports des précédents GEG. Face aux nombreuses critiques, la Russie et les États commanditaires (sponsors) du premier projet de résolution ont modifié leur projet. Pour autant, les États-Unis et États commanditaires n'ont pas retiré leur propre projet de résolution. Pour les États-Unis et les États européens, la deuxième version du projet de résolution du GTCNL contenait toujours des dispositions non acceptables et ne reflétait pas correctement le rapport de 2015 du GEG sur lequel il affirmait se baser. Deux projets concurrents de

résolutions sur les TIC dans le contexte de la sécurité internationale, l'un porté par la Russie, l'autre par les États-Unis, ont donc été débattus au sein de la Première commission de l'AGNU.

Ces débats se sont tenus sur fond de vives tensions entre les États. Ainsi, selon le communiqué de presse faisant état des débats, l'Iran

> s'en est pris au pays qui présente un projet de résolution hypocrite dans le but d'imposer le *statu quo*. Celui-ci, a-t-il accusé, considère le cyberespace comme un champ de bataille et pratique activement le développement d'armes cybernétiques. […] Ceux qui visent à imposer leur supériorité veulent bien sûr maintenir le *statu quo* et rejettent l'élaboration de règles internationales qui limiteraient leurs capacités à agir dans le cyberespace (AG/DSI/3613)[4].

Le représentant de la République populaire de Chine a quant à lui demandé si le fait pour un État de voter contre le projet de résolution proposé par la Russie lui permettrait d'obtenir un « ticket » pour participer au GEG (AG/DSI/3619). L'image de deux blocs d'États opposés a donc été renforcée tant par les États commanditaires des deux résolutions que par le contexte d'adoption de ces deux résolutions et la teneur des débats. Ces deux « blocs » s'articulent autour de deux approches souvent analysées comme diamétralement opposées, d'un côté celle des États-Unis et des États occidentaux se qualifiant généralement de *like-minded States*, d'un autre côté, celle de la Chine et de la Russie (Grigsby 2018). Il convient néanmoins de nuancer tant l'homogénéité de ces deux blocs d'États que l'antagonisme de leurs positions respectives.

Premièrement, plutôt que de blocs, il s'agit de groupes d'États qui partagent certaines caractéristiques dans leur approche de la régulation du cyberespace sans pour autant qu'elles soient identiques. Il existe notamment d'importantes divergences entre l'approche de la Chine et celle de la Russie (Broeders *et al*. 2019), comme il en existe entre les approches française et étatsunienne. Deuxièmement, la majorité des États à l'ONU ne faisait partie d'aucun des deux groupes à l'origine de ces résolutions, limitant ainsi la notion de deux blocs d'États structurant les oppositions dans les négociations internationales. Plus important encore, la vaste majorité des États membres des

4. L'Iran fait ici fort probablement référence – entre autres – à Stuxnet, nom d'un ver informatique supposément développé par les États-Unis et Israël qui ont visé en 2010 les centrales nucléaires iraniennes Natanz en vue de saboter le programme nucléaire iranien.

Nations unies a voté en faveur des deux résolutions. La Résolution intitulée « Progrès de l'informatique et des télécommunications et sécurité internationale » (5 décembre 2018, A/RES/73/27) a été adoptée par 119 voix contre 46, avec 14 abstentions (A/73/PV.45) et la Résolution intitulée « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale » (22 décembre 2018, A/RES/73/266) a été adoptée par 138 voix contre 12, avec 16 abstentions (A/73/AG/PV.65). Pour un certain nombre d'États, si ces deux processus sont concurrents, ils revêtent aussi chacun des intérêts différents. La composition limitée et basée sur l'expertise du GEG permet de véritables avancées sur le fond des questions, tandis que la composition non limitée du GTCNL permet quant à elle une approche plus inclusive, ouvrant la possibilité de faire entendre la voix et les attentes de tous les États (De Tomas Colatin 2019). La première session de travail du GTCNL qui s'est tenue à New York en septembre 2019 a d'ailleurs démontré l'intérêt d'un grand nombre d'États pour la participation à ces discussions et pour y faire entendre leur voix, ce qui s'est confirmé lors de la deuxième session formelle tenue en février 2020. Les deux processus en cours n'opposent donc pas deux blocs d'États homogènes et, de par leur composition, offrent une certaine complémentarité. Malgré le climat hostile dans lequel ils sont nés et qui révèle de fortes tensions géopolitiques, ils offrent aux États – en théorie du moins – la possibilité de dépasser leurs clivages pour leur permettre de fonctionner en parallèle, voire en synergie. Les ambassadeurs Guilherme de Aguiar Patriota et Jürg Lauber, respectivement présidents du GEG et du GTCNL, ont d'ailleurs affiché, dès leur prise de fonction, cette ambition constructive.

Les États européens donnent l'impression d'avancer en ordre dispersé dans ces négociations bien qu'il existe aujourd'hui une volonté d'adopter une approche commune. La France s'est affirmée comme un État moteur des discussions internationales dans ce domaine en lançant l'Appel de Paris. Bien que soutenu par les États membres de l'Union européenne, cet Appel reste avant tout une initiative française et non une initiative commune des Européens. De la même manière, malgré l'adoption de la « Cyber Diplomacy Toolbox » par l'Union européenne, mise en œuvre pour la première fois en juillet 2020, certains États semblent plus enclins à agir dans le cadre d'autres coalitions et de concert avec des États non européens (Soesanto 2020). La difficulté pour l'Europe de s'affirmer comme un acteur unifié est renforcée par le fait que dans les processus d'adoption et de négociations des précédentes résolutions, les États

européens ont souvent été perçus comme suiveurs des États-Unis. Néanmoins, il existe aujourd'hui une réelle volonté européenne d'agir de manière concertée et de s'imposer comme un des moteurs des discussions internationales.

L'Europe, au travers de ses États membres, dispose des atouts nécessaires pour s'affirmer comme un des moteurs des discussions internationales et faire valoir ses intérêts (Pawlak 2019). Si les États européens parviennent à agir de concert, l'Europe pourra alors être une véritable force de proposition en mettant notamment en avant son expertise et ses succès dans la mise en œuvre de ses obligations internationales en la matière. À titre d'exemple, la Directive NIS (Directive UE 2016/1148) et le Règlement général sur la protection des données (Règlement UE 2016/679) participent à la mise en œuvre des obligations de diligence (*due diligence* en anglais) et à la « création d'une culture mondiale de la cybersécurité » (A/RES/57/239) des États européens (Delerue *et al.* 2019). Par ailleurs, l'Europe est souvent perçue comme pouvant offrir une approche moins clivante et donc comme étant en capacité de réconcilier les différentes positions.

À l'inverse, les États-Unis, très critiques vis-à-vis des instances multilatérales depuis la prise de fonction de Donald Trump, ont d'emblée annoncé leur réticence à adopter de nouvelles normes, ce qui fait douter les observateurs de leur disposition à adopter une approche constructive et à faire des concessions. Les discussions en cours au sein de l'AGNU et les éventuelles résolutions qui y seront adoptées donneront de précieux éléments sur l'approche des États et l'avenir des discussions. La complémentarité des deux processus a été mise en avant par plusieurs États[5]. Le GTCNL est ouvert à tous les États membres de l'ONU. Tous les États le souhaitant peuvent donc y participer, permettant ainsi de prendre en compte tous les points de vue. *A contrario*, la composition du GEG est limitée à vingt-cinq États membres, « désignés selon le principe d'une représentation géographique » (A/RES/73/266, § 3), et dont les membres permanents du Conseil de sécurité sont membres de droit. Ce faisant, le GEG apparaît comme un organe plus spécialisé. L'analyse de leurs mandats respectifs montre cependant que, s'ils peuvent être complémentaires, ils ne sont pas de nature à faciliter la recherche d'un consensus et d'une cohérence dans les négociations.

5. Cela a été affirmé par un grand nombre de délégations lors des sessions du gtcnl (voir United Nations, Office for Desarmament Affairs, s.d.).

Les mandats des deux processus de négociation

À première vue, les mandats des deux groupes se ressemblent au point de se recouper largement, avec le risque d'empiéter l'un sur l'autre. En effet, les groupes sont tous les deux chargés de travailler sur les normes, règles et principes de comportement responsable des États, les mesures de confiance, le renforcement des capacités et le droit international. Une lecture attentive révèle en réalité plusieurs différences.

Premièrement, le GEG pourra tenir des consultations avec les États ne participant pas au GEG et les organisations régionales compétentes (voir *Digwatch* s.d.). Le GTCNL tiendra quant à lui des sessions informelles de consultations avec le secteur privé et les organisations non gouvernementales. De plus, les acteurs non étatiques sont autorisés à participer aux sessions formelles. Relevons toutefois qu'à la suite du refus de la Chine, seules les organisations accréditées auprès de l'ECOSOC ont pu être autorisées à assister aux sessions formelles. Deuxièmement, la résolution 73/266 définissant le mandat du GEG dispose que le rapport qui sera présenté à l'AGNU sera « assorti d'une annexe contenant les contributions nationales des experts gouvernementaux sur la question de savoir comment le droit international s'applique à l'utilisation des technologies de l'information et des communications par les États » (§3). Par conséquent, les vingt-cinq États participants au GEG vont devoir clarifier leur position sur le droit international applicable aux cyber opérations. C'est notamment ce qu'ont fait la France et les Pays-Bas avec respectivement la publication d'un rapport par le ministère des Armées ; *Droit international appliqué aux opérations dans le cyberespace* (Ministère des Armées 2019) et d'un document officiel du ministère des Affaires étrangères néerlandais intitulé *International Law in Cyberspace* (Royaume des Pays-Bas 2019). Ces deux documents, publiés les 9 septembre et 14 octobre 2019, serviront très certainement de contribution nationale pour les travaux du GEG. Enfin, le GTCNL sera chargé « d'étudier la possibilité d'instaurer un dialogue institutionnel régulier aussi large que possible sous l'égide de l'Organisation des Nations Unies » (A/RES/73/27 : § 5), impliquant des discussions sur la création d'un organe ou processus permanent pour traiter de la question des TIC dans le contexte de la sécurité internationale.

D'autres différences vont cependant soulever des inquiétudes. La première est le calendrier des deux processus. Le GTCNL devait initialement finir ses travaux en 2020, au cours de la 75e session de l'AGNU, soit un an plus tôt que le GEG qui devait s'achever en 2021 au

cours de la 76e session. Le prolongement de la 75e session jusqu'en mars 2021 va permettre de prolonger les travaux du GTCNL, permettant une présentation du rapport lors de la 76e session. Il persistera néanmoins un décalage de quelques mois entre la remise des deux rapports potentiels. Ce décalage de calendrier fait craindre à certains que les quelques États à l'origine de la résolution créant le GTCNL changent d'attitude après la fin des travaux. Autrement dit, ils adopteraient une approche constructive jusqu'à la fin des travaux du GTCNL, de manière à obtenir un consensus sur ses conclusions, avant de se montrer moins coopératifs pour la fin des travaux du GEG, au risque de le conduire à l'échec pour faire prévaloir les résultats des travaux du GTCNL.

Le second élément d'inquiétude est lié au contenu du mandat. Le droit international va être discuté au sein des deux processus et constitue un thème central dans leurs travaux. Cette situation représente à la fois une opportunité et un risque : une opportunité pour les États d'avoir des discussions approfondies sur ces questions et de pouvoir débattre de l'interprétation du droit international dans ce nouveau contexte pour la paix et la sécurité internationales ; mais aussi un risque de voir les deux processus adopter des directions divergentes, créant ainsi une situation instable pour l'ordre juridique international.

Il en est de même pour les normes de comportement responsable des États, que la résolution 73/27 mentionne deux fois dans la définition du mandat du GTCNL. La situation est ainsi délicate à deux égards.

La première mention des normes dans la résolution 73/27 apparaît dès le début de la définition du mandat au paragraphe 5. L'Assemblée générale décide en effet que le GTCNL

> sera chargé, sur la base du consensus, de poursuivre l'élaboration, à titre prioritaire, des règles, normes et principes de comportement responsable des États visés au paragraphe 1 de la présente résolution et de définir des moyens de les appliquer ; d'y apporter des changements ou d'en établir des nouveaux, selon qu'il conviendra. (A/RES/73/27 : §5)

Ce sont donc les normes, telles qu'énoncées dans la résolution, qui devraient constituer la base de travail du GTCNL. Dans la mesure où les normes contenues dans la résolution diffèrent légèrement de celles contenues dans le rapport de 2015 du GEG – bien que s'en réclamant – et où la résolution 73/266 renvoie seulement au rapport de 2015 du GEG, cela implique que la base de travail des deux groupes

pourrait différer. Cela augmentera de fait le risque de contradictions ou de divergences de sens entre les recommandations qui seraient adoptées au sein des différents processus. À titre d'exemple, la recommandation sur la prévention des techniques et outils informatiques malveillants est intégrée dans un paragraphe sur l'intégrité de la chaîne logistique dans le rapport du GEG de 2015 alors qu'elle fait l'objet d'une disposition autonome dans la résolution 73/27. Il y a donc une autonomisation de la problématique dans la résolution 73/27 qui pourrait indiquer le souhait de traiter de façon plus explicite le sujet de la prolifération.

Ce risque s'avère toutefois limité par la pratique des États jusqu'ici. On relève en effet que lors des deux premières sessions du GTCNL, la très grande majorité des États ont indiqué se référer aux normes du GEG et non à celles contenues dans la résolution 73/27. Cela illustre l'absence de consensus sur les normes telles qu'énoncées par la résolution 73/27 mais entraîne également un décalage entre l'application à la lettre du mandat et la pratique adoptée dans la conduite des négociations.

La question de la base de travail peut également entraîner des conséquences sur d'autres aspects des négociations. Le mandat précise que le GTCNL doit « définir les moyens de les appliquer » (A/RES/73/27). Ce faisant, les États membres seront donc chargés de détailler l'opérationnalisation des normes. En effet, dans la mesure où plusieurs d'entre elles sont déclaratoires, elles nécessitent d'être précisées pour être mises en œuvre. Enfin, le mandat ouvre la voie à une remise en cause des acquis des GEG de 2013 et 2015 en prévoyant que les États pourront « y apporter des changements » (A/RES/73/27). Cette remise en cause pourrait également passer par l'établissement de nouvelles normes. Si l'élaboration de nouvelles normes, autorisée par la résolution 73/27, peut impliquer la création de nouvelles normes définissant mieux ce que serait un comportement responsable, elle peut *a contrario* impliquer l'adoption de normes revenant sur des acquis de 2013 et 2015 et visant à garantir le caractère ouvert du cyberespace.

La deuxième mention des normes dans la résolution 73/27 apparaît dans la seconde partie de la définition du mandat. Il n'est cette fois-ci pas précisé de quelles normes il s'agit, induisant ainsi un doute quant aux normes de références. S'agit-il, comme plus haut, des normes telles qu'énoncées par la résolution ou de celles adoptées par les GEG de 2013 et 2015 ?

Il existe donc, à la lecture du mandat, des interrogations au sujet des bases sur lesquelles les négociations doivent être conduites. Ces interrogations semblent pour l'instant être réglées par la pratique qui privilégie les normes du GEG comme base de discussion. Elles pourront néanmoins être potentiellement sources de contradictions entre les deux processus dans la mesure où tant le GEG que le GTCNL sont chargés de travailler sur ces dispositions.

Dès lors que les deux processus ont dans leur mandat la question du droit international et des normes de comportement responsable, la question qui se pose est celle de la répartition du travail. Dans son allocution lors de la première session du GTCNL en juin 2019, le représentant spécial du président de la Fédération de Russie pour la coopération internationale dans le domaine de la sécurité de l'information a proposé que le GTCNL traite de la question des normes de comportement responsable, des mesures de confiance et des mesures de coopération et d'assistance internationales, laissant ainsi celle du droit international au GEG (The Embassy of the Russian Federation 2019). Cette proposition n'a pas été suivie et les deux processus travaillent donc en parallèle sur l'ensemble de ces questions.

Cela appelle deux commentaires. D'un côté, l'absence de répartition, entre les deux groupes, du traitement des questions liées au droit international et de celles concernant les normes de comportement responsable des États peut s'expliquer par le fait qu'il est difficile de dissocier ces deux questions complètement. En effet, elles sont intrinsèquement liées, comme nous le verrons. D'un autre côté, cette situation renforce le risque de doublons en termes de contenu des négociations, mais également le risque de contradictions dans les recommandations formulées par les deux groupes sur les droits et obligations des États dans le cyberespace. Cette absence de répartition révèle surtout un désaccord sur les moyens à employer pour assurer la sécurité et la stabilité du cyberespace.

II – Normes et droit international : entre confusion et désaccord sur les moyens à employer pour assurer la sécurité et la stabilité du cyberespace

Le rapport de 2013 du GEG contient une partie dédiée aux normes, règles et principes de comportement responsable des États dans laquelle les États membres du GEG ont non seulement reconnu l'applicabilité du droit international au cyberespace, mais également

adopté plusieurs normes afin de renforcer la sécurité et la stabilité de l'environnement informatique mondial (respect des libertés fondamentales dans l'utilisation des TIC, intensification de la coopération pour lutter contre l'utilisation d'outils informatiques à des fins criminelles, respect du droit international, etc.). Leur analyse montre que plusieurs d'entre elles s'appuient sur la reconnaissance de l'application du droit international dans le cyberespace et paraphrasent, dans le contexte du numérique, des obligations internationales existantes (Adamson 2020 : 27). Dans le rapport de 2015, les États membres ont choisi de distinguer, dans deux parties différentes du rapport, d'une part les normes de comportement responsable, et d'autre part, le droit international. Or, cette distinction méconnaît les liens pouvant exister entre les normes de comportement responsable, qui relèvent de la *soft law,* c'est-à-dire qu'elles sont juridiquement non contraignantes, et le droit international, dont certaines règles sont rappelées par le GEG. De plus, cette distinction va complexifier la définition des droits et obligations des États dans le cyberespace en introduisant de la confusion sur la nature des règles et en compliquant la conduite des négociations. Enfin, cette distinction dans le rapport ne s'accompagne pas d'une répartition de traitement dans le mandat des groupes, ce qui révèle surtout des désaccords sur les moyens de parvenir à la stabilité et à la sécurité du cyberespace.

A – Une distinction en partie artificielle

La séparation formelle – c'est-à-dire dans deux parties distinctes du rapport – des normes non contraignantes de comportement responsable des États, d'un côté, et du droit international, de l'autre, comporte trois limites.

La première limite est liée au fait que la nature des dispositions est mentionnée dans la partie sur les normes – à savoir des normes juridiquement « facultatives et non contraignantes [qui] ne cherchent pas à limiter ou à interdire des actes qui respectent le droit international » (A/70/174 : 8, § 10).

Il s'agit donc de dispositions dont la violation n'est pas susceptible d'engager la responsabilité internationale de l'État. On peut s'interroger sur l'utilité de cette mention dans le rapport du GEG dans la mesure où, n'étant qu'un rapport d'experts, il ne saurait de toute façon créer des obligations contraignantes pour les États. De même, les dispositions contenues dans la partie consacrée au droit international

dans le rapport de 2015 du GEG ne sont pas plus contraignantes que celles contenues dans la partie consacrée aux normes. Elles restent des recommandations.

La mention du caractère non contraignant des normes peut donc être lue comme introduisant une distinction avec les obligations du droit international étudiées dans une autre partie du rapport. Elle revient à préciser que ces dispositions ne sont pas liées au droit international, renforçant la distinction avec les obligations du droit international énoncées dans une autre partie du rapport (Adamson 2020 : 25).

Mais cette distinction entre normes de comportement responsable et obligations du droit international méconnaît le lien existant entre certaines dispositions non contraignantes et des obligations contraignantes. C'est là la deuxième limite. En effet, ces dispositions, bien que non contraignantes, ne sauraient être qualifiées de non-droit par opposition aux règles de droit qui seraient les seules règles contraignantes. Elles relèvent plutôt de ce « dégradé normatif » (Pellet 1984 : 488) entre le droit et le non-droit. Ces dispositions non contraignantes, souvent appelées *soft law*, peuvent en effet contribuer à l'interprétation des obligations existantes du droit international, voire à la formation de nouvelles obligations internationales (Chinkin 2003 : 30-31), l'absence de caractère contraignant n'entraînant pas une absence d'effet juridique (Combacau et Sur 2014 : 53). En effet, « [l]es États refusent, en recourant à un énoncé de *soft law*, un engagement juridique contraignant, mais ne renoncent pas à toute forme d'engagement » (Cazala 2011 : 47).

Enfin, la troisième limite est liée à la mention, à la fois dans la partie dédiée aux normes du rapport et dans la partie traitant du droit international, de l'obligation de diligence (A/70/174, § 13c et 28e) et de l'obligation de protéger et respecter les droits de l'homme (*ibid*., § 13e et 28b). Ces redondances montrent donc qu'il existe un lien entre les deux et que les États ne parviennent pas entièrement à les distinguer.

Cette analyse montre ainsi les limites de la distinction entre les normes non contraignantes et les obligations du droit international, sur le plan formel. Or, cette distinction s'avère tout aussi artificielle sur le plan matériel, c'est-à-dire en termes de contenu.

L'analyse du contenu des normes de comportement responsable montre qu'elles peuvent être regroupées en deux catégories. Certaines normes identifient des bonnes pratiques qui permettent de renforcer la sécurité et la stabilité de l'environnement informatique mondial,

alors que d'autres sont fondées sur des obligations du droit international appliquées au comportement des États dans le cyberespace (Delerue et Géry 2017). Dès lors, cette seconde catégorie de normes entretient au plan matériel un lien étroit avec le droit international.

La séparation établie entre les obligations du droit international énoncées dans le rapport et les normes va poser deux problèmes, compte tenu de leurs liens : l'un au regard de l'identification des droits et obligations des États, et l'autre au regard de la conduite des négociations.

Premièrement, cette distinction va ainsi poser problème au regard de l'identification des droits et obligations des États. Dès lors qu'une norme de comportement responsable paraphrase une obligation internationale, on peut s'interroger sur la volonté ou non de maintenir le lien existant entre ladite norme et l'obligation internationale en elle-même. Quelles conséquences tirer de cette séparation alors que le contenu est le même ? Cette séparation implique-t-elle que la mise en œuvre dans le cyberespace de l'obligation internationale contenue dans la norme ne serait qu'une simple recommandation, détachée de l'obligation internationale sur laquelle elle est construite ? Cela n'est à notre sens pas le cas, dans la mesure où l'État est tenu quoi qu'il arrive de respecter les obligations internationales. Le message véhiculé peut néanmoins prêter à confusion. Cela peut donner l'impression que la norme serait détachée du droit international pour être autonomisée et, le cas échéant, que le comportement à adopter dans le cyberespace ne serait plus fondé sur une obligation internationale – et donc contraignant –, mais sur la bonne volonté de l'État.

De plus, certaines normes tendent à interpréter des obligations du droit international tandis que d'autres se limitent à les paraphraser. De même, certaines dispositions contenues dans la partie dédiée au droit international tendent à interpréter des obligations internationales tandis que d'autres se contentent de les rappeler. Dès lors, comment identifier dans quels cas il s'agit d'un simple rappel du droit international et dans quels cas il s'agit de l'interprétation d'une obligation internationale pour le cyberespace ?

Lorsqu'une même obligation, comme dans le cas de l'obligation de diligence, est citée dans les deux parties du rapport, faut-il considérer que la disposition énoncée dans la partie traitant du droit international a une valeur supérieure à celle citée dans la partie dédiée aux normes dans la mesure où il est précisé que les normes n'ont pas

vocation à limiter les droits et obligations des États ? Selon l'énoncé de l'obligation paraphrasée ou sur laquelle la disposition se base et selon la réponse retenue, les conséquences quant aux droits et obligations des États pourraient différer. À titre d'exemple, lorsque la disposition dans la partie traitant du droit international interprète de façon restreinte une obligation internationale tandis que la disposition dans la partie dédiée aux normes se contente de la paraphraser, cela signifie-t-il que la première disposition a plus de poids – puisqu'elle se situe dans la section droit international – et, le cas échéant, que l'interprétation à retenir de l'obligation internationale est plus restreinte dans son contenu lorsqu'elle est appliquée au cyberespace ?

Deuxièmement, cette distinction risque de poser problème au regard de la conduite des négociations internationales, tant au sein du GTCNL que du GEG. Les États vont discuter des normes et du droit international à deux moments différents, car les sessions de travail sont organisées par thématiques et amènent donc à traiter des normes puis du droit international de façon séparée. Or, les deux questions étant liées, notamment en termes de contenu, il existe un risque que les États traitent deux fois de la même question et adoptent des positions différentes, voire contradictoires. De plus, dans la mesure où les discussions en cours sur les normes se concentrent principalement sur leur opérationnalisation, c'est-à-dire leur mise en œuvre concrète, les dispositions qui vont être adoptées participeront ainsi à l'interprétation des obligations internationales. Or, la question du contenu englobe aussi les aspects non traités par les dispositions qui précisent la mise en œuvre des normes et interprètent donc des obligations internationales. Faudra-t-il considérer que si certaines précisions ne sont pas apportées, c'est parce qu'elles ne découlent pas de la mise en œuvre de l'obligation internationale dont l'application au cyberespace est précisée ? Ou alors faut-il considérer que les éléments non mentionnés n'ont aucune conséquence quant à l'interprétation de l'obligation internationale ?

La distinction établie entre les normes de comportement responsable et les dispositions relatives au droit international n'est donc pas aussi claire et stricte que ce que le rapport laisse entendre. *In fine*, c'est la notion même de norme de comportement responsable dans sa relation au droit international qui, au plan matériel, peut être remise en cause. Elle soulève néanmoins la question de savoir si les normes « sont en effet destinées à promouvoir et à renforcer le droit international ou si [le cadre du] "comportement responsable des États" est une voie détournée du droit international » (Tikk 2020 : 7, traduction

des auteurs)[6]. Au plan formel, la distinction entre les normes et les dispositions relatives au droit international va pouvoir servir de tremplin pour justifier l'élaboration d'un traité.

B – Une distinction facilitant l'argument du besoin d'un traité

En raison des spécificités du cyberespace, la question du besoin de nouvelles règles s'est posée très rapidement. Ainsi, dès 2000, la Russie argumentait en faveur d'un nouveau traité portant spécifiquement sur les TIC dans le contexte de la sécurité internationale, expliquant que le droit international positif ne pouvait pas permettre de répondre aux défis spécifiques du cyberespace et d'encadrer les comportements des États (A/54/213 : 8-10, Russie). *A contrario*, de nombreux États occidentaux estimaient que de nouvelles règles n'étaient pas nécessaires (A/54/213 : 6-8, États-Unis ; 13, Royaume-Uni). La reconnaissance de l'application du droit international aurait pu mettre un terme au débat. Puisque le droit international s'applique aux comportements des États dans le cyberespace, il n'y a alors pas de vide juridique manifeste. Les comportements des États sont encadrés par le droit international existant et il n'est donc pas nécessaire d'adopter de nouvelles règles. En revanche, les normes de comportement responsable des États pourraient servir à compléter et préciser les obligations internationales (Tikk *et al.* 2018 : 20-21), sans pour autant répondre aujourd'hui aux questions pratiques relatives à l'éventuel contenu de règles précises et prenant en compte les caractéristiques du cyberespace. Pourtant, malgré un apparent consensus sur l'application du droit international, la question du traité a pleinement réémergé en 2019, facilitée par la distinction établie entre les normes et le droit international. Elle illustre des vues divergentes sur les moyens d'assurer la sécurité du cyberespace.

D'un côté, certains États comme la Russie souhaitent élaborer de nouvelles obligations internationales dont la violation serait susceptible d'engager la responsabilité internationale de l'État. Sans remettre en cause l'application du droit international positif, ils considèrent qu'il ne permet pas de saisir toutes les spécificités du cyberespace et que de nouvelles règles sont donc nécessaires. De l'autre, certains États comme les États-Unis préfèrent utiliser des règles de *soft law*, non

6. Original : « are indeed intended to promote and enhance international law or whether "responsible state behavior" is a deflected route around international law ».

contraignantes, et dont la violation ne peut, en tant que telle, engager la responsabilité d'un État. Pour ces États, le droit international positif est suffisamment flexible pour encadrer les comportements des États. En revanche, en raison des spécificités du cyberespace, des normes de comportement sont nécessaires en complément afin de préciser les attentes de la communauté internationale.

Cela s'explique pour plusieurs raisons. D'une part, cette opposition remonte aux sources des discussions onusiennes sur la cybersécurité. Elle illustre l'utilisation du droit international pour tenter de limiter les capacités des États les plus avancés, en l'occurrence les États-Unis. D'autre part, elle exprime des visions différentes de la légalité internationale (Roberts 2017). Du point de vue de la doctrine russe, ces normes n'ont vocation qu'à devenir des obligations internationales, conformément à une vision légaliste fondée sur le développement et le respect des obligations du droit international. Sans pour autant remettre en cause le droit international et bien qu'il existe d'importantes différences entre eux, les États occidentaux ont une vision plus politique dans laquelle les engagements politiques et les engagements juridiques sont complémentaires. Cette préférence peut également s'expliquer par le fait que les États occidentaux ne souhaitent pas se contraindre juridiquement dans un contexte où les rapports de force lors de la négociation d'un traité ne seraient pas nécessairement en leur faveur et où il existe de fortes oppositions sur le fond des sujets.

L'opposition s'est donc cristallisée sur la question de la nécessité du traité et de la valeur de ses dispositions, sans discussion sur son contenu éventuel.

En matière de contenu, la question qui se pose est celle de savoir si un futur traité devrait créer de nouvelles obligations internationales – par exemple en transformant des bonnes pratiques énoncées comme normes de comportement responsable en obligations internationales –, ou s'il devrait préciser la façon dont les obligations internationales existantes doivent être interprétées, afin de mieux définir les droits et obligations des États dans le cyberespace.

Premièrement, la question de l'interprétation du droit international dans le contexte particulier qui nous intéresse n'a pas nécessairement vocation à être réglée par l'adoption d'un traité. Rappelons en effet que chaque État est libre, dans la limite de ce que le droit international lui permet, de retenir ses propres interprétations. En revanche, la communication par les États de leurs approches sur

l'application des normes de droit international pourrait jouer un rôle important dans l'identification de la pratique des États (Delerue 2018). En ce sens, la demande qui est faite aux États participant au sixième GEG de fournir une contribution nationale « sur la question de savoir comment le droit international s'applique à l'utilisation des technologies de l'information et des communications » (ONU, Résolution A/RES/73/266 : § 3) pourrait apporter des éléments de réponse pertinents. À l'heure actuelle, moins d'une dizaine d'États dans le monde ont communiqué de manière substantielle sur leur approche (Roguski 2020). Deuxièmement, l'identification de nouvelles obligations internationales ne peut résulter que d'un travail d'interprétation approfondi et de la pratique des États sur l'application du droit international dans le cyberespace. En effet, comment identifier quelles nouvelles règles seraient nécessaires si l'on n'a pas préalablement établi quels comportements étaient déjà couverts par le droit positif ? Par ailleurs, le fait d'élaborer des règles très précises et restreignant de fait le champ matériel de règles coutumières du droit international peut certes apporter de la clarté sur le court terme, mais comporte également un risque d'obsolescence ou d'affaiblissement de ces règles coutumières dont l'application est envisagée dans le contexte du numérique (Grange et Norodom 2019 : 15-16). La flexibilité et la capacité d'adaptation offertes par des principes généraux ne devraient ainsi pas être oubliées au seul motif des nouveaux développements technologiques.

Enfin, la distinction opérée entre les normes de comportement et le droit international offre un argument en faveur de l'élaboration de nouvelles obligations internationales. En effet, c'est à ce stade que l'on peut identifier une contradiction dans l'argumentaire des États refusant tout débat sur l'élaboration d'un traité mais défendant les normes de comportement, voire soutenant l'adoption de nouvelles normes. Ainsi, selon la position française, l'existence de vides juridiques justifiant l'adoption de nouvelles obligations internationales n'a pas été démontré (France 2019b). Pour autant, la France défend activement les normes adoptées en 2013 et 2015 et l'Appel de Paris qui contient également de nouvelles normes, notamment celle sur l'interdiction des opérations offensives par les acteurs non étatiques. L'adoption de ces normes pourrait ainsi être perçue comme le marqueur d'un vide juridique qu'il conviendrait de combler, et donc être utilisée pour justifier l'ouverture de discussions sur un traité international. En ce sens, la proposition russe de confier le sujet des normes de comportement au GTCNL signale un regain d'intérêt pour la Russie de faire adopter un traité international dans ce domaine. En effet,

le format du GTCNL, ouvert à tous les États membres, pourrait constituer un cadre idéal pour avancer vers l'élaboration d'un traité. Il importe cependant de souligner que le souhait d'un traité n'est pas partagé par tous les États – et qu'il peut être explicitement rejeté, comme cela s'est vu lors des sessions du GTCNL[7] –, y compris parmi ceux généralement associés à la Russie. Ainsi, la position chinoise est plus prudente et révèle le souhait de poursuivre l'étude de l'interprétation du droit international et des conséquences attachées à son application aux comportements des États dans le cyberespace.

En distinguant les normes de comportement du droit international, les États membres du quatrième GEG ont donc non seulement introduit une distinction largement artificielle et partiellement démentie par le contenu même des normes, mais également ravivé les tensions autour de la question du traité, exacerbées par le contexte géopolitique. L'enjeu du traité est aujourd'hui un point de divergence fondamental, bloquant toute avancée de fond sur le contenu même des droits et obligations des États dans le cyberespace. Or, cette situation est renforcée par les oppositions sur le contenu des règles de droit international devant être discutées.

Conclusion

Le droit international, instrument de la politique extérieure des États, est devenu un nœud gordien dans les négociations internationales sur la sécurité et la stabilité du cyberespace. Cet article démontre ainsi sa place désormais centrale dans les travaux des deux processus en cours à l'ONU, le GEG et le GTCNL, sur la paix et la stabilité dans le cyberespace.

Au plan politique, les normes de comportement responsable ont indéniablement un rôle à jouer. Elles peuvent guider les États dans l'identification de ce qui constitue un comportement responsable et poser les jalons d'un futur droit international du cyberespace. Il faut souligner, néanmoins, le caractère relativement artificiel de la distinction établie entre les normes juridiquement non contraignantes et le droit international. En analysant en profondeur la distinction opérée dans ces travaux, notre article met en lumière le lien étroit entre

7. Pour connaître les positions des États sur ce sujet, voir les contributions transmises par les États dans le cadre du GTCNL (United Nations, Office for Desarmament Affairs, s.d.).

certaines normes et des obligations de droit international. Certaines normes découlent directement d'obligations de droit international, comme l'obligation de diligence, et semblent avant tout servir à les interpréter. Dans ces conditions, il semble donc difficile d'opérer une distinction stricte. Il serait en effet contre-productif, voire dangereux juridiquement, qu'une norme basée sur une obligation de droit international et ladite norme évoluent de façon distincte au risque d'évoluer dans des directions opposées.

Dans le contexte international actuel, les normes non contraignantes apparaissent comme un palliatif au droit international pour deux raisons principales. Premièrement, parce qu'elles offrent aux États la possibilité de s'accorder sur l'interprétation de certaines obligations de droit international et sur d'autres éléments constitutifs d'un comportement vertueux dans le cyberespace, sans pour autant les graver dans le marbre. Ainsi, ces normes viennent préciser le comportement que devraient adopter les États dans le cyberspace, tant au regard du droit international existant que du consensus politique qui s'est dégagé, sans pour autant créer de nouvelles contraintes. Deuxièmement, ces normes pourraient à terme servir de base à la transformation des règles et principes existants du droit international, voire à la formation de nouvelles règles conventionnelles ou coutumières. C'est un processus long et incertain qu'il ne faut néanmoins pas négliger, car il est à l'origine de nombreuses obligations existantes du droit international. Ces deux remarques soulignent un peu plus le caractère souvent artificiel de la distinction entre normes et droit international. De ces observations découle la nécessité de prendre en compte, dans l'adoption de normes basées sur un consensus politique, leur lien avec le droit international et leurs potentielles conséquences sur son évolution.

Finalement, la distinction entre les normes non contraignantes et le droit international semble être avant tout le résultat des rapports de force entre les États ayant pris part aux précédents GEG, voire d'une relative polarisation autour des positions des États-Unis et des États occidentaux d'un côté, et celles de la Russie et de la Chine d'un autre côté. Cet article a démontré qu'en réalité, cette relative polarisation est une fiction et qu'il existe une mosaïque d'approches différentes partageant de nombreuses similitudes par-delà les deux « blocs » généralement décrits. Cette réalité rappelle la diversité d'approches existantes sur l'application du droit international en général, et en particulier lorsque l'on s'intéresse au droit international applicable aux cyber opérations. Cette situation réaffirme le besoin pour

les États de communiquer de manière substantielle sur leur approche et leur interprétation des règles et principes du droit international, ce qui n'a été fait que par une poignée d'États à l'heure actuelle.

François Delerue
Université de Leyde
La Haye
Pays-Bas

francois.delerue@eui.eu

Frédérick Douzet
Institut Français de Géopolitique
Saint-Denis
France

fdouzet@gmail.com

Aude Géry
GEODE
Aubervilliers
France

gery.aude@gmail.com

Bibliographie

Adamson Liisi, 2020, « International Law and International Cyber Norms : A Continuum ? », dans Dennis Broeders et Bibi van den Berg (dir.), *Governing Cyberspace : Behavior, Power and Diplomacy*, Lanham, Rowman & Littlefield : 19-44.

Broeders Dennis, Liisi Adamson et Rogier Creemers, 2019, *A Coalition of the Unwilling ? Chinese and Russian Perspectives on Cyberspace*, Leyde, The Hague Program, Leiden Asia Center et Université de Leyde. Consulté sur Internet (https://scholarlypublications.universiteitleiden.nl/access/item%3A2967052/view) le 1er septembre 2021.

Cahin Gérard, 2001, *La coutume internationale et les organisations internationales. L'incidence de la dimension institutionnelle sur le processus coutumier*, Paris, Pedone.

Cazala Julien, 2011, « Le *soft law* international entre inspiration et aspiration », *Revue interdisciplinaire d'études juridiques*, vol. 66, no 1 : 41-84.

Chinkin Christine, 2003, « Normative Development in the International Legal System », dans Dinah Shelton (dir.), *Commitment and Compliance : The Role of Non-Binding Norms in The International Legal Systems*, Oxford, Oxford University Press.

Combacau Jean et Serge Sur, 2014, *Droit international public*, Paris, L.G.D.J.

Cour internationale de Justice, 1950, *Affaire du Détroit de Corfou*, arrêt, 9 avril 1950, *C.I.J. Recueil 1950*.

De Tomas Colatin Samuele, 2019, « A Surprising Turn of Events : un Creates Two Working Groups on Cyberspace », ccd coe. Consulté sur Internet (https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/) le 1er septembre 2021.

DELERUE François et Aude GÉRY, 2017, « État des lieux et perspectives sur les normes de comportement responsable des États et mesures de confiance dans le domaine numérique », Note Stratégique, CEIS.

DELERUE François, Joanna KULESZA et Patryk PAWLAK, 2019, « The Application of International Law in Cyberspace : Is There a European Way ? » *EU Cyber Direct – Policy in Focus*. Consulté sur Internet (https://eucyberdirect.eu/content_research/application-of-international-law-european-way/) le 1er septembre 2021.

DESFORGES Alix et Frédérick DOUZET, 2018, « Du cyberespace à la datasphère. Lenouveau front pionnier de la géographie », *NETCOM*, vol. 32, nos 1-2 : 87-108.

DESFORGES Alix, 2018, *Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale. L'exemple de la France*, thèse de doctorat, Université Paris 8 Vincennes-Saint-Denis.

Digwatch, s.d., « UN GGE and OEWG ». Consulté sur Internet (https://dig.watch/processes/un-gge) le 1er septembre 2021.

DOUZET Frédérick et Aude GÉRY, 2020, « War and Peace in Cyberspace : Obama's Multifaceted Legacy », dans François VERGNIOLLE DE CHANTAL (dir.), *Obama's Fractured Presidency : Policies and Politics*, Édimbourg, Edinburgh University Press : 181-208.

DUPÉRÉ Sabrina, 2017, « Les différentes couches composant le cyberespace », dans Hugo LOISEAU et Elena WALDISPUEHL (dir.), *Cyberespace et sciences politiques. De la méthode au terrain, du virtuel au réel*, Québec, Presses de l'Université du Québec : 67-88.

FERNANDEZ Julian, 2011, « Un enjeu et un moyen de la diplomatie des États », *Questions internationales,* numéro thématique *À quoi sert le droit international ?* no 49 : 12-21.

GRANGE Maryline et Anne-Thida NORODOM, 2019, « Propos Introductifs », dans Maryline GRANGE et Anne-Thida NORODOM (dir.), *Cyberattaques et droit international. Problèmes choisis*, Paris, Pedone : 11-20.

GRIGSBY Alex, 2018, « The UN Doubles Its Workload on Cyber Norms, And Not Everyone is Pleased », *Council of Foreign Relations,* blogue, 15 novembre. Consulté sur Internet (https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased) le 1er septembre 2021.

KLEIN Jean, 1971, « Le traité sur l'espace et la réglementation des armements », *Politique étrangère*, vol. 36, no 3 : 271-285.

KRIEGER Heike et Georg NOLTE, 2016, « The International Rule of Law : Rise or Decline ? Points of Departure », *KFG Working Paper Series*, no 1.

LADREIT DE LACHARRIÈRE Guy, 1983, *La politique juridique extérieure*, Paris, Economica.

LOISEAU Hugo, 2017, « Les défis méthodologiques du cyberespace en sciences sociales et politiques », dans Hugo LOISEAU et Elena WALDISPUEHL (dir.), *Cyberespace et sciences politiques : de la méthode au terrain, du virtuel au réel*, Québec, Presses de l'Université du Québec : 37-66.

MINISTÈRE DES ARMÉES (FRANCE), 2019, *Le droit international appliqué aux opérations dans le cyberespace,* 4 octobre. Consulté sur Internet (https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqué+aux+opérations+Cyberespace.pdf) le 1er septembre 2021.

PAWLAK Patryk, 2019, « Rebooting the EU's Cyber Diplomacy », *EU Cyber Direct Ideas in Focus*. Consulté sur Internet (https://eucyberdirect.eu/content_research/rebooting-the-eus-cyberdiplomacy/) le 1er septembre 2021.

PELLET Alain, 1984, « Le "bon droit" et l'ivraie – Plaidoyer pour l'ivraie (Remarques sur quelques problèmes de méthode en droit international du développement) », dans *Le droit des peuples à disposer d'eux-mêmes : méthodes d'analyse du droit international. Mélanges offerts à Charles Chaumon*, Paris, Pedone : 465-493.

Pert Alison, 2017, « International Law in a Post-Post-Cold War World : Can It Survive ? Current Challenges to International Law », Wiley Online Library, *Asia & the Pacific Policy Studies* (https://doi.org/10.1002/app5.174).

République de Cuba, 2017, *71 UNGA : Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Representaciones Diplomáticas de Cuba en El Exterior, 23 juin.

Roberts Anthea, 2017, *Is International Law International ?* Oxford, Oxford University Press.

Roguski Przemyslaw, 2020, *Application of International Law to Cyber Operations : A Comparative Analysis of States' Views*, The Hague Program on Cyber Norms, Policy Brief.

Royaume des Pays-Bas, 2019, *Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace*, rendue publique le 15 octobre 2019, Annexe « International Law in Cyberspace ».

Soesanto Stefano, 2020, « Europe's Incertitude in Cyberspace », *Lawfare,* blogue, 3 août. Consulté sur Internet (https://www.lawfareblog.com/europes-incertitude-cyberspace) le 1er septembre 2021.

Streltsov A.A., 2007, « La sécurité de l'information au niveau international. Description et aspects juridiques », Forum du désarmement, Les technologies de l'information et la sécurité internationale.

The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, 2019, « Statement by Amb. Andrey Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security at the First Session of the UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security », New York, 3-4 juin. Consulté sur Internet (https://rusemb.org.uk/article/541) le 1er septembre 2021.

The Ministry of Foreign Affairs of the Russian Federation, 2017, « Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in this Sphere », 29 juin. Consulté sur Internet (https://www.mid.ru/en/main_en/-/asset_publisher/G51iJnfMMNKX/content/id/2804288) 1er septembre 2021.

Tikk Eneken et Mika Kerttunen, 2018, *Parabasis : Cyber-Diplomacy in Stalemate*, Nupi Report.

Tikk Eneken, 2020, « International Law in Cyberspace : Mind the Gap », *EU Cyber Direct*. Consulté sur Internet (https://eucyberdirect.eu/content_research/international-law-in-cyberspace-mind-the-gap/) le 1er septembre 2021.

United Nations, Office for Desarmament Affairs, s.d., « Open-Ended Working Group ». Consulté sur Internet (https://www.un.org/disarmament/open-ended-working-group/) le 1er septembre 2021.

U.S. Department of State, 2019, *Joint Statement on Advancing Responsible State Behavior in Cyberspace*, 23 septembre. Consulté sur Internet (https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/) le 1er septembre 2021.