IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

EU CYBER DIRECT

Novembre 2020

LES REPRÉSENTATIONS GÉOPOLITIQUES DU DROIT INTERNATIONAL DANS LES NÉGOCIATIONS INTERNATIONALES SUR LA SÉCURITÉ ET LA STABILITÉ DU CYBERESPACE

François Delerue, Frédérick Douzet
et Aude Géry

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

ÉTUDE – n° 75

Le projet EU Cyber Direct soutient les efforts de cyberdiplomatie de l'Union européenne et contribue ainsi au développement d'un ordre international sûr, stable et fondé sur l'état de droit dans le cyberespace grâce à des dialogues approfondis avec des pays partenaires stratégiques et des organisations régionales/internationales. Le projet EU Cyber Direct est financé par la Commission européenne dans le cadre de l'Instrument de partenariat, projet de coopération numérique internationale : Confiance et sécurité dans le cyberespace.

Site internet : https://eucyberdirect.eu

Twitter : @EUCyberDirect

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

EU CYBER DIRECT

LES REPRÉSENTATIONS GÉOPOLITIQUES DU DROIT INTERNATIONAL DANS LES NÉGOCIATIONS INTERNATIONALES SUR LA SÉCURITÉ ET LA STABILITÉ DU CYBERESPACE

François Delerue

Chercheur Cyberdéfense et droit international à l'IRSEM

Frédérick Douzet

Professeure des universités à l'Institut français de géopolitique, directrice de GEODE

Aude Géry

Post-doctorante, GEODE

Pour citer cette étude
François Delerue, Frédérick Douzet, Aude Géry, *Les Représentations géopolitiques du droit international dans les négociations internationales sur la sécurité et la stabilité du cyberespace*, Étude n° 75, IRSEM/EU Cyber Direct, novembre 2020.

Dépôt légal
ISSN : 2268-3194
ISBN : 978-2-11-152714-0

DERNIÈRES ÉTUDES DE L'IRSEM

74. *Réalités opérationnelles de l'environnement arctique. Approches transdisciplinaires et transsectorielles des impacts du changement climatique dans les sous-régions arctiques*
Magali VULLIERME (dir.)

73. *La Diplomatie des garde-côtes en Asie du Sud-Est*
Benoît de TRÉGLODÉ et Éric FRÉCON (dir.)

72. *La Criticité des matières premières stratégiques pour l'industrie de défense*
Raphaël DANINO-PERRAUD

71. *Le Sri Lanka, l'Inde et le Pakistan face à la* Belt and Road Initiative *chinoise*
Raphaëlle KHAN

70. *Risques géopolitiques, crises et ressources naturelles. Approches transversales et apport des sciences humaines*
Sarah ADJEL, Angélique PALLE et Noémie REBIÈRE (dir.)

69. *Contemporary Society-centric Warfare: Insights from the Israeli experience*
Jonathan (Yoni) SHIMSHONI and Ariel (Eli) LEVITE

68. *Les États-Unis divisés : la démocratie américaine à l'épreuve de la présidence Trump*
Frédérick GAGNON, Frédéric HEURTEBIZE et Maud QUESSARD (dir.)

67. *Le Financement chinois dans le secteur des transports en Afrique : un risque maîtrisé*
Juliette GENEVAZ et Denis TULL

66. *L'Expérience militaire dans les médias (2008-2018). Une diversification des formes de récits*
Bénédicte CHÉRON

ÉQUIPE

Directeur
Jean-Baptiste JEANGÈNE VILMER

Directeur scientifique
Jean-Vincent HOLEINDRE

Secrétaire général
CRG1 (2S) Étienne VUILLERMET

Chef du soutien à la recherche
Caroline VERSTAPPEN

Éditrice
Chantal DUKERS

Retrouvez l'IRSEM sur les réseaux sociaux :

@ https//www.irsem.fr

@IRSEM1

AVERTISSEMENT : l'IRSEM a vocation à contribuer au débat public sur les questions de défense et de sécurité. Ses publications n'engagent que leurs auteurs et ne constituent en aucune manière une position officielle du ministère des Armées.

© 2020 Institut de recherche stratégique de l'École militaire (IRSEM).

PRÉSENTATION DE L'IRSEM

Créé en 2009, l'Institut de recherche stratégique de l'École militaire (IRSEM) est un organisme extérieur de la Direction générale des relations internationales et de la stratégie (DGRIS) du ministère des Armées. Composé d'une quarantaine de personnes, civiles et militaires, sa mission principale est de renforcer la recherche française sur les questions de défense et de sécurité.
L'équipe de recherche est répartie en six domaines :
• Le domaine Espace euratlantique – Russie analyse les évolutions stratégiques et géopolitiques en Amérique du Nord, en Europe, en Russie et dans l'espace eurasiatique qui comprend l'Europe orientale (Moldavie, Ukraine, Biélorussie), le Caucase du Sud (Arménie, Géorgie, Azerbaïdjan) et les cinq pays d'Asie centrale. Il s'intéresse plus particulièrement à la compétition de puissances dans cette zone, aux évolutions du rôle de l'OTAN, à la sécurité maritime et aux stratégies d'influence.
• Le domaine Afrique – Asie – Moyen-Orient analyse les évolutions stratégiques et géopolitiques en Afrique, Asie et Moyen-Orient, autour des axes transversaux suivants : autoritarisme politique et libéralisation économique dans les pays émergents ; rôle et place des armées et des appareils de sécurité dans le fonctionnement des États et des sociétés ; enjeux stratégiques et de sécurité régionale ; idéologies, nationalismes et recomposition des équilibres interétatiques régionaux.
• Le domaine Armement et économie de défense s'intéresse aux questions économiques liées à la défense et, plus largement, a vocation à traiter des questions stratégiques résultant des développements technologiques, des problématiques d'accès aux ressources naturelles et de celles liées aux enjeux environnementaux. Les travaux de recherche du domaine s'appuient sur une approche pluridisciplinaire, à la fois qualitative et quantitative, qui mobilise des champs scientifiques variés : économie de défense, histoire des technologies, géographie.
• Le domaine Défense et société est à l'interface des problématiques spécifiques au monde militaire et des évolutions sociétales auxquelles celui-ci est confronté. Les dimensions privilégiées sont les suivantes : lien entre la société civile et les armées, sociologie du

personnel militaire, intégration des femmes dans les conflits armés, relations entre pouvoir politique et institution militaire, renouvellement des formes d'engagement, socialisation et intégration de la jeunesse, montée des radicalités. Outre ses activités de recherche, le domaine Défense et société entend aussi promouvoir les questions de défense au sein de la société civile, auprès de l'ensemble de ses acteurs, y compris dans le champ académique.

• Le domaine Stratégies, normes et doctrines a pour objet l'étude des conflits armés contemporains, en particulier sous leurs aspects politiques, militaires, juridiques et philosophiques. Les axes de recherche développés dans les productions et événements réalisés portent sur le droit international, en particulier sous l'angle des enjeux technologiques (cyber, intelligence artificielle, robotique), les doctrines de dissuasion, la maîtrise des armements avec la lutte contre la prolifération et le désarmement nucléaires. Les transformations des relations internationales et leurs enjeux de puissance et de sécurité ainsi que la philosophie de la guerre et de la paix font également partie du champ d'étude.

• Le domaine Renseignement, anticipation et menaces hybrides mène des recherches portant sur la fonction stratégique « connaissance et anticipation » mise en avant par le Livre blanc de la défense depuis 2008. Ce programme a donc d'abord pour ambition de contribuer à une compréhension plus fine du renseignement entendu dans son acception la plus large (c'est-à-dire à la fois comme information, processus, activité et organisation) ; il aspire ensuite à concourir à la consolidation des démarches analytiques, notamment dans le champ de l'anticipation ; enfin, il travaille sur les différentes dimensions de la guerre dite « hybride », en particulier les manipulations de l'information. Le domaine contribue du reste au renforcement du caractère hybride de l'IRSEM en diffusant des notes se situant à l'intersection de la recherche académique et de l'analyse de renseignement en sources ouvertes.

BIOGRAPHIES

François Delerue est chercheur en cyberdéfense et droit international à l'IRSEM et enseignant à Sciences Po Paris. Il est également rapporteur pour le droit international de l'Academic Advisory Board du projet EU Cyber Direct. Il mène des recherches sur les questions de cyberdéfense et de cybersécurité sous l'angle juridique, stratégique et politique. Il s'intéresse tout particulièrement au droit international, aux normes et à la coopération internationale, ainsi qu'aux différents types d'acteurs impliqués (États, entreprises privées, organisations non gouvernementales, etc.). Plus généralement, il s'intéresse à l'impact des nouvelles technologies (conquête spatiale, robotique, intelligence artificielle, etc.) sur le droit international et les relations internationales. Son ouvrage *Cyber Operations and International Law* est paru chez Cambridge University Press en mars 2020.

Contact : francois.delerue@irsem.fr
Twitter : @francoisdelerue

Frédérick Douzet est professeure des universités en géopolitique à l'Institut français de géopolitique de l'université Paris 8 et directrice du projet Géopolitique de la datasphère (GEODE). Ses recherches portent sur les enjeux stratégiques et géopolitiques de la révolution numérique. Elle est membre de la Global Commission on the Stability of Cyberspace depuis février 2017 et du comité d'éthique de la Défense depuis janvier 2020. En 2017, elle a participé au comité de rédaction de la *Revue stratégique de défense et de sécurité nationale*. De 2013 à 2018, elle a dirigé la Chaire Castex de cyberstratégie de l'Institut des hautes études de Défense nationale (IHEDN). Frédérick Douzet a été nommée membre junior de l'Institut universitaire de France en 2006 et a reçu plusieurs prix pour ses recherches. Elle a coordonné le numéro 177-178 de la revue *Hérodote* « Géopolitique de la datasphère » (2020).

Contact : fdouzet@gmail.com
Twitter : @geode_science

Aude Géry est post-doctorante au sein de GEODE, centre de recherche et de formation sur la politique de la datasphère de l'université Paris 8. Sa thèse porte sur la lutte contre la prolifération des armes numériques en droit international. Ses recherches portent plus généralement sur le droit international des technologies de l'information et de la communication dans le contexte de la sécurité internationale, à la fois sous un angle juridique et géopolitique. Elle travaille ainsi sur les stratégies juridiques des États, les négociations internationales en cours et la coopération internationale.

Contact : gery.aude@gmail.com
Twitter : @AudeGery

SOMMAIRE

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 de cette étude est donc d'analyser – et de donner des pistes de réflexion sur – la place du droit international 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.

Cette étude est composée de trois parties. Dans un premier temps, elle expose dans quel contexte sont nés ces deux processus et quels sont leurs mandats respectifs et la place qu'y tient le droit international. Dans un deuxième temps, elle s'intéresse aux ambiguïtés et conséquences associées à la distinction établie entre normes de comportement et droit international. Enfin, la dernière partie se concentre sur l'interprétation de certaines règles du droit international que sont, d'un côté, les réponses autorisées par le droit international en réaction à une cyberopération et, de l'autre côté, le principe de souveraineté, et analyse les motivations géopolitiques qui la sous-tendent.

INTRODUCTION

Il y a presque deux ans, 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[1]. Ce texte unique en son genre est né de la rencontre des volontés des autorités françaises 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 cyberespace. 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 le 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 ».

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 du cinquième Groupe d'experts gouvernementaux chargé 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 puissance n'ont cessé de prévaloir, conduisant à l'adoption de deux résolutions concurrentes par l'Assemblée générale des

1. « Appel de Paris pour la confiance et la sécurité dans le cyberespace », 12 novembre 2018.

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

Nations unies (AGNU) en décembre 2018 et la mise en place de deux processus de négociation concurrents. Dans ce contexte, le droit international est un élément central des discussions entre États 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.

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, suivant qu'il est considéré comme échappant, ou pas, à la souveraineté des États. 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[3]. Dès lors, la seule question qui se pose est celle de savoir comment le droit international existant s'y applique. Cependant, les caractéristiques du cyberespace compliquent la mise en œuvre 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 de l'espace numérique, 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

3. Alix Desforges, *Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France*, thèse, Université Paris 8 Vincennes-Saint-Denis, 2018, 398 p. ; Alix Desforges et Frédérick Douzet, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *NETCOM*, 32:1-2, 2018, p. 87-108.

se fait de son intérêt national[4] ». La « politique juridique extérieure[5] » 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 de l'espace numérique, révèle différentes représentations de la menace. Elle traduit également en termes juridiques la stratégie des États sur ces questions et dépeint les différentes visions de l'ordre juridique international.

De tout temps la question du droit international a 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. L'observateur avisé aura noté que ce sujet, dans le cadre de la régulation de l'espace numérique, 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 ainsi 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, ont échoué notamment à cause de questions liées au droit international. Après l'échec du dernier GEG en 2017, on a assisté à un double phénomène : le renforcement du rôle central du droit international comme argument dans les stratégies diplomatiques des États et son instrumentalisation accrue dans les discours à travers l'opposition entre ceux qui le respectent et ceux qui ne le respectent pas, ceux qui le soutiennent et ceux qui le remettent en cause[6]. Produit naturel des rapports de force, il en est devenu

4. Julian Fernandez, « Un enjeu et un moyen de la diplomatie des États », *Questions internationales,* n° 49, « À quoi sert le droit international ? », mai-juin 2011, p. 14.

5. Guy Ladreit de Lacharrière, *La Politique juridique extérieure*, Economica, 1983, 236 p.

6. Voir notamment : *Joint Statement on Advancing Responsible State Behavior in Cyberspace*, 23 septembre 2019.

l'instrument privilégié dans le cadre des négociations sur les TIC dans le contexte de la sécurité internationale. Or, compte tenu du contexte d'adoption des résolutions 73/27 « Progrès de l'informatique et des télécommunications et sécurité internationale » et 73/266 « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale » en 2018 créant respectivement le Groupe de travail à composition non limitée (GTCNL)[7] et le sixième GEG, ainsi que des précédents rapports des GEG sur lesquels elles se fondent, le traitement de la question du droit international révèle de fortes oppositions. Ces désaccords se concentrent, d'une part, sur les moyens à employer pour assurer la sécurité et la stabilité de l'espace numérique et, d'autre part, sur le contenu des négociations qui illustrent la perception du risque de militarisation du cyberespace associée aux possibles réponses autorisées par le droit international pour des faits internationalement illicites. Pour autant, négocier sur des principes protecteurs tels que le principe de souveraineté capable de limiter l'action des États sur le territoire d'autres États, n'est pas exempt de difficultés en raison de l'enchevêtrement des enjeux.

L'objet de cette étude est donc d'analyser, et de donner des pistes de réflexions, sur la place du droit international dans le cadre des deux processus en cours à l'ONU et de se pencher sur la façon dont il est instrumentalisé dans les présentes négociations. Dans un premier temps, nous expliquerons dans quel contexte sont nés ces deux processus et quels sont leurs mandats respectifs. Dans un deuxième temps, nous discuterons 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. Enfin, nous examinerons les représentations géopolitiques associées à l'interprétation de certaines règles du droit international.

7. En anglais : Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG).

I. ÉLÉMENTS DE CONTEXTE SUR LE GEG ET LE GTCNL

Les deux processus mis en place à la demande de l'Assemblée générale des Nations unies sont le reflet des tensions géopolitiques actuelles. Si leur composition et leur calendrier diffèrent, leurs mandats se recoupent très largement. Un bref rappel sur les précédents GEG et les discussions à l'ONU 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.

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 cybercapacités des États a été introduite à l'Assemblée générale des Nations unies sous le thème des « progrès de la téléinformatique dans le contexte de la sécurité internationale » par la Fédération de Russie en 1998, donnant lieu à l'adoption de la résolution 53/70 le 4 décembre 1998. Depuis, l'Assemblée générale adopte chaque année une résolution 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 ce n'est vraiment qu'à partir de 2010 que ces travaux ont commencé à porter leurs fruits. Les participants aux travaux du premier GEG de 2004 n'avaient 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[1] ». 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 (document ONU A/65/201), 2013 (document ONU A/68/98) et 2015 (document ONU 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.

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[2].

Le rapport de 2015 du GEG, qui pour la première fois avait explicitement comme mandat de traiter du droit international[3], est allé plus loin en consacrant sa sixième partie au droit international et en y listant plusieurs règles. Depuis, de nombreux États ont confirmé qu'ils partageaient cette approche dans leurs

1. A. A. Streltsov, « La Sécurité de l'information au niveau international : description et aspects juridiques », *Les Technologies de l'information et la sécurité internationale, Forum du désarmement*, 2007, p. 7.

2. ONU, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurite internationale*, 24 juin 2013, document des Nations unies A/68/98, para. 19.

3. ONU, *Progrès de l'informatique et des télécommunications et sécurité internationale*, Résolution de l'Assemblée générale des Nations unies, 27 décembre 2013, A/RES/68/243.

contributions volontaires transmises au secrétaire général des Nations unies[4].

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 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 final. Les experts gouvernementaux cubain et russe expliquèrent qu'une telle inscription pourrait servir à justifier la militarisation du cyberespace[5] 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.

LE GROUPE DE TRAVAIL À COMPOSITION NON LIMITÉE (GTCNL) ET LE SIXIÈME GROUPE D'EXPERTS GOUVERNEMENTAUX (GEG)

Le Groupe de travail à composition non limitée et le sixième Groupe d'experts gouvernementaux 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

4. Voir entre autres : ONU, *Les progrès de l'informatique et des télécommunications et sécurité internationale*, Rapport du secrétaire général, 9 septembre 2013, document des Nations unies A/68/156/Add.1 ; ONU, *Progrès de l'informatique et des télécommunications et sécurité internationale*, Rapport du secrétaire général, 30 juin 2014, document des Nations unies A/69/112 ; ONU, *Progrès de l'informatique et des télécommunications et sécurité internationale*, Rapport du secrétaire général, 18 septembre 2014, document des Nations unies A/69/112/Add.1.

5. Cuba, *71 UNGA: Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Representaciones Diplomáticas de Cuba en El Exterior, 23 juin 2017 ; Russie, *Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in this Sphere*, ministère des Affaires étrangères de la Fédération de Russie, 29 juin 2017.

particulièrement tendu entre les États. Pour la première fois depuis le début des discussions en 1998, deux résolutions sur les TIC dans le contexte de la sécurité internationale, au lieu d'une habituellement, 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 Groupe de travail à composition non limitée (GTCNL) et du Groupe d'experts gouvernementaux (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[6], a proposé un premier projet de résolution en octobre 2018. Il 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, soutenus par de nombreux États européens[7], ont déposé en réaction un projet concurrent de résolution, établissant un sixième GEG. Face aux nombreuses

6. Il s'agit de l'Algérie, l'Angola, l'Azerbaïdjan, le Bélarus, la Bolivie, le Burundi, le Cambodge, la Chine, Cuba, l'Érythrée, la Fédération de Russie, le Kazakhstan, Madagascar, le Malawi, la Namibie, le Népal, le Nicaragua, l'Ouzbékistan, le Pakistan, la République arabe syrienne, la République démocratique du Congo, la République démocratique populaire lao, la République islamique d'Iran, la République populaire démocratique de Corée, les Samoa, la Sierra Leone, le Suriname, le Tadjikistan, le Turkménistan, le Venezuela et le Zimbabwe (document des Nations unies A/C.1/73/L.27/Rev.1).

7. Il s'agit de l'Allemagne, l'Australie, l'Autriche, la Belgique, la Bulgarie, le Canada, la Croatie, Chypre, le Danemark, l'Espagne, l'Estonie, les États-Unis d'Amérique, la Finlande, la France, la Géorgie, la Grèce, la Hongrie, l'Irlande, Israël, l'Italie, le Japon, la Lettonie, la Lituanie, le Luxembourg, le Malawi, Malte, les Pays-Bas, la Pologne, le Portugal, la Roumanie, le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Slovaquie, Slovénie, Suède, Ukraine, Tchéquie (document des Nations unies A/C.1/73/L.37).

critiques, la Russie et les États sponsors du premier projet de résolution ont modifié leur projet. Pour autant, les États-Unis et États sponsors 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 fonder. 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 discutés 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[8] ». 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[9]. L'image de deux blocs d'États opposés a donc été renforcée tant par les États sponsors des deux résolutions que par le contexte de leur adoption et la teneur des débats. Ces deux « blocs » s'articulent autour de deux approches souvent analysées comme diamétralement opposées,

8. L'Iran fait ici fort probablement référence – entre autres – à Stuxnet, nom d'un ver informatique supposément développé par les États-Unis et Israël visant les centrales nucléaires iraniennes Natanz en 2010 en vue de saboter le programme nucléaire iranien (ONU, *Première Commission : les délégations réfléchissent aux moyens de renforcer la sécurité dans le cyberespace*, 30 octobre 2018, couverture des réunions et communiqués de presse des Nations unies [document des Nations unies AG/DSI/3613]).

9. ONU, *La Première Commission achève ses travaux avec un nombre record de projets de résolution mis aux voix*, 8 novembre 2018, couverture des réunions et communiqués de presse des Nations unies, document des Nations unies AG/DSI/3619.

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. 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 sans pour autant qu'elles soient identiques. Il existe notamment d'importantes divergences entre l'approche de la Chine et celle de la Russie[10], comme il en existe entre les approches française et étatsunienne. Deuxièmement, la majorité des États membres de 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 a voté en faveur des deux résolutions[11]. Pour un certain nombre d'États, si ces deux processus sont concurrents, ils revêtent aussi chacun des intérêts différents. La composition limitée et fondée sur l'expertise du GEG permet de véritables avancées sur le fond des questions, tandis que la composition non limitée du GTCNL permet une approche plus inclusive, ouvrant la possibilité de faire entendre la voix et les attentes de tous les États. 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 de participer à ces discussions et d'y faire entendre leur voix, ce qui s'est confirmé lors de la deuxième session formelle de février 2020. Les deux processus en cours n'opposent donc pas deux blocs d'États homogènes et, de par leur composition,

10. Dennis Broeders, Liisi Adamson, Rogier Creemers, *A coalition of the unwilling? Chinese and Russian perspectives on cyberspace*, Policy Brief, novembre 2019, 16 p.

11. La résolution intitulée *Progrès de l'informatique et des télécommunications et sécurité internationale* (5 décembre 2018, Résolution de l'Assemblée générale A/RES/73/27) a été adoptée par 119 voix contre 46, avec 14 abstentions (document des Nations unies 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, Résolution de l'Assemblée générale A/RES/73/266) a été adoptée 138 voix contre 12, avec 16 abstentions (document des Nations unies A/73/PV.65).

présentent une certaine complémentarité. Malgré le climat hostile dans lequel ils sont nés et qui révèle de fortes tensions géopolitiques, ils offrent – en théorie du moins – aux États 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, certains États semblent plus enclins à agir dans le cadre d'autres coalitions et de concert avec des États non européens. La difficulté d'affirmation de l'Europe comme un acteur unifié est renforcée par le fait que, dans les processus d'adoption et de négociation des précédentes résolutions, les 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 acteur majeur 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. 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[12] et le Règlement général sur la protection des

12. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé

données[13] 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[14] » des États européens. 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 l'adoption 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'Assemblée générale des Nations unies et les éventuelles résolutions qui y seront adoptées donneront de précieux éléments sur l'approche des États et le futur des discussions. La complémentarité des deux processus a été mise en avant par plusieurs États. Le GTCNL est ouvert à l'ensemble des membres de l'ONU, 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[15] », 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.

commun de sécurité des réseaux et des systèmes d'information dans l'Union (Directive NIS).

13. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données – RGPD).

14. Résolution de l'Assemblée générale des Nations unies 30 janvier 2003, A/RES/57/239.

15. Résolution de l'Assemblée générale des Nations unies A/RES/73/266, para. 3.

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 des États non membres du GEG et les organisations régionales compétentes (Union africaine, Union européenne, Organisation des États américains, Organisation pour la sécurité et la coopération en Europe et le Forum régional de l'Association des nations de l'Asie du Sud-Est). 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 du Conseil économique et social (ECOSOC) de l'ONU ont pu assister aux sessions formelles. Deuxièmement, la résolution 73/266 définissant le mandat du GEG dispose que le rapport qui sera présenté à l'Assemblée générale 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[16] ». Par conséquent, les vingt-cinq États participants au GEG vont devoir clarifier leur position sur le droit international applicable aux cyberopérations. C'est notamment ce qu'ont fait la France et les Pays-Bas avec respectivement la publication par le ministère des Armées du rapport *Le Droit international appliqué aux opérations dans le cyberespace*[17] et d'un document officiel du ministère des Affaires

16. *Ibid.*

17. France, *Le Droit international appliqué aux opérations dans le cyberespace*, ministère des Armées, 4 octobre 2019.

étrangères néerlandais intitulé *International Law in Cyberspace*[18]. Ces deux documents, publiés les 9 septembre et 14 octobre 2019, serviront très certainement de contribution nationale pour les travaux du GEG[19]. 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[20] », 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, à cause de la crise sanitaire mondiale due à la pandémie de Covid-19, va permettre de prolonger les travaux du GTCNL et de faire une présentation du rapport lors de la 75e session. Il persistera néanmoins un décalage de quelques mois entre la remise des deux potentiels rapports. 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.

18. Pays-Bas, *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 ».

19. Pour une étude comparée des positions des États en matière de droit international appliqué aux opérations dans le cyberespace, voir Przemyslaw Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program on Cyber Norms, Policy Brief, 2020, 48 p.

20. Résolution de l'Assemblée générale des Nations unies A/RES/73/27, para. 5

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[21].

Ce sont donc les normes, telles qu'énoncées dans la résolution, qui devraient constituer la base de travail du GTCNL. Dans la mesure où elles diffèrent légèrement de celles contenues dans le rapport de 2015 du GEG – bien que s'en revendiquant – 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

21. *Ibid.*

dans la résolution 73/27. Il y a donc dans cette dernière une autonomisation de la problématique 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 observée 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 avoir des conséquences sur d'autres aspects des discussions. Le mandat précise que le GTCNL doit « définir les moyens de les appliquer[22] ». 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[23] », ce qui pourrait 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 la création de normes susceptibles de porter atteinte au caractère ouvert du cyberespace, revenant ainsi 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 s'il s'agit de celles énoncées dans la résolution 73/27 et/ou de celles adoptées par les GEG de 2013 et 2015.

Il existe donc, à la lecture du mandat, des interrogations relatives aux bases sur lesquelles les négociations doivent être

22. *Ibid.*
23. *Ibid.*

conduites. Elles semblent pour l'instant être réglées par la pratique qui privilégie les normes du GEG mais des contradictions pourraient apparaître 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[24]. Cette proposition n'a pas été suivie et les deux processus travaillent donc en parallèle sur l'ensemble de ces questions.

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

24. Russie, *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 June 2019*, Ambassade de la Fédération de Russie auprès du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, 7 juin 2019.

II. NORMES ET DROIT INTERNATIONAL : ENTRE CONFUSION ET DÉSACCORD SUR LES MOYENS À EMPLOYER POUR ASSURER LA SÉCURITÉ ET LA STABILITÉ DE L'ESPACE NUMÉRIQUE

Dès 2011, dans l'*International Strategy for Cyberspace* publiée par la Maison Blanche[1], les États-Unis appelaient à l'élaboration de normes de comportement responsable des États dans l'espace numérique. 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 dans l'espace numérique mais également adopté plusieurs normes afin de renforcer la sécurité et la stabilité de l'environnement informatique mondial. Leur analyse montre que plusieurs de ces normes s'appuient sur la reconnaissance de l'application du droit international dans l'espace numérique et paraphrasent, dans le contexte du numérique, des obligations internationales existantes. Dans le rapport de 2015, les États membres ont choisi de faire figurer dans deux parties différentes les normes de comportement responsable et les dispositions relatives au droit international. Or cette distinction méconnaît les liens pouvant exister entre les premières, qui sont de la *soft law* c'est-à-dire non juridiquement contraignantes, et le second, 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, on ne relève aucune

1. États-Unis, *International Strategy for Cyberspace*, Maison Blanche, mai 2011, p. 9. Voir notamment : Frédérick Douzet et Aude Géry, « War and Peace in Cyberspace: Obama's Multifaceted Legacy », *in* François Vergniolle de Chantal (dir.), *Obama's Fractured Presidency. Policies and Politics*, Edinburgh University Press, 2020.

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 de l'espace numérique.

UNE DISTINCTION EN PARTIE ARTIFICIELLE SUR LES PLANS FORMEL ET MATÉRIEL

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 – juridiquement non contraignantes –, alors qu'elle ne l'est pas dans celle dédiée au droit international. Ainsi, le rapport dispose qu'il s'agit de

> normes facultatives et non contraignantes de comportement responsable des États [qui] peuvent contribuer à réduire les risques qui pèsent sur la paix, la sécurité et la stabilité internationales. De ce fait, elles ne cherchent pas à limiter ou à interdire des actes qui respectent le droit international[2].

Leur violation n'est donc pas susceptible d'engager la responsabilité internationale de l'État.

Or dans la mesure où le rapport de 2015 du GEG est un rapport d'experts et non un traité de droit international, toutes les dispositions qu'il contient, y compris celles incluses dans la partie dédiée au droit international, sont par nature juridiquement non contraignantes. C'est également le cas des résolutions de l'Assemblée générale qui, bien que pouvant participer au processus de formation du droit international[3], sont dépourvues de

2. ONU, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, 22 juillet 2015, document des Nations unies A/70/174, p. 8, para. 10.

3. Gérard Cahin, *La Coutume internationale et les organisations internationales. L'incidence de la dimension institutionnelle sur le processus coutumier*, Publication de la RGDIP, nouvelle série, n° 52, Pedone, 2001, 782 p.

tout caractère contraignant. On peut donc s'interroger sur l'utilité de cette mention.

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[4].

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[5] » 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[6], l'absence de caractère contraignant n'entraînant pas une absence d'effet juridique[7]. 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[8] ».

4. Liisi Adamson, « International Law and International Cyber Norms. A Continuum? », *in* Dennis Broeders, Bibi van den Berg (dir.), *Governing Cyberspace. Behavior, Power and Diplomacy*, Rowman & Littlefield, 2020, p. 25.

5. Alain Pellet, « Le "bon droit" et l'ivraie – Plaidoyer pour l'ivraie (Remarques sur quelques problèmes de méthode en droit international du développement) », *in Le Droit des peuples à disposer d'eux-mêmes : méthodes d'analyse du droit international. Mélanges offerts à Charles Chaumon*, Pedone, 1984, p. 488.

6. Christine Chinkin, « Normative Development in the International Legal System », *in* Dinah Shelton (ed.), *Commitment and Compliance. The Role of Non-Binding Norms in The International Legal Systems*, Oxford University Press, 2000, p. 30-31.

7. Jean Combacau et Serge Sur, *Droit international public*, LGDJ, Domat, 2014 (11e éd.), p. 53.

8. Julien Cazala, « Le *soft law* international entre inspiration et aspiration », *Revue interdisciplinaire d'études juridiques*, 2011/1, vol. 66, p. 47.

Enfin, la troisième limite est liée à la mention, à la fois dans la partie dédiée aux normes du rapport et dans celle traitant du droit international, de l'obligation de diligence[9] et de l'obligation de protéger et respecter les droits de l'homme[10]. 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 donc les limites de la distinction entre normes non contraignantes et dispositions paraphrasant des 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 contenus.

L'analyse du contenu des normes de comportement responsable montre qu'elles peuvent être regroupées en deux catégories. Certaines 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 l'espace numérique[11]. Dès lors, cette seconde catégorie de normes entretient sur le 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

9. ONU, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurite internationale*, 22 juillet 2015, document des Nations unies A/70/174, p. 9, para. 13 (c) et p. 15, para. 28 (e).

10. *Ibid.*, para. 13 (e) et 28 (b).

11. François Delerue et Aude Géry, *État des lieux et perspectives sur les normes de comportement responsable des États et mesures de confiance dans le domaine numérique*, Note stratégique, CEIS, 2017.

de maintenir ou non le lien existant entre les deux. Quelles conséquences tirer de cette séparation alors même que le contenu est le même ? Implique-t-elle que la mise en œuvre et le respect de l'obligation reprise 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 ainsi véhiculé pourrait donner l'impression que la norme serait détachée du droit international pour être autonomisée et, le cas échéant, que le comportement à adopter dans l'espace numérique ne serait plus fondé sur une obligation internationale mais sur la bonne volonté de l'État.

De plus, certaines normes et dispositions contenues dans la partie dédiée au droit international semblent interpréter des obligations du droit international tandis que d'autres se limitent à les paraphraser. Dès lors, il est difficile de différencier un simple rappel d'une règle de droit international de l'interprétation spécifique d'une obligation internationale pour le cyberespace.

Lorsqu'une même obligation 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 fonde 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 – car 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 thématique, avec une session dédiée aux normes et une autre au droit international. Or les deux questions étant matériellement liées, 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 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 à l'espace numérique est précisée ? Ou alors faut-il considérer que les éléments non mentionnés n'ont aucune conséquence quant à l'interprétation de l'obligation internationale ?

Les problèmes dans la conduite des négociations risquent de se complexifier selon que les discussions se fondent sur les normes contenues dans la résolution 73/27 (GTCNL) ou sur celles des précédents rapports du GEG, comme le fait la majorité des États. En effet, l'opérationnalisation des normes nécessite préalablement d'identifier les normes de base retenues. La norme sur l'obligation de diligence de la résolution 73/27 offre un bon exemple[12]. Elle est composée de la norme du GEG sur l'obligation de diligence[13] et du paragraphe relatif à cette même obligation dans la partie consacrée au droit international[14]. La norme du GEG paraphrase le célèbre *dictum* de la Cour internationale de Justice dans l'*Affaire du détroit de Corfou* disposant

12. ONU, *Progrès de l'informatique et des télécommunications et sécurité internationale*, Résolution de l'Assemblée générale A/RES/73/27, 5 décembre 2018, para. 1.3.

13. Document des Nations unies A/70/174, para. 13 (c).

14. *Ibid.*, para. 28 (e).

qu'un État ne devrait pas laisser sciemment son territoire être utilisé à des fins contraires aux droits d'autres États[15]. Le paragraphe correspondant dans la partie dédiée au droit international du rapport contient une disposition se concentrant sur le recours aux intermédiaires par les États et le fait de ne pas laisser son territoire être utilisé par des acteurs non étatiques pour commettre des faits internationalement illicites. Ce paragraphe paraît interpréter l'obligation de diligence en précisant son implication quant au comportement à adopter vis-à-vis des intermédiaires et acteurs non étatiques, interrogeant sur la volonté des États de limiter son application dans le contexte numérique à ces deux cas. Selon l'interprétation que l'on retient de ce paragraphe, l'obligation de diligence est donc plus précise ou plus restreinte que l'obligation telle qu'énoncée par la Cour internationale de Justice et reprise dans la partie traitant des normes. Or dans la mesure où ces deux dispositions sont accolées dans la résolution 73/27 mais pas dans le rapport du GEG, selon que l'on prend l'un ou l'autre texte comme référence pour la définition de son opérationnalisation, les dispositions adoptées ne seront pas les mêmes, entraînant un risque de confusion quant à ce qui est attendu des États.

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, sur le 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[16] ». Sur le plan formel, la distinction

15. Cour internationale de Justice, *Affaire du détroit de Corfou*, arrêt, 9 avril 1950, *CIJ Recueil 1950*, p. 22.

16. Eneken Tikk, International Law in Cyberspace: Mind the gap, Research Focus, 2020, p. 7 (traduction des auteurs). Original : « *are indeed intended to promote and enhance international law or whether "responsible state behavior" is a deflected route around international law* ».

entre les normes et les dispositions relatives au droit international va pouvoir servir de tremplin pour justifier l'élaboration d'un traité.

UNE DISTINCTION FACILITANT L'ARGUMENT DU BESOIN D'UN TRAITÉ

En raison des spécificités de l'espace numérique, la question du besoin de nouvelles règles s'est posée très rapidement. Ainsi, dès 2000 la Russie argumentait en faveur d'un nouveau traité, expliquant que le droit international positif ne pouvait pas permettre de répondre aux défis spécifiques à l'espace numérique et encadrer les comportements des États[17]. *A contrario*, de nombreux États occidentaux estimaient que de nouvelles règles n'étaient pas nécessaires. La reconnaissance de l'application du droit international aux comportements des États dans l'espace numérique aurait pu mettre un terme au débat et signifier l'absence 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 peuvent servir à compléter et préciser les obligations internationales. Pourtant, malgré un apparent consensus, 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 de l'espace numérique.

Une opposition se focalisant sur la valeur de l'instrument

Pour les promoteurs du traité, il s'agit d'élaborer un instrument juridiquement contraignant afin de définir explicitement les droits et obligations des États dans l'espace numérique. Ils ne remettent pas en cause l'application du droit international

17. *Les Progrès de la téléinformatique dans le contexte de la sécurité international*, Rapport du secrétaire général, 10 août 1999, document des Nations unies A/54/213, Russie, p. 8-10.

positif, mais considèrent qu'elle ne permet pas pour autant de saisir toutes les spécificités de l'espace numérique. Cette position relève d'une vision exceptionnaliste du droit international fondée sur l'incapacité du droit international général à réguler certains phénomènes et implique le développement d'une *lex specialis*, c'est-à-dire de règles de droit spécifiques pour réguler ces phénomènes. Pour ceux s'y opposant, le droit international positif est suffisamment flexible pour encadrer les comportements des États. En revanche, en raison des spécificités de l'espace numérique, des normes de comportement sont nécessaires en complément afin de préciser les attentes de la communauté internationale. Ces normes n'ont cependant pas vocation, au moins à court et moyen terme, à devenir des obligations internationales. Cette interprétation est confirmée par l'énoncé même de la notion de norme de comportement, celle-ci n'ayant pas pour objet de « limiter ou interdire des actes qui respectent le droit international[18] ». Ainsi, plus que le contenu des règles, c'est la question de leur valeur qui fait débat. D'un côté, certains États comme la Russie souhaitent élaborer de nouvelles obligations internationales dont la violation serait susceptible d'engager la responsabilité internationale des États. De l'autre, certains États comme les États-Unis préfèrent utiliser des règles de *soft law*, non contraignantes, et dont la violation ne peut, en tant que telle, engager la responsabilité d'un État. 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.

Cela s'explique pour plusieurs raisons. D'une part, cet antagonisme remonte aux sources des discussions sur la cybersécurité à l'ONU. Il illustre l'utilisation du droit international pour tenter de limiter les capacités des États les plus avancés et s'inscrit dans un rapport de force géopolitique. D'autre part, il exprime des visions différentes de la légalité internationale. Du point de

18. ONU, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, 22 juillet 2015, document des Nations unies A/70/174, p. 8, para. 10.

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 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. Ne cherchant pas nécessairement à développer des règles contraignantes, ils font le choix d'engagements non contraignants[19].

Cette préférence peut également s'expliquer par le fait qu'ils 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. Si cet élément sera pallié par les étapes de la signature et de la ratification auxquels ils seront libres de procéder après l'ouverture à la signature du potentiel traité adopté, l'existence même de ce traité pourrait les placer dans une position délicate. L'absence de signature et de ratification serait certainement instrumentalisée pour les montrer du doigt comme des États n'étant pas en faveur de la paix et de la stabilité de l'espace numérique. Plus largement, il convient de souligner que nous sommes actuellement dans une période peu propice au développement de nouveaux traités multilatéraux et du droit international en général, un certain nombre d'États se montrant particulièrement critiques à l'égard du cadre juridique international et de toute forme de contrainte qui en découlerait[20].

Or, il importe de faire deux distinctions importantes. D'un côté, celle entre l'*instrumentum* – c'est-à-dire le type d'instrument juridique – et son contenu. De l'autre, celle qui existe entre les notions de contraignant et d'obligatoire. Un traité est un instrument juridique contraignant. C'est un « accord conclu entre

19. Anthea Roberts, *Is International Law International?*, Oxford University Press, 2017, 432 p.

20. Heike Krieger et Georg Nolte, *The International Rule of Law – Rise or Decline? – Points of Departure*, KFG Working Paper Series, n° 1 2016 ; François Delerue, « Reinterpretation or Contestation of International Law in Cyberspace? », *Israel Law Review*, 52:3, 2019, p. 295-298.

deux ou plusieurs sujets du droit international, destiné à produire des effets de droit et régi par le droit international[21] ». Il a pour conséquence de créer, à la charge des États parties, des obligations internationales qui devront être mises en œuvre par lesdits États en vertu du principe *pacta sunt servanda*. Pour autant, un instrument contraignant pourra contenir des dispositions générales laissant une grande marge d'interprétation aux États dans leur mise en œuvre. Leur respect pourra donc se matérialiser de façons très différentes. Tel est par exemple le cas de la Convention-cadre sur le changement climatique ouverte à la signature à la suite de la Conférence de Rio en 1992. Comme expliqué par Alan Boyle : « [c]e traité impose effectivement certains engagements aux parties, mais ses principaux articles, qui traitent des politiques et des mesures de lutte contre les émissions de gaz à effet de serre, sont formulés de manière si prudente et obscure et sont si peu précis qu'il n'est pas certain que de véritables obligations soient créées[22] ». *A contrario*, des dispositions non contraignantes pourront avoir un caractère obligatoire en raison du vocabulaire employé, de leur précision – qui impliquera une mise en œuvre uniforme – ou de l'existence de mécanismes de suivi poussés. Ainsi, « [l]a technique ou le moule conventionnel ne confèrent pas à eux seuls à ces obligations une intensité donnée[23] ». Par conséquent, le formalisme juridique ne saurait présumer du caractère obligatoire des dispositions[24]. En d'autres termes, il convient de dépasser la seule considération du type d'instrument en présence et de regarder concrètement son contenu.

21. Patrick Daillier, Mathias Forteau, Alain Pellet, *Droit international public*, LGDJ, 2009 (8e éd.), p. 132.

22. Alan E. Boyle, « Some Reflections on the Relationship of Treaties and Soft Law », *The International and Comparative Law Quarterly*, vol. 48, n° 4, 1999, p. 907 (traduction des auteurs). Original : « *[T]his treaty does impose some commitments on the parties, but its core articles, dealing with policies and measures to tackle greenhouse gas emissions, are so cautiously and obscurely worded and so weak that it is uncertain whether any real obligations are created*. »

23. Jean Combacau et Serge Sur, *Droit international public*, *op. cit.*, p. 150.

24. R. R. Baxter, « International Law in "Her Infinite Variety" », *The International and Comparative Law Quarterly*, vol. 29, n° 5, 1980, p. 549-566.

Au-delà de l'instrument, quel contenu pour un futur traité ?

En matière de contenu, la question qui se pose est de savoir si un futur traité devrait créer de nouvelles obligations internationales – par exemple en transformant des 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 l'espace numérique.

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 règles de droit international pourrait jouer un rôle important dans l'identification de leur pratique[25]. En ce sens, la demande qui est faite aux États membres du 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[26] » pourrait apporter des éléments de réponse pertinents. En effet, si les vingt-cinq États membres, et en particulier les membres permanents du Conseil de sécurité (Chine, États-Unis,

25. L'échange d'informations sur les stratégies juridiques en matière de cyberopération constitue une étape importante dans le développement de la pratique des États. Or l'existence d'une pratique suffisante est indispensable pour que la Commission du droit international puisse éventuellement être saisie de cette question. Sa saisine, qui aurait pour but d'aboutir à la codification du droit international dans ce domaine, pourrait alors, dans une certaine mesure, constituer une voie alternative à l'adoption d'un traité. Elle ne résoudrait cependant pas la question des éventuelles nouvelles obligations internationales qui pourraient être adoptées. Cette hypothèse n'est cependant pas aujourd'hui envisageable, tant pour des raisons politiques que pour des motifs tenant aux conditions de saisine de la CDI (François Delerue, « The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC? », *ESIL Reflections*, n° 7, 2018.

26. Résolution de l'Assemblée générale des Nations unies A/RES/73/266, para. 3.

France, Royaume-Uni et Russie), se plient à cet élément du mandat, il sera alors possible d'avoir une base solide sur les points de divergence et de convergence dans leurs approches du droit international applicable aux cyberopérations. Il convient de noter qu'à l'heure actuelle moins d'une dizaine d'États dans le monde ont communiqué de manière substantielle sur leur approche[27]. De plus, les normes de comportement responsable des États sont un moyen permettant de s'accorder sur l'interprétation de certaines règles de droit international dans un contexte particulier. En ce sens, plusieurs normes adoptées par les GEG précédents participent à l'interprétation du droit international.

Deuxièmement, l'identification de nouvelles obligations internationales ne devrait 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 ? En ce sens, l'exemple de la protection des infrastructures électorales contre les attaques informatiques visant à interférer avec des élections est significatif. La pertinence de cette proposition de la Global Commission on the Stability of Cyberspace (GCSC)[28] que l'on retrouve également dans l'Appel de Paris, pose question quand le principe de non-intervention trouve déjà indiscutablement à s'appliquer en matière d'infrastructure électorale. Si elle peut être vue comme une mise en œuvre de ce principe, ne mène-t-elle pas à son affaiblissement, et ce faisant à celui de la protection des processus électoraux qu'il implique par son caractère non contraignant et le langage employé ? Au-delà de cet exemple, il s'agit également d'identifier la pertinence et le risque d'obsolescence à choisir des normes

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

28. La Global Commission on the Stability of Cyberspace (GCSC) est un groupe international d'experts du monde académique, du secteur privé, du gouvernement et de la société civile qui a travaillé à l'élaboration de propositions de normes visant à assurer la stabilité du cyberespace.

trop précises et restreignant de fait le champ matériel des règles coutumières du droit international. 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, à ce stade 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 existantes, 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 démontrée[29]. Pour autant, la France défend activement les normes adoptées en 2013 et 2015 et l'Appel de Paris qui contient également de nouvelles normes. Ces positions peuvent être perçues comme contradictoires puisque l'adoption de ces normes pourrait ainsi être interprétée 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. La proposition russe de confier le sujet des normes de comportement au GTNCL 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 favorable pour servir ce projet. Il est donc probable que la Russie utilise ce processus pour proposer à nouveau d'en discuter et promouvoir l'idée selon laquelle un traité serait nécessaire. C'est d'ailleurs ce qui a été fait par la délégation russe lors des sessions formelles du GTCNL. Le cas échéant, on comprend d'autant plus que la disposition sur l'apport de preuves lors de la formulation d'accusations de cyberopérations, qui était ini-

29. France, *Réponse de la France à la résolution 73/27 relative aux « Progrès de l'informatique et des télécommunications et sécurité internationale » et à la résolution 73/266 relative à « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale »*, ministère des Affaires étrangères et de l'Europe, 13 mai 2019.

tialement dans la partie consacrée au droit international dans le rapport de 2015 du GGE, ait été qualifiée de norme de comportement responsable dans la résolution 73/27 puisqu'il s'agirait de la transformer en une véritable obligation internationale. Cette disposition, bien que présente dans la partie VI du rapport de 2015, est explicitement rejetée par les États-Unis et la France qui ont affirmé qu'elle ne saurait impliquer la création d'une nouvelle obligation internationale. Or, en qualifiant cette disposition de norme et selon l'objectif d'élaboration d'un traité, elle pourrait alors avoir vocation à devenir une nouvelle obligation internationale.

Il importe cependant de souligner que le souhait d'un traité n'est pas partagé par tous les États, 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. Sans rejeter le besoin éventuel de nouvelles règles de droit, elle ne s'inscrit donc pas dans cette vision exceptionnaliste.

Quelle que soit la stratégie de la Russie quant à un éventuel traité, l'analyse du caractère normatif et des effets juridiques des dispositions adoptées constitue aujourd'hui un enjeu de taille pour tenter de retrouver son chemin dans les méandres des droits et obligations des États dans l'espace numérique. La pratique des États tant en matière de droit international qu'au regard des normes de comportement reste pour l'instant embryonnaire. Or, elle est fondamentale en raison de son rôle dans la formation du droit international. Par ailleurs, quand bien même ces instruments ne sont pas contraignants, les États les ayant adoptés sont tenus de se comporter de bonne foi. La mise en place d'un mécanisme de suivi de type déclaratoire, sur le modèle proposé par la France au G7[30] et qui pourrait se fonder sur les contributions volontaires des États au secrétaire général des Nations unies, constituerait ainsi un moyen de renforcer ces normes, tout

30. G7, Ministérielle Affaires étrangères, *Déclaration de Dinard sur l'initiative pour des normes dans le cyberespace*, Dinard, 5 avril 2019.

comme pour les mesures de confiance et les mesures de coopération et d'assistance internationales adoptées.

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 l'espace numérique. Or cette situation est renforcée par les oppositions sur le contenu des règles de droit international devant être discutées.

III. INTERPRÉTATION DU DROIT INTERNATIONAL : ENTRE RISQUE DE MILITARISATION DE L'ESPACE NUMÉRIQUE ET ENCHEVÊTREMENT DES ENJEUX

Le principe de l'applicabilité du droit international est aujourd'hui consensuel. Ce qu'il recouvre ne fait, en revanche, l'objet d'aucun accord, entraînant ainsi des risques de blocage importants. L'échec du GEG en 2017 était dû au refus de quelques États de voir l'application au cyberespace de certaines branches du droit international explicitée dans le rapport final. Cette opposition a été présentée par certains commentaires[1] comme une remise en cause générale de l'applicabilité du droit international dans le cyberespace. Or il n'en est rien.

Contrairement à ce qui peut souvent être affirmé, ni la Chine ni la Russie ne remettent en cause le principe même de l'applicabilité du droit international et de la Charte des Nations unies, dans son intégralité, au cyberespace. Leurs positions se ressemblent, avec quelques nuances. Ces deux États ont exprimé leur souhait de se concentrer sur des principes protecteurs du droit international – tels le principe de souveraineté ou celui de non-intervention – et la précision des droits et obligations primaires des États, plutôt que sur les règles organisant les réactions aux violations du droit international – telles que la légitime défense et les contre-mesures. Le refus de débattre de l'application de l'article 51 de la Charte des Nations unies (droit de légitime défense) dans le cyberespace n'est aucunement une remise en cause de l'applicabilité de cette règle. Il repose sur des arguments à la fois politiques et juridiques, notamment liés aux faiblesses en matière d'attribution juridique et aux standards de preuve utilisés en la matière. D'après leur analyse, ces obstacles

1. États-Unis, Michele G. Markoff, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, US Department of State, 23 juin 2017.

juridiques rendraient inopérant ce droit de légitime défense, sans pour autant le remettre en cause dans son existence. Cette subtilité dans leur raisonnement est souvent niée par d'autres acteurs étatiques, soit par simplicité soit par intérêt politique. Or elle est d'autant plus importante que, politiquement, il ne fait que peu de sens pour un État de vouloir renoncer à son droit de légitime défense. Il est d'ailleurs intéressant de relever que si le discours russe sur ce droit est très critique, jamais la Russie n'a énoncé son reniement.

Par ailleurs, quelques mois après l'échec du cinquième GEG, les dirigeants des BRICS (Brésil, Russie, Inde, Chine et Afrique du Sud) adoptèrent la Déclaration de Xiamen le 5 septembre 3017, rappelant leur attachement à l'applicabilité du droit international aux technologies de l'information et de la communication :

> Nous considérons que l'ONU a un rôle central à jouer dans l'élaboration de normes universellement acceptées de comportement responsable des États dans l'utilisation des TIC afin de garantir un environnement pacifique, sûr, ouvert, coopératif, stable, ordonné, accessible et équitable dans le domaine des TIC. Nous soulignons l'importance primordiale des principes du droit international inscrits dans la Charte des Nations unies, en particulier la souveraineté des États, l'indépendance politique, l'intégrité territoriale et l'égalité souveraine des États, la non-ingérence dans les affaires intérieures d'autres États et le respect des droits de l'homme et des libertés fondamentales. Nous soulignons la nécessité de renforcer la coopération internationale contre l'utilisation abusive des TIC à des fins terroristes et criminelles, réaffirmons l'approche générale définie dans les déclarations de eThekwini, Fortaleza, Ufa et Goa à cet égard, et reconnaissons la nécessité d'un instrument réglementaire universel contraignant sur la lutte contre l'utilisation criminelle des TIC sous les auspices des Nations unies, comme énoncé dans la déclaration d'Ufa[2].

2. BRICS, *BRICS Leaders Xiamen Declaration*, 2017 BRICS Summit, 4 septembre 2017, para. 56 (traduction des auteurs). Original : « *We consider the UN has a central role in developing universally accepted norms of responsible state behavior in the use of ICTs to ensure a peaceful, secure, open, cooperative, stable, orderly, accessible and equitable ICT environment. We emphasize the paramount importance of the principles of international law enshrined in the Charter of the United Nations, particularly the state sovereignty, the political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states and respect for human rights and fundamental freedoms. We emphasize the need to enhance international cooperation against terrorist and criminal misuse of ICTs, reaffirm the general*

Cette opposition sur l'interprétation du droit international qui a cristallisé les tensions entre États, repose sur des désaccords liés aux représentations associées à l'interprétation de certaines règles du droit international. En effet, les États vont adopter des interprétations qui peuvent différer en fonction des menaces qui leur semblent prioritaires ou de leurs intérêts stratégiques. En d'autres termes, le débat ne porte pas sur les règles de droit international elles-mêmes, mais sur leur interprétation. En effet, ces règles sont relativement flexibles permettant donc différentes interprétations et, par conséquent, les États n'en ont pas tous les mêmes. La traduction juridique des différentes représentations des menaces va être particulièrement marquée dans le cas des réponses autorisées par le droit international en réaction à un fait internationalement illicite. Mais elle va également être compliquée par l'enchevêtrement des enjeux, illustrant la difficulté pour un État à se positionner sur l'interprétation du droit international en prenant en compte tous ses intérêts stratégiques.

LES RÉPONSES AUTORISÉES PAR LE DROIT INTERNATIONAL : L'ARGUMENT DE LA MILITARISATION DE L'ESPACE NUMÉRIQUE

Les discussions du GGE en 2017 ont achoppé sur le paragraphe de droit international. Certains États ne souhaitaient pas voir à nouveau[3] inscrite de mention du droit des conflits armés, des contre-mesures et de la légitime défense[4] car, selon eux, cela pourrait servir de base à la militarisation du cyberespace. Ces points de désaccord entre les États soulignent l'absence de consensus sur la mise en œuvre des modalités de réponse aux cyberopérations telles qu'organisées par le droit international. En réaction à un acte inamical, un État pourra adopter des

approach laid in the eThekwini, Fortaleza, Ufa and Goa declarations in this regard, and recognize the need for a universal regulatory binding instrument on combatting the criminal use of ICTs under the UN auspices as stated in the Ufa Declaration. »

3. Ils avaient déjà été mentionnés dans le rapport du GEG de 2015 (document des Nations unies A/70/174).

4. Pourtant déjà mentionnés dans le rapport du GEG de 2015 (document des Nations unies A/70/174).

mesures de rétorsion tandis qu'en réaction à un fait internationalement illicite il pourra adopter des mesures de rétorsion ou des contre-mesures[5], la légitime défense n'étant invocable qu'en réaction à une agression armée[6].

Il est fort probable que la question des formes de réponses qui pourraient être invoquées et mises en œuvre par un État victime d'une cyberopération devienne à nouveau un sujet de désaccord, voire de tension, au sein du GEG ou du GTCNL. Cette question est cruciale à un moment où les attributions politiques et/ou imputations[7] publiques se multiplient. Depuis le piratage de Sony Pictures en novembre 2014, attribué par les États-Unis à la Corée du Nord, on assiste à un changement de stratégie de la part de plusieurs États qui ont décidé de dénoncer publiquement certaines attaques informatiques, allant jusqu'à s'exprimer de façon coordonnée (attribution semi-collective) voire conjointe (attribution collective). L'analyse des discours d'attribution montre une évolution qui révèle trois dynamiques. Premièrement, ces discours s'inscrivent dans le cadre de rapports de force opposant principalement les *Five Eyes*[8] et quelques-uns de leurs alliés

5. Les contre-mesures désignent des actes, qui seraient illicites dans des circonstances normales, pris par un État en réaction à un acte lui-même illicite d'un autre État. Le fait qu'un acte soit pris en contre-mesure est considéré comme une circonstance excluant l'illicéité. Voir notamment : François Delerue et Aude Géry, « Le droit international et la cyberdéfense » *in* Didier Danet, Amaël Cattaruzza et Stéphane Taillat, *La Cyberdéfense – Politique de l'espace numérique*, Armand Colin, 2018, p. 68.

6. Voir notamment : François Delerue, *Cyber Operations and International Law*, Cambridge University Press, 2020, chap. 10. Voir aussi le schéma sur l'attribution, la qualification juridique et les modalités de réponse à une cyberopération au regard du droit international dans : François Delerue, *International Law in Cyberspace Matters: This Is How and Why*, EU Cyber Direct, *Ideas in Focus*, 2019.

7. La volonté des États d'invoquer la responsabilité politique ou juridique des États auxquels ils imputent les cyberopérations énoncées n'est pas toujours claire. Ce flou entourant cette pratique n'est pas de nature à clarifier et à apaiser le débat sur les modalités de réaction aux violations du droit international ou aux actes inamicaux.

8. L'expression *Five Eyes* désigne l'alliance entre les services de renseignement de cinq États anglophones (Australie, Canada, États-Unis, Nouvelle-Zélande et Royaume-Uni).

à la Russie et la Chine. Deuxièmement, leur contenu montre que les États, sans pour autant qualifier juridiquement les comportements qu'ils dénoncent, invoquent *a minima* l'ordre juridique international et les normes de comportement responsable adoptées par les GEG de 2013 et 2015. La stratégie de *naming and shaming* a, selon ses défenseurs, pour but d'établir la responsabilité au moins politique des États attaquants et de renforcer la sécurité et la stabilité de l'espace numérique. Elle s'est matérialisée avec l'adoption en marge de l'Assemblée générale des Nations unies par 27 États, dont la France, d'une *Déclaration conjointe en faveur du comportement responsable des États dans le cyberespace* (*Joint Statement on Advancing Responsible State Behavior in Cyberspace* dans sa version officielle en anglais) en date du 23 septembre 2019 et aussi appelée l'« Appel de New York[9] ». Troisièmement, ces discours sont souvent accompagnés de l'adoption de sanctions[10].

Ces éléments de contexte sont importants pour comprendre pourquoi, politiquement, il existe une opposition sur la question des réponses aux cyberopérations étatiques. Elle résulte non seulement des frictions entre des groupes d'États mais également des incertitudes quant aux qualifications juridiques, non explicitées, retenues par les États pour adopter des mesures, non définies, en réponse aux attaques informatiques dénoncées. En d'autres termes, la relative incertitude qui plane quant à l'interprétation du droit international par les États fait peser une certaine insécurité juridique sur la justification qui pourrait

9. *Joint Statement on Advancing Responsible State Behavior in Cyberspace*, 23 septembre 2019.

10. À titre d'exemple, voir États-Unis, *Treasury Imposes Sanctions Against the Government of the Democratic People's Republic of Korea*, Département du Trésor, 2 janvier 2015 (piratage de Sony Pictures) ; États-Unis, *Press Call on the Administration Responses to Russian Malicious Cyber Activity and Harassment*, Maison Blanche, 29 décembre 2016 (interférence dans les élections) ; États-Unis, *Treasury Targets Supporters of Iran's Islamic Revolutionary Guard Corps and Networks Responsible for Cyber-Attacks Against the United States*, Département du Trésor, 14 septembre 2017 ; États-Unis, *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks*, Département du Trésor, 15 mars 2018 (interférence dans les élections et NotPetya).

être invoquée pour prendre des mesures de réponse. C'est ce nouveau contexte de relative insécurité juridique qui explique, en partie, la frilosité de certains États sur la codification de l'interprétation de certaines branches du droit international pour le cyberespace.

Sur le plan du droit international, ces incertitudes reposent sur des interprétations divergentes, y compris entre des États pourtant qualifiés de *like-minded*, et dont certaines tendent à favoriser le recours à la force. La première divergence repose sur l'existence d'un seuil entre le recours à la force (article 2§4 de la Charte des Nations unies) et l'agression armée (article 51). Le premier ouvre le droit à l'adoption de contre-mesures, alors que la seconde déclenche le droit de légitime défense. Or les États-Unis ne reconnaissent pas cette distinction, le droit de légitime défense étant, selon eux, déclenché dès lors qu'un État recourt à la force en violation de l'article 2§4[11]. Cette interprétation a pour conséquence d'abaisser le seuil du recours à la légitime défense, et donc potentiellement à la force, comme réponse à un fait internationalement illicite.

Le deuxième point de divergence est lié à la théorie des contre-mesures armées. Contrairement à la légitime défense, les contre-mesures ne peuvent en aucun cas prendre la forme d'un recours à la force. C'est ce qui ressort notamment des *Articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite*[12]. Un courant minoritaire de la littérature suggère que, tout en maintenant la distinction entre les seuils du recours à la force et de l'agression armée, un État qui serait victime d'un recours à la force n'atteignant pas le seuil de l'agression armée pourrait mettre en œuvre des contre-mesures armées[13]. Ces der-

11. Voir notamment : Harold Hongju Koh, « International Law in Cyberspace », *Harvard International Law Journal,* vol. 54, p. 1-12, sur la base du discours prononcé à la 2012 USCYBERCOM Inter-Agency Legal Conference.

12. Commission du droit international des Nations unies, *Articles sur la responsabilité de l'État pour fait internationalement illicite et commentaires y relatifs,* annexé à la résolution 56/83 de l'Assemblée générale en date du 12 décembre 2001, et rectifié par document A/56/49 (Vol. I)/Corr.3, article 50 (1) (a).

13. Cette théorie a notamment été soutenue par la Juge Bruno Simma dans son opinion individuelle dans l'*affaire des Plates-formes pétrolières (République islamique d'Iran c. États-Unis d'Amérique*) (Cour internationale de Justice, *Affaire des Plates-formes pétrolières [République islamique d'Iran c. États-Unis d'Amérique]*, arrêt, 6 novembre 2003, *CIJ Rec. 2003*, Opinion individuelle, p. 331-334, para. 12-16. On la retrouve longuement développée, et implicitement soutenue, dans le *Manuel de Tallinn 2.0*, dans le commentaire sous la règle 22, voir : Michael N. Schmitt et Liis Vihul (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017 (2e éd.), p. 123-125.

nières devraient respecter le double critère de nécessité et de proportionnalité, qui s'applique aussi aux contre-mesures et à la légitime défense. Cette théorie vient remettre en cause l'équilibre entre ces deux formes de réponse car elle autorise les États à adopter, en réponse à un acte sous le seuil de l'agression armée, des mesures qui impliqueraient un recours à la force. Compte tenu des incertitudes quant à l'identification des différents seuils de qualification, ces interprétations pourraient conduire à favoriser la conduite de cyberopérations aux effets potentiellement déstabilisateurs.

Le troisième point de divergence porte sur l'adoption de contre-mesures collectives afin de soutenir l'État lésé par la cyberopération. Leur application en réponse à des cyberopérations a été défendue par la présidente de l'Estonie lors du discours d'ouverture de la CyCon[14]. Bien qu'il contienne plusieurs ambiguïtés, le régime des contre-mesures collectives est défini par les *Articles de la CDI sur la responsabilité de l'État pour fait internationalement illicite*. Or la proposition estonienne vise à s'en exonérer pour les élargir[15]. Dans un contexte où certains États imputent des cyberopérations dont ils n'ont pas été victimes[16] à d'autres États, notamment dans le cadre

14. Estonie, *President of the Republic at the opening of CyCon 2019*, 29 mai 2019 : « *[a]mong other options for collective response, Estonia is furthering the position that states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation* ».

15. Przemyslaw Roguski, « Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea », *in 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*, NATO CCD COE Publication, 2020, p. 43-62.

16. C'est notamment le cas de la Nouvelle-Zélande qui a attribué les NotPetya et la tentative de piratage de l'OIAC à la Russie tout en déclarant qu'elle n'en avait pas été victime, voir : Nouvelle-Zélande, National Cyber

d'attributions collectives et semi-collectives, cette proposition est perçue comme déstabilisatrice et source de clivages et tensions futures et pourrait constituer un point de blocage important. La France[17] a d'ailleurs exprimé son opposition à la proposition estonienne.

Enfin, le dernier point de divergence porte sur l'assimilation voire la confusion entre l'obligation de diligence et la théorie du *unable-unwilling*. Le non-respect de son obligation de diligence par un État permet à l'État victime d'adopter, sous certaines conditions, des mesures de rétorsion et des contre-mesures sans pour autant ouvrir droit à la mise en œuvre du droit de légitime défense[18]. *A contrario*, la théorie du *unable* or *unwilling* a été utilisée par les États-Unis pour justifier le recours à la force sur le territoire d'États, sans leur consentement, parce qu'ils étaient incapables ou réticents à prendre les mesures nécessaires pour mettre un terme à l'utilisation de leur territoire par des groupes armés. C'est un principe hautement controversé que, jusqu'ici, seuls les États-Unis ont invoqué et dont ils semblent aujourd'hui se distancer. Considérer que la théorie du *unable* or *unwilling* et l'obligation de diligence sont identiques a donc pour conséquence de légitimer le recours à la force dans des situations où il est aujourd'hui proscrit par le droit international. Toute mention de ce principe dans une partie dédiée à la régulation internationale ou aux menaces risquerait donc d'être perçue comme une façon de faciliter le recours à la force contre un État dont le territoire aurait été utilisé pour mener des cyberopérations contre un autre État.

Ces quatre points illustrent les motifs juridiques d'opposition dans les négociations sur les réponses autorisées par le

Security Centre, *New Zealand joins international condemnation of NotPetya cyber-attack*, 16 février 2018 ; Nouvelle-Zélande, Government Communications Security Bureau, *Malicious cyber activity attributed to Russia*, 4 octobre 2018.

17. France, *Le Droit international appliqué aux opérations dans le cyberespace*, *op. cit.*, p. 8.

18. Cette position a été rappelée avec force par la France dans le Livre blanc sur l'application du droit international aux opérations dans le cyberespace, rejetant sans ambiguïté la théorie du *unable* or *unwilling*, *ibid.*, p. 10).

droit international en réaction à un fait internationalement illicite. Facilitant la conduite de cyberopérations en réaction à un acte inamical ou un fait internationalement illicite ils conduisent, selon leurs détracteurs, à la militarisation de l'espace numérique aux dépends d'un cyberespace ouvert, sûr, accessible et pacifique. *A contrario*, et malgré les difficultés prévisibles de l'exercice, ces pays estiment que les négociations devraient porter sur des principes protecteurs et stabilisateurs, notamment les principes de souveraineté et de non-intervention.

LE PRINCIPE DE SOUVERAINETÉ : L'INTERPRÉTATION AU DÉFI DE L'ENCHEVÊTREMENT DES ENJEUX

La souveraineté, attribut même de l'État, est à la base du droit international[19]. Plusieurs corollaires découlent de ce principe, dont l'égalité souveraine des États, leur liberté d'agir dans le périmètre de leur souveraineté et la non-intervention dans les affaires intérieures d'un autre État. Cela implique notamment de limiter le droit pour un État de mener des cyberopérations contre un autre État. C'est donc en ce sens que ces corollaires sont considérés comme protecteurs et stabilisateurs. Chercher à déterminer quelles cyberopérations seraient constitutives d'une violation de la souveraineté et de l'intégrité territoriale d'un État ou du principe de non-intervention est un véritable défi. En effet, en raison de l'enchevêtrement des enjeux – une même question de droit peut se poser dans des contextes très variés et soulever des interprétations différentes en raison d'intérêts stratégiques parfois opposés – et du choix des États de ne pas aborder tel ou tel type de cyberopération ou sujet, par exemple le cyberespionnage, il est difficile de parvenir à un consensus sur l'interprétation de ces principes dans le contexte numérique.

19. Cour internationale de Justice, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique)*, fond, arrêt du 27 juin 1986, *CIJ Recueil 1986*, para. 263, p. 133.

En matière de respect de la souveraineté et de l'intégrité territoriale d'un État, le critère territorial sert de pierre angulaire pour définir les contours des droits et obligations des États. Or, dans le contexte numérique, il peut se trouver malmené face à un phénomène qui fait fi des frontières. On assiste alors à un double mouvement. D'un côté, les États reconnaissent tous aujourd'hui que leur souveraineté s'exerce sur les infrastructures situées sur le territoire[20], conduisant ainsi à territorialiser le cyberespace en se raccrochant non seulement à la couche physique[21] mais également en recourant à d'autres mécanismes, comme la théorie des effets[22]. D'un autre côté, une partie de la doctrine et plusieurs États procèdent à une remise en cause partielle de cette territorialité en se fondant sur des arguments technico-politiques[23] et en interprétant de façon déraisonnable

20. Voir notamment : ONU, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, 24 juin 2013, document des Nations unies A/68/98 ; ONU, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, 22 juillet 2015, document des Nations unies A/70/174.

21. C'est notamment la position adoptée par la France : « [t]oute cyberattaque à l'encontre des systèmes numériques français ou toute production d'effets sur le territoire français via des moyens numériques par un organe étatique, une personne ou une entité exerçant des prérogatives de puissances publiques ou par une personne ou des personnes agissant sur les instructions ou les directives ou sous le contrôle d'un État est constitutive d'une violation de souveraineté » (France, *Le Droit international appliqué aux opérations dans le cyberespace*, *op. cit.*, p. 7).

22. La théorie des effets est utilisée par les États pour identifier un titre de compétence leur permettant d'agir dans un domaine donné. Ainsi, les États vont invoquer l'existence d'effets sur leur territoire résultant d'une activité numérique pour identifier un titre de compétence. Voir Edouard Treppoz, « Jurisdiction in the Cyberspace », *Swiss Review of International and European Law*, vol. 26, n° 2, 2016, p. 273-288.

23. Voir notamment l'analyse de la position des États sur cette question dans Przemyslaw Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program on Cyber Norms, Policy Brief, 2020, p. 4-7.

le critère territorial[24] ou en mettant en avant d'autres titres de compétence[25].

Cette problématique est fondamentale lorsque l'on s'interroge sur deux questions en particulier. La première est celle de l'exercice d'une compétence d'exécution extraterritoriale[26] notamment en matière pénale. Il est traditionnellement admis qu'un État ne peut collecter de preuve sur le territoire d'un autre État en l'absence d'une règle permissive, que celle-ci soit conventionnelle, c'est-à-dire que l'autorisation découlerait d'un traité préexistant entre les États concernés, ou le fruit de l'accord de l'État territorialement compétent[27]. La seconde est celle de l'espionnage et de l'assimilation – ou non – d'une intrusion dans un système d'information à une intrusion sur le territoire d'un

24. États-Unis, United States District Court, Southern District of New York, *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation (Microsoft Corporation vs. United States of America)*, 25 avril 2014, 15 F, Supp. 3d, 475-476 ; États-Unis, Court of Appeals for the Second Circuit, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation (Microsoft Corporation vs. United States of America)*, 14 juillet 2016, affaire 14-2985. Pour les réactions officielles sur l'affaire, voir notamment « Lettre de Viviane Reding à un membre du Parlement européen », 24 juin 2013 ; États-Unis, Court of Appeals for the Second Circuit, « Brief of *Amicus Curiae* Ireland », 23 décembre 2014, affaire 14-2985, document 164, p. 1 ; États-Unis, Supreme Court, « Brief *Amicus Curiae* of the U.N. Special Rapporteur on the Right to privacy Joseph Cannataci in Support of Neither Party », 13 décembre 2017, affaire 17-2, p. 29-36 ; États-Unis, Supreme Court, « Brief of *Amicus Curiae* Jan Philipp Albrecht, Siphie In'T Veld, Viviane Reding, Birgit Sippel, and Axel Voss, Members of the European Parliament in Support of Respondent Microsoft Corporation », 18 janvier 2018, affaire 17-2, p. 6.

25. Cloud Act H.R.4943 ; H. R. 1625, Pub. L. 115- 141 ; Patrick Jacob, « La compétence des États à l'égard des données numériques », *Revue critique de droit international privé*, n° 3, 2019, p. 665-679.

26. « La compétence d'exécution est le pouvoir que possède un État de mettre en œuvre une règle générale ou une décision individuelle par des actes matériels d'exécution pouvant aller jusqu'à la mise en œuvre de la contrainte étatique » (Brigitte Stern, « Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit », *AFDI*, vol. 32, 1986, p. 11).

27. Cour permanente de Justice internationale, *Affaire du « Lotus »*, arrêt du 7 septembre 1927, Série A, n° 10, p. 18-19 ; voir également : Jonathan Bourguignon, « La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'État », *in* SFDI, *Internet et le droit international*, Colloque de Rouen, Pedone, 2014, p. 357-372.

État[28]. La première question relève des débats sur la lutte contre la cybercriminalité et ne devrait donc pas être abordée au sein du GEG ou du GTCNL. La seconde relève de la paix et la sécurité internationales et, bien qu'elle ne soit pas traitée pour des raisons politiques, devrait avoir toute sa place dans les négociations en cours. Ceci est d'autant plus le cas que la plupart des cyberopérations conduites par les États sont le fait des services de renseignement. De plus, toute exploitation d'une vulnérabilité à des fins de renseignement crée un risque pour tous, cette faille pouvant être exploitée à d'autres fins par d'autres acteurs malveillants. De plus, les outils offensifs développés par les États à des fins de renseignement peuvent être dérobés et réutilisés, participant ainsi directement à leur prolifération et à l'instabilité internationale. Envisagée sous deux angles différents, ce sujet revient à poser la question suivante : le fait de pénétrer de façon non autorisée dans les systèmes d'information[29] situés sur le territoire d'un État porte-t-il atteinte à son intégrité territoriale et constitue-t-il une violation de sa souveraineté[30] ? Or de

28. Sur l'application du droit international aux activités d'espionnage dans le cyberespace, voir notamment : Russell Buchan, *Cyber Espionage and International Law*, Bloomsbury Publishing, 2018.

29. On distingue ici le cas de la collecte directe de preuves de celui de l'injonction de transmettre des données délivrées par un juge dans le cas de l'enquête pénale. Dans ce dernier cas, on assiste à un recul du critère de la territorialité des données au profit du critère de rattachement personnel. En ce sens, voir Jennifer Daskal, « Borders and Bits », *Vanderbilt Law Review*, n° 71, 2018, p. 179-240 ; Patrick Jacob, « La compétence des États à l'égard des données numériques : du nuage au brouillard... en attendant l'éclaircie ? », *Revue critique de droit international privé,* n° 3, 2019, p. 665-680.

30. Sur la licéité de l'espionnage, il convient de rappeler qu'en droit international, rien n'interdit aux États de mener des activités d'espionnage. En d'autres termes, l'espionnage en temps de paix ne constitue pas en lui-même un acte internationalement illicite. Cette analyse fait consensus. Néanmoins, deux courants de pensée s'affrontent sur la licéité des actes d'espionnage. Le courant majoritaire considère que l'espionnage n'est pas illicite en lui-même et qu'aucune norme de droit international ne limite la possibilité pour les États de s'y livrer, mais que ces activités peuvent constituer des violations connexes du droit international si elles violent des normes spécifiques du droit international. À titre d'exemple, il est tout à fait licite pour un État d'espionner un autre État, mais le fait d'envoyer ses agents sur le territoire d'un autre État constituerait une violation de la souveraineté de cet État. Le courant minoritaire adopte

la réponse à cette question découle la mise en œuvre des règles secondaires sur la responsabilité de l'État pour fait internationalement illicite, déterminant notamment les mesures que l'État lésé peut prendre pour amener l'État responsable à s'acquitter de ses obligations internationales.

Cette situation illustre la difficulté à cloisonner les sujets traités lorsqu'ils ramènent à une même question et, le cas échéant, le risque d'aboutir à des conclusions contradictoires. Pour éviter ce problème, la solution serait de prendre en compte la finalité de l'acte. Dans cette hypothèse, instaurer une distinction serait indéniablement, et à juste titre, perçu comme une instrumentalisation du principe de souveraineté afin de rendre licites des cyberopérations menées à des fins d'espionnage. Elle montre également les limites de toute négociation sur l'interprétation du droit international dans le contexte numérique. Compte tenu des positions antagonistes sur ce sujet, il semble difficile de pouvoir parvenir à un consensus sur un principe pourtant à la base de l'ordre juridique international et dont découlent d'autres principes du droit international ainsi que la définition de nombreux droits et obligations. Cela interroge alors sur la délimitation entre ce qui devrait faire l'objet d'un consensus dans le cadre de négociations internationales et ce qui devrait relever de l'interprétation de chaque État.

Les points de divergence entre États sur l'interprétation du droit international sont donc nombreux, qu'ils portent sur la question des normes primaires, à travers l'exemple de la souveraineté, ou secondaires, pour les réponses à un acte internationalement illicite. Des positions identiques sur un point précis peuvent être adoptées par des États perçus comme antagonistes (par exemple,

une approche que l'on peut qualifier de fonctionnelle. Il considère que l'espionnage n'est pas illicite en droit international et que cela rejaillit sur les actes d'espionnage. Ainsi, ces actes qui devraient constituer des actes internationalement illicites en temps normal, comme la violation de la souveraineté d'un État, ne seraient pas illicites, car perpétrés à des fins d'espionnage et que l'espionnage est licite en droit international. Pour une analyse de la place de l'espionnage en droit international, voir Fabien Lafouasse, *L'Espionnage dans le droit international*, Éditions Nouveau Monde, 2012, 492 p.

le cas de l'approche de la France et de la Russie sur la violation de souveraineté) tandis que ces mêmes États peuvent fortement s'opposer sur d'autres. De même, la notion de *like-minded* est une fiction qui ne résiste pas à un examen attentif des politiques juridiques internationales des États. Or ces divergences risquent d'être accentuées par la distinction artificielle établie, comme nous l'avons vu plus haut, entre la notion de norme de comportement responsable et le droit international.

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 de l'espace numérique. Cette étude démontre ainsi sa place désormais centrale dans les travaux des deux processus en cours à l'ONU sur la paix et la stabilité dans le cyberespace, le GEG et le GTCNL.

Sur le plan politique, les normes de comportement responsable ont indéniablement un rôle à jouer. Elles peuvent orienter 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 néanmoins souligner 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 étude met en lumière le lien étroit entre certaines normes et des obligations de droit international. Certaines normes découlent directement d'obligations de droit international, comme l'obligation de diligence à titre d'exemple, 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 fondée sur une obligation de droit international et ladite obligation évoluent de façon distincte voire opposée.

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. 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. Là encore, ces deux remarques soulignent un peu plus le caractère souvent artificiel de la distinction entre normes et droit international. L'adoption de normes fondées sur un consensus politique doit donc prendre en compte leur lien avec le droit international et leurs potentielles conséquences sur son évolution.

Finalement, la distinction opérée semble être avant tout le résultat des rapports de force observés lors des 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 de l'autre côté. En réalité, cette relative polarisation est une fiction et il existe une mosaïque d'approches différentes partageant de nombreuses similitudes par-delà les deux « blocs » généralement décrits. Une diversité d'approche existe concernant l'application du droit international en général, et en particulier lorsque l'on s'intéresse à son application aux cyberopérations. Cette situation réaffirme le besoin pour les États de communiquer de manière substantielle sur leur approche et l'interprétation des règles et principes du droit international, ce qui n'a été fait que par une poignée d'entre eux à l'heure actuelle.

Notre étude s'est concentrée sur les normes de comportement et le droit international dans les travaux à l'ONU. Les États, en tant que principaux sujets du droit international et membres des Nations unies, en sont donc les premiers protagonistes. Il est néanmoins nécessaire de prendre en compte la montée en puissance, en particulier sur les thématiques liées aux TIC, de nouveaux acteurs. En effet, les acteurs non étatiques sont aujourd'hui particulièrement actifs dans la réflexion sur les normes[1]. Certaines initiatives visent à proposer et promouvoir

1. Il n'est plus possible d'étudier ces questions et les processus étatiques en cours, notamment à l'ONU, sans s'intéresser aux actions des acteurs non étatiques, qu'il s'agisse d'entreprises privées comme Microsoft ou de groupes d'experts comme la Global Commission for the Stability of Cyberspace (GCSC). Il conviendra notamment de s'intéresser à l'influence de ces acteurs sur le GEG et le GTCNL. Par exemple, on pourrait s'interroger sur l'éventuelle influence

de nouvelles normes de comportement responsable. Dans ce contexte de multiplication des initiatives d'acteurs non étatiques et du développement de normes non contraignantes, on constate néanmoins que le droit international reste le pilier de l'ordre juridique international, y compris lorsqu'il s'agit de définir les droits et obligations des États dans l'espace numérique. À travers les débats et oppositions qu'il suscite, c'est toute son utilité en tant que droit organisant la coexistence pacifique des États qui est réaffirmée. Il ne constitue néanmoins certainement pas une panacée[2] et reste le résultat des rapports de force dans un contexte où les tensions géopolitiques sont exacerbées.

du projet de Convention de Genève numérique proposé par Microsoft sur la proposition faite par certains États d'ouvrir les négociations en vue de l'adoption d'un traité juridiquement contraignant.

2. François Delerue, *Cyber Operations and International Law*, Cambridge University Press, 2020, p. 493-498.

BIBLIOGRAPHIE

ADAMSON Liisi, « International Law and International Cyber Norms. A Continuum? », *in* Dennis Broeders, Bibi van den Berg (dir.), *Governing Cyberspace. Behavior, Power and Diplomacy*, Rowman & Littlefield, 2020, p. 25.

BAXTER R. R., « International Law in "Her Infinite Variety" », *The International and Comparative Law Quarterly*, vol. 29, n° 5, 1980.

BOURGUIGNON Jonathan, « La recherche de preuves informatiques et l'exercice extraterritorial des compétences de l'État », in SFDI, *Internet et le droit international*, Colloque de Rouen, Pedone, 2014.

BOYLE Alan E., « Some Reflections on the Relationship of Treaties and Soft Law », *The International and Comparative Law Quarterly*, vol. 48, n° 4, 1999.

BROEDERS Dennis, ADAMSON Liisi et CREEMERS Rogier, *A coalition of the unwilling? Chinese and Russian perspectives on cyberspace*, Policy Brief, novembre 2019.

BUCHAN Russell, *Cyber Espionage and International Law*, Bloomsbury Publishing, 2018.

CAHIN Gérard, *La Coutume internationale et les organisations internationales. L'incidence de la dimension institutionnelle sur le processus coutumier*, Publication de la RGDIP, nouvelle série, n° 52, Pedone, 2001.

CAZALA Julien, « Le *soft law* international entre inspiration et aspiration », *Revue interdisciplinaire d'études juridiques*, 2011/1, vol. 66.

CHINKIN Christine, « Normative Development in the International Legal System », *in* Dinah Shelton (ed.), *Commitment and Compliance. The Role of Non-Binding Norms in The International Legal Systems*, Oxford University Press, 2000.

COMBACAU Jean et SUR Serge, *Droit international public*, LGDJ, Domat, 2014 (11e éd.).

DAILLIER Patrick, FORTEAU Mathias et PELLET Alain, *Droit international public*, LGDJ, 2009 (8e éd.).

DASKAL Jennifer, « Borders and Bits », *Vanderbilt Law Review*, n° 71, 2018.

DELERUE François, *Cyber Operations and International Law*, Cambridge University Press, 2020.

DELERUE François, *International Law in Cyberspace Matters: This Is How and Why*, EU Cyber Direct, *Ideas in Focus*, 2019.

DELERUE François, « Reinterpretation or Contestation of International Law in Cyberspace? », *Israel Law Review*, n° 52:3, 2019.

DELERUE François, « The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC? », *ESIL Reflections*, n° 7, 2018.

DELERUE François et GÉRY Aude, « Le droit international et la cyber-défense » *in* Didier Danet, Amaël Cattaruzza et Stéphane Taillat, *La Cyberdéfense – Politique de l'espace numérique*, Armand Colin, 2018.

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

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

DESFORGES Alix et DOUZET Frédérick, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », *NETCOM*, 32:1-2, 2018.

DOUZET Frédérick et GÉRY Aude, « War and Peace in Cyberspace: Obama's Multifaceted Legacy », *in* François Vergniolle de Chantal (dir.), *Obama's Fractured Presidency. Policies and Politics*, Edinburgh University Press, 2020.

FERNANDEZ Julian, « Un enjeu et un moyen de la diplomatie des États », *Questions internationales,* n° 49, « À quoi sert le droit international ? », mai-juin 2011.

JACOB Patrick, « La compétence des États à l'égard des données numériques : du nuage au brouillard... en attendant l'éclaircie ? », *Revue critique de droit international privé,* n° 3, 2019.

KOH Harold Hongju, « International Law in Cyberspace », *Harvard International Law Journal,* vol. 54, sur la base du discours prononcé à la 2012 USCYBERCOM Inter-Agency Legal Conference.

KRIEGER Heike et NOLTE Georg, *The International Rule of Law - Rise or Decline? - Points of Departure*, KFG Working Paper Series, n° 1, 2016.

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

LAFOUASSE Fabien, *L'Espionnage dans le droit international*, Éditions Nouveau Monde, 2012.

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

ROBERTS Anthea, *Is International Law International?*, Oxford University Press, 2017, 432 p.

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

SCHMITT Michael N. et VIHUL Liis (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017 (2e éd.).

STERN Brigitte, « Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit », *AFDI*, vol. 32, 1986.

STRELTSOV A. A., « La Sécurité de l'information au niveau international : description et aspects juridiques », *Les technologies de l'information et la sécurité internationale, Forum du désarmement*, 2007.

TIKK Eneken, *International Law in Cyberspace: Mind the gap*, Research Focus, 2020.

TREPPOZ Edouard, « Jurisdiction in the Cyberspace », *Swiss Review of International and European Law*, vol. 26, n° 2, 2016.

ÉTUDE – n° 75

LES REPRÉSENTATIONS GÉOPOLITIQUES DU DROIT INTERNATIONAL DANS LES NÉGOCIATIONS INTERNATIONALES SUR LA SÉCURITÉ ET LA STABILITÉ DU CYBERESPACE

François Delerue, Frédérick Douzet et Aude Géry

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 de cette étude est donc d'analyser – et de donner des pistes de réflexion sur – la place du droit international 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.

Cette étude est composée de trois parties. Dans un premier temps, elle expose dans quel contexte sont nés ces deux processus et quels sont leurs mandats respectifs et la place qu'y tient le droit international. Dans un deuxième temps, elle s'intéresse aux ambiguïtés et conséquences associées à la distinction établie entre normes de comportement et droit international. Enfin, la dernière partie se concentre sur l'interprétation de certaines règles du droit international que sont, d'un côté, les réponses autorisées par le droit international en réaction à une cyberopération et, de l'autre côté, le principe de souveraineté, et analyse les motivations géopolitiques qui la sous-tendent.

IRSEM, École militaire
1, place Joffre, case 38 - 75700 Paris SP 07
irsem.fr

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE