L'ONU, la cybersécurité et la lutte contre la cybercriminalité : le difficile consensus

Karine Bannelier-Christakis

L'ONU, la cybersécurité et la lutte contre la cybercriminalité : le difficile consensus

Karine BANNELIER,
Maître de conférence HDR en droit international, Directrice du Grenoble Alpes Cybersecurity Institute

Marc Watin-Augouard
Général d'Armée (2S),
fondateur du Forum InCyber

NOVEMBRE 2025

agora
INCYBER FORUM

INTRO-DUCTION

Le cyberespace étant par nature international, l'Organisation des Nations Unies aurait pu tenir les rênes de sa gouvernance, à partir du moment où la transformation numérique prenait une dimension mondiale.

Mais, dans les premières décennies de son développement, internet est resté dans la main des États-Unis, des *majors* de la Silicon Valley. Ensemble, ils ont imposé la norme technique qui précède la norme juridique et la norme politique. Comme la plupart des États, l'ONU est restée en retrait, au moins jusqu'en 1998.

Cette année-là, selon la Résolution 73 de la Conférence de plénipotentiaires de l'Union internationale des Télécommunications (UIT), institution spécialisée de l'ONU, la tenue d'un Sommet mondial sur la société de l'information (SMSI) est décidée. Il comprend deux phases : l'une à Genève (2003) et l'autre à Tunis (2005). L'objectif est d'édifier « une société de l'information à dimension humaine, inclusive et privilégiant le développement, une société de l'information, dans laquelle chacun ait la possibilité de créer, d'obtenir, d'utiliser et de partager l'information et le savoir et dans laquelle les individus, les communautés et les peuples puissent ainsi mettre en œuvre toutes leurs potentialités en favorisant leur développement durable et en améliorant leur qualité de vie, conformément aux buts et aux principes de la Charte des Nations Unies ainsi qu'en respectant pleinement et en mettant en œuvre la Déclaration universelle des droits de l'homme ». Le Sommet affirme le concept de l'universalité de l'Internet ainsi que les principes d'ouverture, d'accessibilité et de participation d'acteurs multiples sur lesquels repose un Internet respectant les droits de l'homme. De son côté, l'UNESCO exerce un rôle de chef de file dans la mise en œuvre de six des onze grandes orientations du SMSI, à savoir l'accès à l'information et au savoir, le téléenseignement, la cyberscience, la diversité culturelle et linguistique, les médias et les dimensions éthiques de la société de l'information et du savoir, en faisant de l'égalité des sexes une priorité transversale. En 2025, l'Assemblée générale de l'ONU examinera les résultats du SMSI+20 (vingt ans après le premier sommet).

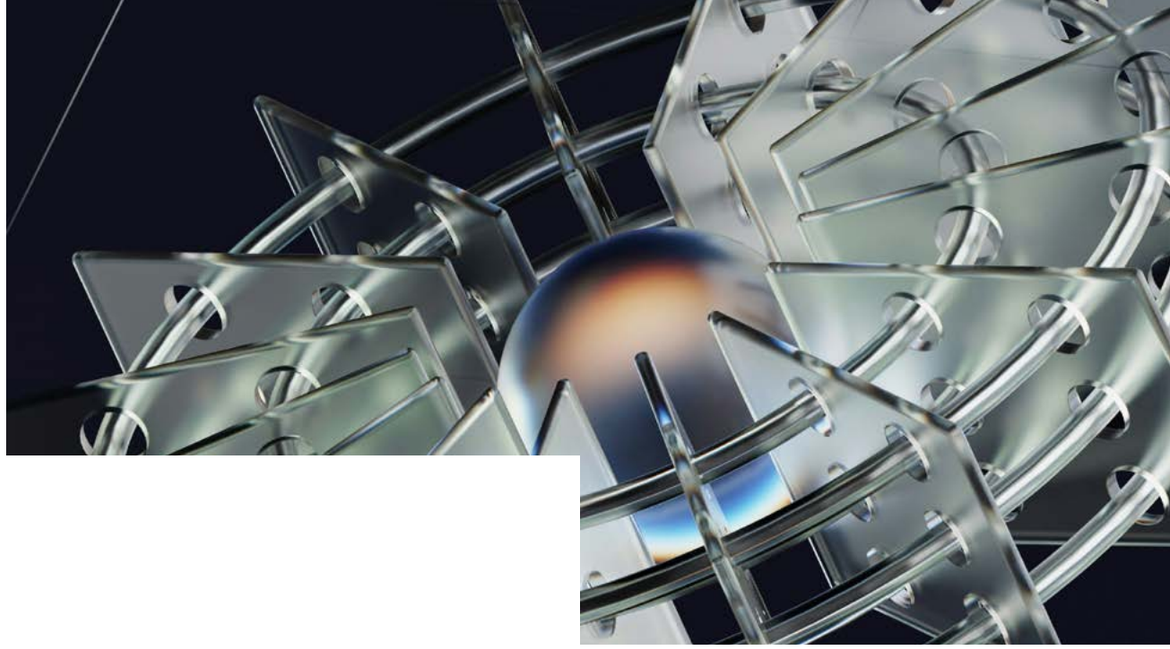
S'agissant de la cybersécurité - dont la définition donnée par l'ANSSI est un état, résultat de la sécurité des systèmes d'information, de la lutte contre la cybercriminalité et de la cyberdéfense - une résolution prise la même année à l'initiative de la Fédération de Russie marque le commencement d'une démarche collective qui connaît des succès variables, voire des échecs. Les travaux des groupes d'experts gouvernementaux (GGE), des groupes de travail à composition non limitée sur la sécurité des technologies de l'information et de la communication (GTCNL/ *Open Ended Working Group* - OEWG), la prise en main de la cybersécurité par le Conseil de sécurité et les négociations relatives à une convention des Nations Unies contre la cybercriminalité soulignent la volonté de l'ONU de contribuer au développement d'un espace numérique régulé et pacifié, au moment où les tensions internationales se manifestent notamment par des cyberattaques de plus en plus violentes dans leurs effets.

KARINE BANNELIER
Maître de Conférence HDR en droit international, directrice du Grenoble Alpes Cybersecurity Institute, directrice du Master Sécurité internationale, cybersécurité et défense de l'université de Grenoble

MARC WATIN-AUGOUARD, GÉNÉRAL D'ARMÉE (2S)
Fondateur du Forum InCyber (FIC), président de l'Agora

PARTIE I
L'ONU et la cybersécurité

PARTIE II
Une convention des Nations Unies contre la cybercriminalité : quelles obligations et quelles garanties pour quels crimes ?



SOMMAIRE

Introduction 01

PARTIE I : L'ONU et la cybersécurité.
Les GGE issus de la résolution du 4 décembre 1998 02

PARTIE II : Une convention des Nations Unies contre la cybercriminalité : quelles obligations et quelles garanties pour quels crimes ? 16

Conclusion 26

PARTIE I

L'ONU ET LA CYBERSÉCURITÉ. LES GGE ISSUS DE LA **RÉSOLUTION DU 4 DÉCEMBRE 1998**

La Résolution A/RES/ 53/70 AG du 4 décembre 1998, relative aux progrès de la téléinformatique dans le contexte de la sécurité internationale, est une initiative de la Fédération de Russie. L'ONU invite les États membres à partager leurs points de vue sur « l'opportunité d'élaborer des principes internationaux qui renforceraient la sécurité des systèmes mondiaux d'information et de télécommunications et contribueraient à lutter contre le terrorisme de l'information et la criminalité ».

Cette résolution est à l'origine de la création des groupes d'experts gouvernementaux sur la cybersécurité. Quinze États participent au premier qui, faute de consensus, ne permet pas l'adoption, en 2004, d'un rapport. Les participants se déclarent « vaincus par la complexité ».

À ce premier GGE succède un second, créé en 2009. Celui-ci débouche sur un rapport (A/65/201) soulignant que les risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information figurent parmi les problèmes les plus graves du XXIe siècle. L'utilisation des TIC pour des activités perturbatrices est de plus en plus le fait d'États qui développent des techniques informatiques comme instruments de guerre et de renseignement, ainsi qu'à des fins politiques. Le rapport ajoute au constat que des personnes, des groupes ou des organisations, notamment criminelles, agissant pour le compte d'autrui, exécutent des activités perturbatrices en ligne, suscitent une inquiétude croissante. La complexité et la portée de plus en plus étendue des activités criminelles accroissent les possibilités d'actes pernicieux. Même si on n'a guère d'indices d'une utilisation des TIC pour des opérations de perturbation à des fins terroristes, cette éventualité pourrait devenir plus réelle à l'avenir. La question de l'attribution se pose : « Il peut être difficile d'établir l'origine d'un acte perturbateur, l'identité de son auteur ou sa motivation. Souvent, ce n'est qu'à partir de la cible, des conséquences ou d'autres éléments indirects que l'on peut déduire l'identité de l'auteur, qui peut agir depuis pratiquement n'importe quel lieu ». Le rapport appelle les États à collaborer entre eux et avec le secteur privé et la société civile. Une large coopération internationale est indispensable pour que les mesures visant à améliorer la sécurité de l'information soient efficaces. Parmi les recommandations, très générales dans leur formulation, le GGE préconise d' « adopter des mesures de confiance, de stabilité et de réduction des risques qui répondent aux conséquences de l'utilisation des TIC par les États, avec notamment des échanges de vues entre pays sur l'utilisation des TIC dans les conflits », de développer les échanges d'informations sur les législations et stratégies nationales ; d'élaborer des termes et des définitions communs liés à la sécurité de l'information ; de renforcer les capacités dans les pays les moins avancés.

Plus intéressant est le rapport du 3e GGE (A/68/98 du 24 juin 2013). S'inscrivant dans la continuité des travaux du précédent groupe d'experts, il considère que le droit international et, en particulier, la Charte des Nations Unies sont applicables et essentiels au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement informatique ouvert, sûr, pacifique et accessible. Cette reconnaissance est très importante, car la création d'un droit *sui generis,* propre au cyberespace, était initialement imaginée, dans la mesure où certains considéraient le cyberespace comme un espace qui n'était pas régulé par le droit international. Le rapport considère néanmoins nécessaire de s'entendre sur la façon dont les normes découlant du droit international s'appliquent aux États et à l'utilisation qu'ils font des outils informatiques.

Le rapport souligne notamment que « les États sont tenus d'honorer leurs obligations internationales quant aux faits internationalement illicites qui leur sont imputables. Ils s'interdisent d'utiliser leurs agents pour commettre de tels actes et veillent à ce que des agents non étatiques n'utilisent pas leur territoire pour faire un usage illégal des outils informatiques ». Cette dernière mention renvoie à l'application dans l'espace numérique d'un principe cardinal du droit international découlant de la souveraineté des États, à savoir le principe de due diligence, tel qu'exprimé par la jurisprudence de la Cour internationale de justice (notamment dans l'Affaire du Détroit de Corfou-1949).

Le succès des travaux du 3e GGE intervient après l'échec du sommet de l'Union Internationale des Télécommunications (UIT).

Le sommet, à Dubaï (2012), avait pour objectif la révision du Traité portant Règlement des Télécommunications internationales (RTI) issu de la Conférence administrative télégraphique et téléphonique internationale de Melbourne (CAMTT-24/11- 9/12 1988). À cette occasion se manifeste la coupure en deux blocs : celui qui derrière la Russie, la Chine, l'Arabie Saoudite, l'Iran, veut une gouvernance sur l'internet et celui qui rassemble les occidentaux, lesquels veulent défendre une gouvernance de l'internet conforme aux principes démocratiques. Les premiers veulent un contrôle des contenus sous prétexte de sauvegarder la sécurité nationale. Les pays occidentaux craignent de voir l'UIT et donc Internet dirigée par une majorité de pays non démocratiques. Ainsi, selon le communiqué officiel, la France n'a « pas pu se rallier au texte adopté par la conférence, car certaines dispositions du nouveau traité sont susceptibles d'être interprétées comme une remise en cause des principes fondant notre position et celle des pays européens sur l'Internet».

Cette profonde divergence est toujours d'actualité et est sans doute encore renforcée, de nos jours, en raison de l'invasion russe en Ukraine qui bénéficie du soutien des États totalitaires. Elle n'empêche pas cependant la constitution d'un cinquième GGE qui aboutit à un rapport de consensus, en 2015. Le rapport (A/70/174) confirme l'applicabilité du droit international et, notamment, de la Charte des Nations Unies, telle qu'elle était affirmée dans le rapport de 2013. Il liste onze normes volontaires et non contraignantes de comportement responsable des États dans le cyberespace. Les États sont appelés à s'abstenir d'utiliser des TIC d'une manière que ne serait pas conforme à ces normes. Le GGE 2015 approfondit la notion d'applicabilité du droit international. La Charte et le droit international impliquent que les États respectent les principes suivants :

— Égalité souveraine

— règlement des différends internationaux par des moyens pacifiques, de telle manière que la paix et la sécurité internationales ainsi que la justice ne soient pas mises en danger

— abstention, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies

— respect des droits de l'homme et des libertés fondamentales et non-intervention dans les affaires intérieures d'autres États

Par sa résolution du 23 décembre 2015 (A/RES/70/237), l'Assemblée générale crée un nouveau GGE. Puisque les GGE de 2013 et de 2015 ont acté le principe de l'applicabilité du droit international dans le cyberespace, la résolution invite ce nouveau groupe à poursuivre « l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité informatique et des mesures collectives qui pourraient être prises pour y parer, de la manière dont le droit international s'applique à l'utilisation de l'informatique et des technologies des communications par les États, ainsi que des normes, règles et principes de comportement responsable des États, des mesures de confiance et de renforcement des capacités ». Il faut donc maintenant entrer dans la « granularité » du droit international et répondre à la question « comment ? ».

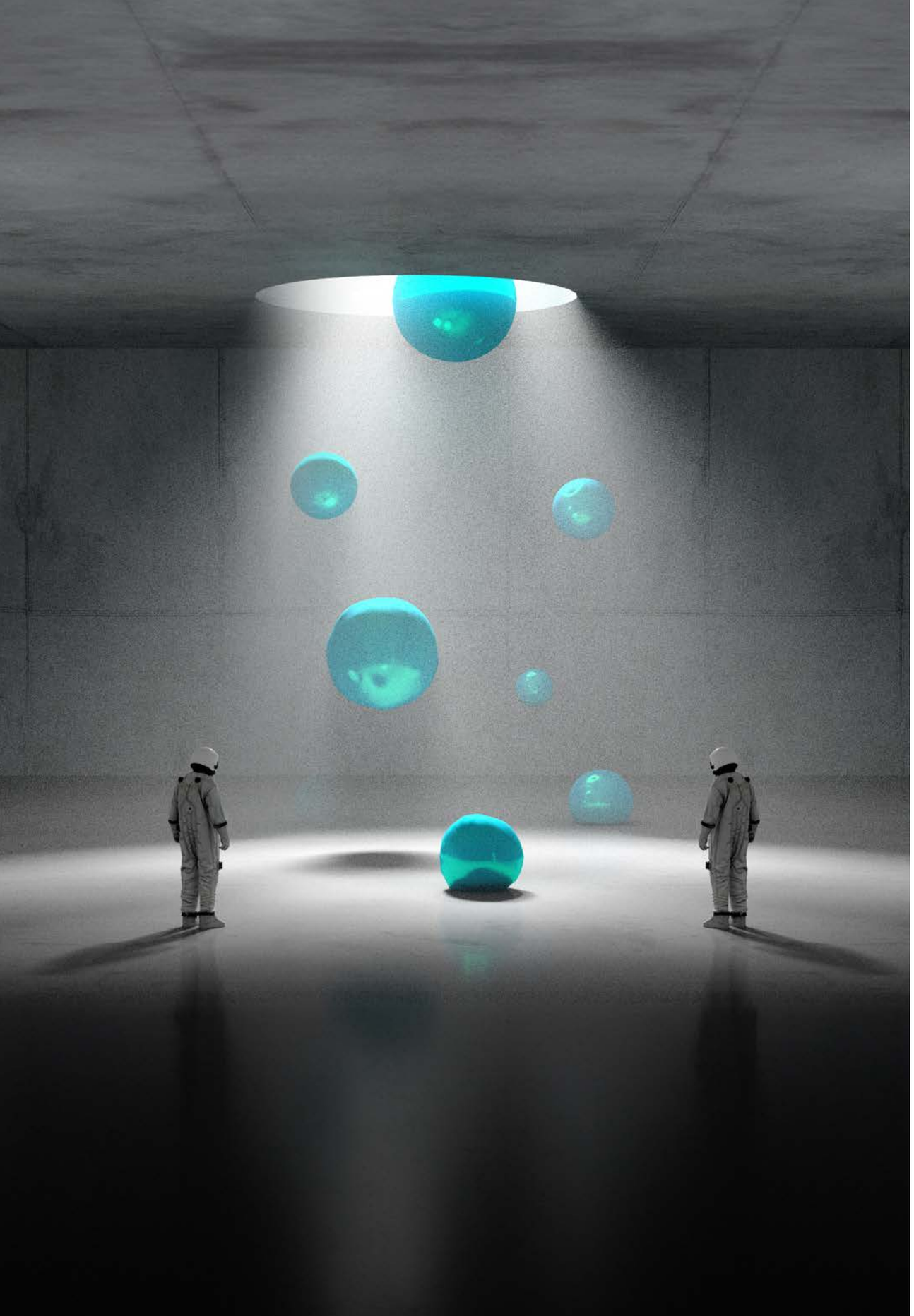
En 2017, dans un contexte tendu (attaques Wanacry, NotPeytia) le Groupe d'experts gouvernementaux ne parvient pas à publier un rapport consensuel, car les experts gouvernementaux se montrent divisés. Plus on entre dans le détail, plus les oppositions se manifestent. Trois questions principales semblent constituer des points d'achoppement :

— La question de l'application de contre-mesures et de sanctions par des États victimes de cyber-attaques. Cela n'est pas du goût de ceux qui craignent que leurs actions ne débouchent sur des ripostes. Selon Cuba une telle reconnaissance consisterait à légitimer certaines actions punitives

— Comment le droit humanitaire international doit-il s'appliquer au cyberespace ? Cuba, en particulier, s'oppose à l'équivalence entre l'utilisation malveillante des TIC et la notion d'attaque armée. Certains États craignent, en effet, une réaction de la victime, ce qui est en soi un aveu. La Chine fait valoir que l'application du droit international humanitaire au cyberespace légitimerait les opérations militaires dans le cyberespace

— Une cyberattaque remplit-elle les critères d'une attaque armée, permettant de mettre en œuvre le principe de légitime défense ? La Fédération de Russie, la Chine et Cuba estiment que l'article 51 de la Charte des Nations Unis, octroyant aux États un droit naturel à la légitime défense, ne doit pas pouvoir s'appliquer au cyberespace. Pour ces États, une telle reconnaissance entraînerait une militarisation du cyberespace, argument fallacieux au regard de leur comportement habituel

L'échec du GGE motive sans doute les décisions de l'Assemblée générale à la fin de l'année 2018 qui illustrent bien le clivage entre deux conceptions du cyberespace.



La **concurrence** entre groupes d'experts gouvernementaux et groupes de travail à composition non limitée

Sur une proposition des États-Unis, il est décidé de constituer un nouveau GGE (2019-2021). La résolution 73/266 « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale », adoptée par l'Assemblée générale le 22 décembre 2018, est soutenue par les États occidentaux, mais aussi par d'autres États, notamment l'Inde, l'Argentine et l'Afrique du Sud.

Quelques jours auparavant, le 5 décembre 2018, sur l'initiative de la Fédération de Russie, une autre résolution est adoptée (A/RES/73/27) qui crée un Groupe de travail à composition non limitée (GTCNL/*Open Ended Working Group* - OEWG) intitulé *Progrès de l'informatique et des télécommunications et sécurité internationale*. Votent en faveur de cette résolution la Russie, la Chine, l'Iran, Cuba, matérialisant ainsi le bloc qui s'est constitué lors de la Conférence de Dubaï. Mais se joignent également à l'initiative des États comme l'Inde, l'Argentine, l'Afrique du Sud qui ont également été favorables à la constitution du GGE. Ce n'est pas de l'inconséquence, mais l'espoir d'une solution plus rapide avec des groupes concurrents. La divergence qui peut sembler naître de ces résolutions n'est qu'apparente. Tout d'abord, l'Assemblée générale reprend les « acquis » des GGE précédents dans la résolution créant le GTCNL/OEWG (2019-2020). Le texte de la résolution est particulièrement explicite : « Confirmant la conclusion à laquelle est parvenu le Groupe d'experts gouvernementaux dans ses rapports de 2013 et 2015, à savoir que le droit international, et en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique, que la mise en place, sur une base facultative et non contraignante, de normes, règles et principes de comportement responsable des États en matière d'utilisation du numérique peut réduire les risques pesant sur la paix, la sécurité et la stabilité internationales et que, compte tenu de la spécificité du numérique, de nouvelles normes pourraient être progressivement élaborées [...] Décide, en vue de rendre le processus de négociation de l'Organisation des Nations Unies sur la sécurité d'utilisation du numérique plus démocratique, inclusif et transparent, de constituer à partir de 2019 un groupe de travail à composition non limitée qui 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 par 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 ; d'étudier la possibilité d'instaurer un dialogue institutionnel régulier aussi large que possible sous l'égide de l'Organisation des Nations Unies ».

PRINCIPES RETENUS PAR L'ASSEMBLÉE GÉNÉRALE DE L'ONU

RÉSOLUTION AG A/RES/73/27 DU 5 DÉCEMBRE 2018

1. Conformément aux buts des Nations Unies, notamment le maintien de la paix et de la sécurité internationales, les États coopèrent à l'élaboration et à l'application de mesures visant à accroître la stabilité et la sécurité d'utilisation des technologies numériques, et à prévenir les pratiques numériques jugées nocives ou susceptibles de compromettre la paix et la sécurité internationales.

2. Les États remplissent leurs obligations internationales quant aux faits internationalement illicites qui leur sont imputables en droit international. Toutefois, le signe qu'une activité numérique a été lancée depuis le territoire ou les infrastructures numériques d'un État ou y trouve son origine peut être insuffisant à lui seul pour imputer l'activité en question à cet État. Les accusations concernant l'organisation et l'exécution d'actes illicites portées contre des États doivent être étayées. En cas de problème, les États examinent toutes les informations pertinentes, y compris le contexte plus large de l'événement, la difficulté de déterminer les responsabilités dans le domaine du numérique et la nature et l'ampleur des conséquences.

3. Les États ne permettent pas sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies numériques. Ils ne font pas appel à des intermédiaires pour commettre des faits internationalement illicites à l'aide des technologies numériques et veillent à ce que des acteurs non étatiques n'utilisent pas leur territoire pour commettre de tels actes.

4. Les États réfléchissent à la meilleure façon de coopérer pour échanger des informations, s'entraider et engager des poursuites en cas d'utilisation terroriste ou criminelle des technologies numériques et à la meilleure façon d'appliquer d'autres mesures collectives afin de parer à ces risques. Ils seront peut-être amenés à réfléchir à l'opportunité d'élaborer de nouvelles mesures dans ce domaine.

5. Les États, lorsqu'ils veillent à une utilisation sûre des technologies numériques, respectent les résolutions 20/8 et 26/13 du Conseil des droits de l'homme, en date du 5 juillet 20124 et du 26 juin 20145 , sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, ainsi que les résolutions 68/167 et 69/166 sur le droit à la vie privée à l'ère du numérique afin de garantir le plein respect des droits de l'homme, y compris le droit à la liberté d'expression, qu'elle a adoptées l'une le 18 décembre 2013 et l'autre le 18 décembre 2014.

6. Un État ne mène ni ne soutient sciemment une activité numérique qui est contraire aux obligations qu'il a contractées en vertu du droit international et qui endommage intentionnellement des infrastructures essentielles ou qui compromet l'utilisation et le fonctionnement d'infrastructures essentielles à la fourniture de services au public.

7. Les États prennent les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies numériques en tenant compte de sa résolution 58/199 du 23 décembre 2003 sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information et d'autres résolutions.

8. Les États répondent aux demandes d'aide que leur adressent d'autres États dont des infrastructures essentielles sont exposées à des actes de malveillance numérique, sous réserve que ces demandes soient justifiées. Ils donnent également suite aux demandes visant à atténuer les conséquences d'activités numériques malveillantes dirigées contre des infrastructures essentielles d 'un autre État qui sont exercées depuis leur territoire, en tenant dûment compte du principe de souveraineté.

9. Les États prennent des mesures raisonnables pour garantir l'intégrité de la chaîne d'approvisionnement, de sorte que les utilisateurs finaux puissent avoir confiance dans la sécurité des produits numériques.

10. Les États s'attachent à prévenir la prolifération des techniques et des outils numériques malveillants et l'utilisation furtive de fonctionnalités néfastes.

11. Les États encouragent le signalement responsable des failles numériques et se communiquent des informations sur les moyens de les corriger afin de limiter voire d'éliminer les risques potentiels pour les systèmes et les infrastructures qui utilisent les technologies numériques ou en dépendent.

12. Les États s'abstiennent de mener ou de soutenir sciemment des activités visant à endommager les systèmes informatiques des équipes d'intervention d'urgence agréées (équipes d'intervention informatique d'urgence ou équipes d'intervention en cas d'atteinte à la sécurité du cyberespace) d'un autre État. Un État ne doit pas se servir d'équipes d'intervention d'urgence agréées pour se livrer à des actes de malveillance au niveau international.

13. Les États incitent le secteur privé et la société civile à s'associer au renforcement de la sécurité numérique et à l'utilisation des technologies numériques, y compris pour ce qui est de la sécurité de la chaîne d'approvisionnement en produits et services numériques et coopèrent avec eux afin de mieux leur faire comprendre la manière dont ils peuvent faciliter l'application de règles de comportement responsable dans le cyberespace.

La résolution 73/266 est rédigée en des termes similaires : « Réaffirmant la conclusion à laquelle parvient le Groupe d'experts gouvernementaux dans ses rapports de 2013 et 2015, à savoir que le droit international, et en particulier la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement ouvert, sûr, stable, accessible et pacifique en matière de technologies de l'information et des communications, que la mise en place, sur une base facultative et non contraignante, de normes, règles et principes de comportement responsable des États en matière d'utilisation de ces technologies peut réduire les risques pesant sur la paix, la sécurité et la stabilité internationales et que, compte tenu de la spécificité de ces technologies, de nouvelles normes pourraient être progressivement élaborées, Réaffirmant également la conclusion du Groupe d'experts gouvernementaux selon laquelle les mesures de confiance volontaires peuvent aider à promouvoir la confiance entre les États et à réduire le risque de conflit en augmentant la prévisibilité et en limitant les malentendus, et ainsi contribuer largement à répondre aux préoccupations des États concernant l'utilisation qu'ils font des technologies de l'information et des communications et marquer une avancée importante dans la promotion de la sécurité internationale, réaffirmant en outre la conclusion du Groupe d'experts gouvernementaux selon laquelle il est également essentiel pour la sécurité internationale d'aider à renforcer les capacités dans le domaine de la sécurité informatique, en renforçant les capacités des États en matière de coopération et d'action collective et en encourageant l'utilisation des technologies de l'information et des communications à des fins pacifiques [...] ».

Les deux groupes s'appuient donc sur une base commune. Leurs mandats ne sont pas formulés en des termes identiques, mais poursuivent les mêmes objectifs. Pour le GGE : « l'examen des mesures collectives qui pourraient être prises pour parer aux risques qui se posent ou pourraient se poser dans le domaine de la sécurité informatique, et notamment des normes, règles et principes de comportement responsable des États, des mesures de confiance et de renforcement des capacités et de la manière dont le droit international s'applique à l'utilisation des technologies de l'information et des communications par les États, en vue de définir une vision commune et de l'appliquer efficacement ». Le GNCTL, quant à lui, a pour mission de « poursuivre l'élaboration, à titre prioritaire, des règles, normes et principes de comportement responsable des États visés par 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 ; d'étudier la possibilité d'instaurer un dialogue institutionnel régulier aussi large que possible sous l'égide de l'Organisation des Nations Unies ».

Tandis que le GGE rassemble 25 États, le GTCNL est ouvert à tous les États membres de l'ONU et associe, dans la mesure du possible, à la réflexion les parties intéressées du secteur privé, du monde universitaire et de la société civile qui peuvent ainsi exprimer leurs points de vue sur les questions discutées.

> [...] la Charte des Nations Unies, est applicable et essentiel au maintien de la paix et de la stabilité ainsi qu'à la promotion d'un environnement numérique ouvert, sûr, stable, accessible et pacifique.

Groupe de travail à composition non limitée 2019-2020

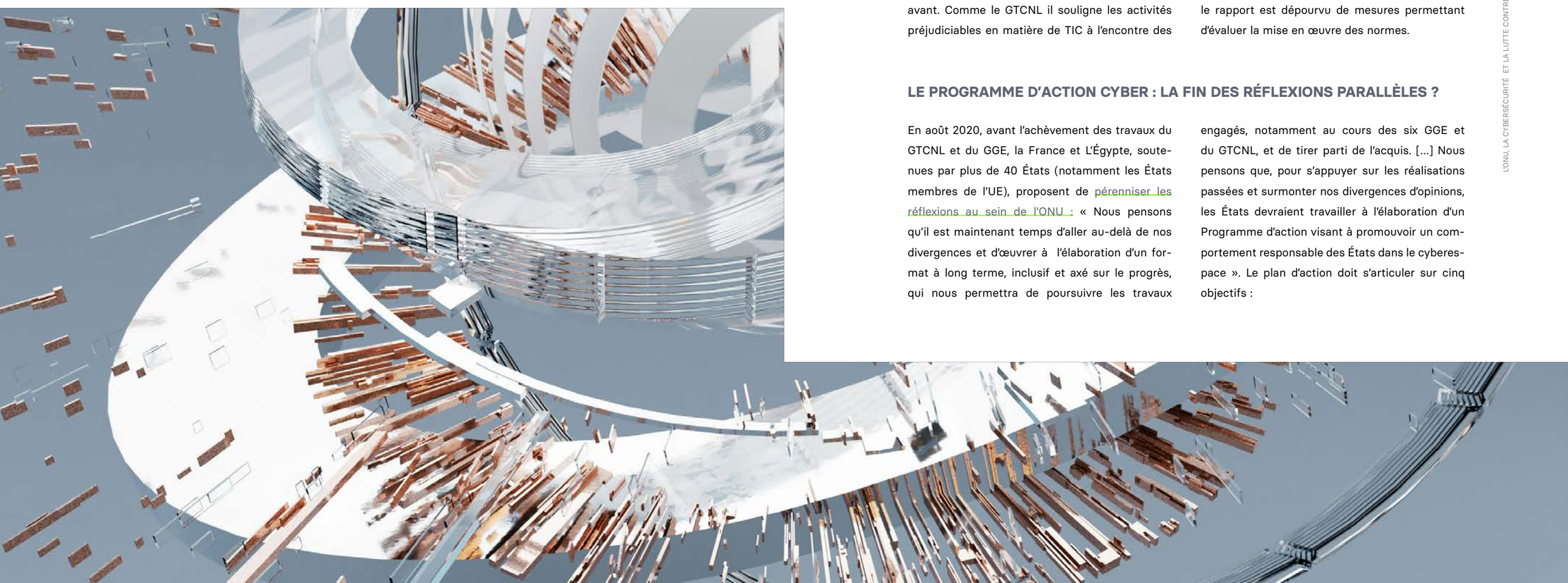
Le GTCNL/OEWG est le premier à publier un rapport de consensus (A/AC.290/2021/CRP du 10 mars 2021).

S'appuyant sur les travaux des GGE précédents, il précise que les normes ne remplacent ni ne modifient les obligations ou les droits des États en vertu du droit international, qui sont contraignants, mais fournissent plutôt des orientations spécifiques supplémentaires sur ce qui constitue un comportement responsable d'un État dans l'utilisation des TIC. Les États ne devraient pas mener ou soutenir sciemment des activités dans le domaine des TIC, contraires à leurs obligations en vertu du droit international, qui endommagent intentionnellement des infrastructures critiques ou entravent d'une autre manière l'utilisation et le fonctionnement d'infrastructures critiques pour fournir des services au public. En outre, les États devraient continuer à renforcer les mesures visant à protéger toutes les infrastructures critiques contre les menaces liées aux TIC et à intensifier les échanges sur les meilleures pratiques en matière de protection des infrastructures critiques. Ils doivent chercher à prévenir la prolifération d'outils et de techniques informatiques malveillants et l'utilisation de fonctions cachées nuisibles et encourager le signalement responsable des vulnérabilités.

Le rapport propose des mesures de confiance, le renforcement des capacités, la possibilité d'établir un dialogue institutionnel régulier avec une large participation sous les auspices de l'ONU. Les résultats sont modestes, sans doute pour aboutir à un consensus. Les mesures de transparence, de coopération et de stabilité peuvent contribuer à prévenir les conflits, à éviter les perceptions erronées et les malentendus, et à réduire les tensions. Parmi ces mesures, les États recommandent la mise en place de points de contact nationaux, « mesure utile pour la mise en œuvre de nombreuses autres mesures de confiance et inestimable en temps de crise ».

Dans ses efforts pour parvenir à un consensus et promouvoir la paix, la sécurité, la coopération et la confiance internationales, le GTCNL aurait dû consacrer une partie de ses propositions à la responsabilité, c'est-à-dire à un mécanisme permettant de demander des comptes aux États pour leurs actions en matière de cybersécurité, une sorte de « cyberexamen par les pairs », comme l'a proposé la fondation ICT4Peace. Le consensus est sans doute davantage un rapport de compromis qui satisfait a minima toutes les parties prenantes. Il exprime aussi une volonté de continuer à travailler ensemble.

Avant la remise du rapport du GTCNL, la résolution 75/240 du 31 décembre 2020 décide de constituer, à partir de 2021 et sous l'égide de l'Organisation des Nations Unies, un nouveau groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) qui sera chargé, sur la base du consensus de veiller à ce que le processus de négociation démocratique, inclusif et transparent sur la sécurité d'utilisation du numérique se poursuive de manière ininterrompue.



Le 6e groupe d'experts **gouvernementaux**

Le Groupe d'experts gouvernementaux publie son rapport (A/76/135 du 14 juillet 2021) quatre mois après celui du GTCNL.

Le GGE réaffirme l'applicabilité du droit international, et en particulier de la Charte des Nations Unies dans son intégralité, à l'environnement des TIC. C'est un progrès très important, car l'échec du GGE 2017 résultait notamment d'un désaccord sur l'applicabilité de l'article 51 de la Charte. Le groupe précise que le droit international humanitaire ne s'applique qu'aux situations de conflit armé. Toutefois, l'application aux TIC des principes juridiques internationaux établis, notamment les principes d'humanité, de nécessité, de proportionnalité et de distinction, doit être étudiée plus avant. Comme le GTCNL il souligne les activités préjudiciables en matière de TIC à l'encontre des infrastructures critiques. Il constate une augmentation de l'utilisation malveillante par les États de campagnes d'information secrètes basées sur les TIC pour influencer les processus, les systèmes et la stabilité globale d'un autre État. Si les normes et le droit international existant se côtoient, les normes reflètent les attentes de la communauté internationale et établissent des principes pour un comportement responsable des États. D'autres normes pourraient être élaborées au fil du temps et, le cas échéant, d'autres obligations contraignantes pourraient être élaborées à l'avenir. Mais le rapport est dépourvu de mesures permettant d'évaluer la mise en œuvre des normes.

LE PROGRAMME D'ACTION CYBER : LA FIN DES RÉFLEXIONS PARALLÈLES ?

En août 2020, avant l'achèvement des travaux du GTCNL et du GGE, la France et L'Égypte, soutenues par plus de 40 États (notamment les États membres de l'UE), proposent de pérenniser les réflexions au sein de l'ONU : « Nous pensons qu'il est maintenant temps d'aller au-delà de nos divergences et d'œuvrer à l'élaboration d'un format à long terme, inclusif et axé sur le progrès, qui nous permettra de poursuivre les travaux engagés, notamment au cours des six GGE et du GTCNL, et de tirer parti de l'acquis. [...] Nous pensons que, pour s'appuyer sur les réalisations passées et surmonter nos divergences d'opinions, les États devraient travailler à l'élaboration d'un Programme d'action visant à promouvoir un comportement responsable des États dans le cyberespace ». Le plan d'action doit s'articuler sur cinq objectifs :

- Créer un cadre et un engagement politique basés sur des recommandations, des normes et des principes déjà convenus
- Organiser régulièrement des réunions de travail, axées sur la mise en œuvre -Intensifier la coopération et le renforcement des capacités
- Organiser régulièrement des conférences de révision pour s'assurer que le Plan d'action est toujours parfaitement adapté aux besoins et aux menaces
- Organiser des consultations avec d'autres parties prenantes (entreprises privées, ONG, société civile…), des organisations régionales, des représentants d'autres processus de l'ONU, et des initiatives multipartites pertinentes traitant des questions liées à la cybersécurité dans le contexte de la sécurité internationale

Le 23 septembre 2022, la France et l'Allemagne organisent une réunion ministérielle, à l'occasion de la semaine de haut niveau de la 77e session de l'Assemblée générale des Nations Unies, sur le thème « Structurer la cybersécurité mondiale : Appel à l'action pour le développement d'un comportement étatique responsable et le renforcement des capacités de mise en œuvre ». Les États participant à l'événement accueillent favorablement la proposition visant à établir un Programme d'action des Nations Unies (PoA) pour un comportement étatique responsable dans l'utilisation des technologies de l'information et de la communication (TIC) en matière de sécurité internationale. Le 13 octobre 2022, la délégation française dépose un projet de résolution intitulé « Programme d'action destiné à promouvoir le comportement responsable des États en matière d'utilisation du numérique dans le contexte de la sécurité internationale » (A/C.1/77/L.73) qui précise que cette proposition est également formulée par le groupe de travail à composition non limitée (2021-2025) dans son premier rapport d'activité annuel. Le principe d'un Programme d'action est retenu par la Résolution adoptée par l'Assemblée générale le 7 décembre 2022 (A/RES/77/37). Après avoir été approuvée par la 1ère Commission, la résolution pour un programme d'action à l'ONU (A/C.1/78/L.60/Rev.1 du 24 octobre 2023), portée par la France avec la Colombie et les États-Unis, est adoptée par l'Assemblée générale, le 4 décembre 2023, à une majorité de 158 États. Le projet de résolution concurrent, porté par la Russie (A/C.1/78/L.11 du 12 octobre 2023), bénéficie de 112 voix favorables et est lui aussi adopté. Comme pour la création simultanée du GGE et du GTCNL, en 2018, de nombreux États votent pour les deux résolutions.

Aux travaux de l'Assemblée générale s'ajoutent à partir de 2021 les réunions *ad hoc* du Conseil de sécurité.

LE CONSEIL DE SÉCURITÉ S'APPROPRIE LA CYBERSÉCURITÉ

Le 29 juin 2021, le Conseil de sécurité tient son premier débat formel sur la cybersécurité et les risques liés à l'utilisation malveillante des nouvelles technologies. La présidence estonienne est à l'origine de cette initiative. La pandémie du Covid-19 touche à sa fin. Les confinements successifs ont favorisé une croissance très forte des cyberattaques. Intervient devant le Conseil la Haute-Représentante pour les affaires de désarmement Mme Izumi Nakamitsu, ce qui souligne, comme elle le rappelle, que ces cyberattaques ouvrent de nouveaux domaines potentiels de conflit. Ces incidents, dit-elle, contribuent à une diminution de la confiance entre les États, présentent en outre un risque spécifique pour les infrastructures critiques rendues possibles par les TIC, tels que le secteur financier, les réseaux électriques et les installations nucléaires. Franck Riester, ministre délégué auprès du Ministre de l'Europe et des affaires étrangères de la France, soutient la légitimité de l'intervention du Conseil de sécurité qui doit « pouvoir veiller à la paix et la sécurité dans le cyberespace qui est devenu un terrain de compétition stratégique entre puissances et où les usages malveillants des TIC, par des acteurs étatiques comme non étatiques, prolifèrent, notamment dans le contexte de la pandémie de Covid-19 qui a accentué notre dépendance à ces technologies ». Mais la Russie n'est pas de cet avis. Pour elle, les discussions sur l'application du droit international dans le cyberespace sont loin d'être achevées ; l'organe idoine pour ces discussions est l'Assemblée générale. Elle défend évidement les travaux du GTCNL/OEWG dont elle est l'inspiratrice.

Trois ans plus tard, le 20 juin 2024, le Conseil de sécurité débat du renforcement de son rôle dans la lutte contre les cybermenaces et la sécurisation du cyberespace. Un débat est organisé avec l'intervention de plus de 70 délégations. António Guterres, Secrétaire général, rappelle les dangers des cyberactivités malveillantes qui sont le fait d'acteurs aussi bien étatiques que non étatiques, mais aussi de criminels, et l'instrumentalisation croissante des cyberattaques à des fins hostiles. Ce débat, une fois de plus, met en lumière les clivages au sein de l'ONU. Tandis qu'une majorité de délégations invite le Conseil à jouer son rôle en incitant à établir des normes et des cadres internationaux pour un comportement responsable des États dans le cyberespace, la Russie relance la question du bien-fondé de l'inscription de cette question à l'ordre du jour du Conseil, jugeant qu'elle devrait être débattue dans le cadre de plateformes spécialisées disposant de l'expertise nécessaire afin d'éviter toute politisation. « Tant que le problème de l'attribution des cyberattaques n'aura pas été résolu, toute discussion au sein du Conseil risque de se transformer en un nouvel échange d'accusations non prouvées et de conduire à un clivage plus profond au sein de la communauté internationale », selon les propos de son représentant. La République de Corée et la Slovénie jouent les modérateurs en saluant les travaux en cours du GTCNL (2021-2025) et en estimant que le Conseil pourrait jouer un rôle complémentaire en examinant les cyberactivités malveillantes de manière plus approfondie.

CONCLUSION

Depuis 1998 au moins, l'ONU s'empare du sujet de la cybersécurité. L'évolution de la menace le justifie. Ses impacts dépassent les limites de la cybercriminalité classique pour affecter la paix dans le monde. Mais la communauté internationale est trop clivée pour pouvoir aboutir à des résultats immédiats. Les laborieuses recherches de consensus des groupes de travail en témoignent. L'opposition entre deux blocs est une constante depuis que l'ONU a attrait les questions relatives à la gouvernance de l'internet (cf. l'échec du Sommet de Dubaï en 2012) et à la cybersécurité. Les négociations relatives à un traité international sur la cybercriminalité, engagées sur l'initiative de la Russie, sont terminées. Le projet de convention doit être soumis au vote de l'Assemblée générale, lors de sa 79e session qui débute en septembre 2024. Là encore, deux conceptions du cyberespace et des droits de l'homme s'opposent.

PARTIE II

UNE CONVENTION DES NATIONS UNIES CONTRE LA CYBERCRIMINALITÉ : QUELLES OBLIGATIONS ET QUELLES GARANTIES POUR QUELS CRIMES ?

Le 8 août 2024, après plus de deux ans de difficiles négociations, les États ont adopté par consensus un projet de convention des Nations Unies contre la cybercriminalité destiné à être soumis pour approbation à l'Assemblée Générale lors de sa prochaine session. Dans un contexte géopolitique particulièrement tendu, l'adoption de cette convention constitue un succès diplomatique indéniable qui témoigne de la capacité de l'ONU et de ses États membres à négocier et à trouver un compromis sur un enjeu crucial où la coopération internationale est indispensable.

Cette convention qui devrait permettre aux États de lutter plus efficacement contre la cybercriminalité[1] mais aussi, comme nous le verrons, contre la criminalité en général ne doit néanmoins pas occulter les nombreuses réticences et divergences qui ont marqué ces négociations ainsi que les inquiétudes que cet instrument peut susciter.

Au cœur des divergences et inquiétudes se trouve une question d'équilibre : comment parvenir à une coopération internationale efficace dans la lutte contre la cybercriminalité et la criminalité en général tout en offrant une protection forte des libertés fondamentales ? Pour nombre d'experts, la coopération internationale dans la lutte contre la cybercriminalité ne peut être efficace qu'à la double condition : celle d'un champ infractionnel délimité et clairement défini et celle de garanties importantes en matière de droits de l'homme et de protection des données personnelles. Un champ infractionnel trop large ou mal défini couplé à des garanties insuffisantes pourrait faire de cette convention un instrument dangereux entre les mains de régimes autoritaires souhaitant l'utiliser pour légitimer leur politique de surveillance de masse et de répression de leur opposants, voire pour exiger des autres États une coopération internationale pour conduire leur politique. Ce qui relève déjà d'un équilibre délicat entre États démocratiques partageant les mêmes valeurs dans le cadre de la Convention de Budapest et de son Protocole 2 constitue une véritable gageure dans un cadre universel où les États ne partagent pas le même niveau de protection en matière de droits de l'homme. Il n'est à cet égard pas certain que le projet de convention finalement adopté ait trouvé cet équilibre et ne puisse pas être instrumentalisé par des régimes autoritaires. L'intitulé même de ce projet (Projet de convention des Nations Unies contre la cybercriminalité. Renforcement de la coopération internationale pour la lutte contre certaines infractions commises aux moyens de systèmes d'information et de communication et pour la communication de preuves sous formes électroniques d'infractions graves) soulève de nombreuses questions quant à ses finalités, finalités qui dépassent largement la lutte contre la cybercriminalité, et le champ de la coopération internationale que celle-ci implique.

> Pour nombre d'experts, la coopération internationale dans la lutte contre la cybercriminalité ne peut être efficace qu'à la double condition : celle d'une champ infractionnel délimité et clairement défini et celle de garanties importantes en matière de droits de l'homme et de protection des données personnelles.

1 Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, *Projet de convention des Nations Unies contre la cybercriminalité. Renforcement de la coopération internationale pour la lutte contre certaines infractions commises aux moyens de systèmes d'information et de communication et pour la communication de preuves sous formes électroniques d'infractions graves,* ONU, Assemblée générale, A/AC. 291/L.15, 7 août 2024.

CONTEXTE :

Un projet controversé

Dès le début, le projet d'une convention des Nations Unies contre la cybercriminalité a été accueilli avec scepticisme par de nombreux États, notamment occidentaux, ainsi que par nombre d'experts et organisations non gouvernementales doutant de la nécessité d'un tel instrument.

Il convient de rappeler à cet égard que c'est à l'initiative de la Russie soutenue par la Chine et six autres États (Biélorussie, Cambodge, République populaire démocratique de Corée, Myanmar, Nicaragua et Venezuela), que le 27 décembre 2019, l'Assemblée Générale des Nations Unies a adopté la résolution 74/247 intitulée « Lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles » dont l'objectif était de négocier une Convention des Nations Unies contre la cybercriminalité.

Cette résolution soulignait que les technologies de l'information et de la communication « peuvent entraîner une augmentation de la criminalité, tant en matière de sévérité que de complexité » et qu'il est donc nécessaire de « renforcer la coordination et la coopération entre les États dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, notamment en fournissant aux pays en développement qui en font la demande une assistance technique ». Pour ce faire, la résolution décidait de créer un Comité *ad hoc* des Nations Unies pour élaborer « une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles ».

Le fait qu'une telle résolution ait été initiée par la Russie, un État souvent accusé d'abriter des cybercriminels de toutes sortes pouvait soulever bien des interrogations quant aux objectifs réels d'une telle démarche et l'existence d'un agenda caché. Sans doute pour cette raison – et d'autres encore, la communauté internationale s'est montrée divisée sur l'opportunité de telles négociations comme en témoigne le vote de la résolution 74/247 adoptée à une très faible majorité de 79 voix pour, la forte opposition de 60 États et 33 abstentions.

Au cours du débat, la Chine et la Russie ont exprimé leur soutien à cette résolution soulignant la nécessité d'adopter une convention qui comblerait un vide juridique et bénéficierait en particulier aux pays en développement[2]. À l'inverse, le représentant des États-Unis a dénoncé un projet qui pourrait étouffer les efforts mondiaux de lutte contre la cybercriminalité[3] et la Finlande (s'exprimant au nom de l'Union européenne) a fait part de son scepticisme rappelant que des négociations organisées en l'absence de consensus créeraient de nouveaux problèmes, seraient très conflictuelles et qu'un traité qui aboutirait dans de telles circonstances aurait des normes limitées, accentuant ainsi la fracture numérique et économique[4].

Les préoccupations des pays occidentaux et plus généralement des États membres de la Convention de Budapest ainsi que de nombreux experts étaient principalement de deux ordres. D'une part, la crainte que l'adoption d'un traité de l'ONU sur la cybercriminalité soit source de fragmentation en raison de l'existence d'autres instruments clés – et en particulier la Convention de Budapest de 2001 du Conseil de l'Europe sur la cybercriminalité. L'hostilité bien connue de la Russie à l'égard de la Convention de Budapest faisait d'ailleurs aussi craindre que cette initiative soit une tentative de concurrencer ou d'affaiblir cet instrument. L'autre crainte était que la convention des Nations Unies puisse être instrumentalisée par des États autoritaires.

Ces inquiétudes ont été renforcées par les activités et positions ultérieures de la Russie qui n'a pas hésité à soumettre à l'ONU, bien en amont des négociations, un projet de convention incluant pas moins de 89 articles. Ce projet soulevait de nombreux problèmes, parmi lesquels un champ infractionnel extrêmement large et mal défini assorti d'importantes obligations de coopération et ceci avec des garanties en matière de protection des libertés fondamentales très insuffisantes voire inexistantes. L'objectif de la publication de ce projet était clairement d'influencer les négociations comme en témoigne une soumission écrite de la Chine soulignant que : *« Un projet de convention globale a également été proposé par un État membre pour fournir une référence importante pour la négociation de la Convention. [5] »*.

Quelques semaines avant l'ouverture des négociations à l'ONU, le projet russe semblait ainsi avoir beaucoup d'influence notamment auprès d'États qui ne sont pas parties à la convention de Budapest et pour lesquels un instrument onusien constituait la promesse de mécanismes de coopération internationale et d'entraide judiciaire dont ils manquaient cruellement. Cependant, lorsque le 28 février 2022 s'est ouverte la première session du Comité *ad hoc* de l'ONU chargé d'élaborer une Convention de l'ONU contre la cybercriminalité, le contexte géopolitique avait changé, la Russie ayant lancé quatre jours auparavant l'invasion de l'Ukraine.

Sans surprise, le débat général a été marqué par cette crise. De nombreux États, notamment occidentaux, ont exprimé leur soutien à l'Ukraine et ont fermement condamné l'agression russe comme une violation majeure du droit international et de la Charte des Nations Unies. Ces États n'ont pas manqué de souligner combien il était difficile de négocier dans un tel contexte avec la Russie, un État qui viole les règles fondamentales du droit international. En dépit de ce contexte particulièrement tendu, les délégations des États se sont largement engagées et investies dans ces négociations.

2 ONU, Assemblée Générale, *Meeting Coverage,* 74e session, GA 12235, 27 décembre 2019.

3 *Ibid.*

4 *Ibid.*

5 Comité *ad hoc* des Nations Unies, *China's Suggestions on the Scope, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes,* 1ère Session, New York, 28 février-11 mars 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf.

RÉSULTAT :

Un instrument complexe reposant sur un équilibre incertain entre lutte contre la criminalité et protection des libertés fondamentales

QUELS CRIMES ? UN CHAMP INFRACTIONNEL LARGE

Le champ infractionnel de la convention a constitué l'une des questions les plus âprement discutées. Le document initial de négociation ne comprenait pas moins de 28 « cyber crimes » auxquels se sont ajoutées de nouvelles infractions au cours des négociations. La majorité de ces infractions a toutefois été rejetée du projet de convention finalement adopté.

De façon consensuelle, les États ont très vite convenu que la Convention de l'ONU devrait inclure les crimes « cyberdépendants », à savoir les crimes qui n'existeraient pas sans les technologies de l'information et de la communication (comme par exemple l'accès illégal à un système informatique). Un certain nombre de pays, notamment la Russie et la Chine, souhaitaient néanmoins que le champ infractionnel aille au-delà des crimes « cyberdépendants » et intègre une longue série de crimes dits « cyber-permettants », à savoir des crimes qui peuvent être commis sans les technologies de l'information et des communications (TIC) mais dont la commission peut être facilitée, amplifiée ou accélérée par ces technologies. Il en va ainsi par exemple du blanchiment d'argent qui peut être commis sans le recours aux TIC mais où un système informatique peut être utilisé pour les faciliter et les accélérer. C'est cette seconde catégorie qui a généré de nombreuses controverses. Si les États se sont finalement assez rapidement accordés pour inclure les crimes liés aux abus sexuels sur des enfants, la plupart des crimes dits « cyber-permettants » ont rencontré de vives oppositions, soit parce qu'ils étaient déjà couverts par d'autres instruments, soit en raison des risques de violation des libertés fondamentales. Les pays occidentaux se sont ainsi fortement opposés à l'introduction de certains « crimes de contenu » hautement controversés tels que l'« incitation à des activités subversives ou armées», les « infractions liées à l'extrémisme », les « infractions liées au terrorisme » ou encore la « diffusion de fausses informations », infractions qui pourraient être facilement instrumentalisés par des régimes autoritaires.

Le projet de convention adopté peut à cet égard être considéré comme un succès pour les pays occidentaux dans la mesure où celui-ci comprend un nombre limité de onze crimes (sept crimes « cyber-dépendants » et quatre crimes « cyber-permettants ») dont la majorité relève déjà de la convention de Budapest. Les sept crimes « cyberdépendants » sont ainsi repris pratiquement mot pour mot (et dans le même ordre) des articles de cette dernière[6]. S'agissant des quatre crimes « cyber-permettants », trois sont des crimes de contenu liés à des infractions sexuelles. Les articles 14 et 15 portent ainsi sur des infractions sexuelles commises contre des mineurs (« Infractions relatives à des contenus en ligne représentant des abus sexuels ou l'exploitation sexuelles d'enfants » et « sollicitation ou manipulation psychologique aux fins de commettre une infraction sexuelle à l'encontre d'un enfant »), tandis que l'article 16 porte sur des infractions dont les victimes sont des personnes majeures (« diffusion non consentie d'images intimes »).

L'intégration de ces trois crimes de contenu de nature sexuelle appelle principalement deux remarques. Il convient tout d'abord de noter que les infractions sexuelles liées aux enfants font déjà l'objet d'un article dans la convention de Budapest. Le projet de convention des Nations Unies, tout en s'inspirant de celui-ci, vient le développer à travers deux articles qui tiennent compte des évolutions et de l'ampleur du phénomène. S'agissant de la « diffusion non consenties d'images intimes », il s'agit d'une nouveauté qui ne figure pas dans la convention de Budapest. En raison de sa nouveauté, l'opportunité d'un tel article a été longtemps discutée avant que ce dernier ne soit finalement intégré dans le projet de convention. Il semble que l'ampleur et la gravité de ce phénomène, qui est largement lié au développement et à l'utilisation des TIC, ait convaincu les États de la nécessité d'intégrer un article spécifique.

Le dernier crime retenu dans le projet de convention, le « blanchiment du produit du crime » (art. 17), est un crime qui lui non plus ne figure pas dans la convention de Budapest. Au regard toutefois des possibilités de blanchiment qu'offrent aujourd'hui les TIC, notamment avec l'essor des cryptomonnaies, l'intégration d'un tel article n'est guère surprenante et manifeste la volonté des États de renforcer leur coopération pour lutter plus efficacement contre ce crime.

Ce qui est peut-être plus surprenant en revanche, c'est le fait que les infractions liées aux atteintes à la propriété intellectuelle, qui figurent dans la Convention de Budapest (art. 10) n'aient pas été intégrées dans le projet de convention des Nations Unies. Ceci peut en effet surprendre dans

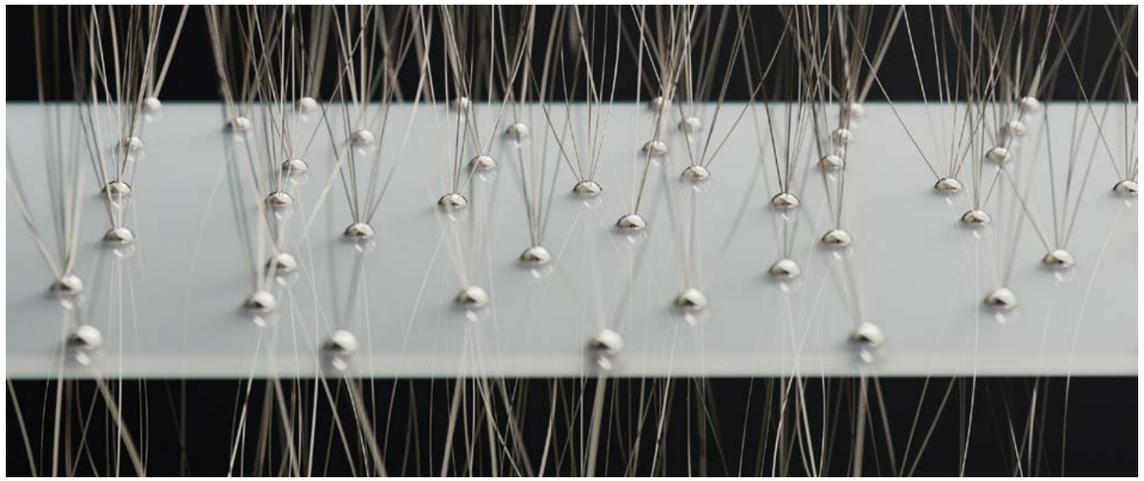
6 Il s'agit de : l'« accès illégal (art. 7) ; l'« interception illégale (art. 8) ; l'« atteinte à l'intégrité de données électroniques » (art. 9) ; l'« atteinte à l'intégrité d'un système d'information et de communication » (art. 10) ; l' « utilisation abusive de dispositifs » (art. 11) ; la « falsification en rapport avec les systèmes d'information et de communication » (art. 12) et le « vol ou fraude en rapport avec les systèmes d'information et de communication » (art. 13).

la mesure où le cyberespace constitue un espace particulièrement favorable à la prolifération du vol de propriété intellectuelle. Plusieurs raisons pourraient néanmoins expliquer cette non-intégration, notamment le fait que certaines de ces infractions peuvent relever du cyberespionnage dans la guerre économique et que les États qui se livrent à ces pratiques ont sans doute souhaité éviter qu'un instrument des Nations Unies ne viennent ainsi leur imposer de criminaliser ces actes dans leur ordre juridique interne et de sanctionner leurs auteurs.

L'adoption d'un projet de convention comprenant un nombre limité d'infractions largement consensuelles et qui, pour la plupart, figurent déjà dans la convention de Budapest, constitue sans doute un succès pour tous ceux qui souhaitaient arrimer la convention des Nations Unies à celle de Budapest. Néanmoins, le champ infractionnel de ce projet de convention peut aussi susciter des inquiétudes légitimes.

Le champ infractionnel n'est en effet pas figé et pourrait s'élargir assez rapidement. Les crimes qui ont été exclus pourraient ainsi réapparaître à la table des négociations dans un futur proche. En effet, les articles 61 et 62 prévoient que la convention peut être complétée par un ou plusieurs protocoles additionnels adoptés lors d'une conférence des parties. La proposition de tels Protocoles doit être présentée par un minimum de 60 États puis être adoptée de préférence par consensus. Toutefois, en cas d'absence de consensus, une « majorité des deux tiers au moins des États parties présents à la réunion de la conférence des parties et exprimant leur vote » peut adopter ces protocoles. Cela signifie donc que rien n'empêche la Russie ou la Chine soutenue par une soixantaine d'États de proposer l'adoption d'un ou plusieurs protocoles pour essayer d'intégrer les crimes de contenu qui ont été si difficiles à exclure du projet de convention. Les articles 61 et 62 pourraient ainsi faire peser une épée de Damoclès sur les libertés fondamentales et vont exiger de la part des États démocratiques et de la société civile une vigilance infaillible et continue.

Par ailleurs, il convient aussi de remarquer que les obligations procédurales, notamment en matière de détection et de répression ainsi que les obligations de coopération internationale, vont au-delà des onze cybercrimes identifiés et définis par le projet de convention. Comme l'intitulé de la convention l'indique, l'objectif n'est pas seulement de renforcer la coopération internationale pour les onze cybercrimes identifiés par la convention mais aussi pour les « infractions graves », à savoir celles passible d'une peine privative de liberté « dont le maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde » (art. 2).



Plus encore, les obligations procédurales de la convention s'appliquent aussi à la collecte de preuves sous forme électronique pour « toute infraction pénale », cyber ou pas, grave ou pas (art.23§1 c.). Le champ infractionnel de la convention est donc en réalité large, il va bien au-delà de la lutte contre les cybercrimes identifiés par la convention et repose en partie sur le droit pénal interne des États.

Certes, d'autres instruments des Nations Unies de lutte contre la criminalité connaissent des champs infractionnels larges, comme par exemple la Convention des Nations Unies contre la criminalité transnationale organisée qui s'applique elle aussi aux « infractions graves » passibles d'une peine privative de liberté dont le maximum ne doit pas être inférieur à quatre ans (art. 2 et 3). Néanmoins, le champ infractionnel de cet instrument ne va pas au-delà des « infractions graves » et les mécanismes procéduraux ne sont pas aussi intrusifs que ceux prévus par le projet de convention contre la cybercriminalité. Quant aux obligations en matière de coopération internationale, elles restent classiques en portant principalement sur les mécanismes bien connus d'entraide judiciaire.

L'instrument le plus proche de l'actuel projet de convention des Nations Unies reste en définitive la convention de Budapest qui couvre elle aussi trois types d'infractions : les cybercrimes identifiés et définis par la convention, « les autres infractions pénales commises au moyen d'un système informatique » et enfin « toute infraction pénale », chaque infraction étant assortie d'obligations variables en termes de coopération internationale et de mesures procédurales. Le fait que le champ infractionnel de ces deux instruments, couvrant respectivement « toute infraction pénale » puisse être dans une certaine mesure comparable n'est toutefois pas nécessairement rassurant. La convention de Budapest est en effet arrimée au Conseil de l'Europe et les garanties en matière de protection des droits de l'homme et des libertés fondamentales sont de ce fait bien assurées. Or, comme nous le verrons, cela n'est pas nécessairement le cas pour le projet de convention des Nations Unies.

QUELLES OBLIGATIONS ?

Le projet de convention impose aux États parties trois grandes séries d'obligations. La première série consiste pour les États à adopter les mesures nécessaires dans leur ordre juridique interne pour conférer le caractère d'infraction pénale aux onze cybercrimes identifiés par le projet de convention et leur permettre de poursuivre, juger et sanctionner leurs auteurs (art. 7-21).

La seconde série d'obligations faite aux États est d'adopter un certain nombre de mesures procédurales destinées à habiliter leurs autorités à prendre les mesures nécessaires aux fins d'enquêtes, de détection et de répression. Ces mesures sont applicables, sauf disposition contraire (art. 23), pour les onze cybercrimes identifiés par la convention mais aussi pour les « infractions graves » ainsi que pour « toute infraction pénale ». Détaillées dans le chapitre IV du projet de convention (mesures procédurales et détection et répression), ces mesures sont nombreuses et particulièrement intrusives, qu'il s'agisse de l'interception de données de contenu (art. 30) ; de la collecte en temps réel de données de trafic (art. 29) ; de la perquisition et saisie de données électroniques stockées (art. 28) ; de la préservation et divulgation partielle accélérées de données de trafic (art. 26) ; de la préservation accélérée de données électroniques stockées (art. 25) ou encore des injonctions, notamment à un fournisseur de service offrant des prestation sur le territoire de l'État, de communiquer des données relatives aux personnes abonnées (art. 27.b).

La troisième série d'obligations concerne la coopération internationale. Celle-ci s'applique d'une part aux enquêtes, poursuites et procédures judiciaires concernant les 11 cybercrimes identifiés par le projet de convention et, d'autre part, à la collecte, l'obtention, la préservation et la communication de preuves sous forme électroniques pour les 11 cybercrimes ainsi que pour toute « infraction grave » (art. 35). Cette coopération internationale passe principalement par différents mécanismes d'entraide judiciaire détaillés aux articles 40 et suivants du projet de convention. Au-delà des mécanismes généraux d'entraide judiciaire de l'article 40 (principes généraux et procédures d'entraide judiciaire), le projet de convention intègre aussi des mécanismes de coopération et d'entraide spécifiques, comme par exemple le fait pour un État de demander à un autre État d'ordonner ou d'imposer la préservation rapide de données électroniques stockées (art. 42) ; de perquisitionner des données électroniques stockées (art. 44) ou encore de collecter en temps réel des données de trafic (art. 45).

QUELLES PROTECTIONS ET GARANTIES ?

L'introduction dans le projet de convention de garanties en matière de protection des libertés fondamentales et des données personnelles a fait l'objet d'importants débats. Tandis que pour certaines délégations, notamment celles des États membres de l'UE, ces garanties et protections étaient indispensables, d'autres délégations se sont montrées moins enclines, voire hostiles, à l'inclusion de telles dispositions. Nous ne reviendrons pas ici en détail sur ces controverses ni sur les nombreux projets d'articles proposés puis rejetés[7] et nous nous concentrons ici sur qui a finalement été retenu.

En matière de coopération internationale, il convient de noter que plusieurs garanties ont été apportées, garanties qui devraient permettre aux États de refuser des demandes d'entraide judiciaire au nom de la protection des libertés fondamentales et des données personnelles. C'est ainsi que l'article 36 (protection des données personnelles) prévoit qu'un État n'est pas tenu de transférer des données personnelles en vertu de la convention si cela ne peut pas être fait conformément à ses lois applicables en matière de protection des données personnelles.

Par ailleurs, le paragraphe 22 de l'article 40 (principes généraux et procédures d'entraide judiciaire) souligne que les États requis n'ont pas l'obligation d'accorder l'entraide judiciaire s'ils ont de « sérieuses raisons de penser que la demande a été présentée aux fins de punir une personne en raison de son sexe, de sa race, de sa langue, de sa religion, de sa nationalité, de son origine ethnique ou de ses opinions politique (…) ». Enfin, et de façon plus générale, le fait que les États puissent invoquer l'absence de double incrimination pour refuser de fournir une aide judiciaire au titre de cet article constitue une protection supplémentaire contre des demandes liberticides.

L'introduction de ces motifs de refus dans le cadre de la coopération internationale et des demandes d'entraide ne doit toutefois pas occulter le fait que les protections accordées par la convention peuvent sembler bien légères au regard du caractère intrusif des mesures procédurales prévues dans le chapitre IV du projet de convention. L'article 24 (conditions et garanties) semble à cet égard bien limité, et sa tournure pour le moins alambiquée peut susciter certaines interrogations.

Selon celui-ci, chaque « État partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus au présent chapitre soient soumises aux conditions et garanties prévues par son droit interne, lesquelles doivent assurer la protection des droits humains, conformément aux obligations qui lui incombent en vertu du droit international des droits humains, et doivent intégrer le principe de proportionnalité ».

Comme on le comprend, cette référence aux garanties prévues par le « droit interne » des États n'est pas nécessairement très rassurante et le renvoi « aux obligations qui lui incombent » en vertu du droit international reste finalement très vague et relatif. Le seul principe cité dans cet article est finalement le principe de proportionnalité qui certes est fondamental mais ne peut pas suffire à lui seul. Par ailleurs, la convention n'instaure pas l'obligation d'un contrôle juridictionnel ou d'une autre forme de contrôle indépendant, ni de droit à un recours efficace. Bien que souhaitée, l'opportunité de ces garanties est laissée à l'appréciation des États (art. 24§2). Certes, au-delà de cet article 24, il convient d'ajouter l'article 6 (respect des droits humains) qui s'applique à l'ensemble des dispositions de la convention et qui complète donc la protection. Cet article rappelle que les États doivent s'acquitter de leurs obligations au titre de la convention « d'une manière compatible avec les obligations que leur impose le droit international des droits humains » et que rien dans cette convention ne peut être interprétée comme « autorisant la répression des humains ou des libertés fondamentales, notamment des droits liés à la liberté d'expression, de conscience, d'opinion, de religion ou de conviction, de réunion pacifique et d'association, conformément au droit international des droits humains applicables (…) ».

On peut certes se féliciter d'un tel rappel, néanmoins les protections de l'article 6 restent minimales et celui-ci ne prévoit pas de mesures renforcées ou spécifiques. De ce point de vue, les inquiétudes que pouvaient susciter dès le départ l'adoption d'une telle convention en matière de protection des libertés fondamentales et des données personnelles ne sont pas vraiment levées et l'équilibre espéré reste incertain.

7 Voir à cet égard nos analyses : *« So Close, So Far: UN Committee Tasked With Cybercrime Convention Hits Snooze »*, Lawfare, 26 Mars 2024 (avec E. Lostri) ; *« The U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights »*, Lawfare, 31 janvier, 2023.

CONCLUSION

« Là où il y a une volonté, il y a un chemin », selon William Hazlitt (1822). Il n'est pas contestable que l'ONU manifeste une volonté de progresser tous États réunis vers une plus grande cybersécurité. Il existe bien une route commune, celle tracée par des consensus sur l'applicabilité du droit international au cyberespace, à la définition de certaines infractions qui relèvent de la cybercriminalité. Mais certaines voies divergent dès lors que les questions portent sur la place de l'humain, sur le respect de sa liberté, de sa vie privée, sur la neutralité du net. La technologie commande souvent le droit, mais dans le cyberespace, plus sans doute que dans tout autre milieu, eu égard à son caractère englobant, la philosophie s'invite pour mettre le droit à l'épreuve du sens. « Science sans conscience n'est que ruine de l'âme » disait Rabelais ; la conscience est la condition de la régulation dans un domaine qui touche à l'essentiel, à l'existentiel.

agora
INCYBER FORUM

RETROUVEZ NOS DERNIÈRES ACTUALITÉS
ET NOS PROCHAINS ÉVÉNEMENTS SUR :

agora-incyber.com