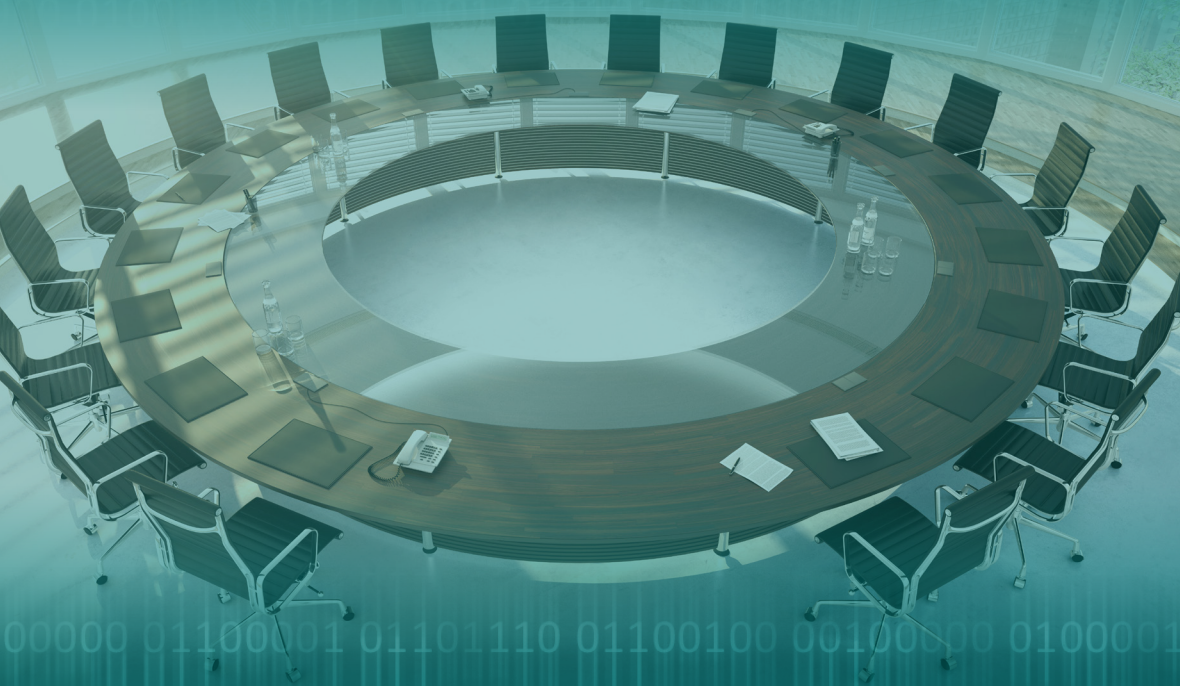
Manuel relatif à l'élaboration d'une position nationale sur le droit international et les activités cybernétiques

Un guide pratique à l'intention des États



Kubo Mačák, Talita Dias et Ágnes Kasper

Republic of Estonia
Ministry of Foreign Affairs

MOFA
Ministry of Foreign Affairs of JAPAN

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

University of Exeter

Première publication en 2025. Traduction française publiée en 2026.

Ce manuel a été élaboré en collaboration avec le Ministère des Affaires étrangères de l'Estonie, le Ministère des Affaires étrangères du Japon, le Centre d'excellence pour la cyberdéfense coopérative, accrédité par l'OTAN et l'université d'Exeter.

Cet ouvrage a bénéficié du soutien financier de l'Economic and Social Research Council (Conseil de recherche économique et sociale) dans le cadre du programme Impact Accelerator Account Award (numéro de subvention : ES/X004198/1 ; référence : ESRC/015).

Conçu et mis en page par le Studio de conception multimédia de l'université d'Exeter.

Citation suggérée : Kubo Mačák, Talita Dias et Ágnes Kasper, *Manuel relatif à l'élaboration d'une position nationale sur le droit international et les activités cybernétiques : Un guide pratique à l'intention des États* (2025)

Imprimé : ISBN 978-9916-9227-0-5 PDF : ISBN 978-9916-9227-1-2 (pdf)

TABLE DES MATIÈRES

REMERCIEMENTS

La réalisation du présent projet a été possible grâce au généreux soutien financier de l'Impact Acceleration Account (IAA) du Conseil de recherche économique et sociale du Royaume-Uni (ESRC), qui a permis l'élaboration et la publication de ce manuel. Nous tenons à exprimer notre profonde gratitude pour cette contribution.

Nous souhaitons également exprimer nos sincères remerciements à nos partenaires institutionnels – le Ministère des Affaires étrangères de l'Estonie, le Ministère des Affaires étrangères du Japon, le Centre d'excellence pour la cyberdéfense coopérative, accrédité par l'OTAN (CCDCOE) et l'université d'Exeter – pour leur soutien indéfectible et leur collaboration tout au long du projet.

Nous exprimons notre profonde gratitude à Mme Karine Veersalu du CCDCOE, responsable du projet, dont les compétences organisationnelles, la détermination constante et l'attitude positive ont permis au projet de se dérouler dans les meilleures conditions à tout moment.

Merci également au personnel de nos partenaires institutionnels qui nous a apporté un soutien essentiel tout au long du projet et dont le dévouement et l'expertise ont été indispensables à sa réussite. Nous tenons tout particulièrement à remercier Mme Anna-Maria Osula et Mme Liisa Sulavee du Ministère des Affaires étrangères de l'Estonie ; M. Yukiya Hamamoto, M. Munehito Nakatani, M. Kimihiko Okano, M. Satoru Onoda et M. Kentaro Tahara du Ministère des Affaires étrangères du Japon ; Mme Hedi Jüriöö du CCDCOE ; Mme Danielle Payne et M. James Woodhams de l'université d'Exeter ; ainsi que Mme Anne Blickhan et M. Yaroslav Halieiev, qui étaient à l'époque chercheurs invités au CCDCOE.

Un grand merci à notre comité consultatif, dont les conseils ont permis de définir l'orientation du projet dès le début et dont l'examen par ses pairs de la version préliminaire du manuel a été essentiel à sa forme finale. Nous exprimons notre profonde gratitude à tous les membres du comité consultatif : Mme Kerry-Ann Barrett, le Dr Cordula Droege, le professeur Mohamed Helal, le professeur Zhixiong Huang, le Dr Giacomo Persi Paoli, le professeur Marco Roscini, le professeur Johanna Weaver et Mme Danielle Yeow.

Nous remercions chaleureusement les représentants gouvernementaux des 46 États qui ont participé aux trois tables rondes régionales. Leur engagement réfléchi et leur volonté de dialogue ont considérablement influencé le contenu et l'orientation du manuel. Nous sommes également très reconnaissants envers les experts qui ont enrichi les discussions lors de chaque table ronde, notamment Mme Kristel-Amelie Aimre, le professeur Mariana Salazar Albornoz, M. Benjamin Ang, Mme Larissa Schneider Calza, M. Samit D'Cunha, M. Yukiya Hamamoto, le professeur Mamadou Hébié, le professeur Mohamed Helal, le professeur Zhixiong Huang, le professeur Nnenna Ifeanyi-Ajufo, le Dr So Jeong Kim, Mme Eddah Mogaka, Mme Harriet Moynihan, le Dr Anna-Maria Osula, Mme Kimberley Raleigh, M. Marcus Song, Mme Liis Vihul, Mme Danielle Yeow et M. Robert Young. Nous tenons également à remercier les

personnes qui ont pris la parole lors des tables rondes au nom des institutions partenaires, témoignant ainsi de leur précieux soutien au projet, notamment le professeur Hajer Gueldich, Son Excellence M. Jens Hanefeld, Mme Irina Höhn, le professeur Mart Noorma, Mme Eleliis Rattam, Son Excellence M. Tanel Sepp et Son Excellence M. Priit Turk.

Nous souhaitons également remercier les nombreuses personnes et institutions qui ont soutenu l'organisation des différentes tables rondes.

Nous remercions l'Organisation des États américains pour son partenariat et son aide dans le cadre de la table ronde sur les perspectives latinoaméricaines et caribéennes, qui s'est tenue à Washington, DC, en particulier Mme Kerry-Ann Barrett et M. David Moreno, ainsi que Mme Maria Tolppa du CCDCOE pour la prise de notes.

Concernant la table ronde Asie-Pacifique, qui s'est tenue à Singapour, nous remercions le Centre de droit international de l'Université nationale de Singapour, en particulier Mme Danielle Yeow, Mme Ying Li Loh et Mme Geraldine Ng, ainsi que M. Aayush Mallik de l'Université nationale de Singapour et Mme Hanyu Zhang de l'Université de Wuhan pour la prise de notes.

Nous tenons à remercier l'Union africaine, en particulier la conseillère juridique, Mme Hajer Gueldich, ainsi que le personnel du Bureau du conseiller juridique, notamment M. Francis Adanlao, Mme Meseret Assefa, Mme Mitchel Mauyakufa et M. Taona Mwanyisa, pour la table ronde organisée à Addis-Abeba à l'intention des États membres de l'Union africaine. Nous remercions également le Ministère fédéral allemand des Affaires étrangères et l'Agence allemande de coopération internationale (Deutsche Gesellschaft für Internationale Zusammenarbeit, GIZ) pour leur soutien à la table ronde, en particulier Mme Sofia Klumpp et Mme Juliane Kolsdorf.

Nous exprimons notre profonde gratitude à l'Université de technologie de Tallinn pour son soutien aux trois tables rondes, grâce à la bourse de recherche destinée aux jeunes scientifiques.

Pour finir, nous remercions vivement le Dr Nicolas Bouchet pour sa relecture attentive du document, Patricia Lachelier pour son travail de traduction en français, ainsi que l'équipe du Design Studio de l'université d'Exeter pour son travail créatif et professionnel dans la conception et la réalisation du présent manuel.

Kubo Mačák, Talita Dias et Ágnes Kasper
Mai 2025

LISTE DES ABRÉVIATIONS

AGNU	Assemblée générale des Nations Unies
ANASE	Association des nations de l'Asie du Sud-Est
ARSIWA	Articles sur la responsabilité de l'État pour faits internationalement illicites
CADH	Convention américaine relative aux droits de l'homme
CADHP	Charte africaine des droits de l'homme et des peuples
CDH	Conseil des droits de l'homme
CDHNU	Conseil des droits de l'homme des Nations Unies
CDI	Commission du droit international
CEDH	Convention européenne des droits de l'homme
CEDH	Cour européenne des droits de l'homme
CERT	Équipe d'intervention d'urgence informatique
CIADH	Cour interaméricaine des droits de l'homme
CICR	Comité international de la Croix-Rouge
CIJ	Cour internationale de justice
CPA	Cour permanente d'arbitrage
CPI	Cour pénale internationale
DIDH	Droit international des droits de l'homme
DIH	Droit international humanitaire
DPI	Droit pénal international
GEG	ou Groupe d'experts gouvernementaux des Nations Unies, travaille sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale
GTCNL	Groupe de travail à composition non limitée
HCDH	Haut-Commissariat des Nations Unies aux droits de l'homme
IP	Protocole Internet

OEA	Organisation des États américains
ONU	Organisation des Nations Unies
OSCE	Organisation pour la sécurité et la coopération en Europe
OTAN	Organisation du traité de l'Atlantique Nord
PIDCP	Pacte international relatif aux droits civils et politiques
PIDESC	Pacte international relatif aux droits économiques, sociaux et culturels
TIC	Technologies de l'information et de la communication
TPIY	Tribunal pénal international pour l'ex-Yougoslavie
UA	Union africaine
UE	Union européenne
UK	Royaume-Uni
UNIDIR	Institut des Nations Unies pour la recherche sur le désarmement
UNODA	Bureau des affaires de désarmement des Nations Unies
USA	États-Unis d'Amérique

SOMMAIRE

À mesure que les États s'engagent de plus en plus dans des activités cybernétiques, les questions relatives à l'application du droit international en la matière ont pris de l'importance. Si tout le monde s'accorde à dire que le droit international s'applique dans le contexte cybernétique, les avis divergent quant à la manière dont les règles et principes spécifiques doivent s'appliquer. De nombreux États ont contribué au débat en publiant des positions nationales : à savoir des déclarations officielles exposant leur point de vue juridique sur des aspects clés du droit international dans le contexte cybernétique.

Le présent Manuel fournit des conseils pratiques aux États qui élaborent ou révisent leur position nationale, en s'appuyant sur les contributions de 46 États ayant participé à des tables rondes régionales organisées à Addis-Abeba, Singapour et Washington, DC en 2024, ainsi que sur des recherches originales menées dans le cadre de ce projet. Il présente les principales motivations, les étapes procédurales, les questions juridiques de fond et les stratégies de présentation efficaces, offrant ainsi une approche structurée que les États peuvent adopter à différentes étapes du processus.

Principaux points à retenir

- **Les positions nationales remplissent plusieurs fonctions :** une fonction de communication, en engageant le dialogue avec les parties prenantes nationales et internationales ; une fonction de transformation, en clarifiant et en adaptant les cadres juridiques aux nouvelles réalités ; et une fonction de prévention, en réduisant le risque d'interprétation erronée tout en façonnant les évaluations des violations et les réponses appropriées, favorisant ainsi la dissuasion.
- **Le processus d'élaboration varie en fonction du contexte national, mais suit des étapes communes, parmi lesquelles :** obtenir un mandat ; constituer une équipe de base dotée d'une expertise juridique, politique et technique ; mener une analyse juridique et politique ; consulter les parties prenantes et gérer les dynamiques interinstitutionnelles ; déterminer le format final ; et obtenir les autorisations nécessaires.
- **Les approches rédactionnelles peuvent être classées en deux grandes catégories :** déductive ou inductive. L'approche déductive se base sur des règles établies, puis analyse leur application dans le contexte cybernétique. L'approche inductive part des défis cybernétiques réels et examine comment le droit international s'y applique. Les États peuvent combiner les deux approches, en recourant éventuellement à des scénarios ou à des études de cas pour plus de clarté.

- **Les positions nationales portent sur un large éventail de questions juridiques de fond :** elles comprennent notamment des principes fondamentaux tels que la souveraineté, la non-intervention et l'interdiction du recours à la force. Elles abordent également des régimes spécialisés tels que le droit international humanitaire, le droit international des droits de l'homme et le droit pénal international. Les États devraient adapter le choix des thèmes en fonction de leurs intérêts nationaux et de leurs priorités juridiques.
- **Bien que tous les États soient d'accord sur le fait que le droit international doit s'appliquer au contexte cybernétique, des divergences importantes subsistent :** Celles-ci portent notamment sur la question de savoir si des concepts tels que la souveraineté et la diligence due constituent des règles autonomes, comment déterminer les seuils de violation et comment classer certaines activités cybernétiques (comme le cyberespionnage) au regard du droit international.
- **Le format et le mode de diffusion des positions nationales conditionnent leur impact :** certains États ont publié leurs positions sous forme de communications individuelles, de discours gouvernementaux et de déclarations dans des forums multilatéraux. Une structure claire, une accessibilité et une diffusion stratégique permettent de renforcer leur portée et leur influence.
- **Les positions nationales permettent de clarifier le cadre juridique de la gouvernance du cyberespace :** elles identifient les domaines d'accord, de désaccord et les vides juridiques éventuels. À mesure que davantage d'États publient leurs positions, ces documents continueront de façonner l'interprétation, la mise en œuvre et le développement du droit international dans le contexte cybernétique et au-delà.
- **Les développements futurs pourraient inclure :** la publication de positions nationales plus détaillées par un plus grand nombre d'États, une coordination régionale renforcée, l'adoption de nouveaux instruments internationaux si un consensus se dégage sur certaines lacunes spécifiques, et une mise en œuvre au niveau national, par exemple en intégrant les normes juridiques internationales dans la législation nationale, la doctrine militaire et les cadres politiques.

Le présent Manuel propose une approche pratique et structurée aux États qui élaborent ou révisent leur position nationale, contribuant ainsi à renforcer la clarté juridique, la prévisibilité et la stabilité dans le cyberespace. En décrivant les pratiques existantes, les défis communs et les considérations stratégiques, il constitue une ressource essentielle pour les gouvernements, les praticiens du droit et les décideurs politiques qui s'intéressent à l'application du droit international dans le contexte cybernétique.

CHAPITRE 1 :

INTRODUCTION

Au cours des dernières décennies, le développement rapide des technologies de l'information et de la communication (TIC) a apporté d'innombrables avantages aux individus et aux sociétés à travers le monde. L'émergence du cyberespace a permis l'apparition de nouveaux moyens de communication, de collaboration et de coordination plus efficaces. Ces technologies ont transformé les économies, donné plus de pouvoir aux communautés et amélioré l'accès à l'information à une échelle sans précédent. Cependant, elles posent également des défis importants. Des opérations cybernétiques hostiles ont causé des perturbations dans le monde entier, entraînant des coûts humains considérables et affectant les intérêts essentiels des États. Aujourd'hui, il est reconnu à l'échelle internationale que les cyberactivités malveillantes peuvent avoir des conséquences dévastatrices dans les domaines de la sécurité, de l'économie, de la société et de l'humanitaire, qui dépassent souvent les frontières nationales.[1]

Alors que ces évolutions se produisent à l'échelle mondiale, le droit international joue un rôle crucial dans la régulation des activités cybernétiques et l'atténuation de leurs impacts. Depuis 2013, un consensus s'est dégagé parmi les États sur le fait que le droit international est applicable et essentiel au maintien de la paix, de la sécurité et de la stabilité dans l'environnement des TIC[2]. Cependant, des divergences subsistent quant à la manière dont les règles et principes spécifiques du droit international peuvent être appliqués dans le contexte cybernétique.

Ces discussions portent sur des aspects fondamentaux du droit international, tels que la responsabilité des États, la souveraineté, la non-intervention et l'interdiction du recours à la force. Elles portent également sur des régimes spécialisés, notamment le droit international humanitaire, le droit international des droits de l'homme et le droit pénal international.

La clarification et le développement du droit dans ce domaine passent en grande partie par la publication de positions nationales concernant le droit international et les activités cybernétiques. Ces déclarations officielles exposent la manière dont les États interprètent et appliquent les règles et principes juridiques internationaux fondamentaux aux activités cybernétiques, façonnant ainsi le discours juridique international et influençant l'élaboration de règles et de pratiques. À l'heure où nous rédigeons le présent document, 33 États ont publié de telles positions, ainsi que deux organisations régionales – l'Union africaine (UA) et l'Union européenne (UE) – qui ont publié des positions communes (voir **l'annexe B** pour la liste de ces documents). Plusieurs autres États envisagent de publier leur propre position nationale, tandis que certains, qui ont déjà adopté une position, envisagent de la réviser ou de la mettre à jour.

1 Assemblée générale des Nations Unies, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,* A/75/816 (18 mars 2021), paragraphe 18.

2 Assemblée générale des Nations Unies, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* A/68/98 (24 juin 2013), paragraphe 19.

La clarification et le développement du droit international dans le contexte cybernétique se font principalement par le biais des positions nationales, c'est-à-dire des déclarations officielles expliquant comment les États interprètent et appliquent les règles juridiques clés dans le cadre des activités cybernétiques.

Le présent Manuel examine cette tendance croissante en s'appuyant sur les positions nationales rendues publiques, les discussions menées dans le cadre de forums multilatéraux et les conclusions tirées de consultations à huis clos avec des représentants des États. Il fournit des orientations pratiques aux gouvernements qui souhaitent élaborer ou réviser leur position nationale, en proposant une approche structurée du processus, du contenu et de la présentation de ces documents.

Project

Le présent Manuel est le fruit d'un projet collaboratif mené par un **consortium d'institutions** comprenant le Ministère des Affaires étrangères de l'Estonie, le Ministère des Affaires étrangères du Japon, le Centre d'excellence pour la cyberdéfense coopérative, accrédité par l'OTAN et l'université d'Exeter. Le projet a également bénéficié du soutien d'institutions partenaires, notamment l'Union africaine, l'Organisation des États américains, le Ministère fédéral allemand des Affaires étrangères, le Centre de droit international de l'université nationale de Singapour et l'université de technologie de Tallinn.

Dans le cadre de cette initiative, l'équipe chargée du projet a organisé, entre septembre et novembre 2024, trois **tables rondes** régionales à huis clos qui ont réuni des représentants d'États des Amériques (Washington, DC), d'Asie et du Pacifique (Singapour) et d'Afrique (Addis-Abeba). Ces tables rondes, auxquelles ont participé 77 représentants de 46 États, ont constitué une source précieuse d'informations pour le présent Manuel. Elles ont permis des échanges directs entre les représentants des gouvernements qui ont déjà publié leur position nationale, ceux qui sont en train d'élaborer la leur et ceux qui envisagent de le faire. La liste complète des événements organisés dans le cadre du projet avant la publication du présent Manuel figure à **l'annexe D**.

Les discussions menées lors de ces tables rondes se sont déroulées conformément à la **règle de Chatham House**. Par conséquent, le Manuel ne permet pas d'attribuer les idées ou les opinions exprimées lors de ces réunions à des personnes, des États ou des institutions spécifiques, ni de révéler leur identité ou leur affiliation. Le cas échéant, il indique si une observation particulière a été formulée par un représentant d'un État participant ou par un expert invité, sans toutefois les identifier ni divulguer leur affiliation spécifique. La liste complète des États ayant participé à ce processus consultatif figure à **l'annexe C**.

Ce projet s'appuie sur d'autres initiatives dans ce domaine et les complète. Il s'inspire notamment du projet *Cyber Law Toolkit,* une ressource en ligne de premier plan en matière de droit international et d'opérations cybernétiques.[3] La base de données exhaustive du Toolkit sur les positions nationales a constitué une référence essentielle, permettant une analyse détaillée des points de vue des États dans le présent Manuel. De même, *le Recueil de bonnes pratiques : Élaboration d'une position nationale sur l'interprétation du droit international et l'utilisation des TIC par les États,* publié par l'Institut des Nations Unies pour la recherche sur le désarmement en 2024, est une ressource plus concise qui identifie les meilleures pratiques et les enseignements procéduraux des États qui ont déjà élaboré des positions nationales.[4] Le *Manuel de Tallinn 2.0* a également servi de référence clé pour l'analyse juridique présentée dans le présent Manuel, en particulier en ce qui concerne l'interprétation du droit international dans le contexte cybernétique.[5] Ces initiatives ont apporté une contribution significative dans ce domaine, et le présent Manuel est conçu pour soutenir leurs efforts.

3 Consultez la page : https://cyberlaw.ccdcoe.org.

4 UNIDIR, *A Compendium of Good Practices : Developing a National Position on the Interpretation of International Law and State Use of TIC* (2024).

5 Michael N. Schmitt (éd.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).

Positions nationales et communes

Le présent Manuel se concentre sur l'élaboration des **positions nationales** relatives à l'application du droit international dans le contexte cybernétique. L'un des principaux enseignements tirés du projet porte sur la diversité des formats et des approches utilisés par les États pour exprimer leurs positions. Certains ont publié des documents de synthèse spécifiques, tandis que d'autres ont exprimé leur point de vue dans des discours ou des déclarations officiels prononcés dans le cadre de forums multilatéraux. Ces derniers ont parfois été suivis de la publication d'un document plus complet. **Le chapitre 5** examine ces choix plus en détail, ainsi que leurs implications juridiques et politiques.

Compte tenu de la diversité des documents disponibles, il était nécessaire de définir des critères clairs pour déterminer ceux qui devaient être inclus dans notre analyse. Bien que les opinions puissent diverger quant à ce qui constitue une position nationale, nous avons, aux fins du présent Manuel, retenu les documents qui remplissent toutes les conditions suivantes :

1. **Publication officielle :** le document doit être accessible au grand public, et non pas uniquement partagé dans le cadre de réunions à huis clos, telles que les réunions privées de conseillers juridiques ou les sessions à huis clos des groupes d'experts gouvernementaux (GEG) des Nations Unies.
2. **Émission par un organe étatique :** le document doit être officiellement émis par une ou plusieurs entités gouvernementales (telles que le Ministère des Affaires étrangères ou le cabinet du Premier ministre) ou délivré par un fonctionnaire s'exprimant au nom du gouvernement (tel qu'un diplomate de haut rang ou un procureur général).
3. **Disponibilité sous forme écrite dans un référentiel public :** le document doit être publié dans son intégralité dans un format destiné à être accessible au public à long terme, par exemple sur un site web gouvernemental, dans le recueil volontaire du GEG ou sous forme de soumission officielle au Groupe de travail à composition non limitée (GTCNL) des Nations Unies.
4. **Publié dans le but d'exprimer des avis juridiques spécifiques quant à l'application du droit international dans le contexte cybernétique :** l'objectif principal du document doit être d'aborder des questions juridiques de fond, plutôt que, ou du moins en plus, de simplement réaffirmer des engagements généraux envers le droit international ou de discuter de questions politiques, de normes non obligatoires relatives au comportement responsable des États ou d'autres questions non juridiques.

Une liste complète des documents répondant à ces critères est fournie en **Annexe B**. Par souci de cohérence, les citations dans l'ensemble du Manuel les mentionnent sous la forme abrégée de « position nationale de [l'État] ».

Alors que les instances multilatérales des Nations Unies, telles que le Groupe de travail à composition non limitée, se concentrent principalement sur l'utilisation des TIC par les États, les positions nationales ont souvent dépassé ce cadre pour aborder également le comportement des acteurs non étatiques. Par exemple, certaines positions nationales se demandent si les cyberactivités menées par des acteurs non étatiques peuvent constituer une attaque armée, quelles sont les obligations des groupes armés non étatiques en vertu du droit international humanitaire et quelles sont les responsabilités des États en matière de diligence due concernant le comportement cybernétique des acteurs non étatiques relevant de leur compétence. Quelques positions font également référence aux obligations liées à la cybercriminalité. Toutefois, ce sujet a été largement abordé dans le cadre de négociations distinctes, notamment au sein de la Troisième Commission de l'Assemblée générale des Nations Unies, lesquelles ont abouti à l'adoption de la Convention des Nations Unies sur la cybercriminalité à la fin de l'année 2024. Dans l'ensemble, les positions nationales ont une portée large et englobent diverses questions liées à l'interprétation et à l'application du droit international aux activités cybernétiques.

En même temps que ce projet était en cours, l'UA et l'UE ont chacune **publié une position** commune exprimant les vues partagées de leurs États membres sur l'application du droit international dans le contexte cybernétique.[6] Ces documents ressemblent beaucoup aux positions nationales dans leur structure et leur substance, mais leur processus d'élaboration a été différent, car ils ont été élaborés par consensus entre plusieurs États plutôt que pour exprimer une perspective nationale unique. Compte tenu de leur importance, le présent Manuel se fonde sur les positions communes de l'UA et de l'UE et les cite tout au long de son analyse. Dans le cadre du Groupe de travail à composition non limitée, des groupes d'États ont également publié à plusieurs reprises des déclarations interrégionales conjointes traitant de l'application du droit international à l'utilisation des TIC. Cependant, étant donné que ces positions communes et ces déclarations conjointes impliquent des dynamiques juridiques et politiques distinctes, le présent Manuel ne propose pas de lignes directrices spécifiques pour leur élaboration. Cela étant dit, une grande partie de son analyse et de ses recommandations peuvent s'appliquer *mutatis mutandis* à ces efforts.

6 Positions communes de l'UA (2024) et de l'UE (2024).

Importance juridique des positions nationales

Le statut des positions nationales en droit international reste incertain. Les positions elles-mêmes sont pour la plupart muettes sur cette question. Celles qui évoquent leurs objectifs généraux les présentent généralement comme des efforts visant à promouvoir la sécurité juridique ou à favoriser une vision commune, plutôt que comme des revendications spécifiques quant à leur signification juridique.[7] À titre exceptionnel, certaines positions indiquent explicitement que leur objectif vise à « développer le droit coutumier » en général[8] ou à « promouvoir » une vision indicative de l'émergence d'une nouvelle règle spécifique.[9]

Les discussions menées lors des tables rondes organisées dans le cadre du projet ont été tout aussi peu concluantes et ont porté sur des sujets très variés. Quelques participants se sont demandé si les positions nationales pouvaient être considérées comme autre chose que des documents politiques, laissant entendre qu'elles n'avaient aucune valeur juridique indépendante. À l'autre extrémité du spectre, d'autres ont avancé l'idée que les positions nationales pouvaient être considérées comme des actes unilatéraux donnant lieu à des obligations juridiques internationales pour l'État qui les émet. Ces points de vue divergents illustrent bien que le débat sur le rôle précis des positions nationales dans l'élaboration du droit international est toujours d'actualité, qu'il est nécessaire que les États s'engagent davantage et que des recherches universitaires supplémentaires soient menées sur cette question.

Le présent Manuel ne cherche pas à clore ce débat, mais plutôt à mettre en évidence les points d'accord. En dépit d'un certain scepticisme, la plupart des participants aux tables rondes organisées dans le cadre du projet ont convenu que les positions nationales sont plus que de simples déclarations de politique générale. Étant donné qu'elles sont publiées sous forme de déclarations officielles quant à l'application du droit international, elles présentent par nature une certaine valeur juridique, du moins en ce qui concerne les sources du droit international auxquelles elles se réfèrent, notamment les traités et le droit international coutumier.

Lorsque les positions nationales interprètent **le droit des traités**, elles peuvent contribuer à la pratique ultérieure des États dans l'application dudit traité. En vertu des règles d'interprétation des traités, si cette pratique établit l'accord des parties sur une interprétation particulière, elle pourrait devenir déterminante pour les questions en jeu.[10] Cependant, la plupart des traités mentionnés dans les positions nationales, tels que la Charte des Nations Unies et les Conventions de Genève, comptent plus de 150 États parties, dont la plupart n'ont pas encore publié de telles positions. Même s'il existe un large consensus parmi les États qui l'ont fait, cela ne suffit pas pour établir un accord interprétatif définitif à ce stade.[11]

7 Voir, par exemple, les positions nationales du Danemark (2023), p. 447, de la Finlande (2020), p. 1, de l'Allemagne (2021), pp. 1-2, du Japon (2021), p. 1, de la Pologne (2022), p. 1, de la Suède (2022), p. 1, de la Suisse (2021), p. 1, et des États-Unis (2021), p. 136.

8 Position nationale de la Pologne (2022), p. 1.

9 Position nationale de l'Estonie (2019).

10 Convention de Vienne sur le droit des traités (1969), article 31(3)(b).

11 CDI, *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties,* A/73/10 (2018), conclusion 10(1).

Pour l'instant, les interprétations communes qui se dégagent ne peuvent donc servir que de moyens d'interprétation supplémentaires, indiquant les domaines dans lesquels un consensus semble se dégager, mais qui ne sont pas encore définitifs.[12]

Les positions nationales font également souvent référence **aux règles du droit international coutumier**. Le plus souvent, les États le font pour affirmer le caractère coutumier d'une règle ou d'un ensemble de règles particulier, telles que les interdictions d'intervention[13] et de recours à la force[14] ou le droit de la responsabilité de l'État.[15] Il arrive parfois que les États invoquent la coutume de manière négative, rejetant l'émergence d'une règle particulière dans le cadre du droit international coutumier.[16]

Le droit international coutumier résulte de la combinaison de deux éléments essentiels : la pratique des États (un comportement général et constant de la part des États) et *l'opinio juris* (l'acceptation que ce comportement est

12 Convention de Vienne sur le droit des traités (1969), article 32.

13 Positions nationales de l'Australie (2021), p. 2, du Brésil (2021), p. 18, du Costa Rica (2023), paragraphe 23, du Danemark (2023), p. 449, de l'Allemagne (2021), p. 4, de l'Iran (2020), art. III 1, de l'Italie (2021), p. 4, de la Norvège (2021), p. 4, de la Suisse (2021), p. 3, du Royaume-Uni (2022) et des États-Unis (2021), p. 139.

14 Positions nationales du Brésil (2021), p. 19, du Costa Rica (2023), paragraphe 35, d'Israël (2021), p. 398, de la Norvège (2021), p. 5, de la Pologne (2022), p. 5, de la Suède (2022), p. 3, et des États-Unis (2021), p. 137.

15 Positions nationales de l'Australie (2021), p. 5, du Canada (2022), paragraphe 32, du Costa Rica (2023), paragraphe 10, de l'Estonie (2021), p. 28, de l'Allemagne (2021), p. 10, de l'Irlande (2023), paragraphe 20, de la Pologne (2022), p. 6, de la Suisse (2021), p. 5, et des États-Unis (2021), p. 141.

16 Cf. par exemple les positions nationales d'Israël (2021), p. 404, du Royaume-Uni (2021), paragraphe 12, et des États-Unis (2021), p. 141, qui rejettent l'émergence d'une règle coutumière de diligence due.

le fruit d'une obligation juridique).[17] Il est assez incontestable que les positions nationales peuvent être considérées comme des expressions de l'*opinio juris,* dans la mesure où elles expriment la conviction juridique d'un État qu'une certaine catégorie de comportements est autorisée, requise, interdite ou même non réglementée en vertu du droit international coutumier, selon le cas.[18]

Cependant, la question de savoir si les positions nationales peuvent également être considérées comme des pratiques étatiques est plus délicate. Étant donné que le droit international coutumier se développe généralement de manière inductive, par la répétition des comportements des États, plutôt que de manière déductive, par des déclarations généralisées, il est peu probable que les positions écrites puissent à elles seules être considérées à la fois comme des pratiques et comme une *opinio juris.*[19] Cela étant dit, les positions nationales peuvent être considérées comme évidence de pratique étatique lorsqu'elles décrivent le comportement spécifique d'un État en matière de cybersécurité, mais de tels exemples sont jusqu'à présent très rares.[20] Même si les positions nationales (ou certaines parties de celles-ci) étaient acceptées comme des exemples de pratique, en raison de leur nombre limité, elles ne remplissent pas encore la condition de généralité nécessaire à l'émergence d'une nouvelle règle coutumière.[21] Cela pourrait toutefois changer à mesure que davantage d'États publient leurs positions nationales.

La signification juridique du silence d'un État en réponse à la publication des opinions d'autres États n'est pas clairement établie. Certains affirment que les États doivent contester les interprétations avec lesquelles ils ne sont pas d'accord, tandis que d'autres rejettent l'idée que l'inaction puisse être considérée comme une acceptation.

Se pose également la question de savoir si **le silence des États** qui n'ont pas pris position au niveau national équivaut à une acceptation tacite des interprétations dominantes ou à l'émergence de nouvelles règles coutumières. Ce point a fait l'objet d'un débat important lors des tables rondes. En droit international, le silence n'est considéré comme une acceptation tacite que dans des circonstances exceptionnelles, les critères pertinents étant notamment que l'État en question reste silencieux dans des circonstances qui exigent une réponse, qu'il ait connaissance de ces circonstances et qu'un délai raisonnable se soit écoulé.[22]

17 Statute of the International Court of Justice, article 38(1)(b).

18 Cf. également CDI, *Draft conclusions on the identification of customary international law, with commentaries,* A/73/10 (2018), conclusion 2, commentaire, paragraphe 4.

19 Sur l'objection du « double comptage » de manière plus générale, cf. Maurice Mendelson, « The Formation of Customary International Law », (1998) 272 Recueil des Cours 155, 206–207.

20 Cf. par exemple la position nationale de la France (2021), p. 12, qui stipule que « la plupart des opérations cybernétiques menées par les forces armées françaises dans une situation de conflit armé [consistent] principalement en la collecte d'informations [et] ne répondent pas à la définition d'une attaque ». Cf. également le chapitre 4, section 3.a, consacré à la définition d'une attaque au regard du droit international humanitaire.

21 ILC, *Draft conclusions on the identification of customary international law, with commentaries,* A/73/10 (2018), conclusion 8(1).

22 CDI, *Draft conclusions on the identification of customary international law, with commentaries,* A/73/10 (2018), conclusion 10(3); CDI, *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties,* A/73/10 (2018), 15, conclusion 10(2).

La question de savoir si la publication des opinions d'autres États sur le droit international dans le contexte cybercriminel crée une telle situation reste posée. Si certains participants ont fait valoir que les États doivent contester activement les interprétations avec lesquelles ils ne sont pas d'accord, d'autres ont rejeté l'idée que l'inaction seule devait être considérée comme une acceptation juridique. Indépendamment du débat juridique, il a été généralement admis que, d'un point de vue politique, il est prudent pour les États de réagir aux interprétations qu'ils jugent incorrectes ou contraires à leurs intérêts, afin d'éviter que celles-ci ne soient progressivement acceptées par un nombre croissant d'États.

Structure du manuel

Le présent Manuel est composé de six chapitres, organisés selon une progression logique qui reprend les considérations et les étapes généralement suivies par les États pour élaborer une position nationale. Après cette introduction :

- **Le chapitre 2** se penche sur les motivations qui sous-tendent l'élaboration d'une position nationale. Il examine les raisons pour lesquelles les États choisissent d'exprimer leur point de vue sur le droit international et les activités cybernétiques ou s'abstiennent de le faire.
- **Le chapitre 3** décrit le processus d'élaboration d'une position nationale, en mettant en évidence les bonnes pratiques, les défis et les enseignements tirés des États qui ont entrepris cette démarche.
- **Le chapitre 4** traite des questions juridiques de fond couramment abordées lors de l'élaboration des positions nationales, en identifiant les points d'accord principaux, les discussions en cours et les questions juridiques émergentes.
- **Le chapitre 5** propose des conseils sur la présentation des positions nationales, notamment sur le choix du format, du style, de la langue et du mode de diffusion.
- La **conclusion** fait la synthèse des principaux enseignements et examine les orientations futures des positions nationales dans l'élaboration du discours juridique international.

Outre les chapitres importants, le manuel comprend une liste de vérification pratique **pour l'élaboration d'une position nationale (annexe A)**. Cet outil résume les étapes clés, les considérations et les bonnes pratiques décrites dans le texte principal, et est conçu pour aider les responsables à planifier, rédiger et présenter leurs positions nationales.

En proposant une approche structurée pour l'élaboration, le contenu et la présentation des positions nationales, le présent Manuel vise à aider les États dans toutes les étapes du processus, aussi bien ceux qui envisagent de publier une première position nationale que ceux qui souhaitent affiner et actualiser une position existante. Il a également pour objectif d'aider les gouvernements, les praticiens, les chercheurs et les décideurs politiques dans leur travail, et de contribuer ainsi aux efforts plus larges visant à renforcer la clarté, la prévisibilité et la stabilité juridiques dans le cyberespace.

CHAPITRE 2 :

MOTIVATIONS

EN BREF

Ce chapitre présente les raisons pour lesquelles les États élaborent des positions nationales sur le droit international dans le cyberespace. Il décrit les principales motivations, telles que la promotion de la clarté juridique, la prévention des erreurs d'appréciation et l'élaboration de normes internationales, et souligne comment ces positions peuvent servir à la fois des objectifs nationaux et internationaux. Les États peuvent agir pour renforcer leur crédibilité, s'aligner sur leurs partenaires ou répondre à des menaces. En comprenant ces motivations, il est plus facile de déterminer les éléments à inclure dans une position et la meilleure façon de l'utiliser dans les débats juridiques et politiques mondiaux.

1. Introduction

Aujourd'hui, il est communément admis que les cyberactivités malveillantes peuvent avoir des conséquences dévastatrices sur les plans sécuritaire, économique, social et humanitaire[1]. En conséquence, les mesures prises pour prévenir et contrer les menaces ou les défis cybernétiques, par le biais du droit international ou d'autres moyens, sont motivées par des considérations complexes et souvent contradictoires. Les positions nationales constituent des outils juridiques et politiques précieux pour faire face à ces menaces et défis dans le cyberespace. Elles sont élaborées pour des raisons explicites ou implicites et peuvent poursuivre des intérêts et des objectifs externes ou internes, susceptibles de peser différemment selon les États. Ces considérations déterminent la décision d'élaborer ou non une position nationale, les questions à traiter et leur niveau de détail, ainsi que les positions juridiques à adopter sur les questions de fond choisies (par exemple, la souveraineté, la diligence due et les contre-mesures). Des facteurs tels que la taille du territoire, la population, l'économie ou les capacités d'un État, ainsi que d'autres éléments objectifs mais dépendants du contexte, influencent également ces choix.

Ce chapitre identifie et analyse les facteurs de motivation qui sous-tendent les décisions relatives aux différents aspects des positions nationales. Sans prétendre à l'exhaustivité, il a pour objectif d'aider les États à repérer les moments critiques du processus décisionnel, à comprendre les implications potentielles des diverses approches et à formuler des arguments convaincants en faveur de la voie retenue. **Les principaux facteurs de motivation** peuvent être classés selon leur dimension

1 Assemblée générale des Nations Unies, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/75/816 (18 mars 2021), paragraphe 18.

externe ou interne, et selon les fonctions des positions nationales : communicative, transformatrice et préventive. Ces motivations influencent la manière dont ces fonctions sont mobilisées pour atteindre les **objectifs explicites ou implicites** d'une position nationale.

L'élaboration et la publication d'une position nationale est un **choix**. Cependant, le fait de ne pas en élaborer ou en publier une sous la forme de document spécifique et consolidé, ou encore de reporter ou prolonger son élaboration, ne signifie pas nécessairement que l'État reste silencieux. Les États peuvent choisir d'exprimer leurs points de vue juridiques par d'autres moyens et sous d'autres formes, tels que des contributions orales et écrites au Groupe de travail à composition non limitée (GTCNL) des Nations Unies, qui peuvent constituer des alternatives moins coûteuses en ressources. Les sections suivantes explorent les motivations et les objectifs contenus dans les positions nationales existantes et synthétisent les principales conclusions tirées des tables rondes du projet.

2. Motivations, fonctions et objectifs généraux

a. Motivations générales

L'élaboration d'une position nationale découle d'une convergence de motivations interdépendantes. Ces déclarations sont contextuelles et présentent naturellement le point de vue de l'État qui les adopte.

En exposant clairement leurs motivations politiques générales, les États peuvent aligner leur position nationale sur leurs intérêts particuliers et définir les objectifs spécifiques qu'ils souhaitent poursuivre.

Par exemple, alors que certains États se concentrent sur l'impact social ou économique des activités cybernétiques et leur relation par rapport au développement,[2] d'autres se concentrent sur les implications des activités cybernétiques dans les conflits armés.[3]

Bien que les positions nationales aient émergé dans le contexte du droit international et soient généralement considérées comme une question relevant des juristes internationaux, de nombreux États semblent reconnaître que la question de l'application du droit international dans le cyberespace est (pour paraphraser Georges Clemenceau) trop importante pour être laissée à leurs seuls soins. L'articulation d'une position nationale sur le droit international a **des conséquences concrètes et influence** la manière dont les États déploient leur puissance et réagissent au déploiement de la puissance dans et à travers le cyberespace. Par conséquent, les principaux facteurs qui déterminent le choix d'élaborer ou non une position nationale et la manière de la formuler découlent de considérations politiques tant externes qu'internes. Parmi les facteurs externes, on peut citer le fait de se sentir poussé à suivre un groupe d'États ou la pression exercée par des partenaires et le milieu universitaire. Ces facteurs

2 Cf., par exemple, les positions nationales de la Chine (2021), p. 1, et du Costa Rica (2023), paragraphes 2 à 4.

3 Cf. par exemple la position nationale d'Israël (2021), p. 396.

sont centrés sur la nécessité de restreindre le comportement des États et définissent l'étendue de l'autonomie des États dans et à travers le cyberespace. Toutefois, les positions nationales peuvent également jouer un rôle important au niveau national, outre leur rôle évident au niveau international qui consiste à traiter des questions juridiques internationales. Par exemple, l'élaboration d'une position nationale peut aider un État à calibrer sa réponse en cas d'incidents cybernétiques internationaux, à clarifier ses obligations juridiques et à identifier les lacunes en matière de gouvernance nationale qui nécessitent une attention particulière.

b. Fonctions communicatives, transformatrices et préventives des positions nationales

Les positions nationales ont **une fonction communicative** en engageant le dialogue avec les acteurs concernés à différents niveaux dans le cadre du débat plus large sur l'application du droit international dans le contexte cybernétique. Si le thème du droit international et du cyberespace n'est pas nouveau et figure à l'ordre du jour des Nations Unies depuis au moins 1998, la tendance à rédiger et à exprimer publiquement des positions ne s'est manifestée qu'environ deux décennies plus tard. Le fait de communiquer et de déclarer une position sur l'application du droit international aux activités cybernétiques à la communauté internationale et au public national témoigne d'un haut niveau de maturité dans la compréhension et la prise en compte des différents intérêts en jeu. Cela indique également qu'un État souhaite faire connaître sa position et qu'il a tout intérêt et l'intention de participer activement aux processus juridiques internationaux pertinents. Une position nationale permet de faire savoir, tant à l'intérieur qu'à l'extérieur, qu'un État respecte les règles et attend des autres qu'ils en fassent de même.

En adaptant le cadre existant du **comportement responsable** des États aux nouvelles réalités, les positions nationales exercent une fonction transformatrice. Les déclarations contenues dans les positions nationales peuvent avoir des effets juridiques : en tant que principaux législateurs du droit international, les États contribuent ainsi à la clarification, au développement et à l'évolution des règles (voir **l'introduction** sur la valeur juridique des positions). Les positions nationales visent

souvent à transformer les règles de conduite dans le cyberespace, mais peuvent différer considérablement quant au niveau d'intensité souhaité. L'élaboration d'une position peut donc viser à passer de zones d'ombre à plus de clarté, à préciser et consolider les règles existantes, à proposer un moyen de trouver un terrain d'entente ou à définir l'ambition d'établir des instruments juridiques obligatoires supplémentaires dans ce domaine (ce qui reste controversé entre les États). Même si les changements généraux peuvent être subtils et progressifs, en clarifiant l'application des règles existantes, les États commencent à définir des attentes communes et à fixer les limites juridiques de leur comportement dans le cyberespace. La clarification est donc plus qu'un simple exercice technique ; elle est motivée par le besoin perçu ou réel de remodeler la dynamique des relations internationales dans l'environnement numérique.

Les positions nationales assurent **une fonction préventive** en termes d'atténuation des conséquences négatives des actions menées par des acteurs étatiques et non étatiques dans le cyberespace, ce qui peut également servir de motivation pour élaborer et publier une position. En proposant une interprétation d'une règle de droit international, et parfois en ajoutant des exemples illustratifs pour plus de clarté, les États définissent les circonstances dans lesquelles ils considèrent qu'un certain type de comportement dans le cyberespace constitue une violation du droit international et fixent la limite entre les comportements légaux et illégaux pour eux-mêmes et pour les autres. Le fait de clarifier l'application des règles favorise la responsabilisation en cas de violation et a un effet dissuasif. Par conséquent, la perspective de conséquences juridiques est un facteur qui garantit la retenue et le respect des droits d'un État.

c. Objectifs généraux et résultats attendus

De nombreuses positions nationales expliquent au moins en partie les objectifs ou les raisons qui ont motivé leur publication. Comme il s'agit de textes soigneusement rédigés, l'explication peut se concentrer sur les raisons pour lesquelles un État particulier a décidé d'élaborer une position et mettre en lumière les objectifs poursuivis, les résultats escomptés et les avantages pour cet État et la communauté internationale. Les objectifs et les attentes exprimés explicitement ou implicitement indiquent la manière dont les fonctions communicatives, transformatrices et préventives des positions nationales sont mises en œuvre et appliquées. En d'autres termes, les objectifs sont **les résultats souhaités et les finalités orientées** vers l'avenir que les États souhaitent atteindre en élaborant une position nationale.

Ces objectifs et attentes se recoupent souvent, témoignant de la nature complexe et multiforme du cyberespace. Plusieurs thèmes interdépendants ont émergé lors des tables rondes organisées dans le cadre du projet, et les objectifs juridiques et/ou politiques spécifiques ou les résultats escomptés font généralement référence à certains aspects liés au renforcement de la paix et de la sécurité internationales, au renforcement de l'ordre juridique international ou à la consolidation de l'environnement national.

3. Les objectifs spécifiques et leurs motivations

a. Prévenir les erreurs de calcul et l'escalade – accroître la prévisibilité et la stabilité à grande échelle

Formulation des objectifs

En exprimant clairement leur interprétation du droit international dans le contexte cybernétique, les États pourraient chercher à minimiser les malentendus et à prévenir une escalade involontaire des activités cybernétiques, ce qui pourrait contribuer à renforcer la paix et la sécurité internationales.

Cette approche proactive vise à **réduire le risque de conflit** résultant d'éventuelles erreurs d'appréciation ou d'interprétation des actions dans le domaine numérique. Elle est explicitement exprimée, par exemple, dans les positions nationales de l'Australie, du Canada et de la France.[4] Comme le souligne la France, **une confiance accrue** est également essentielle pour atteindre cet objectif.

En outre, les États peuvent publier une déclaration pour souligner et faire savoir qu'ils ne sont pas disposés à accepter un certain niveau d'interférence dans leurs affaires souveraines. Comme l'a fait remarquer un représentant d'État : « Vous ne voulez pas que votre silence soit interprété comme un consentement.[5] » Étant donné que les petits États sont sans doute plus vulnérables face à ce type d'activités cybernétiques, il est d'autant plus important pour eux de faire connaître leur position.[6] Cette **clarté** accrue contribue à réduire le risque d'erreurs d'appréciation et d'interprétation.

Une position nationale peut également avoir pour objectif d'accroître la **prévisibilité** du comportement des États et **la stabilité** dans le cyberespace. Cela découle d'une vision commune de l'application du droit international dans le contexte cybernétique, et cette prévisibilité – soulignée, par exemple, par les positions nationales de l'Australie, de Singapour et des États-Unis[7] – contribue à un environnement international plus stable et plus sûr. L'objectif peut être formulé comme suit : « Favoriser un comportement **responsable des États** dans le cyberespace », démarche qui devrait également contribuer à cet objectif. Par exemple, le Canada déclare dans sa position nationale qu'il « estime que l'articulation des positions nationales sur la manière dont le droit international s'applique à l'action des États dans le cyberespace renforcera le dialogue international et favorisera l'émergence

4 Positions nationales de l'Australie (2021), p. 1, du Canada (2022), paragraphe 5, de la France (2019), p. 4.

5 Observation faite lors de la table ronde sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

6 Observation faite lors de la table ronde sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

7 Cf. par exemple les positions nationales de l'Australie (2021), p. 1, de Singapour (2021), p. 85, et des États-Unis (2021), p. 136.

d'une vision commune et d'un consensus sur le comportement légal et acceptable des États ».[8] La position nationale de l'Australie ajoute que « même lorsque les points de vue divergent, le fait de mieux comprendre les positions respectives des États peut renforcer la prévisibilité et réduire le risque d'erreurs d'appréciation, susceptibles d'entraîner une escalade dans le comportement des États ».[9] De nombreux États considèrent le droit international comme un élément fondamental du cadre régissant le comportement responsable des États dans le cyberespace .

On peut faire valoir que ces objectifs peuvent être plus facilement atteints ; c'est pourquoi certains ont encouragé la participation d'un plus grand nombre de voix et une plus grande diversité dans les discussions, en favorisant l'élaboration de positions nationales et en montrant l'exemple, notamment par leur participation et leur adhésion à divers forums et processus multilatéraux.[10] Cette approche pourrait renforcer la **légitimité** de ces processus et de leurs résultats.

Motivations

Les objectifs susmentionnés découlent sans doute de la nécessité d'assurer la sécurité nationale, de promouvoir la prospérité économique, d'améliorer la vie des citoyens et de renforcer la position d'un État au sein de la communauté internationale. Ces motivations ne sont pas propres au contexte cybernétique. Il est certain que le concept de positions nationales est **relativement nouveau** et que les États ont longtemps géré leurs relations dans le cyberespace sans y avoir recours. Après tout, le droit international s'applique aux activités cybernétiques même en l'absence de positions nationales. Cependant, en cas d'incertitude quant à son application, le cyberespace peut être perçu comme un domaine juridiquement ambigu ou opaque, et les malentendus ou les interprétations erronées des incidents cybernétiques pourraient accroître le risque de conflits involontaires. Par conséquent, il est sans doute plus difficile de promouvoir la stabilité et la prévisibilité dans le cyberespace sans une définition claire des règles de droit international applicables.[11] En général, l'expression des points de vue permet **de mieux connaître la position des États**. En d'autres termes, un État qui a une position nationale avec des concepts et des définitions communs[12] peut permettre aux autres de comprendre son point de vue et d'agir en conséquence.

Si un État adopte une position nationale fondée sur des concepts et des définitions communs, cela permet aux autres de comprendre son point de vue et d'agir en conséquence.

8 Cf. la position nationale du Canada (2022), paragraphe 5.

9 Cf. la position nationale de l'Australie (2021), p. 1.

10 f. par exemple, les positions nationales du Canada (2022), paragraphe 6, et du Costa Rica (2023), paragraphe 5.

11 Observation faite lors de la table ronde sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

12 Cf. par exemple, la position nationale de l'Allemagne (2021), p. 2.

Plusieurs représentants d'États ont exprimé leur inquiétude quant au fait que les voix de nombreuses régions restent **sous-représentées**, ce qui conduit à des discussions **inégales**. La mise à l'écart ou l'exclusion de certaines régions pourrait créer un favoritisme et des préjugés, réels ou perçus, dans le processus de cristallisation de l'application des règles existantes. Cela pourrait nuire à l'efficacité de la gouvernance, de la mise en œuvre et de la responsabilité. Par conséquent, plus les États s'expriment, plus la discussion devient inclusive et moins il y aura de contestations ultérieures quant à la légitimité des processus régionaux et des Nations Unies. De plus, le domaine du cyberespace offre une opportunité unique d'exprimer les points de vue des États, d'être proactif et de maintenir la dynamique des efforts visant à maintenir la paix et la sécurité internationales.[13]

b. Renforcer la conformité et la responsabilité – dissuader et prévenir les violations

Formulation des objectifs

En publiant leurs positions nationales, les États sont encouragés à **respecter leurs obligations juridiques internationales** et sont davantage **tenus responsables** en cas de violations. Ce faisant, ils contribuent à la paix et à la sécurité internationales et renforcent l'ordre juridique international. Les positions nationales servent également à dissuader les acteurs malveillants, un objectif qui figure parmi les priorités des États. Par exemple, l'Estonie fait valoir que le fait d'avoir une position nationale « pourrait également avoir un effet dissuasif, car nous avons désormais une vision plus claire de la manière dont nous percevons et réagissons aux opérations cybernétiques à l'avenir ».[14]

13 Observation faite lors de la table ronde sur les perspectives de l'Amérique latine et des Caraïbes (rapport consigné par les auteurs).

14 Position nationale de l'Estonie (2019).

Dans sa position nationale, le Japon déclare qu'il « espère que l'approfondissement d'une vision commune – notamment en ce qui concerne les activités dans le cyberespace qui constituent une violation du droit international et les outils dont disposent, en vertu du droit international, les États dont les intérêts juridiques ont été lésés par des opérations cybernétiques – dissuadera de recourir à des activités malveillantes dans le cyberespace ».[15] La position nationale de la France de 2019 – l'une des premières à avoir été publiée – indique que « si la France a l'intention de prévenir, protéger, anticiper, détecter et répondre aux cyberattaques et faire le nécessaire pour les attribuer, elle se réserve également le droit de répondre à celles qui ciblent ses intérêts ».[16] L'Iran utilise également sa position nationale pour exprimer ses intentions de dissuasion en des termes forts, notamment en promettant des conséquences « fermes et décisives » en cas de violation de ses « politiques ».[17] Toutefois, de telles formulations restent exceptionnelles et la majorité des positions nationales utilisent un ton plus coopératif et moins conflictuel, même lorsqu'elles font connaître leurs lignes rouges.

Motivations

Les outils cybernétiques font désormais partie intégrante des conflits actuels. Par conséquent, chaque dirigeant gouvernemental devra répondre aux questions suivantes : **comment agir, comment réagir** et **quelles sont les options juridiques** en cas de violations commises dans ou via le cyberespace.[18] La conformité et la responsabilité ne sont possibles que si l'application des règles de conduite est **suffisamment claire** et si les États comprennent où se situent les limites de leur autonomie. Cela est également nécessaire pour signaler d'éventuelles violations des règles, mais aussi pour déterminer et sélectionner les réponses juridiques appropriées. En outre, l'élaboration d'une position globale et cohérente n'est pas anodine et témoigne d'une forme de « cyberpuissance » douce : la capacité **d'exercer une influence** sur le cyberespace.[19] Les États pourraient avoir intérêt à renvoyer l'image d'une cyberpuissance.

En outre, comme le souligne la position nationale de l'Australie, l'efficacité du droit international dépend de la mise en œuvre diligente et du respect par les États de leurs obligations juridiques, ainsi que des efforts de collaboration visant à faire respecter ces obligations et à garantir la responsabilité en cas de violation.[20]

15 Position nationale du Japon (2021), p. 2.

16 Position nationale de la France (2019), p. 5.

17 Position nationale de l'Iran (2020).

18 Observation faite lors de la «Singapore International Cyber Week» dans le cadre du panel intitulé «National Positions on International Law in Cyberspace: Challenges, Opportunities, and Best Practices», le 15 octobre 2024, à Singapour (rapport conservé par les auteurs).

19 George Christou, «Cyber Diplomacy: From Concept to Practice», *Tallinn Paper n° 14*, NATO CCDCOE (2024), 5.»

20 Cf. la position nationale de l'Australie (2021), p. 1.

Cette déclaration met l'accent sur les facteurs interdépendants qui contribuent au succès du droit international, notamment la clarté des règles, le respect constant de ces règles par les parties concernées, le partage d'informations et la dénonciation des violations, ainsi que les conséquences de ces dernières. En d'autres termes, le droit international ne peut être efficace si les États se contentent de le respecter en théorie.

c. Façonner l'évolution du droit international – lever les incertitudes juridiques

Définition des objectifs

Les déclarations contenues dans une position nationale peuvent clairement souligner que l'État émetteur vise à « **contribuer au débat** sur les modalités d'application du droit international »,[21] ou que la position nationale est un instrument destiné à **clarifier** l'application du droit international aux activités cybernétiques.[22]

D'autres formulations similaires ont été utilisées.[23] Ces objectifs peuvent être liés à l'objectif général de renforcement de l'ordre juridique international. Un autre objectif peut être de clarifier la base sur laquelle l'État s'appuie pour répondre aux actes illicites commis par d'autres États et des acteurs non étatiques dans le cyberespace.[24] Par exemple, la souveraineté, l'interdiction du recours à la force et le principe de non-ingérence sont largement considérés comme les trois critères clés permettant de déterminer la licéité des opérations cybernétiques. La plupart des positions nationales exprimées jusqu'à présent accordent une grande attention à ces trois thèmes et aux mesures de réponse connexes en cas de violation (abordées plus en détail au **chapitre 4**).

Les positions nationales ne se limitent pas strictement à interpréter et à clarifier les règles existantes. Elles peuvent également servir à en **proposer de nouvelles**, à souligner l'importance de certaines règles ou à attirer l'attention sur d'autres. Par exemple, dans leurs positions nationales, la Russie et Cuba préconisent l'adoption d'une nouvelle convention universelle obligatoire sur la sécurité internationale de l'information.[25] Il est donc clair que ces positions nationales visaient à communiquer le point de vue de l'État sur la manière dont le droit international devrait évoluer dans ce domaine. À l'inverse, certains États ont clairement indiqué qu'ils **ne voyaient pour l'instant aucune nécessité d'élaborer un nouvel instrument juridiquement obligatoire**.[26]

21 Cf. la position nationale de l'Allemagne (2021), p. 1.

22 Cf. la position nationale de l'Autriche (2024), p. 3.

23 Cf. par exemple, les positions nationales du Danemark (2023), p. 447, de l'Estonie (2019), des Pays-Bas (2019), p. 1, et de la Suisse (2021), p. 2.

24 Cf. la position nationale du Danemark (2023), p. 447.

25 Cf. les positions nationales de Cuba (2024), paragraphe 4, et de la Russie (2021), p. 80.

26 Cf. par exemple, les positions nationales de l'Autriche (2024), p. 3, de la République tchèque (2020), p. 2, de l'Estonie (2021), p. 24, de la Roumanie (2021), p. 75, et de la Suède (2022), p. 1..

En tentant de trouver un juste milieu, d'autres ont exprimé l'avis selon lequel ces options ne s'excluent pas nécessairement l'une l'autre. Par exemple, la position nationale du Brésil stipule qu'« il est important d'identifier les points de **convergence** entre les États sur cette question et, lorsque des divergences sont identifiées, de travailler conjointement à une plus grande cohérence dans l'interprétation des règles existantes. Si nécessaire, l'élaboration de normes supplémentaires devrait également être envisagée comme un moyen de combler les **vides juridiques** potentiels et de lever les incertitudes qui subsistent ».[27] Les vides juridiques, les interprétations divergentes des règles existantes et l'application de règles différentes à des cas similaires ne sont pas rares en droit international. Par conséquent, si la convergence des points de vue juridiques est un objectif louable, elle ne nécessite pas nécessairement une uniformité totale. En revanche, l'élaboration d'un nouveau traité obligatoire nécessiterait un consensus sur toutes les dispositions négociées, un objectif qui implique généralement des délibérations et des accords plus poussés entre les États.

Dans le cadre des tables rondes organisées pendant le projet, il est apparu que les positions nationales pouvaient également avoir pour objectif de sensibiliser aux discussions clés et de mettre en évidence les besoins en matière de renforcement des capacités sur ces questions. Les États doivent tenir compte d'un **réseau complexe d'intérêts** dans leurs relations internationales. Comme l'a fait remarquer un représentant d'État, le soutien à un nouvel instrument juridiquement obligatoire pour le cyberespace risque d'être utilisé comme monnaie d'échange dans les négociations interétatiques sur d'autres questions sans rapport, en particulier lorsque l'importance des discussions sur l'application du droit international dans le contexte cybernétique est peu connue.[28]

Motivations

L'un des principaux moteurs de la définition d'une position nationale repose sur la volonté de contribuer **activement** à l'état de droit international dans le contexte dynamique du cyberespace, plutôt que de se contenter d'en accepter les règles. En partageant leurs points de vue, les États peuvent influencer et façonner l'interprétation et l'évolution du droit international dans le contexte cybernétique. Par exemple, la Suisse considère les positions nationales des États comme une « contribution importante à la concrétisation de l'application du droit international dans le cyberespace ».[29] Ce facteur semble largement reconnu et compris, tant dans les positions nationales publiées à ce jour que de manière intuitive parmi les États qui aspirent à en élaborer une.[30]

27 Position nationale du Brésil (2021), p. 18. (Soulignement ajouté.)

28 Observation faite lors du Troisième symposium annuel en présentiel sur le droit international et le droit cybernétique, «Future Conflict: The International Law of Cyber and Information Convergence», dans le cadre du panel intitulé «Navigating legal Dynamics: National Perspectives on International Law and Potentials for Convergence», American University, 24 septembre 2024, Washington, DC (rapport conservé par les auteurs).

29 Cf. la position nationale de la Suisse (2021), p. 1.

30 Plusieurs observations faites lors des trois tables rondes organisées dans le cadre du projet (rapports conservés par les auteurs).

À première vue, l'élaboration d'une position nationale peut sembler relever d'un exercice théorique. En réalité, il s'agit d'une entreprise beaucoup plus **complexe et lourde de conséquences**, qui touche aux règles fondamentales du droit international relatives à la paix et à la sécurité dans le cyberespace. En ce sens, les positions nationales expriment les points de vue des États sur ces questions cruciales. Par conséquent, le silence et la non-participation au consensus émergent sur ces questions peuvent se révéler extrêmement dommageables. Au cours des tables rondes organisées dans le cadre du projet, plusieurs représentants d'États ont exprimé leur inquiétude quant au fait que le silence pouvait être (mal) interprété comme une acceptation des conceptions des autres sur des concepts juridiques clés tels que la souveraineté, la non-intervention et l'interdiction du recours à la force.[31] On peut supposer que ce risque deviendra plus important avec le temps, à mesure que davantage d'États exprimeront leur point de vue et que la conception internationale de ces concepts juridiques continuera à se cristalliser.

En outre, il ne suffit pas que les États développent leur propre interprétation des règles. Cette interprétation doit également être **communiquée et divulguée** si elle doit influencer l'application du droit international existant ou son évolution future dans le contexte cybernétique. Comme l'indique la position nationale de la Pologne, « la pratique consistant à présenter publiquement des positions sur des questions clés relatives au droit international renforce la sécurité juridique et la transparence, tout en contribuant à renforcer le respect des engagements internationaux et en offrant la possibilité de développer le droit coutumier.[32] » Le fait de réduire le flou juridique est étroitement lié au respect de l'état de droit, car l'incertitude rend la mise en œuvre et l'application plus difficiles.

Conscients de la nature évolutive du cyberespace, les États ont reconnu la nécessité de traiter et de réduire les flous juridiques, en identifiant les lacunes potentielles dans l'application du droit international dans ce contexte. En exprimant clairement leurs positions, les États peuvent contribuer à combler ces lacunes et à **réduire les risques liés à des interprétations juridiques ambiguës**.

Outre ces considérations, les **petits États** peuvent considérer la formulation d'une position nationale comme un moyen **d'affirmer et de protéger leurs** droits sur la scène internationale, où les grandes puissances dominent souvent. D'autre part, les grands États ont automatiquement leur place à la table des négociations, mais, comme l'ont fait remarquer leurs représentants lors des tables rondes organisées dans le cadre du projet, les **responsabilités et la pression** qui leur incombent les obligent à mener les discussions.[33]

31 Observation faite lors de la table ronde sur les perspectives africaines (rapport conservé par les auteurs).

32 Position nationale de la Pologne (2022), p. 1.

33 Observation faite lors de la table ronde du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

D'autre part, certains facteurs motivent les États à faire preuve de retenue et à ne pas prendre de décisions précipitées lorsqu'ils annoncent la nécessité de nouvelles règles. De nombreux États considèrent qu'à l'heure actuelle, ce domaine évolue trop rapidement et est trop instable pour permettre la négociation d'un traité mondial efficace. Le contenu substantiel d'un tel traité reste également flou, alors que les États commencent seulement à réfléchir à leur position et qu'il existe à la fois des convergences et des divergences sur des questions clés. Par conséquent, ces considérations alimentent également les formulations selon lesquelles les États précisent ce qui **ne fait pas partie** de leurs objectifs ou qu'ils n'ont pas l'intention d'orienter les discussions dans cette direction.

Lorsqu'il s'agit de déterminer quelles questions de fond doivent être incluses dans sa position nationale, un État prend généralement en considération des facteurs tels que **l'importance** de la question dans le contexte cybernétique, sa capacité à contribuer à la clarification de la question pertinente et la mesure dans **laquelle une coordination** nationale réussie est probable.[34] Dans certains cas, la reconnaissance croissante de la nécessité d'une approche de la cybersécurité centrée sur l'humain, qui tienne compte des besoins et des vulnérabilités diversifiés des individus et des communautés, peut également être prise en compte.[35] Il est également possible de présenter des questions politiques plus larges dans les positions nationales. Certains États, comme la Chine, soulignent la nécessité de s'attaquer à la fracture numérique et d'empêcher la politisation des questions technologiques et de cybersécurité.[36] Les États dont les infrastructures cybernétiques sont sous-développées peuvent être particulièrement intéressés, par exemple, par les aspects juridiques internationaux des ambassades de données et, plus généralement, du cloud computing,[37] et reviennent sans cesse sur la nécessité de renforcer les capacités.

34 Observation faite lors de la table ronde sur les perspectives pour l'Asie et le Pacifique (rapport conservé par les auteurs).

35 Cf. la position nationale du Costa Rica (2023), paragraphe 5.

36 Position nationale de la Chine (2021), p. 1.

37 Observation faite lors de la table ronde sur les perspectives africaines (rapport conservé par les auteurs).

De leur côté, les petits États sont naturellement intéressés par les réponses collectives apportées en cas de violation du droit international.[38] Lorsqu'une interprétation ou un avis **diverge** des autres ou se démarque d'une manière ou d'une autre (par exemple, le Brésil considère que l'interception des télécommunications constitue une violation de la souveraineté.[39] et l'Estonie estime que les contre-mesures collectives sont autorisées en vertu du droit international[40]), il est d'autant plus important de connaître les opinions de la majorité silencieuse, car le droit évolue dans ce domaine.[41]

Les positions nationales exercent une influence **au-delà du contexte cybernétique**, car elles abordent souvent des questions plus **larges** relevant du droit international général. Les positions nationales ne formulent pas d'objectifs clairs à cet égard, mais cette question a été soulevée à plusieurs reprises lors des tables rondes organisées dans le cadre du projet. La conséquence des discussions sur l'application du droit international aux activités cybernétiques est particulièrement visible lorsque les États expriment leur point de vue sur la portée, le contenu et les éléments des différentes règles primaires et secondaires du droit international en termes généraux, avant de les appliquer au contexte cybernétique spécifique. Ces expressions sont susceptibles d'influencer l'interprétation et la compréhension des règles pertinentes dans d'autres domaines du droit international.

La question de la souveraineté illustre clairement ce point. En 2018, le Royaume-Uni a émis l'avis que la souveraineté était un principe du droit international, mais pas une règle pouvant être violée en tant que telle.[42] De nombreux États ont rapidement réagi en déclarant dans leurs positions nationales que la souveraineté était une règle autonome du droit international et qu'elle impliquait une obligation indépendante.[43] Bien que la question ait été soulevée dans le contexte cybernétique, les déclarations contenues dans les positions nationales à ce sujet sont larges et se rapportent souvent également au droit international général. Autre question d'actualité : l'assistance des États tiers dans la prise de contre-mesures. L'Estonie soulève la question des contre-mesures collectives dans sa position nationale.[44] Mais **un débat est actuellement en cours**, plusieurs États ayant des éléments à ajouter.[45] Ces deux questions sont examinées plus en détail au **chapitre 4**, consacré au contenu des positions nationales.

38 Cf., par exemple, les positions nationales du Costa Rica (2023), paragraphe 15, et de l'Estonie (2019 et 2021, p. 28).

39 Position nationale du Brésil (2021), p. 18.

40 Position nationale de l'Estonie (2019 et 2021, p. 28).

41 Observation faite lors de la table ronde sur les perspectives pour l'Amérique latine et les Caraïbes (rapport conservé par les auteurs).

42 Position nationale du Royaume-Uni (2018).

43 Cf., par exemple, les positions nationales de l'Autriche (2024), p. 4, du Brésil (2021), p. 18, du Danemark (2023), p. 448-449, et de la Nouvelle-Zélande (2020), paragraphe 12.

44 Cf. la position nationale de l'Estonie (2019)..

45 Cf. par exemple les positions nationales de l'Autriche (2024), p. 9, du Canada (2022), paragraphe 37, du Costa Rica (2023), paragraphe 15, de la France (2021), p. 4, et de l'Irlande (2023), paragraphe 26.

d. Amélioration des cadres d'action nationaux et renforcement de la cyber-résilience

Formulation des objectifs

Bien que les objectifs nationaux soient rarement énoncés explicitement dans les positions nationales, il ressort des tables rondes organisées dans le cadre du projet que de nombreux États considèrent qu'une meilleure compréhension des comportements autorisés constitue l'un des principaux résultats attendus de l'élaboration d'une telle position. Cette meilleure compréhension peut servir de cadre pour guider les activités cybernétiques des États et leur réponse aux incidents cybernétiques. Ce cadre garantit la conformité des actions des États avec le droit international et réduit le risque de conséquences imprévues.[46] La publication d'une position nationale fournit également aux parties prenantes nationales un **point de référence** sur les comportements attendus.

L'élaboration d'une position nationale peut avoir pour objectif de renforcer la **cyberrésilience** de l'État. Le fait d'avoir une position nationale contribue à renforcer la résilience et la préparation face aux opérations cybernétiques malveillantes. En ce sens, les positions nationales et communes permettent aux États d'ajuster leurs réponses, car elles les amènent à déterminer, consolider et clarifier leurs points de vue internes. De plus, le fait de travailler sur ce sujet améliore sans doute la **coordination interinstitutionnelle** sur les questions cybernétiques en établissant des lignes de communication, en clarifiant les domaines de responsabilité et en mobilisant les principaux acteurs au sein des gouvernements.

Bien qu'ils le mentionnent rarement de manière explicite, de nombreux États considèrent l'élaboration de positions nationales comme un moyen de clarifier quels comportements sont autorisés dans le cyberespace.

Motivations

L'élaboration d'une position nationale peut être considérée comme un **exercice de confrontation à la réalité**. Elle permet à un État de mieux évaluer son état de préparation, d'identifier et de comprendre les intérêts des différents acteurs nationaux, et de mettre en évidence les idées fausses et les divergences. Bien que l'élaboration d'une position nationale soit un exercice juridique, les discussions avec les parties prenantes façonnent le langage, la structure et la portée du document. Ces discussions enrichissent également les perspectives juridiques d'arguments techniques et politiques importants, et peuvent apporter un éclairage nouveau sur les différentes implications de l'adoption d'interprétations juridiques. À titre d'exemple, on peut se demander s'il est viable et réaliste de plaider en faveur d'une norme de diligence due plus élevée, et si un État peut s'y conformer.[47]

46 Cf. par exemple la position nationale des États-Unis (2021), p. 136.

47 Observation faite lors de la table ronde sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

En outre, clarifier davantage la manière dont le droit international s'applique dans le contexte cybernétique implique des **mesures nationales correspondantes**, qui peuvent prendre la forme d'une réglementation.[48] Les parties prenantes nationales doivent également tenir compte de leur réalité et de l'application de la loi. Comme l'a souligné un représentant de l'État, le fait d'avoir une position nationale permet de garantir que les différents organes de l'État et les autres acteurs ne se livrent pas à des actes qui pourraient constituer des actes internationalement illicites.[49] Les positions nationales constituent un excellent **point de référence** pour les différentes agences qui souhaitent communiquer avec leurs partenaires, leurs pairs et le grand public. Elles centralisent et harmonisent les déclarations relatives au comportement des États dans le cyberespace, et les parties prenantes considèrent la position nationale comme une ligne directrice et une contrainte pour les déclarations non coordonnées. Ce document est donc précieux pour fournir des conseils juridiques concis et coordonner les communications internes et externes sur les questions liées au cyberespace.

Lorsqu'un incident cybernétique se produit, le temps manque souvent pour réfléchir à la manière dont le droit international s'applique. **La cyberrésilience et la préparation** nécessitent que des mesures soient prises avant tout incident.

En adoptant une position nationale claire et cohérente, les États peuvent renforcer leurs cadres juridiques et politiques internes, fournissant ainsi une base solide pour la prise de décision dans le domaine complexe et souvent ambigu des opérations cybernétiques. L'environnement numérique est vaste et divers organismes gouvernementaux ont des responsabilités couvrant différents aspects du cyberespace. Sans une attention et des efforts particuliers, les gouvernements risquent de ne pas avoir une vue d'ensemble et de ne pas savoir où se situent les compétences et les capacités de leurs agences. L'élaboration d'une position nationale est une bonne occasion de **cartographier** comment fonctionnent les réseaux gouvernementaux et ce qui peut être mis en place en cas de crise.[50] Il est probable que cela entraîne également des changements au niveau national en termes de rôles, de compétences et de procédures, ainsi que la création de scénarios plausibles pour des exercices de simulation et l'élaboration de réponses potentielles. Ces éléments sont particulièrement importants pour renforcer la résilience en temps de crise.[51]

48 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

49 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

50 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport versé au dossier des auteurs).

51 Plusieurs observations faites lors des trois tables rondes organisées dans le cadre du projet (rapports conservés par les auteurs)..

En outre, dans le cas des parties prenantes nationales participant à l'élaboration d'une position nationale, le simple fait de siéger à la table des négociations constitue en soi un exercice de renforcement des capacités. Les considérations internes et le processus d'élaboration d'une position nationale peuvent amener les acteurs nationaux (par exemple, ceux qui travaillent dans les domaines de la défense, de l'application de la loi ou des affaires économiques) à se réunir dans une même salle pour examiner conjointement des questions clés. Comme l'a résumé un représentant de l'État, « le processus lui-même a sa valeur ».[52]

4. Facteurs contraignants et risques

Si nombre d'entre elles expriment clairement certaines de leurs motivations et leur raison d'être, les positions nationales et communes publiées à ce jour restent généralement **muettes sur les risques et les limites** de l'exercice. Là encore, les raisons en sont très contextuelles et varient d'un pays à l'autre, en fonction du climat économique, social et géopolitique et des caractéristiques propres à l'environnement national et international.

Les États sont **libres de garder le silence** et de choisir de ne pas élaborer de position nationale. Ayant compris l'importance et la pertinence d'une telle démarche, nombre d'entre eux sont en train d'en élaborer une, et il semble y avoir deux raisons principales pour lesquelles les États n'ont pas (encore) de position nationale : **le manque de sensibilisation et le manque de capacités**.

En outre, comme le montrent les tables rondes organisées dans le cadre du projet, les questions clés portent également sur les points à exclure et les raisons de cette exclusion, la manière de hiérarchiser les différents enjeux, le niveau de détail à atteindre, la manière de parvenir à un accord national concernant les divergences, l'opportunité, le moment et la manière de publier le texte, ainsi que l'opportunité et le moment où il convient de revoir une position existante.

a. Manque de capacités

Le manque de capacités dû à la rareté des ressources constitue une contrainte majeure qui influe sur les décisions tout au long du processus d'élaboration d'une position nationale. Il s'agit d'une **entreprise complexe qui nécessite d'importantes ressources**. De nombreux États (voire la plupart) ne disposent pas des ressources nécessaires pour le faire ou pour le faire efficacement, du moins à certains égards. Cette situation peut conduire à redéfinir les priorités en matière d'élaboration d'une position nationale : même si tous les avantages soulignés dans la section précédente sont compris, ils peuvent être relégués au second plan par des questions jugées plus urgentes ou plus importantes. Divers problèmes (par exemple,

52 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Amérique latine et dans les Caraïbes (rapport conservé par les auteurs).

les barrières linguistiques, le manque de connaissances techniques ou juridiques, le coût prohibitif de la participation, l'absence ou la méconnaissance des documents d'orientation et de référence ou leurs limites, et le manque de coordination ou de clarté quant aux compétences au sein du gouvernement) peuvent faire apparaître l'élaboration d'une position nationale comme une tâche ardue. Par conséquent, la décision d'aller de l'avant sera inévitablement une décision politique. Cependant, en refusant complètement de s'engager dans ce processus, les États risquent de laisser à d'autres États une influence démesurée sur l'interprétation du droit international.

De nombreux États pourraient également ne pas se sentir à l'aise ou manquer d'expérience dans le processus de collecte des pratiques étatiques en tant qu'élément du droit international coutumier, qui n'est souvent pas accessible au public. De même, la nécessité d'une position nationale ou commune peut sembler lointaine si aucun incident cybernétique à grande échelle ne s'est encore produit. Il serait donc avantageux pour les États de **partager** leurs expériences et de faire preuve de transparence quant à leurs pratiques.[53]

b. Absence de volonté politique

Certains dirigeants gouvernementaux peuvent ne pas avoir conscience ou ne pas reconnaître l'importance d'élaborer une position nationale sur le droit international dans le contexte cybernétique. D'autres peuvent ne manifester aucun intérêt pour le droit international. En conséquence, certains États peuvent simplement manquer de volonté politique pour élaborer une position nationale. Cependant, le **prix** à payer pourrait être de ne pas contribuer au développement de la pratique des États en tant qu'élément du droit international coutumier dans le contexte cybernétique et de ne pas préserver la marge de manœuvre nécessaire pour s'opposer de manière persistante à la pratique des autres.

La prudence peut également **s'expliquer** par le nombre limité d'États ayant jusqu'à présent publié une position nationale, ce qui peut entraîner une réticence à suivre leur exemple. En effet, la formulation d'une position implique une réflexion approfondie dès le départ, car les États sont généralement réticents à modifier radicalement leur position officielle sur des principes fondamentaux tels que l'interdiction du recours à la force.[54] Sur cette base, les États peuvent estimer nécessaire d'attendre que la question prenne davantage d'importance et soit clarifiée, afin de conserver une certaine souplesse pour les discussions futures.

Cependant, l'élaboration des positions nationales ne doit pas nécessairement être un exercice ponctuel, mais plutôt être considérée comme faisant partie d'un processus, tant au niveau interne qu'externe, dans le cadre du développement du droit international. Par conséquent, les positions nationales ne sont pas nécessairement des documents définitifs, mais plutôt des documents évolutifs, et les États peuvent décider de les réviser. Au cours des événements organisés dans le cadre du projet,

53 Observation faite lors de l'atelier et du lancement du projet à CyCon intitulé « National Position on International Law in Cyberspace : Challenges, Opportunities and Best Practices », 28 mai 2024, Tallinn (rapport conservé par les auteurs).

54 Observation faite lors de la « Singapore International Cyber Week » dans le cadre du panel intitulé « National Positions on International Law in Cyberspace : Challenges, Opportunities, and Best Practices », le 15 octobre 2024, à Singapour (rapport conservé par les auteurs).

plusieurs représentants d'États ont fait remarquer que les États qui ont publié leur position devraient étudier celles des autres et revoir continuellement la leur afin de parvenir progressivement à des interprétations communes ou partagées.[55] Il ne s'agit pas nécessairement de changer d'interprétation, mais plutôt de s'appuyer sur les versions précédentes et d'approfondir et de clarifier certaines questions, à mesure que la compréhension des questions pertinentes s'améliore et que la discussion progresse.

c. Non-divulgation

L'élaboration d'une position nationale n'implique pas nécessairement sa divulgation immédiate ou rapide. Les États ne sont pas tenus de publier leur position, en tout ou en partie, pour bénéficier des avantages liés au processus d'élaboration. Ils peuvent choisir de ne pas donner la priorité à la publication de leurs points de vue pour diverses raisons, notamment :

- Une volonté d'être flexible et de ne pas se positionner de façon prématurée.
- Une approche prudente consistant à attendre que les autres présentent leurs positions avant de dévoiler la sienne, et à éviter toute confrontation géopolitique inutile.
- Un manque de préparation pour communiquer certains points de vue, laissant ainsi de côté des questions sensibles, controversées ou peu claires.
- Un manque de confiance et une réticence à mener des discussions franches.[56]

d. Omissions stratégiques

Le processus d'élaboration d'une position nationale ou commune peut aboutir à la décision d'omettre stratégiquement certaines questions de la position nationale, de poursuivre les discussions internes à ce sujet et de se concentrer sur les questions pour lesquelles l'État a déjà une opinion bien arrêtée et une grande confiance. Par exemple, les États membres de l'UA ont décidé de ne pas aborder dans leur position commune des questions portant sur les immunités diplomatiques, la licéité des contre-mesures et les conditions permettant d'invoquer l'état de nécessité, compte tenu des désaccords qui existent à ce sujet.[57] Les États **ne devraient pas se sentir obligés** d'aborder toutes les questions examinées au **chapitre 4** ou de le faire immédiatement.

De plus, les États peuvent ne pas vouloir **révéler leur réflexion** au-delà d'un certain seuil de généralité, et donc limiter la profondeur de la discussion dans des domaines sensibles tels que le niveau à partir duquel une action dans le cyberespace peut être qualifiée d'attaque armée. Quoi qu'il en soit, les États sont inévitablement **sélectifs** choix des questions qu'ils souhaitent aborder, car ils ne peuvent pas toutes

55 Observation faite lors de l'atelier et du lancement du projet à la conférence CyCon, intitulé « National Position on International Law in Cyberspace : Challenges, Opportunities and Best Practices », 28 mai 2024, Tallinn (rapport conservé par les auteurs).

56 Observation faite lors du Troisième symposium annuel en présentiel sur le droit international et le droit cybernétique, « Future Conflict : The International Law of Cyber and Information Convergence », dans le cadre du panel intitulé « Navigating Legal Dynamics : National Perspectives on International Law and Potentials for Convergence », American University, 24 septembre 2024, Washington, DC (rapport conservé par les auteurs).

57 Position commune de l'UA (2024), paragraphe 10.

les couvrir.[58] De plus, si certains sujets ne sont pas abordés, les parties prenantes risquent d'interpréter le silence d'un État comme une intention particulière ou de donner au texte une signification qui n'était pas celle voulue par ses rédacteurs. Enfin, dans une période **géopolitique** difficile, l'importance d'une question pour la communauté internationale peut également être un facteur déterminant dans le choix des questions à omettre. À cet égard, les tables rondes organisées dans le cadre du projet ont révélé une certaine perplexité quant au peu d'attention accordée par les positions nationales existantes à des questions clés telles que le règlement pacifique des différends ou le droit à l'autodétermination.[59] Pour répondre à ce besoin, le manuel traite ces deux questions de manière assez détaillée au **chapitre 4**.

e. Maintien de la flexibilité politique et opérationnelle

Les États craignent d'être contraints par leurs déclarations publiques. Il est vrai que dans le cyberespace, la situation peut évoluer rapidement, dans la mesure où la technologie se développe à un rythme que la politique et le droit peinent à suivre. Par conséquent, les positions nationales ne se veulent pas exhaustives, mais, comme l'a fait remarquer un représentant d'État lors des tables rondes organisées dans le cadre du projet, elles contribuent à atténuer certaines préoccupations et doivent parfois faire preuve d'une certaine *souplesse*.[60]

La publication de déclarations très détaillées peut également se retourner contre l'État s'il ne se comporte pas conformément aux normes qu'il s'est lui-même fixées, risquant ainsi d'importantes répercussions politiques. En ce sens, le silence peut être considéré comme un moyen d'échapper à la responsabilité. La réticence des États à exprimer leur *opinio juris* constitue un autre frein important, car cela peut les empêcher d'apporter des ajustements ultérieurs. Ils peuvent donc hésiter à publier autre chose que des **déclarations générales et vagues**.[61] Si les déclarations générales conservent une certaine utilité, elles peuvent toutefois être considérées comme insuffisantes pour démontrer un engagement sincère à respecter les règles.

Le fait de conserver une ambiguïté constructive et une flexibilité opérationnelle justifie en grande partie pourquoi les États hésitent à adopter une position nationale. Les parties prenantes nationales, en particulier les forces armées et les agences de renseignement, peuvent également considérer que la clarification des règles risque de restreindre leurs activités et de les éloigner d'une zone grise qui leur offre certains avantages et libertés ainsi qu'une marge de manœuvre maximale. Cette situation peut **créer des tensions** entre les parties prenantes nationales qui peuvent avoir des approches différentes en matière de relations internationales. Par exemple, les représentants de l'État ont souligné que certaines agences gouvernementales ont une approche plus diplomatique, tandis que d'autres sont formées et raisonnent en

58 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

59 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

60 Observation faite lors de la Singapore International Cyber Week dans le cadre du panel intitulé « Positions nationales sur le droit international dans le cyberespace : défis, opportunités et bonnes pratiques », le 15 octobre 2024, à Singapour (rapport conservé par les auteurs).

61 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

termes de sécurité ou de stratégie militaire. **Concilier** ces différentes perspectives peut constituer un défi de taille, lequel nécessite une discussion ouverte et une volonté de compromis. Il est également important de garder à l'esprit que la clarté des règles ne se limite pas à contraindre, mais **protège également** ceux qui les respectent.[62] Par exemple, de nombreux États peuvent se montrer réticents à accepter que la diligence due devienne obligatoire, car il peut être difficile de prévenir, d'arrêter ou de corriger des activités dans le cyberespace si l'on ne contrôle pas l'infrastructure.[63] D'un autre côté, c'est précisément en raison de l'interdépendance des infrastructures cybernétiques que d'autres États seraient enclins à fixer des attentes en matière de diligence due.[64] Cette logique n'est pas différente de celle qui prévaut en matière de diligence due dans le droit de l'environnement.[65]

f. Absence de consensus

Le droit international continue d'évoluer et il n'existe pas de consensus clair sur la manière dont les règles spécifiques doivent être interprétées et appliquées dans le contexte cybernétique. Les États peinent donc à élaborer une position nationale cohérente. Pour certains, l'absence de consensus peut susciter du **scepticisme** à l'égard de telles initiatives ou faire douter de l'utilité même d'une position nationale ou commune. Cela peut également freiner la dynamique ou démotiver les États, qui ne savent pas dans quelle mesure les positions nationales ou communes contribuent à l'élaboration du droit international coutumier.[66]

Si l'absence de consensus peut être considérée comme un facteur contraignant, elle n'empêche pas pour autant l'expression d'opinions juridiques ou la réalisation de progrès significatifs dans ce domaine. Le système juridique international fonctionne depuis longtemps sans accord universel sur tous les points de droit, et les **différences entre les obligations juridiques** des États – telles que les variations dans le cadre de l'adhésion aux traités – **sont une caractéristique bien établie** du système. Dans ce contexte, l'élaboration de positions nationales peut contribuer à clarifier les interprétations juridiques et à promouvoir la convergence au fil du temps, même en l'absence d'accord complet.

La diversité des points de vue existants pourrait également inciter certains États à plaider en faveur d'un nouvel instrument juridique obligatoire, soit pour combler les lacunes perçues, soit pour harmoniser les interprétations. Bien que cette option reste ouverte, elle nécessiterait, comme toute initiative visant à conclure un traité, un consensus important entre les États. Il convient de rappeler que dans d'autres domaines du droit international où des divergences persistent depuis longtemps, comme le droit de la responsabilité de l'État, les États continuent de s'appuyer sur le

62 Observation faite lors de la table ronde du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

63 Plusieurs observations faites lors des trois tables rondes du projet (rapports conservés par les auteurs).

64 Observation faite lors de la table ronde du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

65 Observation faite lors de la table ronde sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

66 Observation faite lors de la table ronde du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs)..

droit international coutumier plutôt que de chercher à adopter un traité multilatéral obligatoire. Ce constat souligne combien il est **complexe** de parvenir à un accord sur un instrument obligatoire et invite à réfléchir davantage au rôle que peuvent jouer les positions nationales dans la définition des attentes juridiques et la promotion d'une compréhension commune dans le contexte cybernétique.

5. Conclusion

Il est essentiel de bien comprendre **pourquoi** un État a élaboré ou élabore une position nationale. Les positions nationales exercent une fonction communicative en engageant le dialogue avec les acteurs nationaux et internationaux concernés. Elles assument également une fonction transformatrice dans la mesure où elles contribuent à clarifier et à adapter le cadre juridique existant aux nouvelles réalités. En exprimant et en clarifiant la position des États, les positions nationales remplissent une fonction préventive, car elles réduisent le risque d'interprétations erronées et d'erreurs d'appréciation, et elles contribuent à établir des normes pour évaluer le caractère illicite d'un comportement et les réponses à apporter en cas de violation, favorisant ainsi la dissuasion. Les positions nationales fixent également des objectifs et des résultats escomptés, lesquels peuvent être formulés en termes prospectifs. Ces objectifs et résultats escomptés comprennent généralement le renforcement de la paix et de la sécurité internationales, le renforcement de l'ordre juridique international, une meilleure compréhension entre les parties prenantes nationales et la contribution au renforcement de la cyber-résilience.

Il est essentiel de bien comprendre pourquoi un État a élaboré ou élabore une position nationale.

La décision d'adopter une position nationale est **influencée par des facteurs internes et externes**. Chaque position exprime les priorités et les préoccupations spécifiques de l'État concerné, souvent en fonction des cybermenaces les plus pressantes auxquelles il est confronté. Cependant, chaque État évolue dans un contexte qui lui est propre, qu'il s'agisse de la taille de son territoire, de sa population, de son économie ou de ses capacités, ou encore du degré de coordination entre les différentes agences, de la volonté politique et des ressources disponibles. Le choix de ne pas élaborer de position nationale peut être influencé par des considérations juridiques, politiques ou économiques. Les tables rondes organisées dans le cadre du projet ont révélé deux raisons récurrentes à ce choix : un manque de capacités et un manque de volonté politique. Cependant, certains facteurs peuvent également limiter le contenu ou l'utilisation prévue des positions nationales, notamment le manque de transparence totale, le maintien d'une flexibilité politique et opérationnelle ou l'absence de consensus interne.

Ce qui nous amène au processus de réalisation, objet du chapitre suivant.

CHAPITRE 3 :

PROCESSUS

EN BREF

Dans ce chapitre, nous présentons les étapes pratiques à suivre pour préparer une position nationale. Nous soulignons l'importance d'une coordination précoce, d'un engagement de l'ensemble du gouvernement et d'un processus de rédaction structuré. Nous examinons également les acteurs qui doivent être impliqués, des conseillers juridiques aux parties prenantes externes, et la manière de gérer les dynamiques interinstitutionnelles. Bien que le processus diffère d'un État à l'autre, la clarté, l'inclusivité et la planification stratégique sont essentielles. Ce chapitre propose une feuille de route flexible pour aider les États à élaborer des positions nationales cohérentes, crédibles et adaptées au contexte.

1. Introduction

Le processus d'élaboration d'une position nationale varie considérablement d'un État à l'autre, et il n'existe pas de modèle universel applicable à tous les cas. Cependant, certains éléments clés se retrouvent généralement, même si leur ordre peut varier : obtenir un mandat, nommer des rédacteurs, mener des recherches sur les ressources et les pratiques existantes, consulter les parties prenantes, puis rédiger, adopter et diffuser la position.

Sur le plan conceptuel, l'élaboration d'une position nationale s'inscrit dans le cycle des politiques publiques, mais elle est intrinsèquement liée aux perspectives du droit international, ce qui nécessite l'intégration de considérations politiques, juridiques et opérationnelles.

Par conséquent, le processus doit prendre en compte toutes ces dimensions.

Chacune de ces étapes nécessite des ressources et des capacités institutionnelles. Le renforcement des capacités reste un facteur essentiel pour tous les États, en particulier ceux qui ont une expérience ou des cadres institutionnels limités dans ce domaine, afin d'élaborer et de formuler des positions nationales sur l'application du droit international dans le cyberespace.

Ce chapitre commence par examiner brièvement la double nature politique et juridique du processus avant de décrire les étapes pratiques que les États peuvent suivre pour élaborer une position nationale. Ces étapes comprennent l'identification des facteurs susceptibles de déclencher le processus, la détermination des parties prenantes concernées et de leurs rôles, la préparation, la planification et le commencement, le renforcement des capacités, la recherche, l'analyse et la rédaction, l'adoption et la publication, et enfin le suivi, la réflexion et la révision.

2. Les positions nationales en matière de politique publique et de procédures juridiques

La tendance récente des États à élaborer et à publier leur position nationale sur l'application du droit international dans le cyberespace reflète **l'évolution progressive** des efforts déployés pour lutter contre les menaces actuelles et potentielles associées à l'utilisation des technologies de l'information et de la communication (TIC).[1] Le droit international est un outil parmi d'autres – au même titre que les mesures de confiance, les mécanismes techniques et d'autres interventions – que les États utilisent pour relever les défis que pose la cybersécurité. L'élaboration d'une position nationale est, à la base, une réponse politique délibérée aux problèmes de cybersécurité auxquels un État est confronté.

Par conséquent, les positions nationales font intrinsèquement partie du **processus d'élaboration des politiques publiques**, dans la mesure où la loi incarne des valeurs et des choix politiques en constante évolution. La formulation d'une position implique de prendre en compte les préoccupations de politique étrangère et intérieure ainsi que les considérations de droit international, celles-ci étant inextricablement liées. À cette complexité s'ajoute la nature technique du domaine. Par conséquent, la question de savoir comment procéder (abordée dans ce chapitre) est souvent tout aussi difficile que celle de savoir ce qui doit être inclus (abordée au **chapitre 4)**.

La littérature et les modèles décrivant les mécanismes du processus d'élaboration des politiques publiques sont nombreux.[2] Ce processus est généralement décrit en plusieurs étapes, telles que l'identification du problème et la définition des priorités, la formulation des politiques, la prise de décision, la mise en œuvre et l'évaluation. Des orientations spécifiques à certains domaines, notamment les cadres pour l'élaboration de stratégies nationales en matière de cybersécurité,[3] peuvent fournir des informations précieuses sur la gestion du processus d'élaboration des politiques au sens large. Ces stratégies font souvent référence au droit international, comme en témoigne le Chili qui reconnaît que « le défi consiste notamment à être capable d'identifier et d'interpréter les réglementations pertinentes du droit international applicable ».[4] De même, la stratégie de cybersécurité 2020 de l'UE[5] a engagé le bloc à élaborer une position commune, adoptée en 2024. Cependant, si de telles stratégies peuvent contribuer à initier le processus, elles manquent généralement d'orientations détaillées sur les tâches juridiques impliquées, lesquelles exigent l'expertise de professionnels du droit. L'élaboration d'une position nationale s'appuie nécessairement sur des méthodologies et des processus juridiques propres à la discipline juridique.

1 Assemblée générale des Nations Unies, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* A/68/98 (24 juin 2013), par. 1-2.

2 Pour de plus amples informations sur les principales approches et études, voir Evangelia Petridou, « Theories of the Policy Process » (2014) 42 Policy Studies Journal S12.

3 *Guide to Developing a National Cybersecurity Strategy,* 2e édition (2021).

4 Gouvernement du Chili, *National Cybersecurity Policy* (2017-2022), 22.

5 Commission européenne, *The EU's Cybersecurity Strategy for the Digital Decade* (2020), 20.

Le développement et la publication de positions nationales détaillées constituent une tendance relativement récente. Sous l'impulsion répétée du Groupe de travail à composition non limitée (GTCNL) des Nations Unies, plus de trente États ont, à ce jour, rendu publique leur position nationale, et ce nombre ne cesse de croître. Toutefois, comme l'ont relevé plusieurs représentants d'États dans le cadre de ce projet, cette dynamique pourrait susciter des **attentes inédites**. Les États peuvent se sentir forcés de présenter, dans un seul document, leur conception globale de l'application du droit international, ce qui représente un niveau d'exhaustivité rarement observé dans d'autres contextes.[6] La complexité, associée à ces nouvelles attentes, soulève des questions importantes sur la manière de concevoir le processus d'élaboration d'une position nationale et sur la pertinence de combiner différentes méthodes à cette fin.

Le processus d'élaboration d'une position nationale comporte des implications importantes. Premièrement, il n'existe aucun protocole universellement reconnu pour en garantir le succès. Toutefois, certains éléments communs se dégagent des processus analysés dans le cadre de la préparation du présent Manuel. Deuxièmement, compte tenu de la complexité et du caractère interdisciplinaire de cet exercice, les États intègrent souvent une **combinaison d'étapes et de techniques** issues des processus d'élaboration des politiques publiques et de méthodologies propres au droit international. Troisièmement, les différences entre les positions nationales montrent que l'interprétation des règles est étroitement liée aux divergences politiques. Il est donc important de recourir à des méthodes empiriques et à des discussions fondées sur des scénarios tout au long du processus.

Les sections suivantes explorent les éléments clés du processus, en s'appuyant sur les pratiques existantes et les défis à relever. Cependant, ces éléments ne sont pas forcément présentés dans un ordre précis. Chaque État peut adapter le processus en fonction de la répartition des compétences, des procédures administratives et de la culture institutionnelle qui lui sont propres. Afin d'aider les responsables gouvernementaux à mener à bien cette tâche, le présent Manuel comprend également une liste de vérification concise décrivant les étapes clés, les considérations et les bonnes pratiques pour élaborer une position nationale (cf. **annexe A**).

6 Observation faite lors de l'atelier et du lancement du projet à CyCon, intitulé « National Position on International Law in Cyberspace : Challenges, Opportunities and Best Practices », 28 mai 2024, Tallinn (rapport conservé par les auteurs).

3. Facteurs déclenchants

Les États peuvent être amenés à élaborer une position nationale pour diverses raisons, même s'il peut parfois s'avérer difficile de simplement inscrire la question **à l'ordre du jour**. Dans certains cas, une cyberattaque majeure constitue un catalyseur évident,[7] et les parties prenantes n'ont guère besoin d'être convaincues. Cependant, il n'est pas toujours nécessaire de vivre des expériences douloureuses pour prendre conscience de l'importance de cette question.

Dans de nombreux cas, la participation à des discussions internationales pousse les États à élaborer une position ou, dans certains cas, à officialiser leurs opinions déjà formées.[8] Par exemple, les rapports du GTCNL ont à plusieurs reprises encouragé les États à partager leurs points de vue nationaux sur l'application du droit international à l'utilisation des TIC,[9] faisant ainsi de la soumission d'un tel document à l'ONU un objectif concret.[10] Lorsqu'ils prennent l'engagement de présenter une position nationale dans un forum international, les États peuvent se sentir contraints d'y donner suite afin de démontrer leur leadership et de servir d'exemple.[11]

L'élaboration d'une position nationale peut également être motivée par la nécessité de soutenir les messages de dissuasion ou de clarifier le cadre juridique régissant les capacités cyberoffensives.

Par exemple, la stratégie adoptée par l'Australie en 2016 en matière de cybersécurité reconnaît publiquement l'existence de capacités offensives dans le cyberespace et indique que l'État utilisera ces capacités conformément au droit international.[12] Une telle déclaration peut amener à préciser davantage comment les règles existantes sont censées s'appliquer aux opérations cybernétiques.

---

7 Observation faite lors du Troisième symposium annuel en présentiel sur le droit international et cybernétique, « Future Conflict : The International Law of Cyber and Information Convergence », dans le cadre du panel intitulé « Navigating Legal Dynamics : National Perspectives on International Law and Potentials for Convergence », American University, 24 septembre 2024, Washington, DC (rapport archivé par les auteurs).

8 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

9 Cf. par exemple, Assemblée générale des Nations Unies, *Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report,* A/AC.290/2021/CRP.2 (10 mars 2021), paragraphe 38 ; Assemblée générale des Nations Unies, *Report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025,* A/77/275 (8 août 2022), paragraphe 15 ; Assemblée générale des Nations Unies, *Report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025,* A/78/265 (1er août 2023), paragraphe 33 ; Assemblée générale des Nations Unies, *Report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025,* A/79/214 (22 juillet 2024), paragraphe 40.

10 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

11 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

12 Gouvernement australien, Australia's Cyber Security Strategy (2016), 28.

Les pressions internes peuvent également jouer un rôle. Les critiques formulées par les universitaires ou la société civile à l'égard de l'inaction perçue de l'État peuvent faire passer cette question au premier plan de l'agenda politique.[13] Par ailleurs, les États peuvent être amenés à engager ce processus en raison de la nécessité de mettre en œuvre une stratégie de cybersécurité, comme ce fut le cas pour l'Union européenne.[14] Certaines positions nationales permettent de déduire ce qui a motivé leur élaboration (ou leur consolidation), tandis que quelques-unes mentionnent explicitement leurs facteurs déclencheurs. Par exemple, le Japon indique dans sa position nationale qu'elle « a été élaborée à la demande du président du GEG [Groupe d'experts gouvernementaux des Nations Unies], à titre de contribution nationale ».[15] L'élaboration d'une position nationale peut également être motivée par des orientations politiques plus générales ; ainsi, la position de la Pologne indique qu'elle constitue « la continuation naturelle des deux années de participation de la Pologne en tant que membre non permanent du Conseil de sécurité (2018-2019), période durant laquelle le respect du droit international a été l'une des priorités de la Pologne ».[16]

Ces facteurs déclenchants ont contribué de manière significative à sensibiliser les parties prenantes, à définir la répartition des rôles dans le processus et à obtenir le mandat nécessaire pour lancer les premières étapes.

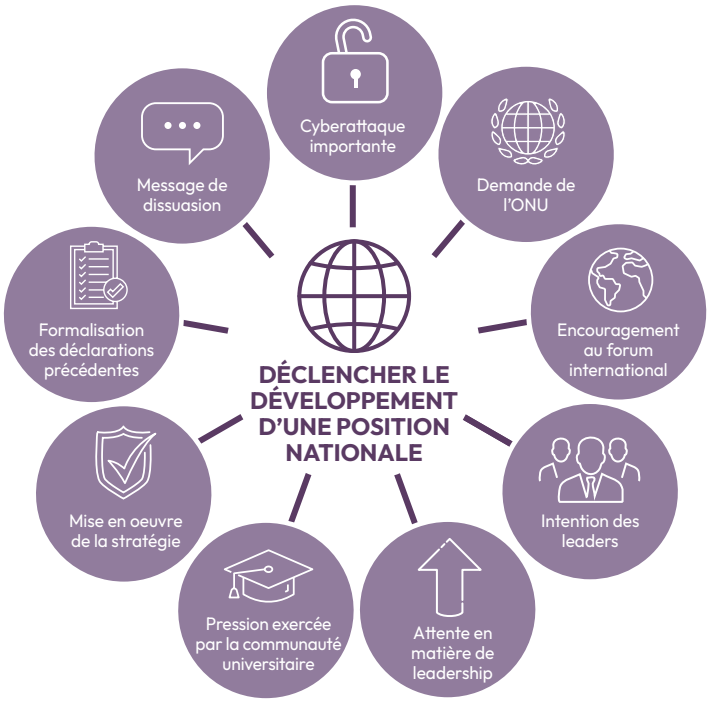


Figure 1 : Facteurs susceptibles de déclencher l'élaboration d'une position nationale.

13 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

14 Commission européenne, The EU's Cybersecurity Strategy for the Digital Decade (2020), 20.

15 Position nationale du Japon (2021), p. 1.

16 Position nationale de la Pologne (2022), p. 1.

4. Les parties prenantes et leurs rôles

À mesure que l'on prend conscience de l'importance et des défis liés à l'application du droit international dans le contexte cybernétique, le nombre d'acteurs impliqués dans l'élaboration des positions nationales augmente également. Ce qui n'était au départ qu'un débat restreint inclut désormais un **large éventail d'opinions**. Il est essentiel de recenser les acteurs concernés et de clarifier leurs rôles. En général, ces acteurs comprennent des agences gouvernementales, des consultants, des acteurs de la société civile et des universitaires, chacun exerçant un niveau d'influence différent.

Les États doivent s'efforcer de constituer une équipe multidisciplinaire composée d'experts **juridiques, politiques et techniques**. En effet, l'élaboration d'une position nationale nécessite une compréhension nuancée de trois dimensions interdépendantes : les cadres juridiques (ce qui est autorisé ou interdit), les implications stratégiques des décisions politiques (ce qui est préférable) et les réalités techniques du cyberespace (ce qui est possible). En fin de compte, une position nationale bien conçue doit concilier ces trois dimensions.

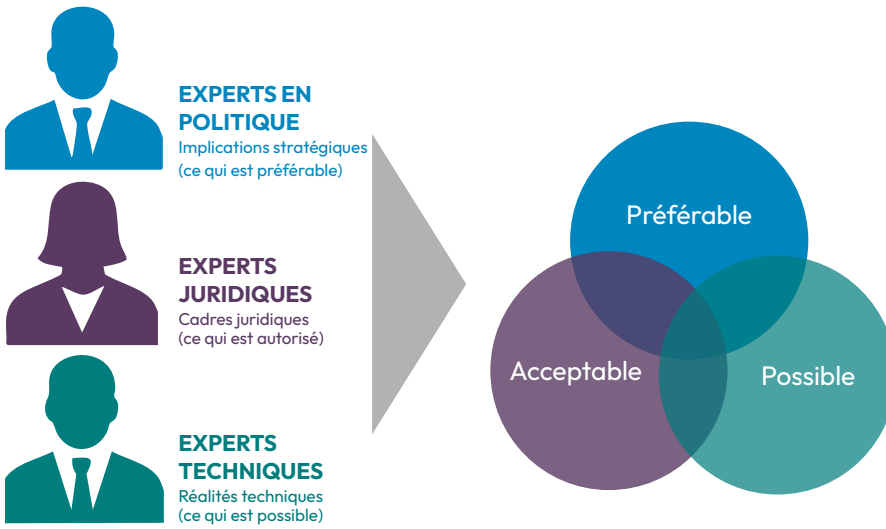


Figure 2 : Composition de l'équipe de rédaction.

Il est essentiel **d'identifier les agences** appelées à participer au processus, les personnes disposant de l'autorité nécessaire pour s'engager dans ce processus et/ou adopter une position, ainsi que les compétences qu'elles peuvent apporter.[17] Dans certains cas, les choses sont simples, par exemple lorsque la législation confère à une agence spécifique le pouvoir d'interpréter le droit international. Plus souvent, plusieurs agences ont un intérêt dans le processus, notamment celles qui s'occupent, par exemple, de la sécurité nationale, des affaires économiques, des infrastructures et des données numériques, de la défense, des affaires étrangères, des affaires juridiques et des communications.[18]

Certains États peuvent juger opportun de faire appel à plusieurs organismes, par exemple un organisme compétent en droit international et un autre disposant d'une expertise technique. Dans certains cas, comme l'a indiqué un expert gouvernemental, « la décision concernant les organismes qui participeront et celui qui dirigera les opérations a été prise de manière organique.[19] Dans d'autres cas, cette décision est prise de manière centralisée et les rôles sont attribués par les voies officielles. Quelle que soit l'agence qui prend la direction des opérations, il est essentiel de sensibiliser les autres institutions concernées, en particulier celles qui, au départ, ne considèrent pas cette question comme une priorité.[20] Au cours des tables rondes organisées dans le cadre du projet, les représentants des États ont souligné à plusieurs reprises la nécessité d'un large **soutien politique**, sans lequel le processus risque de stagner, voire de rester inachevé.

Les positions nationales ont une incidence sur le travail et les obligations des agences techniques et opérationnelles. Il s'agit d'entités dont les activités peuvent être considérées comme relevant de la pratique étatique et qui possèdent une expérience pratique ainsi qu'une connaissance approfondie des opérations cybernétiques. Par conséquent, leur contribution est déterminante dans l'élaboration des positions nationales. Les experts techniques et les agences telles que les équipes d'intervention en cas d'urgence informatique, les équipes d'intervention en cas d'incident de sécurité informatique et les centres d'opérations de sécurité jouent un rôle crucial, notamment dans l'analyse des effets des opérations cybernétiques aux niveaux national et international. Ces agences sont généralement chargées de détecter les incidents cybernétiques, d'y remédier et d'en atténuer les conséquences, tout en collaborant avec leurs homologues internationaux. Elles détiennent souvent des **informations essentielles** sur les opérations cybernétiques attribuables à des États, même si ces données sont parfois techniquement complexes, classifiées ou inaccessibles aux

Les contributions des agences techniques et opérationnelles peuvent influencer considérablement les positions nationales, qui à leur tour affectent leur travail.

17 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

18 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

19 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

20 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

professionnels du droit. Selon la répartition des capacités et des compétences, il en va de même pour les agences opérationnelles, telles que les services de renseignement et les forces de l'ordre, qui ont souvent **un accès direct aux données relatives aux activités cybernétiques** de divers acteurs, y compris des États. C'est également le cas des informations détenues par les agences de défense et les forces armées, qui disposent parfois de renseignements précieux sur les opérations cybernétiques. Le fait d'impliquer tous ces acteurs dans le processus, ne serait-ce qu'à titre consultatif, permet de garantir que les positions nationales s'appuient sur les réalités opérationnelles et reflètent une approche nationale cohérente, en particulier sur les questions où se croisent les considérations juridiques, techniques et militaires.

Le rôle du **rédacteur** compte parmi les plus influents dans ce processus. Si la rédaction d'une position nationale relève d'un effort collectif impliquant les parties prenantes au sein du gouvernement et parfois en dehors de celui-ci,[21] la nomination d'un ou plusieurs rédacteurs dédiés est cruciale. Ceux-ci seront chargés de diriger le processus juridique, de rédiger le texte initial et de veiller à ce que le produit final soit clair, cohérent et reflète le consensus entre les parties concernées.

Il est important de noter que le rédacteur n'est pas toujours le même que l'organisme chef de file ou le responsable politique du processus de développement. Si le chef de file est également le rédacteur, il est probable qu'il oriente le contenu de la discussion. Cependant, si les deux rôles sont séparés, le chef de file aura probablement le contrôle politique et le pouvoir de décision final, tout en garantissant la contribution technique et juridique des institutions de soutien. Dans un troisième modèle, l'organisme qui fait office de rédacteur peut être fortement soutenu par des organisations internationales ou des experts externes pour coordonner et faire avancer le processus (dans certains cas, des experts externes ont même été chargés de rédiger une première ébauche de la position).

Plusieurs participants à la table ronde ont fait remarquer que la désignation d'un ou plusieurs responsables de la rédaction et/ou du chef de file pouvait entraîner une **concurrence**, voire des conflits de compétences, entre les institutions. À l'inverse, d'autres ont souligne que certaines agences pourraient être **réticentes** à assumer le rôle de rédacteur principal, ce qui conduirait à une situation où la tâche « incomberait à tout le monde et à personne à la fois ».[22] Pour éviter cette situation, le choix du rédacteur et de l'agence principale devrait être effectué dès le début du processus ; ceux-ci devraient disposer de solides compétences en droit international et être capables de coordonner, négocier et trouver les compromis nécessaires pour mener à bien le processus. De même, l'agence principale devra généralement coordonner et collaborer avec les autres parties prenantes impliquées dans le processus afin de trouver des compromis.

21 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

22 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé by les auteurs).

Le moment où cela se produira dépendra de la manière dont le processus aura été conçu et du degré de maturité du débat sur la cybersécurité dans l'État

Certaines positions nationales se distinguent par leur structure et leur orientation. C'est le cas, par exemple, de la position nationale française de 2019, qui accorde une attention particulière au droit international humanitaire (DIH), davantage que la plupart des autres positions.[23] Cela reflète probablement le fait que cette position a été élaborée par le ministère des Armées et montre que le rédacteur principal et/ou l'agence responsable disposaient d'une expertise approfondie en droit applicable en temps de conflit armé.[24]

Étant donné que les compétences et les rôles liés au droit international leur incombent souvent, les ministère des Affaires étrangères sont souvent les principaux moteurs de la politique et du processus. Cependant, il peut arriver qu'il n'y ait pas d'agence principale chargée du droit international.[25] Dans certains États, les **compétences en matière de droit international** sont réparties entre deux ou plusieurs agences et les responsabilités peuvent être partagées, tandis que dans d'autres cas, une seule agence (ou aucune) dispose des connaissances et de l'expertise nécessaires. En outre, de nombreuses parties prenantes impliquées dans le processus peuvent ne pas avoir de formation juridique, sans parler d'expertise en droit international. Dans tous les cas, l'agence chef de file devrait pouvoir expliquer la pertinence d'une position nationale aux autres parties prenantes, notamment en quoi les décisions relatives à l'application du droit international aux activités cybernétiques peuvent les affecter. Cependant, cela fonctionne dans les deux sens : il est tout aussi important que les agences opérationnelles expliquent ce qu'elles font, afin que les experts juridiques et politiques aient une bonne compréhension des pratiques et ne se déconnectent pas de la réalité.

L'agence principale devrait pouvoir expliquer la pertinence d'une position nationale aux autres parties prenantes. Les agences opérationnelles devraient expliquer ce qu'elles font, afin que les experts juridiques et politiques aient une bonne compréhension de la pratique et ne se déconnectent pas de la réalité.

23 Position nationale de la France (2019), pp. 12-16.

24 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

25 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

Compte tenu de la rareté des compétences pertinentes, les **réseaux informels** jouent un rôle considérable. Par exemple, la participation aux discussions du GEG ou aux consultations du Manuel de Tallinn a aidé les États à renforcer leurs capacités et leur a permis de s'appuyer sur ces réseaux pour élaborer leur position.[26] Par conséquent, la création et l'adhésion à des réseaux informels permettent aux États d'exploiter une ressource très précieuse et de remédier à leurs faiblesses. Cependant, le recours à des experts et consultants externes peut nécessiter des engagements formels et être soumis à des restrictions, telles que des préoccupations en matière de sécurité ou des limites en matière de communications externes.[27]

De nombreux représentants d'États consultés dans le cadre de l'élaboration du présent manuel ont souligné le **rôle de la participation publique** dans la définition des positions nationales.[28] Cela permet de sensibiliser l'opinion publique, d'apporter de nouvelles perspectives, de légitimer le produit final et d'accroître la réceptivité de la société à l'égard des positions adoptées. Dans certains États, la participation du public peut même être une obligation légale. Dans d'autres cas, cela peut se faire de manière plus informelle.[29] Comme l'a souligné un représentant, le rôle du gouvernement peut se limiter à coordonner les positions et les opinions dans les secteurs concernés, le ministère des Affaires étrangères agissant en quelque sorte comme porte-parole.[30] Dans ce cas, la participation de tous est une priorité absolue.

Cependant, l'inclusion peut également compliquer le processus, entraînant potentiellement des retards dans la finalisation de la position nationale. Elle soulève également la question de savoir à quel moment il convient de consulter le public afin de laisser aux agences concernées le temps de réfléchir et de ne pas divulguer prématurément des informations sensibles. Si les consultations sont souhaitables en principe, elles n'ont pas été systématiques dans l'élaboration des positions nationales existantes.[31] Au minimum, les consultations devraient impliquer les principales parties prenantes, même si le grand public n'est pas inclus.

Enfin, il ne faut pas négliger le rôle des **entrepreneurs politiques**. Ces derniers sont des personnes très motivées, visionnaires ou universitaires dévoués qui se chargent de développer une position et la défendent avec habileté. Ces personnes peuvent apporter une contribution significative au processus en termes de leadership, d'expertise dans le domaine concerné et, en un mot, de capacité à faire bouger les choses.

26 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

27 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Afrique (rapport conservé par les auteurs).

28 Plusieurs observations faites lors des trois tables rondes organisées dans le cadre du projet (rapports conservés par les auteurs).

29 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

30 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

31 Plusieurs observations faites lors des trois tables rondes organisées dans le cadre du projet (rapports conservés par les auteurs).

5. Préparation, planification et lancement

Les préparatifs en vue de l'élaboration d'une position nationale commencent généralement par l'inscription de la question à l'ordre du jour ou par des efforts visant à persuader les décideurs de le faire (cf. **section 3** du présent chapitre). Au cours des étapes préliminaires, il convient d'examiner les rôles et les compétences, notamment en désignant une organisme chef de file (cf. **section 4** du présent chapitre). Que cela se fasse avant, parallèlement ou après le lancement officiel du processus et l'attribution d'un mandat à l'agence responsable dépend des spécificités de chaque État.

Au cours de la **phase de préparation et de planification**, il convient de préciser plusieurs détails importants. Il s'agit notamment de définir la portée de la position nationale, les participants et leur rôle, ainsi que le processus à suivre (c'est-à-dire les mesures à prendre et leur ordre d'exécution, ainsi que le calendrier).[32] Si certains représentants des États ont préconisé une approche proactive (« prenez simplement un stylo et rédigez un premier projet »),[33] cela pourrait ne pas correspondre à la culture bureaucratique de tous les États.[34]

Pour la préparation et la planification de projets, il existe un outil méthodologique largement utilisé, qui consiste à poser cinq questions essentielles : **Qui ? Quoi ? Pourquoi ? Quand ? Où ? Comment ?** Chaque catégorie aide à poser les questions essentielles pour guider le processus :

Qui ?	Les principales parties prenantes, notamment les décideurs, les experts, les autorités et les autres participants, etc.
Quoi ?	Portée, caractéristiques, livrables, résultats, événements, ressources, etc
Pourquoi ?	Objectifs, motivations, considérations politiques et juridiques, etc
Quand ?	Étapes, échéances, dates limites, etc
Où ?	Localisation physique et virtuelle des ressources, événements, etc
Comment ?	Méthodes, processus, procédures, plans, repères, suivi, allocation des ressources, etc.

32 UNIDIR, *A Compendium of Good Practices : Developing a National Position on the Interpretation of International Law and State Use of TIC* (2024), 17-18.

33 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

34 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

Pour **commencer**, il y a lieu d'établir des références de base ainsi que les hypothèses nécessaires, notamment quant à l'applicabilité du droit international aux comportements dans le cyberespace et à la manière dont la position envisagée traitera cette question. Il importe de définir clairement la finalité lors de l'élaboration d'une position nationale. La portée et la nature de la tâche (ainsi que le résultat attendu) doivent être déterminées avec rigueur, car elles conditionneront les exigences institutionnelles. L'interprétation du droit international peut relever de la compétence exclusive de certains organismes, la publication d'une déclaration officielle peut nécessiter l'approbation de l'autorité compétente, telle que le Conseil des ministres, ce qui est susceptible d'influer sur les délais, les procédures et d'autres éléments du plan.

La définition de la portée d'une position nationale peut s'avérer difficile dans un premier temps. Comme indiqué au **chapitre 4**, de nombreux domaines du droit international sont applicables aux TIC. Toutefois, ceux-ci peuvent être établis par ordre de priorité en fonction des besoins et des intérêts actuels de l'État. Dans ce contexte, certains représentants étatiques ont souligné l'importance de thématiques transversales telles que l'utilisation d'Internet et l'impact des technologies émergentes sur la paix internationale, tandis que d'autres ont souligné les enjeux relatifs à la lutte contre les discours de haine, la discrimination en ligne, ainsi que l'hostilité et la violence sur les réseaux sociaux.[35] D'autres stratégies visant à définir le champ d'application consistent à commencer par les questions les plus faciles à traiter, telles que la Charte des Nations Unies ou d'autres questions moins controversées, avant d'aborder les questions plus complexes.[36]

La planification doit tenir compte des **ressources disponibles**. Il est essentiel de réfléchir à la meilleure façon d'utiliser les ressources limitées de l'État pour élaborer une position nationale appropriée. Ces ressources comprennent le temps, le personnel et le financement nécessaire pour l'équipement, les fournitures, les consultants externes, la littérature et les télécommunications. La rareté des ressources peut avoir une incidence sur la manière dont les discussions aux niveaux national, régional et international seront organisées, le cas échéant. Différentes stratégies peuvent être utilisées pour maximiser les ressources et une réflexion créative peut s'avérer nécessaire. Pour combler les lacunes en matière de ressources, on pourrait envisager les stratégies créatives suivantes :

- Recruter des stagiaires et des bénévoles
- Impliquer la communauté universitaire nationale et les experts du secteur.
- Demander des subventions et des possibilités de financement.
- Collaborer avec les organisations régionales.
- Participer à des cours, tables rondes, séminaires et conférences (en personne ou à distance).
- Utiliser des sources librement accessibles et des projets internationaux existants.

35 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives africaines (rapport conservé par les auteurs).

36 Observations faites lors des tables rondes organisées dans le cadre du projet sur les perspectives de l'Asie et du Pacifique et sur les perspectives de l'Amérique latine et des Caraïbes (rapports conservés par les auteurs).

La durée du processus d'élaboration d'une position nationale peut varier de quelques mois à plusieurs années, en fonction de la complexité des enjeux et des capacités de l'État. Toutefois, il ressort des tables rondes organisées dans le cadre du projet qu'il ne s'agit pas d'un effort ponctuel : les positions peuvent et doivent être régulièrement réexaminées et actualisées pour tenir compte des nouveaux développements en matière de politique nationale, régionale ou multilatérale, ainsi que du droit international et de l'évolution de l'environnement cybernétique. Afin de garantir l'élaboration en temps opportun de la position nationale, il y a lieu d'établir des calendriers détaillés assortis d'échéances précises. L'objectif poursuivi est de gérer efficacement le processus, y compris le temps qu'il faut pour procéder aux consultations internes et externes, aux révisions et à l'approbation finale.

6. Renforcement des capacités

Pour élaborer efficacement une position nationale sur le droit international et les activités cybernétiques, il est essentiel de **renforcer** les capacités de toutes les parties prenantes concernées. Cela suppose un renforcement des compétences juridiques et techniques afin de garantir une compréhension approfondie du droit international et de son application aux TIC. Les activités de renforcement des capacités peuvent inclure notamment des exercices, des ateliers, des programmes de formation et des conférences, et elles tirent grandement parti de la collaboration aux niveaux bilatéral, régional et international. Ces activités doivent respecter les **principes de renforcement des capacités** définis par le Groupe de travail à composition non limitée (GTCNL) pour la période 2019-2021.[37] Ces principes sont divisés en trois catégories que sont : le processus et l'objectif, les partenariats et les personnes.

a. Processus et objectif

- Le renforcement des capacités doit être un processus durable, comprenant des activités spécifiques menées par et pour différents acteurs.
- Les activités spécifiques doivent répondre à un objectif clair et être axées sur les résultats, tout en soutenant l'objectif commun d'un environnement TIC ouvert, sécurisé, stable, accessible et pacifique.
- Les activités de renforcement des capacités doivent être fondées sur des données probantes, politiquement neutres, transparentes, responsables et sans conditions.
- Le renforcement des capacités doit être entrepris dans le plein respect du principe de souveraineté des États.
- Il peut être nécessaire de faciliter l'accès aux technologies pertinentes.

37 Assemblée générale des Nations Unies, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/75/816 (18 mars 2021), paragraphe 56.

b. Les partenariats

- Le renforcement des capacités doit être fondé sur la confiance mutuelle et axé sur la demande, correspondre aux besoins et priorités identifiés au niveau national et être entrepris dans le strict respect de l'appropriation nationale. Les partenaires doivent participer volontairement.
- Étant donné que les activités de renforcement des capacités doivent être adaptées à des besoins et contextes spécifiques, toutes les parties sont des partenaires actifs ayant des responsabilités communes mais différenciées, notamment en matière de collaboration dans la conception, l'exécution, le suivi et l'évaluation des activités de renforcement des capacités.
- La confidentialité des politiques et des plans nationaux doit être protégée et respectée par tous les partenaires.

c. Les personnes

- Le renforcement des capacités doit respecter les droits de l'homme et les libertés fondamentales, être sensible au genre et inclusif, universel et non discriminatoire.
- La confidentialité des informations sensibles doit être garantie.

Le renforcement des capacités reste un **défi** pour la plupart des États, même ceux qui disposent d'une expertise avancée, dans la mesure où la technologie évolue rapidement et où les discussions continuent de prendre de l'ampleur. Cela ne signifie pas pour autant que les besoins en matière de renforcement des capacités soient uniformes. Certains États disposent désormais de connaissances approfondies et d'équipes d'experts prêts à élaborer ou à réviser leur position nationale, et ces États pourraient agir en tant que donateurs pour le renforcement des capacités. D'autres États peuvent disposer de capacités solides, par exemple en matière de droit international général et dans certains domaines spécialisés, auquel cas les efforts de renforcement des capacités pourraient se concentrer davantage sur des questions spécifiques au cyberespace. Dans certains cas, cependant, une approche globale du renforcement des capacités peut s'avérer nécessaire.

Il est important de noter que la simple présence de professionnels qualifiés ne se traduit pas nécessairement par un renforcement effectif des capacités au sein des agences gouvernementales. Le plus important est de savoir si les fonctionnaires directement impliqués dans l'élaboration de la position nationale de l'État disposent de l'expertise nécessaire et s'ils sont en mesure de comprendre et de relever les défis juridiques et politiques associés. Cela revêt une importance particulière étant donné que les experts et les diplomates peuvent être réaffectés, mutés ou quitter la fonction publique : le même vivier de compétences n'est donc **pas toujours disponible** au sein d'une agence.

La familiarisation avec ce domaine nécessite souvent un certain niveau de **formation technique**.[38] Après tout, le cyberespace est un environnement créé par l'homme, basé sur des techniques et des normes d'ingénierie, mais ses répercussions sont vastes et affectent les sociétés et la vie quotidienne de manière tangible et intangible. De nombreuses questions juridiques dans ce domaine dépendent de la compréhension des détails spécifiques de la technologie.

Les États devraient activement mettre en œuvre des initiatives de renforcement des capacités pour toutes les parties prenantes impliquées dans l'élaboration de leur position nationale. Toutefois, il convient de donner la priorité au renforcement des capacités des organismes chefs de file et des parties prenantes clés. L'élaboration d'une position nationale et le renforcement des capacités **vont de pair**. En effet, le renforcement des capacités est une étape nécessaire pour garantir que la position soit éclairée, exhaustive et alignée sur les réalités du domaine cybernétique.

La diversité et le succès des initiatives mondiales, régionales et nationales de renforcement des capacités à travers le monde témoignent des avantages que présentent le partage d'expériences et la collaboration avec des acteurs non étatiques, notamment les universités et la société civile. En se faisant une idée des débats actuels dans ce domaine, les États peuvent mieux cerner les questions qu'ils souhaitent aborder dans leur position nationale et les points de vue qu'ils souhaitent adopter à leur sujet.[39]

38 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

39 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

Le Groupe de travail à composition non limitée a mis un accent particulier sur le renforcement des capacités, lequel constitue l'un des éléments centraux de son mandat. Il existe des **initiatives et des programmes de renforcement des capacités dans le domaine cybernétique** au sein des Nations Unies. Parmi les exemples récents (mais généraux), on peut citer la Table ronde mondiale de 2024 sur le renforcement des capacités en matière de TIC,[40] qui a porté sur une multitude de questions, allant même au-delà du droit international et des positions nationales, ou encore le projet de Portail mondial pour la coopération et le renforcement des capacités en matière de sécurité des technologies de l'information et de la communication.[41] En 2023, le Secrétariat des Nations Unies a mené un exercice de cartographie pour faire le point sur les efforts existants en matière de renforcement des capacités de sécurité des TIC.[42] Des dizaines de contributions ont été soumises par des États, des universités et des acteurs de la société civile, dont beaucoup ont énuméré des initiatives et des projets liés au renforcement des capacités en matière de droit international dans le contexte cybernétique. Ces informations sont disponibles dans la base de données documentaire du Groupe de travail à composition non limitée sur la sécurité et l'utilisation des technologies de l'information et de la communication.[43] Sur la base de cet exercice de cartographie, le Secrétariat des Nations Unies a compilé un document résumant les principales initiatives de renforcement des capacités par domaine thématique, y compris le droit international.[44]

Quelques exemples d'initiatives consacrées au droit international :

i. **Cyber Law Toolkit :**[45] Le *Cyber Law Toolkit* est une ressource accessible à l'échelle mondiale, élaborée par un consortium réunissant l'Agence nationale tchèque de cybersécurité et de sécurité de l'information, le Comité international de la Croix-Rouge (CICR), le Centre d'excellence pour la cyberdéfense coopérative, accrédité par l'OTAN, l'Université d'Exeter, le US Naval War College et l'Université de Wuhan. Accessible gratuitement à tous, y compris aux fonctionnaires gouvernementaux et aux professionnels du droit, le Toolkit comprend, au moment de la rédaction du présent document :

   a. Un nombre croissant de scénarios (actuellement 32) explorant l'applicabilité du droit international aux opérations cybernétiques.

   b. Une base de données répertoriant les positions nationales existantes sur l'application du droit international dans le contexte cybernétique.

   c. Une base de données d'exemples, qui recense actuellement plus de 70 incidents cybernétiques.

40 La table ronde mondiale sur le renforcement des capacités en matière de sécurité des TIC, qui s'est tenue à New York le 10 mai 2024, a été le premier événement organisé sous les auspices des Nations Unies consacré à la question du renforcement des capacités. Cf. rapport connexe : Giacomo Persi Paoli, Samuele Dominioni, Aamna Rafiq, Lenka Filipová, *Accelerating TIC Security Capacity-Building: Takeaways from the Global Roundtable on TIC Security Capacity Building*, UNIDIR, Genève (2024).

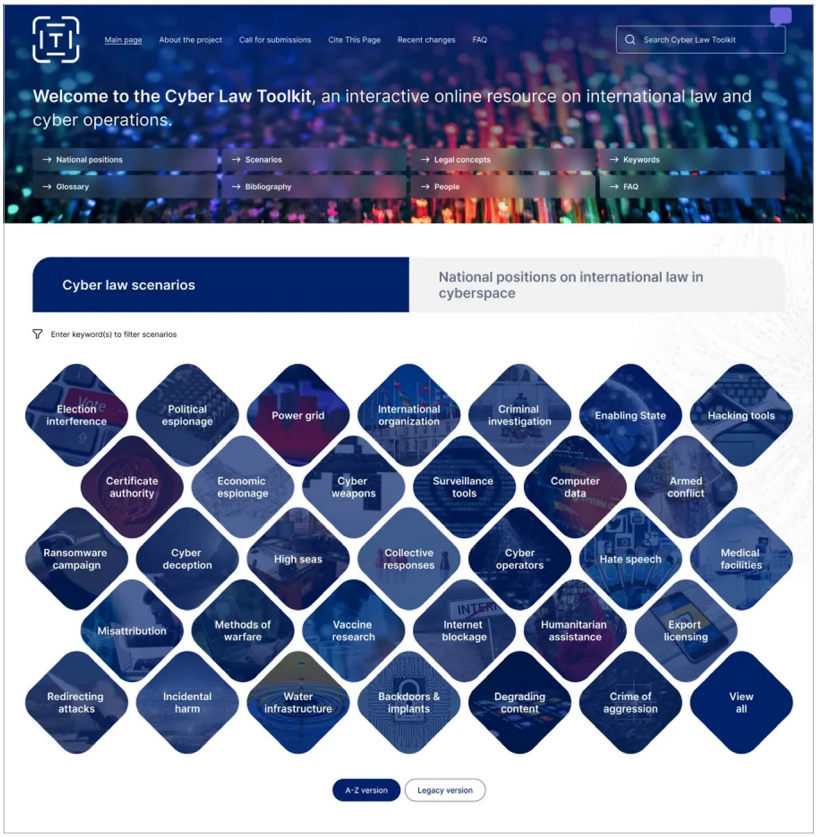
41 Cf. Assemblée générale des Nations Unies, *Initial report outlining the proposal for the development and operationalization of a dedicated Global Information and Communications Technologies Security Cooperation and Capacity-Building Portal*, A/AC.292/2025/1 (14 janvier 2025).

42 Secrétariat de l'ONU, *ODA/2023-00042/TIC-Mapping Exercise* (2 octobre 2022).

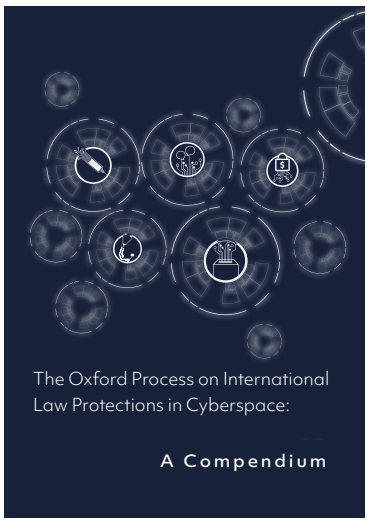
43 UNODA, Open-Ended Working Group on Information and Communication Technologies, *Documents*.

44 Assemblée générale des Nations Unies, *Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional levels*, A/AC.292/2024/2 (22 janvier 2024).

45 Cf. https://cyberlaw.ccdcoe.org.



ii. **Le processus d'Oxford sur les protections du droit international dans le cyberespace :** Lancée en 2020 par l'Oxford Institute for Ethics, Law and Armed Conflict en partenariat avec Microsoft, cette initiative a donné lieu à cinq « déclarations d'Oxford sur les protections du droit international dans le cyberespace ». Ces déclarations sont le fruit d'une collaboration entre des experts juridiques internationaux du monde entier visant à préciser quels comportements sont interdits ou autorisés dans le cyberespace en vertu du droit international dans divers contextes, notamment les soins de santé, la recherche et le développement de vaccins, les élections, la réglementation des opérations d'information et le ransomware.

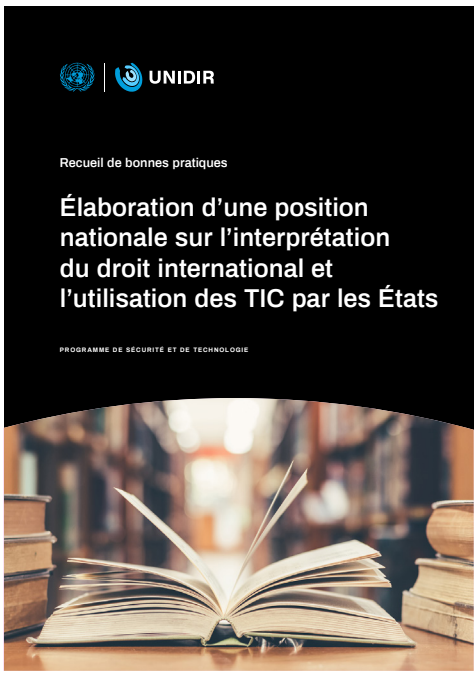


iii. **Ressources du CICR sur le DIH et le cyberespace :** Le CICR fournit des ressources et des conseils sur l'application du DIH au cyberespace aux décideurs politiques, notamment par le biais de dialogues bilatéraux, d'ateliers et de publications.[46] Le CICR pourrait également être en mesure de conseiller les États sur la partie de leur position nationale relative au DIH. Parmi les autres activités organisées par le CICR, on peut citer des programmes d'action humanitaire en coopération avec les milieux universitaires, des tables rondes et d'autres initiatives de collaboration.

46 CICR, *International humanitarian law and cyber operations during armed conflicts* (2019).

De nombreux pays et organisations internationales proposent des formations et des cours destinés aux fonctionnaires, notamment l'Association des nations de l'Asie du Sud-Est (ANASE), l'Organisation pour la sécurité et la coopération en Europe (OSCE) et l'Organisation des États américains (OEA). L'Estonie a lancé les Ateliers de Tallinn sur le droit international et les cyberopérations, basés sur des scénarios. L'objectif principal de ces ateliers thématiques est de créer un forum de discussion international entre les partenaires et d'offrir la possibilité d'examiner les questions de droit international les plus pertinentes liées au comportement des États dans le cyberespace. Cinq ateliers ont été organisés et les rapports des quatre premiers ont été publiés dans un recueil.[47]

En plus de ce qui précède, le *Recueil des bonnes pratiques 2024 : Élaboration d'une position nationale sur l'interprétation du droit international et l'utilisation des TIC par les États,* publié par l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR)[48] est une ressource structurée, concise et axée sur les processus. Il propose une compilation des meilleures pratiques et des informations exploitables, une lecture indispensable pour les responsables de l'élaboration d'une position nationale. De nombreux experts gouvernementaux consultés dans le cadre de ce projet ont souligne l'utilité pratique de ce recueil.[49]



47 Ministère des Affaires étrangères de l'Estonie, *Tallinn Workshops on International Law and Cyber Operations: Compendium of reports* (2023).

48 UNIDIR, *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of TIC* (2024).

49 Plusieurs observations faites lors des trois tables rondes organisées dans le cadre du projet (rapports conservés par les auteurs).

7. Recherche, analyse et rédaction

a. Approches

Aux premiers stades de l'élaboration d'une position nationale, de nombreux États ne disposent que d'une expérience et d'une expertise limitées dans ce domaine. Seuls quelques-uns ont déjà acquis des connaissances préalables, souvent grâce à leur participation à des initiatives telles que le GEG et le processus du Manuel de Tallinn. Par conséquent, l'élaboration d'une position nationale nécessite généralement des recherches approfondies, la collecte d'informations et des consultations.

Les États adoptent généralement l'une des deux approches suivantes pour structurer ce processus : l'approche par élimination ou l'approche par inclusion.

- **Approche par élimination :** Cette méthode commence par la rédaction d'un document de recherche approfondi qui identifie les thèmes communs et les domaines nécessitant des recherches supplémentaires. Ce document est ensuite progressivement affiné, adapté et simplifié afin de définir la position nationale.[50]
- **Approche par inclusion :** Cette méthode commence par un plan général qui est développé et révisé au fur et à mesure de l'avancement du projet, en intégrant les recherches supplémentaires et les commentaires reçus en cours de route.[51]

Quelle que soit l'approche choisie, le processus s'étend généralement sur plusieurs mois, voire plusieurs années, et implique de multiples itérations du projet.[52]

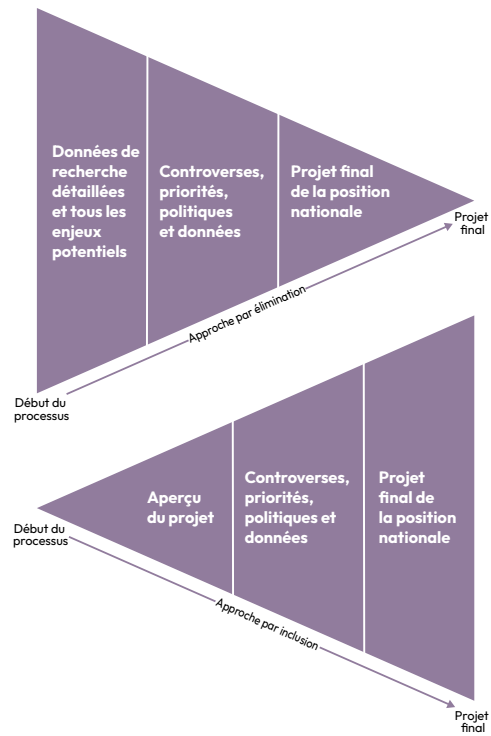


Figure 3 : Deux principales approches de rédaction.

50 Observation faite lors du Troisième symposium annuel en présentiel sur le droit international et la cyberlégislation, « Future Conflict : The International Law of Cyber and Information Convergence », dans le cadre du panel intitulé « Navigating Legal Dynamics : National Perspectives on International Law and Potentials for Convergence », American University, 24 septembre 2024, Washington, DC (rapport conservé par les auteurs).

51 Observations faites lors des tables rondes organisées dans le cadre du projet sur les perspectives en Asie et dans le Pacifique et sur les perspectives en Amérique latine et dans les Caraïbes (rapports conservés par les auteurs).

52 Observations faites lors des tables rondes organisées dans le cadre du projet ont indiqué une durée d'un à trois ans et au moins trois itérations du projet.

b. Sources du droit international et autres références

L'élaboration d'une position nationale nécessite des recherches approfondies afin de recueillir des informations pertinentes et d'évaluer les questions juridiques et politiques associées. Une grande partie des informations initiales peut être recueillie par le biais de recherches documentaires, principalement à partir de sources accessibles au public. Il s'agit notamment de documents juridiques et politiques, de rapports et de publications universitaires, spécifiques au cyberespace ou généraux. Ces documents sont indispensables au processus de recherche et à la définition d'une position nationale, notamment pour comprendre les débats actuels et leurs implications, les politiques nationales et les domaines prioritaires potentiels.

Il est important de distinguer ces documents de référence des sources formelles du droit international définies à l'article 38 du Statut de la Cour internationale de justice (CIJ). Si les sources formelles – telles que les traités, le droit international coutumier et les principes généraux du droit – sont essentielles à la préparation des positions nationales, d'autres documents fournissent des informations de fond, un contexte et des lignes directrices indispensables. Les différentes sources suivantes peuvent être consultées pendant le processus de rédaction :

- **Positions nationales :** Les positions nationales existantes constituent une ressource essentielle. Elles peuvent être comparées et analysées, et fournissent une base pour la compréhension et l'inspiration dans le choix des thèmes ou des interprétations.[53]
- **Documents provenant des instances spécialisées et des groupes d'experts des Nations Unies :** Des discussions spécifiques ont eu lieu au sein de la Première Commission de l'Assemblée générale des Nations Unies, et des groupes d'experts ont étudié les questions relatives au droit international et au cyberespace. Les résultats des six GEG[54] et des deux GTCNL (2019-2021[55] et 2021-2025[56]) sont rassemblés et mis à disposition sur le site web du Bureau des affaires de désarmement des Nations Unies (UNODA). Ils comprennent les comptes rendus des déclarations des gouvernements soumises à ces groupes.

53 The *Cyber Law Toolkit*, disponible à l'adresse , rassemble une série de positions nationales et communes.

54 UNODA, Group of Governmental Experts on Developments in The Field of Information and Telecommunications in The Context of International Security.

55 UNODA, Open-Ended Working Group on Developments in The Field of Information and Telecommunications in The Context of International Security.

56 UNODA, Open-ended Working Group on Security of and in the Use of Information and Communications Technologies.

- **Autres sources de l'ONU :** Diverses entités, organes, comités, agences et institutions des Nations Unies ont abordé différents aspects du droit international susceptibles de concerner les TIC. On peut citer notamment les résolutions de l'Assemblée générale des Nations Unies, les textes de la Commission du droit international (CDI),[57] les rapports et publications de l'UNIDIR,[58] les comptes rendus des déclarations faites devant la Sixième Commission de l'Assemblée générale des Nations Unies, ainsi que d'autres documents et publications spécialisés.
- **Sources académiques axées sur le cyberespace :** Il s'agit d'une catégorie très vaste qui comprend d'innombrables ouvrages universitaires et articles de revues consacrés à différents aspects du droit international dans le contexte cybernétique. Certaines positions nationales font référence à des sources universitaires spécifiques, par exemple les *Manuels de Tallinn,* la « *Cyber Law Toolkit* » et *le Processus d'Oxford*.[59] Des publications telles que la Revue internationale de la Croix-Rouge, « *International Law Studies* » ou le « *Journal of Cyber Policy* » proposent également des articles en libre accès sur le droit international et les activités cybernétiques.
- **Documents provenant d'organisations internationales :** Divers documents thématiques publiés par des organisations internationales traitent directement ou indirectement de cette question. On peut citer, à titre d'exemple, les publications de l'ANASE,[60] de l'UA,[61] du Conseil de l'Europe,[62] de l'UE,[63] du CICR,[64] de l'OEA,[65] aet de l'OSCE.[66]
- **Sources primaires et secondaires du droit international :** La plupart des États utilisent les sources traditionnelles du droit international, telles qu'énoncées à l'article 38 du Statut de la CIJ, et se réfèrent expressément aux traités internationaux, au droit international coutumier, aux principes généraux du droit, à la jurisprudence internationale et aux ouvrages universitaires. Ces sources sont essentielles pour élaborer des déclarations juridiques bien fondées et convaincantes.

57 Il s'agit principalement du projet d'articles de la CDI, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries* (2001).

58 UNIDIR, Cyber security.

59 Cf. par exemple, les positions nationales de l'Autriche (2024), p. 3, du Costa Rica (2023), paragraphe 6, et de la République tchèque (2024), p. 1.

60 ANASE, Cyber security.

61 Position commune de l'UA (2024).

62 Pour les questions relatives aux droits de l'homme et à l'État de droit, y compris la Convention de Budapest, voir le Conseil de l'Europe.

63 Conseil de l'Union européenne, *Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace* (2024).

64 Cf. les documents du CICR sur les opérations cybernétiques et de renseignements.

65 OEA, Cybersecurity Program.

66 OSCE, Cyber/TIC Security.

- **Sources nationales :** Certains États font référence à leur législation et à leurs politiques nationales[67] ainsi qu'aux déclarations et aux documents stratégiques des organisations régionales dont ils sont membres.[68] En outre, la jurisprudence nationale, les mémorandums internes, les positions exprimées dans le cadre de processus internationaux et de nombreuses autres ressources nationales peuvent être utilisés par les rédacteurs d'une position nationale pour clarifier les déclarations et mieux comprendre le contexte, les faits historiques et les arguments antérieurs. Les positions nationales non publiées partagées entre partenaires proches peuvent également constituer des sources influentes et utiles.

c. Consultations

Si le calendrier des consultations varie, il convient en général de les organiser dès le début du processus. Cela dépend toutefois du calendrier des efforts de renforcement des capacités ainsi que de l'approche globale adoptée pour le processus de rédaction (c'est-à-dire s'il adopte une approche d'élimination ou d'inclusion). Les États ont adopté l'un des deux principaux modèles de consultation suivants :

- **Modèle de routage parallèle :** La version la plus simple de ce modèle consiste à ce que toutes les agences ou parties prenantes (désignées par PP dans les figures 4 à 6) commencent à coordonner les différents points de vue dès le début et poursuivent cette coordination tout au long du processus. Une autre solution consiste à ce qu'une ou deux agences prennent l'initiative dès le début (indiquées par PP1 dans la figure 5) et que les autres agences soient invitées à participer aux discussions une fois la position définie.[69] Le projet peut être consolidé de temps à autre après des cycles de consultation (indiqués par les flèches dans les figures 4 et 5).

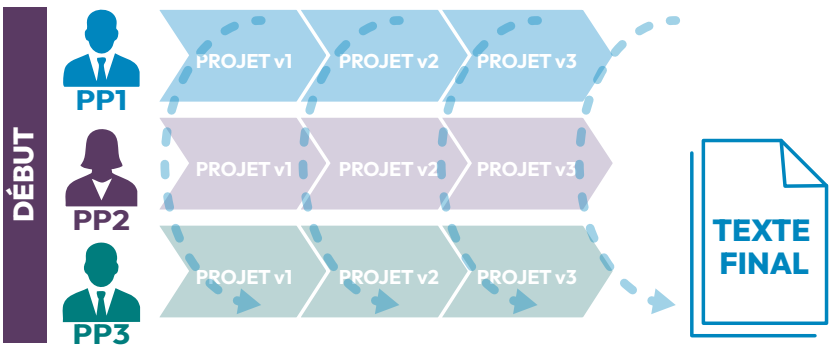


Figure 4 : Routage parallèle avec coordination globale.

67 Cf. par exemple, les positions nationales de Cuba (2024), paragraphes 1-2, et du Kenya (2021), pages 53-54.

68 Cf. par exemple, la position nationale de la Pologne (2022), pp. 1-2.

69 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

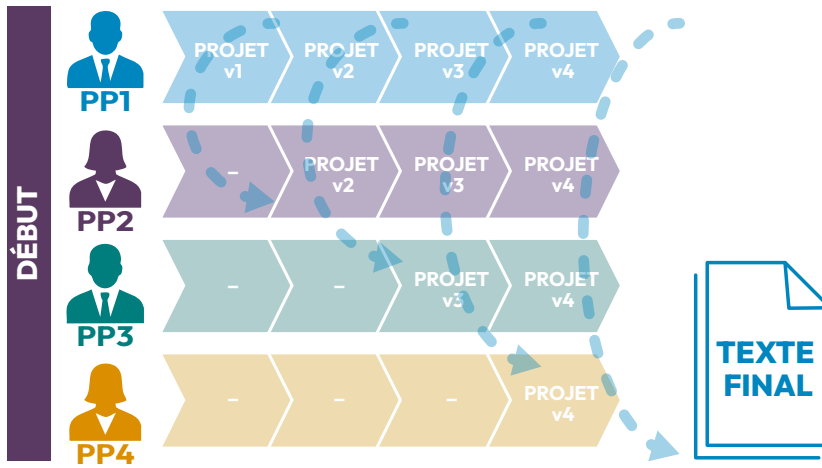


Figure 5 : Acheminement parallèle avec coordination centrale.

Les parties prenantes concernées peuvent être consultées en tant que groupe unique ou de manière progressive à mesure que la position s'affine. Cependant, les consultations progressives risquent de créer des flux de travail parallèles, lesquels peuvent être longs et difficiles à coordonner, harmoniser et consolider. Un spécialiste consulté pour la rédaction du présent Manuel a suggéré de diffuser un plan annoté (plutôt qu'un projet complet) pour obtenir jusqu'à trois commentaires par sujet, avant de décider quels domaines nécessitent davantage de travail.[70]

70 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport disponible auprès des auteurs).

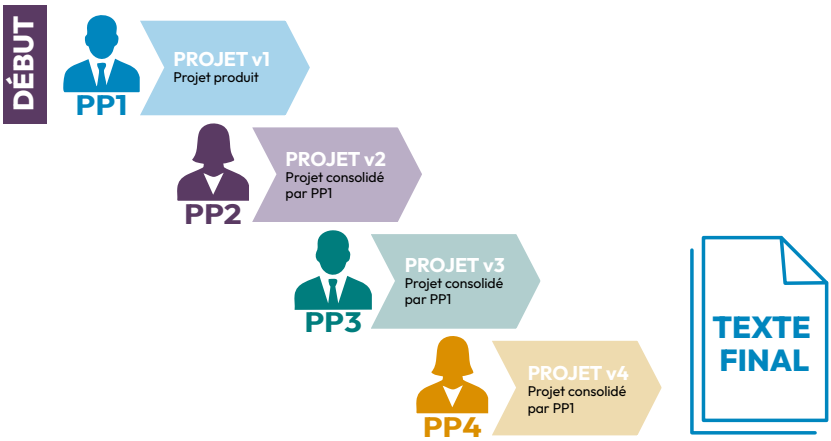


Figure 6 : Acheminement continu avec coordination centrale.

- **Modèle d'acheminement continu :** Cette approche consiste à mener des consultations de manière continue, en diffusant les projets de manière séquentielle auprès des différents groupes de parties prenantes (voir figure 6). Il est possible que certaines parties prenantes n'aient qu'une seule occasion de formuler des commentaires et des suggestions. Cependant, ce modèle est plus rationalisé et peut être plus facile à gérer.

Les deux modèles peuvent également être combinés, et les différentes étapes peuvent être répétées.

Les consultations peuvent être internes ou externes, notamment :

- **Des collaborations interinstitutionnelles ou interministérielles :** Pour élaborer une position nationale cohérente, il est essentiel de mettre en place une collaboration interinstitutionnelle efficace, laquelle implique un dialogue régulier avec les ministères concernés. Il peut s'agir des agences nationales chargées de la cybersécurité, de divers ministères (par exemple, ceux de la défense, de la justice, de l'intérieur et des communications), ainsi que des forces armées et des organes juridiques, tels que le bureau du procureur général ou les instances judiciaires.[71]
- **Des consultations avec des représentants de gouvernements étrangers :** La collaboration ou la consultation avec d'autres États sur une base bilatérale ou multilatérale peut s'avérer utile à différentes étapes du processus. Par exemple, les rédacteurs ou les experts impliqués dans l'élaboration de la position nationale d'un autre État peuvent contribuer à la conception et au lancement du processus. De même, les consultations externes peuvent servir d'exercice de renforcement des capacités pour l'équipe centrale de l'État et les autres parties impliquées

71 UNIDIR, *A Compendium of Good Practices*: Developing a National Position on the Interpretation of International Law and State Use of TIC (2024), 20.

dans le processus.[72] Des experts externes peuvent également apporter leur contribution pendant le processus de rédaction, par exemple en donnant des conseils sur des questions de fond ou de procédure, ou en facilitant la poursuite des discussions au niveau régional.

- **Des consultations avec les parties prenantes non étatiques :** Ces parties prenantes peuvent être des associations professionnelles nationales ou internationales, des groupes de réflexion, des cabinets de conseil, des industries, des groupes autochtones, des académiques ou des membres individuels de la société civile (voir la **section 4** du présent chapitre). Comme l'a fait remarquer un représentant de l'État lors des tables rondes organisées dans le cadre du projet, dans les États où les processus d'élaboration des politiques publiques sont très inclusifs, il convient également de tenir compte du phénomène de « lassitude face aux consultations ». Dans l'ensemble, les États devraient s'efforcer de trouver le juste équilibre entre les contributions utiles et la collaboration, sans submerger les parties prenantes consultées.

Les consultations peuvent également **prendre différentes formes**. Elles peuvent être formelles ou informelles, écrites ou orales, en personne ou virtuelles (ou hybrides), interactives ou unidirectionnelles. Les consultations informelles permettent d'éviter les obstacles bureaucratiques importants. Elles peuvent donc être plus faciles et plus rapides à organiser et offrent une plus grande liberté et flexibilité dans l'échange de points de vue. Elles peuvent favoriser une réflexion novatrice et le développement de relations. Cependant, les consultations informelles ne conviennent pas à toutes les situations. Des réunions formelles peuvent s'avérer nécessaires pour les questions complexes qui nécessitent une documentation détaillée et des comptes rendus officiels. Les enquêtes et les questionnaires peuvent être utiles dans des contextes internes et externes, en particulier lorsque différentes agences participent aux discussions.[73] Cependant, les parties prenantes concernées peuvent manquer d'intérêt ou de ressources, ou être réticentes à répondre en raison, par exemple, du caractère sensible ou confidentiel de certaines questions (telles que celles relatives à l'attribution ou au DIH). Enfin, les réunions publiques ou les séances d'écoute peuvent s'avérer particulièrement utiles au début du processus de rédaction.[74] Ces séances peuvent prendre la forme de réunions publiques et consistent essentiellement en une communication unidirectionnelle entre les représentants gouvernementaux chargés d'élaborer une position nationale et les membres intéressés du public ou de l'industrie. L'objectif principal est de recueillir des idées, des préoccupations, des commentaires et des suggestions qui pourraient être utilisés ultérieurement dans le cadre du processus, ou d'identifier les domaines et les questions qui bénéficient d'un soutien suffisant pour faire l'objet de déclarations publiques.

72 Commentaire lors du Troisième Symposium annuel en présentiel sur le droit international et cybernétique, « Conflits futurs : le droit international de la cybernétique et de la convergence de l'information », dans le cadre du panel « Naviguer dans la dynamique juridique : perspectives nationales sur le droit international et les possibilités de convergence », American University, 24 septembre 2024, Washington, DC (rapport conservé par les auteurs). Consultez également, par exemple, la série d'ateliers de Tallinn organisés par le ministère des Affaires étrangères de l'Estonie.

73 Observations faites lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

74 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives en Asie et dans le Pacifique (rapport conservé par les auteurs).

d. Analyse

En ce qui concerne la nature juridique des positions nationales et le processus de leur élaboration, il existe une vaste littérature consacrée à la détermination de **l'existence et du contenu des règles**.[75] Avant même que le Groupe d'experts gouvernementaux ne rende sa conclusion historique en 2013 sur l'applicabilité du droit international dans le contexte cybernétique,[76] les discussions sur la manière dont les différentes règles s'appliquent s'intensifiaient déjà. Les positions nationales portent sur l'identification des règles applicables, en particulier le droit international coutumier, ainsi que sur leur interprétation en matière de comportement dans le cyberespace. Pour élaborer leurs positions nationales, les États peuvent recourir à la logique déductive et inductive, y compris conjointement (voir également le chapitre 5 sur le format et le style).

La stratégie de cadrage fait appel au **raisonnement déductif**, qui consiste à identifier en premier lieu les questions les plus faciles à traiter, telles que l'applicabilité de la Charte des Nations Unies (voir la **section 5** du présent chapitre). Les positions nationales font souvent référence aux rapports du GEG et du GTCNL, qui énoncent généralement l'applicabilité du droit international dans le contexte cybernétique, puis passent de cette déclaration générale à des règles plus spécifiques. La logique déductive peut être vérifiée en trouvant des exemples et des scénarios qui confirment l'exactitude des conclusions sur des règles spécifiques.

D'autre part, le **raisonnement inductif** se manifeste par une logique qui commence par identifier les problèmes et les incidents, tels que le ransomware ou la désinformation, puis élabore une position autour de ces questions. Comme mentionné au **chapitre 5**, de nombreux États font référence à des scénarios dans leurs documents de position[77] et un nombre encore plus important d'États encouragent ou auraient utilisé des scénarios dans le processus d'élaboration.[78]

75 Cf. par exemple, les *Manuels de Tallinn* 1.0 et 2.0.

76 Assemblée générale des Nations Unies, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (24 juin 2013), paragraphe 19.

77 Voir, par exemple, les positions nationales de l'Australie (2021), de l'Autriche (2024), du Canada (2022), du Costa Rica (2023), de la République tchèque (2024), de l'Italie (2021), des Pays-Bas (2019) et du Royaume-Uni (2022).

78 Plusieurs observations faites lors des trois tables rondes organisées dans le cadre du projet (rapports conservés par les auteurs).

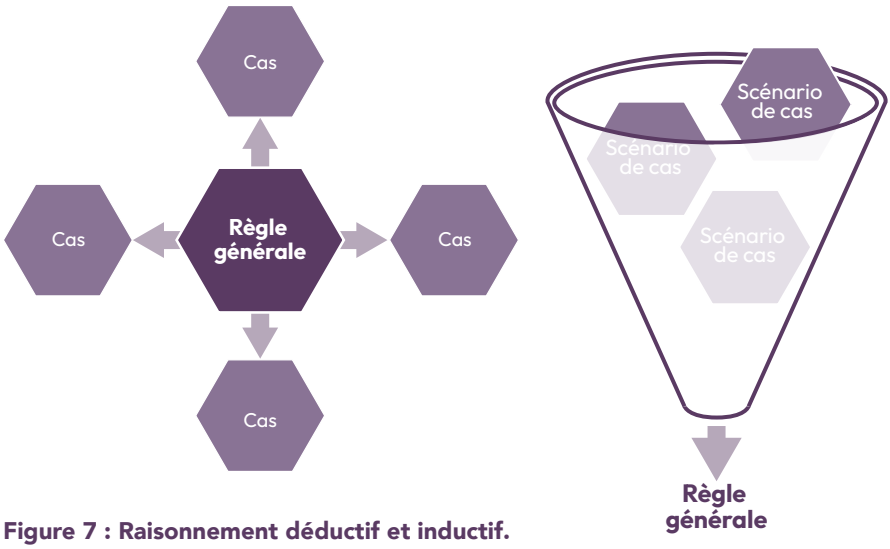


Figure 7 : Raisonnement déductif et inductif.

Le fait d'examiner différentes formulations abstraites d'un concept et de « reproduire » un scénario peut mettre en lumière des différences pratiques importantes dans l'application réelle, et facilite l'illustration d'une position dans le texte ou lors des consultations. Cependant, au cours des tables rondes organisées dans le cadre du projet, il est apparu que, malgré leur utilité, certains États peuvent être réticents à s'engager dans des discussions basées sur des scénarios, du moins dans les forums mondiaux. Au moins un expert gouvernemental a suggéré que ces discussions peuvent être considérées comme trop révélatrices de la position de l'État au sujet du cas. Un représentant d'État a déclaré que cette réticence peut être due à leur utilisation peu fréquente et au fait que certains États se sentent défavorisés.[79]

D'autres conseils sur l'identification des règles et des outils d'interprétation sont disponibles ici :

- Projet de conclusions de la CDI sur l'identification du droit international coutumier (2018).[80]
- Projet de conclusions de la CDI sur l'identification et les conséquences juridiques des normes impératives du droit international général (*jus cogens*) (2022).[81]
- La Convention de Vienne sur le droit des traités (1969).

79 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport conservé par les auteurs).

80 CDI, *Draft conclusions on the identification of customary international law, with commentaries*, A/73/10 (2018).

81 CDI, *Draft conclusions on identification and legal consequences of peremptory norms of general international law (jus cogens)* (2022).

8. Adoption et diffusion

Pour conclure et approuver une position nationale, il est nécessaire de mener une réflexion approfondie afin de s'assurer que toutes les parties prenantes concernées sont alignées et que cette position reflète fidèlement les opinions de l'État. L'État doit également déterminer quel(s) organe(s) interne(s) est (sont) compétent(s) pour **adopter ou approuver officiellement** la position nationale, conformément à ses cadres juridiques nationaux. Cette décision est souvent prise pendant la phase de planification, comme indiqué à la **section 5** du présent chapitre.

L'adoption ou l'approbation officielle de la position nationale peut également nécessiter le respect d'un **processus institutionnel** clairement défini. Il s'agit notamment de désigner l'autorité spécifique chargée de l'approuver. Il est important de clarifier cette question dès le début. Par exemple, certains États peuvent exiger que la position soit soumise à un organe législatif pour approbation, tandis que d'autres peuvent imposer son adoption par un organisme exécutif particulier, tel qu'un ministère ou un conseil des ministres.

Les États peuvent choisir de garder une position nationale interne ou non publiée. Les positions nationales incluses dans le présent manuel ont été rendues publiques, par exemple en les publiant dans un journal officiel, en les affichant sur un site web gouvernemental ou encore en les présentant à des forums internationaux tels que le Groupe de travail à composition non limitée GTCNL ou des plateformes similaires. Comme indiqué plus en détail au **chapitre 5**, les pratiques de diffusion des positions nationales publiques varient et reflètent la nature et les formats différents de ces documents.

9. Suivi, réflexion et révision

Après avoir élaboré une position nationale, un État peut souhaiter examiner si des mesures supplémentaires sont nécessaires pour **mettre en œuvre** certains éléments spécifiques de ladite position. Si une mise en œuvre est requise, il convient de préparer un plan de travail détaillé et un budget afin de soutenir ces efforts. En outre, si la position définit certains objectifs, des mécanismes doivent être mis en place pour suivre et évaluer les progrès accomplis au fil du temps.

Il arrive également que les positions nationales soient réexaminées, lorsque certaines questions nécessitent un **examen plus approfondi** ou que les interprétations juridiques ont **évolué**. Cette révision n'implique pas nécessairement un changement radical de perspective, mais peut s'appuyer sur des points de vue déjà exprimés. À mesure que la technologie et ses applications continuent d'évoluer, il est inévitable que de nouvelles questions se posent, nécessitant une mise à jour de la position nationale.

Un État peut souhaiter examiner si des mesures supplémentaires sont nécessaires pour mettre en œuvre certains éléments spécifiques de la position.

Néanmoins, la révision d'une position nationale n'est pas sans difficultés. La capacité d'un État à modifier sa position peut être limitée par la nécessité de **justifier** ces modifications par de nouvelles circonstances, preuves ou considérations qui n'avaient pas été prises en compte auparavant. Des changements soudains ou importants dans la position peuvent avoir des conséquences importantes au niveau de la réputation, ce qui peut nuire à la crédibilité de l'État sur la scène internationale.[82]

10. Conclusion

L'élaboration d'une position nationale relève d'un **processus politique et juridique**, déclenché par diverses circonstances. Celles-ci peuvent aller de cyberattaques importantes à la réalisation d'engagements internationaux ou nationaux.

Une première étape essentielle consiste à identifier les parties prenantes concernées et à clarifier leurs mandats et leurs rôles. Il convient de constituer une équipe centrale, souvent composée de représentants de différentes agences et issus de divers horizons professionnels, avec un ou plusieurs rédacteurs chargés de la coordination et de la rédaction du texte. L'équipe doit être composée d'experts politiques et techniques ainsi que de juristes internationaux, dans la mesure où tous apportent des perspectives différentes mais essentielles sur les comportements **préférables, autorisés et possibles** dans le cyberespace.

Lors des phases de préparation et de planification, il convient d'aborder diverses **questions organisationnelles**, notamment qui fera quoi, pourquoi, où, quand et comment. Le renforcement des capacités est une composante essentielle du processus et peut s'avérer pertinent à toutes les étapes. De nombreuses initiatives et ressources sont disponibles pour aider les États à acquérir l'expertise nécessaire.

La **phase de collecte, de recherche et d'analyse des données** peut être abordée de différentes manières. On peut commencer par rédiger un document complet ou dresser une liste exhaustive des questions, puis affiner le tout afin de mieux définir la position nationale. On peut également partir d'un bref résumé annoté, puis l'étoffer progressivement au fur et à mesure que le processus avance. Les **consultations** jouent un rôle important dans ce processus et nécessitent une coordination et une gestion minutieuses afin de garantir que les contributions des parties prenantes soient efficacement intégrées.

82 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives africaines (rapport conservé par les auteurs).

La plupart des positions nationales adoptent une approche déductive, en partant des règles établies du droit international, puis en analysant la manière dont elles s'appliquent dans le contexte cybernétique. Cependant, une approche inductive, qui commence par des défis spécifiques (par exemple, les cyberattaques basées sur l'IA ou le ransomware), puis examine la manière dont le droit international s'applique, peut également être utile. Ces **approches peuvent être combinées**, certains États intégrant des scénarios et des exemples pour illustrer leur position.

En fonction de l'État, l'adoption d'une position nationale peut nécessiter de respecter certaines **exigences institutionnelles spécifiques**, telles que l'approbation du parlement ou d'un organe exécutif. L'élaboration d'une position nationale ne se limite pas nécessairement à un exercice ponctuel et peut faire l'objet d'une révision.

CHAPITRE 4 :

CONTENU

EN BREF

Ce chapitre passe en revue les principales questions juridiques abordées dans les positions nationales, notamment les règles et principes fondamentaux du droit international (tels que la souveraineté, la diligence due et la non-intervention), ainsi que les régimes juridiques spécialisés (tels que le droit international humanitaire, le droit international des droits de l'homme et le droit pénal international). Il souligne les points d'accord et les points de discussion clés afin d'aider les États à déterminer les thèmes à aborder et le niveau d'engagement à adopter.

1. Introduction

En matière de droit international et d'activités cybernétiques, les positions nationales existantes couvrent un large éventail de questions de fond. Au-delà des questions importantes liées au droit international, elles examinent les différents aspects de la menace cybernétique actuelle, tels que l'impact du ransomware, la désinformation et le cyberespionnage. Elles abordent également des défis politiques majeurs, tels que la nécessité de réduire la division numérique, de favoriser le développement international, de renforcer les capacités, de lutter contre la cybercriminalité ou d'élaborer de nouvelles règles pour le cyberespace. Le choix des thèmes abordés et les opinions exprimées à ce sujet reflètent la position d'un État sur des questions politiques, sociales et culturelles complexes découlant de l'utilisation généralisée des technologies de l'information et de la communication (TIC) à l'échelle nationale et internationale.

Aujourd'hui, tout le monde s'accorde à dire que le droit international s'applique à l'utilisation des TIC, et presque toutes les positions nationales adoptées à ce jour en témoignent explicitement ou implicitement. En affichant sa position, un État reconnaît implicitement que le droit international s'applique et régit les activités cybernétiques. Toutefois, ce constat ne signifie pas pour autant qu'il existe un consensus sur les règles spécifiques du droit international qui s'appliquent, sur la manière dont elles s'appliquent dans le contexte cybernétique et sur le fait qu'elles soient suffisantes ou non pour relever les défis dans ce contexte. Les positions nationales ont porté sur les domaines les plus controversés du droit international tels qu'ils s'appliquent aux activités cybernétiques, et de nombreux points de désaccord sont apparus. Outre les débats de fond abordés tout au long de ce chapitre, certains États ont fait valoir qu'un nouvel instrument juridiquement obligatoire était nécessaire pour combler les lacunes relevées dans l'application du droit international existant en matière d'activités cybernétiques.[1]

1 Cf. par exemple les positions nationales de la Chine (2021), p. 3, de Cuba (2024), paragraphe 4, du Pakistan (2023), paragraphe 8, et de la Russie (2021), p. 80.

Ce chapitre s'articule autour de trois axes principaux concernant les questions juridiques soulevées par l'application du droit international en matière d'activités cybernétiques. Il commence par examiner les règles et principes fondamentaux du droit international, notamment la souveraineté, la non-intervention, l'interdiction du recours à la force, la diligence due, le règlement pacifique des différends et l'autodétermination. Il aborde ensuite trois régimes juridiques spécialisés : le droit international humanitaire, le droit international des droits de l'homme et le droit pénal international, et examine comment leur règles s'appliquent dans le contexte cybernétique. Enfin, il analyse le droit de la responsabilité de l'État, en mettant l'accent sur l'attribution, les contre-mesures et l'état de nécessité.

Ces débats sont essentiels pour déterminer comment les cadres juridiques existants peuvent s'adapter aux défis uniques posés par les TIC. Les positions nationales se sont imposées comme le vecteur principal grâce auquel les États ont contribué à ces grands débats juridiques. Comme l'indique **l'introduction** du présent Manuel, les positions nationales peuvent être considérées comme des éléments probants de *l'opinio juris* et, de manière plus controversée, de la pratique des États dans le cadre de la formation du droit international coutumier. En conséquence, les États ont la possibilité de maintenir le statu quo ou de développer le droit international par le biais de leurs positions nationales.

Ce chapitre présente une vue d'ensemble des questions de droit international public les plus fréquemment abordées dans les positions nationales et communes publiées à ce jour (voir également la figure 8, pages 122 et 123), ainsi que dans les discussions multilatérales pertinentes, notamment dans le cadre des processus mandatés par les Nations Unies, tels que le Groupe d'experts gouvernementaux (GEG) et le Groupe de travail à composition non limitée (GTCNL) des Nations Unies. Le choix des thèmes retenus reflète également les points soulevés de manière récurrente par les participants aux tables rondes du projet. Outre la présentation des différents points de vue sur l'application de ces règles et principes du droit international dans le contexte cybernétique, ce chapitre examine également les considérations politiques qui les sous-tendent.

Pour permettre aux lecteurs d'approfondir ces sujets, ce chapitre comprend des codes QR – cliquables dans la version numérique – lesquels renvoient aux pages correspondantes du *Cyber Law Toolkit*. Ces pages fournissent des informations régulièrement mises à jour, des analyses juridiques approfondies et un aperçu comparatif des positions nationales sur chaque question.

2. Règles et principes fondamentaux

La présente section porte sur six règles et principes fondamentaux du droit international qui s'appliquent aux activités cybernétiques. Quatre de ces règles et principes, la souveraineté, l'interdiction d'intervention, l'interdiction du recours à la force et la diligence due, figurent dans plusieurs positions nationales et comptent parmi les sujets les plus fréquemment abordés dans ce domaine. Les deux autres, le règlement pacifique des différends et le droit à l'autodétermination, ont reçu moins d'attention, mais ils commencent à apparaître plus régulièrement dans les positions nationales et les discussions multilatérales. Si la plupart s'accordent à dire que ces six règles s'appliquent aux activités cybernétiques, les États les interprètent et les appliquent de manière différente. Dans l'ensemble, cette section décrit Les approches adoptées par les États dont les positions ont étés publiées à ce jour, en soulignant les points de convergence et les questions en suspens.

a. La souveraineté

La souveraineté est un principe fondamental du droit international. Selon une définition classique, énoncée dans la sentence arbitrale de 1928 relative *à l'île de Palmas*[2], la souveraineté signifie « à l'égard d'une partie du globe [...] le droit d'y exercer, à l'exclusion de tout autre État, les fonctions d'un État ». Il est généralement admis que la souveraineté s'applique dans le contexte cybernétique.[3] Cependant, le débat persiste quant à sa nature juridique précise : s'agit-il d'une règle autonome du droit international ou simplement d'un principe directeur ?

Il est largement admis que la souveraineté s'applique dans le contexte cybernétique, bien que le débat persiste quant à savoir s'il s'agit d'une règle individuelle du droit international ou simplement d'un principe directeur.

2 *Île de Palmas (États-Unis c. Pays-Bas)* (1928) II *RIAA* 829, 838.

3 Assemblée générale des Nations Unies, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135 (14 juillet 2021), paragraphes 70, 71(b).

La plupart des États qui se sont prononcés sur cette question considèrent la souveraineté comme une **règle fondamentale du droit international**, et dont la violation engage la responsabilité de l'État. Il convient de noter que cette règle peut déclencher le droit de l'État victime de prendre des contre-mesures à l'encontre de l'État responsable de la violation. Cette position a été adoptée par plusieurs États, notamment l'Autriche, le Brésil, le Canada, la Tchéquie, l'Estonie, la Finlande, la France, l'Allemagne, l'Iran, l'Italie, le Japon, les Pays-Bas, la Nouvelle-Zélande, la Norvège, la Roumanie et la Suède.[4] Elle a également été approuvée dans la position commune de l'Union africaine (UA) et dans la position commune de l'Union européenne (UE).[5]

Par ailleurs, certains considèrent que la souveraineté n'est qu'un **principe du droit international** qui régit les interactions entre États, sans pour autant constituer une règle primaire autonome. À ce jour, un seul État, le Royaume-Uni, a adopté cette position. Cette approche veut que les opérations cybernétiques ne puissent violer la souveraineté de l'État dans lequel ou contre lequel elles sont menées. Toutefois, ces opérations peuvent néanmoins constituer une intervention interdite, un recours à la force ou d'autres actes internationalement illicites.

Une **approche intermédiaire** consiste simplement à reconnaître que la souveraineté s'applique dans le contexte cybernétique, sans préciser si elle constitue une règle de droit international. Certains États ayant adopté cette position soulignent en outre la complexité de la question et indiquent qu'ils continuent à l'étudier. Cette approche permet aux États de conserver une certaine souplesse opérationnelle et de se réserver la possibilité d'adopter une position plus définitive à l'avenir. Parmi les États qui ont adopté cette position figurent l'Australie, Israël, le Kenya et les États-Unis.[6]

L'opinion dominante selon laquelle la souveraineté constitue une règle autonome implique que tous les États sont tenus de respecter la souveraineté des autres États. Cependant, il n'existe actuellement aucun consensus sur les critères exacts permettant de déterminer dans quels cas les opérations cybernétiques constituent une violation de la souveraineté, et les positions des États à ce sujet varient considérablement. Deux approches principales se sont dégagées à cet égard : l'approche fondée sur l'accès et l'approche fondée sur les effets.

4 Cf. les positions nationales de l'Autriche (2024), p. 4, du Brésil (2021), p. 18 ; du Canada (2022), paragraphes 10 et 14 et suivants, de la République tchèque (2024), paragraphes 1 et 3, de l'Estonie (2021), p. 24, de la Finlande (2020), pp. 1-2, de la France (2021), pp. 2-3, de l'Allemagne (2021), pp. 2-3, de l'Iran (2020), art. II.2, de l'Italie (2021), p. 4, du Japon (2021), p. 2, des Pays-Bas (2021), p. 7, de la Nouvelle-Zélande (2020), paragraphes 11-15, de la Norvège (2021), p. 3, de la Roumanie (2021), p. 76, et de la Suède (2022), p. 2.

5 Cf. les positions communes de l'UA (2024), paragraphe 12, et de l'UE (2024), p. 4.

6 Cf. les positions nationales de l'Australie (2021), p. 5 ; d'Israël (2021), p. 402 ; du Kenya (2021), p. 53, et des États-Unis (2021), p. 139.

- Dans le cadre de **l'approche fondée sur l'accès** (également appelée approche fondée sur la pénétration ou approche puriste) : toute pénétration non autorisée des systèmes TIC situés sur le territoire d'un État est considérée comme une violation de la souveraineté de cet État. Cela inclut des opérations telles que l'installation d'une « porte dérobée » dans un système TIC ou l'exfiltration de données à partir d'un tel système. Les États favorables à cette approche peuvent choisir de la soutenir pour ses qualités protectrices.[7] Cependant, les États qui s'y opposent soulignent son incompatibilité potentielle avec la conception et le fonctionnement de l'internet, en particulier le fait que toute communication en ligne implique, par définition, l'entrée dans le réseau du destinataire.[8]
- **L'approche fondée sur les effets** : elle suppose qu'une opération cybernétique ait produit un effet ou un préjudice quelconque sur l'État victime pour être qualifiée de violation de la souveraineté. Les effets ou préjudices interdits susceptibles d'être identifiés dans la littérature comprennent la violation de l'intégrité territoriale de l'État victime et le fait d'interférer avec les fonctions gouvernementales inhérentes de l'État victime ou de s'en emparer.[9]
  - Une opération peut **porter atteinte à l'intégrité territoriale d'un État** de plusieurs manières. La plus évidente consiste à causer des dommages matériels, des destructions, des blessures ou la mort. Les actes ayant de tels effets peuvent être considérés à la fois comme des violations du principe de non-intervention et comme des recours à la force (voir ci-dessous). Certains États ont intégré dans leur position nationale la notion de perte de fonctionnalité des systèmes installés dans un autre État, même si cette perte n'entraîne pas de dommages matériels.[10]
  - On entend par **fonctions intrinsèquement gouvernementales** les activités qui relèvent exclusivement de la compétence d'un État et qui ne peuvent être exercées par des acteurs non étatiques que sur délégation de l'État, telles que la défense nationale, le maintien de l'ordre, la fourniture de services sociaux, l'organisation d'élections ou encore la diplomatie. On parle d'ingérence dans ces activités lorsqu'elles sont perturbées,[11] par exemple lorsque les résultats d'une élection sont trafiqués par des moyens cybernétiques. On parle d'usurpation lorsqu'une opération cybernétique consiste à exercer une fonction qui relève de la compétence exclusive de l'État concerné, par exemple l'exercice de pouvoirs de police sur le territoire d'un autre État sans son consentement.

7 Harriet Moynihan, *The Application of International Law to State Cyberattacks : Sovereignty and Non-Intervention* (Chatham House 2019), § 61, qualifiant cette approche de « protection maximale ».

8 Cf. par exemple, la position nationale des États-Unis (2021), p. 140, qui déclare que « la conception même de l'Internet peut entraîner une certaine emprise sur d'autres juridictions souveraines ».

9 Michael N. Schmitt (éd.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) (*Manuel de Tallinn 2.0*), commentaire de la règle 4.

10 Cf. par exemple, les positions nationales de l'Autriche (2024), p. 4, du Canada (2022), paragraphes 16-17, du Costa Rica (2023), paragraphe 20, du Danemark (2023), p. 449, et de la Norvège (2021), pp. 3-4.

11 *Manuel de Tallinn 2.0*, commentaire de la règle 4.

La question du **cyberespionnage** reste en suspens. Bien que le droit international ne le réglemente pas en tant que tel, la licéité de l'espionnage peut être difficile à concilier avec les conceptions plus larges de la souveraineté exposées ci-dessus, en particulier l'approche fondée sur l'accès. Si toute collecte non autorisée de données à l'étranger constitue une violation de la souveraineté, de nombreuses opérations de cyberespionnage seraient alors concernées. Certains États, dont l'Autriche, le Costa Rica et la Pologne, ont exprimé dans leurs positions nationales des points de vue suggérant qu'ils considèrent au moins certains types de cyberespionnage comme une violation de la souveraineté. Selon la position du Brésil, les interceptions de télécommunications sont par définition illégales car elles violent la souveraineté de l'État.[12]

En revanche, certains États adoptent expressément le point de vue opposé dans leurs positions nationales. Par exemple, le Canada affirme que « certaines activités cybernétiques, telles que le cyberespionnage, ne constituent pas une violation de la souveraineté territoriale »,[13] tandis que la Nouvelle-Zélande indique qu'elle « ne considère pas que la souveraineté territoriale interdise toute intrusion non autorisée dans un système TIC étranger » et que « les activités de pur espionnage [...] ne seraient pas internationalement illicites ».[14] En fin de compte, la qualification du cyberespionnage reste incertaine et devrait continuer à influencer les positions des États sur la question de la souveraineté dans le cyberespace.

b. La non-intervention

Le principe de non-intervention (également appelé interdiction d'intervention) est un corollaire de la souveraineté des États et une règle bien établie du droit international coutumier. Il interdit aux États d'intervenir, directement ou indirectement, dans les affaires intérieures ou extérieures d'autres États par des moyens contraignants.[15] Il ne fait aucun doute que le principe de non-intervention s'applique dans le contexte cybernétique. Pour qu'un acte, y compris une opération cybernétique, soit considéré comme une intervention interdite, il doit remplir deux conditions essentielles.

Tout d'abord, il doit porter sur des **questions relevant des affaires intérieures ou extérieures d'un État**, c'est-à-dire son « ***domaine réservé*** » : en d'autres termes, les questions sur lesquelles chaque État est libre de décider, telles que le choix de ses systèmes politique, économique, social et culturel, ainsi que la définition de sa politique étrangère.[16]

12 Position nationale du Brésil (2021), p. 18.

13 Position nationale du Canada (2022), paragraphe 19.

14 Position nationale de la Nouvelle-Zélande (2020), paragraphe 14.

15 CIJ, *Activités militaires et paramilitaires au/contre le Nicaragua (Nicaragua c. États-Unis)* (Fond) [1986] CIJ Rep 14 *(Affaire du Nicaragua)*, paragraphe 205.

16 CIJ, *Affaire du Nicaragua, paragraphe 205. Cf. également CIJ, Affaire relative aux activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda)* (fond) [2005] CIJ Rep 168, paragraphes 162-164; *Manuel de Tallinn 2.0*, commentaire de la règle 66, paragraphes 6-8.

Pour certains, le contenu du « *domaine réservé* » est limité par la portée et la nature des obligations juridiques internationales d'un État.[17] Selon ce point de vue, plus un État a accepté de règles internationales, moins il dispose de liberté dans ses affaires intérieures ou extérieures et plus la portée de son « *domaine réservé* » est restreinte. Pour d'autres, la portée du « *domaine réservé* » d'un État est établie et correspond à une liste standard de fonctions intrinsèquement souveraines.[18]

Dans le cyberespace comme dans d'autres contextes, l'adoption de la première approche limiterait les domaines dans lesquels l'intervention est considérée comme illégale et réduirait donc la portée et l'importance du principe de non-intervention. Par exemple, si un État a convenu de certaines normes sanitaires internationales, toute intervention relative à ces normes par des moyens cybernétiques ou non cybernétiques ne serait pas considérée comme une intervention interdite. En revanche, une approche stricte du *domaine réservé* entraînerait un élargissement du champ d'application du principe de non-intervention. Si l'on reprend l'exemple ci-dessus, le fait qu'un État ait accepté certaines obligations internationales dans le domaine des soins de santé ne le priverait pas entièrement de sa liberté en la matière. Après tout, les États conservent leur pouvoir discrétionnaire et leur autorité ultime dans les domaines où ils exercent leur autorité gouvernementale.[19]

La plupart des positions nationales et communes adoptées jusqu'à présent ont suivi cette dernière approche et n'ont pas restreint les domaines relevant du *domaine réservé* d'un État.[20] Cette approche « protectrice » semble découler d'une volonté de limiter les opérations cybernétiques intrusives menées ou soutenues par d'autres États. Le point de vue opposé semble lié aux stratégies cyber « expansionnistes » visant à préserver la capacité d'un État à mener des activités cybernétiques à l'étranger.[21]

17 Cf., par exemple, *Manuel de Tallinn 2.0*, commentaire sur la règle 66, paragraphes 7 et 13; Katja S Ziegler, « Domaine réservé » (avril 2013), *Max Planck Encyclopedia of International Law*, section C; Marco Roscini, *International Law and the Principle of Non-Intervention* (OUP 2024) 162–164.

18 Cf. par exemple Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Chatham House 2019), paragraphe 107. Cf. également la discussion dans Tsvetelina van Benthem, Talita Dias et Duncan B Hollis, « Information Operations under International Law » (2022) 55 *Vanderbilt Journal of Transnational Law* 1217, 1260-1261.

19 Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Chatham House 2019), paragraphe 106.

20 Cf., par exemple, les positions nationales du Costa Rica (2023), paragraphes 23 à 25, de la République tchèque (2024), paragraphe 9(a), du Danemark (2023), p. 450, et de l'Irlande (2023), paragraphes 8 à 10, qui énumèrent tous des domaines non exhaustifs relevant du *domaine réservé* d'un État), ainsi que la position nationale du Canada (2022), paragraphe 22, qui définit la portée de la non-intervention autour des « fonctions intrinsèquement souveraines ».

21 Cf. par exemple la position nationale des États-Unis (2021), p. 140, qui soutient que la non-intervention « est généralement considérée comme une règle relativement restrictive du droit international coutumier ».

La contrainte est le deuxième élément constitutif d'une intervention interdite : l'acte en question doit être de **nature contraignante**. Selon la Cour internationale de justice (CIJ), « [l]'élément de contrainte [...] constitutif de l'intervention prohibée et formant son essence même ».[22] La contrainte peut être directe, exercée par les organes d'un État contre ceux d'un autre, ou indirecte, prenant la forme d'un soutien aux actes contraignants menés par des acteurs non étatiques ou d'actes visant la population de l'État victime (par opposition à son gouvernement).[23] On peut citer comme exemple d'intervention directe une action militaire sur le territoire d'un autre État. Parmi les exemples d'intervention indirecte, on peut citer le soutien apporté par un État à des actions subversives menées par des acteurs non étatiques ou à des opérations d'influence visant à modifier les comportements de la population de l'État victime, telles que certaines formes de propagande et de désinformation. L'intervention indirecte est particulièrement prononcée dans le contexte cybernétique, compte tenu de la prolifération des TIC parmi les acteurs non étatiques, y compris en tant qu'auteurs ou victimes d'opérations cybernétiques malveillantes.

La contrainte est un élément essentiel d'une intervention interdite : l'acte en question doit être de nature contraignante.

Cependant, il n'existe pas de définition généralement acceptée de la contrainte en droit international.[24] Deux approches principales permettent de la définir dans le contexte cybernétique, en se concentrant sur deux éléments distincts :

a. L'approche **fondée sur l'intention**, selon laquelle un acte est considéré comme une contrainte s'il vise à obliger l'État victime à modifier son comportement à l'égard d'une question relevant de son *domaine réservé*.[25]

b. L'approche **fondée sur les effets**, selon laquelle la contrainte se traduit par une privation effective de contrôle ; en d'autres termes, pour être considéré comme une contrainte, l'acte doit priver de facto l'État victime de sa capacité à contrôler ou à régir les questions relevant de son *domaine réservé*.[26]

22 CIJ, *Affaire Nicaragua*, paragraphe 205.

23 CIJ, *Affaire Nicaragua*, paragraphe 205; Assemblée générale des Nations Unies, *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*, A/RES/36/103 (9 décembre 1981), annexe, partie II, lettres f, g, j, l, m et n.

24 Mohamed Helal, « *On Coercion in International Law* » (2019) 52(1) NYU Journal of International Law and Politics 1, 3. Cf. également Marco Roscini, *International Law and the Principle of Non-Intervention* (OUP 2024), 147–158.

25 Cf. par exemple les positions nationales de *l'Autriche (2024)*, pp. 5-6, du *Canada (2022)*, paragraphe 22, de la *République tchèque (2024)*, paragraphes 9-11, de *l'Estonie (2021)*, p. 25, de *l'Allemagne (2021)*, p. 5, de l'Italie (2021), pp. 4-5, des *Pays-Bas (2019)*, p. 3, de la *Norvège (2021)*, p. 4, et de la *Suisse (2021)*, p. 3. C'est également l'avis approuvé par la majorité des experts du *Manuel de Tallinn 2.0*: cf. *Manuel de Tallinn 2.0*, commentaire de la règle 66, paragraphe 19.

26 Cf. par exemple les positions nationales de *l'Australie (2021)*, p. 3, de *la Nouvelle-Zélande (2020)*, paragraphes 9-10, et du *Royaume-Uni (2022)*.

Chaque approche conduit à des résultats différents et repose sur des considérations politiques différentes. Par exemple, dans une affaire impliquant une interférence dans un processus électoral, que la plupart des États s'accordent à considérer comme une intervention interdite,[27] *l'approche fondée sur l'intention* exigerait de démontrer que l'opération cybernétique en question visait à influencer le processus électoral d'un État. Il peut être difficile de prouver l'intention, en particulier dans le contexte cybernétique, lequel est caractérisé par le secret. Toutefois, cette exigence garantit que les politiques ou les actions des États qui ont des conséquences involontaires à l'étranger ne sont pas considérées comme des interventions interdites.

À l'inverse, *l'approche fondée sur les effets* exigerait de démontrer que l'opération cybernétique en question a produit des résultats concrets, lesquels ont réellement affecté la capacité d'un État à organiser des élections, par exemple en rendant inutilisables les machines à voter ou en dissuadant les électeurs de voter. Cette approche présente toutefois l'inconvénient de rendre difficile la démonstration d'un lien de causalité entre certains types d'opérations cybernétiques, telles que les opérations d'influence, et la privation effective de la capacité d'un État à contrôler ses affaires intérieures ou extérieures. Elle semble motivée par la nécessité de prévenir et de sanctionner les interventions préjudiciables, nonobstant la difficulté d'obtenir la preuve d'une intention contraignante.

Ces approches peuvent également varier. Par exemple, la position commune de l'UA approuve une version plus étendue de *l'approche fondée sur l'intention*, selon laquelle la contrainte est « une politique [...] visant à imposer des restrictions à la volonté d'un État étranger ».[28] Ainsi, selon l'UA, il n'est pas nécessaire de recourir à la contrainte pour qu'il y ait violation du principe de non-intervention; dès lors qu'il existe une politique visant à imposer des restrictions, les menaces ou les tentatives infructueuses visant à interférer peuvent constituer une intervention interdite.[29] Le Costa Rica adopte une vision encore plus étendue, en déclarant qu'« il suffit qu'un État ait l'intention de contraindre un another État, emploie des méthodes contraignantes ou finisse par produire des effets coercitifs dans un autre État » pour que le principe de non-intervention soit violé.[30] À cet égard, la contrainte peut être démontrée de différentes manières, à savoir par la présence d'une intention de contrainte, d'effets contraignants ou par l'utilisation de méthodes restrictives susceptibles de priver un État de sa capacité à contrôler ou à choisir la manière de gérer ses affaires intérieures ou extérieures, indépendamment de l'intention ou des effets causés.[31]

27 Cf. par exemple les positions nationales de l'Australie (2021), p. 3, du Brésil (2021), p. 19, du Canada (2022), paragraphe 24, de l'Allemagne (2021), p. 5, d'Israël (2021), p. 403, de la Nouvelle-Zélande (2020), paragraphe 10, de la Norvège (2021), p. 4, de Singapour (2021), p. 83, du Royaume-Uni (2018, 2021, paragraphe 9, et 2022) et des États-Unis (2016, pp. 13-14, 2020 et 2021, p. 140).

28 Position commune de l'UA (2024), paragraphe 31.

29 Position commune de l'UA (2024), paragraphe 32.

30 Position nationale du Costa Rica (2023), paragraphe 24.

31 Cf. Antonio Coco, Talita Dias et Tsvetelina van Benthem, « Illegal: The SolarWinds Hack under International Law » (2022) 33(4) European Journal of International Law 1275, 1280-1281.

Bien que l'interdiction d'intervention ne s'applique qu'entre États, un État peut enfreindre cette obligation en soutenant les actes contraignants d'acteurs non étatiques.[32] Les violations de l'interdiction engagent la responsabilité de l'État.

c. Recours à la force

L'interdiction du recours à la force est inscrite à l'article 2(4) de la Charte des Nations Unies, qui exige des États qu'ils « s'abstiennent, 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, ou à tout autre moyen contraire aux buts des Nations Unies ».[33] Cette règle, qui reflète le droit international coutumier,[34] est également considérée comme une norme impérative du droit international général (ou *jus cogens*).[35] Il ne fait aucun doute qu'elle s'applique dans le contexte cybernétique,[36] et, à ce titre, elle figure dans pratiquement toutes les positions nationales et communes publiées.

Comme le précise l'expression « dans leurs relations internationales », l'interdiction du recours à la force **s'applique généralement uniquement entre États**.[37] Cela signifie que les acteurs non étatiques – tels que les groupes de pirates informatiques, les gangs de ransomware ou les mouvements rebelles – sont exclus de son champ d'application, à moins que leur comportement ne soit imputable à un État.[38] Toutefois, les opérations cybernétiques menées par des acteurs non étatiques qui ne sont pas attribuables à des États mais qui constitueraient autrement un recours à la force ne sont pas

Il ne fait aucun doute qu'elle s'applique dans le contexte cybernétique et, à ce titre, elle figure dans pratiquement toutes les positions nationales et communes publiées.

32 Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Chatham House 2019), paragraphe 79.

33 Charte des Nations Unies (adoptée le 26 juin 1945, entrée en vigueur le 24 octobre 1945) 1 UNTS 16 (Charte des Nations Unies) Article 2(4).

34 CIJ, *Conséquences juridiques de la construction d'un mur dans le territoire palestinien occupé* (avis consultatif) [2004] CIJ Rep 136 (*avis consultatif sur le mur*), paragraphe 87; CIJ, *Affaire du Nicaragua, paragraphes* 187 à 190. Voir également les positions nationales du Brésil (2021), p. 19, d'Israël (2021), p. 398, de la Suède (2022), p. 8, et des États-Unis (2021), p. 137.

35 Cf. par exemple Christian Tams, « Article 2(4) » dans Bruno Simma et al (éd.), *The Charter of the United Nations: A Commentary*, Vol I (OUP 2024) 359–360, paragraphe 137. Cf. également les positions nationales de l'Autriche (2024), p. 6, du Brésil (2021), p. 19, de Cuba (2024), paragraphe 12, de la République tchèque (2024), paragraphe 24, et la position commune de l'UA (2024), paragraphe 38.

36 Cf., par exemple, Assemblée générale des Nations Unies, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,* A/76/135 (14 juillet 2021), paragraphe 71(d).

37 Cf. Christian Tams, « Article 2(4) » dans Bruno Simma et al (éd.), *The Charter of the United Nations: A Commentary,* Vol I (OUP 2024) 333–338, qui soutient que la portée de l'interdiction s'étend également aux « régimes de facto stabilisés » et aux organisations internationales.

38 Marco Roscini, Cyber Operations and the Use of Force in International Law (OUP 2014), 44.

exemptes de toute réglementation en droit international. Ces activités peuvent engager la responsabilité pénale individuelle des personnes concernées (voir la section sur le droit pénal international ci-dessous) ou impliquer les obligations de diligence due des États qui ne parviennent pas à prévenir, à mettre fin ou à corriger ces opérations (voir la section sur la diligence due ci-dessous).

Le terme **« force » n'est pas défini en droit international**, mais il est communément admis que la qualification d'une opération donnée comme recours à la force ne dépend pas des moyens utilisés. Comme l'a observé la CIJ dans son avis consultatif sur les « Armes nucléaires », l'interdiction s'applique « à tout recours à la force, quelles que soient les armes utilisées ».[39] Autrement dit, en principe, le recours aux capacités cybernétiques peut être considéré comme un recours à la force au même titre que le recours à des moyens cinétiques. L'interdiction s'étend également aux menaces de recours à la force, qui, dans le contexte cybernétique, peuvent inclure des opérations susceptibles d'entraîner le recours à la force ou des menaces verbales proférées en ligne.[40]

Plutôt que de se concentrer sur les moyens, l'approche prédominante visant à déterminer si une opération cybernétique constitue un recours à la force consiste à se référer à ses effets ou à ses conséquences (approche fondée sur les effets). Sur cette base, trois grandes catégories d'opérations cybernétiques ont émergé:

- De nombreux États considèrent qu'une opération cybernétique constitue un recours à la force si elle produit des **effets comparables à ceux d'un acte classique** (cinétique) couvert par l'interdiction. Cela est évident si l'opération cybernétique entraîne des destructions physiques ou des pertes en vies humaines. Parmi les exemples cités dans les positions publiées, on peut citer les dommages graves causés à une centrale électrique,[41] la collision de trains,[42] ou l'ouverture d'un barrage au-dessus d'une zone peupléee.[43]
- La question de savoir si les opérations cybernétiques qui entraînent la **perte de fonctionnalité** d'infrastructures cybernétiques sans causer de dommages matériels constituent un recours à la force est moins évidente. Comme l'indique la position nationale de l'Italie, une telle interprétation pourrait se justifier car la dépendance des sociétés modernes à l'égard des technologies cybernétiques permet désormais d'interrompre des services essentiels sans causer de dommages physiques.[44] lParmi les exemples cités par les États figurent la perturbation grave d'infrastructures critiques,[45] la mise hors service

39 CIJ, *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion)[1996] CIJ Rep 226 (avis consultatif sur les armes nucléaires), paragraphe 39.

40 Cf. Duncan B Hollis et Tsvetelina van Benthem, « *Threatening Force in Cyberspace* », dans Laura A Dickinson et Edward W Berg (éd.), Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold (OUP 2024).

41 Cf. les positions nationales de l'Autriche (2024), p. 7, et de la Pologne (2022), p. 5.

42 Cf. la position nationale d'Israël (2021), p. 399.

43 Cf. la position nationale des États-Unis (2012).

44 Cf. la position nationale de l'Italie (2021), p. 8.

45 Cf. la position nationale de l'Irlande (2023), paragraphe 18.

ou l'interruption du fonctionnement d'infrastructures électriques,[46] ou la désactivation de systèmes de défense antimissile.[47]

- Quant à la qualification des opérations cybernétiques causant un **préjudice purement économique**, la controverse est encore plus vive. Traditionnellement, l'interdiction du recours à la force était considérée comme limitée à la force armée, excluant d'autres formes de contrainte (telles que la pression économique), qui pouvaient tout au plus être qualifiées de violations du principe de non-intervention.[48] Cependant, en raison du potentiel des opérations cybernétiques à causer des dommages économiques importants et généralisés, plusieurs États ont désormais exprimé dans leurs positions nationales leur réticence à exclure la possibilité que de telles opérations cybernétiques puissent être qualifiées de recours à la force. Il s'agit là d'une des questions sur lesquelles il est nécessaire de recueillir l'avis d'un plus grand nombre d'États.[49]

Le caractère incertain de ces questions transparaît clairement dans l'affirmation récurrente des États selon laquelle l'évaluation visant à déterminer si une opération cybernétique constitue un recours à la force doit être effectuée au cas par cas.[50] Les États conservent ainsi une certaine souplesse dans ce domaine en rapide évolution. Afin de promouvoir la stabilité juridique, les États pourraient envisager de définir des critères pour procéder à ces évaluations. Le *Manuel de Tallinn 2.0* offre des orientations utiles à cet égard, en énumérant des facteurs tels que la gravité, le caractère invasif et la nature militaire de l'opération en question.[51] Certains États l'ont déjà fait dans leurs positions nationales.[52]

Le recours à la force est considéré comme illégal à moins qu'il ne soit consenti par l'État territorial,[53] autorisé par le Conseil de sécurité des Nations Unies,[54] ou exercé dans le cadre de la légitime défense.[55] **Si un recours à la force dans le cyberespace est qualifié d'attaque armée**,[56] **l'État victime peut invoquer son**

46 Cf. les positions nationales du Costa Rica (2023), paragraphe 10, et de la Norvège (2021), p. 6.

47 Cf. la position nationale de la Pologne (2022), p. 5, ainsi que la position commune de l'UA (2024), paragraphe 40.

48 Christian Tams, « Article 2(4) » dans Bruno Simma et al (éd.), *The Charter of the United Nations: A Commentary, Vol I* (OUP 2024) 315, paragraphe 47. Cf. également la position nationale de Cuba (2024), paragraphe 12.

49 Cf. par exemple les positions nationales du Danemark (2023), p. 451, de la France (2019), p. 7, des Pays-Bas (2019), p. 4, et de la Norvège (2021), p. 6.

50 Cf. par exemple les positions nationales du Canada (2022), paragraphe 45, du Costa Rica (2023), paragraphe 36, de la République tchèque (2024), paragraphe 27, du Danemark (2023), pages 451-452, de l'Allemagne (2021), page 6, de l'Italie (2021), page 8, des Pays-Bas (2019), page 4, de la Norvège (2021), p. 5, de la Pologne (2022), p. 5, de la Roumanie (2021), p. 77, de la Suède (2022), p. 4, et des États-Unis (2021), p. 137, ainsi que la position commune de l'UA (2024), paragraphe 41.

51 *Manuel de Tallinn 2.0*, commentaire de la règle 69, paragraphe 9.

52 Cf. par exemple les positions nationales de la République tchèque (2024), paragraphe 27, du Danemark (2023), p. 451, de la France (2021), p. 7, de l'Allemagne (2021), p. 6, de la Norvège (2021), p. 5, des Pays-Bas (2019), p. 4, de la Roumanie (2021), p. 77, de Singapour (2021), p. 84, et des États-Unis (2012 et 2021, p. 137), ainsi que la position commune de l'UA (2024), paragraphe 41.

53 Cf. par exemple les positions nationales de l'Australie (2021), p. 3, et de la Roumanie (2021), p. 77.

54 Cf. *Charte des Nations Unies*, articles 39 à 42.

55 Cf. *Charte des Nations Unies*, article 51.

56 Cf. CIJ, *Affaire Nicaragua*, paragraphes 191 et 195, qui déclare que seules les « formes les plus graves de recours à la force » peuvent être qualifiées d'attaques armées et qui identifie « l'ampleur et les effets » comme les critères permettant d'évaluer si un recours à la force peut être qualifié comme tel.

droit à la légitime défense, et les États tiers peuvent recourir à la force dans le cadre de la légitime défense collective à sa demande.[57] La CIJ a précisé que seules les « formes les plus graves de recours à la force » constituent des attaques armées et a identifié « l'ampleur et les effets » comme critères permettant d'évaluer si un acte constitue un recours à la force. Cette approche se retrouve dans de nombreuses positions nationales et communes,[58] à l'exception notable des États-Unis, qui affirment que tout recours à la force constitue une attaque armée.[59]

De même que pour le recours à la force cinétique, il n'existe pas de **seuil universellement accepté pour déterminer quels types de recours à la force dans le cyberespace constituent des attaques armées**. Les États s'accordent généralement à dire que ce seuil est atteint lorsque les opérations entraînent des pertes humaines importantes ou des dommages matériels considérables.[60] Parmi les exemples cités dans les positions nationales publiées, on peut citer le fait de provoquer le dysfonctionnement d'un réacteur nucléaire, causant ainsi des dommages graves et des pertes humaines,[61] ou de provoquer une panne grave et prolongée d'infrastructures nationales essentielles.[62] Dans le contexte cybernétique comme dans d'autres, la question de savoir si les agissements d'acteurs non étatiques peuvent constituer une attaque armée et donc justifier le droit de l'État victime à recourir à la force dans le cadre de la légitime défense sur le territoire de l'État d'où provient l'attaque fait l'objet d'un débat permanent.[63]

Tout recours à la légitime défense doit respecter les deux **exigences de nécessité et de proportionnalité**.[64] Premièrement, le recours à la force dans le cadre de la légitime défense doit être nécessaire pour repousser l'attaque armée. Par conséquent, si, par exemple, des mesures de cyberdéfense passives et non contraignantes suffisaient à cette fin, l'État se verrait interdire le recours à la force.[65] Deuxièmement, la proportionnalité exige que la riposte ne dépasse pas ce qui est nécessaire pour contrer l'attaque. Il est important de noter que l'État victime n'est pas tenu de riposter par des mesures similaires; il peut recourir à des moyens cybernétiques

57 Cf. *Charte des Nations Unies*, article 51, et CIJ, *affaire Nicaragua*, paragraphes 195 et 199.

58 Cf. par exemple les positions nationales de l'Autriche (2024), p. 7, du Brésil (2021), p. 20, du Costa Rica (2023) paragraphe 37, du Danemark (2023), pp. 451-452, de Cuba (2024) paragraphe 6, de la République tchèque (2024), paragraphe 29, de la France (2021), p. 5, de l'Allemagne (2021), p. 15, de l'Italie (2021), p. 9, des Pays-Bas (2019), p. 8, de la Norvège (2021), p. 5, de la Suède (2022), p. 4, de la Suisse (2021), p. 4, ainsi que les positions communes de l'UA (2024), paragraphe 41, et de l'UE (2024), p. 10.

59 Voir la position nationale des États-Unis (2012).

60 Cf. par exemple les positions nationales de l'Autriche (2024), p. 7, de la France (2021), p. 5, de l'Italie (2021), p. 8, de la Nouvelle-Zélande (2020), paragraphe 7, et du Royaume-Uni (2018).

61 Cf. les positions nationales de la Nouvelle-Zélande (2020), paragraphe 8, et du Royaume-Uni (2018).

62 Cf. les positions nationales de la France (2021), pp. 5-6, de la Norvège (2021), p. 6, et de Singapour (2021), p. 84.

63 Cf. par exemple les positions nationales de l'Autriche (2024), p. 7-8, du Danemark (2023), p. 452, de l'Allemagne (2021), p. 16, d'Israël (2021), p. 399, de l'Italie (2021), p. 9, des Pays-Bas (2019), p. 9, de la Pologne (2022), p. 6, et des États-Unis (2021), p. 137, qui affirment toutes que les attaques armées peuvent être perpétrées par des acteurs non étatiques, tandis que les positions nationales du Brésil (2021), p. 20, et de la France (2021), p. 6, soutiennent que seuls les États peuvent commettre des attaques armées.

64 Cf. CIJ, *Affaire Nicaragua*, par. 176; CIJ, *Avis consultatif sur les armes nucléaires*, par. 41; CIJ, *Affaire relative aux plateformes pétrolières (Iran c. États-Unis)* (Arrêt) [2003] *CIJ Rep 161*, par. 74.

65 Cf. par exemple la position nationale des États-Unis (2021), p. 142.

ou cinétiques, à condition que les exigences de nécessité et de proportionnalité soient respectées.[66] Cette flexibilité garantit que le droit à la légitime défense reste effectif même lorsque l'État auteur de l'attaque ne fait pas appel à des capacités cybernétiques.[67]

d. Diligence due

La « diligence due » désigne une norme de conduite que l'on retrouve dans différentes obligations internationales, telles que les obligations positives en matière de droits de l'homme évoquées ci-dessous. Elle désigne également deux obligations d'application générale en droit international.

La première repose sur le principe énoncé par la CIJ dans l'*affaire du Canal de Corfou*, qui reconnaît « **l'obligation pour tout État de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États** ».[68] Cette obligation générale de prévention se fonde sur le droit international coutumier et découle de la souveraineté des États[69] Elle peut être violée lorsqu'un État sait ou aurait dû savoir qu'un acte contraire aux droits d'un autre État est commis à partir de son territoire ou par son intermédiaire, et qu'il ne prend pas de mesures raisonnables pour y mettre fin ou l'empêcher, et que le préjudice se concrétise.[70]

La deuxième obligation générale de diligence due concerne **le principe** « **d'utilisation non dommageable** du territoire »[71] lequel découle du droit international coutumier et se reflète dans le projet d'articles de la Commission du droit international (CDI) sur la prévention des dommages transfrontaliers résultant d'activités dangereuses.[72] Il s'agit d'une obligation qui consiste à « prendre toutes les mesures appropriées pour prévenir tout dommage transfrontalier significatif ou, en tout état de cause,

66 Cf. par exemple les positions nationales de l'Autriche (2024), p. 7, du Canada (2022), paragraphe 47, de l'Estonie (2021), p. 30, de la Finlande (2020), p. 7, de la France (2021), p. 6-7, de l'Allemagne (2021), p. 15, d'Israël (2021), p. 399, des Pays-Bas (2019), p. 8, de la Nouvelle-Zélande (2020), paragraphe 24, de la Norvège (2021), p. 9, de la Pologne (2022), p. 5, de la Suède (2022), p. 4, du Royaume-Uni (2021), paragraphe 6, et des États-Unis (2021), p. 137.

67 Cf. la position nationale de la Pologne (2022), p. 5.

68 CIJ, *Affaire du canal de Corfou* (Royaume-Uni *c.* Albanie) (Fond) [1949] *CIJ Rec. 4*, 22.

69 Cf. CIJ, *Usines de pâte à papier sur le fleuve Uruguay* (Argentine *c.* Uruguay) (Arrêt) [2010] *CIJ Rep 14*, par. 101; *Island of Palmas* (États-Unis *c.* Pays-Bas) (1928) *II RIAA 829*, 839.

70 Cf. Conseil de l'Union européenne, *Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace* (2024), 5; Talita Dias et Antonio Coco, *Cyber Due Diligence in International Law* (ELAC 2021) 784–789. Pour les experts du *Manuel de Tallinn 2.0*, les critères cumulatifs suivants doivent être remplis: l'existence d'un acte contraire aux droits d'un État victime, cet acte doit être commis à partir ou par le biais de l'infrastructure sous le contrôle de l'État responsable, cet acte aurait été illégal s'il avait été commis par l'État lui-même, cet acte a des conséquences négatives graves; l'État en a connaissance effective ou constructive, et l'État ne prend pas les mesures réalisables pour mettre fin à cet acte. Voir le *Manuel de Tallinn 2.0*, commentaire de la règle 6.

71 Cf. *Affaire Trail Smelter* (États-Unis *c.* Canada) (1941) *3 RIAA 1911*, p. 1963; CIJ, *Usines de pâte à papier sur le fleuve Uruguay* (Argentine *c.* Uruguay) (Jugement) [2010] *CIJ Rec. 14*, paragraphes 101, 187, 197, 204, 223.

72 ILC, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities*, with commentaries, A/56/10 (2001).

pour en réduire au minimum le risque », lorsque ce dommage trouve son origine sur le territoire ou dans la juridiction d'un État et affecte de manière significative des personnes, des biens ou l'environnement dans un autre État.[73] Si la portée du projet d'articles de la CDI se limitait aux activités causant des dommages physiques,[74] le principe d'utilisation non dommageable du territoire n'a jamais été destiné à se limiter aux questions écologiques.[75] Certains considèrent que le principe d'utilisation non dommageable du territoire s'applique également aux dommages non physiques, tels que les dommages financiers ou les atteintes à la réputation d'un État.[76]

Dans le contexte du cyberespace, le GGE a reconnu que « les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des actes internationalement illicites à l'aide des TIC »[77] Cependant, **la controverse persiste quant à savoir si la diligence due constitue une obligation contraignante applicable aux opérations cybernétiques**.

Pour certains États, la diligence due n'est qu'une norme non contraignante dans le contexte cybernétique.[78] Ils ont souligné que la diligence due a été définie par le GEG comme une norme volontaire non contraignante régissant le comportement responsable des États et que les pratiques des États ne suffisent pas à étayer l'existence d'une telle obligation dans le contexte cybernétique. La réticence à accepter que la diligence due puisse s'appliquer dans le contexte cyber semble provenir de la crainte que les États ne soient pas en mesure de prévenir ou d'arrêter les opérations cyber malveillantes, eu égard à leur nature souvent secrète et rapide. Par exemple, il serait difficile d'empêcher l'exploitation de fonctionnalités dissimulées et préjudiciables dans un logiciel sans en avoir connaissance. On craint également que le fait d'accepter la diligence due comme une obligation contraignante n'entraîne de fréquentes violations de cette obligation, ce qui entraînerait des contre-mesures et augmenterait le risque d'escalade des conflits dans le cyberespace.

Cependant, un grand nombre d'États ont accepté de reconnaître dans leurs positions nationales que le principe du canal de Corfou est applicable et donc contraignant dans le cyberespace comme dans d'autres contextes.[79] Quelques autres États ont également approuvé l'applicabilité du principe d'utilisation non dommageable du territoire dans le contexte cyber.[80] Ce point de vue est motivé par la nécessité de

73 CIJ, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, avec commentaires*, A/56/10 (2001), articles 2 et 3.

74 CIJ, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, avec commentaires*, A/56/10 (2001), commentaire de l'article 1, paragraphes 16-17.

75 ONU, *Fourth report on international liability for injurious consequences arising out of acts not prohibited by international law*, par Robert Q. Quentin-Baxter, rapporteur spécial, A/CN.4/373 et Corr.1 & .2 (27 juin 1983), paragraphe 17.

76 Cf., par exemple, la position nationale de la République tchèque (2024), paragraphe 18; Talita Dias et Antonio Coco, *Cyber Due Diligence in International Law* (ELAC 2021) 790–794.

77 Assemblée générale des Nations Unies, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/70/174 (22 juillet 2015), paragraphe 13(c).

78 Cf. par exemple les positions nationales du Canada (2022), paragraphes 26-27, d'Israël (2021), p. 404, de la Nouvelle-Zélande (2020), paragraphe 16, et du Royaume-Uni (2021), paragraphe 12.

79 Cf. par exemple les positions nationales de l'Autriche (2024), p. 10, de la Colombie (2025), p. 9, de l'Estonie (2019 et 2021, p. 26), de la Finlande (2020), p. 4, de la France (2019), p. 10, de l'Allemagne (2021), p. 3, de l'JIItalie (2021), p. 6, du Japon (2021), p. 5, des Pays-Bas (2019), p. 4, de la Suisse (2021), p. 7, et de la Suède (2022), p. 4, ainsi que les positions communes de l'UA (2024), paragraphe 21, et de l'UE (2024), p. 5.

80 Cf. les positions nationales du Costa Rica (2023), paragraphe 29, de la République tchèque (2024), paragraphe 18, et de la Norvège (2021), p. 7.

combler le vide en matière de responsabilité qui pourrait résulter de la difficulté d'attribuer les opérations cybernétiques à des États et de l'utilisation croissante de proxys dans le contexte cybernétique. En effet, la diligence due tiendrait les États responsables de ne pas avoir empêché, arrêté ou corrigé les opérations cybernétiques préjudiciables menées par des acteurs non étatiques ou des États tiers à partir de leur territoire ou de leurs infrastructures TIC. Cela inclut les activités menées par les cybercriminels, telles que le ransomware et les attaques contre la chaîne d'approvisionnement informatique.

Les États qui ont approuvé la diligence due en tant **qu'obligation contraignante ont souligné son caractère comportemental plutôt que résultatif :** les États doivent prendre des mesures raisonnables pour prévenir, arrêter ou corriger les opérations cybernétiques malveillantes menées à partir de leur territoire ou de leurs infrastructures, ou par leur intermédiaire. Dans leurs positions nationales, ces États ont également souligné que cette obligation est soumise à la condition d'une connaissance réelle ou constructive ainsi qu'à la capacité de prendre des mesures réalisables en fonction des circonstances.[81] Par conséquent, la diligence due ne constituerait pas une charge insurmontable pour les États, en particulier les pays en développement, en exigeant, par exemple, de surveiller en permanence les activités cybernétiques ou de prévenir toutes les activités cybernétiques malveillantes se déroulant sur le territoire d'un État.

Il est généralement admis que le sujet de la diligence due doit être étudié plus en profondeur. Cela vaut particulièrement pour la signification concrète de la diligence due, c'est-à-dire les différentes mesures que les États peuvent être amenés à adopter pour prévenir, mettre fin ou corriger les activités cybernétiques malveillantes. On trouve des exemples de telles mesures dans plusieurs normes de comportement responsable des États énoncées par le GEG, telles que les normes « g » (sur la protection des infrastructures critiques), « h » (sur les réponses aux demandes d'assistance d'autres États) et « j » (sur la notification responsable des vulnérabilités des TIC).[82] Parmi les autres exemples de comportement vigilant, on peut citer la mise en place et l'application d'un cadre juridique pour la cybercriminalité et les autres cybermenaces, la création d'une équipe d'intervention en cas d'urgence informatique (CERT), la réalisation d'évaluations des risques cybernétiques et le développement de partenariats public-privé pour renforcer la cybersécurité.[83]

> **Il est convenu que la diligence due nécessite une étude plus approfondie, en particulier en ce qui concerne les mesures pratiques que les États doivent prendre pour prévenir, mettre fin ou corriger les activités cybernétiques malveillantes.**

81 Cf. par exemple les positions nationales de l'Autriche (2024), p. 10, de la République tchèque (2020 et 2024, paragraphe 15), de l'Estonie (2019 et 2021, p. 26), de l'Irlande (2023), paragraphe 13, et du Japon (2021), p. 5, ainsi que les positions communes de l'UA (2024), paragraphe 23, et de l'UE (2024), p. 5.

82 Cf. Assemblée générale des Nations Unies, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,* A/70/174 (22 juillet 2015), paragraphe 13.

83 Cf. Talita Dias et Antonio Coco, *Cyber Due Diligence in International Law* (ELAC 2021) 165–205.

e. Règlement pacifique des différends

Le règlement pacifique des différends figure parmi les principes fondamentaux du droit international, consacrés par la Charte des Nations Unies[84] et inscrits dans le droit international coutumier.[85] Il découle de l'interdiction du recours à la force et impose aux États de régler leurs différends internationaux par des moyens pacifiques.[86] Il est largement admis que cette obligation s'applique également au contexte cybernétique,[87] conformément à l'engagement réaffirmé à maintes reprises par les États de promouvoir un environnement des TIC « ouvert, sûr, stable, accessible et pacifique ».[88]

Cependant, les positions nationales présentent des divergences quant à la manière dont cette obligation est formulée. Certaines l'interprètent au sens large comme couvrant tout différend international,[89] une opinion soutenue par le libellé clair de l'article 2(3) de la Charte des Nations Unies, qui n'impose aucune condition supplémentaire.[90] D'autres limitent l'obligation aux différends « susceptibles de mettre en danger la paix et la sécurité internationales »[91] Ce critère, qui figure à l'article 33(1) de la Charte des Nations Unies, est également repris dans le *Manuel de Tallinn 2.0* pour limiter la portée de l'obligation dans son ensemble.[92]

Il appartient aux parties de choisir les moyens de règlement des différends,[93] le

84 Charte des Nations Unies, articles 2(3) et 33.

85 CIJ, Affaire Nicaragua, paragraphe 290.

86 Alain Pellet, « Peaceful Settlement of International Disputes » dans Rüdiger Wolfrum (éd.), Max Planck Encyclopedia of Public International Law (édition en ligne, OUP 2013), paragraphes 2-3.

87 Assemblée générale des Nations Unies, *Report of the* Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/70/174 (22 juillet 2015), paragraphe 28(b) et Assemblée générale des Nations Unies, *Report of the* Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135 (14 juillet 2021), paragraphe 71(a). Voir également les positions nationales de l'Autriche (2024), p. 11, du Canada (2022), paragraphe 41, de la Chine (2021), p. 3, de la Colombie (2025), p. 10, du Costa Rica (2023), paragraphe 17, de la Tchéquie (2024), paragraphe 21, de l'Estonie (2021), p. 29, de la France (2019), p. 2, du Japon (2021), p. 6, du Kenya (2021), p. 54, Singapour (2021), p. 85, Suisse (2021), p. 2, et Royaume-Uni (2021, paragraphe 7, et 2022).

88 Voir, par exemple, les positions nationales du Brésil (2021), p. 17, de la Colombie (2025), p. 4, de l'Estonie (2021), p. 23, de la Finland p (2020), p. 1, de l'Irlande (2023), paragraphe 2, de l'Italie (2021), p. 3, du Kenya (2021), p. 52, la Nouvelle-Zélande (2020), paragraphe 1, la Norvège (2020), p. 1, le Pakistan (2023), paragraphe 7, Singapour (2021), p. 83, la Suède (2022), p. 1, Suisse (2021), p. 1, et Royaume-Uni (2021), paragraphe 1, ainsi que la position commune de l'UA (2024), paragraphe 3. (Souligné par nos soins.)

89 Voir, par exemple, les positions nationales du Canada (2022), paragraphe 41, du Costa Rica (2023), paragraphe 17, de la République tchèque (2024), paragraphe 21, du Japon (2021), p. 6, et de Singapour (2021), p. 85, ainsi que les positions communes de l'UA (2024), paragraphe 35, et de l'UE (2024), p. 9.

90 Christian Tomuschat, « Article 2(3) » dans Bruno Simma et al (éd.), The Charter of the United Nations : A Commentary, Vol I (OUP 2024), 283, paragraphe 42.

91 Voir, par exemple, les positions nationales de l'Autriche (2024), p. 11, de l'Estonie (2021), p. 29, et de la Suisse (2021), p. 2.

92 *Manuel de Tallinn 2.0*, commentaire de la règle 65, paragraphe 2.

93 CIJ, Affaire de la compétence en matière de pêcherie (Espagne *c.* Canada) (Compétence de la Cour) [1998] *CIJ Rec.* 432, paragraphe 56.

recours à des organismes ou accords régionaux.[94] Cette liste n'est pas exhaustive et les États peuvent également recourir à d'autres moyens pacifiques appropriés ou combiner plusieurs d'entre eux.[95] Toutefois, comme l'affirme la Déclaration de Manille de 1982, ils doivent le faire de bonne foi et dans un esprit de coopération.[96] Conformément à la Charte des Nations Unies, le Conseil de sécurité des Nations Unies peut également demander aux parties de régler le différend par des moyens pacifiques si le différend est susceptible de compromettre le maintien de la paix et de la sécurité internationales. [97]

Dans le contexte cybernétique, les différends entre États peuvent revêtir des dimensions factuelles et juridiques :

- **Les différends factuels** relatifs au cyberespace portent souvent sur l'attribution technique, c'est-à-dire l'identification de la machine utilisée pour mener une opération cybernétique particulière et la recherche de la ou des personnes ou groupes impliqués. Ils peuvent également porter sur les effets de l'opération, le moment de son exécution ou même sur la question de savoir si elle a réellement eu lieu. À cet égard, les mécanismes d'enquête sont importants.[98] Il est tout à fait envisageable que des mécanismes d'attribution formels soient développés à l'avenir pour relever ces défis.[99]
- **Les différends juridiques** portent généralement sur la question de savoir si une activité cybernétique affectant négativement un État est juridiquement imputable à un autre État et si elle constitue une violation d'une règle applicable du droit international. Ces différends peuvent être soumis à un règlement judiciaire, notamment à la CIJ en tant qu'organe judiciaire principal des Nations Unies. Sous réserve que les conditions de compétence et de recevabilité soient remplies, la CIJ est compétente pour statuer sur tout différend relatif au droit international, y compris l'application du droit international aux activités cybernétiques.

94 Charte des Nations Unies, Article 33(1).

95 Alain Pellet, « Peaceful Settlement of International Disputes » dans Rüdiger Wolfrum (éd.), Max Planck Encyclopedia of Public International Law (édition en ligne, OUP 2013), paragraphe 31.

96 Assemblée générale des Nations Unies, Manila *Declaration on the Peaceful Settlement of International Disputes*, A/RES/37/10 (15 novembre 1982), section I, paragraphe 5.

97 Charte des Nations Unies, article 33(2).

98 Nicholas Tsagourias, « Cyber Disputes as International Legal Disputes », dans Nicholas Tsagourias, Russell Buchan et Daniel Franchini (éd.), Peaceful Settlement of Inter-State Cyber Disputes (Hart 2024), 20.

99 Cf., par exemple, Yuval Shany et Michael N. Schmitt, « An International Attribution Mechanism for Hostile Cyber Operations » (2020) 96 International Law Studies 196.

Les États pourraient souhaiter utiliser leurs positions nationales pour exprimer leur point de vue sur la manière dont les différends internationaux factuels et juridiques impliquant les TIC devraient être résolus. Pour ce faire, ils pourraient notamment exprimer leur opinion sur la création éventuelle de mécanismes d'attribution ou d'autres mécanismes d'enquête,[100] encourager d'autres États à accepter la compétence obligatoire de la CIJ ou s'abstenir de le faire,[101] et explorer comment les TIC peuvent être utilisées pour permettre de régler pacifiquement les différends cybernétiques et non cybernétiques.[102]

Au cours des discussions multilatérales sur l'utilisation des TIC par les États et la sécurité internationale, certains États ont exprimé leur inquiétude quant au fait que les particularités liées au cyberespace pourraient favoriser les mesures unilatérales plutôt que le règlement pacifique des différends.[103] D'une part, il est vrai que l'obligation de rechercher le règlement pacifique des différends ne compromet pas les autres droits des États en vertu du droit international, notamment le droit de prendre des contre-mesures licites et le droit de recourir à la force dans le cadre de la légitime défense en réponse à une attaque armée.[104] D'autre part, comme expliqué ci-dessus, le recours à ces mesures unilatérales n'est possible que dans des conditions strictes. Si ces critères ne sont pas remplis, les États doivent s'efforcer de bonne foi de régler les différends par des moyens pacifiques. En tout état de cause, ils doivent s'abstenir de toute mesure qui mettrait en danger la paix et la sécurité internationales.[105]

Dans le cyberespace, les différends entre États peuvent porter à la fois sur des faits (par exemple, l'attribution technique) et sur le droit (par exemple, l'attribution juridique ou la qualification d'opérations comme violations du droit international).

100 Cf. par exemple la position nationale de Cuba (2024), paragraphes 23-24.

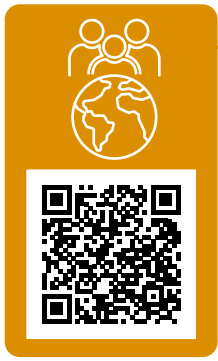
101 Cf. par exemple les positions nationales de la Suisse (2021), p. 2, et du Royaume-Uni (2022).

102 Cf. par exemple la position commune de l'UA (2024), paragraphe 37.

103 Assemblée générale des Nations Unies, Chair's Summary of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, A/AC.290/2021/CRP.3 (10 mars 2021), paragraphe 7.

104 Cf. par exemple, les positions nationales du Canada (2022), paragraphe 42, de la République tchèque (2024), paragraphe 23, de l'Estonie (2021), p. 29, et de Singapour (2021), p. 85.

105 Charte des Nations Unies, article 2(3). Cf. également *Manuel de Tallinn 2.0*, commentaire de la règle 65, paragraphe 12.



f. L'autodétermination

Le droit à l'autodétermination a été reconnu par l'Assemblée générale des Nations Unies comme l'un des « principes fondamentaux du droit international ».[106] Il est inscrit dans la Charte des Nations Unies,[107] le Pacte international relatif aux droits civils et politiques (PIDCP)[108] et le Pacte international relatif aux droits économiques, sociaux et culturels (PIDESC). [109]De plus, il est largement considéré comme une expression du droit international coutumier.[110] L'obligation correspondante de respecter ce droit est considérée comme une obligation envers la communauté internationale dans son ensemble,[111] et elle constitue potentiellement une norme impérative du droit international général (*jus cogens*).[112]

Si le droit à l'autodétermination relève des droits de l'homme fondamentaux,[113] il se distingue des autres droits abordés dans la section consacrée au droit international relatif aux droits de l'homme ci-dessous en ce qu'il s'agit d'un **droit collectif**. Le titulaire du droit n'est pas un individu, mais un groupe défini, communément appelé « un peuple ». Bien que le droit international ne définisse pas formellement le terme « un peuple », celui-ci est généralement compris comme désignant un groupe partageant un héritage historique, culturel ou linguistique commun et ayant un lien avec un territoire spécifique, qui s'identifie également comme tel.[114]

L'autodétermination peut être divisée en deux dimensions : interne et externe. **L'autodétermination interne** fait référence au droit pour un peuple de poursuivre librement son évolution politique, économique, sociale et culturelle dans le cadre d'un État existant.[115] **L'autodétermination externe** implique le droit pour un peuple de déterminer son statut international, par exemple en accédant à l'indépendance

106 Assemblée générale des Nations Unies, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, A/RES/2625 (XXV) (24 octobre 1970), annexe.

107 Charte des Nations Unies, article 1(2).

108 PIDCP, article 1.

109 PIDESC, Article 1.

110 CIJ, *Effets juridiques de la séparation de l'archipel des Chagos de Maurice en 1965* (Avis consultatif) [2019] CIJ Rep 95 (Avis consultatif sur les Chagos), paragraphe 155.

111 CIJ, *Affaire relative au Timor oriental* (Portugal c. Australie) (Jugement) [1995] Recueil CIJ 90, par. 29 ; CIJ, Avis consultatif sur le mur, par. 88.

112 Cf. par exemple, CDI, *Draft articles on Responsibility of States for Internationally Wrongful Acts*, avec commentaires (2001) (ARSIWA), commentaire de l'article 26, paragraphe 5 ; CIJ, Avis consultatif sur les îles Chagos, Separate Opinion of Judge Robinson, paragraphe 77 ; CIJ, *Conséquences juridiques découlant des politiques et pratiques d'Israël dans le territoire palestinien occupé*, y compris Jérusalem-Est (avis consultatif) (19 juillet 2024), paragraphe 233 (limitant cette conclusion aux situations d'occupation étrangère).

113 CIJ, Avis consultatif sur les îles Chagos, paragraphe 144.

114 Milena Sterio, *The Right to Self-Determination under International Law* (Routledge 2013), 16 ; Tom Sparks, *Self-Determination in the International Legal System* (Bloomsbury 2023), 24.

115 Assemblée générale des Nations Unies, *Déclaration sur l'octroi de l'indépendance aux pays et aux peuples coloniaux*, résolution 1514 (XV) (14 décembre 1960) 2 ; CIJ, *Conséquences juridiques découlant des politiques et pratiques d'Israël dans le territoire palestinien occupé*, y compris Jérusalem-Est (avis consultatif) (19 juillet 2024), paragraphe 241.

en tant qu'État souverain ou en choisissant de s'intégrer à un autre État.[116] Il est généralement admis que le droit à l'autodétermination externe ne s'applique que dans des circonstances exceptionnelles, par exemple lorsqu'un peuple est soumis à l'oppression ou à la domination coloniale.[117]

Au moment de la rédaction du présent document, seules trois positions nationales traitent du droit à l'autodétermination. La position de l'Italie fait référence au droit à l'autodétermination interne comme une « règle accessoire » au principe de souveraineté.[118] De même, celle de l'Iran stipule que la souveraineté doit être « interprétée à la lumière des autres principes juridiques fondamentaux », y compris l'autodétermination.[119] La position de la Russie reconnaît également l'applicabilité de « l'autodétermination des peuples » dans le contexte cybernétique, sans toutefois donner plus de détails.[120]

Les États pourraient souhaiter clarifier plusieurs aspects du droit à l'autodétermination dans le contexte cybernétique dans leurs positions nationales ou communes.

Premièrement, certains ont fait valoir que la **cyber-interférence dans les processus électoraux d'un autre État** pouvait être incompatible avec la dimension interne du droit à l'autodétermination.[121] Si une telle interférence peut simultanément constituer une violation des principes de souveraineté et/ou de non-intervention, les États pourraient souhaiter clarifier les lignes de démarcation entre ces concepts et la manière de les concilier en cas de conflit de normes. Par exemple, une intervention étrangère visant à soutenir l'autonomie démocratique dans un État doté d'un régime autoritaire peut être en contradiction avec le principe de souveraineté, mais conforme au principe d'autodétermination.[122]

Au moment de la rédaction de ce Manuel, rares sont les positions nationales qui traitent du droit à l'autodétermination. Cependant, plusieurs de ses dimensions peuvent être concernées par les opérations cybernétiques et pourraient être utilement abordées dans de futures positions.

116 Karen Knop, Diversity and Self-Determination in International Law (CUP 2009), p. 18.

117 Cf., par exemple, Reference re Secession of Quebec [1998] 2 RCS 217, par. 112.

118 Position nationale de l'Italie (2021), p. 4.

119 Position nationale de l'Iran (2020), paragraphe II.5.

120 Position nationale de la Russie (2021), p. 79.

121 Cf. par exemple Nicholas Tsagourias, « Electoral Cyber Interference, Self-Determination and the principe of non-intervention in cyberspace », dans Dennis Broeders et Bibi van den Berg (éd.), Governing Cyberspace : Behavior, Power, and Diplomacy (Rowman & Littlefield 2020) ; Marco Roscini, International Law and the Principle of Non-Intervention (OUP 2024) 399–400.

122 Jens D. Ohlin, « Did Russian Cyber-Interference in the 2016 Election Violate International Law ? » (2017) 95 Texas Law Review 1579, 1597.

Deuxièmement, il est généralement admis que le droit à l'autodétermination comprend le **droit d'exercer une souveraineté permanente sur les ressources naturelles**.[123] Comme l'a souligné le secrétaire général des Nations Unies, António Guterres, « les technologies numériques d'aujourd'hui sont similaires aux ressources naturelles telles que l'air et l'eau ».[124] En parallèle, les États ont reconnu dans le Pacte numérique mondial que certaines technologies, notamment les logiciels open-source et les données ouvertes, doivent être considérées comme des « biens publics numériques » ou des infrastructures publiques numériques.[125] Par conséquent, les États pourraient être amenés à déterminer quelles technologies numériques ou quels éléments de l'espace numérique, tels que l'accès aux réseaux de communication mondiaux ou l'attribution équitable des adresses IP, constituent des ressources soumises à la souveraineté permanente ou des biens publics numériques. Si l'on considère que ces technologies sont soumises à la souveraineté, le refus d'y donner accès pourrait, dans certaines circonstances, constituer une violation du droit à l'autodétermination.

Troisièmement, le droit à l'autodétermination **protège les peuples contre les actes visant à diviser la population et à compromettre son intégrité en tant que peuple**.[126] Dans le contexte cybernétique, il peut s'agir de campagnes de désinformation à grande échelle visant à contraindre la population à se déplacer et à modifier la composition démographique d'un territoire. Autre exemple possible : l'imposition de coupures Internet à un peuple par l'État qui le contrôle, privant ainsi les communautés de l'accès à des services vitaux et perturbant la cohésion sociale. Les États pourraient souhaiter préciser dans quelle mesure ces actes cybernétiques relèvent du droit à l'autodétermination.

123 CIJ, Affaire relative aux activités armées sur le territoire du Congo (République démocratique du Congo *c.* Ouganda) (Fond) [2005] *CIJ Rec.* 168, par. 244 ; CIJ, *Conséquences juridiques découlant des politiques et pratiques d'Israël dans le territoire palestinien occupé*, y compris Jérusalem-Est (Avis consultatif) (19 juillet 2024), paragraphe 240.

124 Assemblée générale des Nations Unies, Our Common Agenda Policy Brief 5 : A Global Digital Compact – An Open, Free and Secure Digital Future for All, A/77/CRP.1/Add.4 (25 avril 2023), paragraphe 31.

125 Assemblée générale des Nations Unies, Global Digital Compact, A/79/L.2 (2024), paragraphe 14.

126 CIJ, *Conséquences juridiques découlant des politiques et pratiques d'Israël dans le territoire palestinien occupé*, y compris Jérusalem-Est (avis consultatif) (19 juillet 2024), paragraphe 239.

3. Régimes spécialisés

La présente section examine comment trois régimes spécialisés du droit international – le droit international humanitaire (DIH), le droit international des droits de l'homme (DIDH) et le droit pénal international (DPI) – s'appliquent aux activités cybernétiques. Ces régimes ont été retenus car ils sont fréquemment mentionnés dans les positions nationales publiées à ce jour, bien que d'autres régimes spécialisés aient également été parfois inclus dans ces positions.[127] Chaque régime fournit un cadre juridique distinct régissant les activités cybernétiques qui relèvent de son champ d'application. Ces régimes ont en commun la volonté de protéger les individus contre tout préjudice, y compris ceux résultant de l'utilisation des technologies modernes telles que les cybercapacités.

a. Droit international humanitaire

Le DIH est un ensemble de règles visant à limiter les effets des conflits armés sur le plan humanitaire. Il fixe des limites quant au comportement des parties au conflit et, plus largement, des États, protégeant ainsi les victimes des conflits armés, notamment la population civile. Dans les années 2010, la question de **l'applicabilité du DIH aux opérations cybernétiques** a fait l'objet d'un débat entre les États.[128] Cependant, à la suite de l'adoption du rapport du GEG en 2021 et de son approbation ultérieure par l'Assemblée générale des Nations Unies et le Groupe de travail à composition non limitée, les États s'accordent désormais largement pour dire que tel est le cas et que le fait d'affirmer cette applicabilité ne légitime pas les conflits ni n'encourage la militarisation.[129] Toutes les positions nationales portant sur le DIH, y compris celles émises par des États auparavant sceptiques,[130] ont approuvé ce point

127 Cf. par exemple la position nationale de l'Autriche (2024), p. 14, qui comprend une section sur le droit diplomatique et consulaire.

128 Anders Henriksen, « The end of the road for the UN GGE process : The future regulation of cyberspace » (2019) 5(1) Journal of Cybersecurity 1 ; Eneken Tikk et Mika Kerttunen, The Alleged Demise of the UN GGE : An Autopsy and Eulogy, Cyber Policy Institute (2017).

129 Cf. Assemblée générale des Nations Unies, *Report of the* Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135 (14 juillet 2021), paragraphe 71(f) ; Assemblée générale des Nations Unies, *Report of the* open-ended working group on security of and in the use of information and communications technologies 2021-2025, A/79/214 (22 juillet 2024), paragraphe 36(b)(ii). Cf. également la 34e Conférence internationale de la Croix-Rouge et du Croissant-Rouge, Resolution 2 : Protecting Civilians and Other Protected Persons and Objects Against the Potential Human Cost of TIC Activities During Armed Conflict, 34IC/24/R2 (octobre 2024).

130 Cf. par exemple, Bureau de représentation de Cuba à l'étranger, « 71 UNGA : Cuba at the final session of the Group of Governmental Experts on the developments in the field of information and telecommunications in the context of international security » (23 juin 2017).

de vue comme point de départ.[131] En conséquence, les discussions internationales se sont orientées vers la manière dont le DIH s'applique dans le cyberespace.

Les États s'accordent désormais largement pour dire que le droit international humanitaire s'applique aux opérations cybernétiques menées pendant les conflits armés tout en affirmant que cette applicabilité ne légitime pas les conflits ni n'encourage la militarisation.

Si la plupart des règles du DIH s'appliquent en période de conflit armé, **certaines obligations doivent également être respectées ou mises en œuvre en temps de paix**. Il s'agit notamment du devoir de respecter et de faire respecter le DIH,[132] de l'obligation de faire connaître le DIH aussi largement que possible, notamment par l'instruction des forces armées,[133] de l'obligation de procéder à des examens juridiques des nouvelles armes, moyens et méthodes de guerre,[134] et du devoir de prévenir et de réprimer l'utilisation abusive des emblèmes protecteurs tels que la croix rouge, le croissant rouge et le cristal rouge.[135] Si la plupart des positions adoptées publiquement fournissent peu ou pas de détails sur ces obligations en temps de paix, le fait de souligner leur pertinence dans le contexte cybernétique offre aux États qui ne prévoient pas de s'engager dans un conflit armé l'occasion de mettre l'accent sur l'importance du DIH.

On peut distinguer deux types de **relations entre les opérations cybernétiques et les conflits armés**. D'une part, les opérations cybernétiques peuvent être menées dans le cadre d'un conflit armé existant. Pour autant qu'elles aient un lien avec le conflit, elles sont régies et donc limitées par le DIH. D'autre part, les opérations cybernétiques peuvent éventuellement donner lieu à un conflit armé là où il n'en existait pas auparavant. Dans ce cas, l'émergence du conflit armé déclenche l'application du DIH à tous les comportements qui y sont liés. Le DIH fait la distinction entre les conflits armés internationaux et non internationaux.

131 Cf. les positions nationales de l'Australie (2021), p. 3, de l'Autriche (2024), p. 16, du Brésil (2021), p. 22, du Canada (2022), paragraphe 48, du Costa Rica (2023), paragraphe 38, de Cuba (2024), paragraphe 16, de la République tchèque (2020 et 2024, paragraphe 37), du Danemark (2023), p. 454, de l'Estonie (2021), p. 26, de la Finlande (2020), p. 7, de la France (2019), p. 13, Allemagne (2021), p. 7, de l'Irlande (2023), paragraphe 29, d'Israël (2021), p. 399, de l'Italie (2021), p. 9, du Japon (2021), p. 6, du Kenya (2021), p. 54, des Pays-Bas (2019), p. 5, de la Nouvelle-Zélande (2019), paragraphe 25, de la Norvège (2021), p. 9, du Pakistan (2023), paragraphe 9, de la Pologne (2022), p. 7, de la Roumanie (2021), p. 77, de Singapour (2021), p. 85, de la Suède (2022), p. 6, Suisse (2021), p. 8, du Royaume-Uni (2018 et 2021, paragraphe 22) et des États-Unis (2012, 2016, p. 8, 2020 et 2021, p. 138), ainsi que les positions communes de l'UA (2024), paragraphe 47, et de l'UE (2024), p. 2.

132 Article 1 commun aux Conventions de Genève de 1949 ; Protocole additionnel I, article 1(1) ; Jean-Marie Henckaerts et Louise Doswald-Beck (éd.), Customary International Humanitarian Law : Volume I, Rules (CICR et CUP 2005) (Étude du CICR sur le DIH coutumier) Règles 139 et 144 ; 26e Conférence internationale de la Croix-Rouge et du Croissant-Rouge, Resolution 1 : International Humanitarian Law – From Law to Action, 26IC/95/R1 (3 décembre 1995), paragraphe 2.

133 Conventions de Genève I/II/III/IV, articles 47/48/127/144 ; Protocole additionnel I, article 83 ; Protocole additionnel II, article 19.

134 Protocole additionnel I, article 36.

135 Cf. Convention de Genève I, articles 53-54.

- On considère qu'un **conflit armé international** survient lorsque deux États ou plus recourent à la force armée.[136] Ce critère n'implique généralement pas un niveau d'intensité particulier.[137] Il existe donc un large consensus sur le fait que les opérations cybernétiques ayant des effets comparables à ceux des opérations cinétiques peuvent donner lieu à un conflit armé international.[138]

- Un **conflit armé non international** se caractérise par des combats entre un État et un groupe armé non étatique organisé ou entre plusieurs groupes de ce type. L'identification d'un conflit armé non international peut s'avérer plus complexe, car elle nécessite de franchir un seuil d'intensité plus élevé.[139] La question de savoir si les opérations cybernétiques, en particulier celles qui n'ont pas d'effets cinétiques, peuvent franchir ce seuil reste posée.[140] Néanmoins, quelques positions nationales ainsi que la position commune de l'UA affirment que les opérations cybernétiques pourraient déclencher un conflit armé non international.[141] Cette question reste ouverte et nécessite que davantage d'États se prononcent.

D'autres questions importantes qui requièrent l'attention des États concernent la portée de **l'interdiction des attaques contre les civils et les biens civils**. Cette interdiction, codifiée dans le Protocole additionnel I aux Conventions de Genève et inscrite dans le droit international coutumier,[142] s'applique, comme le reste du droit international humanitaire, aux opérations cybernétiques menées pendant un conflit armé. Cependant, l'interprétation des termes « attaques » et « biens » dans le contexte cybernétique reste sujette à débat.

136 TPIY, *Prosecutor v. Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-A (2 October 1995) para 70.

137 CICR, How is the term « armed conflict » defined in international humanitarian law?, Document d'opinion (2024) 9.

138 CICR (éd.), Commentary on the Third Geneva Convention (CUP 2021), commentaire de l'article 2, paragraphe 288.

139 Cf., par exemple, TPIY, *Prosecutor v. Limaj* (jugement) ICTY-03-66-T (30 novembre 2005), paragraphe 84 ; TPIY, *Prosecutor v.* Boškoski and Tarčulovski (jugement) ICTY-04-82-T (10 juillet 2008), paragraphe 175.

140 CICR (éd.), Commentary on the Third Geneva Convention (CUP 2021), commentaire sur l'article 3 commun, paragraphe 471 ; Permanent Mission of Lichtenstein to the United Nations, The Council of Advisers' Report on the Application of the Rome Statute to Cyberwarfare (août 2021), 33-36.

141 Cf. notamment les positions nationales de l'Autriche (2024), p. 17, du Costa Rica (2023), paragraphe 43, de la France (2019), p. 12, de l'Allemagne (2021), p. 7, et de l'Irlande (2023), paragraphe 30, ainsi que la position commune de l'UA (2024), paragraphe 49.

142 Protocole additionnel I, article 52(1) ; étude du CICR sur le DIH coutumier, règles 1 et 7.

- Tout d'abord, il convient de déterminer à **quel moment les opérations cybernétiques peuvent être qualifiées d'« attaques »** au sens du DIH, lequel constitue un point de référence essentiel pour de nombreuses règles régissant la conduite des hostilités. Outre l'interdiction des attaques contre les civils et les biens civils, celles-ci comprennent l'interdiction des attaques indiscriminées,[143] l'interdiction des attaques disproportionnées[144] et l'obligation de prendre toutes les précautions possibles pour éviter ou au moins réduire les dommages collatéraux causés aux civils et aux biens civils lors d'une attaque.[145] L'article 49 du Protocole additionnel I définit les attaques comme « des actes de violence contre l'adversaire, qu'ils soient offensifs ou défensifs ». En supposant qu'une attaque puisse être définie par ses effets,[146] les opérations cybernétiques provoquant des effets violents tels que la mort, des blessures ou des dommages constitueraient des attaques.[147] Cependant, le débat persiste quant à savoir si les opérations cybernétiques provoquant une perte de fonctionnalité, sans dommage physique aux systèmes cibles, peuvent également être qualifiées d'attaques. Un nombre croissant d'États souscrivent à une interprétation qui inclut la perte de fonctionnalité,[148] tandis que d'autres limitent la qualification d'attaques aux opérations susceptibles de causer des dommages physiques.[149] Néanmoins, il semble y avoir un consensus sur le fait qu'une opération cybernétique peut constituer une attaque lorsque la perte de fonctionnalité est susceptible de causer des dommages physiques, des blessures ou la mort.[150] Ce serait le cas pour une opération cybernétique visant à couper l'électricité d'un aérodrome militaire et susceptible, par conséquent, de provoquer le crash d'un avion militaire.[151] Compte tenu de l'impact potentiellement grave des opérations cybernétiques sur les services de première nécessité, même en l'absence de dommages physiques, il est essentiel de clarifier la frontière entre les attaques et les autres opérations cybernétiques.

- Deuxièmement, la question de la protection des données civiles – telles que les bases de données relatives à la sécurité sociale, à la fiscalité ou aux élections – en tant qu'« objets » civils fait également l'objet d'un débat. En vertu du DIH, tous les objets sont protégés contre les attaques, y compris par des moyens cybernétiques, à moins qu'ils ne soient considérés comme des objectifs militaires, tels que définis à l'article 52(2) du Protocole

143 Protocole additionnel I, article 51(4) ; Étude du CICR sur le DIH coutumier, règles 11 et 12.

144 Protocole additionnel I, articles 51(5)(b) et 57 ; Étude du CICR sur le DIH coutumier, règle 14.

145 Protocole additionnel I, article 57 ; Étude du CICR sur le DIH coutumier, règle 15.

146 Cordula Droege, « Get Off My Cloud : Cyber Warfare, International Humanitarian Law, and the Protection of Civilians » (2012) 94(886) Revue internationale de la Croix-Rouge 533, 557.

147 Voir le *Manuel de Tallinn 2.0*, règle 92.

148 Cf., par exemple, les positions nationales de l'Autriche (2024), p. 17, de la Colombie (2025), p. 13, du Costa Rica (2023), paragraphe 20, de la France (2019), p. 13, de l'Allemagne (2021), p. 8, du Japon (2021), p. 7, et la Nouvelle-Zélande (2020), paragraphe 20.

149 Cf., par exemple, les positions nationales du Danemark (2023), p. 455, et d'Israël (2021), pp. 400-401.

150 *Manuel de Tallinn 2.0*, commentaire de la règle 92, paragraphe 15.

151 Position nationale d'Israël (2021), pp. 400-401.

additionnel I.[152] On peut donc se demander si les **données civiles peuvent être considérées comme des objets civils** et bénéficier ainsi des protections prévues par le DIH. Certains États estiment que les données, prétendument immatérielles, invisibles et intangibles, ne peuvent être considérées comme des biens au sens du DIH.[153] Toutefois, cette interprétation a été critiquée car elle exclut les opérations cybernétiques visant les données civiles du champ d'application des règles relatives à la conduite des hostilités qui concernent uniquement les biens civils, créant ainsi un vide juridique important en matière de protection.[154] Une autre perspective préconise une interprétation plus large du terme « bien », en l'alignant sur l'objectif humanitaire général du DIH.[155] En effet, les opérations cybernétiques qui interfèrent avec les données civiles peuvent perturber les services publics, nuire aux entreprises privées et affecter les individus, soulignant ainsi la nécessité d'étendre les protections du DIH à ces données.[156] En conséquence, un nombre croissant d'États considèrent que la protection des biens civils s'étend aux données civiles.[157]

Même si certaines **opérations cybernétiques ne relèvent pas du champ d'application de l'interdiction des attaques contre les civils** et les biens civils, elles ne sont pas pour autant exemptes de toute réglementation au regard du DIH. Les règles applicables comprennent l'obligation de faire preuve d'une prudence constante afin d'épargner la population civile et les biens civils pendant les opérations militaires.[158] D'autres restrictions interdisent les opérations dirigées contre des biens spécifiquement protégés, tels que les infrastructures médicales[159] et les biens utilisés pour les opérations de secours humanitaire,[160] ainsi que les opérations visant à détruire des biens indispensables à la survie de la population civile, tels que les systèmes d'approvisionnement en eau ou les infrastructures agricoles.[161]

152 Cf. Protocole additionnel I, article 52(2) : « En ce qui concerne les biens, les objectifs militaires se limitent aux biens qui, par leur nature, leur emplacement, leur destination ou leur utilisation, contribuent effectivement à l'action militaire et dont la destruction totale ou partielle, la capture ou la neutralisation, dans les circonstances du moment, offre un avantage militaire certain. »

153 Cf., par exemple, les positions nationales du Danemark (2023), p. 455, et d'Israël (2021), p. 401. Cf. également le *Manuel de Tallinn 2.0*, commentaire de la règle 100, paragraphe 5.

154 Kubo Mačák et Laurent Gisel, « The Legal Constraints of Cyber Operations in Armed Conflicts », dans Rajeswari Pillai Rajagopalan (ed), Future Warfare and Technology : Issues and Strategies (Wiley 2022) 148.

155 Cf., par exemple, Robert McLaughlin, « Data as a Military Objective », Institut australien des affaires internationales (20 septembre 2018).

156 Cf. Kubo Mačák, « Military Objectives 2.0 : The Case for Interpreting Computer Data as Objects under International Humanitarian Law » (2015) 48 Israel Law Review 55.

157 Cf., par exemple, les positions nationales de l'Autriche (2024), p. 18, de la Colombie (2025), p. 18, du Costa Rica (2023), paragraphe 50, de la Finlande (2020), p. 7, de l'Allemagne (2021), p. 8, et de la Roumanie (2021), p. 78.

158 L'application de cette règle aux cyberopérations a été confirmée par la position nationale de plusieurs États, notamment l'Autriche (2024), p. 18, la République tchèque (2024), paragraphe 42, le Costa Rica (2023), paragraphe 52, le Danemark (2023), p. 455, la Finlande (2020), p. 7, la France (2019), p. 15, et l'Allemagne (2021), p. 9.

159 Cf. Convention de Genève I, article 19 ; Convention de Genève IV, article 18 ; Protocole additionnel I, article 12 ; Protocole additionnel II, article 11(1) ; Étude du CICR sur le droit international humanitaire coutumier, règle 28.

160 Convention de Genève IV, article 59(3) ; Protocole additionnel I, article 70(4) ; Étude du CICR sur le droit international humanitaire coutumier, règle 32.

161 Protocole additionnel I, article 54 ; Protocole additionnel II, article 14 ; Étude du CICR sur le DIH coutumier, règle 54. Voir également Conseil de sécurité des Nations Unies, Résolution 2573 (2021) S/RES/2573 (27 avril 2021).

Ainsi, le DIH continue d'imposer des contraintes importantes sur la manière dont une opération cybernétique peut être menée, même lorsqu'elle ne constitue pas une attaque ou lorsque les données qu'elle vise ne sont pas considérées comme des biens civils. La clarification de ces contraintes offre aux États qui élaborent leurs positions nationales ou communes l'occasion de renforcer encore la protection des civils contre les dommages causés par les opérations cybernétiques pendant les conflits armés.

b. Droit international des droits de l'homme

Aujourd'hui, il est communément admis que les droits de l'homme s'appliquent aussi bien en ligne que hors ligne.[162] Cela signifie que les États doivent respecter, protéger et garantir les droits de l'homme dans le cyberespace, conformément à leurs obligations en vertu des traités relatifs aux droits de l'homme et du droit international coutumier.[163] Les traités relatifs aux droits de l'homme comprennent le PIDCP et le PIDESC, ainsi que des traités régionaux tels que la Convention européenne des droits de l'homme (CEDH), la Convention américaine des droits de l'homme (CADH) et la Charte africaine des droits de l'homme et des peuples (CADHP).[164] Tous ces traités prévoient la création d'organes judiciaires ou quasi judiciaires chargés de surveiller le respect des droits de l'homme, à savoir le Comité des droits de l'homme (pour le PIDCP) ; le Comité des droits économiques, sociaux et culturels (pour le PIDESC) ; la Cour européenne des droits de l'homme (pour la CEDH) ; la Cour interaméricaine des droits de l'homme (pour la CADH) ; et la Cour africaine des droits de l'homme et des peuples (pour la CADHP).

Les traités internationaux et le droit international coutumier reconnaissent[165] un large éventail de **droits de l'homme particulièrement pertinents à l'ère numérique**, notamment les libertés d'opion et d'expression, le droit de réunion, le droit à la vie privée et le droit à la non-discrimination. Compte tenu de la numérisation croissante des services publics, les droits à la vie, à la santé et à l'éducation, ainsi qu'à des conditions de travail justes et favorables, peuvent également être affectés par des comportements malveillants dans le cyberespace. Par exemple, pendant la pandémie

162 Cf., par exemple, UNHRC, Promotion, protection et jouissance des droits de l'homme sur Internet, A/HRC/RES/32/13 (1er juillet 2016), paragraphe 1 ; Assemblée générale des Nations Unies, *Report of the* Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/70/174 (22 juillet 2015), paragraphe 28(b).

163 HRC, *Observation générale* n° 31 [80] : The nature of the general legal obligation imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13 (26 mai 2004) (*Observation générale* n° 31), paragraphes 6 à 8.

164 Pacte international relatif aux droits civils et politiques (16 décembre 1966) 999 UNTS 171 ; Convention internationale sur l'élimination de toutes les formes de discrimination raciale (21 décembre 1965) 660 UNTS 195 ; Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telle que modifiée par les protocoles n° 11 et 14, *ETS 5*, (4 novembre 1950) ; Convention américaine relative aux droits de l'homme, Treaty Series, n° 36 (1969) ; Charte africaine des droits de l'homme et des peuples, CAB/LEG/67/3 rev. 5, 21 *ILM* 58 (1982) (27 juin 1981).

165 Par exemple, les droits de l'homme définis dans la Déclaration Universelle des Droits de l'Homme (résolution 217 A (III) de l'Assemblée générale des Nations Unies du 10 décembre 1948) sont considérés comme faisant partie du droit international coutumier. Cf. ONU, Proclamation de Téhéran, Acte final de la Conférence internationale sur les droits de l'homme, Téhéran, 22 avril-13 mai 1968, A/CONF.32/41, 3. Cf. également, de manière générale, William A. Schabas, The Customary International Law of Human Rights (OUP 2021).

de COVID-19, des cyberattaques et des opérations d'influence ont ciblé le secteur des soins de santé, compromettant les efforts visant à protéger la vie et la santé des patients.[166] De même, la diffusion en ligne de discours haineux peut non seulement constituer une discrimination illégale à l'égard des individus, mais aussi alimenter la violence, en particulier dans les contextes fragiles.[167] La modération en ligne de ces contenus a été effectuée par des personnes travaillant dans des conditions difficiles.[168]

Cependant, les obligations inscrites dans la plupart des traités relatifs aux droits de l'homme ne s'appliquent qu'au sein de la **compétence d'un État,** c'est-à-dire dans le champ d'application de chaque traité.[169] Il ne fait aucun doute que les États ont compétence en matière de droits de l'homme sur leur territoire : la compétence est avant tout territoriale. Mais la mesure dans laquelle cette compétence s'étend au-delà des frontières nationales est controversée. Cette question est cruciale dans le contexte cybernétique, car un nombre important d'opérations cybernétiques sont menées à partir d'infrastructures TIC situées dans différents États et peuvent affecter à distance les droits de l'homme des individus dans les États d'origine, de transit et de cibles. Par exemple, la surveillance électronique peut être effectuée à l'aide de câbles et de serveurs situés sur plusieurs territoires et peut porter atteinte à la vie privée d'individus au-delà des frontières internationales. Bien que certains États contestent l'application extraterritoriale des droits de l'homme,[170] l'opinion dominante veut que ces obligations puissent, au moins dans certaines circonstances, s'étendre aux actions d'un État en dehors de ses frontières.[171] Différents modèles ou approches de la compétence extraterritoriale en matière de droits de l'homme ont été approuvés par différents États et organes de défense des droits de l'homme,[172] notamment :

a. Le **modèle spatial**, selon lequel les obligations en matière de droits de l'homme s'appliquent dans les zones placées sous le contrôle effectif d'un État.[173]

b. b. Le **modèle personnel,** selon lequel les obligations en matière de droits de l'homme naissent dès lors qu'un État exerce un contrôle ou une autorité effective sur des personnes.[174]

166 Cf., par exemple, US Cybersecurity & Infrastructure Security Agency, « COVID-19 Exploited by Malicious Cyber Actors » (8 avril 2020) ; Marko Milanovic et Michael Schmitt, « Cyber attacks and cyber (mis) information operations during a pandemic » (2020) 11(1) Journal of National Security Law and Policy 247.

167 Talita Dias, « Finding Common Ground : The Right to be Free from Incitement to Discrimination, Hostility, and Violence in the Digital Age » (2024) 16(4) Global Responsibility to Protect 391, 392.

168 Andrew Arsht et Daniel Etcovitch, « The Human Cost of Online Content Moderation », Jolt Digest (2 mars 2018).

169 169 Cf., par exemple, l'article 2, paragraphe 1, du PIDCP, qui utilise la formulation « toutes les personnes se trouvant sur le territoire [d'un État] et relevant de sa compétence ».

170 Cf., par exemple, les opinions exprimées par les États-Unis dans leur position nationale (2021) et dans le Comité des droits de l'homme des Nations Unies, Examen des rapports présentés par les États parties en vertu de l'article 40 du Pacte, Troisièmes rapports périodiques des États parties dus en 2003 : États-Unis d'Amérique, CCPR/C/USA/3 (2005), 109-110.

171 Cf., par exemple, CIJ, Conséquences juridiques résultant des politiques et pratiques d'Israël dans le territoire palestinien occupé, y compris Jérusalem-Est (avis consultatif) (19 juillet 2024), paragraphe 99.

172 Pour un aperçu général, voir Marko Milanovic, Extraterritorial Application of Human Rights Treaties : Law, Principles, and Policy (OUP 2011) ; Priya Urs, Talita Dias, Antonio Coco et Dapo Akande, The International Law Protections against Cyber Operations Targeting the Healthcare Sector (ELAC 2023), 170–173.

173 CEDH, *Banković and others* v. Belgium and others (App n° 52207/99) (12 décembre 2001), paragraphe 80.

174 CEDH, *Al-Skeini and others* v. United Kingdom (App n° 55721/07) (7 juillet 2011), paragraphes 136-137.

c. Le **modèle fonctionnel**, selon lequel la compétence est définie par le contrôle effectif de la jouissance des droits de l'homme, même si ce contrôle est exercé à distance, comme dans le cas de la surveillance étrangère.[175]

Le modèle spatial est le plus restrictif. Il part du principe que les États ne sont pas en mesure de respecter, protéger ou garantir les droits de l'homme sans un contrôle territorial effectif. Dans le contexte cybernétique, l'adoption de cette approche signifierait qu'un État n'aurait pas compétence sur des actes commis sur son territoire mais affectant à distance les droits d'individus dans d'autres États, tels que la surveillance électronique ou des interventions dans le processus électoral d'autres pays. Le modèle personnel va plus loin en élargissant le concept de la compétence aux situations dans lesquelles un État exerce un contrôle physique sur des personnes. Il a été initialement conçu pour couvrir les situations de détention pendant un conflit armé, dans lesquelles l'État responsable n'exerce pas de contrôle territorial mais a la capacité de violer physiquement les droits de l'homme. Cependant, ce modèle exclurait toujours la plupart des activités en ligne ayant une incidence indirecte sur les droits de l'homme dans d'autres États en l'absence de proximité physique entre le ou les auteurs et la ou les victimes. Le modèle fonctionnel est le plus large, car il met l'accent sur la jouissance des droits de l'homme, qu'ils soient physiques ou non physiques. Il couvre donc un large éventail d'activités en ligne, indépendamment de la proximité physique entre le ou les auteurs et la ou les victimes. Ce modèle repose sur l'idée que les États ne sont pas autorisés à violer les droits de l'homme dans d'autres États dans la mesure où ils ne peuvent pas le faire chez eux. Il tient également compte de l'évolution rapide des technologies et des nouvelles méthodes utilisées pour violer les droits de l'homme.

La compétence juridictionnelle n'est pas une condition préalable aux obligations en matière de droits de l'homme en vertu du droit international coutumier. Néanmoins, la portée extraterritoriale des obligations coutumières en matière de droits de l'homme, ainsi que la capacité d'un État à remplir ces obligations, font l'objet d'un débat.[176]

175 CDH, *Observation générale* n° 36 : Article 6 : Droit à la vie, CCPR/C/GC/36 (3 septembre 2019) (*Observation générale* 36), paragraphes 21 et 63. Voir également Sarah H. Cleveland, « Embedded International Law and the Constitution Abroad » (2010) 110 Columbia Law Review 225 ; Yuval Shany, « Taking Universality Seriously : A Functional Approach to Extraterritoriality in International Human Rights Law » (2013) 7 The Law and Ethics of Human Rights 47.

176 Ryan Fisher (éd.), Operational Law Handbook (National Security Law Department, the Judge Advocate General's School, Armée des États-Unis, 2022), p. 96.

Les États ont des obligations négatives et positives en matière de droits de l'homme, tant en ligne que hors ligne.

Les obligations négatives exigent des États qu'ils respectent les droits de l'homme en s'abstenant de toute intervention illégale.[177] Les obligations positives exigent des États qu'ils protègent les droits de l'homme contre toute intervention illégale d'autres États et d'acteurs non étatiques, et qu'ils garantissent les conditions nécessaires à la réalisation progressive des droits de l'homme en prenant des mesures actives.[178] Les obligations positives en matière de droits de l'homme désignent des obligations de comportement mesurées à l'aune d'une norme de diligence due : les États doivent faire tout leur possible pour protéger et garantir les droits de l'homme dans la mesure de leur compétence et de leur capacité d'agir.[179] À l'ère numérique, il est particulièrement important de protéger les droits de l'homme contre les agissements d'acteurs non étatiques, notamment les entreprises technologiques et les cybercriminels. Les obligations positives en matière de droits de l'homme sont distinctes des autres obligations de diligence due, y compris celles qui sont d'application générale évoquées ci-dessus.

Actuellement, l'opinion dominante veut que les **entreprises** n'aient pas d'obligations contraignantes en matière de droits de l'homme en vertu du droit international.[180] Cependant, dans sa position nationale, l'Autriche avance que « les entreprises commerciales, indépendamment de leur taille, de leur secteur d'activité, de leur contexte opérationnel et de leur structure, sont également tenues de respecter les droits de l'homme.[181] En tout état de cause, conformément aux Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, les entreprises ont la responsabilité de respecter les droits de l'homme, notamment en faisant preuve de diligence due pour identifier, prévenir, atténuer et rendre compte de leur impact sur les droits de l'homme en ligne et hors ligne.[182]

Les **droits absolus**, tels que la liberté d'opinion et l'interdiction de la torture, ne doivent jamais faire l'objet de mesures de restrictions, y compris par des moyens informatiques. Les **droits conditionnels**, tels que le droit à la vie privée et la liberté d'expression, peuvent faire l'objet de mesures de restriction légitimes. Les conditions desdites mesures sont définies par les dispositions des traités pertinents et les règles coutumières. Toutefois, en règle générale, les mesures de restriction légitimes en matière de droits de l'homme sont soumises aux exigences suivantes :

177 Cf. par exemple, CDH, *Observation générale* n° 31, para 6.

178 CDH, *Observation générale* n° 31, paragraphe 8 ; CIDH, *Velásquez Rodríguez c. Honduras* (Fond) (Ser C) n° 4 (29 juillet 1988), paragraphe 177.

179 Cf. Antonio Coco et Talita de Souza Dias, « Cyber Due Diligence » : A Patchwork of Protective Obligations in International Law (2021) 32 European Journal of International Law 795.

180 Cf. par exemple, la position commune de l'UA (2024), paragraphe 56.

181 Cf. la position nationale de l'Autriche (2024), p. 13. (Soulignement ajouté.)

182 Cf. HCDH, « *Guiding Principles on Business and Human Rights* : Implementing the United Nations Protect, Respect and Remedy" Framework », (2011), principes 11 à 15.

a. **Légalité –** Les restrictions doivent être fondées sur des lois accessibles et sont soumises à un contrôle judiciaire.

b. **Légitimité** – Les restrictions doivent être imposées dans un but légitime d'intérêt public, tel que la sécurité nationale ou la protection des droits d'autrui.

c. **Nécessité** – Les restrictions doivent constituer le moyen le moins restrictif possible pour atteindre l'objectif légitime.

d. **Proportionnalité** – la restriction en question doit être proportionnée à l'importance de l'objectif recherché.[183]

Ces conditions doivent être respectées par les États lorsqu'ils mènent des opérations cybernétiques et prennent d'autres mesures en ligne pour protéger des objectifs légitimes, tels que la surveillance ciblée de criminels présumés et les réglementations en matière de sécurité en ligne.

À l'heure où la militarisation du cyberespace s'intensifie, il est également important de garder à l'esprit que le **DIDH continue de s'appliquer pendant les conflits armés, au même titre que le DIH.**[184] Lorsque les deux régimes offrent des niveaux de protection différents aux civils, par exemple dans le contexte des frappes ciblées, seule une analyse au cas par cas permet de déterminer lequel est le plus approprié à la situation.[185] En règle générale, plus le conflit est proche du champ de bataille, plus le DIH est approprié pour le réglementer, et vice-versa.

Le fait de ne pas respecter, protéger ou garantir les droits de l'homme peut engager la responsabilité de l'État. Les droits de l'homme constituant des obligations erga omnes, c'est-à-dire des obligations envers tous les États parties à un traité ou envers la communauté internationale dans son ensemble, toute violation des droits de l'homme peut être invoquée par tout État partie au traité concerné ou par tout État dans le cas d'obligations coutumières en matière de droits de l'homme.[186] Comme indiqué ci-dessous, la question de savoir si les États non victimes peuvent prendre des contre-mesures en réponse à de telles violations reste controversée.

183 CDH, *Observation générale* n° 31, paragraphe 6 ; CDH, *Observation générale* n° 34 : Article 19 : Libertés d'opinion et d'expression, CCPR/C/GC/34 (12 septembre 2011), paragraphes 21-36.

184 CDH, *Observation générale* n° 31, paragraphe 11 ; CIJ, Nuclear Weapons Advisory Opinion, paragraphe 25 ; CIJ, Wall Advisory Opinion, paragraphes 105-106 ; CIJ, Case Concerning Armed Activities in the Territory of the Congo (République démocratique du Congo *c.* Ouganda) (Fond) [2005] CIJ Rep 168, paragraphe 216.

185 Cordula Droege, « Elective affinities ? Human rights and humanitarian law » (2008) 90 International Review of the Red Cross 501.

186 Cf. CDI, ARSIWA, article 48.

c. Droit pénal international

Les individus peuvent commettre ou encourager des crimes internationaux (y compris les crimes internationaux fondamentaux que sont l'agression, les crimes de guerre, le génocide et les crimes contre l'humanité) par des moyens cybernétiques ou non cybernétiques. Le fait qu'une opération cybernétique constitue ou non un crime international dépendra de l'interprétation du crime et de ses éléments dans chaque cas, y compris le comportement (actus reus) et les éléments psychologiques (mens rea), ainsi que le ou les modes de participation. Les crimes internationaux fondamentaux sont punissables en vertu du droit international coutumier et de certains traités, tels que le Statut de la Cour pénale internationale (CPI).[187] Les opérations cybernétiques constituant des crimes internationaux peuvent être poursuivies devant les tribunaux pénaux internationaux et nationaux compétents.[188]

Les opérations cybernétiques constituant des crimes internationaux peuvent être poursuivies devant les tribunaux nationaux ou internationaux compétents.

Cela inclut la CPI, laquelle est compétente, en règle générale, dès lors qu'un élément constitutif du crime est commis sur le territoire ou par un ressortissant d'un État partie au Statut de la CPI ou d'un État ayant accepté la compétence de la Cour.[189] L'utilisation des TIC pour commettre ou favoriser des crimes internationaux est loin d'être hypothétique. Par exemple, dans le contexte de la guerre en Ukraine, certaines opérations cybernétiques visant des civils et des infrastructures civiles pourraient non seulement constituer des violations du droit international humanitaire, mais aussi des crimes de guerre.[190]

En 2023, le procureur de la CPI a annoncé l'élaboration d'une politique relative à la poursuite des « crimes cybernétiques », y compris les crimes commis entièrement par des moyens cybernétiques et les situations dans lesquelles des opérations cybernétiques facilitent ou permettent des comportements non cybernétiques qui constituent un crime international.[191] Au moment de la rédaction du présent document, le projet de politique a été soumis à la consultation publique.[192] Néanmoins, à ce

187 Cf. Statut de Rome de la Cour pénale internationale (adopté le 17 juillet 1998, entré en vigueur le 1er juillet 2002) 2187 UNTS 90 (tel que modifié) (« Statut de la CPI »).

188 Cf. Robert Cryer, Darryl Robinson et Sergey Vasiliev, An Introduction to International Criminal Law and Procedure (CUP 2019), parties II et III.

189 Statut de la CPI, Article 12(2)-(3).

190 Cf. Lindsay Freeman, « Ukraine Symposium – Accountability for Cyber War Crimes », Articles of War (14 avril 2023) ; Andy Greenberg, « The Case for War Crimes Charges Against Russia's Sandworm Hackers », Wired (12 mai 2022).

191 CPI, « Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system » (22 janvier 2024).

192 CPI, « ICC Office of the Prosecutor launches public consultation on policy on cyber-enabled crimes under the Rome Statute » (7 mars 2025).

jour, seule la position nationale de l'Autriche couvre l'applicabilité du droit pénal international dans le cyberespace.[193]

La plupart des questions soulevées par l'application du DPI dans le cadre du cyberespace se posent également dans d'autres contextes. Par exemple, il est difficile de prouver l'intention nécessaire pour condamner quelqu'un pour génocide (l'intention de détruire, en tout ou en partie, un groupe national, religieux, ethnique ou racial tel quel),[194] que l'acte ait été commis en ligne ou hors ligne. De même, la question de savoir si un acte est suffisamment grave pour être admissible devant la CPI n'est pas propre aux actes commis dans le cyberespace.[195] Cependant, certaines difficultés découlent spécifiquement de l'application du droit pénal international aux activités cybernétiques.

Pour interpréter les règles du DPI afin de déterminer si des activités cybernétiques constituent ou permettent de commettre des crimes internationaux, il est nécessaire de respecter le **principe de légalité et ses corollaires** (non-rétroactivité, interprétation stricte, interdiction de l'analogie et in dubio pro reo).[196] Autrement dit, les définitions des crimes, l'élément intentionnel et les modes de participation ne peuvent être étendus au-delà de ce que le texte autorise raisonnablement afin de condamner des individus pour des actes commis dans le cyberespace.[197] Le principe de légalité protège les individus contre toute sanction pénale sans notification préalable équitable et constitue un droit de l'homme fondamental reconnu dans les traités et le droit international coutumier.[198]

L'interprétation des **crimes de guerre** dans le contexte cybernétique pourrait également soulever des défis spécifiques. Les crimes de guerre constituent des violations graves des Conventions de Genève et d'autres violations graves du DIH.[199] Le fait de diriger des attaques contre des civils ou des biens civils constitue un crime de guerre. Cependant, dans la jurisprudence de la CPI, des désaccords sont apparus quant à savoir si un comportement peut être qualifié d'attaque en raison de ses conséquences, et cette question est particulièrement pertinente dans le contexte cybernétique.[200] Comme indiqué ci-dessus, on ne sait pas non plus si les opérations cybernétiques causant

193 Cf. la position nationale de l'Autriche (2024), p. 20.

194 Convention sur la prévention et la répression du crime de génocide (signée le 9 décembre 1948, entrée en vigueur le 12 janvier 1951) 78 UNTS 277 (Convention sur le génocide), article 2.

195 Cf. Statut de la CPI, article 17(1)(d). Cf. également Marco Roscini, « Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes » (2019) 30 Criminal Law Forum 247.

196 Cf., par exemple, Statut de la CPI, articles 22 à 24.

197 Cf. Dapo Akande, « Sources of International Criminal Law », dans Antonio Cassese (dir.), The Oxford Companion to International Criminal Justice (OUP 2009), p. 44-45.

198 Cf., par exemple, PIDCP, article 15(1). Cf. également Talita Dias, Beyond Imperfect Justice : The Principles of Legality and Fair Labelling in International Criminal Law (Brill 2022) ; Kenneth S. Gallant, The Principle of Legality in International and Comparative Criminal Law (CUP 2010).

199 Cf. Statut de la CPI, article 8(2).

200 Dans le cadre de la CPI, *Prosecutor v.* Ntaganda, Appeals Judgment on the appeals of Mr. Bosco Ntaganda and the Prosecutor against the decision of Trial Chamber VI of 8 July 2019 entitled "Judgment" (30 mars 2021), ICC-01/04-02/06-2666-Red 30-03-2021, paragraphes 1164-1166 et annexe I, Separate opinion of Judges Morrison and Hofmanski, ICC-01/04-02/06-2666-Anx1.

des dommages non physiques et fonctionnels peuvent être considérées comme des attaques,[201] et dans quelle mesure leurs effets indirects peuvent être pris en compte.[202] De même, la controverse autour de la question de savoir si les données civiles constituent un bien civil est également pertinente pour l'interprétation des crimes de guerre, comme indiqué ci-dessus.[203]

Le **génocide** désigne le fait de commettre des actes potentiellement destructeurs dans l'intention de détruire, en tout ou en partie, un groupe national, religieux, ethnique ou racial en tant que tel.[204] Les cas où le génocide est entièrement commis par des moyens cybernétiques sont rares. Néanmoins, les discours en ligne peuvent constituer une instigation au génocide ou un crime distinct d'incitation directe et publique au génocide.[205] Cependant, il n'est pas clair si et dans quelle mesure les nouvelles formes d'expression en ligne, telles que le partage et l'appréciation de publications, peuvent constituer une participation au génocide ou une incitation à celui-ci.

Les **crimes contre l'humanité** constituent des violations graves des droits de l'homme commises dans le cadre d'une attaque généralisée ou systématique contre une population civile.[206] Ils peuvent être perpétrés ou rendus possibles par des moyens cybernétiques, tels que les technologies de surveillance.[207] Si la plupart des actes constituant des crimes contre l'humanité nécessitent de recourir à des moyens physiques (par exemple, le meurtre, l'extermination et la torture), les crimes de persécution et les « autres actes inhumains » peuvent être commis entièrement par des moyens cybernétiques.

201 Comparez, par exemple, les positions nationales du Danemark (2023), p. 455, et d'Israël (2021), p. 400, qui les positions nationales de l'Autriche (2024), p. 17, de la Colombie (2025), p. 13, du Costa Rica (2023), par. 49, de la France (2019), p. 13, de l'Allemagne (2021), p. 8, du Japon (2021), p. 7, et la Nouvelle-Zélande (2020), par. 25. Cf. également Mission permanente du Liechtenstein, The Council of Advisers' Report on the Application of the Rome Statute to Cyberwarfare (août 2021), paragraphe 12.

202 Comparez, par exemple, la position nationale du Royaume-Uni (2021), paragraphe 24, avec le CICR, IHL and challenges of armed conflicts (octobre 2015), 41.

203 Comparez, par exemple, les positions nationales de l'Autriche (2024), p. 18, de la Colombie (2025), p. 18, du Costa Rica (2023), paragraphe 50, de la Finlande (2020), p. 7, de l'Allemagne (2021), p. 8, et de la Roumanie (2021), p. 78, qui les positions nationales du Danemark (2023), p. 455, et d'Israël (2021), p. 401.

204 Cf. Convention sur le génocide, article 2, et Statut de la CPI, article 6.

205 Cf. Convention sur le génocide, article 3(c) et le Statut de la CPI, article 25(3)(b) et (e).

206 Cf. par exemple, Statut de la CPI, article 7, et CDI, *Draft articles on* Prevention and Punishment of Crimes Against Humanity (2019), article 1.

207 Par exemple, Centre européen pour les droits constitutionnels et humains, « Surveillance in Syria : European firms may be aiding and abetting crimes against humanity ».

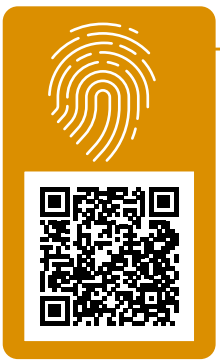
Le **crime d'agression** est une violation grave de l'interdiction du recours à la force commise par une personne occupant une position de leadership. Dans le Statut de la CPI, un acte d'agression doit également, par sa nature, sa gravité et son ampleur, constituer une violation manifeste de la Charte des Nations Unies.[208] Comme indiqué ci-dessus, certaines opérations cybernétiques peuvent constituer un recours illicite à la force si leur ampleur et leurs effets sont comparables à ceux d'un recours à la force armée, par exemple lorsqu'elles entraînent des pertes en vies humaines ou des destructions matérielles. Toutefois, compte tenu de la définition plus restrictive du crime d'agression et de l'application du principe de légalité, seules les opérations cybernétiques les plus graves et manifestement illégales constitueront ce crime.

Les crimes internationaux peuvent être commandités par différentes **formes de participation**.[209] La participation active, la complicité et la responsabilité du commandement sont particulièrement pertinentes dans le cyberespace, car les cyberactivités sont plus susceptibles de contribuer à la perpétration d'un crime international par des moyens non cybernétiques que de constituer en elles-mêmes un tel crime. La question de la causalité est importante dans le contexte cybernétique : dans quelle mesure les effets indirects ou répercussions des opérations cybernétiques peuvent-ils être considérés comme causés par le comportement individuel en question ? La responsabilité pénale individuelle sera probablement engagée si ces effets sont intentionnels. Cependant, la causalité devient cruciale lorsque l'individu peut être condamné sur la base d'un comportement imprudent ou négligent. De nombreuses opérations cybernétiques susceptibles de provoquer des conséquences catastrophiques seront évitées grâce aux progrès de la cybersécurité, et dans ces cas, l'opération cybernétique peut constituer une tentative de crime international lorsque le comportement est intentionnel.[210]

208 Cf. Statut de la CPI, article 8 bis.
209 Cf. Statut de la CPI, articles 25 et 28.
210 Cf. Statut de la CPI, article 25(3)(f).

4. Responsabilité de l'État

Cette section examine comment le droit relatif à la responsabilité de l'État s'applique aux activités cybernétiques. De manière générale, cet ensemble de lois régit la responsabilité des États pour les actes internationalement illicites et les conséquences juridiques qui en découlent. Bien qu'ils n'aient pas été codifiés dans un traité contraignant, les Articles sur la responsabilité de l'État pour les faits internationalement illicites (2001) de la CDI sont largement considérés comme une expression du droit international coutumier. Il est largement admis que ces règles s'appliquent au contexte cybernétique,[211] mais certains États ont fait remarquer que leur application n'est pas toujours simple en raison des caractéristiques uniques des TIC.[212] Cette section examine trois thèmes clés qui ont retenu le plus l'attention dans le contexte cybernétique : l'attribution, les contre-mesures et l'état de nécessité. Elle met en évidence les domaines faisant l'objet d'un consensus général ainsi que les aspects qui restent en suspens ou contestés.



a. Attribution

L'attribution est l'un des éléments constitutifs de la responsabilité de l'État. Elle désigne le lien juridiquement défini entre un acte (ou une omission) donné et un État.[213] Lorsque les critères pertinents sont remplis, le comportement en question est considéré comme attribuable à l'État, ce qui signifie que le droit le considère comme le comportement propre de l'État. Si ce comportement attribuable enfreint une obligation juridique applicable qui lie l'État, il constitue un fait internationalement illicite dont l'État est légalement responsable.[214]

En règle générale, le comportement des organes de l'État est attribuable à l'État,[215] ce qui n'est pas le cas des actions des acteurs non étatiques, sauf dans des conditions spécifiques.[216]

211 Cf., par exemple, les positions nationales de l'Australie (2021), p. 5, de l'Autriche (2024), p. 8, du Canada (2022), paragraphe 32, de la Colombie (2025), p. 14, de la République tchèque (2024), paragraphe 52, du Danemark (2023), p. 452, de l'Estonie (2019 et 2021, p. 28), de la Finlande (2020), p. 5, de l'Italie (2021), pp. 5-6, de la Norvège (2021), p. 6, de la Suède (2022), p. 5, de la Suisse (2021), p. 5, ainsi que les positions communes de l'UA (2024), paragraphe 61, et de l'UE (2024), p. 8. Cf. également *Manuel de Tallinn 2.0*, 80, paragraphe 4.

212 Cf., par exemple, la position nationale de l'Italie (2021), p. 6 ; de la Chine (2021), *Déclaration sur l'applicabilité du droit international au sein du Groupe de travail à composition non limitée* (16 décembre 2021).

213 CDI, ARSIWA, commentaire de l'article 2, paragraphe 12.

214 CDI, ARSIWA, commentaire de l'article 2, paragraphe 12.

215 CDI, ARSIWA, Article 4.

216 Cf. notamment CDI, ARSIWA, article 8.

- Les **organes de l'État** comprennent des entités telles que les unités cybermilitaires, les agences de renseignement civiles, les responsables de l'application de la loi et toute autre entité ou personne physique qui compose l'organisation de l'État. Ce concept couvre également les organes mis à la disposition d'un État par un autre État,[217] tels que les membres de l'équipe d'intervention en cas d'urgence informatique (CERT) d'un État détachés dans un autre État et opérant sous l'autorité exclusive de l'État d'accueil.[218] Il est important de noter que le comportement d'un organe étatique est attribuable à l'État concerné même si cet organe outrepasse ses pouvoirs ou enfreint les instructions qui lui ont été données (c'est-à-dire agit ultra vires).[219]
- Les activités des **acteurs non étatiques** telles que les opérations cybernétiques menées par des hacktivistes individuels, des groupes de pirates informatiques ou des gangs de ransomware, peuvent être attribuées à un État dans certaines conditions. C'est le cas lorsqu'ils agissent en totale dépendance vis-à-vis de l'État[220] ou sous ses instructions, sa direction ou son contrôle.[221] Le degré de contrôle requis reste sujet à débat : la CIJ a affirmé que l'exercice d'un « contrôle effectif » était nécessaire,[222] tandis que le Tribunal pénal international pour l'ex-Yougoslavie a élaboré un critère moins strict de « contrôle général », applicable aux groupes organisés aux fins de la classification des conflits armés.[223] Seuls quelques États se sont prononcés sur cette question jusqu'à présent, et ceux qui l'ont fait ont tous approuvé le critère du contrôle effectif.[224] Il semble que cela soit dû à la crainte qu'un critère moins strict en matière d'attribution puisse donner lieu à des abus. Enfin, le comportement d'un acteur non étatique est également attribuable à un État si ledit acteur était habilité à exercer des fonctions gouvernementales[225] ou si l'État reconnaît et adopte par la suite ce comportement comme étant le sien.[226]

Les cyberactivités menées par des acteurs non étatiques peuvent être attribuées à un État lorsqu'elles sont menées sous le contrôle de celui-ci, mais la question de savoir quel est le seuil de contrôle requis reste posée.

217 CDI, ARSIWA, Article 6.

218 *Manuel de Tallinn 2.0*, commentaire de la règle 16, paragraphe 4.

219 CDI, ARSIWA, Article 7.

220 2CIJ, Affaire Nicaragua, paragraphe 110 ; CIJ, Affaire relative à l'application de la Convention sur la prévention et la répression du crime de génocide (Bosnie-Herzégovine *c.* Serbie-et-Monténégro) (Jugement) [2007] CIJ Rep 43 (Affaire du génocide en Bosnie), paragraphe 392.

221 CDI, ARSIWA, Article 8.

222 CIJ, Affaire Nicaragua, paragraphe 115 ; CIJ, Affaire du génocide en Bosnie, paragraphe 400.

223 TPIY, *Prosecutor v.* Tadić (Appeal Judgment) IT-94-1-A (15 juillet 1999), paragraphes 116 et suivants.

224 Cf. les positions nationales du Brésil (2021), p. 21, de l'Irlande (2023), paragraphe 22, des Pays-Bas (2019), p. 6, et de la Norvège (2021), p. 6.

225 CDI, ARSIWA, Article 5.

226 CDI, ARSIWA, Article 11.

Lorsqu'un État victime invoque la responsabilité internationale d'un autre État dans le cadre d'une cyberactivité, cela sous-entend qu'il considère que cette activité est attribuable à cet État. Bien que le droit international ne réglemente pas les étapes procédurales permettant de parvenir à une telle conclusion, il est généralement admis que toute allégation d'acte illicite doit être raisonnablement étayée.[227] Cependant, les États ne sont pas tenus, en vertu du droit international, de divulguer publiquement les éléments sur lesquels ils fondent leur attribution. Cette interprétation a été confirmée dans plusieurs positions nationales.[228]

Même si une cyberactivité n'est pas attribuable à un État, celui-ci peut néanmoins être tenu responsable dans certaines circonstances exceptionnelles pour ne pas avoir pris de mesures raisonnables afin de prévenir, de faire cesser ou de corriger cette activité. Cette responsabilité ne découle pas de l'activité elle-même, mais du fait que l'État a manqué à son obligation de diligence due, laquelle a été examinée plus en détail ci-dessus.

b. Contre-mesures

Les contre-mesures sont des réponses à des actes internationalement illicites qui, autrement, seraient illégaux, mais qui sont autorisés afin d'inciter un État responsable d'un acte illicite à se conformer à ses obligations en vertu du droit international.[229] Elles constituent une circonstance excluant l'illicéité et sont bien établies dans le droit international coutumier.[230] Les contre-mesures doivent être distinguées des mesures de rétorsion, lesquelles sont des actes hostiles mais licites pris par l'État victime à l'encontre de l'État responsable (tels que la suspension des relations diplomatiques).[231]

227 Assemblée générale des Nations Unies, Rapport du Groupe d'experts gouvernementaux sur la promotion d'un comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, A/70/174 (22 juillet 2015), paragraphe 28(f) ; *Report of the* Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135 (14 juillet 2021), paragraphe 71(g). Cf. également, par exemple, les positions nationales du Brésil (2021), p. 21, de l'Allemagne (2021), p. 12, de la Russie (2021), p. 80, et de la Suisse (2021), p. 6.

228 Cf., par exemple, les positions nationales de l'Australie (2021), p. 5, du Canada (2022), paragraphe 33, de la République tchèque (2024), paragraphe 58, du Danemark (2023), p. 452, de la Finlande (2020), p. 6, de la France (2019), p. 11, de l'Allemagne (2021), p. 12, d'Israël (2021), pp. 404-405, de l'Italie (2021), p. 5, des Pays-Bas (2019), p. 6, de la Nouvelle-Zélande (2020), paragraphe 20, de la Suède (2022), p. 5, de la Suisse (2021), p. 6, du Royaume-Uni (2018 et 2021, paragraphe 15) et des États-Unis (2016, p. 19 et 2021, p. 141), ainsi que la position commune de l'UE (2024), p. 8.

229 CDI, ARSIWA, Commentaire, partie 3, chapitre 2, paragraphe 1.

230 CDI, ARSIWA, article 22, paragraphes 1 et 2, et commentaire du chapitre II de la troisième partie, paragraphe 1.

231 Elizabeth Zoller, Peacetime Unilateral Remedies : An Analysis of Countermeasures (Transnational 1984) 5.

La plupart des États acceptent l'applicabilité des contre-mesures aux opérations cybernétiques.[232] En effet, les contre-mesures constituent l'un des rares moyens dont disposent les États pour faire respecter le droit international en l'absence d'une force de police mondiale.[233]

En raison de l'augmentation du nombre d'opérations cybernétiques illicites et de leur sophistication, les contre-mesures constituent un outil important de responsabilisation dans le cyberespace.

Cependant, au moins un État, le Brésil, a remis en question leur statut coutumier de manière générale.[234] Ce point de vue semble s'inspirer des objections soulevées par plusieurs pays en développement concernant l'inclusion des contre-mesures dans les articles de la CDI sur la responsabilité de l'État au début des années 2000.[235] D'autres ont condamné le recours aux contre-mesures dans le contexte cybernétique, craignant une escalade du conflit et la militarisation du cyberespace.[236] Ce sujet est controversé, c'est pourquoi, par exemple, il est expressément exclu de la position commune de l'UA.[237]

Afin de garantir que les contre-mesures ne donnent pas lieu à des abus, elles sont soumises à des **conditions strictes sur le fond et sur la forme** conformément au droit international général. Ainsi, les contre-mesures doivent avoir pour seul objectif d'amener l'État responsable à se conformer à ses obligations, être proportionnées au préjudice subi, être temporaires et réversibles dans la mesure du possible, et être conformes à certaines obligations internationales telles que l'interdiction du recours à la force et le respect des droits de l'homme fondamentaux.[238] Cependant, les contre-mesures ne doivent pas nécessairement être de même nature. En d'autres termes, le droit international n'exclut pas le recours à des contre-mesures cybernétiques pour répondre à un acte internationalement illicite non cybernétique, et vice versa. En outre, avant de prendre des contre-mesures, l'État victime doit adresser une demande préalable à l'État responsable pour qu'il se conformer à ses obligations internationales. En règle générale, l'État victime doit également notifier l'État responsable et lui proposer de négocier avant de recourir à des contre-

232 Cf., par exemple, les positions nationales de l'Australie (2021), p. 5, du Canada (2022), paragraphe 34, de l'Estonie (2019), de la Finlande (2020), p. 5, de la France (2019), p. 11, de l'Allemagne (2021), p. 14, d'Israël (2021), p. 403, de l'Italie (2021), p. 7, du Japon (2021), p. 7, des Pays-Bas (2019), p. 7, de la Norvège (2021), p. 7, de la Roumanie (2021), p. 81, de la Suisse (2021), p. 7, du Royaume-Uni (2018, 2021, paragraphe 15) et des États-Unis (2016, p. 19).

233 Cf. Elisabeth Zoller, Peacetime Unilateral Remedies : An Analysis of Countermeasures (Transnational 1984).

234 Cf. la position nationale du Brésil (2021), p. 21.

235 Cf. Annuaire de la Commission du droit international 2000, Vol. I (Nations Unies 2000), p. 306-310.

236 Cf., par exemple, la position nationale de la Chine (2021), Déclaration au sein du Groupe de travail à composition non limitée (16 décembre 2021).

237 Cf. position commune de l'UA (2024), paragraphe 61.

238 CDI, ARSIWA, articles 49 à 51, 52(3) et 53.

mesures, sauf si l'urgence exige une action immédiate, par exemple pour préserver ses droits.[239] Des contre-mesures peuvent être prises lorsque des négociations sont en cours ou qu'un différend est en cours devant un organe de règlement des différends. Toutefois, elles doivent être suspendues si l'organe de règlement des différends a le pouvoir de rendre des décisions contraignantes ordonnant des mesures équivalentes et si la violation antérieure a cessé.[240]

La manière dont ces conditions générales s'appliquent dans le contexte cybernétique fait l'objet d'un débat. Par exemple, certains États ont fait valoir dans leurs positions nationales que l'exigence d'une demande préalable pouvait être levée dans les cas urgents.[241] Cette opinion repose sur la crainte que, en formulant une demande préalable, l'État victime perde l'effet de surprise ou révèle des capacités cybernétiques sensibles.[242]

La notion de **contre-mesures collectives** – à savoir les contre-mesures prises par des États autres que l'État victime – reste controversée, en particulier dans le cyberespace.[243] L'utilisation incohérente de ce terme ajoute à l'incertitude qui entoure cette question. Le débat sur la légalité des contre-mesures collectives a pris une importance particulière depuis la formation d'alliances cybernétiques et la mise en place de réponses conjointes aux opérations cybernétiques malveillantes.[244] Certains États ont exprimé leur soutien en faveur de la prise de contre-mesures dans l'intérêt général, c'est-à-dire en réponse à des violations d'obligations erga omnes, telles que celles relatives à la protection des droits de l'homme.[245] Quelques États ont également soutenu la prise de contre-mesures au nom des États tiers victimes, quel que soit le type d'obligation violée.[246] Le soutien aux contre-mesures collectives repose sur l'idée de solidarité internationale et sur celle de la protection des droits de l'homme et d'autres valeurs collectives. Les contre-mesures collectives pourraient également remédier aux inégalités en matière de capacités cybernétiques en permettant aux États les plus avancés de prendre des mesures au nom des plus faibles. Cependant, d'autres États ont rejeté la legalité des contre-

239 CDI, ARSIWA, article 52(1) et (2).

240 CDI, ARSIWA, article 52(3).

241 241 Cf. les positions nationales du Costa Rica (2023), paragraphe 14, de l'Italie (2021), p. 7, de la Suisse (2021), p. 6, du Royaume-Uni (2018 et 2021, paragraphe 19) et des États-Unis (2016, p. 22, 2020 et 2021, p. 142).

242 242 Cf. Henning Lahmann, Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution (CUP 2020), 138.

243 243 Cf. Talita Dias, Countermeasures in international law and their role in cyberspace (Chatham House 2024) 33–54.

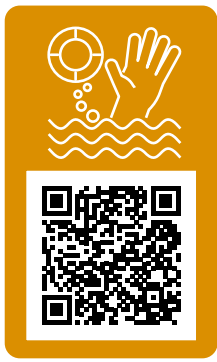
244 244 Cf. par exemple Ashley Deeks, « Defend Forward and Cyber Countermeasures » Hoover Working Group on National Security, Technology, and Law (2020), 8–9 ; Michael N. Schmitt et Sean Watts, « Collective cyber countermeasures? » (2021) 12 Harvard National Security Journal 373.

245 245 Cf. par exemple les positions nationales de l'Autriche (2024), p. 9, de la Colombie (2025), p. 17, de l'Irlande (2023), paragraphes 25-26, et de la Pologne (2022), p. 8.

246 246 Cf. par exemple les positions nationales du Costa Rica (2023), paragraphe 15, et de l'Estonie (2019).

mesures collectives en vertu du droit international.[247] Ces points de vue semblent reposer sur des préoccupations liées à une course aux armements cybernétiques, à des effets disproportionnés, à une escalade du conflit et à la déstabilisation des relations conventionnelles.[248] La position adoptée par les États sur les contre-mesures collectives dans d'autres contextes, tels que la guerre en Ukraine, pourrait également déterminer leur point de vue dans le contexte cybernétique.[249]

Enfin, certains États ont suggéré que des États tiers pourraient aider ou assister un État victime dans la prise de ses contre-mesures, y compris dans le contexte cybernétique.[250] Ce point de vue repose sur la compréhension que l'État victime agit de manière légale et que l'État qui lui apporte son assistance n'encourt lui-même aucune responsabilité internationale, à condition que son assistance – qui peut inclure des mesures telles que la fourniture de fonds, de renseignements, de formation ou d'équipements – soit elle-même légale au regard du droit international.[251]



c. Nécessité

À l'instar des contre-mesures, l'état de nécessité est une circonstance qui exclut le caractère illicite d'un comportement qui serait autrement incompatible avec les obligations internationales d'un État. La plupart des États conviennent que l'état de nécessité est fondé sur le droit international coutumier, comme le reconnaît la CIJ.[252] Il s'agit toutefois d'un moyen de défense exceptionnel, dans la mesure où il ne peut être invoqué qu'en cas de **danger grave et imminent pour les intérêts essentiels** d'un État, de son peuple ou de la communauté internationale.[253] Même dans ces circonstances, l'action de l'État ne doit pas porter gravement atteinte aux intérêts essentiels de l'État ou des États concernés ni à ceux de la communauté internationale.[254] Autrement dit, l'impact

247 247 Cf., par exemple, les positions nationales du Canada (2022), paragraphe 37, et de la France (2021), p. 4.

248 Cf., par exemple, Assemblée générale des Nations Unies, Sixième Commission, Compte rendu analytique de la 15e séance, A/C.6/55/SR.15 (13 novembre 2000), par. 25 (Israël) ; Assemblée générale des Nations Unies, Sixth Committee, Summary record of the 14th meeting, A/C.6/55/SR.14 (10 novembre 2000), paragraphe 31 (Royaume-Uni) ; et Chine, « Statement by the Chinese Delegation at the Thematic Debate of the First Committee of the 72th UNGA » (2017).

249 Cf. par exemple, Conseil de l'UE (2023), « Sanctions de l'UE – Nouveau considérant dans la décision du Conseil », (PESC) 2023/191 du 27 janvier 2023 – Contre-mesures, WK 5169/2023 INIT, paragraphe 4 ; Italie, Tribunal administratif régional du Latium (deuxième session), N. 08669/2022 REG.PROV. COLL, N. 04902/2022 REG.RIC., Sentence (2022).

250 Cf. par exemple les positions nationales du Canada (2022), paragraphe 37, et du Danemark (2023), p. 454.

251 CDI, ARSIWA, Commentaire de l'article 16, paragraphes 5–6 ; Talita Dias, Countermeasures in international law and their role in cyberspace (Chatham House, 2024), p. 50–54 ; Miles Jackson et Federica Paddeu, « The Countermeasures of Others » (2024) 118(2) American Journal of International Law 231, 254–255.

252 Cf. CDI, ARSIWA, Commentaire de l'article 25, paragraphe 14 ; CIJ, Projet Gabčíkovo-Nagymaros (Hongrie/Slovaquie) (Arrêt) [1997] *CIJ Rec.* 7, paragraphe 51.

253 CDI, ARSIWA, article 25(1)(a) et commentaire, paragraphe 15.

254 CDI, ARSIWA, article 25(1)(b).

des actes justifiés par l'état de nécessité ne doit pas être plus important que le préjudice évité.[255] En outre, l'état de nécessité ne peut être invoqué par les États qui ont contribué de manière substantielle à la situation dans laquelle ils se trouvent ou lorsque l'obligation internationale en question exclut cette défense.[256] Par exemple, l'état de nécessité ne peut justifier les violations de l'interdiction du recours à la force, qui comporte ses propres exceptions.[257]

Plusieurs États ont reconnu l'applicabilité de la nécessité dans le contexte cybernétique dans leurs positions nationales.[258] La nécessité a également été évoquée comme une justification possible pour les opérations cybernétiques défensives contre des dommages en cours ou imminents, souvent appelées « cyberdéfense active » ou « défense avancée ».[259]

À la différence des contre-mesures, **il est possible d'invoquer l'état de nécessité même lorsqu'il n'y a pas de violation du droit international par un État**. Cela signifie que la défense ne dépend pas de l'attribution et peut être invoquée en réponse aux actes d'acteurs non étatiques. La nécessité peut justifier des actions qui, autrement, violeraient les droits d'États non responsables si les conditions susmentionnées sont remplies. De plus, la nécessité ne dépend pas d'un préjudice réel et peut être invoquée à titre préventif contre des menaces imminentes. Comme l'ont indiqué les Pays-Bas dans leur position nationale, la nécessité « vise principalement à donner à un État la possibilité de protéger ses propres intérêts et de minimiser le préjudice qu'il subit ».[260]

Ces caractéristiques rendent l'argument de l'état de nécessité particulièrement attrayant dans le contexte cybernétique, compte tenu des difficultés d'attribution évoquées ci-dessus. Cependant, les États ont souligné le caractère exceptionnel de cette défense et les conditions très strictes auxquelles elle est soumise. Cela permet d'éviter les abus et le risque d'escalade du conflit, qui pourrait se révéler particulièrement important dans l'environnement du cyberespace, marqué par son évolution rapide et son caractère interconnecté.

À la différence des contre-mesures, l'état de nécessité peut être invoqué même en l'absence d'un acte illicite préalable commis par un autre État, ce qui en fait une option intéressante dans le contexte cybernétique où l'attribution est souvent incertaine.

255 CDI, ARSIWA, Commentaire de l'article 25, paragraphes 1 et 17.

256 CDI, ARSIWA, Article 25(2).

257 CDI, ARSIWA, Commentaire de l'article 25, paragraphe 21.

258 Cf. les positions nationales du Costa Rica (2023), paragraphe 16, de la République tchèque (2024), paragraphe 61, de la France (2019), p. 8, de l'Allemagne (2021), p. 14, du Japon (2021), p. 5, des Pays-Bas (2019), pp. 7-8, de la Norvège (2021), p. 9, de la Suède (2022), p. 6, de la Suisse (2021), p. 7, ainsi que la position commune de l'UE (2024), p. 9.

259 Cf. « Applying the Plea of Necessity to Cyber Operations », compte rendu de réunion, Chatham House, International Law Programme (27 septembre 2023) ; Henning Lahmann, « The Plea of Necessity in Cyber Emergencies » (2023) 92 Nordic Journal of International Law 422.

260 Position nationale des Pays-Bas (2019), p. 8.

Il a été noté que la nécessité peut être **invoquée en réponse à des dommages physiques et non physiques**.[261] Dans leurs positions nationales, certains États ont proposé les exemples suivants d'opérations cybernétiques qui pourraient constituer un « danger grave et imminent » menaçant un « intérêt essentiel » et donc déclencher l'invocation de l'état de nécessité : une coupure d'Internet[262] et une opération cybernétique visant des infrastructures critiques,[263] telles qu'une centrale nucléaire.[264] Dans ce contexte, l'imminence désigne non seulement les dangers proches dans le temps, mais aussi ceux qui sont certains ou inévitables.[265]

5. Conclusion

Dans ce chapitre, nous avons présenté un aperçu des principales questions juridiques de fond pertinentes aux fins de l'élaboration des positions nationales sur l'application du droit international dans le cadre des activités cybernétiques. La sélection de ces questions s'est appuyée sur les positions publiées à ce jour, les discussions multilatérales en cours au sein du Groupe de travail à composition non limitée (GTCNL) et les consultations à huis clos organisées dans le cadre du présent projet.

La structure du chapitre reposait sur trois grandes catégories. Tout d'abord, il a été question des principes fondamentaux du droit international, notamment la souveraineté, la non-intervention, l'interdiction du recours à la force, la diligence due, le règlement pacifique des différends et l'autodétermination. Ensuite, nous avons examiné l'applicabilité et l'interprétation de trois régimes spécialisés du droit international : le DIH, le DIDH et le DPI. Enfin, nous avons abordé le droit régissant la responsabilité des États, en mettant l'accent sur l'attribution, les contre-mesures et l'état de nécessité.

Dans tous ces domaines, l'analyse a révélé des points de convergence et de divergence importants entre les États. Les États conviennent que le droit international s'applique à l'utilisation des TIC en général et aux régimes spécifiques examinés dans le présent chapitre. Ils s'accordent également souvent sur les éléments des règles applicables (par exemple, le fait qu'un acte doit porter sur des questions relevant des affaires intérieures ou extérieures d'un État et être de nature contraignante pour constituer une intervention interdite). Parfois, ils conviennent aussi qu'une question, telle que la diligence due, nécessite une étude plus approfondie.

261 Cf. par exemple les positions nationales de la République tchèque (2024), paragraphe 68, de l'Allemagne (2021), p. 15, et des Pays-Bas (2019), p. 8.

262 Position nationale des Pays-Bas (2019), p. 8.

263 Position nationale de l'Allemagne (2021), pp. 14-15.

264 Cf. « Applying the Plea of Necessity to Cyber Operations », résumé de la réunion, Chatham House, International Law Programme (27 septembre 2023), paragraphe 5.

265 CIJ, Projet Gabčíkovo-Nagymaros (Hongrie/Slovaquie) (Arrêt) [1997] CIJ Rep. 7, par. 54.

Il subsiste toutefois d'importantes divergences. On peut notamment se demander si une règle donnée constitue une obligation individuelle dans le contexte cybernétique (comme c'est le cas pour la souveraineté et la diligence due), à partir de quel seuil une opération cybernétique peut être qualifiée de violation de la règle en question (par exemple, la souveraineté et les interdictions d'intervention et de recours à la force) et comment qualifier une catégorie de comportements menés par des moyens cybernétiques (tels que le cyberespionnage). Ces divergences motivent les États à poursuivre le débat et à contribuer aux discussions en cours.

La présentation générale contenue dans ce chapitre fournit ainsi aux États qui élaborent leur position nationale une feuille de route leur permettant de sélectionner les questions ou les thèmes à inclure (ou à éviter), de naviguer entre les points de discorde, de se forger une opinion sur ces différentes questions et, enfin, de trouver un terrain d'entente sur la manière dont le droit international s'applique dans le contexte cybernétique. Une fois ces questions de fond abordées, l'étape suivante consiste à décider de la manière dont la position nationale doit être présentée, notamment son format, son style, son langage et ses stratégies de diffusion. C'est ce que nous aborderons dans le chapitre suivant.

		Positions communes													
		AU	EU	AU	AT	BR	CA	CN	CO	CR	CU	CZ	DK	EE	FI
Règles et principes fondamentaux	Souveraineté	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Non-intervention	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Recours à la force	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Diligence due	●	●	●	●	●	●	●	●	●		●	●	●	●
	Règlement pacifique des différends	●	●	●	●	●	●	●	●	●	●	●		●	
	Autodétermination														
Régimes spécialisés	DIH	●	●	●	●	●	●		●	●	●	●	●	●	●
	DIDH	●	●	●	●	●	●		●	●		●	●	●	●
	DPI				●										
Responsabilité de l'État	Attribution	●	●	●	●	●	●		●	●	●	●	●	●	●
	Contre-mesures		●	●	●	●	●		●	●		●	●	●	●
	Nécessité		●		●					●		●			●

Figure 8 : Aperçu des positions communes et nationales par thème abordé.

Positions nationales

	FR	DE	IR	IE	IL	IT	JP	KZ	KE	NL	NZ	NO	PK	PL	RO	RU	SG	SE	CH	UK	US
	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	●	●	●	●	●	●	●			●	●	●	●	●	●	●	●	●	●	●	●
	●	●	●	●	●	●	●			●	●	●	●	●	●	●	●	●	●	●	●
	●	●		●	●	●	●			●	●	●		●	●			●	●	●	●
	●						●		●		●	●	●			●	●		●	●	
			●			●										●					
	●	●		●	●	●	●		●	●	●	●	●	●	●		●	●	●	●	●
				●		●	●	●	●	●	●	●		●	●		●	●	●	●	●
	●	●		●	●	●	●			●	●	●		●	●	●		●	●	●	●
	●	●		●	●	●	●			●	●	●		●	●	●	●	●	●	●	●
	●	●					●			●		●						●	●		

CHAPITRE 5 :

PRÉSENTATION

EN BREF

Le présent chapitre traite de la manière dont les États peuvent présenter et diffuser leurs positions nationales. Il compare les formats écrits et oraux, examine la longueur, la structure, le langage et les exemples utilisés, et présente les différentes options de diffusion. La clarté, la portée et l'impact d'une position dépendent du choix qui est fait. Le chapitre encourage les États à trouver un équilibre entre l'autorité juridique et l'accessibilité, et à adapter leur approche en fonction de leurs objectifs, de leur public et des ressources disponibles.

1. Introduction

Bien que les positions nationales publiées jusqu'à présent couvrent une liste de sujets plutôt cohérente, comme indiqué au **chapitre 4**, elles ont été présentées de différentes manières. Les premières ont été prononcées sous forme de discours gouvernementaux, mais la tendance s'est progressivement orientée vers la publication de documents écrits distincts. La longueur des positions nationales varie également considérablement, allant de documents concis de quelques pages seulement à des documents plus détaillés dépassant les 20 pages. Certaines sont très générales, tandis que d'autres abordent de manière plus approfondie des questions complexes de droit international et/ou des défis spécifiques liés au cyberespace, y compris des scénarios ou des exemples d'opérations cybermalveillantes. La structure des positions varie également, certaines utilisant des titres clairs, des paragraphes numérotés et/ou des résumés. La plupart des positions nationales ont été publiées en anglais, certaines étant également publiées ou traduites dans d'autres langues. Les positions nationales ont été diffusées à différents publics à l'aide de diverses stratégies, notamment des communiqués de presse, des publications croisées dans des revues académiques ou des blogs, des annonces sur les réseaux sociaux et des événements visant à discuter de leur contenu.

La présentation d'une position nationale ne se limite pas à une simple réflexion sur les particularités nationales ou régionales ; elle détermine également en grande partie son impact. Ce chapitre se propose d'analyser les différentes tendances en matière de format, de style, de langage et de diffusion des positions nationales. Il examine également pourquoi ces choix sont importants et quelles sont leurs implications pour le statut, le contenu et l'impact des positions nationales.

Comme indiqué dans **l'introduction** du présent Manuel, une position nationale est considérée comme une déclaration publique, publiée sous forme écrite, laquelle exprime le point de vue d'un État sur une ou plusieurs questions fondamentales relatives à l'application du droit international dans le cyberespace.

Les États ont néanmoins exprimé leur point de vue sur divers aspects de l'application du droit international dans le cyberespace sous d'autres formes. Par exemple, de nombreux États ont fait des remarques orales et/ou soumis des déclarations écrites au Groupe de travail à composition non limitée GTCNL des Nations Unies sur les questions de droit international qu'ils estiment devoir être incluses dans ses rapports annuels.[1] Parmi ces États figurent plusieurs pays du Sud qui n'ont pas encore publié de position nationale, tels que le Chili,[2] l'Afrique du Sud[3] et certains États membres du Forum des îles du Pacifique.[4] Ces déclarations peuvent en fait servir de base ou de point de départ à l'élaboration d'une position nationale à part entière. Toutefois, dans la mesure où elles n'expriment pas les opinions substantielles d'un État sur la manière dont les différentes règles et principes du droit international s'appliquent aux activités cybernétiques, elles ne relèvent pas du champ d'application du présent Manuel – comme indiqué ci-dessous, jusqu'à présent, seuls trois États ont utilisé leurs déclarations au GTCNL pour présenter leurs positions nationales.

Certains choix politiques déterminent le format, le style, le langage et les stratégies de diffusion des positions nationales.

Il s'agit avant tout du choix du statut juridique de la position nationale, c'est-à-dire de déterminer si elle constitue une preuve de la pratique des États et/ou de *l'opinio juris,* une aide à l'interprétation ou une simple déclaration politique. Par ailleurs, comme indiqué au **chapitre 3**, il est important de déterminer si la position suivra une approche déductive du droit international (en énonçant les règles pertinentes de manière abstraite, puis en expliquant comment elles s'appliquent dans le contexte cybernétique) ou une approche inductive (en partant de défis factuels spécifiques dans le contexte cybernétique, puis en déterminant les règles qui s'appliquent). Enfin, les fonctions, les objectifs et/ou les motivations d'une position nationale influenceront également les choix en matière de format, de style, de langage et de diffusion. Comme indiqué au **chapitre 2**, les fonctions générales d'une position nationale peuvent inclure la communication ou la collaboration avec différentes parties prenantes, la transformation ou l'adaptation du droit international applicable aux activités cybernétiques et la prévention des comportements illégaux. Cela peut se traduire par des objectifs et des motivations spécifiques, notamment la prévention des erreurs d'appréciation et des escalades en renforçant la prévisibilité et la stabilité à grande échelle, l'amélioration de la conformité et de la responsabilité, et l'orientation de l'évolution du droit international en remédiant à l'incertitude juridique.

1 Cf. par exemple, Autriche, Pre-Draft *Report of the* OEWG – TIC: Comments by Austria (31 mars 2020).

2 Ministère des Relations extérieures du Chili, Derecho Internacional, ONU, New York, Groupe de travail à composition non limitée, sixième session de fond (11-15 décembre 2023).

3 Cf. Afrique du Sud, Statement by South Africa in the ninth session of the Open-Ended Working Group on security of and in the use of TICs (2021-2025) - International Law, ONU, New York (4 décembre 2024).

4 Forum des îles du Pacifique, Statement delivered by PIF Chair on behalf of the Pacific Islands Forum, ONU (New York, 4 décembre 2024).

2. Format et style

Aux fins du présent chapitre, le format et le style d'une position nationale englobent sa forme (orale ou écrite), sa longueur (longue ou concise) et d'autres éléments structurels tels que l'utilisation d'exemples ou d'études de cas, de résumés, de titres, de références, de paragraphes numérotés et de supports visuels.

a. Forme orale vs Forme écrite

i. Les déclarations

Le concept de position nationale a vu le jour lorsque le conseiller juridique du département d'État américain, Harold Hongju Koh, a exposé le point de vue de son pays concernant le droit international dans le cyberespace lors d'un discours prononcé à la conférence juridique interinstitutionnelle du Cyber Command en 2012. Ce discours a été publié et est devenu une référence quant à la position des États-Unis sur l'application des différentes règles et principes du droit international aux technologies de l'information et de la communication (TIC).[5] Il a été prononcé dans le contexte de discussions capitales sur ce sujet, lesquelles ont principalement eu lieu au sein du Groupe d'experts gouvernementaux (GEG)[6] des Nations Unies en 2009-2010 et 2012-2013, ainsi que pendant le processus qui a conduit à la publication de la première édition du Manuel de Tallinn en 2013.[7] Dans deux autres discours prononcés en 2016[8] et 2020,[9] les États-Unis ont abordé des sujets ou des domaines plus spécifiques du droit international qui avaient été discutés au sein du GEG en 2014-2015, notamment la souveraineté, le droit international humanitaire (DIH), la non-intervention et le droit international des droits de l'homme (DIDH).[10]

5 Position nationale des États-Unis (2012).

6 Cf. Assemblée générale des Nations Unies, *Report of the* Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/65/201 (30 juillet 2010), par. 14 et 16 ; Assemblée générale des Nations Unies, Developments in the field of information and telecommunications in the context of international security. *Report of the* Secretary-General, A/66/152 (15 juillet 2011), p. 6, 18-19 ; Assemblée générale des Nations Unies, *Report of the* Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98 (24 juin 2013), par. 11, 16 et 19. Cf. également Eneken Tikk-Ringas, Developments in the Field of Information and telecommunication in the context of international security: Work of the UN first Committee 1998-2012, ICT4Peace (2012), p. 9-10 ; Camino Kavanagh, The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century, UNIDIR (2017), p. 16-19.

7 Cf. CCDCOE, Manuel de Tallinn ; Wikipédia, « Manuel de Tallinn ».

8 Position nationale des États-Unis (2016).

9 Position nationale des États-Unis (2020).

10 Assemblée générale des Nations Unies, *Report of the* Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174 (22 juillet 2015), paragraphe 28.

En 2016, Norbert Riedel, commissaire chargé de la politique cyber internationale au Ministère fédéral allemand des Affaires étrangères, a prononcé un discours intitulé « La cybersécurité comme dimension de la politique de sécurité » à Chatham House.[11] Bien que ne portant pas spécifiquement sur le droit international, ce discours abordait brièvement la manière dont, selon l'Allemagne, la souveraineté, l'interdiction du recours à la force et le droit international humanitaire devaient être compris dans le contexte cyber. Ce discours n'a pas été présenté comme la position nationale de l'Allemagne, qui a été publiée sous la forme d'un document écrit distinct en 2021, mais il en a constitué la base.[12]

En 2018, toujours à Chatham House, le Procureur général britannique, Jeremy Wright, a présenté la première position nationale du pays dans un discours intitulé « Cyber and International Law in the 21st Century » (Cyberespace et droit international au XXIe siècle).[13] Cette position a été reprise par le Royaume-Uni en 2022.[14] En 2019, la Présidente Kersti Kaljulaid a dévoilé la première position nationale de l'Estonie dans un discours prononcé lors de l'ouverture de la conférence phare de l'OTAN sur les cyberconflits, « CyCon ».[15] Israël a emboîté le pas en 2020 avec un discours prononcé par son Procureur général adjoint, Roy Schöndorf, à l'US Naval War College. Ce discours a été publié sous forme d'article académique[16] et d'article de blog.[17]

11 Ministère fédéral allemand des Affaires étrangères, « Cyber Security as a Dimension of Security Policy ». Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, à Chatham House, Londres (18 mai 2015).

12 Position nationale de l'Allemagne (2021).

13 Position nationale du Royaume-Uni (2018).

14 Position nationale du Royaume-Uni (2022).

15 Position nationale de l'Estonie (2019), pp. 23-30.

16 Roy Schöndorf, « Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations » (2021) International Law Studies, 97, pp. 395-406.

17 Roy Schöndorf, « Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations », EJIL: Talk! (9 décembre 2020).

La publication d'une position nationale sous la forme d'un discours officiel du gouvernement peut être un moyen efficace d'attirer l'attention des publics cibles et de donner plus de visibilité au document. En général, la prononciation d'un discours officiel revêt un certain caractère solennel, en particulier lorsqu'il est prononcé par un représentant de l'État de premier plan, tel que le Président ou le Procureur de la République. Étant donné qu'un discours gouvernemental peut rassembler différentes parties prenantes, il offre également une bonne occasion de poser des questions et de recueillir des commentaires. Les discours ont tendance à être moins formels et plus concis, accessibles et mémorables, ce qui permet de créer un lien plus étroit avec le public. Ils peuvent ainsi renforcer la portée et l'impact d'une position nationale auprès des différentes parties prenantes. D'un autre côté, leur format moins structuré peut être plus difficile à suivre, en particulier pour les non-juristes. On risque également de susciter l'attente de nouveaux discours ou de discours de suivi sur le droit international dans le cyberespace. Enfin, la nature orale d'un discours limite nécessairement l'étendue et la profondeur de la position nationale : il ne peut aborder qu'un nombre restreint de thèmes ou de questions, et uniquement à un niveau général.

ii. Déclarations de l'ONU

Certains États – le Brésil,[18] la Tchéquie[19] et la Finlande[20] – ont présenté leurs points de vue sur le droit international et les activités cybernétiques dans des déclarations orales avant la deuxième session de fond du Groupe de travail à composition non limitée en 2020. Dans le cas de la Finlande, bien que la déclaration orale n'ait jamais été publiée, elle a été suivie d'une présentation plus longue qui est devenue la position nationale écrite indépendante du pays.[21] Les États disposent d'un temps limité pour lire leurs déclarations pendant les sessions du Groupe de travail à composition non limitée (généralement 3 à 5 minutes). Par conséquent, ces déclarations couvrent un éventail de sujets plus restreint et sont plus concises et générales dans leur style. Cependant, le cadre des Nations Unies exige un ton plus formel que d'autres environnements institutionnels, tels que les conférences ou les universités.

Tout comme les discours, **les déclarations faites aux Nations Unies peuvent constituer un moyen efficace d'attirer l'attention des États membres et des parties prenantes qui assistent ou suivent la session du GTCNL concernée**. Cependant, si les transcriptions ne sont pas publiées et facilement accessibles, il se peut que les personnes qui n'ont pas assisté ou suivi la réunion concernée, y compris d'autres États, ne soient pas informées du contenu des déclarations ou n'y aient pas facilement accès. C'est pourquoi le présent Manuel ne considère pas les déclarations non publiées ou inaccessibles comme des positions nationales.

18 Position nationale du Brésil (2020).

19 Position nationale de la République tchèque (2020).

20 Cf. Marja Lehto, « Finland's views on International Law and Cyberspace » (2023), Nordic Journal of International Law 92(3), 456–469, et Michael Schmitt, « Finland Sets Out Key Positions on International Cyber Law », Just Security (27 octobre 2020).

21 Position nationale de la Finlande (2020).

iii. Documents écrits autonomes

À mesure que de nouveaux domaines ou thèmes du droit international dans le cyberespace étaient abordés dans différents forums, notamment à l'ONU et dans les milieux universitaires, les États ont commencé à envisager de publier leurs positions nationales sous forme de documents écrits distincts. L'Australie a été la première à le faire en 2017, en publiant sa position nationale en annexe de sa stratégie internationale en matière de cyberengagement.[22] Elle a été suivie par la France[23] et les Pays-Bas en 2019.[24] La position nationale de la France a été publiée par son Ministère des armées, tandis que celle des Pays-Bas a fait l'objet d'une lettre adressée à son parlement. L'Iran, la Finlande et la Nouvelle-Zélande ont publié des positions nationales distinctes en 2020.[25]

C'est dans ce contexte marqué par la multiplication des publications de positions nationales que le Groupe d'experts gouvernementaux GEG a invité, en 2019, les États à soumettre « des contributions nationales volontaires sur la question de l'application du droit international à l'utilisation des technologies de l'information et de la communication ».[26] Cette initiative visait à encourager davantage d'États à publier une position nationale écrite consolidant leurs points de vue sur l'application du droit international aux activités cybernétiques dans un document unique. L'objectif était de renforcer la transparence, la prévisibilité et la compréhension mutuelle sur cette question. Quinze États ont répondu à l'appel du GEG et leurs positions ont été publiées dans un recueil officiel du GEG en 2021.[27] Parmi eux figuraient l'Australie, le Brésil, l'Estonie, l'Allemagne, le Japon, le Kazakhstan, le Kenya, les Pays-Bas (qui ont soumis une copie de leur position nationale de 2019), la Norvège, la Roumanie, la Russie, Singapour, la Suisse, le Royaume-Uni et les États-Unis.

Suite à la publication du recueil officiel du GEG, plusieurs autres États ont publié leur position nationale sous la forme d'un document distinct. L'Italie l'a fait en 2021.[28] Et la même année, la France a publié une version anglaise de sa position de 2019.[29] Toujours en 2021, la Chine a publié deux documents de position : un document plus général sur « l'élaboration de règles internationales dans le cyberespace »[30] et un autre sur « l'application du principe de souveraineté dans le cyberespace ».[31] Le

22 Position nationale de l'Australie (2017).

23 Position nationale de la France (2019).

24 Position nationale des Pays-Bas (2019).

25 Positions nationales de l'Iran (2020), de la Finlande (2020) et de la Nouvelle-Zélande (2020).

26 Assemblée générale des Nations Unies, Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing responsible State behaviour in cyberspace in the context of international security, A/RES/73/266 (2 janvier 2019), paragraphe 3.

27 Assemblée générale des Nations Unies, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, A/76/136 (13 juillet 2021).

28 Position nationale de l'Italie (2021).

29 Position nationale de la France (version anglaise) (2021).

30 Position nationale de la Chine (généralités) (2021).

31 Position nationale de la Chine (souveraineté) (2021).

Canada, la Pologne et la Suède ont publié leurs positions nationales en 2022 ;[32] le Costa Rica, le Danemark, l'Irlande et le Pakistan en 2023 ;[33] l'Autriche, Cuba et la République tchèque en 2024 ;[34] et la Colombie en 2025.[35] L'UA et l'UE ont publié des positions communes en 2024.[36]

Les documents écrits autonomes ont pris une place de choix dans la publication des positions nationales. Ils permettent une plus grande couverture et un plus grand niveau de détail, ils sont donc tout indiqués pour les États qui souhaitent publier des positions plus complètes et plus influentes. Le processus de publication d'une position écrite autonome est généralement plus formel que celui de la publication de discours, de déclarations ou d'articles académiques. On s'attend également à ce que les positions écrites autonomes fassent référence en matière de droit international dans le cyberespace, ce qui signifie que les enjeux sont généralement plus importants avec ce format. Par conséquent, la rédaction d'une position écrite autonome peut prendre plus de temps et impliquer davantage d'acteurs gouvernementaux que la rédaction d'un discours, d'une déclaration ou d'un article académique. D'une part, la position nationale est ainsi plus affinée et plus représentative. D'autre part, les documents peuvent devenir plus complexes, et donc moins accessibles à un public non spécialisé.

iv. Articles académiques

Comme évoqué plus haut, la position nationale des États-Unis de 2016 a d'abord été présentée sous forme de discours, puis publiée l'année suivante en tant qu'article académique dans le Berkeley Journal of International Law.[37] Israël a procédé de la même manière, en publiant en 2021 le discours prononcé par son Procureur général adjoint sous la forme d'un article académique dans International Law Studies.[38] En 2023, le Nordic Journal of International Law a publié un numéro spécial qui regroupait les positions nationales déjà publiées de la Finlande, de la Norvège et de la Suède, tout en dévoilant la position nationale du Danemark, chacune étant accompagnée d'une introduction rédigée par les conseillers juridiques responsables.[39]

32 Positions nationales du Canada (2022), de la Pologne (2022) et de la Suède (2022).

33 Positions nationales du Costa Rica (2023), du Danemark (2023), de l'Irlande (2023) et du Pakistan (2023).

34 Positions nationales de l'Autriche (2024), de Cuba (2024) et de la République tchèque (2024).

35 Position nationale de la Colombie (2025).

36 Positions communes de l'UA (2024) et de l'UE (2024).

37 Brian J. Egan, « International Law and Stability in Cyberspace » (2017) 35 Berkeley Journal of International Law 35, 169-180.

38 Roy Schöndorf, « Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations » (2021) International Law Studies, 97, 395-406.

39 Jeppe Mejer Kjelgaard et Ulf Melgaard, « Denmark's Position Paper on the Application of International Law in Cyberspace » (2023) Nordic Journal of International Law, 92(3), p. 446-455 ; Marja Lehto, « Finland's views on International Law and Cyberspace » (2023) Nordic Journal of International Law, 92(3), p. 456-469 ; Vibeke Musæus, « Norway's Position Paper on International Law and Cyberspace » (2023) Nordic Journal of International Law, 92(3), p. 470-488 ; Ola Engdahl, « Sweden's Position Paper on the Application of International Law in Cyberspace » (2023) Nordic Journal of International Law, 92(3), p. 489-497.

La publication de positions nationales sous forme d'articles académiques peut apporter rigueur et autorité juridique à la publication, compte tenu des normes élevées de révision par les pairs et/ou de révision éditoriale auxquelles les articles universitaires sont généralement soumis. Les articles universitaires constituent également un moyen efficace d'atteindre et d'influencer un public juridique spécialisé, en particulier les académiques. En revanche, ils sont parfois difficilement accessibles aux non-spécialistes, en raison du langage complexe généralement utilisé dans les articles universitaires et du fait que peu de non-spécialistes connaissent l'existence des publications académiques.

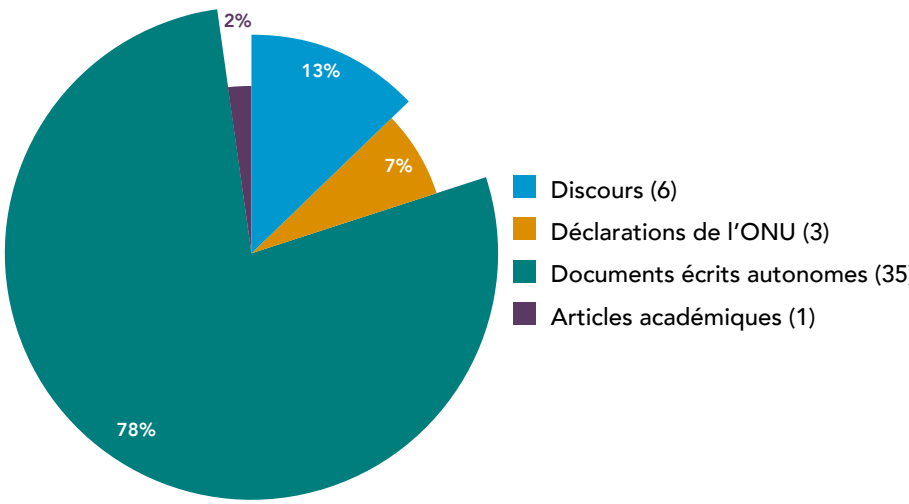
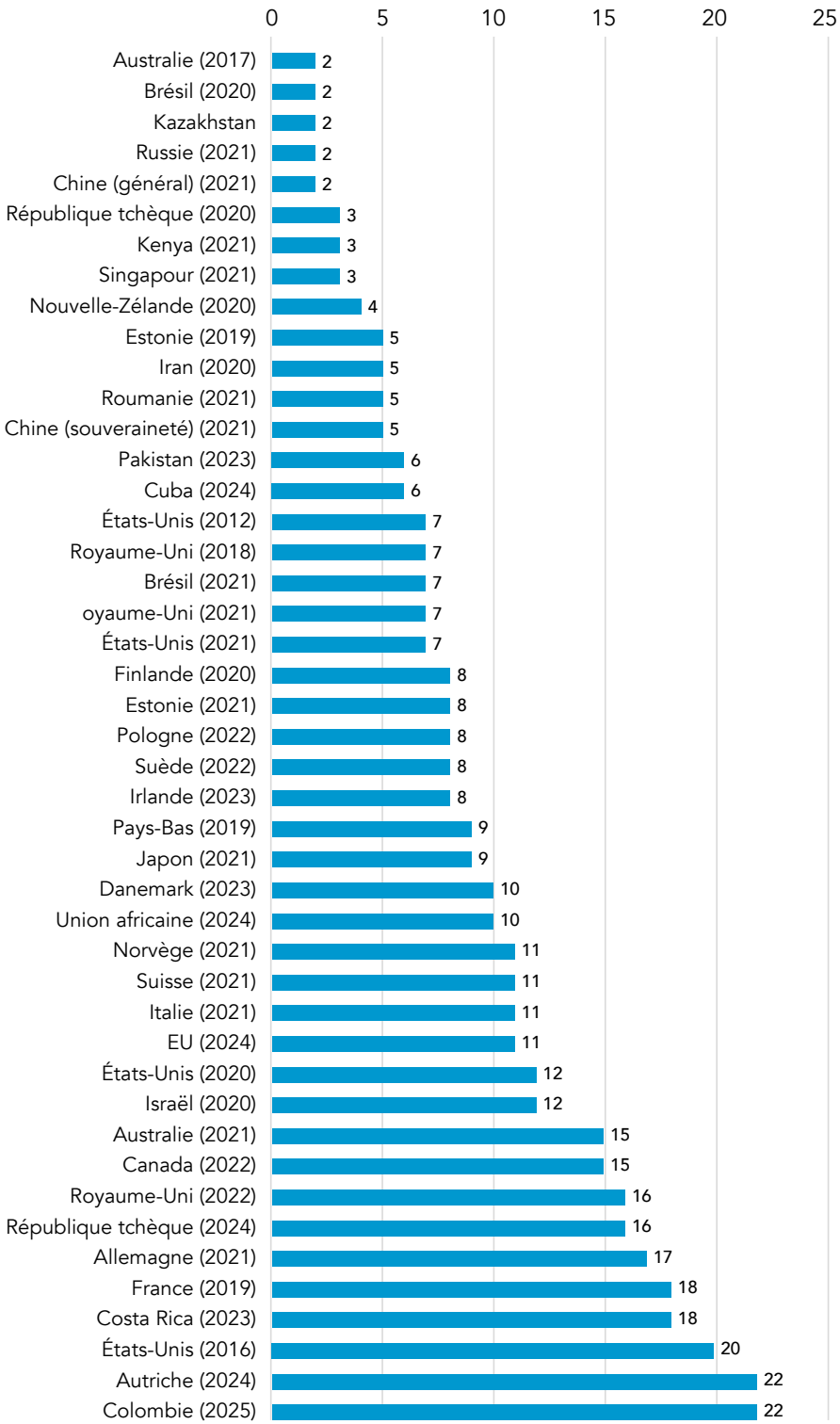


Figure 9 : Proportion des positions nationales et communes exprimées oralement par rapport à celles exprimées par écrit.

b. Longueur

La longueur des positions nationales publiées à ce jour varie de manière significative : les plus courtes font deux pages (par exemple, Australie (2017), Kenya, Kazakhstan et Russie), tandis que les plus longues s'étendent sur 22 pages (Autriche et Colombie). Cependant, comme l'indique le graphique ci-dessous, on constate une préférence pour les documents détaillés plus longs, d'une moyenne de neuf pages, dont la plupart ont été initialement publiés sous forme écrite.

Figure 10 : Positions nationales et communes selon le volume (en nombre de pages).



Le fait que les documents plus longs soient privilégiés s'explique par l'étendue et la rigueur de l'analyse que permet le format autonome. Par exemple, les positions nationales de l'Autriche et du Costa Rica (respectivement 22 et 18 pages) ont reçu un accueil favorable parmi les académiques, certains saluant leur sophistication, leur détail, leur ampleur et leurs nuances.[40] Comme indiqué au **chapitre 4**, un grand nombre de règles, de principes et de régimes peuvent s'appliquer au cyberespace, et chacun soulève des questions complexes d'interprétation juridique et de mise en œuvre. Par conséquent, l'étendue et la rigueur de l'analyse sont particulièrement importantes si la position nationale vise à développer ou à clarifier le droit international existant tel qu'il s'applique dans le contexte cybernétique ou à influencer la recherche académique. L'étendue et la rigueur favorisent également une plus grande transparence et une meilleure responsabilité. Dans le même temps, un niveau de détail trop élevé et un formalisme ou un jargon juridique excessifs peuvent nuire à la clarté et à l'accessibilité d'une position nationale, en particulier pour un public non juriste.That is not to say that concise national positions have less value.

Toutefois, cela ne signifie pas pour autant que les positions nationales concises ont moins de valeur. Elles peuvent être utiles si un État souhaite se concentrer sur quelques domaines ou thèmes clés du droit international tels qu'ils s'appliquent dans le contexte cybernétique.[41] Les positions nationales concises sont également appropriées si l'objectif visé consiste simplement à reconnaître l'applicabilité générale du droit international et/ou de certaines règles, principes ou régimes dans le cyberespace, sans entrer dans les détails ou les complexités de leur application dans ce contexte.[42] De même, si l'objectif de la position nationale est de signaler des zones d'incertitude ou des lacunes, un document concis pourrait être plus approprié. Les déclarations politiques portant sur des questions telles que la situation en matière de cybermenaces, le renforcement des capacités ou l'instauration de la confiance ne nécessitent pas non plus le même niveau de détail que les analyses juridiques et peuvent être présentées de manière plus concise et informelle.[43] Par conséquent, des positions concises peuvent être utiles pour mener des discussions diplomatiques de haut niveau sur des questions politiques plus larges concernant l'applicabilité du droit international dans le contexte cybernétique. Dans le même ordre d'idées, les praticiens ont tendance à préférer les documents courts, étant donné le temps limité dont ils disposent pour étudier en détail les positions nationales. Par exemple, lors des tables rondes organisées dans le cadre du projet, le format concis de la position nationale de la Nouvelle-Zélande (quatre pages) a été salué par un représentant de l'État comme étant « élégant » et un modèle à suivre.[44] Un format concis est également approprié si l'objectif d'une position nationale se résume à informer un public plus large de non-spécialistes du droit international, notamment les décideurs politiques, les acteurs industriels et la société civile.

40 Cf. Chris Carpenter et Duncan B. Hollis, « A Victim's Perspective on International Law in Cyberspace », Lawfare (28 août 2023) ; Przemysław Roguski, « Austria's Progressive Stance on Cyber Operations and International Law », Just Security (25 juin 2024).

41 Cf. par exemple la position nationale de l'Estonie (2019).

42 Cf. par exemple les positions nationales du Brésil (2020), de la Chine (2021) (général), du Kenya (2021).

43 Cf. par exemple les positions nationales de la Chine (2021) (général) et de la Russie (2021).

44 Observation faite lors de la table ronde organisée dans le cadre du projet sur les perspectives de l'Amérique latine et des Caraïbes (rapport disponible auprès des auteurs).

c. Scénarios et exemples

Plusieurs positions nationales font référence à des exemples d'opérations cybermalveillantes pour illustrer des violations potentielles ou souligner l'importance du droit international dans le contexte cybernétique. Il peut s'agir d'exemples portant sur des opérations cybermalveillantes générales (telles que le cyberespionnage, les interférences électorales, la désinformation et le ransomware)[45] ou sur des incidents réels (par exemple, la cyberattaque NotPetya).[46] Deux positions nationales vont plus loin et incluent des scénarios hypothétiques plus détaillés d'opérations cybernétiques susceptibles de violer le droit international.[47] Le fait d'inclure des exemples ou des scénarios permet d'améliorer la clarté et la précision. Ils peuvent notamment éclairer les conséquences juridiques ou les implications de l'adoption d'une certaine interprétation ou de la promotion d'une nouvelle règle de droit international dans le contexte cybernétique. Ils permettent également de garantir que les positions nationales sont pertinentes et pratiques dans le contexte cybernétique et ne constituent pas de simples reformulations abstraites du droit international. En particulier, des exemples d'incidents cybernétiques réels peuvent planter le décor et expliquer les motivations qui ont conduit à l'adoption d'une position nationale. Les exemples ou les scénarios sont également essentiels si un État décide de suivre l'approche inductive dans sa position, c'est-à-dire en partant de certains faits pour ensuite expliquer comment le droit s'applique à ceux-ci.

45 45 Cf. par exemple les positions nationales du Costa Rica (2023), du Royaume-Uni (2022) et des États-Unis (2016).

46 46 Cf. par exemple les positions nationales du Royaume-Uni (2018 et 2022).

47 47 Cf. par exemple les positions nationales de l'Australie (2021) et de l'Autriche (2024).

d. Références

La plupart des positions nationales publiées à ce jour font référence à des décisions rendues par des cours et tribunaux internationaux, à des traités, à des documents des Nations Unies (en particulier les travaux de la Commission du droit international) et à des sources académiques (notamment les manuels de Tallinn). Ces références prennent la forme de notes de bas de page,[48] de notes de fin,[49] et/ou d'une bibliographie.[50] **Les références peuvent conférer une plus grande autorité juridique à une position nationale, la rendant plus convaincante pour différents publics, y compris d'autres États et des académiques**. Cependant, un nombre excessif de références peut rendre un document visuellement peu attrayant et difficile à lire, en particulier si les références sont présentées sous forme de notes de bas de page. Par conséquent, pour être efficace, le référencement doit trouver un équilibre entre l'autorité juridique et l'accessibilité. Les hyperliens vers les documents cités dans les notes de bas de page peuvent également améliorer l'accessibilité en permettant aux lecteurs de trouver plus facilement les documents pertinents. Pour les positions nationales plus concises et informelles, telles que celles publiées sous forme de déclarations ou de discours de l'ONU, puis publiées sous forme d'articles de blog, il est possible d'inclure des hyperliens vers les ouvrages référencés dans le corps du texte plutôt que d'énumérer les citations complètes dans les notes de bas de page.

e. Titres, résumés et paragraphes numérotés

La grande majorité des positions nationales publiées présentent des titres. Ils permettent de structurer une position autour de domaines, de thèmes ou de questions clairs relevant du droit international dans le contexte cybernétique, généralement du plus général au plus spécifique. **Cette méthode améliore considérablement la clarté et la lisibilité d'une position nationale.**

Les résumés sont également importants pour la clarté et l'accessibilité, notamment pour les documents plus longs, car ils permettent de mettre en évidence les messages clés véhiculés dans la position nationale. Les résumés sont particulièrement utiles pour les praticiens, notamment les juristes et les diplomates gouvernementaux, qui disposent de peu de temps pour lire les positions dans leur intégralité. Néanmoins, seules six positions nationales publiées à ce jour contiennent des résumés (Australie (2017), Autriche, Estonie (2021), France, Norvège et Pologne). Dans les positions nationales de l'Autriche, de l'Estonie (2021), de la France et de la Norvège, les résumés sont présentés dans des encadrés, pour une meilleure lisibilité. Dans les positions nationales de l'Australie (2017) et de la Pologne, les résumés se présentent sous la forme de titres accompagnés de phrases courtes qui résument les principaux points à retenir des sections concernées. Cela permet au lecteur d'identifier rapidement les questions abordées dans la position et les principales conclusions retenues.

48 Cf. par exemple les positions nationales de l'Autriche (2024), du Costa Rica (2023), de Cuba (2024), de la République tchèque (2024) et de l'Irlande (2023).

49 Cf. par exemple les positions nationales du Canada (2022) et de la Colombie (2025).

50 Cf. par exemple la position nationale de la Colombie (2025).

Les paragraphes numérotés sont également utiles pour faire référence à des points spécifiques soulevés dans le document, permettant ainsi à d'autres de citer facilement la position. Il convient d'en tenir compte si l'objectif d'une position consiste à influencer le public, en particulier d'autres États et des académiques. Cependant, seules quelques positions nationales et une position commune publiées à ce jour contiennent des paragraphes numérotés.[51]

f. Supports visuels

Certaines positions nationales ont été intégrées dans des documents spécialement conçus à cet effet, comme ceux de l'Australie (2017 et 2021), de la Colombie, de la France (2019) et de la Nouvelle-Zélande. Cependant, aucun d'entre eux ne comporte de supports visuels tels que des tableaux, des graphiques ou des infographies. Ces ressources ont été utilisées avec succès dans d'autres documents sur la cyberpolitique, tels que la stratégie internationale de cyberengagement de l'Australie (qui, comme indiqué, contient en annexe sa position nationale de 2017)[52] et les explications[53] sur les 11 normes du GEG relatives au comportement responsable des États[54]. **Les supports visuels pourraient être intégrés afin d'améliorer l'accessibilité des positions nationales**, que ce soit dans le même document ou dans des stratégies de diffusion distinctes, comme indiqué ci-dessous.

51 Positions nationales du Canada (2022), du Costa Rica (2023), de Cuba (2024), de la République tchèque (2024), de l'Irlande (2023), de la Nouvelle-Zélande (2020), du Pakistan (2023) et du Royaume-Uni (2021), ainsi que la position commune de l'UA (2024).

52 Commonwealth d'Australie, Ministère des Affaires étrangères et du Commerce, Australia's International Cyber Engagement Strategy (octobre 2017), p. 8-9, 16, 85.

53 Cf. par exemple, Institut australien de politique stratégique, Centre international de politique cybernétique, The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN (mars 2022).

54 Assemblée générale des Nations Unies, *Report of the* Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/70/174 (22 juillet 2015), paragraphe 13.

3. La langue

Aux fins du présent chapitre, le terme « langue » désigne l'utilisation de la terminologie juridique et la ou les langues réelles de publication.

a. Terminologie juridique

Toutes les positions nationales publiées à ce jour ont utilisé le lexique traditionnel du droit international dans leur analyse des règles, principes et régimes internationaux tels qu'ils s'appliquent dans le contexte cybernétique. Cela est essentiel si l'objectif d'une position est de développer ou de clarifier la manière dont le droit international s'applique dans le contexte cybernétique. Cependant, les **États doivent faire preuve de précision et de cohérence lorsqu'ils utilisent des termes juridiques** tels que « souveraineté », « compétence », « attaque » et « contrainte ». Ces termes, parmi d'autres, ont non seulement une signification particulière en droit international, mais font également l'objet d'un débat important. Il est donc essentiel de préciser dans une position nationale ce qu'un État entend par ces termes. Il convient non seulement de fournir une définition juridique, mais aussi de situer chaque concept dans le cadre des débats existants et d'indiquer, le cas échéant, la position défendue par l'État sur la question.

Par exemple, lorsqu'un État aborde la question de la souveraineté dans le cadre de ses activités cybernétiques, il est utile de préciser s'il fait référence au débat entre la souveraineté en tant que principe et la souveraineté en tant que règle,[55] ou aux corollaires de la souveraineté étatique, tels que la compétence et la non-intervention.[56] De même, si l'objectif d'une position nationale est de prendre position sur ces débats, il est important d'indiquer clairement quelle est cette position. À l'inverse, si un État ne souhaite pas prendre position de manière ferme sur un débat donné, soit parce qu'il n'a pas encore pris de décision, soit parce que les preuves ne sont pas concluantes, il doit le dire clairement.

Des mots clés ont été utilisés pour communiquer ces intentions. Par exemple, lorsqu'une position nationale affirme qu'un État « doit », « est tenu » ou « est obligé » de faire ou de s'abstenir de faire quelque chose, elle exprime l'opinion que le comportement en question est fondé sur une obligation juridique contraignante. On peut aussi exprimer le caractère obligatoire d'une règle en droit international en disant qu'elle constitue la lex lata (c'est-à-dire la loi en vigueur). À l'inverse, l'utilisation de termes tels que « devrait », « peut » ou « pourrait » implique que l'État ne considère pas le comportement en question comme requis en vertu du droit international.[57] De même, un État peut affirmer qu'une déclaration est lex ferenda (c'est-à-dire ce que la loi devrait être) ou constitue une « norme non obligatoire » s'il ne la considère pas comme obligatoire en vertu du droit international. De même, si un État estime que le droit international ne régit pas encore un certain

55 Cf. par exemple les positions nationales de l'Autriche (2024), pp. 4-5, et du Royaume-Uni (2018), p. 7.

56 Cf. par exemple la position nationale de l'Chine (2021) (souveraineté), p. 2.

57 Cf. par exemple, les positions nationales du Canada (2022), paragraphe 26, et de la Nouvelle-Zélande (2020), paragraphe 16.

comportement, il peut affirmer qu'il n'existe pas suffisamment de preuves de la pratique des États et/ou de *l'opinio juris*[58], qu'une « plus grande » pratique des États et/ou opinio juris est nécessaire[59], ou qu'il n'est « pas convaincu » que la règle en question se soit « cristallisée ».[60] En revanche, si un État considère que les preuves existantes de la pratique des États et/ou de *l'opinio juris* sont incertaines ou non concluantes pour permettre une affirmation définitive du droit, il pourra indiquer que la question requiert des études ou une « réflexion » complémentaires.[61]

Le choix des termes peut également refléter le statut juridique d'une position nationale : celle-ci peut être adoptée en tant que pratique étatique et/ou *opinio juris*, comme aide à l'interprétation ou comme déclaration politique.

Il est également possible que le statut d'une position nationale varie en fonction des questions ou des thèmes abordés. Par exemple, l'Estonie exprimait probablement son opinio juris aux fins de développer le droit international coutumier en matière de contre-mesures collectives en déclarant qu'elle « faisait avancer [sa] position » sur la question.[62] En revanche, la Norvège a clairement indiqué dès le début de sa position nationale qu'elle présentait son « interprétation de certaines obligations du droit international applicables aux opérations cybernétiques ».[63] Lorsqu'un État utilise un langage exhortatif, par exemple en affirment que les États « devraient » se comporter d'une certaine manière, il s'agit probablement d'une simple déclaration politique. Des déclarations de ce type figurent, par exemple, dans les positions nationales du Canada, de la Chine et de la Nouvelle-Zélande.[64]

Comme indiqué au **chapitre 2**, les positions nationales ont également utilisé une **terminologie distincte pour promouvoir différentes politiques juridiques** en matière de cybersécurité, notamment pour confirmer que le droit international existant est suffisant pour réglementer les activités cybernétiques ou pour affirmer qu'un nouvel instrument juridiquement contraignant est nécessaire à cet effet.[65] Par exemple, la position nationale de l'Autriche affirme que « le droit international s'applique dans son intégralité aux activités cybernétiques » et que l'Autriche « ne voit pas la nécessité d'élaborer un nouvel instrument juridiquement contraignant

58 Cf. par exemple les positions nationales d'Israël (2021), p. 404, et du Royaume-Uni (2021), paragraphe 12.

59 Cf. par exemple la position nationale du Canada (2022), paragraphe 25.

60 Cf. par exemple la position nationale de la Nouvelle-Zélande (2020), paragraphe 17.

61 Cf. par exemple la position nationale du Brésil (2021), p. 23.

62 Position nationale de l'Estonie (2019).

63 Position nationale de la Norvège (2021), p. 2.

64 Voir, par exemple, les positions nationales du Canada (2022), par. 26 (« aucun État ne devrait sciemment permettre que son territoire soit utilisé pour des actes contraires aux droits d'autres États »), de la Chine (2021) (général) (par exemple : « iii. Les États devraient renforcer la protection des infrastructures vitales des TIC »), et de la Nouvelle-Zélande (2020), par. 16 (« les États ne devraient pas sciemment permettre que leur territoire soit utilisé pour commettre des actes internationalement illicites au moyen des TIC »).

65 Cf. par exemple, les positions nationales de la Chine (2021) (souveraineté), p. 1, de Cuba (2024), paragraphes 4-5, du Pakistan (2023), paragraphe 8, et de la Russie (2021), p. 80.

relatif aux activités cybernétiques internationales »[66]. De même, la position commune de l'UE soutient que le droit international « s'applique pleinement au cyberespace » et « est adapté à l'ère numérique ».[67] À l'inverse, la position nationale de la Chine déclare que « la communauté internationale devrait élaborer des normes, des règles et des principes universellement acceptés dans le cadre des Nations Unies, afin de relever conjointement les risques et les défis et de préserver la paix, la sécurité et la prospérité dans le cyberespace ».[68] Dans le même ordre d'idées, la position nationale de la Russie « préconise une conception plus large du développement et de l'amélioration progressifs du droit international, tenant compte des caractéristiques spécifiques des TIC », en « adoptant une convention universelle obligatoire sur la sécurité internationale de l'information au niveau des Nations Unies ».[69]

b. Langue de publication et de traduction

ont été publiées en anglais. L'anglais est la langue couramment utilisée dans les milieux juridiques, diplomatiques et académiques concernés, notamment au sein du GEG et du GTCNL, ainsi que dans le cadre des processus de Tallinn et d'Oxford. Afin de garantir que les positions soient conformes au lexique juridique international existant, clairement comprises par la majorité des parties prenantes et favorisent une compréhension commune entre les États, il est important de les publier en anglais. Par exemple, en anglais, le terme « norme » est désormais compris comme une attente ou une norme de comportement non obligatoire, telle que les normes du GEG relatives au comportement responsable des États dans le cyberespace. Cependant, le terme équivalent dans d'autres langues, comme le français (norme) ou l'italien, le portugais et l'espagnol (norma), peut également désigner une règle obligatoire. Il en va de même pour les concepts en informatique et dans d'autres domaines techniques, qui ont une terminologie anglaise établie. **Par conséquent, l'utilisation de l'anglais dans les positions nationales peut garantir la clarté et la précision et éviter les malentendus, en particulier lorsqu'il s'agit de termes juridiques et techniques.**

Quelques États ont choisi de publier leur position nationale dans d'autres langues. C'est le cas des États dont la langue officielle n'est pas l'anglais. Citons par exemple les positions nationales de la France (publiée en français en 2019 et traduite en anglais en 2021),[70] de la Finlande (publiée en finnois et en anglais en 2020),[71] du Kazakhstan (publiée uniquement en russe dans le recueil officiel du GEG en 2021), de la Suisse (publiée en anglais et en français dans le recueil officiel du GEG en 2021), de la Russie (publiée en anglais et en russe dans le recueil officiel du GEG en 2021), de Cuba (publiée en espagnol en 2024) et de la Colombie (publiée en anglais et en espagnol en 2025). Le Canada a publié sa position nationale en 2022

66 Position nationale de l'Autriche (2024), p. 3. Cf. également, par exemple, la position nationale du Costa Rica (2023), paragraphe 7.

67 Position commune de l'UE (2024), pp. 3-4.

68 Position nationale de la Chine (2021) (généralités), p. 1.

69 Position nationale de la Russie (2021), p. 80.

70 Position nationale de la France (2021).

71 Cf. les versions finnoise et anglaise de la position nationale de la Finlande (2020).

dans ses deux langues officielles : l'anglais et le français.[72] Le Royaume-Uni a publié sa position nationale de 2021 dans le recueil officiel du GEG dans toutes les langues officielles de l'ONU : l'arabe, le chinois, l'anglais, le français, le russe et l'espagnol.

La publication d'une position nationale dans des langues autres que l'anglais présente plusieurs avantages. Tout d'abord, elle permet de rendre cette position plus accessible à un public non anglophone, tant au niveau national qu'international. Bien que l'anglais soit la langue la plus parlée au monde, la grande majorité de la population vivant dans les pays du Sud ne parle pas anglais : à l'heure actuelle, environ 13% de la population mondiale parle anglais et seulement 5% sont de langue maternelle anglaise.[73] Le mandarin, l'hindi, l'espagnol, le français et l'arabe sont les langues les plus parlées après l'anglais.[74] Par conséquent, la publication d'un document national dans une ou plusieurs de ces langues peut renforcer l'inclusivité, combler les lacunes en matière de connaissances et réduire la fracture numérique. Deuxièmement, comme l'ont souligné plusieurs représentants d'États lors des tables rondes organisées dans le cadre du projet, la publication d'une position nationale dans une ou plusieurs langues autres que l'anglais peut garantir que les parties prenantes nationales, y compris au sein du gouvernement et de la société civile, non seulement comprennent la position nationale, mais s'approprient également le processus et ses résultats.[75] De même, si une position nationale est élaborée au niveau national ou régional dans une langue autre que l'anglais, la publication de cette position dans cette langue permet de garantir la cohérence de la terminologie juridique et de la signification. À cet égard, chaque langue, région et/ou pays possède ses propres traditions et expressions juridiques et culturelles. Par conséquent, la publication d'une position nationale dans une langue locale permet de tenir compte de ces traditions et expressions, garantissant ainsi que la position est conforme et adaptée au contexte local. Enfin, la publication d'une position nationale en plusieurs langues, comme l'a fait le Royaume-Uni en 2021, permet de contrôler les traductions officielles et donc de garantir la cohérence de leur interprétation.

72 Position nationale du Canada (2022) (versions anglaise et française).

73 Encyclopaedia Britannica, « Languages by total number of speakers » ; Dylan Lyons, « How Many People Speak English, And Where Is It Spoken? », Babbel (10 mars 2021) ; Encore, « What Is the Most Spoken Language in the World. »

74 Cf. Encyclopaedia Britannica, « Languages by total number of speakers » ; Wikipedia, « List of languages by total number of speakers » ; Statista, « The most spoken languages worldwide in 2023. »

75 Observations faites lors des tables rondes organisées dans le cadre du projet sur les perspectives en Asie-Pacifique et en Amérique latine et dans les Caraïbes (rapports conservés par les auteurs).

Cependant, certaines considérations doivent être prises en compte lorsqu'il s'agit de décider si une position doit être publiée ou traduite dans des langues autres que l'anglais. Comme indiqué ci-dessus, certains termes juridiques et techniques peuvent avoir une signification différente ou tout simplement ne pas exister dans d'autres langues. Par exemple, le concept de « souveraineté en tant que règle » est difficile à traduire en français, ce qui peut prêter à confusion.[76] Par conséquent, il est recommandé de publier au moins une version en anglais de la position nationale si celle-ci vise à développer ou à clarifier le droit international tel qu'il s'applique dans le contexte cybernétique. En outre, que la position nationale soit initialement publiée en anglais ou dans une autre langue, **il est essentiel de veiller à ce que toute traduction soit précise et cohérente**.

76 Cf. Aude Géry, « Navigating France's Views on Sovereignty in Cyberspace : Why Might France Not Be in the "Sovereignty-As-A-Rule" and in the "Pure Sovereignty" Camps », EJIL: Talk! (19 septembre 2024).

4. Diffusion

Les positions nationales sont des documents officiels à caractère juridique ou politique. À ce titre, elles sont publiées et diffusées par les **voies officielles gouvernementales et diplomatiques**. Comme indiqué au **chapitre 3**, ces canaux comprennent les journaux officiels et les communiqués de presse[77], les sites web gouvernementaux[78] et les référentiels en ligne nationaux ou internationaux, tels que la bibliothèque numérique des Nations Unies (pour les positions nationales figurant dans le recueil officiel du GEG)[79] et la base de données documentaire du GTCNL[80] (où de nombreuses positions nationales autonomes ont été publiées). La publication des positions nationales par le biais de ces canaux renforce leur autorité et garantit que les acteurs juridiques et diplomatiques qui connaissent bien ces canaux puissent facilement les trouver. **Il est particulièrement utile de publier les positions nationales dans la base de données documentaire du GTCNL**, dans la mesure où il s'agit d'une plateforme bien connue pour les documents officiels relatifs à ses discussions sur les implications des TIC pour la paix et la sécurité. Ainsi, les gouvernements, mais également les autres parties prenantes qui suivent les travaux du Groupe de travail à composition non limitée (telles que l'industrie, la société civile et le monde universitaire) peuvent avoir accès aux positions nationales.

Comme indiqué ci-dessus, certaines positions nationales ont été publiées sous forme **d'articles académiques**. Dans le cas du Danemark, la position nationale a été publiée exclusivement sous forme d'article académique. Dans d'autres cas, l'article se présente sous la forme d'une transcription d'un discours officiel (par exemple, Israël et États-Unis (2016)) ou d'une réédition d'un document de synthèse autonome (par exemple, Finlande, Norvège et Suède). Cette stratégie de diffusion peut être appropriée pour cibler un public académique. Toutefois, comme indiqué précédemment, il est possible que les articles académiques soient difficilement accessibles à d'autres publics, soit en raison de leur format et de leur style, soit en raison de leur portée, car les non-spécialistes peuvent ne pas être familiers avec les publications académiques.

Le fait de publier une position nationale, ou une version de celle-ci, sur un **blog** permet également d'élargir son audience auprès d'un public non spécialisé. Par exemple, la position d'Israël a initialement été présentée sous la forme d'un discours qui a également été publié sur le blog *EJIL: Talk*![81]. Cela a permis d'accroître la visibilité de cette position auprès des juristes internationaux et des non-spécialistes qui suivent ce blog.

77 Cf. par exemple, Conseil de l'UE, « Cyberspace : Council approves declaration on a common understanding of application of international law to cyberspace » (18 novembre 2024).

78 Cf. par exemple les positions nationales du Canada (2022), de la France (2019), des Pays-Bas (2019) et du Royaume-Uni (2018, 2021 et 2022).

79 Bibliothèque numérique de l'ONU.

80 UNODA, Open-Ended Working Group on Information and Communication Technologies, Documents.

81 Roy Schöndorf, « Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations », EJIL: Talk! (9 décembre 2020).

Un commentaire sur la position commune de l'UA, rédigé par son principal auteur (Mohamed Helal, rapporteur spécial de l'UA sur le droit international dans le cyberespace), a été publié sur le même blog.[82] Cette publication comprenait des remarques sur les thèmes abordés par la position commune ainsi que sur le processus qui a conduit à son adoption par l'UA. Elle a non seulement accru la visibilité de la position commune, mais également suscité un plus grand intérêt à son égard. Les articles de blog peuvent être particulièrement utiles pour expliquer une position nationale à des non-spécialistes, surtout s'ils sont rédigés dans un langage plus accessible, sans jargon juridique ou technique.

Qu'elles soient publiées sous forme de discours, de déclaration à l'ONU, de document écrit autonome ou d'article académique, **la grande majorité des positions nationales publiées à ce jour sont disponibles en ligne**. Comme indiqué ci-dessus, celles-ci sont disponibles sur les sites web des gouvernements, dans les versions en ligne des revues académiques et dans la base de données de documents du GTCNL.[83] Des bases de données non officielles ont également republié les positions nationales en ligne. Le *Cyber Law Toolkit*[84] est l'une des plus populaires, avec des positions nationales classées par pays et par thème dans un format accessible. Le portail sur la cyberpolitique de l'Institut des Nations Unies pour la recherche sur le désarmement présente également les positions nationales par pays, à l'aide d'une carte du monde interactive.[85]

La publication en ligne des positions nationales est importante pour plusieurs raisons. Premièrement, les publics cibles — qu'ils appartiennent au gouvernement, à l'industrie ou à la société civile — sont dispersés à travers le monde et beaucoup d'entre eux ne peuvent pas assister aux réunions ou aux événements au cours desquels les positions nationales sont annoncées, lues ou discutées. Deuxièmement, les habitudes de consultation en ligne se développent dans toutes les catégories démographiques. Troisièmement, la publication en ligne des positions nationales est plus efficace, notamment en termes de temps et de coût, et plus respectueuse de l'environnement. Quatrièmement, les formats numériques facilitent les recherches par mot-clé et les traductions automatiques, ce qui permet au public d'accéder plus facilement aux positions nationales dans différentes langues. En résumé, la publication en ligne d'une position nationale garantit qu'elle peut être consultée facilement et rapidement par toutes les parties prenantes concernées, où qu'elles se trouvent.

82 Mohamed Helal, « The Common African Position on the Application of International Law in Cyberspace : Reflections on a Collaborative Lawmaking Process », EJIL: Talk!, 5 février 2024.

83 UNODA, Open-Ended Working Group on Information and Communication Technologies, Documents.

84 Consultez le site https://cyberlaw.ccdcoe.org

85 Cf. UNIDIR, Cyber Policy Portal.

Dans le même ordre d'idées, le recours aux **réseaux sociaux** pour annoncer la publication d'une position nationale et/ou la commenter peut constituer une stratégie de diffusion efficace auprès d'un public composé d'experts et de non-experts.[86] De nombreux diplomates, juristes gouvernementaux, représentants de l'industrie et académiques sont inscrits sur les réseaux sociaux et suivent l'évolution de la politique cybernétique ou du droit international dans le cyberespace par le biais de leurs réseaux sociaux. De même, le public est largement présent sur les réseaux sociaux. Ils sont donc plus susceptibles de consulter et de réagir à la publication d'une position nationale si celle-ci est annoncée dans un message sur les réseaux sociaux. Les publications sur les réseaux sociaux peuvent également être utilisées pour faire connaître une position nationale publiée en anglais à un public non anglophone et vice-versa, en particulier s'il n'est pas possible d'organiser une traduction officielle de la position elle-même dans d'autres langues. Les vidéos explicatives publiées sur les réseaux sociaux et d'autres plateformes en ligne peuvent également contribuer à faire connaître les positions nationales et à les rendre plus accessibles à différents publics, en particulier aux non-spécialistes.

Il existe une autre stratégie de diffusion visant à accroître la visibilité et l'impact d'une position nationale : organiser des **événements publics et/ou privés** afin de faire connaître le document et/ou d'en discuter le contenu avec différentes parties prenantes. Comme indiqué ci-dessus, cela peut se faire lorsque la position nationale est présentée sous forme de discours lors de conférences ou d'événements spéciaux, comme dans le cas des positions nationales de l'Estonie (2019), d'Israël, du Royaume-Uni (2018 et 2022) et des États-Unis (2012, 2016 et 2020). En outre, les événements parallèles organisés en marge des réunions du Groupe de travail à composition non limitée et de son futur mécanisme permanent à New York peuvent constituer une excellente occasion d'annoncer et de faire connaître la position nationale. Par exemple, en mars 2024, un événement parallèle au Groupe de travail à composition non limitée a été organisé afin de diffuser la position commune de l'UA auprès des audiences de l'ONU et africaines, qui ont pu participer à l'événement en ligne. Des échanges nationaux ou régionaux et des conférences académiques peuvent également être organisés afin de sensibiliser les publics locaux à la publication d'une position nationale. Par exemple, la position nationale de l'Italie a été discutée lors d'une conférence à l'université de Bologne en novembre 2021.[87] Ces événements sont particulièrement utiles s'ils offrent aux publics locaux l'occasion de discuter, dans les langues locales, d'une position nationale qui n'a été publiée qu'en anglais.

86 Par exemple : Bert Theuermann, X Post, 31 mai 2024 ; République de Pologne (« Rzecznik MSZ »), X Post, 29 décembre 2022 ; Politique étrangère au Canada, X Post, 28 avril 2022 ; Allemagne auprès des Nations Unies, X Post, 9 mars 2021.

87 François Delerue, Conférence sur « The Application of International Law to Cyberspace » organisée à l'université de Bologne, EU Cyber Direct (12 novembre 2021).

Enfin, les États devraient envisager d'inclure des **supports visuels** dans le cadre d'une stratégie de communication globale. Plusieurs représentants d'États consultés dans le cadre de ce projet ont souligné que le travail sur le fond d'une position nationale devait s'accompagner d'une attention particulière à la présentation. Comme indiqué ci-dessus, les supports visuels peuvent inclure la composition, les infographies, les tableaux et les graphiques.

Figure 11 : Exemples de stratégies de diffusion des positions nationales.

5. Conclusion

Comme nous l'avons vu tout au long de ce chapitre, chaque format, style, langue et mode de diffusion choisis pour exprimer une position nationale présente des avantages et des inconvénients. En fin de compte, ces choix sont façonnés par le statut juridique, l'approche et les objectifs que les États se sont fixés pour leurs positions. Par exemple, si une position nationale est publiée à titre de preuve de *l'opinio juris* d'un État ou de ses interprétations et vise à influencer l'élaboration ou l'interprétation du droit international, un document écrit bien structuré et détaillé, publié en anglais, serait peut-être plus approprié. À l'inverse, si une position nationale vise à formuler des commentaires politiques ou à sensibiliser le public à des questions générales de droit international dans le cyberespace, un document ou un discours plus court et moins structuré, publié en anglais et/ou dans d'autres langues, pourrait suffire. Néanmoins, quels que soient le statut, l'approche et les objectifs d'une position nationale, son contenu doit être clairement compris et pris en compte de manière appropriée par les publics concernés. Les États doivent donc établir un équilibre délicat entre autorité et accessibilité lorsqu'ils réfléchissent à la manière de présenter leurs positions nationales.

En suivant les tendances éprouvées en matière de format, de style, de langage et de stratégies de diffusion abordées dans ce chapitre, il est possible de parvenir à cet équilibre. Les États et les autres parties prenantes peuvent également ainsi compiler, comparer et mettre en contraste les positions nationales afin d'identifier les points de consensus, les désaccords et les lacunes en ce qui concerne la compréhension de l'application du droit international dans le cyberespace. Cependant, chaque État a des besoins, des aspirations et des traditions culturelles et juridiques qui lui sont propres. Par conséquent, tout comme pour le choix des questions de fond à traiter et du processus à suivre, il n'existe pas de modèle unique de présentation des positions nationales. Il existe plutôt un ensemble d'options et d'éléments qui peuvent être combinés et adaptés en fonction des différentes intentions. Il appartient aux États de décider quelles options suivre ou s'ils souhaitent établir de nouvelles tendances.

CHAPITRE 6 :

CONCLUSION

Les positions nationales ont modifié la manière dont le droit international est compris dans le contexte numérique. À mesure qu'un nombre croissant d'États ont publié leurs points de vue sur l'application du droit international aux activités numériques, ce domaine s'est éloigné des zones d'ombre pour gagner en lisibilité. Il subsiste toutefois des incertitudes et des divergences quant aux règles et principes internationaux applicables aux technologies de l'information et de la communication (TIC), à leur mode d'application et à la nécessité d'élaborer de nouvelles règles. Une convergence totale sur ces questions est pratiquement impossible et n'est peut-être même pas souhaitable : le droit international est vaste, bon nombre de ses questions sont complexes, et une multitude d'États et d'autres acteurs ayant des histoires, des cultures et des agendas différents participent à l'élaboration, à l'interprétation et à l'application du droit. Toutefois, comme nous l'avons vu tout au long de ce Manuel, les positions nationales et communes ont permis de dégager beaucoup plus facilement les points de convergence et de divergence, ainsi que les lacunes éventuelles. Cette cartographie est essentielle pour favoriser le dialogue et instaurer la confiance entre les États, permettant ainsi de progresser dans ce domaine, même lorsque des accords communs ne sont pas possibles.

En ce sens, les positions nationales sont devenues un outil précieux pour les États et les autres parties prenantes dans ce domaine, notamment les académiques, les représentants de l'industrie et les membres de la société civile. Au moment de la rédaction de ce Manuel, 33 États ont publié une position nationale et deux organisations régionales — l'Union africaine (UA) et l'Union européenne (UE) — ont publié des positions communes (voir **annexe B**). D'autres États ont fait part de leur intention d'élaborer une position nationale, tandis que certains de ceux qui ont déjà adopté une position pourraient souhaiter la revoir ou la mettre à jour. Afin de les guider dans le processus d'élaboration ou de révision d'une position nationale, le présent Manuel examine les questions clés qui pourraient se poser en cours de route.

Tout d'abord, comme indiqué dans **l'introduction**, les positions nationales peuvent avoir des implications juridiques dans le contexte cybernétique et au-delà. Plus précisément, elles peuvent être considérées comme des évidences *d'opinio juris* et, de manière plus controversée, comme des pratiques étatiques. À ce titre, elles peuvent contribuer au développement du droit international coutumier. De même, les positions nationales peuvent constituer une pratique ultérieure dans l'application des traités internationaux ou des moyens supplémentaires pour interpréter ces traités. On peut également se demander si le silence des États qui n'ont pas encore publié des positions nationales peut être considéré comme une acceptation tacite des règles coutumières ou des interprétations des traités avancées par d'autres États dans leurs positions. En droit international, le silence des États ne peut être considéré comme une acceptation tacite d'une règle coutumière ou d'une interprétation d'un traité que si certaines conditions strictes sont remplies.

Il s'agit notamment de l'existence de circonstances suffisamment spécifiques justifiant une réaction, d'une connaissance adéquate et du passage d'un délai raisonnable.[1]

Les positions nationales ont eu des répercussions juridiques qui ne se sont pas limitées aux activités cybernétiques : elles ont également touché l'ensemble du droit international. En effet, la tendance à publier les positions nationales a été motivée par la difficulté à appliquer du droit ancien à une technologie nouvelle et omniprésente : les opérations cybermalveillantes ont été menées à une vitesse sans précédent et ont eu des répercussions à l'échelle internationale, remettant en question les concepts traditionnels du droit international, tels que la souveraineté, la non-intervention et les notions d'« attaque » et d'« objet » dans le droit international humanitaire (DIH). En explorant la manière dont les règles et principes internationaux d'application générale doivent être compris dans le contexte cybernétique, les positions nationales ont relancé des débats fondamentaux qui sont pertinents dans d'autres contextes. Il s'agit par exemple de savoir si la souveraineté et la diligence due donnent lieu à des obligations pour les États et si les États tiers peuvent recourir à des contre-mesures collectives.

Le **chapitre 2** a présenté les différentes motivations qui poussent à élaborer une position nationale (ou à choisir de ne pas le faire). Trois fonctions principales ont été identifiées : communiquer aux différentes parties prenantes le point de vue d'un État sur l'application du droit international aux activités cybernétiques (fonction communicative) ; transformer ou adapter les règles du droit international telles qu'elles s'appliquent dans ce contexte, notamment en développant le droit international coutumier ou en proposant de nouvelles interprétations des traités (fonction transformatrice) ; et dissuader, prévenir et/ou atténuer les conséquences négatives des opérations cybermalveillantes menées par des États et des acteurs non étatiques (fonction préventive).

Ces fonctions peuvent être remplies par le biais d'objectifs spécifiques et formulées sous forme de motivations différentes. Plus précisément, les positions nationales peuvent prévenir les erreurs d'appréciation et l'escalade en renforçant la prévisibilité et la stabilité des relations internationales. De même, elles peuvent encourager le respect des règles et la responsabilisation en dissuadant et en prévenant les opérations cybernétiques illicites. Les positions nationales peuvent également influencer l'évolution du droit international applicable aux activités cybernétiques et remédier au flou juridique. En outre, l'impact positif des positions nationales peut se faire sentir au niveau national. Elles peuvent notamment contribuer à clarifier ce que signifie un comportement responsable de l'État pour les parties prenantes nationales, favoriser la cyber-résilience nationale, améliorer la coordination interinstitutionnelle et stimuler d'importants développements juridiques et politiques.

1 CDI, Draft conclusions on the identification of customary international law, with commentaries, A/73/10 (2018), 120, conclusion 10(3) ; CDI, Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties, (2018), 15, conclusion 10(2).

Cependant, plusieurs facteurs pourraient compliquer la réalisation de ces objectifs par les États. Le manque des capacités est l'un des principaux obstacles. La grande majorité des positions nationales publiées à ce jour ont été émises par des pays développés. L'élaboration de la position commune de l'UA a été rendue possible grâce à des efforts concertés de renforcement des capacités et à un leadership fort de la part de l'organisation.[2] Le processus d'élaboration d'une position nationale nécessite d'importantes ressources, et des investissements considérables sont nécessaires pour combler les disparités en matière de capacités entre les pays développés et les pays en développement. Parallèlement, il arrive que certains États n'aient pas la volonté politique nécessaire pour s'engager dans le processus d'élaboration d'une position nationale. D'autres États peuvent craindre que la publication d'une position nationale ne limite leur liberté d'action ou ne suscite encore plus de désaccords sur l'application du droit international aux activités cybernétiques. Il est donc important de continuer à discuter des différentes fonctions et objectifs des positions nationales, en insistant sur le fait qu'elles peuvent favoriser la transparence et instaurer la confiance entre les États, même lorsqu'il n'est pas possible de parvenir à une vision commune sur le fond.

Le **chapitre 3** a présenté les différentes étapes susceptibles d'intervenir dans l'élaboration d'une position nationale. Pour commencer, les États devraient réfléchir aux parties prenantes internes et externes qu'ils souhaitent associer au processus, en gardant à l'esprit qu'il est fortement recommandé de combiner des compétences juridiques, politiques et techniques. La désignation d'un organisme particulier chargé de coordonner le processus et de rédiger la position peut également s'avérer utile. Une série de mesures organisationnelles pourraient être nécessaires. Il s'agit notamment d'attribuer des rôles aux différentes parties prenantes et d'examiner des questions telles que la portée et les objectifs de la position, le lieu des réunions et autres tâches correspondantes, le calendrier et les différentes méthodes de réalisation de chaque tâche. Certains États pourraient également souhaiter renforcer leurs capacités dans différents domaines, notamment le droit international, la politique cybernétique et la cybersécurité, avant de pouvoir élaborer une position nationale.

Lorsqu'il s'agit de rédiger une position nationale, les États peuvent adopter différentes stratégies. Ils peuvent, par exemple, partir d'un texte complet et le peaufiner au fil des discussions. À l'inverse, un texte ou un plan plus simple peut être développé pour devenir un document de position complet.

2 Mohamed Helal, « The Common African Position on the Application of International Law in Cyberspace : Reflections on a Collaborative Lawmaking Process », EJIL: Talk! (5 février 2024).

Au cours de la phase de rédaction, les États peuvent recourir à des sources formelles et informelles, ainsi qu'à des consultations avec des parties prenantes internes ou externes. De plus, l'adoption d'une position nationale peut également être soumise à un processus institutionnel défini, y compris une approbation formelle par une autorité spécifique. Les positions nationales peuvent faire l'objet d'un réexamen, dans la mesure où les États peuvent décider d'ajuster ou de réviser leur position initiale sur les différentes questions en jeu.

Ces différentes étapes et stratégies de rédaction montrent que l'élaboration et la publication d'une position nationale n'est pas chose facile, et qu'elle peut s'avérer particulièrement difficile pour les États confrontés à des capacités insuffisantes ou à des obstacles politiques. Il est regrettable que les efforts considérables déployés par toutes les parties prenantes dans ce processus ne débouchent pas nécessairement sur la publication d'une position. Cependant, les États ne doivent pas se laisser décourager. Le processus lui-même est précieux, quel que soit son résultat. Il peut, par exemple, favoriser un dialogue et une coordination accrus entre les agences nationales, aider les États à formuler des positions internes qui n'ont pas besoin d'être publiées et mieux les préparer aux discussions dans le cadre des processus multilatéraux. En particulier, les connaissances acquises lors des sessions de formation, de discussion et/ou de rédaction d'une position nationale peuvent être utilisées dans les négociations diplomatiques et dans des contributions plus ciblées au sein du Groupe de travail à composition non limitée (GTCNL) des Nations Unies et d'autres forums multilatéraux. Comme indiqué dans différents chapitres du présent Manuel, les États peuvent également utiliser ces contributions pour exprimer leur point de vue sur la manière dont les différentes règles et principes du droit international s'appliquent aux activités cybernétiques.

Le **chapitre 4** a présenté une vue d'ensemble des différentes questions de fond abordées à ce jour dans les positions nationales, ainsi que les considérations politiques qui ont guidé les États dans le choix et l'approche de ces questions. Bien qu'il existe certaines variations dans le choix des thèmes et dans la précision de l'analyse, les positions nationales publiées à ce jour présentent une liste largement cohérente de questions ou de domaines du droit international. Il s'agit notamment des règles et principes fondamentaux, tels que le principe de souveraineté et ses corollaires, y compris la non-intervention, l'interdiction du recours à la force et la diligence due, ainsi que le règlement pacifique des différends et l'autodétermination. Les positions nationales traitent également de régimes spécialisés du droit international, notamment le DIH, le droit international des droits de l'homme (DIDH) et le droit pénal international. La responsabilité de l'État, qui régit les conséquences des violations des obligations internationales, occupe également une place importante, notamment en ce qui concerne l'attribution, les contre-mesures et la nécessité.

Les positions nationales permettent aux États de comprendre leurs divergences, d'en débattre de manière constructive et de rechercher un terrain d'entente lorsque l'occasion se présente.

Certaines questions ont fait l'objet d'un accord entre les positions nationales, notamment, comme point de départ, le fait que le droit international s'applique aux activités cybernétiques. Il existe également un accord sur le fait que le DIH et le DIDH sont en principe applicables aux TIC. De plus, il se dégage un consensus autour des éléments constitutifs de règles ou de principes spécifiques, tels que la non-intervention et la responsabilité de l'État. Toutefois, comme indiqué précédemment, les positions nationales ont révélé des points de désaccord. Il s'agit notamment de savoir si certains principes donnent également lieu à des obligations, quels sont les seuils ou les conditions qui déclenchent une violation de certaines obligations, et si et dans quelle mesure certains types d'activités cybernétiques — telles que le cyberespionnage — peuvent constituer des violations. Comme indiqué précédemment, certains désaccords sont inévitables, en particulier dans un système juridique décentralisé comme le droit international. De même, tous les désaccords ne sont pas nécessairement préjudiciables à la paix et à la sécurité internationales. Cependant, il est essentiel que les désaccords soient connus afin d'être discutés et, si nécessaire, résolus. Les positions nationales permettent aux États de comprendre leurs différences, d'en débattre de manière constructive et de rechercher un terrain d'entente lorsque l'occasion se présente.

Le contenu des positions nationales n'est pas le seul élément important : leur présentation est tout aussi cruciale, car elle déterminera l'impact qu'elles pourraient avoir. Le **chapitre 5** a examiné les différentes options dont disposent les États en matière de format, de style, de langage et de diffusion de leur position nationale. Ces caractéristiques varient considérablement d'une position nationale à l'autre parmi celles publiées à ce jour et reflètent des choix politiques importants, notamment en ce qui concerne le statut juridique, l'approche et les objectifs de ces positions. Si certaines positions nationales ont été publiées sous forme de discours gouvernementaux, de déclarations à l'ONU et d'articles académiques, la grande majorité d'entre elles ont été publiées sous forme de documents écrits autonomes. Leur style varie également entre des documents courts de deux à cinq pages et des documents plus longs pouvant atteindre 22 pages. Les positions nationales plus courtes sont naturellement plus générales et accordent parfois la priorité aux questions de politique. Les positions plus longues couvrent un champ plus large et approfondissent des questions juridiques spécifiques, de sorte qu'elles sont plus appropriées si l'objectif est de clarifier et/ou de développer le droit international applicable aux activités cybernétiques. La plupart des positions nationales contiennent des références et des titres, ce qui peut renforcer leur autorité juridique, leur lisibilité et leur clarté. Les résumés, les paragraphes numérotés, les exemples et les supports visuels peuvent également améliorer considérablement l'accessibilité d'une position, mais seuls quelques-uns intègrent ces éléments.

Toutes les positions nationales emploient le lexique traditionnel du droit international et utilisent une terminologie spécifique pour indiquer leur position sur différentes questions juridiques. La plupart des positions nationales et les deux positions communes ont été publiées en anglais, la *lingua franca* du droit international et de la diplomatie. Cela a permis de garantir l'utilisation d'une terminologie juridique cohérente et la visibilité auprès des publics concernés, notamment les juristes gouvernementaux, les diplomates et les académiques. Toutefois, afin de rendre les positions nationales plus accessibles à d'autres publics, en particulier aux parties prenantes nationales et étrangères du Sud Global, les États pourraient envisager de publier leurs positions nationales dans d'autres langues que l'anglais, notamment dans les autres langues officielles de l'ONU (arabe, chinois, français, russe et espagnol). Les États devraient également envisager différentes stratégies pour diffuser leurs positions auprès des publics cibles, notamment en les publiant dans des bases de données en ligne, des revues académiques, des blogs et des réseaux sociaux, ainsi qu'en organisant des événements publics et privés pour en discuter. Dans l'ensemble, lorsqu'ils décident du format, du style, de la langue et des stratégies de diffusion à adopter, les États devraient chercher à établir un équilibre entre l'autorité juridique et l'accessibilité.

Et ensuite ?

Si les positions nationales sont devenues le vecteur principal par lequel les États expriment leurs points de vue sur le droit international dans le contexte cybernétique, davantage d'États devraient se sentir habilités à élaborer et à publier leurs positions s'ils le souhaitent. Comme indiqué précédemment, cette démarche nécessite des efforts concertés pour sensibiliser à l'importance des positions nationales et renforcer les capacités des États en matière de droit international et d'élaboration de positions, en accordant la priorité aux plus démunis.

Comme indiqué dans l'introduction, l'équipe principale à l'origine de ce projet a organisé trois consultations régionales avec des représentants d'États d'Afrique, des Amériques, d'Asie et du Pacifique. Ces consultations avaient pour objectif d'échanger des points de vue sur les différents thèmes abordés dans le présent Manuel et de comprendre quelles mesures sont nécessaires pour combler les disparités existant entre les États en matière de capacités. Il serait toutefois souhaitable d'étendre ces discussions à d'autres régions, en particulier à l'Europe de l'Est et au Moyen-Orient, en tenant bien compte des différences linguistiques et culturelles susceptibles d'influer sur la compréhension du droit international dans ces régions. Ce thème pourrait également faire l'objet de discussions plus approfondies dans les forums internationaux, notamment à l'ONU. Le futur mécanisme permanent qui pourrait succéder au GTCNL dans les discussions générales sur les implications des TIC en matière de sécurité serait particulièrement bien placé pour poursuivre le dialogue sur les positions nationales au sein des Nations Unies.[3]

3 Cf. Assemblée Générale des Nations Unies, Developments in the field of information and telecommunications in the context of international security, A/79/214 (2024), paragraphes 5, 7, 56-60.

Des discussions ont également eu lieu concernant l'adoption d'autres instruments ou documents relatifs à l'application du droit international au cyberespace. Par exemple, la position commune de l'UA suggère que « le processus d'articulation des règles du droit international applicables à l'utilisation des TIC dans le cyberespace bénéficierait de l'adoption d'une déclaration des Nations Unies sur ce sujet ».[4] Il est peu probable que le Conseil de sécurité des Nations Unies adopte une résolution sur l'application du droit international aux activités cybernétiques, compte tenu des désaccords persistants entre ses membres permanents. D'autre part, une majorité d'États membres de l'ONU pourrait soutenir l'adoption d'une résolution sur ce sujet par l'Assemblée générale des Nations Unies, peut-être sur la base des travaux du successeur du GTCNL. Néanmoins, le contenu de cette déclaration serait probablement de nature générale, comme la plupart des résolutions adoptées jusqu'à présent par l'Assemblée générale des Nations Unies.

Certains ont également proposé que l'Assemblée générale ou un autre organe compétent des Nations Unies sollicite un avis consultatif de la Cour internationale de justice (CIJ) sur l'application du droit international aux activités cybernétiques.[5] Cependant, il est possible que la CIJ ne soit pas la mieux placée pour résoudre cette question, étant donné qu'un nombre important de domaines et de questions relevant du droit international, allant des règles générales et des régimes spécialisés aux questions de responsabilité des États, sont pertinents pour les activités cybernétiques. D'autres ont supposé que la Commission du droit international lancerait une étude et publierait finalement un rapport sur le sujet, mais rien n'indique qu'une telle initiative ait été prise au moment de la rédaction du présent document. Il convient toutefois de noter que la question de l'application du droit international aux activités cybernétiques est actuellement examinée par l'Institut de droit international.[6]

4 Position commune de l'UA (2024), paragraphe 7.

5 Cf. Statut de la Cour internationale de Justice, article 96.

6 Institut de droit international, The Applicability of International Law to Cyber Activities (2023).

Comme indiqué dans le présent Manuel, certains États ont proposé l'adoption d'un traité juridiquement contraignant régissant différents aspects des TIC, tels que la sécurité de l'information ou des données.[7] Différentes parties prenantes ont également proposé l'adoption d'un traité visant à élargir les protections déjà offertes par le droit international existant dans le contexte cybernétique, comme une convention de Genève numérique ou une convention pour la protection des infrastructures critiques contre les cyberopérations.[8] Si ces propositions peuvent ou non aboutir, elles ne sont pas nécessairement en contradiction avec les efforts visant à clarifier l'application du droit international existant aux activités cybernétiques, notamment par le biais des positions nationales. Les deux types d'initiatives peuvent coexister et se compléter.

Les positions nationales peuvent également favoriser l'adoption de législations et de documents politiques nationaux visant à internaliser et à développer davantage les critères relatifs au comportement responsable des États dans le contexte cybernétique. En particulier, les États peuvent définir dans leurs lois nationales les mesures pratiques qui, selon eux, devraient être prises au niveau national pour mettre en oeuvre des obligations telles que la souveraineté, la non-intervention et la diligence due, ainsi que la protection des droits de l'homme contre les opérations cybernétiques. De même, les États peuvent intégrer et développer leurs points de vue sur l'application du DIH aux TIC dans leurs propres manuels militaires ou règles d'engagement.

Que ce soit au niveau national ou international, il est également possible d'engager des discussions plus pratiques sur le contenu des positions nationales, par exemple au moyen d'exercices basés sur des scénarios ou des études de cas. Comme indiqué au chapitre 5, de nombreuses positions nationales approfondissent les complexités et les controverses liées aux différentes règles et principes internationaux particulièrement pertinents dans le contexte cyber. Cependant, elles le font, pour la plupart, de manière très abstraite : en effet, seules quelques positions font référence à des incidents réels, notamment à des exemples d'opérations cyber qui pourraient hypothétiquement enfreindre le droit international, ou proposent des mesures pratiques pour mettre en oeuvre les obligations internationales dans le contexte cyber.

Enfin, compte tenu de l'impact globalement positif des positions nationales, y compris sur le droit international en général, ce modèle peut être mis à profit pour favoriser le dialogue et la vision commune sur d'autres défis mondiaux qui ont donné lieu à un flou juridique et à des désaccords entre les États. C'est particulièrement le cas pour les questions qui ne font l'objet d'aucun traité spécifique et/ou d'aucune instance permanente de discussion ou de jugement multilatéral, par exemple : les autres technologies émergentes telles que l'intelligence artificielle. En réalité, les États ont déjà commencé à publier leurs points de vue nationaux sur la manière

7 Par exemple, Fédération de Russie, Updated Concept of the Convention of the United Nations on Ensuring International Information Security, (2023) ; République populaire de Chine, Initiative mondiale sur la sécurité des données, (2022).

8 Cf., par exemple, Patryk Pawlak et Aude Géry, « Why the World Needs a New Cyber Treaty for Critical Infrastructure », Carnegie Endowment for International Peace (28 mars 2024) ; Microsoft, « The need for a Digital Geneva Convention » (14 février 2017).

dont ils considèrent que le droit international, en particulier le DIH, s'applique aux systèmes d'armes autonomes létales.[9] Et l'Assemblée générale des Nations Unies a récemment invité les États membres à soumettre leurs points de vue sur les implications de l'utilisation de l'intelligence artificielle dans le domaine militaire, au-delà des armes autonomes létales, pour la paix et la sécurité internationales, y compris sur la manière dont le droit international traite cette question.[10]

D'autres domaines tels que l'espace extra-atmosphérique et les droits de l'homme dans les conflits armés pourraient également bénéficier de déclarations sur la manière dont le droit international existant traite les nouveaux défis, compte tenu de leur évolution rapide et de l'absence d'un forum multilatéral dédié. Ces déclarations n'ont pas besoin d'être aussi exhaustives que les positions nationales publiées dans le cadre des TIC, la plupart de ces positions couvrant déjà de manière très détaillée les questions générales de droit international (par exemple, la souveraineté, la non-intervention et la diligence due). Les positions nationales sur l'intelligence artificielle et d'autres questions pourraient s'appuyer sur cet acquis, en ciblant des questions plus spécifiques du droit international qui présentent des défis concrets dans ces contextes.

Quelle que soit l'évolution future des positions nationales, et indépendamment de l'adoption éventuelle de nouveaux instruments ou d'accords supplémentaires sur le droit international dans le domaine cybernétique et dans d'autres contextes, une chose est claire : les positions publiées jusqu'à présent témoignent des progrès déjà accomplis par les États, sur lesquels ils peuvent continuer à s'appuyer dans un environnement difficile. Elles montrent que, même si des divergences juridiques et des tensions géopolitiques persistent, un dialogue constructif est possible. Nous espérons que ce Manuel motivera les États à poursuivre dans cette voie, favorisant ainsi la transparence, la discussion et une vision commune sur la manière dont le droit international peut contribuer à résoudre les plus grands défis mondiaux, tant en ligne que hors ligne.

9 Cf. Assemblée Générale des Nations Unies, Lethal autonomous weapons systems : *Report of the* Secretary-General, A/79/88 (1er juillet 2024).

10 Assemblée générale des Nations Unies, Artificial intelligence in the military domain and its implications for international peace and security, A/RES/79/239 (31 décembre 2024).

Manuel relatif à l'élaboration d'une position nationale sur le droit international et les activités cybernétiques :
Un guide pratique à l'intention des États

BIBLIOGRAPHIE

Livres et monographies

Cryer, Robert, Robinson, Darryl, et Vasiliev, Sergey. *An Introduction to International Criminal Law and Procedure* (CUP 2019).

Dias, Talita. *Beyond Imperfect Justice: The Principles of Legality and Fair Labelling in International Criminal Law* (Brill 2022).

Gallant, Kenneth S. *The Principle of Legality in International and Comparative Criminal Law* (CUP 2010).

Knop, Karen. *Diversity and Self-Determination in International Law* (CUP 2009).

Lahmann, Henning. *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (CUP 2020).

Milanovic, Marko. *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (OUP 2011).

Roscini, Marco. *Cyber Operations and the Use of Force in International Law* (OUP 2014).

— International Law and the Principle of Non-Intervention (OUP 2024).

Schabas, William A. *The Customary International Law of Human Rights* (OUP 2021).

Sparks, Tom. *Self-Determination in the International Legal System* (Bloomsbury 2023).

Sterio, Milena. *The Right to Self-Determination under International Law* (Routledge 2013).

Urs, Priya, Dias, Talita, Coco, Antonio, et Akande, Dapo. *The International Law Protections against Cyber Operations Targeting the Healthcare Sector* (ELAC 2023).

Zoller, Elizabeth. *Peacetime Unilateral Remedies: An Analysis of Countermeasures* (Transnational 1984).

Ouvrages édités et textes de référence

Fisher, Ryan (éd.), *Operational Law Handbook (National Security Law Department, the Judge Advocate General's School,* (United States Army, 2022).

Henckaerts, Jean-Marie, et Doswald-Beck, Louise (éd.), *Customary International Humanitarian Law: Volume I, Rules* (CICR et CUP 2005).

CICR (éd.), *Commentary on the Third Geneva Convention* (CUP 2021).

Schmitt, Michael N (éd.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).

Contributions à des ouvrages collectifs

Akande, Dapo. « Sources of International Criminal Law », in Antonio Cassese (éd.), *The Oxford Companion to International Criminal Justice* (OUP 2009).

Hollis, Duncan B., et van Benthem, Tsvetelina. « Threatening Force in Cyberspace », in Laura A. Dickinson et Edward W. Berg (éds), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (OUP 2024).

Mačák, Kubo. et Gisel, Laurent. *« The Legal Constraints of Cyber Operations in Armed Conflicts », in Rajeswari Pillai Rajagopalan (éd.), Future Warfare and Technology: Issues and Strategies* (Wiley 2022).

Pellet, Alain. « Peaceful Settlement of International Disputes », in Rüdiger Wolfrum (éd.), *Max Planck Encyclopedia of Public International Law* (éd. en ligne, OUP 2013).
Tams, Christian. « Article 2(4) », in Bruno Simma et al (éds), The Charter of the United Nations: A Commentary, Vol I (OUP 2024).

Tomuschat, Christian. « Article 2(3) », in Bruno Simma et al (éds), *The Charter of the United Nations: A Commentary, Vol I* (OUP 2024).

Tsagourias, Nicholas. *« Cyber Disputes as International Legal Disputes », in Nicholas Tsagourias, Russell Buchan, et Daniel Franchini (éds), Peaceful Settlement of Inter-State Cyber Disputes* (Hart 2024).

— « Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace », in Dennis Broeders et Bibi van den Berg (éds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield 2020).

Ziegler, Katja S. « Domaine réservé » in Rüdiger Wolfrum (éd.), *Max Planck Encyclopedia of Public International Law* (éd. en ligne, OUP 2013).

Articles de revues

Cleveland, Sarah H. *« Embedded International Law and the Constitution Abroad »* (2010) 110 Columbia Law Review 225.

Coco, Antonio. et de Souza Dias, Talita. *« Cyber Due Diligence: A Patchwork of Protective Obligations in International Law »* (2021) 32 European Journal of International Law 795.

Coco, Antonio., Dias, Talita., et van Benthem, Tsvetelina. *« Illegal: The SolarWinds Hack under International Law »* (2022) 33(4) European Journal of International Law 1275.

Deeks, Ashley. *« Defend Forward and Cyber Countermeasures », Hoover Working Group on National Security, Technology, and Law* (2020).

Dias, Talita. *« Finding Common Ground: The Right to be Free from Incitement to Discrimination, Hostility, and Violence in the Digital Age »* (2024) 16(4) Global Responsibility to Protect 391.

Droege, Cordula. *« Elective affinities? Human rights and humanitarian law »* (2008) 90 International Review of the Red Cross 501.

— *« Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians »* (2012) 94(886) International Review of the Red Cross 533.

Egan, Brian J. *« International Law and Stability in Cyberspace »* (2017) 35(1) Berkeley Journal of International Law 169.

Engdahl, Ola. *« Sweden's Position Paper on the Application of International Law in Cyberspace »* (2023) 92(3) Nordic Journal of International Law 489.

Helal, Mohamed. « *On Coercion in International Law* » (2019) 52(1) NYU Journal of International Law and Politics 1.

Henriksen, Anders. « *The end of the road for the UN GGE process: The future regulation of cyberspace* » (2019) 5(1) Journal of Cybersecurity 1.

Jackson, Miles, et Paddeu, Federica. « *The Countermeasures of Others* » (2024) 118(2) American Journal of International Law 231.

Kjelgaard, Jeppe Mejer, and Melgaard, Ulf. « *Denmark's Position Paper on the Application of International Law in cyberspace* » (2023) 92(3) Nordic Journal of International Law 446.

Lahmann, Henning. « *The Plea of Necessity in Cyber Emergencies* » (2023) 92(3) Nordic Journal of International Law 422.

Lehto, Marja. « *Finland's views on International Law and Cyberspace* » (2023) 92(3) Nordic Journal of International Law 456.

Mačák, Kubo. « *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law* » (2015) 48 Israel Law Review 55.
Mendelson, Maurice. « *The Formation of Customary International Law* » (1998) 272 Recueil des Cours 155.

Milanovic, Marko, et Schmitt, Michael N. « *Cyber attacks and cyber (mis)information operations during a pandemic* » (2020) 11(1) Journal of National Security Law and Policy 247.

Musæus, Vibeke. « *Norway's Position Paper on International Law and Cyberspace* » (2023) 92(3) Nordic Journal of International Law 470.

Ohlin, Jens D. « *Did Russian Cyber-Interference in the 2016 Election Violate International Law?* » (2017) 95 Texas Law Review 1579.

Roscini, Marco. « *Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes* » (2019) 30 Criminal Law Forum 247.

Schmitt, Michael N. et Watts, Sean. « *Collective cyber countermeasures?* » (2021) 12 Harvard National Security Journal 373.

Schöndorf, Roy. « *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations* » (2021) 97 International Law Studies 395.

Shany, Yuval. « *Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law* » (2013) 7 Le droit et l'éthique des droits de l'homme 47.

Shany, Yuval. et Schmitt, Michael N. « *An International Attribution Mechanism for Hostile Cyber Operations* » (2020) 96 Études de droit international 196.
van Benthem, Tsvetelina, Dias, Talita, et Hollis, Duncan B. « *Information Operations under International Law* » (2022) 55 Vanderbilt Journal of Transnational Law 1217.

Rapports sélectionnés et autres sources en ligne

Australie, *Australia's Cyber Security* (2016).

— Ministère des Affaires étrangères et du Commerce, *Australia's International Cyber Engagement Strategy* (octobre 2017).

Institut australien de politique stratégique, *Centre international de politique cybernétique, The UN norms of responsible state behaviour in cyberspace Guidance on implementation for Member States of ASEAN* (mars 2022).

Autriche, *Pre-Draft Report of the OEWG – TIC: Comments by Austria (31 mars 2020). Chatham House, Applying the Plea of Necessity to Cyber Operations, résumé de la réunion, Programme de droit international* (27 septembre 2023).

Chili, *Ministère des Relations extérieures, Derecho Internacional, ONU, New York, GTCNL, sixième session de fond* (11-15 décembre 2023).

— *National Cybersecurity Policy* (2017-2022).

Chine (République populaire de), *Global Initiative on Data Security* (2022).

Mission chinoise auprès des Nations Unies, *Statement by the Chinese Delegation at the Thematic Debate of the First Committee of the 72th UNGA* (2017).

Christou, *George. Cyber Diplomacy: From Concept to Practice, Document de Tallinn n° 14, NATO CCDCOE* (2024).

Conseil de l'Union européenne, *EU sanctions – New recital in Council Decision*, (PESC) 2023/191 du 27 janvier 2023 – Contre-mesures, WK 5169/2023 INIT (2023).

Représentation de Cuba à l'étranger, *71 UNGA: Cuba at the final session of the Group of Governmental Experts on the developments in the field of information and telecommunications in the context of international security* (23 juin 2017).

Dias, Talita. *Countermeasures in international law and their role in cyberspace* (Chatham House 2024).

Estonie, *Ministère des Affaires étrangères, Tallinn Workshops on International Law and Cyber Operations, Compendium of reports* (2023).

Commission européenne, *The EU's Cybersecurity Strategy for the Digital Decade (2020). Allemagne, Ministère fédéral des Affaires étrangères, « Cyber Security as a Dimension of Security Policy ». Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London, Londres* (18 mai 2015).

CICR, *International humanitarian law and the challenges of contemporary armed conflicts* (octobre 2015).

— *International humanitarian law and cyber operations during armed conflicts* (2019).

— *How is the term « armed conflict » defined in international humanitarian law?, Document d'opinion* (2024).

Kavanagh, *Camino. The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century, UNIDIR* (2017).

McLaughlin, *Robert. Data as a Military Objective, Institut australien des affaires internationales* (20 septembre 2018).

Microsoft, *« The need for a Digital Geneva Convention »* (14 février 2017).

Moynihan, *Harriet. The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (Chatham House 2019).

National Cybersecurity Guide, *Guide to Developing a National Cybersecurity Strategy, 2e édition* (2021).

Forum des îles du Pacifique, *Statement delivered by PIF Chair on behalf of the Pacific Islands Forum, ONU* (New York, 4 décembre 2024).

Mission permanente du Liechtenstein auprès des Nations Unies, *The Council of Advisers' Report on the Application of the Rome Statute to Cyberwarfare* (août 2021).

Persi Paoli, *Giacomo, Dominioni, Samuele, Rafiq, Aamna, et Filipová, Lenka. Accelerating TIC Security Capacity-Building: Takeaways from the Global Roundtable on TIC Security Capacity-Building, UNIDIR, Genève* (2024).

Fédération de Russie, *Updated Concept of the Convention of the United Nations on Ensuring International Information Security* (2023).

Afrique du Sud, *Statement by South Africa in the ninth session of the Open-Ended Working Group on security of and in the use of TICs (2021-2025) - Droit international, ONU, New York* (4 décembre 2024).

Assemblée Générale des Nations Unies, *Report of the International Law Commission on the work of its fifty-second session*, A/CN.4/513 (15 février 2001).

— *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/65/201 (30 juillet 2010).

— *Developments in the field of information and telecommunications in the context of international security. Rapport du Secrétaire général*, A/66/152 (15 juillet 2011).

— *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (24 juin 2013).

— *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/70/174 (22 juillet 2015).

— *Open-ended working group on developments in the field of information and telecommunications in the context of international security. Rapport final de fond*, A/AC.290/2021/CRP.2 (10 mars 2021).

— *Open-ended working group on developments in the field of information and telecommunications in the context of international security. Rapport final de fond*, A/AC.290/2021/CRP.2 (10 mars 2021).

— *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/75/816 (18 mars 2021).

— Recueil officiel des contributions nationales volontaires sur la question de savoir comment le droit international s'applique à l'utilisation des technologies de l'information et de la communication par les États, *soumises par les experts gouvernementaux participant au Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale, créé en application de la résolution 73/266 de l'Assemblée générale* A/76/136* (13 juillet 2021).

— *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135 (14 juillet 2021).

— *Report of the open-ended working group on security of and in the use of information and communications technologies, 2021-2025* (8 août 2022).

— *Report of the open-ended working group on security of and in the use of information and communications technologies, 2021-2025*, A/78/265 (1er août 2023).

— *Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional levels*, A/AC.292/2024/2 (22 janvier 2024).

— *Lethal autonomous weapons systems: Report of the Secretary-General*, A/79/88 (1er juillet 2024).

— *Report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025*, A/79/214 (22 juillet 2024).

— *Initial report outlining the proposal for the development and operationalization of a dedicated Global Information and Communications Technologies Security Cooperation and Capacity-Building Portal*, A/AC.292/2025/1 (14 janvier 2025).

ONU, *Fourth report on international liability for injurious consequences arising out of acts not prohibited by international law, par Robert Q. Quentin-Baxter, Rapporteur spécial*, A/CN.4/373 et Corr.1&2 (27 juin 1983).

UNIDIR, *A Compendium of Good Practices: Developing a National Position on the Interpretation of International Law and State Use of TIC* (2024).

Traités internationaux, résolutions et autres documents

26e Conférence internationale de la Croix-Rouge et du Croissant-Rouge, *Resolution 1 : International Humanitarian Law – From Law to Action*, 26IC/95/R1 (3 décembre 1995).

34e Conférence internationale de la Croix-Rouge et du Croissant-Rouge, *Resolution 2 : Protecting Civilians and Other Protected Persons and Objects Against the Potential Human Cost of TIC Activities During Armed Conflict*, 34IC/24/R2 (octobre 2024).

Charte africaine des droits de l'homme et des peuples, CAB/LEG/67/3 rev. 5, 21 *ILM* 58 (1982) (27 juin 1981).

American Convention on Human Rights, *Série des traités, n° 36 (ouverte à la signature à partir du 22 novembre 1969, entrée en vigueur le 18 juillet 1978)*, 1144 UNTS 123.

Charter of the United Nations (adoptée le 26 juin 1945, entrée en vigueur le 24 octobre 1945) 1 UNTS 16.

Convention on the Prevention and Punishment of the Crime of Genocide (signée le 9 décembre 1948, entrée en vigueur le 12 janvier 1951) 78 UNTS 277.

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, ETS 5 (4 novembre 1950).

Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (signée le 12 août 1949, entrée en vigueur le 21 octobre 1950) 75 UNTS 3.

Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea [Convention de Genève (II) pour l'amélioration du sort des blessés, des malades et des naufragés des forces armées en mer] (signée le 12 août 1949, entrée en vigueur le 21 octobre 1950) 75 UNTS 85.

Geneva Convention (III) relative to the Treatment of Prisoners of War [Convention de Genève (III) relative au traitement des prisonniers de guerre] (signée le 12 août 1949, entrée en vigueur le 21 octobre 1950) 75 UNTS 135.

Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War [Convention de Genève (IV) relative à la protection des personnes civiles en temps de guerre] (signée le 12 août 1949, entrée en vigueur le 21 octobre 1950) 75 UNTS 287.

CDH, *General Comment No 31 [80]: The nature of the general legal obligation imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13* (26 mai 2004).

— *General Comment No 34: Article 19: Freedoms of opinion and expression, CCPR/C/GC/34* (12 septembre 2011).

— *General Comment No 36: Article 6: Right to Life, CCPR/C/GC/36 (3 septembre 2019)* (*Observation générale 36*).

CDI, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, A/56/10 (2001).

— *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, A/56/10 (2001).

— *Draft conclusions on subsequent agreements and subsequent practice in relation to the interpretation of treaties*, A/73/10 (2018).

— *Draft conclusions on the identification of customary international law, with commentaries*, A/73/10 (2018).

— *Draft articles on Prevention and Punishment of Crimes Against Humanity*, A/74/10 (2019).

— *Draft conclusions on identification and legal consequences of peremptory norms of general international law (jus cogens)*, A/77/10 (2022).

International Convention on the Elimination of All Forms of Racial Discrimination (21 décembre 1965) 660 UNTS 195.

International Covenant on Civil and Political Rights (16 décembre 1966) 999 UNTS 171.

HCDH, *« Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework »* (2011).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocole I) (signé le 12 décembre 1977, entré en vigueur le 7 décembre 1978) 1125 UNTS 3.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocole II) (signé le 12 décembre 1977, entré en vigueur le 7 décembre 1978) 1125 UNTS 609.

Rome Statute of the International Criminal Court (adopté le 17 juillet 1998, entré en vigueur le 1er juillet 2002) 2187 UNTS 90 (tel que modifié).

Statute of the International Court of Justice, du 26 juin 1945, annexé à la Charte des Nations Unies.

Assemblée Générale des Nations Unies, *Declaration on the Granting of Independence to Colonial Countries and Peoples*, Résolution 1514 (XV) (14 décembre 1960).

— *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, A/RES/2625 (XXV) (24 octobre 1970), annexe.

— *Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States*, A/RES/36/103 (9 décembre 1981).

— *Manila Declaration on the Peaceful Settlement of International Disputes*, A/RES/37/10 (15 novembre 1982).

— *Resolution adopted by the General Assembly on 22 December 2018 [on the report of the First Committee (A/73/505)] 73/266. Advancing responsible State behaviour in cyberspace in the context of international security, A/RES/73/266 (2 janvier 2019).*

— *Global Digital Compact*, A/79/L.2 (22 septembre 2024).

— *Artificial intelligence in the military domain and its implications for international peace and security*, A/RES/79/239 (31 décembre 2024).

ONU, Proclamation of Teheran, *Final Act of the International Conference on Human Rights*, Teheran, 22 avril au 13 mai 1968, A/CONF.32/41.

HCDH, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/32/13 (1er juillet 2016).

Universal Declaration of Human Rights (résolution 217 A (III) de l'Assemblée générale des Nations Unies du 10 décembre 1948).

Vienna Convention on the Law of Treaties (adoptée le 23 mai 1969, entrée en vigueur le 27 janvier 1980) 1155 UNTS 331.

Jurisprudence internationale

CEDH, *Banković and others v Belgium and others (App n° 52207/99)* (12 décembre 2001).

— *Al-Skeini and others v United Kingdom (App n° 55721/07)* (7 juillet 2011).

CIDH, *Velásquez Rodríguez v Honduras*, (Fond) (Ser C) n° 4 (29 juillet 1988).

CPI, *Prosecutor v* Ntaganda, *Appeals Judgment on the appeals of Mr Bosco Ntaganda and the Prosecutor against the decision of Trial Chamber VI of 8 July 2019 entitled « Judgment »* (30 mars 2021), ICC-01/04-02/06-2666-Red 30-03-2021.

CIJ, *Corfu Channel Case (Royaume-Uni c. Albanie)* (Fond) [1949] CIJ Rec. 4.

— *Military and Paramilitary Activities in and against Nicaragua (Nicaragua c. États-Unis) (Fond)* [1986] CIJ Rec. 14.

— *East Timor [Timor oriental] (Portugal c. Australie)* (Arrêt) [1995] CIJ Rec. 90.

— *Legality of the Threat or Use of Nuclear Weapons* (avis consultatif) [1996] ICJ Rep 226.

— *Gabčíkovo-Nagymaros Project (Hongrie/Slovaquie)* (Arrêt) [1997] ICJ Rep 7.

— *Fisheries Jurisdiction [Compétence en matière de juridiction sur la pêcherie] (Espagne c. Canada)* (Compétence de la Cour) [1998] CIJ Rec. 432.

— *Case Concerning Oil Platforms [Affaire relative aux plates-formes pétrolières] (Iran c. États-Unis)* (Arrêt) [2003] ICJ Rep 161.

— *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé (avis consultatif)* [2004] ICJ Rep 136.

— *Case Concerning Armed Activities in the Territory of the Congo (Fond)* [2005] ICJ Rep 168.

— *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnie-Herzégovine c. Serbie-et-Monténégro)* (Arrêt) [2007] ICJ Rep 43.

— *Usines de pâte à papier sur le fleuve Uruguay (Argentine c. Uruguay)* (Arrêt) [2010] ICJ Rep 14.

— *Effets juridiques de la séparation de l'archipel des Chagos de l'île Maurice en 1965 (avis consultatif)* [2019] ICJ Rep 95.

TPIY, *Prosecutor v Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) IT-94-1-A (2 octobre 1995).

— *Prosecutor v Tadić* (Appeal Judgment) IT-94-1-A (15 juillet 1999).

— *Prosecutor v Limaj* (Trial Judgment) IT-03-66-T (30 novembre 2005).

— *Prosecutor v Boškoski and Tarčulovski* (Trial Judgment) IT-04-82-T (10 juillet 2008).

Island of Palmas (États-Unis c. Pays-Bas) (1928) II RIAA 829.

Trail Smelter Case (États-Unis c. Canada) (1941) 3 RIAA 1911.

ANNEXE A :
Liste de contrôle pour l'élaboration d'une position nationale

Cette liste de contrôle propose une liste non exhaustive de considérations susceptibles d'aider les États à élaborer ou à revoir leur position nationale quant à l'application du droit international aux activités cybernétiques. Elle est organisée conformément à la structure du Manuel et se présente comme un outil de référence pratique destiné à faciliter la planification, la coordination et la prise de décision au niveau interne. Tous les points ne seront pas pertinents dans tous les contextes et il conviendra peut-être d'adapter leur ordre de présentation pour répondre aux exigences nationales.

Motivations *(pour plus d'informations, voir le chapitre 2)*

- ☐ Identifier les motivations principales justifiant l'élaboration d'une position nationale.
- ☐ Réfléchir aux fonctions que la position nationale devrait remplir (par exemple, communicative, transformatrice, préventive).
- ☐ Définir les objectifs respectifs et les résultats attendus de la position nationale.
- ☐ Identifier les risques, contraintes ou sensibilités éventuels, y compris ceux liés à la divulgation, à la flexibilité opérationnelle, à la capacité disponible ou à l'absence de consensus interne.
- ☐ Décider s'il convient d'élaborer une position nationale.
- ☐ Se demander s'il convient d'adopter une position publique, partielle ou interne uniquement, et déterminer la meilleure façon de gérer les omissions stratégiques si nécessaire.

Processus *(pour plus d'informations, voir le chapitre 3)*

- ☐ Tenir compte des spécificités nationales pour adapter le processus et l'ordre des étapes.
- ☐ Obtenir un mandat pour lancer le processus.
- ☐ Recenser les parties prenantes concernées au sein du gouvernement et d'autres secteurs.
- ☐ Sélectionner l'organisme chef de file et les mécanismes de coordination.
- ☐ Désigner un ou plusieurs rédacteurs et, si possible, une équipe de rédaction multidisciplinaire.
- ☐ Élaborer un plan et un calendrier pour le processus, y compris les étapes importantes. Recourir à la grille d'analyse des 5 questions (*Qui ? Quoi ? Pourquoi ? Quand ? Où ? Comment ?*).
- ☐ Identifier les besoins en matière de renforcement des capacités et réfléchir à la manière d'y répondre (par exemple, grâce à des partenariats, à des formations ou à un soutien externe).

- [ ] Consulter les parties prenantes nationales et internationales concernées, notamment les agences techniques et opérationnelles, les conseillers juridiques et, le cas échéant, le grand public ou la société civile.
- [ ] Effectuer des recherches documentaires et recueillir des documents de référence provenant des positions nationales existantes, des forums multilatéraux, des sources académiques et des documents nationaux.
- [ ] Sélectionner une approche de rédaction (déductive, inductive ou hybride).
- [ ] Rédiger la position selon un processus itératif, comprenant un nombre approprié d'étapes d'examen interne, de consolidation et de perfectionnement.
- [ ] Se préparer à l'adoption formelle conformément aux exigences juridiques ou procédurales nationales.
- [ ] Prévoir des révisions, des mises à jour ou des suivis futurs en fonction de l'évolution de la législation ou des politiques.

Contenu *(pour plus d'informations, voir le chapitre 4)*

- [ ] Définir l'étendue et la profondeur souhaitées de l'analyse, en fonction des intérêts et des priorités nationaux.
- [ ] Consulter les positions nationales existantes et d'autres ressources pertinentes telles que la *Cyber Law Toolkit*, le processus d'Oxford et le Manuel de Tallinn 2.0.
- [ ] Identifier les règles et principes clés du droit international à inclure (par exemple, la souveraineté, la diligence due, la non-intervention, l'interdiction du recours à la force).
- [ ] Décider s'il convient d'inclure des avis sur les régimes spécialisés du droit international (par exemple, le DIH, le droit international des droits de l'homme, le droit pénal international).

Format et diffusion *(pour plus d'informations, voir le chapitre 5)*

- [ ] Choisir un format approprié (par exemple, discours, contribution à un forum multilatéral, article académique ou document écrit autonome).
- [ ] Structurer clairement le document et prévoir l'utilisation de titres, de résumés et de paragraphes numérotés.
- [ ] Définir le ton et le niveau de technicité appropriés pour le public visé.
- [ ] Envisager d'inclure des scénarios pratiques ou des exemples concrets pour illustrer les points clés.
- [ ] Vérifier la cohérence de la terminologie et du cadrage dans tous les sujets.
- [ ] Veiller à l'accessibilité, y compris les traductions éventuelles dans d'autres langues et l'utilisation de supports visuels, le cas échéant.
- [ ] Élaborer une stratégie de diffusion, y compris les options de lancement, telles qu'un événement public ou une annonce en ligne.

ANNEXE B :
Liste des positions communes et nationales sur le droit international et les cyberactivités

Positions communes

1. **L'Union africaine**
   Position commune de l'Union africaine (2024)
2. **Union européenne**
   Position commune de l'Union européenne (2024)

Positions nationales

1. **Australie**
   Position nationale de l'Australie (2017)
   Position nationale de l'Australie (2021)
2. **Autriche**
   Position nationale de l'Autriche (2024)
3. **Brésil**
   Position nationale du Brésil (2020)
   Position nationale du Brésil (2021)
4. **Canada**
   Position nationale du Canada (EN) (2022)
   Position nationale du Canada (FR) (2022)
5. **Chine**
   Position nationale de la Chine (généralités) (2021)
   Position nationale de la Chine (souveraineté) (2021)
6. **Colombie**
   Position nationale de la Colombie (EN) (2025)
   Position nationale de la Colombie (ES) (2025)
7. **Costa Rica**
   Position nationale du Costa Rica (2023)
8. **Cuba**
   Position nationale de Cuba (2024)
9. **République tchèque**
   Position nationale de la République tchèque (2020)
   Position nationale de la République tchèque (2024)
10. **Danemark**
    Position nationale du Danemark (2023)
11. **Estonie**
    Position nationale de l'Estonie (2019)
    Position nationale de l'Estonie (2021)
12. **Finlande**
    Position nationale de la Finlande (EN) (2020)
    Position nationale de la Finlande (FI) (2020)
13. **France**
    Position nationale de la France (EN) (2019)
    Position nationale de la France (FR) (2019)
    Position nationale de la France (EN) (2021)

14. **Allemagne**
Position nationale de l'Allemagne (2021)

15. **Iran**
Position nationale de l'Iran (2020)

16. **Irlande**
Position nationale de l'Irlande (2023)

17. **Israël**
Position nationale d'Israël (2021)

18. **Italie**
Position nationale de l'Italie (2021)

19. **Japon**
Position nationale du Japon (2021)

20. **Kazakhstan**
Position nationale du Kazakhstan (2021)

21. **Kenya**
Position nationale du Kenya (2021)

22. **Pays-Bas**
Position nationale des Pays-Bas (2019)

23. **Nouvelle-Zélande**
Position nationale de la Nouvelle-Zélande (2020)

24. **Norvège**
Position nationale de la Norvège (2021)

25. **Pakistan**
Position nationale du Pakistan (2023)

26. **Pologne**
Position nationale de la Pologne (2022)

27. **Roumanie**
Position nationale de la Roumanie (2021)

28. **Russie**
Position nationale de la Russie (2021)

29. **Singapour**
Position nationale de Singapour (2021)

30. **Suède**
Position nationale de la Suède (2022)

31. **Suisse**
Position nationale de la Suisse (2021)

32. **Royaume-Uni**
Position nationale du Royaume-Uni (2018)
Position nationale du Royaume-Uni (2021)
Position nationale du Royaume-Uni (2022)

33. **États-Unis d'Amérique**
Position nationale des États-Unis (2012)
Position nationale des États-Unis (2016)
Position nationale des États-Unis(2020)
Position nationale des États-Unis (2021)

ANNEXE C :
List of participating States

1. Afrique du Sud
2. Algérie
3. Angola
4. Argentine
5. Bénin
6. Brésil
7. Burundi
8. Cambodge
9. Cameroun
10. Canada
11. Chili
12. Colombie
13. Comores
14. Côte d'Ivoire
15. Égypte
16. El Salvador
17. Estonie
18. États-Unis d'Amérique
19. Éthiopie
20. Gambie
21. Indonésie
22. Japon
23. Kenya
24. Lesotho
25. Malaisie
26. Maroc
27. Mauritanie
28. Mexique
29. Mozambique
30. Nouvelle-Zélande
31. Ouganda
32. Paraguay
33. Pérou
34. Philippines
35. République de Corée
36. République dominicaine
37. République du Congo
38. République sahraouie
39. Uruguay
40. République-Unie de Tanzanie
41. Sénégal
42. Singapour
43. Soudan du Sud
44. Thaïlande
45. Togo
46. Zambie

Inclusion in this Annex reflects participation in the project roundtables and does not imply any recognition of legal status. Likewise, participation in the project does not constitute endorsement of the content of this Handbook.

ANNEXE D :
Liste des événements liés au projet

2024

Lancement du projet « Manuel pour l'élaboration d'une position nationale sur le droit international dans le cyberespace : guide pratique à l'intention des États », 16e Conférence internationale sur les conflits cybernétiques : Over the Horizon (CyCon 2024), 28 mai 2024, Tallinn.

Groupe d'experts : « Naviguer dans les dynamiques juridiques : perspectives nationales sur le droit international et les possibilités de convergence », Troisième symposium annuel en présentiel sur le droit international et cybernétique, Conflits futurs : le droit international en matière de cybernétique et de convergence de l'information, American University, 24 septembre 2024, Washington, DC.

Table ronde sur l'élaboration de positions nationales sur le droit international dans le cyberespace : perspectives latino-américaines et caribéennes, siège de l'Organisation des États américains, 25-26 septembre 2024, Washington, DC.

Groupe d'experts : « Positions nationales sur le droit international dans le cyberespace : défis, opportunités et meilleures pratiques », Singapore International Cyber Week, 15 octobre 2024, Singapour.

Table ronde sur l'élaboration de positions nationales sur le droit international dans le cyberespace : perspectives de l'Asie et du Pacifique, Centre for International Law (CIL), Université nationale de Singapour, 16 octobre 2024, Singapour.

Table ronde pour les États membres de l'Union africaine sur l'élaboration d'une position nationale sur le droit international dans le cyberespace, siège de l'Union africaine, 25-26 novembre 2024, Addis-Abeba.

2025

Lancement du *Manuel sur l'élaboration d'une position nationale sur le droit international et les activités cybernétiques : guide pratique à l'intention des États,* 17e Conférence internationale sur les conflits cybernétiques : la prochaine étape (CyCon 2025), 29 mai 2025, Tallinn.

ISBN 978-9916-9227-0-5

2025HASS007