Cyberattaques
Prévention-réactions : rôle des États et des acteurs privés

Karine Bannelier
Maître de conférences-HDR, Université Grenoble Alpes

Théodore Christakis
Professeur, Université Grenoble Alpes/Institut Universitaire de France

Étude préparatoire à la conférence internationale

« Construire la paix et la sécurité internationales de la société numérique »

Acteurs publics, acteurs privés : rôles et responsabilités

Maison de l'UNESCO, Paris, 6 et 7 avril 2017

Association loi 1901 fondée en 1939

Les Cahiers de la Revue Défense Nationale

SGDSN

Agence nationale de la sécurité des systèmes d'information ANSSI

PRENEZ LA PAROLE POUR LA PAIX DANS LE NUMÉRIQUE

EXPERT EN DROIT

UTILISATEUR DU NUMÉRIQUE

Karine BANNELIER

Karine Bannelier est Maître de conférences-HDR en droit international à l'Université Grenoble Alpes et directrice du Master 2 Sécurité internationale et défense dans cette même Université ainsi qu'à l'Institut d'étude des relations internationales de Paris (Ileri). Chercheuse au Centre d'études sur la sécurité internationale et les coopérations européennes (Cesice), elle est fondatrice du Groupe de recherche « Cyber-Nano-Bio : Enjeux des nouvelles technologies pour la sécurité internationale » et cofondatrice d'AMNECYS (Alpine Multidisciplinary Network on Cyber-security Studies) qui est un réseau multidisciplinaire d'experts travaillant dans le domaine de la cybersécurité. Membre du Grenoble Alpes Data Institute, elle est responsable avec Claude Castelluccia du WorkPackage5 Data Governance, Data Protection and Privacy. Ses recherches portent principalement sur le droit international, le droit de la sécurité internationale, la cybersécurité, la gouvernance et la protection des données. Elle participe à différents réseaux internationaux de recherche dans ces domaines comme le Cyber-Terrorism Project de l'Université de Swansea. Elle a été invitée à présenter des communications dans une vingtaine de pays et a publié ou coédité 7 ouvrages et une quarantaine d'articles.

[karine.bannelier@univ-grenoble-alpes.fr]

Théodore CHRISTAKIS

Théodore Christakis est professeur de droit international à l'Université Grenoble Alpes et membre senior de l'Institut Universitaire de France (IUF) où il mène un projet de recherche sur la sécurité nationale et le droit international, dont un important volet est dédié au droit de la cybersécurité. Il est directeur du Centre d'études sur la sécurité internationale et les coopérations européennes (Cesice) et directeur adjoint du Grenoble Alpes Data Institute. Il est fondateur et coresponsable de l'Interest Group on Peace and Security de l'European Society for International Law, membre de l'International Committee on Use of Force de l'International Law Association, membre du Comité éditorial de la Leiden Journal of International Law (Cambridge University Press) et du Conseil scientifique de la Revue Belge de Droit International (RBDI). Il a aussi été membre pendant 12 ans du conseil exécutif et du bureau de la Société française pour le droit international (SFDI). Au cours de ces dernières années il a été professeur invité à l'Australian National University, College of Law; à l'Università degli Studi di Napoli Federico II ; Chuo University, Tokyo ; Kobe University, Graduate School of International Cooperation Studies ; et à l'Académie de droit international de La Haye. Depuis 2005, il enseigne aussi le droit international à la Paris School of International Affairs (Sciences-Po Paris). Il a été invité à présenter ses travaux dans des conférences, colloques et séminaires organisés dans 25 pays, il a publié ou coédité 9 ouvrages et il est l'auteur ou coauteur de plus de 60 articles scientifiques et chapitres d'ouvrages qui portent sur le droit international public, le droit de la sécurité internationale, la protection internationale et européenne des droits de l'homme, le droit de la cybersécurité et la protection des données.

[theodore.christakis@univ-grenoble-alpes.fr]

Contribuez !
https://jesuisinternet.today

Cyberattaques
Prévention-réactions : rôle des États et des acteurs privés

Karine BANNELIER,
Maître de conférences-HDR, Université Grenoble Alpes.
Théodore CHRISTAKIS,
Professeur, Université Grenoble Alpes/Institut universitaire de France.

Préface de Guillaume POUPARD,
Directeur général de l'Agence nationale
de la sécurité des systèmes d'information (ANSSI).

La *Revue Défense Nationale* est éditée par le Comité d'études de défense nationale
(association loi de 1901)
Adresse géographique : École militaire, 1 place Joffre, Paris VII
Adresse postale : BP 8607, 75325 Paris cedex 07
Fax : 01 44 42 31 89 - www.defnat.fr - redac@defnat.com
Directeur de la publication : Alain Coldefy - Tél. : 01 44 42 31 92
Rédacteur en chef : Jérôme Pellistrandi - Tél. : 01 44 42 31 90
Rédactrice en chef adjointe : Audrey Hérisson
Secrétaire général et *webmaster* : Paul Laporte - Tél. : 01 44 42 31 91
Secrétaire général de rédaction : Pascal Lecardonnel - Tél. : 01 44 42 31 90
Assistante de direction : Marie-Hélène Mounet - Tél. : 01 44 42 31 92
Secrétaires de rédaction : Marie-Hélène Mounet, Jérôme Dollé
Abonnements : Éliane Lecardonnel - Tél. : 01 44 42 38 23
Chargé d'études : Laurent Henninger - Tél. : 01 44 42 31 91
Régie publicitaire (ECPAD) : Karim Belguedour - Tél. : 01 49 60 58 56
DL 90757 - 2e trimestre 2017 - ISSN : 2105-7508 - CP n° 1019 G 85493 du 4 décembre 2014
Imprimée par Bialec, 23 Allée des Grands Pâquis, 54180 Heillecourt

Citation suggérée :

Karine BANNELIER et Théodore CHRISTAKIS, *Cyberattaques - Prévention-réactions : rôle des États et des acteurs privés*, Les Cahiers de la Revue Défense Nationale, Paris, 2017.

Préface
De quelle société numérique voulons-nous ?

Le monde s'accorde sur l'idée que le numérique est une chance pour le partage des savoirs ou le développement économique et qu'il modifie en profondeur le fonctionnement de nos sociétés, de nos entreprises et même de nos modes de vie. Tandis que le commerce, l'énergie, les transports ou l'industrie se transforment en tirant parti des communications électroniques ainsi que de capacités de collecte et de traitement des données toujours plus performantes, certains travaillent à l'avènement d'une « humanité augmentée », connectée en profondeur et en permanence, un monde où l'Homme et la technologie fusionneraient.

Le concert des Nations est directement concerné. Le cyberespace est un nouveau milieu qui pose aux États des questions majeures relatives à leur souveraineté, un lieu où il importe d'être présent et de conserver une autonomie d'action, un lieu de conflictualité où les opérations cybernétiques sont de plus en plus amenées à anticiper et accompagner les conflits. Mais les évolutions numériques ont également d'autres effets sur nos sociétés car, si la manipulation des opinions publiques n'est pas un phénomène nouveau, les opportunités nouvelles offertes par le numérique et ses « réseaux sociaux » exposent davantage les citoyens comme leurs dirigeants politiques à une déstabilisation à faible coût mais à fort impact.

L'agence en charge de la sécurité et de la défense des systèmes d'information que je dirige constate, année après année, l'accroissement du nombre d'attaques informatiques mais également de leur sophistication. Les motivations principales restent l'espionnage ou la déstabilisation de cibles précises, qu'il s'agisse d'autorités gouvernementales, de représentants parlementaires, de services publics, d'industries, de médias… Mais on observe également des agressions de plus en plus massives lorsqu'il s'agit d'attaques informatiques génériques visant les entreprises, les professions libérales ou les particuliers, essentiellement à des fins de gain financier par l'escroquerie, le vol ou le chantage. Enfin, la perspective que des groupes terroristes fassent appel à l'utilisation d'attaques informatiques afin de provoquer des catastrophes industrielles ou écologiques et de détruire des vies humaines ne relève malheureusement plus uniquement de l'anticipation à long terme.

Se préparer à ces attaques informatiques, s'en protéger et les contrer lorsqu'elles se produisent, suffit déjà à occuper une large part des ressources publiques et privées de sécurité et de défense des systèmes d'information. Protéger les infrastructures critiques nationales et les opérateurs essentiels au fonctionnement de la société et de l'économie est aujourd'hui une priorité de nations qui doivent

parallèlement réussir leur transition numérique, à commencer par celle de leurs administrations.

Les organisations internationales travaillent chacune selon leur champ de compétence à l'édiction de bonnes pratiques, de règles de comportement ou à la mise en place des mécanismes de coopération qui devraient permettre aux États de lutter contre la cybercriminalité, d'assurer une certaine résilience des infrastructures critiques et d'éviter l'escalade dans un affrontement numérique nécessairement destructeur pour l'ensemble des belligérants. Depuis plusieurs années un accord se dessine sur l'applicabilité du droit international et de ses principes au cyberespace.

Il reste à harmoniser les propositions et à confronter certaines d'entre elles à la réalité technique du numérique. Des pratiques reconnues et encadrées juridiquement ou des raisonnements valides et appliqués dans le monde matériel peuvent trouver leurs limites dans un mode immatériel et, plus encore, dans le monde hybride dans lequel nous entrons.

Apporter une contribution et partager les réflexions en cours à un niveau international est l'objectif de l'initiative prise par le secrétaire général de la défense et de la sécurité nationale (SGDSN) français *via* la mise en ligne d'une plateforme numérique accessible en 11 langues, de séminaires croisant les expertises juridiques et techniques et de la Conférence internationale tenue à la Maison de l'*UNESCO* les 6 et 7 avril 2017.

L'étude remarquable conduite par Karine Bannelier et Théodore Christakis à la fois précède et accompagne ces réflexions. Au moment où certains acteurs majeurs pourraient être tentés de prendre des mesures susceptibles de déstabiliser gravement le cyberespace et les espoirs numériques qu'il porte, où émerge un marché des vulnérabilités informatiques dont l'analogue dans le monde matériel serait de l'avis général parfaitement inacceptable, cette étude donne les bases et perspectives d'un débat qui ne peut être qu'international.

Je remercie les auteurs de cette étude ainsi que la *Revue Défense Nationale* qui en a permis la publication et bien évidemment l'*UNESCO* dont la devise, « Construire la paix dans l'esprit des hommes et des femmes », s'accorde parfaitement aux objectifs de notre initiative.

Guillaume POUPARD,
Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Avant-propos

La présente étude se propose de conceptualiser et de présenter de façon concise les principales questions que posent, du point de vue du droit international, le rôle des États et des acteurs privés dans la prévention et la réaction aux cyberattaques. Elle représente le résultat de recherches conduites par ses auteurs sur les questions relatives à la sécurité de l'espace numérique, la protection des données et de la vie privée. Elle vise à contribuer à la réflexion d'un lecteur averti (expert en droit ou en cybersécurité) tout en souhaitant rester accessible à des non-spécialistes et au grand public afin de dissiper certaines confusions ou erreurs de perception qui pourraient exister à propos du rôle central que le droit international doit avoir dans ce domaine. La sécurité de l'espace numérique, la lutte contre la cybercriminalité, la gouvernance et la protection des données, sont des enjeux majeurs pour la sécurité internationale et nationale. Alors que les organisations internationales, les États et le secteur privé se mobilisent pour adopter de nouvelles normes et codes de conduite dans ce domaine, le droit international existant apporte déjà un grand nombre de réponses pour assurer la coexistence pacifique et la coopération des nations à l'heure du numérique.

Les auteurs souhaitent remercier Katerina Pitsoli, doctorante en droit de la cybersécurité, en cotutelle entre l'Université de Swansea et l'Université Grenoble Alpes, pour son aide en matière de recherche. Ils souhaitent aussi remercier Claude Castelluccia et Cédric Lauradoux (Inria) pour leurs conseils et, de façon plus générale, tous leurs collègues des différentes disciplines qui ont nourri leur réflexion au sein d'*AMNECYS* (*Alpine Multidisciplinary Network on CYbersecurity Studies*) et du *Grenoble Alpes Data Institute*. Toute erreur est bien entendu la nôtre. Les auteurs souhaitent enfin remercier vivement le Comité d'études de défense nationale (CEDN), éditeur de la *Revue Défense Nationale* qui leur a fait l'honneur d'accepter cette étude pour publication dans la collection des *Cahiers de la* RDN.

La présente étude exprime les opinions strictement personnelles de ses auteurs dans le cadre de leurs recherches académiques et n'engage qu'eux.

Introduction :
Sécurité de l'espace numérique et droit international

Cybersecurity is terrible, and will get worse.
Adi SHAMIR (février 2016)

L'essor dramatique des attaques informatiques dans lesquelles sont impliquées des États et des acteurs non-étatiques constitue une véritable menace pour la paix et la sécurité internationales. Dans son rapport de 2015, le Groupe d'experts gouvernementaux des Nations Unies sur la cybersécurité (GGE) [1] exprimait ainsi son inquiétude face à des « tendances préoccupantes » marquées par une hausse spectaculaire du nombre d'actes de malveillance dirigés notamment contre les infrastructures vitales des États [2]. Ce constat alarmant est aujourd'hui partagé par l'ensemble des acteurs du numérique et de la cybersécurité, qu'il s'agisse des États, des organisations internationales ou des acteurs privés [3]. Non seulement ces attaques menacent les infrastructures numériques critiques mais elles constituent aussi une source majeure de tensions entre les États.

En quelques années, l'espace numérique est ainsi devenu un espace de confrontation entre les États mais aussi entre ces derniers et certains acteurs non-étatiques dont les activités déstabilisatrices constituent une préoccupation majeure pour l'ensemble de la communauté internationale. Ainsi que le soulignait le Secrétaire général des Nations Unies, l'« un des problèmes complexes qui est apparu est l'utilisation malveillante croissante de ces technologies par des extrémistes, des terroristes et des groupes criminels organisés » [4]. Le phénomène est d'autant plus complexe à appréhender que certains États entretiennent des liens plus ou moins étroits avec des groupes non-étatiques et les utilisent comme des « intermédiaires », des « *proxies* », pour développer des activités malveillantes contre les intérêts d'autres États [5].

(1) Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale. Ci-après le « GGE ».

(2) « L'environnement informatique mondial présente toutefois des tendances préoccupantes, notamment la hausse spectaculaire du nombre d'actes de malveillance dans lesquels des États ou des acteurs non-étatiques sont impliqués. Ces tendances font courir un risque à tous les États et l'utilisation malveillante des TIC peut compromettre la paix et la sécurité internationales. 4. Plusieurs États développent des capacités dans ce domaine à des fins militaires. La probabilité que les TIC soient utilisées dans des conflits futurs entre États augmente. 5. Les attaques les plus graves qui sont menées à l'aide des TIC comprennent celles qui sont dirigées contre une infrastructure essentielle d'un État et contre les systèmes d'information correspondants. Le risque d'attaque grave de ce type est à la fois réel et sérieux », Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, rapport de 2015, *Note du Secrétaire général*, A/70/174, 22 juillet 2015 (ci-après *GGE 2015*).

(3) Au mois de février 2017, les participants à la Conférence de l'OSCE sur la protection des infrastructures critiques soulignaient encore le caractère crucial pour la paix et la sécurité internationales de la protection des infrastructures vitales contre les cyberattaques. *Cyber Security for Critical Infrastructure: Strengthening Confidence Building in the OSCE*, Vienne, 15 février 2017.

(4) *GGE 2015*, *supra* note 2, §5.

(5) Sur cette question voir *infra*, Partie I (Introduction).

Pourtant, à côté de ce phénomène important et préoccupant pour la paix et la sécurité internationales, les acteurs privés jouent aussi un rôle prépondérant dans la sécurité du numérique. L'activité du secteur privé à cet égard se développe dans pratiquement tous les domaines, de la prévention des cyberattaques et de la sécurisation des infrastructures numériques aux mesures de « cyberdéfense active » qui peuvent parfois aller jusqu'à l'utilisation de techniques offensives comme le « *hacking back* » (6), en passant par l'attribution des cyberattaques (7). Les activités du secteur privé en matière de sécurité du numérique ne vont toutefois pas sans soulever différentes questions et controverses, tant politiques, qu'éthiques, techniques ou juridiques.

L'objet de cette étude est de contribuer à la réflexion sur ces questions en proposant un éclairage sur un aspect important, qui sera sans doute au centre des préoccupations de la communauté internationale dans les années à venir, à savoir le rôle respectif des acteurs publics et des acteurs privés pour la paix et la sécurité du numérique dans le cadre du droit international.

En 2013, les membres du GGE ont en effet reconnu l'application du droit international et notamment de la Charte des Nations Unies à la sécurité du numérique. Cette reconnaissance a constitué une étape importante pour le GGE ainsi que pour la paix et la sécurité du numérique. L'espace numérique n'est pas un espace de non-droit, il peut être régulé par le droit international, comme le sont pratiquement toutes les activités internationales. Mais l'étape qu'il convient maintenant de franchir est infiniment plus complexe. En effet, il s'agit désormais de déterminer de quelle manière le droit international s'applique dans l'espace numérique ce qui, inévitablement, nous renvoie au problème de l'identification et de l'interprétation des règles existantes mais aussi à la question de leur pertinence et de leurs limites dans l'espace numérique.

Or, force est de constater qu'il existe très peu d'instruments juridiques, en droit international, spécialement dédiés à la cybersécurité. Non seulement les conventions internationales dans ce domaine sont rares mais de plus leur emprise est souvent limitée en raison du faible nombre de participants ou du caractère restreint de leur objet (8), la Convention de Budapest sur la cybercriminalité étant sans doute l'instrument conventionnel le plus abouti (9). Dans ce contexte, il convient alors de faire application de règles conventionnelles et coutumières qui n'ont pas été spécifiquement conçues pour réguler le numérique. Le processus qui consiste ainsi à appliquer des règles à des domaines qui n'avaient pas été envisagés

(6) Terme qui désigne, comme nous le verrons, une contre-attaque numérique susceptible d'utiliser des méthodes aussi variées que le « *hacking* » lui-même. Voir Partie III.

(7) Pour toutes ces questions voir Partie III.

(8) La convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel de 2014, par exemple, n'a été pour l'instant ratifiée par aucun État.

(9) Convention de Budapest de 2001 du Conseil de l'Europe sur la cybercriminalité, ratifiée aujourd'hui par 52 États.

lors de leur élaboration n'est pas inhabituel en droit international mais il implique une certaine prudence. Or, le nombre limité de règles internationales contraignantes conçues spécifiquement pour la régulation de l'espace numérique est symptomatique d'un certain retard pris par les États dans ce domaine qui semble être lié à des divergences importantes, notamment à propos de l'opportunité ou non de développer de nouvelles règles conventionnelles en matière de cybersécurité.

Cette situation a laissé le champ libre à différentes initiatives privées allant du refus de toute régulation, « laisser tranquille internet ! », à la promotion d'une autorégulation du numérique par les acteurs privés eux-mêmes. Certains grands acteurs du numérique se sont aussi engagés dans une nouvelle voie qui consiste à proposer des normes pour réguler, non plus seulement leur propre comportement dans une logique d'autorégulation, mais le comportement des États eux-mêmes. L'initiative la plus aboutie est sans doute celle de Microsoft qui, en 2015, a proposé aux États une série de normes de cybersécurité [(10)], suivie par la publication en 2016 d'un document portant sur la mise en œuvre de ces normes et par un appel, en février 2017, à l'adoption d'une nouvelle convention de Genève pour protéger les civils contre les attaques des États sur internet [(11)]. De nombreuses initiatives académiques et doctrinales se sont aussi emparées de la question de l'identification et de l'interprétation du droit international dans l'espace numérique, les réalisations les plus marquantes en matière de sécurité étant les publications des *Manuels de Tallinn 1* et *2* [(12)].

Ce rôle majeur des acteurs privés dans l'espace numérique constitue un bouleversement radical du paysage du droit international et des relations entre acteurs publics et privés.

Traditionnellement, en effet, le droit international est appelé à intervenir pour protéger certaines catégories spécifiques d'acteurs non-étatiques, soit contre les agissements d'États étrangers (protection des étrangers, protection des investissements…), soit contre les agissements des États dont relèvent les acteurs privés (comme en matière de droits de l'homme, de protection des minorités ou de peuples autochtones). Il peut aussi intervenir pour imposer des obligations directement aux acteurs non-étatiques ainsi qu'aux États à l'égard de ces derniers (comme en matière de lutte contre la piraterie ou en matière de prévention et de

(10) Microsoft, *International Cybersecurity Norms, Reducing Conflict in an Internet-Dependent World*, 2015, suivi en 2016, par un document concernant la mise en œuvre par les États de ces normes, Microsoft, *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, 2016 (https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf).

(11) Brad Smith, « The Need for a Digital Geneva Convention », *RSA Conference*, San Francisco, 14 février 2017 (https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/).

(12) Michael N. Schmitt (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013 (ci-après : *Manuel de Tallinn 1*) et M.N. Schmitt (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017 (ci-après : *Manuel de Tallinn 2.0*). Ce dernier manuel vient tout juste de paraître et les auteurs de la présente étude n'ont pu disposer que d'une édition électronique pour consultation.

répression de certains crimes internationaux tels que le crime de génocide, les crimes contre l'humanité, les crimes de guerre, le crime organisé ou encore le terrorisme…). Depuis le 11 septembre 2001, la lutte contre le terrorisme a d'ailleurs propulsé sur le devant de la scène la question de la place des acteurs non-étatiques en droit international ainsi que la question des droits et des obligations des États à leur égard.

Quels que soient les défis posés par ces questions pour le droit international, généralement les rapports entre les États et les acteurs non-étatiques sont restés marqués par un net déséquilibre au profit des États, lié non seulement à la différence de statut juridique entre les premiers (détenteurs de la souveraineté et de pouvoirs importants) et les seconds (« assujettis » aux États) mais aussi en raison de la puissance de fait, des ressources et des capacités d'action des uns et des autres. De fait, l'État est presque toujours apparu comme disposant d'une puissance inégalée lui conférant une prééminence incontestable sur des acteurs privés tantôt dépendants de sa protection (individus, minorités, investisseurs…) tantôt confrontés à ses pouvoirs de régulation, de juridiction et d'exécution [13].

Ce modèle traditionnel est profondément bouleversé dans le domaine de la sécurité de l'espace numérique et ceci alors que le cyberespace constitue un défi majeur en termes de sécurité nationale, comme le soulignent les nombreux États ayant publié ces dernières années leurs « Stratégies de cybersécurité nationale ».

Les grandes entreprises du numérique semblent, en effet, de plusieurs points de vue, tout aussi puissantes que les États – voire parfois davantage –, pour prévenir les cyberattaques, attribuer les actes malveillants et répondre à ceux-ci. Ainsi que le constataient Michael N. Schmitt et Sean Watts :

> « *Classically, states and non-state actors were differentiated not only by disparities in legal status, but also by significant imbalances in resources and capabilities. Not surprisingly, international law developed a state-centric bias to account for these imbalances. Cyberspace and cyber operations, however, have closed a number of formerly significant gaps between states' and non-state actors' abilities to compromise international peace and security. In fact, some non-state actors now match, if not exceed, the cyber capabilities of many states in this respect* » [14].

Les capacités techniques des géants du numérique et leur puissance économique est sans aucune commune mesure avec celles de nombreux pays, notamment les pays moins avancés technologiquement. L'architecture même d'internet semble renforcer cette situation en constituant un défi pour le mode de gouvernance traditionnel « centralisé » des États et semble ainsi favoriser le rôle des acteurs privés du numérique [15]. Les entreprises privées interviennent ainsi de

(13) Ce phénomène de disparité de force de droit et de fait entre les États et les acteurs non-étatiques est particulièrement manifeste dans les domaines par nature « régaliens » comme la protection de la sécurité nationale, la lutte contre le crime organisé ou la conduite de la politique étrangère.

(14) M.N. Schmitt et Sean Watts, « Beyond State-Centrism: International Law and Non-State Actors in Cyberspace », *Journal of Conflict & Security Law*, vol. 21, n° 3, 2016, p. 1 (https://doi.org/10.1093/jcsl/krw019).

(15) Ce qui ne signifie pas pour autant que la gouvernance de la cybersécurité doit suivre exactement la même architecture que la gouvernance de l'internet.

façon croissante en matière de cybersécurité, soit de façon autonome, soit (là où leur action croise fortement les fonctions régaliennes de l'État) conjointement avec des États dans des relations « public/privé » multiformes qui semblent aller bien au-delà des schémas traditionnels. La structure de ces relations et les partenariats complexes entre États et acteurs privés en matière de cyberdéfense et de cyber-attaque ainsi que leurs conséquences sur le plan juridique et politique restent très largement à identifier et à théoriser. Le rôle capital des acteurs privés dans ces domaines est promis pour durer : d'abord parce que ces acteurs sont directement concernés par la cybercriminalité et les cyberattaques, et ils considèrent donc qu'ils doivent se protéger ; ensuite parce qu'internet, les données, l'intelligence artificielle, les objets connectés (*Internet of Things - IoT*), le *cloud* et toutes ces promesses du numérique qui apparaissent jour après jour, présentent un potentiel gigantesque de croissance que les entreprises sont déterminées à défendre et à exploiter. Le marché de la cybersécurité lui-même s'annonce d'autant plus florissant que les menaces pour la sécurité du numérique ne font que croître avec le temps.

Dans ce contexte, il est urgent de mener une réflexion approfondie sur les rôles respectifs des États et des acteurs privés pour la paix et la sécurité du numérique.

Cette réflexion doit tenir compte de l'extrême complexité du problème, marqué par une grande diversité des acteurs impliqués, qu'il s'agisse des auteurs potentiels des cyberattaques (États, « *proxies* », acteurs privés soutenus ou tolérés par les États, terroristes, cybercriminels, entreprises pratiquant l'espionnage ou voulant tirer un avantage concurrentiel, *hackers* individuels, groupements de *hackers* patriotiques…) ; des victimes potentielles des attaques (États, administrations et collectivités, entreprises, médias, individus…) ; des personnes impliquées dans ces attaques (par exemple les États *via* lesquels les cyberattaques transitent, les entreprises et les individus dont les systèmes sont utilisés à leur insu par les attaquants) ; et, enfin, des auteurs éventuels d'une riposte aux cyberattaques (États, entreprises privées agissant pour elles-mêmes, entreprises privées conduisant une riposte pour le compte d'une autre entreprise…). Cette situation crée un nombre impressionnant de combinaisons en fonction desquelles des réponses différentes et appropriées devront être apportées.

Cette réflexion doit aussi tenir compte du caractère très souvent international ou transnational des cyberattaques qui fait de cette problématique presque naturellement une problématique relative au droit international.

L'objet de notre étude est précisément de présenter les principales réponses que le droit international apporte aujourd'hui à ces questions. Nous adopterons volontairement ici une définition large du terme « cyberattaque » [(16)] pour examiner

(16) Voir en détail *infra*, Partie II (Introduction).

quels doivent être les rôles des États et des acteurs privés en matière de prévention et de riposte aux cyberattaques.

Dans une première partie, nous mettrons l'accent sur les enjeux de la prévention et montrerons que le concept de « cyber-diligence », que nous avons forgé sur la base du droit international existant et de l'obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États, apporte une réponse utile à la question de la vigilance que les États devraient avoir à l'égard des cyber-opérations développées depuis leur territoire par des acteurs privés (I).

Dans une deuxième partie, nous nous pencherons sur les réponses aux cyberattaques qui peuvent être développées de façon conforme au droit international. Nous procéderons pour cela à une classification des réactions possibles aux cyberattaques et proposerons une sorte de « mode d'emploi » pour des États victimes d'attaques qui souhaitent réagir dans les limites de la légalité internationale (II).

Enfin, dans une troisième partie, nous présenterons une étude détaillée des questions relatives au « *hack-back* » et à la « cyberdéfense active ». Après avoir analysé les avantages, les inconvénients et les risques du *hack-back*, nous répondrons à la question de savoir si les acteurs privés peuvent déclencher unilatéralement des mesures cyber-offensives en conformité avec le droit et dans quelle mesure les États peuvent autoriser le *hack-back* et/ou s'appuyer sur des acteurs privés pour conduire des contre-attaques (III).

PARTIE I. Cyber-diligence : un concept clef face aux actes malveillants transnationaux

Introduction

A) Le fait d'une personne privée comme fait de l'État

B) L'« obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États »

1. « Qui peut et n'empêche, pèche » : le concept de cyber-diligence

A) La souveraineté des États au cœur du concept de cyber-diligence

B) La responsabilité des États à l'égard des attaques transnationales et des dommages causés à des États tiers

C) L'utilité du concept de cyber-diligence face aux cyberattaques

2. La cyber-diligence comme norme de comportement responsable et raisonnable

A) Une obligation de comportement et non de résultat

B) Une obligation fondée sur le principe de responsabilité commune mais différenciée ?

3. Un devoir de prévenir et de réagir aux cyberattaques

A) Prévention des cyberattaques et protection des infrastructures critiques numériques

B) Notification et répression des cyberattaques

I. Cyber-diligence : un concept clef face aux actes malveillants transnationaux

Introduction

Le constat du développement croissant dans l'espace numérique de cyber-attaques et de mesures de *hack-back* relevant d'acteurs privés est souvent associé à l'idée selon laquelle les États n'assumeraient aucune obligation ni responsabilité internationale vis-à-vis de tels actes « privés ». L'idée est pourtant largement erronée et semble reposer sur une double incompréhension concernant à la fois l'espace numérique et le droit international qui s'y applique.

Une première source d'erreur vient d'une représentation de l'espace numérique comme ne connaissant ni territoires ni frontières déterminés. En réalité, l'infrastructure physique qui supporte internet, les activités numériques qui s'y développent et les données qui circulent se situent en grande partie sur le territoire des États souverains ou sous leur contrôle [(17)]. La territorialité de l'espace numérique a d'ailleurs été clairement reconnue par les membres du Groupe gouvernemental d'experts des Nations Unies sur la cybersécurité dans leur rapport de 2015 où ils soulignent que « la compétence territoriale des États s'applique aux infrastructures informatiques situées sur leur territoire » [(18)]. Il est ainsi admis que la compétence territoriale des États s'exerce quelles que soient la nature et l'origine des activités, qu'il s'agisse d'activités physiques ou numériques, d'origine publique, privée, nationale ou étrangère.

Une deuxième source d'erreur est de penser que le droit international est muet dès lors que les activités sont d'origine privée, le droit international n'étant supposé réguler que les relations interétatiques. Le droit international est pourtant très clair à cet égard, il s'agit même de l'un de ses piliers : les États, du fait de leur souveraineté, ont des obligations à l'égard des activités privées qui se déroulent sur leur territoire, sous leur juridiction ou sous leur contrôle et ils peuvent, dans certaines hypothèses, être tenus responsables de ces activités.

Ces hypothèses ont été identifiées par la Commission du droit international des Nations Unies (CDI) dans ses articles sur *La responsabilité internationale de l'État pour fait internationalement illicite* adoptés par l'Assemblée générale de

(17) Comme le soulignait en effet Harold H. Koh, « *The physical infrastructure that supports the Internet and cyberactivities is generally located in sovereign territory and subject to the jurisdiction of the territorial State* », *in* H. H. Koh, « International Law in Cyberspace », United States Cyber Command Inter-Agency Legal Conference, Fort Meade, MD, 18 septembre 2012, *Harvard International Law Journal Online*, vol. 54, 2012, p. 6 (www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf).

(18) *GGE 2015*, *supra* note 2, §28 (a).

l'ONU en 2001 [19] et par la jurisprudence internationale. Il existe principalement deux hypothèses où l'État peut être tenu responsable de la conduite de personnes privées. Il s'agit tout d'abord de l'hypothèse où les actes des personnes privées sont considérés comme les actes de l'État lui-même (A) ; il s'agit ensuite de la violation par l'État lui-même de son obligation « de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États » [20] (B).

A) Le fait d'une personne privée comme fait de l'État

Le fait d'une personne privée peut, sous certaines conditions, devenir le fait de l'État et engager sa responsabilité. Deux situations doivent particulièrement retenir notre attention pour la question qui nous occupe : il s'agit, tout d'abord, de la situation où des personnes privées (physiques ou morales) « agissent sur les instructions ou les directives ou sous le contrôle de cet État » [21] ; il s'agit ensuite de la situation où l'État « reconnaît et adopte ledit comportement comme sien » [22]. Dans ces deux situations, les dommages causés à des États tiers du fait des activités de ces personnes privées sont considérés comme une violation du droit international par l'État lui-même [23].

Dans l'espace numérique, le recours à des personnes privées sous la forme d'« intermédiaires » ou de « *proxies* » est une pratique répandue chez certains États qui cherchent ainsi à développer différentes opérations de manière clandestine [24]. En 2013 déjà, le rapport du GGE s'était fait l'écho des préoccupations de la communauté internationale à cet égard en affirmant que : « [l]es États sont tenus d'honorer leurs obligations internationales quant aux faits internationalement illicites qui leur sont imputables. Ils s'interdisent d'utiliser leurs agents pour commettre de tels actes et veillent à ce que des agents non-étatiques n'utilisent pas leur territoire pour faire un usage illégal des outils informatiques » [25]. Dans son rapport de 2015, le GGE a réitéré avec force cette affirmation en soulignant que « [l]es États sont tenus de remplir leurs obligations internationales quant aux faits

(19) Commission du droit international, « Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite et commentaires y relatifs », *Annuaire de la Commission du droit international 2001*, vol. II. Part. 2 (ci-après *ACDI 2001*).

(20) Cour internationale de justice, *Affaire du Détroit de Corfou*, Arrêt du 4 avril 1949, *CIJ Recueil 1949*, p. 22.

(21) Article 8 – Comportement sous la direction ou le contrôle de l'État : « Le comportement d'une personne ou d'un groupe de personnes est considéré comme un fait de l'État d'après le droit international si cette personne ou ce groupe de personnes, en adoptant ce comportement, agit en fait sur les instructions ou les directives, ou sous le contrôle de cet État », *ACDI 2001*, *supra* note 19, p. 26.

(22) Art. 11 – Comportement reconnu et adopté par l'État comme étant le sien : « Un comportement qui n'est pas attribuable à l'État selon les articles précédents est néanmoins considéré comme un fait de cet État d'après le droit international si, et dans la mesure où cet État reconnaît et adopte ledit comportement comme sien », *ibid.*, p. 27.

(23) Voir à cet égard nos analyses *infra* Partie III.

(24) De nombreuses études ont été consacrées à ce phénomène, parmi les plus récentes, voir par exemple, Tim Maurer, « 'Proxies' and Cyberspace », *Journal of Conflict & Security Law*, vol. 21, n° 3, 2016, p. 383-403.

(25) Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, Note du Secrétaire général, A/68/98, 24 juin 2013, §23. (ci-après : *GGE 2013*).

internationalement illicites qui leur sont imputables en droit international » [26] et qu'ils « (…) ne doivent pas faire appel à des intermédiaires pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications » [27].

L'attribution aux États des actes de ces personnes privées reste pourtant une opération sensible et délicate. Il est rare en effet qu'un État reconnaisse et adopte comme étant le sien le comportement de ces personnes. Par ailleurs, le nombre et la diversité des personnes privées développant des activités dans l'espace numérique, l'intensité variable des liens qu'elles entretiennent avec les États, rendent l'imputation à l'État des comportements de ces personnes privées en vertu d'instructions, de directives ou du contrôle particulièrement difficile à établir [28]. Cette opération est d'autant plus délicate dans l'espace numérique que le fait de localiser l'origine d'un acte sur un territoire précis ne suffit pas à imputer l'acte en question à l'État. Ainsi que l'a souligné le GGE dans son rapport de 2015, « (…) le signe qu'une activité informatique a été lancée depuis le territoire ou une infrastructure informatique d'un État, ou y trouve son origine, peut être insuffisant à lui seul pour imputer l'activité en question à cet État » [29]. La question de savoir quel est le degré de certitude exigé pour établir l'imputation d'une cyberattaque à un État est aussi évidemment une question cruciale, le rapport du GGE de 2015 faisant observer que « les accusations d'organiser et d'exécuter des actes illicites portées contre des États devaient être étayées » [30]. Dans la deuxième partie de cette analyse, nous verrons quelles sont les preuves qu'un État doit fournir avant de réagir à une cyberattaque et quel est le degré de certitude exigé par le droit international (*infra* Partie II). Quoi qu'il en soit, l'hypothèse selon laquelle le fait d'une personne privée est considéré comme le fait de l'État pourrait parfois être difficile à mettre en œuvre dans l'espace numérique.

B) L'« obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États »

Les États peuvent aussi être tenus responsables des actes de personnes privées en vertu de l'« obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États » [31]. Cette obligation, exprimée par la Cour internationale de justice dans l'Arrêt du *Détroit de Corfou*,

(26) *GGE 2015*, *supra* note 2, §28 (f), nous soulignons.

(27) *Ibid.*, §28 (e).

(28) Voir notamment sur cette question, M.N. Schmitt et Liis Vihul, « Proxy Wars in Cyber Space: The Evolving International Law of Attribution », *Fletcher Security Review*, vol. I, n° 2, été 2014, p. 55-73 ; Kubo Macak, « Decoding Article 8 of the International Law Commission's Article on State Responsibility: Attribution of Cyber Operations by Non-State Actors », *Journal of Conflict & Security Law*, vol. 21, n° 3, 2016, p. 405-428.

(29) *GGE 2015*, *supra* note 2, §28 (f).

(30) *Ibid.*

(31) *Affaire du Détroit de Corfou*, *op. cit.*, p. 22.

s'intéresse directement à la responsabilité des États en raison d'actes des personnes privées et ceci quelles que soient les relations entre l'État et les personnes privées et quels que soient les actes en question, qu'il s'agisse de cyberattaques, de mesures de *hack-back* ou de toute autre activité. Cette obligation est une obligation de « vigilance », de *due diligence* qui découle directement de la souveraineté des États.

Le concept de cyber-diligence (32) qui exprime cette obligation peut jouer un rôle central dans le développement de la paix et de la sécurité internationales dans l'espace numérique (1). Il indique en effet un standard de comportement raisonnable et responsable des États (2) pour prévenir et faire cesser des cyberattaques lancées par des acteurs privés depuis leur territoire ou leurs infrastructures numériques contre le territoire ou les infrastructures d'autres États (3).

1. « Qui peut et n'empêche, pèche » : le concept de cyber-diligence

« Qui peut et n'empêche, pèche » (33), l'adage d'Antoine Loysel, jurisconsulte français du XVII^{e} siècle, célèbre pour avoir collecté les règles coutumières du Royaume de France, traduit bien ce que le concept de cyber-diligence exprime au XXI^{e} siècle à l'égard des États souverains dans l'espace numérique : intervenir, quand ils le peuvent, pour empêcher des actes portant atteinte aux droits d'États tiers.

A) La souveraineté des États au cœur du concept de cyber-diligence

Dans l'espace numérique, la responsabilité qui incombe aux États d'intervenir, quand ils le peuvent, découle directement de leur souveraineté sur les infrastructures situées sur leur territoire. Comme le soulignaient les membres du GGE dans leur rapport de 2015, « [l]es normes et principes internationaux qui procèdent de la souveraineté étatique s'appliquent à l'utilisation de l'outil informatique par les États ainsi qu'à leur compétence territoriale en matière d'infrastructure informatique » (34).

Aux « normes et principes » qui découlent de la souveraineté étatique sont en effet associés des droits au bénéfice des États mais aussi, corollairement, des devoirs à la charge des États. Cette étroite corrélation entre les droits et les devoirs des États souverains a été très justement exprimée par la Sentence arbitrale rendue

(32) Ce terme a été utilisé dans l'article de Karine Bannelier, « Cyber-Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber-Operations? », *Baltic Yearbook of International Law*, vol. 14, 2014, p. 23-39.

(33) Antoine Loysel, *Institutes coustumieres, ou manuel de plusieurs et diverses reigles, sentences, et prouerbes, tant anciens que modernes, du droict coustumier et plus ordinaire de la France*, A. L'Angelier, Paris, 1607 (https://archive.org/details/1607LoiselInstitutesCoutumieres).

(34) *GGE 2015*, *supra* note 2, §27. En 2013 déjà, le rapport du GGE soulignait que « La politique des États en matière informatique et leur compétence territoriale pour ce qui est des infrastructures informatiques présentes sur leur territoire relèvent de la souveraineté des États et des normes et principes internationaux qui en découlent », Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, A/68/98, 24 juin 2013, §20.

en 1928 dans l'*Affaire de l'île de Palmas*. Selon celle-ci, « la souveraineté territoriale implique le droit exclusif d'exercer les activités étatiques. Ce droit a pour corollaire un devoir : l'obligation de protéger à l'intérieur du territoire, les droits des autres États, en particulier leur droit à l'intégrité et à l'inviolabilité en temps de paix et en temps de guerre » (35).

Les États souverains ont donc le droit au respect de leur intégrité territoriale mais ils ont aussi, en miroir de ce droit, un devoir, celui de ne pas utiliser/ou de ne pas laisser utiliser leur territoire de manière à porter atteinte au droit au respect de l'intégrité territoriale d'un autre État : *sic utere tuo ut alienum no laedas* (36). Comme le soulignait déjà en 1925 la sentence arbitrale rendue dans l'*Affaire des réclamations britanniques dans la zone espagnole du Maroc* : « [l]a responsabilité pour les événements de nature à affecter le droit international, se passant dans un territoire déterminé, va de pair avec le droit d'exercer à l'exclusion d'autres États les prérogatives de la souveraineté » (37).

Le devoir d'utilisation non-dommageable du territoire a été depuis réaffirmé à de maintes reprises par le juge international, son expression la plus fameuse étant sans doute le *dictum* de la Cour internationale de justice dans l'Arrêt du *Détroit de Corfou*, à savoir l'« obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États » (38).

En vertu de leur souveraineté, les États ont donc une obligation de vigilance, de *due diligence*, à l'égard des activités se déroulant sur leur territoire ou sur leur contrôle et, en cas de manquement à cette obligation, ils peuvent, sous certaines conditions, être considérés comme responsables des atteintes portées aux droits d'États tiers.

B) La responsabilité des États à l'égard des attaques transnationales et des dommages causés à des États tiers

Dans l'Arrêt du *Détroit de Corfou*, la CIJ a condamné l'Albanie pour avoir manqué à son obligation de vigilance car des mines sous-marines posées dans ses eaux territoriales avaient causé des dommages à des navires britanniques. Dans cet arrêt, le juge n'a pas condamné l'Albanie pour avoir elle-même posé ces mines, il a juste affirmé que l'Albanie était responsable des dommages causés au Royaume-Uni dans la mesure où, ayant nécessairement eu connaissance de la situation, l'Albanie n'avait pas pris les mesures raisonnables en son pouvoir pour prévenir le dommage.

(35) Cour permanente d'arbitrage, *Affaire de l'île de Palmas, États-Unis c. Pays-Bas*, Sentence arbitrale du 4 avril 1928, *Recueil des sentences arbitrales* (*RSA*), vol. II, p. 839.

(36) « Fait usage de ta propriété de manière à ne pas porter atteinte à celle d'un autre ».

(37) *Réclamations britanniques dans la zone espagnole du Maroc, Grande-Bretagne c. Espagne*, Sentence arbitrale du 1er mai 1925, *RSA*, vol. II, p. 649.

(38) *Affaire du Détroit de Corfou*, *op. cit.*, p. 22.

Cette obligation de vigilance qui découle de la souveraineté des États s'impose ainsi aux États quels que soient les auteurs de ces activités, qu'il s'agisse de personnes publiques ou privées, nationales ou étrangères. Il est à cet égard important de souligner que, historiquement, cette obligation de vigilance s'est tout d'abord développée en lien avec la responsabilité des États pour des activités privées (39). La première application connue de cette obligation par le juge international concernait en effet la responsabilité d'un État, le Royaume-Uni, pour des actes de compagnies privées. Dans l'*Affaire de l'Alabama*, le Royaume-Uni fut condamné pour avoir violé son obligation de *due diligence* en laissant des entreprises privées construire et armer, sur son territoire, le navire *Alabama* destiné à servir dans l'armée des Confédérés contre l'Union durant la guerre de Sécession aux États-Unis (40).

Depuis lors, le principe de *due diligence* a été appliqué par le juge international à propos d'activités et dans des domaines très divers, qu'il s'agisse du droit de la mer (41), des droits de l'homme (42), de protection de l'environnement (43) ou encore de protection des individus, des diplomates et des États étrangers contre des insurrections et des attaques transfrontières lancées par des groupes non-étatiques (44). C'est ainsi par exemple que, dans l'*Affaire des activités armées sur le territoire du Congo* opposant la République démocratique du Congo (RDC) à l'Ouganda, l'Ouganda affirmait, en se fondant notamment sur l'arrêt du Détroit de Corfou, que la RDC avait violé son obligation de *due diligence* en n'empêchant pas des groupes armés de lancer depuis son territoire des attaques contre l'Ouganda (45). Si la Cour internationale de justice a finalement refusé de considérer que l'incapacité dans laquelle se trouvait la RDC de mettre fin à ces attaques constituait, en l'espèce, une violation de son obligation de vigilance, la Cour, comme d'ailleurs la RDC, ont admis qu'une telle obligation s'imposait aux États dans le cadre d'attaques transfrontières menées par des acteurs non-étatiques (46).

(39) Voir Timo Koivurova, « *Due diligence* », *Max Planck Encyclopedia of Public International Law* (www.mpepil.com).

(40) *Réclamations des États-Unis d'Amérique contre la Grande-Bretagne relatives à l'Alabama*, Sentence rendue le 14 septembre 1872 par le tribunal d'arbitrage constitué en vertu de l'article I du Traité de Washington du 8 mai 1871, ONU, *RSA*, vol. XXIX, p. 130.

(41) Voir par exemple, Tribunal international du droit de la mer, *Responsabilités et obligations des États dans le cadre d'activités menées dans la Zone*, Avis consultatif, 1er février 2011, *TIDM Recueil 2011*, p. 10.

(42) Voir par exemple Cour européenne des droits de l'homme, *Affaire Osman c. Royaume-Uni*, Arrêt du 28 octobre 1998, CEDH 1998-VIII.

(43) Voir par exemple, *Affaire de la fonderie du Trail*, Sentence arbitrale du 11 mars 1941, *RSA*, vol. III, p. 907 ou *Affaire des usines de pâte à papier sur le fleuve Uruguay (Argentine c. Uruguay)*, arrêt du 20 avril 2010, *Recueil CIJ 2010*, p. 14.

(44) Voir par exemple *Thomas H. Youmans (USA) v. United Mexican State*, 23 novembre 1926, ONU, *Reports of International Arbitral Awards*, vol. 4. Voir aussi, par exemple, *Affaire du personnel diplomatique et consulaire des États-Unis à Téhéran (États-Unis c. Iran)*, Arrêt du 24 mai 1980, *CIJ Recueil 1980*, p. 3.

(45) *Affaire des activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda)*, Arrêt du 19 décembre 2005, *CIJ Recueil 2005*, §277.

(46) *Ibid.*, §283 et 300-303.

C) L'utilité du concept de cyber-diligence face aux cyberattaques

L'obligation de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États s'impose ainsi aux États quel que soit l'auteur de l'activité mais aussi quelle que soit la nature de l'activité concernée, qu'il s'agisse d'une activité de haute ou de basse technologie, numérique ou physique. En 2001 déjà, la Commission du droit international des Nations Unies, dans son projet d'articles sur la *Prévention des dommages transfrontières résultant d'activités dangereuses* (47), avait insisté sur le fait que le devoir de diligence qui incombe aux États à l'égard des activités dites dangereuses s'impose pour toutes les activités à partir du moment où elles comportent un risque de causer un dommage transfrontière significatif (48). Dans son commentaire de l'article 1, la Commission expliquait ainsi qu'elle refusait de dresser une liste de ces activités au motif qu'une telle liste serait immédiatement dépassée en raison de l'évolution rapide des technologies (49).

Les activités développées dans l'espace numérique n'échappent ainsi pas à la règle. Dans son rapport de 2015, le GGE, sans nommer expressément le concept de cyber-diligence, l'exprime en plusieurs endroits. Il affirme notamment que les États « devraient veiller à ce que des acteurs non-étatiques n'utilisent pas leur territoire pour commettre des faits internationalement illicites à l'aide des technologies de l'information » (50) et qu'ils « ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide de technologies de l'information et des communications » (51).

La question n'est donc pas de savoir si les États ont, ou non, une obligation de ne pas laisser leurs infrastructures numériques être utilisées par des acteurs privés pour conduire des cyberattaques contre d'autres États, car il est clair que l'obligation existe. La question est plutôt de savoir jusqu'où et comment cette obligation s'impose aux États dans l'espace numérique et à partir de quel moment on peut considérer qu'un État « peut mais n'empêche » et engage de ce fait sa responsabilité internationale.

2. La cyber-diligence comme norme de comportement responsable et raisonnable

L'obligation d'utilisation non-dommageable du territoire telle qu'exprimée par la Cour internationale de justice est une obligation dite de *due diligence* qui

(47) CDI, « Projet d'articles sur la prévention des dommages transfrontières résultant d'activités dangereuses et commentaires y relatifs », *Annuaire de la Commission du droit international*, vol. II, n° 2, 2001, p. 405 et s.

(48) *Ibid.*, Article 1, p. 409.

(49) *Ibid.* Voir aussi à cet égard la position de la CIJ dans l'*Affaire des usines de pâte à papier sur le fleuve Uruguay* selon laquelle l'obligation de diligence s'appliquait « vis-à-vis de toutes les activités qui se déroulent sous la juridiction et le contrôle de chacune des parties », *Affaire des usines de pâte à papier sur le fleuve Uruguay*, *op. cit.* §197.

(50) *GGE 2015*, *supra* note 2, §28 (e).

(51) *Ibid.*, §13 (c).

désigne ainsi une obligation de comportement et non une obligation de résultat. C'est là une caractéristique fondamentale de l'obligation qui est unanimement acceptée et qui n'a jamais fait l'objet d'une quelconque remise en cause. Elle exige que les États soient, selon leurs capacités respectives, raisonnablement vigilants à l'égard des activités qui se développent sur leur territoire.

A) Une obligation de comportement et non de résultat

L'exercice par les États de leur souveraineté territoriale ne signifie donc pas que les États doivent nécessairement savoir tout ce qui se passe sur leur territoire ni qu'ils soient en capacité de pouvoir tout empêcher. Le degré de vigilance attendu est celui « d'un bon gouvernement » (52). Toutes les juridictions internationales et tous les organes internationaux qui ont eu à interpréter et à appliquer le principe de *due diligence* affirment que c'est le critère du « raisonnable » qui doit guider son application et qu'il ne peut « imposer aux autorités un fardeau insupportable ou excessif » (53).

Cela signifie, tout d'abord, que la connaissance par un État d'une cyber-attaque lancée par des personnes privées depuis ses infrastructures contre un État tiers ne peut être présumée. Comme l'a bien souligné la Cour internationale de justice dans l'*Affaire du Détroit de Corfou* : « on ne saurait conclure du seul contrôle exercé par un État sur son territoire terrestre ou sur ses eaux territoriales que cet État a nécessairement connu ou dû connaître tout fait illicite international qui y a été perpétré non plus qu'il a nécessairement connu ou dû connaître ses auteurs » (54). Mais inversement, il va aussi de soi que les États souverains ne peuvent pas, raisonnablement, méconnaître tout ce qui se passe sur leur territoire. Comme l'a souligné la Cour internationale de justice dans cette même affaire, « un État, sur le territoire duquel s'est produit un acte contraire au droit international, peut être invité à s'en expliquer. Il est également vrai qu'il ne peut se dérober à cette invitation en se bornant à répondre qu'il ignore les circonstances de cet acte ou ses auteurs. Il peut, jusqu'à un certain point, être tenu de fournir des indications sur l'usage qu'il a fait des moyens d'information et d'enquête à sa disposition » (55).

Une question délicate, qui se pose avec une particulière acuité dans l'espace numérique, est de déterminer dans quelle mesure un État souverain « doit savoir », « devrait savoir » ou « devrait chercher à savoir » et ceci notamment en surveillant les activités qui se déroulent sur son territoire. Cette relation étroite entre connaissance et surveillance a déjà été largement abordée par le juge

(52) CDI, « Projet d'articles sur la prévention des dommages transfrontières résultant d'activités dangereuses et commentaires y relatifs », *op. cit.*, §17, p. 425.

(53) Cour européenne des droits de l'homme, *Affaire Osman c. Royaume-Uni*, Arrêt du 28 octobre 1998, §116.

(54) *Affaire du Détroit de Corfou*, *op. cit.*, p. 18.

(55) *Ibid*.

international, notamment en matière de droits de l'homme dans le cadre des « obligations positives » des États [56] et en matière de protection de l'environnement [57].

Il ressort que les États doivent sans doute exercer un contrôle sur les activités qui se développent sur leur territoire. Ceci ne signifie pas pour autant qu'ils soient autorisés à user d'un tel prétexte afin de développer une surveillance de masse et à éroder les libertés essentielles en commençant par le droit à la vie privée et au respect des correspondances. Comme l'a souligné la Cour internationale de justice dans l'affaire *Application de la Convention pour la prévention et la répression du crime de génocide*, « il est clair que chaque État ne peut déployer son action que dans les limites de ce que lui permet la légalité internationale » [58]. À cet égard, les membres du GGE, dans leur rapport de 2013, ont rappelé la nécessité pour les États de respecter les droits fondamentaux de la personne : « Les actions entreprises par les États pour assurer la sécurité informatique doivent se faire dans le respect des droits de l'homme et des libertés fondamentales énoncés dans la Déclaration universelle des droits de l'homme et dans les autres instruments internationaux » [59]. En 2015, les membres du GGE sont revenus sur cette question fondamentale pour la sécurité du numérique en soulignant « l'importance centrale » du respect par les États des droits de l'homme et des libertés fondamentales et le fait que « [l]es États, lorsqu'ils veillent à une utilisation sûre des technologies de l'information et des communications, devraient respecter les résolutions 20/8 et 26/13 du Conseil des droits de l'homme sur la promotion, la protection et l'exercice des droits de l'homme sur internet, ainsi que les résolutions 68/167 et 69/166 de l'Assemblée générale sur le droit à la vie privée à l'ère du numérique afin de garantir le plein respect des droits de l'homme, y compris le droit à la liberté d'expression » [60].

Le critère du raisonnable permet non seulement d'évaluer dans quelle mesure les États ont, ou devraient avoir, connaissance des activités qui se déroulent sur leur territoire, il permet aussi de déterminer si un État a fourni ses « *best efforts* », a pris toutes les mesures qui sont à sa disposition, pour prévenir ou empêcher l'atteinte aux droits d'un État tiers. Le fait qu'un État échoue finalement et ne parvient pas à empêcher une telle atteinte ne constitue pas, en effet, en tant que tel

(56) Comme l'a dit la Cour européenne des droits de l'homme dans l'*Affaire Osman c. Royaume-Uni*, « face à l'allégation que les autorités ont failli à leur obligation positive… il lui faut se convaincre que lesdites autorités savaient ou auraient du savoir sur le moment qu'un ou plusieurs individus étaient menacés de manière réelle et immédiate dans leur vie du fait des actes criminels d'un tiers, et qu'elles n'ont pas pris, dans le cadre de leurs pouvoirs, les mesures qui, d'un point de vue raisonnable, auraient sans doute pallié ce risque », CEDH, *Osman c. Royaume-Uni*, *op. cit.*, §116.

(57) Dans l'*Affaire des usines de pâte à papier sur le fleuve Uruguay*, la Cour internationale de justice a ainsi estimé que l'obligation de prévention impliquait « le contrôle administratif des opérateurs publics et privés, par exemple en assurant la surveillance des activités entreprises par ces opérateurs, et ce, afin de préserver les droits de l'autre partie », *Affaire des usines de pâte à papier sur le fleuve Uruguay*, *op. cit.*, §197.

(58) *Affaire relative à l'application de la convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c. Serbie-et-Monténégro)*, Arrêt du 26 février 2007, *Recueil CIJ 2007*, §430.

(59) Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, A/68/98, 24 juin 2013, §21.

(60) *GGE 2015*, *supra* note 2, §13 (e).

une violation de l'obligation de vigilance. Ainsi que l'a exprimé la CIJ dans l'affaire *Application de la Convention pour la prévention et la répression du crime de génocide* : « (…) on ne saurait imposer à un État quelconque l'obligation de parvenir à empêcher quelles que soient les circonstances, la commission d'un génocide : l'obligation qui s'impose aux États parties est plutôt celle de mettre en œuvre tous les moyens qui sont raisonnablement à leur disposition en vue d'empêcher, dans la mesure du possible, le génocide. La responsabilité d'un État ne saurait être engagée pour la seule raison que le résultat recherché n'a pas été atteint ; elle l'est, en revanche, si l'État a manqué manifestement de mettre en œuvre les mesures de prévention du génocide qui étaient à sa portée, et qui auraient pu contribuer à l'empêcher. En la matière, la notion de "*due diligence*" qui appelle une appréciation *in concreto*, revêt une importance cruciale » (61).

Au regard de la complexité de l'espace numérique et de la rapidité des activités qui s'y déploient, cette obligation n'impose donc évidemment pas aux États d'empêcher toutes les cyberattaques. Une évaluation des circonstances de l'espèce et des capacités de chacun est nécessaire.

B) Une obligation fondée sur le principe de responsabilité commune mais différenciée ?

Concrètement, plusieurs critères peuvent permettre de déterminer la capacité d'un État à l'égard de ses obligations de diligence dans l'espace numérique. Ces critères concernent à la fois les circonstances de chaque cas d'espèce et la capacité de chaque État qui, comme l'a bien remarqué le juge international, « varie grandement d'un État à l'autre » (62). Dans ses travaux sur la prévention des dommages transfrontières, la Commission du droit international des Nations Unies a souligné que « [l]e niveau économique des États est un des facteurs à prendre en considération pour déterminer si un État s'est acquitté de son devoir de diligence » (63). À côté de ce critère économique, il est clair que, dans l'espace numérique, l'obligation faite aux États de prendre toutes les mesures raisonnables doit être aussi évaluée en fonction du niveau et des capacités technologiques de chacun. Tous les États ne disposent pas en effet des mêmes capacités pour protéger leurs réseaux informatiques contre des utilisations malveillantes. Le concept de cyber-diligence implique donc le principe de responsabilité commune mais différenciée entre les États. Cette responsabilité est différenciée car les États sont inégaux, sur le plan

(61) *Application de la Convention pour la prévention et la répression du crime de génocide*, *op. cit.*, §430.

(62) *Ibid*. Dans l'affaire de l'*Alabama*, les États-Unis définissaient déjà la *due diligence* comme : « Une diligence proportionnée à l'importance du sujet, à la dignité et à la force du pouvoir qui l'exerce », *Réclamations des États-Unis d'Amérique contre la Grande-Bretagne relatives à l'Alabama*, *in* J.-B. Moore, *International Arbitrations to which the United States has been Party*, vol. 1, p. 572-573.

(63) CDI, « Projet d'articles sur la prévention des dommages transfrontières résultant d'activités dangereuses et commentaires y relatifs », *op. cit.*, Article 3, commentaire §13, p. 424. La Commission explique ainsi qu'« il est cependant entendu que le degré de vigilance attendu d'un État dont l'économie et les ressources humaines et matérielles sont bien développées et qui est doté de systèmes et de structures étatiques très élaborés est différent de celui attendu d'États moins bien lotis » Art. 3, commentaires §17, p. 425-426.

économique comme technologique, mais elle est aussi commune car, en raison de l'interconnexion qui caractérise le monde numérique, les vulnérabilités des infrastructures essentielles d'un État peuvent avoir des conséquences graves pour d'autres États. Ainsi que le soulignait le GGE en 2013, « Les différences d'un État à l'autre en termes de capacités à assurer la sécurité informatique peuvent aggraver la vulnérabilité d'un monde interconnecté » (64).

Par ailleurs, il convient de rappeler que, quelles que soient ces inégalités, les États sont souverains et, comme l'a bien souligné la CDI, « une certaine vigilance est censée être exercée dans l'utilisation des infrastructures et la surveillance des activités dangereuses sur le territoire de l'État, ce qui est un attribut naturel de tout gouvernement » (65).

3. Un devoir de prévenir et de réagir aux cyberattaques

Dans l'*Affaire du personnel diplomatique et consulaire des États-Unis à Téhéran*, la CIJ a engagé la responsabilité internationale de l'Iran pour la prise en otage des personnels diplomatiques et consulaires car les autorités iraniennes n'avaient, notamment, pris aucune mesure pour prévenir ou réagir à cette prise d'otages. En effet, selon la Cour, les autorités iraniennes « b) étaient pleinement conscientes, du fait des appels a l'aide de l'ambassade des États-Unis, que des mesures urgentes de leur part s'imposaient ; c) disposaient des moyens de s'acquitter de leurs obligations ; d) ont totalement manqué de se conformer auxdites obligations » (66). Les obligations de prévenir les atteintes aux droits des États tiers et d'y réagir découlent de l'obligation de vigilance et s'imposent de ce fait à l'ensemble des États. Il convient toutefois de s'interroger sur les mesures concrètes que les États devraient ou pourraient raisonnablement prendre pour prévenir l'utilisation de leurs infrastructures numériques par des personnes privées pour lancer des cyberattaques (A) et pour réagir à ces attaques (B).

A) Prévention des cyberattaques et protection des infrastructures critiques numériques

Dans l'*Affaire de l'Alabama*, le tribunal a considéré que « *the British government failed to use due diligence in the performance of its neutral obligation; and especially that it omitted, notwithstanding the warnings and official representations made by the diplomatic agents of the United States during the construction of the said number '290', to take in due time any effective measures of prevention, and that those orders which it did give at last, for the detention of the vessel, were issued so late that*

(64) *GGE 2015*, *supra* note 2, §10.

(65) CDI, « Projet d'articles sur la prévention des dommages transfrontières résultant d'activités dangereuses et commentaires y relatifs », *op. cit.*, art. 3, commentaires §17, p. 426.

(66) *Affaire du personnel diplomatique et consulaire des États-Unis à Téhéran (États-Unis c. Iran)*, Arrêt du 24 mai 1980, *CIJ Recueil 1980*, §68.

their execution was not practicable » [67]. Cette obligation de prévention a ensuite été réaffirmée à plusieurs reprises par le juge international dans différentes affaires. Dans l'*Affaire du Détroit de Corfou*, la Cour internationale de justice a ainsi considéré que l'Albanie était responsable car elle n'avait rien fait pour prévenir le désastre : « En fait, rien ne fut tenté par les autorités albanaises pour prévenir le désastre. Ces graves omissions engagent la responsabilité internationale de l'Albanie » [68]. De la même manière, dans l'*Affaire des activités armées sur le territoire du Congo*, la Cour a jugé l'Ouganda responsable pour le « défaut de la vigilance requise pour prévenir les violations des droits de l'homme et du droit international humanitaire par d'autres acteurs présents sur le territoire occupé, en ce compris les groupes rebelles agissant pour leur propre compte » [69].

Dans l'espace numérique, on pourrait alors se demander si cette obligation de prévention devrait conduire les États à prendre des mesures concrètes, législatives et techniques, pour prévenir l'utilisation sans autorisation de leurs infrastructures numériques par des personnes privées à des fins malveillantes contre d'autres États.

La protection des infrastructures critiques constitue aujourd'hui un aspect essentiel pour la sécurité du numérique comme en témoignent notamment les travaux conduits par l'Assemblée générale des Nations Unies sur la cybersécurité et la protection des infrastructures critiques. Dans sa résolution 64/211 du 21 décembre 2009 intitulée *Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infrastructures essentielles*, l'Assemblée générale a ainsi proposé aux États une « Méthode d'autoévaluation volontaire des efforts nationaux » [70] qui incite les États à développer des mesures de protection de leurs infrastructures numériques critiques. De nombreuses autres organisations internationales, qu'il s'agisse de l'OSCE dans le cadre de ses mesures de confiance [71], de l'OCDE [72], de l'UE [73], de l'UA [74] ou encore de l'Organisation de coopération de Shanghai [75], ont développé des réflexions et des

(67) *Réclamations des États-Unis d'Amérique contre la Grande-Bretagne relatives à l'Alabama*, Sentence rendue le 14 septembre 1872 par le Tribunal d'arbitrage constitué en vertu de l'article I du Traité de Washington du 8 mai 1871, ONU, *RSA*, vol. XXIX, p. 130.

(68) *Affaire du Détroit de Corfou*, *op. cit.*, p. 23.

(69) *Affaire des activités armées sur le territoire du Congo*, *op. cit.*, §179.

(70) A/Res/64/211, 21 décembre 2009, *Création d'une culture mondiale de la cybersécurité et évaluation des efforts nationaux visant à protéger les infrastructures essentielles*.

(71) Voir par exemple, OSCE, *Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, Décision n° 1201, 10 mars 2016.

(72) Voir notamment, OCDE, *Recommendation of The Council on The Protection of Critical Information Infrastructures*, *OECD Ministerial Meeting on the future of the Internet Economy*, Seoul, 17-18 juin 2008.

(73) Voir notamment à cet égard, la Directive (UE) 2016/1148 du Parlement et du Conseil européens du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

(74) Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014.

(75) *Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security*, 16 juin 2009.

propositions importantes dans ce domaine. Ainsi que le résume bien le rapport du GGE de 2015, « Les États devraient prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies de l'information et des communications en tenant compte de la résolution 58/199 de l'Assemblée générale sur la création d'une culture mondiale de la cybersécurité et la protection des infrastructures essentielles de l'information et d'autres résolutions pertinentes » (76).

Il va de soi que l'obligation de prévention est une obligation de comportement qui varie en fonction des capacités de chaque État. À cet égard, on pourrait peut-être considérer que la capacité à légiférer pour interdire l'utilisation à des fins malveillantes d'infrastructures informatiques constitue une capacité commune à tous les États souverains. En revanche, comme nous l'avons déjà souligné, les capacités techniques varient fortement entre les États. Pour pouvoir efficacement prévenir les utilisations malveillantes, il est sans doute nécessaire de développer une coopération technique entre les États. La participation du secteur privé est à cet égard essentielle dans la mesure où de nombreuses infrastructures numériques à travers le monde sont privées.

Au regard de l'ensemble de la jurisprudence et des travaux conduits dans différents *fora* et organisations internationales, il semble que l'on puisse considérer qu'un État qui est manifestement défaillant, qui ne protège pas ses infrastructures numériques, permettant de ce fait à des acteurs privés de les utiliser pour lancer des cyberattaques contre d'autres États pourrait manquer à son devoir de vigilance. Ainsi que l'a souligné la Cour internationale de justice dans l'affaire *Application de la Convention pour la prévention et la répression du crime de génocide* : « la violation de l'obligation de prévenir se produit par omission » (77).

Une question délicate concerne toutefois les obligations des États à l'égard du développement et de l'acquisition par des acteurs privés d'armes ou techniques cyber-offensives qui pourraient être utilisées pour conduire des cyberattaques transfrontières. L'obligation de prévention implique-t-elle de la part des États une réglementation à cet égard ?

Ne pourrait-on pas considérer que l'acquisition par des personnes privées de techniques permettant de conduire des cyberattaques pourrait constituer un risque suffisamment sérieux pour obliger les États à agir ? La réponse est particulièrement délicate dans la mesure où les techniques utilisées pour conduire des cyberattaques peuvent être les mêmes que celles développées pour sécuriser

(76) *GGE 2015*, *supra* note 2, §13.

(77) *Affaire relative à l'application de la Convention pour la prévention et la répression du crime de génocide*, *op. cit.*, §432. Selon la Cour, « l'obligation de prévention et le devoir d'agir qui en est le corollaire prennent naissance, pour un État, au moment où celui-ci a connaissance, ou devrait normalement avoir connaissance, de l'existence d'un risque sérieux de commission d'un génocide. Dès cet instant, l'État est tenu, s'il dispose de moyens susceptibles d'avoir un effet dissuasif à l'égard des personnes soupçonnées de préparer un génocide, ou dont on peut raisonnablement craindre qu'ils nourrissent l'intention spécifique (*dolus specialis*), de mettre en œuvre ces moyens, selon les circonstances », §431.

et défendre des systèmes informatiques, tout dépend finalement de leur usage. La question de la commercialisation des biens et technologies dits à double-usage est largement abordée par l'*Arrangement de Wasnaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage* (78). En dépit toutefois de l'intérêt qu'il présente, cet arrangement reste un instrument juridiquement non contraignant. Or, le développement ces dernières années du commerce des vulnérabilités *zero-day* (à savoir des vulnérabilités non corrigées) mérite sans doute une analyse approfondie du point de vue du droit international, notamment au regard des obligations de prévention des États. Il conviendrait surtout d'analyser dans quelle mesure le commerce par des acteurs privés de vulnérabilité *zero-day* pourrait être considéré comme constituant un risque sérieux de cyberattaques que les États, suivant leur obligation de vigilance, devraient prévenir en réglementant, voire en interdisant, leur commercialisation (79).

B) Notification et répression des cyberattaques

Il est bien établi par la jurisprudence internationale que les États ont une obligation de notification à l'égard des États victimes d'activités dommageables. Cette obligation de notification a notamment été clairement affirmée par la Cour internationale de justice dans l'*Affaire du Détroit de Corfou* comme un principe général du droit international (80). Cela signifie que, dans l'espace numérique, les États qui savent que des cyberattaques sont lancées à partir de leur territoire et de leurs infrastructures contre d'autres États doivent en informer sans tarder ceux-ci. À cet égard, le développement d'une procédure internationale de notification et la coopération internationale entre *CERT/CSIRT* (81) pourraient jouer un rôle essentiel dans la mise en œuvre de cette obligation. Cette coopération pourrait aussi faciliter la notification faite par les États victimes eux-mêmes de cyberattaques en direction des États d'où émanent ces cyberattaques et ceci afin qu'ils prennent les mesures nécessaires pour faire cesser ces attaques et pour en anticiper de nouvelles.

Au-delà de cette obligation de notification, il va aussi de soi que les États doivent prendre toutes les mesures qui sont en leur pouvoir pour faire cesser ces cyberattaques. L'obligation de cessation de l'acte illicite qui incombe ainsi aux États

(78) *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies,* (www.wassenaar.org). Voir notamment à cet égard, Trey Herr, « Malware Counter-Proliferation and the Wassenaar Arrangement », *in* Nikolaos Pissanidis, Henry Roigas et Matthijs Veenendaal (dir.), *2016 8th International Conference on Cyber Conflict: Cyber Power*, NATO CCDCOE Publications, Tallinn, 2016, p. 175-190.

(79) Voir par exemple, Mailyn Fidler, « Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis », *I/S: A Journal of Law and Policy for the Information Society*, vol. 11 n° 2, 2015, p. 405-482.

(80) Le juge a ainsi estimé que « Les obligations qui incombaient aux autorités albanaises consistaient à faire connaître, dans l'intérêt de la navigation en général, l'existence d'un champ de mines dans les eaux territoriales albanaises et à avertir les navires de guerre britanniques, au moment où ils s'approchaient, du danger imminent auquel les exposait ce champ de mines. Ces obligations sont fondées (…) l'obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États », *Affaire du Détroit de Corfou, op. cit.*, p. 22.

(81) *Computer Emergency Response Team/Computer Security Incident Response Team*.

est une obligation classique du droit international qui a été rappelée à différentes reprises par le juge international. C'est ainsi que le GGE souligne, dans son rapport de 2015, que : « Les États devraient répondre aux demandes d'aide appropriée formulées par un autre État dont une infrastructure essentielle est exposée a des actes de malveillance informatique ; ils devraient aussi répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire, en tenant dûment compte de la souveraineté » (82).

Enfin, parallèlement aux mesures techniques qui pourraient être prises par les États pour faire cesser ces cyberattaques, les États devraient aussi enquêter et chercher à identifier les auteurs des attaques, les poursuivre et les condamner. Dans l'*Affaire du Détroit de Corfou*, la Cour avait ainsi reproché à l'Albanie, qu'« à la différence de la Grèce qui a institué aussitôt une commission chargée d'enquêter sur les événements du 22 octobre, le Gouvernement albanais n'a pris aucune décision de cet ordre, pas plus qu'il n'a procédé aux mesures d'instruction judiciaire qui incombent, en pareil cas, au souverain territorial » (83).

L'obligation de prévention constitue donc une obligation de comportement raisonnable ce qui signifie que les États ne peuvent pas être tenus automatiquement responsables au cas où ils échoueraient. Le juge international, dans toutes les affaires précitées n'a engagé la responsabilité internationale d'un État que lorsqu'il estimait que l'État en question n'avait pas pris les mesures raisonnables en son pouvoir, alors qu'il avait connaissance ou aurait dû avoir connaissance de ces risques, pour éviter le dommage. Comme nous l'avons déjà évoqué, l'obligation est proportionnée aux capacités de chaque État. Il est par ailleurs aussi clairement établi qu'une défaillance de la part d'un État, notamment dans la protection de ses infrastructures numériques, n'entraînera la responsabilité internationale de celui-ci qu'à condition que celle-ci soit réellement exploitée par des acteurs non-étatiques pour lancer des cyberattaques. Comme le souligne la Commission du droit international dans son article 14 §3 sur *La responsabilité internationale de l'État pour fait internationalement illicite* : « La violation d'une obligation internationale requérant de l'État qu'il prévienne un événement donné a lieu au moment où l'événement survient » (84).

(82) *GGE 2015*, *supra* note 2 §13 (h).
(83) *Affaire du Détroit de Corfou*, *op. cit.*, p. 19-20.
(84) *ACDI 2001*, *supra* note 19, p. 391.

PARTIE II. Comment répondre aux cyberattaques ? Le cadre général du droit international

Introduction : à la recherche d'une classification des réactions aux cyberattaques

A) La définition des cyberattaques

B) À la recherche d'un critère de classification des réactions admissibles

1. Réactions en l'absence de violation du droit international par un autre État

A) Mécanismes de coopération internationale et de règlement des différends

B) Mesures de rétorsion

C) Mécanismes exceptionnels d'autoprotection (état de nécessité, détresse, force majeure)

2. Réactions en cas de violation du droit international par un autre État

A) Contre-mesures pacifiques

B) Légitime défense en cas « d'agression armée »

II. Comment répondre aux cyberattaques ? Le cadre général du droit international

Introduction : à la recherche d'une classification des réactions aux cyberattaques

Dans cette deuxième partie, nous analyserons les différentes réactions que le droit international propose aux États qui considèrent être victimes de cyberattaques. Nous établirons ainsi une *classification* de ces réactions qui sera ordonnée autour du critère de l'existence ou non d'un « fait internationalement illicite » selon les règles du droit international public.

Notre analyse portera ainsi sur le cadre général du droit international en matière de réaction à des cyberattaques. Ce cadre s'applique en principe dans les relations entre *États* mais nous verrons (ainsi qu'*infra* Partie III) comment les acteurs non-étatiques (telles que les entreprises privées) entrent dans l'équation des réactions aux cyberattaques transnationales et quelles sont les réponses (coopération pénale, mandats d'arrêt, poursuites judiciaires…) les plus adaptées pour ces acteurs.

A) La définition des cyberattaques

Le droit international n'offre pas de définition unanimement acceptée du terme « cyberattaque » et les États proposent des définitions très diverses de celui-ci [(85)]. En dépit de cette diversité, on peut observer que les définitions semblent converger vers une approche large de la notion de « cyberattaque ». Ainsi, par exemple, selon le Canada :

> « Les cyberattaques comprennent l'accès involontaire ou non autorisé à des renseignements électroniques et/ou des infrastructures électroniques ou matérielles utilisés pour traiter, communiquer ou entreposer cette information, ainsi que leur utilisation, leur manipulation, leur interruption ou leur destruction (par voie électronique). La gravité des cyberattaques détermine le niveau d'intervention et les mesures d'atténuation nécessaires, c'est-à-dire la cybersécurité » [(86)].

Pour le Comité international de la Croix-Rouge (CICR) :

> « Les "cyberopérations" peuvent être décrites au sens large comme des opérations dirigées contre un ordinateur ou un réseau informatique, ou par le biais de ceux-ci, grâce à des flux de données. De telles opérations peuvent poursuivre des objectifs divers, comme infiltrer un système informatique pour collecter, exporter, détruire, altérer ou encrypter des données, ou pour déclencher, détourner ou manipuler de toute autre manière des processus contrôlés par le système

(85) Voir, par exemple, la compilation de différentes définitions étatiques de « cyberattaque » proposée par le *NATO Cooperative Cyber Defence Centre of Excellence* (https://ccdcoe.org/cyber-definitions.html).

(86) *Stratégie de cybersécurité du Canada*, 2010, p. 3 (www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-fra.pdf).

informatique infiltré. Toute une série de "cibles" dans le monde réel peuvent ainsi être détruites, altérées ou perturbées, comme les industries, les infrastructures, les télécommunications ou les systèmes financiers » (87).

Et, selon le dictionnaire *Technopedia* :

« *A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft* » (88).

Le terme pourrait donc, pour les besoins de notre analyse, être défini de façon suffisamment large pour inclure des techniques et finalités très diverses. Comme l'a souligné le Royaume-Uni :

« *The term cyberattack can refer to anything from small-scale email scams through to sophisticated large-scale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated aims such as: gaining unauthorised access to sensitive information; causing disruption to IT infrastructure; or causing physical disruption (e.g. to industrial systems)* » (89).

B) À la recherche d'un critère de classification des réactions admissibles

L'enjeu est d'identifier et classer les réactions qui sont admises par le droit international, compte tenu de la grande diversité des « cyberattaques » auxquelles sont confrontés les États, les personnes morales et physiques (90). Il semble assez évident que, en fonction de la *gravité des dommages* causés par des cyberattaques, la réaction des États ne devrait pas être la même, une atteinte grave autorisant logiquement une réaction plus sévère. Mais la gravité du dommage ne peut être le seul critère, ni d'ailleurs être le critère déterminant pour identifier et classer les réponses qui pourraient être admises par le droit international. On peut ainsi imaginer des situations où, malgré la gravité des dommages causés par une cyberattaque, un État ne pourrait pourtant pas être juridiquement habilité à répondre de manière forte, comme en adoptant des contre-mesures (*infra*). Cette hypothèse pourrait se produire, par exemple, dans le cas où une cyberattaque serait le fait exclusif d'un

(87) CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, Genève, 2011, p. 42. (www.icrc.org/fre/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-fr.pdf).

(88) Selon cette même entrée : « *Cyberattack is also known as a computer network attack (CNA). Cyberattacks may include the following consequences: Identity theft, fraud, extortion; Malware, pharming, phishing, spamming, spoofing, spyware, Trojans and viruses; Stolen hardware, such as laptops or mobile devices; Denial-of-service and distributed denial-of-service attacks; Breach of access; Password sniffing; System infiltration; Website defacement; Private and public Web browser exploits; Instant messaging abuse; Intellectual property (IP) theft or unauthorized access* »
(www.techopedia.com/definition/24748/cyberattack).

(89) Voir les définitions de « *Cyber Attack* » référencés par le *CCDCOE* (https://ccdcoe.org/cyber-definitions.html).

(90) Le droit international accepte tout autant le concept de dommage « immédiat » (résultant de l'atteinte à un droit juridiquement protégé de l'État lui-même en tant que sujet du droit international) que la notion de dommage « médiat » (résultant d'une atteinte aux intérêts de personnes privées qui se mue en un dommage affectant l'État lui-même). Ainsi, selon le mécanisme dit de la « protection diplomatique », un État a le droit de présenter une réclamation internationale contre un autre État lorsqu'un de ses ressortissants a subi un dommage du fait d'un acte illicite d'un autre État. On dit alors que l'État « prend fait et cause » pour ses ressortissants, personnes physiques ou morales en faisant valoir son droit à faire respecter le droit international en la personne de ses ressortissants.

acteur privé et alors que l'on ne pourrait ni attribuer cette attaque à un État, ni même reprocher à un État d'avoir manqué à son obligation de diligence due. Inversement, les États pourraient, dans d'autres hypothèses, répondre à une cyberattaque par l'adoption de contre-mesures alors même que l'attaque n'aurait provoqué que des dommages limités, voire aucun dommage car, comme nous le verrons, le dommage n'est pas en principe une condition pour l'exercice des contre-mesures, même s'il peut avoir une influence sur l'évaluation de la proportionnalité de la réponse.

Du point de vue du droit international, il est donc préférable d'adopter un autre critère de classification des réactions admissibles en cas de cyberattaque : celui du fait internationalement illicite. Cette expression désigne une action ou omission attribuable à un État et constituant une violation du droit international (91).

Nous verrons ainsi que certaines réactions à des cyberattaques sont toujours autorisées et ceci même lorsqu'il est impossible de démontrer qu'un État a commis une violation du droit international (1). D'autres réactions ne sont en revanche admissibles que si l'on peut établir qu'un État a commis, par action ou par omission, un fait internationalement illicite (2).

1. Réactions en l'absence de violation du droit international par un autre État

Les mesures que nous allons ici présenter sont à la disposition des États qui souhaitent réagir à une cyberattaque dont ils sont eux-mêmes victimes ou lorsque les victimes sont des personnes physiques ou morales situées sur leur territoire. Pour recourir à ces réactions :

- Il est indifférent que la cyberattaque ait été lancée par un État, par un acteur non-étatique agissant en lien avec un État (par exemple un « *proxy* ») ou par un acteur non-étatique agissant sans *aucun* lien avec un État.

- Il est indifférent que la cyberattaque puisse ou non être attribuée à un État.

- Il est indifférent que cette cyberattaque puisse ou non être considérée comme une violation du droit international.

En d'autres termes, les réactions décrites ci-après sont admises qu'il y ait ou non « fait internationalement illicite » d'un État. Ces réactions sont alors de trois ordres.

(91) Pour une analyse de ces termes, voir *infra* Partie II (2A).

A) Mécanismes de coopération internationale et de règlement pacifique des différends

Le développement de la coopération internationale se situe au cœur des mécanismes de réaction des États à des cyberattaques comme en témoigne le rapport du GGE de 2015 qui y consacre de longs développements dans sa Partie V intitulée « Coopération et assistance internationales en matière de sécurité informatique et de renforcement des capacités » [(92)]. Cette coopération peut se réaliser entre les États concernés (a) mais aussi avec l'aide des organisations internationales compétentes en la matière (b).

a) Coopération entre les États concernés

Que la cyberattaque dont est victime un État constitue ou non un « fait internationalement illicite », la première réaction est sans doute, pour l'État victime, de s'adresser à l'État (ou aux États) d'où est issue l'attaque pour solliciter son intervention et sa coopération.

Des acteurs non-étatiques pourraient, en effet, lancer des cyber-opérations malveillantes transnationales depuis le territoire de certains États sans que ces derniers en aient connaissance. Il est dès lors logique que l'État victime informe les États concernés et leur demande d'agir, dans les meilleurs délais, pour mettre fin à ces cyber-opérations. Comme nous l'avons vu en I^re^ Partie, les États ont, en effet, comme corollaire de leur souveraineté, le devoir de ne pas laisser utiliser leur territoire de manière à porter atteinte à l'intégrité territoriale d'un autre État : *sic utere tuo ut alienum no laedas*. Le GGE a d'ailleurs bien souligné, comme nous l'avons vu, que « les États devraient répondre aux demandes appropriées visant à atténuer les conséquences d'activités informatiques malveillantes dirigées contre une infrastructure essentielle d'un autre État et exercées depuis leur territoire » [(93)].

Le refus des États d'agir pour faire cesser une cyberattaque alors qu'ils ont reçu une notification à cet effet pourrait d'ailleurs être considéré comme un manquement à l'obligation de diligence due, autorisant l'État victime à adopter des contre-mesures. Ainsi, le recours aux mécanismes diplomatiques traditionnels de coopération n'est pas simplement la voie la plus sûre et sans doute la plus efficace, c'est aussi souvent une démarche nécessaire pour établir que l'autre État a *connaissance* des cyberattaques lancées par des acteurs privés depuis son territoire et qu'il ne fait rien pour les empêcher.

La coopération interétatique pour mettre fin à une cyberattaque peut prendre différentes formes. Si l'État d'où émanent les cyberattaques n'est pas en capacité de réagir, l'État victime, voire des États tiers, pourraient lui proposer leur aide technique. C'est notamment ce qu'exprime le GGE lorsqu'il souligne dans

(92) *GGE 2015*, *supra* note 2.
(93) *Ibid.*, §13 (h).

son rapport que « Les États devraient répondre aux demandes d'aides appropriées formulées par un autre État dont une infrastructure essentielle est exposée à des actes de malveillance informatique » [94].

Des opérations de « *hack-back* » (*infra* Partie III) pourraient aussi être développées pour neutraliser les acteurs non-étatiques avec le consentement, et sous le contrôle, tant de l'État victime que de l'État d'origine de l'attaque. Bien entendu, la recherche d'une coopération interétatique efficace n'empêche pas l'État victime d'une cyberattaque de prendre unilatéralement les mesures techniques nécessaires pour neutraliser les effets de cette attaque dans le respect de ses obligations découlant du droit international.

Le dialogue constructif et la coopération entre les États devraient donc être les premières réactions à des cyberattaques. La négociation entre les États devrait d'ailleurs être le mode par excellence de règlement pacifique des différends en cas de cyberattaque. En cas d'échec, les États peuvent aussi recourir aux autres modes de règlement pacifique des différends [95] qu'il s'agisse de la médiation, de l'enquête, de la conciliation ou du règlement juridictionnel.

b) Recours aux organisations internationales compétentes

Ainsi que le constate le rapport du GGE de 2015, la coopération entre les États pour faire face à une attaque informatique pourrait être soutenue et appuyée « par les organisations internationales compétentes, notamment l'ONU et ses institutions » [96].

Une hypothèse envisageable pourrait être la saisine du Conseil de sécurité des Nations Unies si la situation paraît suffisamment grave pour être considérée comme une menace contre la paix et la sécurité internationales. Celui-ci pourrait alors agir, soit dans le cadre du Chapitre VI de la Charte (règlement pacifique des différends), soit dans le cadre du Chapitre VII (action en cas de menace contre la paix, de rupture de la paix et d'actes d'agression). Dans le cadre du Chapitre VI, le Conseil pourrait, par exemple, sur la base de l'article 34, « enquêter sur tout différend ou toute situation qui pourrait entraîner un désaccord entre Nations ou engendrer un différend, afin de déterminer si la prolongation de ce différend ou de cette situation semble devoir menacer le maintien de la paix et de la sécurité internationales ». Il pourrait aussi, sur la base de l'article 37, « recommander tels termes de règlement qu'il juge appropriés ». Dans le cadre du Chapitre VII, le Conseil

(94) *Ibid.*

(95) Voir, par exemple, l'article 2 §3 de la Charte des Nations Unies (« Les membres de l'Organisation règlent leurs différends internationaux par des moyens pacifiques ») et le Chapitre VI de la Charte intitulé « règlement pacifique des différends ». Selon l'article 33 de la Charte : « Les parties à tout différend dont la prolongation est susceptible de menacer le maintien de la paix et de la sécurité internationales doivent en rechercher la solution, avant tout, par voie de négociation, d'enquête, de médiation, de conciliation, d'arbitrage, de règlement judiciaire, de recours aux organismes ou accords régionaux, ou par d'autres moyens pacifiques de leur choix ».

(96) *GGE 2015*, *supra* note 2, §23.

pourrait, s'il considère que la situation est suffisamment grave pour constituer une « menace contre la paix » au sens de l'article 39, recourir aux mesures provisoires prévues par l'article 40, à des mesures de coercition non-militaire (article 41), voire militaires (article 42). Néanmoins, jamais jusqu'à présent le Conseil de sécurité n'a eu à adopter de telles mesures à propos d'une cyberattaque.

Une autre possibilité pour les États concernés pourrait être de saisir les mécanismes régionaux de coopération. On pourrait par exemple penser à l'Agence européenne chargée de la sécurité des réseaux et de l'information (*ENISA*) (97) dont la mission est d'assurer un niveau élevé de sécurité des réseaux et de l'information en collaboration avec les instances nationales et les institutions européennes. On pourrait aussi penser à l'*Asia Pacific Computer Emergency Response Team* (*APCERT*) qui a notamment pour mission de renforcer la coopération régionale et internationale de la région Asie-Pacifique en matière de cybersécurité, d'élaborer conjointement des mesures pour faire face aux incidents de grande envergure et d'aider d'autres *CERT* et *CSIRT* dans la région à effectuer des interventions d'urgence en cas de cyberattaque (98). Un dernier exemple est la « Force de réaction rapide » (*Rapid Reaction Team*, *RRT*) de l'Otan qui est chargée « de porter assistance à un État-membre qui en ferait la demande en cas d'attaque cybernétique significative à l'échelle nationale » (99). Comme il a été souligné, avec les *RRT*, l'Otan est « capable d'offrir sur demande une assistance professionnelle et organisée à ses membres et partenaires, surtout aux pays qui n'ont pas encore les moyens de mettre en place un tel dispositif de cyberdéfense » (100).

B) Mesures de rétorsion

Si la coopération et la négociation ne produisent pas les effets escomptés, l'État victime peut aussi recourir à des mesures de rétorsion. Une mesure de rétorsion est une :

> « Mesure inamicale, licite en elle-même prise par un État en riposte à un comportement inamical d'un autre sujet de droit international que ce comportement soit ou non licite » (101).

Comme expliqué *supra*, il n'existe *aucune condition posée par le droit international pour le déclenchement* de mesures de rétorsion : l'État qui les adopte n'a pas à démontrer qu'un « fait internationalement illicite » a été commis par un autre État, ni ne doit d'ailleurs procéder à une « attribution » de la cyberattaque à un

(97) Voir le site de l'*European Union Agency for Network and Information Security* (www.enisa.europa.eu/).

(98) Voir le site de l'*APCERT* (www.apcert.org/).

(99) Voir « L'équipe Otan de réaction rapide lutte contre les cyberattaques », 13 mars 2012 (www.nato.int/cps/fr/natolive/news_85161.htm).

(100) *Ibid*.

(101) Jean Salmon (dir.), *Dictionnaire de droit international public*, Bruxelles, Bruyant/AUF, 2001 p. 1007. La définition donnée par la Commission du droit international de l'ONU est très similaire. Selon elle, une mesure de rétorsion est « un comportement "inamical", qui n'est pas incompatible avec une éventuelle obligation internationale de l'État qui y recourt, même s'il entend riposter à un fait internationalement illicite ». *ACDI 2001*, *supra* note 19, p. 138.

autre État – même si, sur un plan politique, démontrer l'origine de l'attaque serait sans doute très utile pour légitimer les mesures de rétorsion aux yeux de la communauté internationale.

L'ordre juridique international ne pose pas non plus de conditions pour l'exercice des mesures de rétorsion – autres, bien entendu, que leur conformité avec le droit international. Plus précisément, sur le plan juridique, il n'est nul besoin de respecter un quelconque principe de « nécessité » ou de « proportionnalité ». Les mesures de rétorsion peuvent ainsi être de grande ampleur afin d'envoyer un message fort à l'État qui doit, soit cesser lui-même la cyberattaque (si l'attaque est le fait de ses agents), soit prendre les mesures nécessaires dans le cadre de son obligation de diligence due (si l'attaque est le fait d'acteurs privés situés sur son territoire ou sous sa juridiction). Certes, de telles mesures de rétorsion pourraient être mal perçues par l'État visé et ne pas être appropriées, voire même être contre-productives dans certaines situations. Mais ce sont là des considérations politiques et stratégiques : sur le plan juridique, quelle que soit l'ampleur ou le caractère « disproportionné » (par rapport aux effets d'une cyberattaque) des mesures de rétorsion, il n'y a pas violation du droit international. On peut même penser que, d'un point de vue stratégique, des États pourraient être tentés par les sirènes des mesures de rétorsion fortes car de telles mesures pourraient contribuer à « apaiser » l'opinion publique choquée par une cyberattaque en montrant que l'État victime réagit de façon « ferme » et pourraient peut-être permettre de façon plus efficace d'obtenir la coopération de l'État visé – sans pour autant avoir besoin de recourir à des mesures plus « graves » telles que les contre-mesures analysées *infra*. Ceci étant dit, la pratique diplomatique montre que si l'État destinataire reçoit « mal » le message envoyé par les mesures de rétorsion, considérant ces mesures comme inamicales et inappropriées, il pourrait répondre lui-même par des mesures de rétorsion sur la base du principe de réciprocité.

Plusieurs exemples de mesures de rétorsion peuvent être donnés.

Tout d'abord, des *mesures diplomatiques* qui peuvent aller de la simple convocation d'un ambassadeur à la rupture complète des relations diplomatiques, en passant par le rappel temporaire du chef de la mission diplomatique ou d'autres diplomates, la diminution de la représentation diplomatique ou la déclaration, par l'État accréditaire, comme « *persona non grata* » de certains membres du personnel diplomatique de l'État accréditant – assortie d'une sommation de quitter le pays très rapidement.

Une autre mesure pourrait être de recourir au « *naming and shaming* ». La publication, par les plus hautes autorités de l'État victime, d'un rapport établissant de façon convaincante que la cyberattaque est le fait d'agents d'un autre État ou d'acteurs privés situés sur le sol de ce dernier, pourrait non seulement envoyer un message fort à l'autre État sur la détermination de l'État victime mais aussi largement légitimer des réactions ultérieures plus importantes.

Une troisième série de mesures pourrait concerner la suspension d'avantages accordés sans obligation juridique à l'autre État (par exemple une aide économique ou militaire), la suspension d'investissements en cours ou projetés sur le sol de l'autre pays, la suspension de négociations, l'annulation de visites officielles, le refus de participation à des activités politiques ou culturelles, etc.

Une quatrième série de mesures de rétorsion pourrait être l'adoption d'embargos contre des produits de l'autre pays (ou de certaines de ses entreprises considérées comme impliquées dans la cyberattaque) ou l'adoption de sanctions contre certaines entités ou individus présumés être impliqués dans la cyberattaque. Pour que ces sanctions puissent être considérées comme des mesures de rétorsion, il conviendra néanmoins de s'assurer qu'aucune règle du droit international (telles que celles découlant des engagements pris dans le cadre de la protection internationale des droits de l'homme) n'est violée par ces mesures.

De façon plus générale, toute mesure qui ne franchit pas le « seuil de l'illicéité » en droit international peut être adoptée dans le cadre d'une stratégie de recours à des mesures de rétorsion. Ceci concerne aussi, bien entendu, certaines « cyber-opérations » dirigées contre l'autre État qui, selon les critères actuels du droit international, seraient considérées comme licites [(102)].

C) Mécanismes exceptionnels d'autoprotection (état de nécessité, détresse, force majeure)

Le droit international admet trois mécanismes exceptionnels d'autoprotection qui permettent à un État de réagir à certaines situations, si besoin est par des mesures qui devraient être considérées, en d'autres circonstances, comme illicites. Le point commun de ces trois mécanismes est qu'aucun d'entre eux ne présuppose une violation du droit international par l'État contre les droits duquel ils sont dirigés. Ils offrent aussi aux États qui les invoquent, « un bouclier contre une accusation de violation d'une obligation internationale qui serait par ailleurs fondée » [(103)] dans d'autres circonstances.

La Commission du droit international de l'ONU a classé ces trois mécanismes dans la catégorie des « circonstances excluant l'illicéité ». Selon la logique de la CDI, les « circonstances » en question constituent des faits justificatifs qui abolissent le caractère illicite d'un acte, ou, pour le dire de façon plus simple, qui effacent exceptionnellement l'illégalité d'un acte [(104)].

(102) Sur le « seuil de l'illicéité » voir aussi *infra* Partie II (2A).

(103) Selon les termes de la CDI *in ACDI 2001*, *supra* note 19, p. 75.

(104) Nous avons, néanmoins, dans plusieurs études, essayé de démontrer qu'en réalité les deux plus importantes (état de nécessité et détresse) « circonstances » en question devraient plutôt être considérées comme des « circonstances excluant ou atténuant la responsabilité » des États (et non pas comme excluant l'illicéité de leurs actes). En d'autres termes, les violations du droit international commises sous l'excuse d'état de nécessité ou de la détresse restent des actes illicites, mais la responsabilité de leurs auteurs peut être, selon les circonstances, soit exclue soit, au moins, atténuée. Voir, parmi plusieurs autres études : Théodore CHRISTAKIS, « Les "circonstances excluant l'illicéité" : une illusion optique ? », *in Droit du*

Il convient toutefois de se garder de généraliser l'invocation de ces mécanismes en réaction à une cyberattaque. Le fait que ces excuses ne soient admises qu'à titre « exceptionnel » a été souligné tant par la Commission du droit international de l'ONU (105) que par la Cour internationale de justice (106). Dans les faits, les juridictions internationales n'acceptent que très rarement l'invocation de ces excuses – si rarement que certains auteurs sont allés jusqu'à remettre en cause l'existence même de certaines d'entre elles (107). Tout en considérant que ces trois mécanismes sont acceptés par le droit international positif, nous pensons que pour différentes raisons, notamment les conditions très strictes qui les encadrent, ces mécanismes ne peuvent être acceptés qu'à titre exceptionnel – ce qui diminue leur rôle dans la palette des réactions admissibles aux cyberattaques.

a) La force majeure

Selon l'article 23 du projet de la CDI sur la *Responsabilité internationale de l'État* :

> « 1. L'illicéité du fait d'un État non conforme à une obligation internationale de cet État est exclue si ce fait est dû à la force majeure, consistant en la survenance d'une force irrésistible ou d'un événement extérieur imprévu qui échappe au contrôle de l'État et fait qu'il est matériellement impossible, étant donné les circonstances, d'exécuter l'obligation.
>
> 2. Le paragraphe 1 ne s'applique pas : a) Si la situation de force majeure est due, soit uniquement soit en conjonction avec d'autres facteurs, au comportement de l'État qui l'invoque ; ou b) Si l'État a assumé le risque que survienne une telle situation. »

La force majeure désigne donc une situation où l'État est contraint d'agir d'une manière qui n'est pas conforme à ce que lui impose une obligation internationale à sa charge. Elle diffère de la détresse et de l'état de nécessité en ce sens que le comportement de l'État « est involontaire ou à tout le moins, ne procède en aucune manière d'un choix librement opéré » (108). Comme l'explique la CDI, l'impossibilité matérielle d'exécuter l'obligation qui donne lieu à une situation de force majeure « peut être due à un phénomène naturel ou physique (par exemple intempéries pouvant obliger l'aéronef d'un État à se dérouter vers le territoire d'un autre État, tremblements de terre, inondations ou sécheresses) ou à une activité de l'homme (par exemple perte de contrôle sur une partie du territoire d'un État

pouvoir, pouvoir du droit, Mélanges offerts à Jean Salmon, Bruylant, Bruxelles, 2007, p. 201-248 ; T. CHRISTAKIS, « "Nécessité n'a pas de Loi" ? Rapport introductif sur la nécessité en droit international » *in* T. CHRISTAKIS et Karine BANNELIER (dir.), *La nécessité en droit international*, Colloque de la Société française pour le droit international, Pedone, Paris, 2007, p. 9-62 ; T. CHRISTAKIS, « Quel remède à l'éclatement de la jurisprudence CIRDI sur les investissements en Argentine ? La décision du Comité *ad hoc* dans l'affaire CMS *c*. Argentine », *Revue générale de droit international public*, n° 4, 2007, p. 879-896.

(105) *ACDI 2001*, *supra* note 19, p. 84 §6 pour la détresse et p. 85 (§1 et 2) et p. 88 (§14) pour l'état de nécessité.

(106) *Projet Gabcikovo-Nagymaros (Hongrie/Slovaquie)*, Arrêt, *CIJ Recueil 1997*, §51.

(107) Voir surtout Sarah HEATHCOTE, *State of Necessity and International Law* (thèse n° 772), Université de Genève, Genève, 2005 et S. HEATHCOTE, « Est-ce que l'État de nécessité est un principe de droit international coutumier ? », *Revue Belge de Droit International* (*RBDI*), n° 1, 2007, p. 53-90.

(108) *ACDI 2001*, *supra* note 19, p. 81 §1.

consécutive à une insurrection ou dévastation d'une zone consécutive à des opérations militaires conduites par un État tiers) ou à une combinaison de ces deux éléments » [109]. Cette exception est néanmoins très encadrée. Il est notamment exigé que « la situation doit être à ce point irrésistible que l'État en cause n'a pas vraiment la possibilité d'échapper à ses effets » [110]. La force majeure ne s'étend pas, par contre, aux circonstances dans lesquelles l'exécution d'une obligation a été rendue difficile mais reste possible. On voit alors difficilement dans quelles circonstances la « force majeure » pourrait justifier une cyberattaque (ou une réaction à celle-ci par une pratique de *hack-back*).

b) La détresse

Selon l'article 24 du projet de la CDI sur la *Responsabilité internationale de l'État* :

> « 1. L'illicéité du fait d'un État non conforme à une obligation internationale de cet État est exclue si l'auteur dudit fait n'a raisonnablement pas d'autre moyen, dans une situation de détresse, de sauver sa propre vie ou celle de personnes qu'il a la charge de protéger.
>
> 2. Le paragraphe 1 ne s'applique pas : a) Si la situation de détresse est due, soit uniquement soit en conjonction avec d'autres facteurs, au comportement de l'État qui l'invoque ; ou b) Si ledit fait est susceptible de créer un péril comparable ou plus grave ».

La détresse concerne donc une situation où l'agent d'un État (individu dont les actes sont attribuables à l'État) se trouve dans une situation de péril, soit personnellement, soit à travers des personnes qu'il est en charge de protéger – et n'a raisonnablement pas d'autre moyen de sauver les vies en question que de violer le droit international. Contrairement à une situation de force majeure, l'agent de l'État n'agit pas involontairement mais *fait le choix* de violer le droit international pour sauver des vies – même si ce choix s'impose presque par la situation de péril. En pratique, la détresse a ainsi été invoquée surtout pour justifier les incursions non autorisées dans le territoire aérien ou maritime d'autres États par des navires ou aéronefs en détresse suite à des intempéries, des problèmes mécaniques ou à des difficultés de navigation [111]. Même si une intrusion non-autorisée dans *l'espace numérique* d'un autre État pourrait être imaginée comme le seul moyen pour sauver des vies, cette situation devrait rester exceptionnelle dans le cadre d'une réponse à des cyberattaques.

c) L'état de nécessité

Selon l'article 25 du projet de la CDI sur la *Responsabilité internationale de l'État* :

(109) *Ibid.*, §3.
(110) *Ibid.*
(111) Voir *ibid.*, §§3-6 les exemples donnés par la CDI.

« 1. L'État ne peut invoquer l'état de nécessité comme cause d'exclusion de l'illicéité d'un fait non conforme à l'une de ses obligations internationales que si ce fait : a) Constitue pour l'État le seul moyen de protéger un intérêt essentiel contre un péril grave et imminent ; et b) Ne porte pas gravement atteinte à un intérêt essentiel de l'État ou des États à l'égard desquels l'obligation existe ou de la communauté internationale dans son ensemble.

2. En tout cas, l'état de nécessité ne peut être invoqué par l'État comme cause d'exclusion de l'illicéité : a) Si l'obligation internationale en question exclut la possibilité d'invoquer l'état de nécessité ; ou b) Si l'État a contribué à la survenance de cette situation ».

À la différence de la force majeure, l'état de nécessité ne concerne pas un comportement involontaire ou contraint. À la différence de la détresse, la nécessité réside non pas dans un péril pour la vie de personnes qu'un agent de l'État a la charge de protéger, mais dans un péril grave menaçant les *intérêts essentiels* de l'État.

Cette circonstance est sans doute, parmi les trois, celle qui pourrait être invoquée le plus souvent par des États qui réagissent à des cyberattaques, voire qui déclenchent en premier des cyberattaques en invoquant « un péril grave et imminent » pour leurs « intérêts essentiels ». Le *Manuel de Tallinn 2.0* lui a d'ailleurs consacré de longs développements. Il convient toutefois de noter la grande différence entre la Commission du droit international de l'ONU et le *Manuel de Tallinn 2.0*. En effet, la CDI a formulé l'article 25 de façon négative (« L'État ne peut invoquer l'état de nécessité … que si ») afin de « bien marquer le caractère exceptionnel de l'état de nécessité et le souci de ne pas le voir invoquer abusivement » (112). Le *Manuel de Tallinn* semble vouloir s'écarter de cette formulation prudente en apportant sa propre règle (« *rule 26* ») sur la nécessité de façon positive : « *A State may act pursuant to the plea of necessity…* » (113). Ceci est étonnant car la CDI avait beaucoup insisté sur le fait que l'état de nécessité, compte tenu d'une série de « caractéristiques particulières », « ne pourra être que rarement invoqué pour excuser l'inexécution d'une obligation et cette excuse est soumise à de strictes limitations pour prévenir les abus » (114). Les exemples donnés par la CDI et l'acceptation très limitée de cette excuse par les juridictions internationales (115), semblent confirmer le bien-fondé de cette approche prudente de la CDI et mettre en garde contre toute tentative de s'appuyer très largement sur l'état de nécessité comme un mécanisme général de justification des cyberattaques.

Il serait trop long d'entrer ici dans une analyse détaillée des conditions très restrictives de l'état de nécessité en droit international (116) et leur pertinence dans le domaine de la réaction aux cyberattaques. Rappelons, néanmoins, les principales conditions :

(112) Selon les termes de la CDI elle-même *in ibid.*, p. 88 §14.

(113) Voici le texte entier : « *A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber or non-cyber in nature, to its essential interests when doing so is the sole means of protecting them* », *Manuel de Tallinn 2.0*, *supra* note 12.

(114) *ACDI 2001*, *supra* note 19, p. 85 (§2).

(115) Voir, entre autres, les études citées *supra*, notes 104 et 107.

(116) Voir pour cela *ibid.*

• **L'existence d'un péril grave et imminent.** L'état de nécessité ne peut être invoqué que pour protéger un intérêt essentiel de l'État contre un *péril grave et imminent*. Il va de soi qu'un État ne peut agiter des fantômes pour justifier une violation du droit international et qu'il ne saurait y avoir d'état de nécessité sans un « péril » particulièrement important, immédiat et dûment avéré au moment pertinent : *Vani timoris justa excusatio non est* [117]. La CDI a limité aussi considérablement la marge d'appréciation laissée aux États en soulignant que « le péril doit être objectivement établi » [118].

• **Ce péril doit porter atteinte à « un intérêt essentiel » de l'État.** Cet intérêt peut ainsi être lié à la protection de l'espace numérique et des infrastructures d'importance vitale, ou à d'autres domaines d'activité de l'État.

• **L'exclusivité du moyen utilisé.** La condition selon laquelle le fait incriminé doit constituer « *le seul moyen* de protéger un intérêt essentiel contre un péril grave et imminent » place l'exigence très haut. L'état de nécessité ne peut donc être assimilé à la force majeure : l'État choisit *volontairement* de violer le droit pour protéger ses propres intérêts et, de ce point de vue, la condition de l'exclusivité du moyen vise à limiter, autant que possible, les abus. Certes, ce critère a fait l'objet de critiques de la part de certains auteurs se demandant si les États n'auraient pas la possibilité de le contourner facilement [119]. La CDI n'a néanmoins apporté aucun assouplissement, insistant, dans son commentaire de l'article 25 adopté en 2001, sur le fait que « [l]'excuse est irrecevable si d'autres moyens (par ailleurs licites) sont disponibles, même s'ils sont plus onéreux ou moins commodes » [120].

• **La qualité du droit lésé.** L'état de nécessité ne peut jamais être invoqué pour justifier un fait qui porte « gravement atteinte à un intérêt essentiel de l'État ou des États à l'égard desquels l'obligation existe ou de la communauté internationale dans son ensemble ». Selon la CDI, « le poids de l'intérêt invoqué doit être tel qu'il l'emporte sur toutes les autres considérations, non seulement du point de vue de l'État auteur du fait dont il s'agit, mais selon une appréciation raisonnable des intérêts en présence, qu'ils soient individuels ou collectifs » [121]. Il s'agit donc d'une sorte de contrôle de proportionnalité entre les deux « intérêts essentiels » en cause. Ce critère établit une stricte hiérarchie : l'intérêt sacrifié doit être inférieur à l'intérêt sauvegardé.

(117) Voir Jean SALMON, « Faut-il codifier l'état de nécessité en droit international ? », *in* Jery MAKARCZYK (dir.), *Études de droit international en l'honneur du Juge Manfred Lachs*, La Hague/Boston, Martinus Nijhoff, 1984, p. 251-254.

(118) Commentaire de l'article 25 *in ACDI 2001*, *supra* note 19, §15.

(119) Selon Jean Salmon, par exemple : « Le caractère exclusif du moyen n'est pas très convaincant […] car de deux choses l'une : ou bien on doit épuiser sérieusement les moyens les plus onéreux d'écarter ce péril et alors peu de cas d'état de nécessité répondront aux conditions requises ; ou bien – ce qui est le plus à craindre – celui qui invoque le péril imminent tirera argument de l'imminence même du péril pour ne pas épuiser d'autres moyens » (*supra*, note 117, p. 263).

(120) *ACDI 2001*, *supra* note 19, p. 88, §15.

(121) *Ibid.*, p. 89, §17.

• **Les « mains propres ».** L'État auteur du fait illicite « ne doit pas avoir contribué à la survenance de l'état de nécessité ».

• **La barrière du *jus cogens*.** L'état de nécessité ne peut jamais justifier la violation d'une « obligation découlant d'une *norme impérative* du droit international général », comme le souligne l'article 26 du projet de la CDI. Ainsi, l'état de nécessité ne pourrait pas être invoqué, par exemple, pour commettre une agression contre un autre État.

2. Réactions en cas de violation du droit international par un autre État

Les réactions que nous allons ici étudier ne sont possibles juridiquement que si, lors d'une cyberattaque, un État a violé d'une façon ou d'une autre le droit international. L'existence d'un « fait internationalement illicite » est donc ici indispensable. Bien entendu, rien n'oblige l'État victime d'un tel fait de recourir aux réactions qui seront ici analysées : il a parfaitement la discrétion de recourir plutôt aux mécanismes analysés *supra* (Partie II 1 et surtout A et B) qui restent toujours à sa disposition et qui pourraient être considérés plus appropriés, dans certaines situations, par l'État victime d'une cyberattaque illicite. Par ailleurs, il faut souligner que, selon une règle fondatrice du droit international, « tout fait internationalement illicite de l'État engage sa responsabilité internationale » [(122)]. Ceci signifie qu'un État lésé par un tel fait peut mettre en œuvre les mécanismes internationaux de responsabilité en recourant, par exemple, lorsque cela est possible, à un tribunal arbitral ou à la Cour internationale de justice pour demander à l'État responsable cessation de l'acte illicite, non-répétition et réparation intégrale du préjudice causé par le fait internationalement illicite. Laissant de côté la question de l'engagement de la responsabilité internationale de l'État auteur de cyberattaques, nous nous concentrerons ici sur les deux réactions à l'illicite dont disposent les États victimes d'une cyberattaque, à savoir les contre-mesures pacifiques (A) et la légitime défense en cas d'agression armée (B).

A) Contre-mesures pacifiques

Les contre-mesures peuvent être définies comme des :

> « Mesures qui seraient contraires aux obligations internationales de l'État lésé vis-à-vis de l'État responsable, si elles n'étaient prises par le premier en réaction à un fait internationalement illicite commis par le second, aux fins d'obtenir la cessation et la réparation » [(123)].

Les contre-mesures résultent d'un recours à des procédés de « justice privée » assez largement inconcevable dans les ordres juridiques internes qui reposent sur le principe « nul ne peut se faire justice à soi-même » et où l'État est, en vertu

(122) Règle codifiée par l'article 1 du projet de la CDI sur la responsabilité, *ACDI 2001*, *supra* note 19.
(123) *Ibid.*, p. 137, §1.

de sa souveraineté, le garant de l'exécution du droit [124]. Dans l'ordre juridique international, les contre-mesures « caractérisent un système décentralisé permettant aux États lésés de s'efforcer de faire valoir leurs droits » [125]. Faute d'existence d'une autorité supérieure aux États capable de leur imposer une solution, faute d'existence d'un tiers impartial ayant toujours et de façon automatique compétence pour trancher les litiges entre États – ces derniers sont autorisés non seulement à « se faire justice eux-mêmes », mais aussi à recourir pour cela à des actes en principe illicites. Il s'agit en quelque sorte de l'hommage rendu par le vice à la vertu : les États lésés peuvent recourir à des violations du droit international contre les États responsables de telles violations mais seulement afin de pousser ces derniers à respecter leurs obligations internationales en cessant la violation et en réparant les conséquences de celle-ci. Dans une telle hypothèse, l'illicéité des contre-mesures de l'État lésé est « effacée », « exclue » car il s'agit d'une réponse justifiée à un acte illicite initial d'un autre État qui a pour fonction de ramener ce dernier dans le chemin de la légalité. Contrairement à l'état de nécessité ou à la détresse qui devraient, selon nous, être considérés comme des circonstances « excluant ou atténuant la responsabilité » des États [126], les contre-mesures sont clairement des circonstances « excluant l'illicéité ». La jurisprudence internationale semble confirmer cette conception des contre-mesures comme circonstances « justifiant » un acte illicite [127]. Ceci est aussi confirmé par le fait que, à notre connaissance, il n'a jamais été envisagé, dans la pratique des États et des juridictions internationales, l'existence d'une obligation éventuelle *d'indemnisation* d'une perte causée à la suite de l'adoption de contre-mesures justifiées [128].

Ainsi, dans l'hypothèse d'une cyberattaque constituant un « fait internationalement illicite », l'État victime a le droit de réagir, s'il le souhaite et sous certaines conditions, en recourant contre l'État responsable à des mesures qui constituent normalement des violations du droit international. Ces contre-mesures ne doivent pas nécessairement être de même nature que l'acte illicite initial. Ainsi, un État peut conduire, dans l'exercice de contre-mesures, une action de *hack-back* ou de « cyberattaque en retour » ; mais il peut aussi adopter toute autre mesure pacifique contraire au droit : suspension de l'exécution d'un accord international, sanctions économiques contraires aux règles internationales ou d'autres violations encore de ses obligations à l'égard de l'État responsable. Ces contre-mesures, si elles

(124) Même si les ordres juridiques internes envisagent certaines situations où la victime d'une violation du droit peut recourir à certains mécanismes d'autoprotection sans recourir au juge : tel est le cas surtout de l'exception de l'inexécution en droit civil ou, bien sûr, la légitime défense en droit pénal. Mais ces mécanismes, qui ont leurs équivalents en droit international, se différencient largement de l'autorisation généralisée des contre-mesures en droit international.

(125) *ACDI 2001*, *supra* note 19, p. 137 §1.

(126) *Supra* note 104.

(127) Dans l'*Affaire du Cysne*, par exemple, le tribunal arbitral a souligné que : « un acte contraire au droit international peut se justifier, à titre de représailles, si un acte semblable en avait fourni le motif », Sentence du 30 juin 1930, *RSA*, vol. II, p. 1056. Voir aussi p. 1057.

(128) Toute autre est la question de savoir si un ordre juridique pourrait prévoir des mécanismes d'indemnisation des personnes privées, physiques ou morales, qui ont subi un dommage du fait de contre-mesures adoptées contre des États.

respectent les conditions de déclenchement (a) et d'exercice (b) que nous allons maintenant analyser, seront considérées comme justifiées et n'engageront pas la responsabilité de leur auteur.

a) Conditions de déclenchement :
l'existence d'un fait internationalement illicite d'un État

Les contre-mesures ne sont autorisées qu'à l'encontre de l'État responsable d'un fait internationalement illicite et doivent être dirigées exclusivement contre celui-ci. L'article 2 du projet de la CDI sur la responsabilité explique que :

> « Il y a fait internationalement illicite de l'État lorsqu'un comportement consistant en une action ou une omission : a) Est attribuable à l'État en vertu du droit international ; et b) Constitue une violation d'une obligation internationale de l'État ».

Ainsi, en principe, la survenance d'un dommage matériel n'est pas nécessairement requise pour recourir légitimement à des contre-mesures. Un simple préjudice moral ou juridique pourrait suffire (129). En revanche, pour qu'il y ait « fait internationalement illicite » il faut qu'il existe deux conditions cumulatives : violation d'une obligation internationale et attribution de cette violation à un État.

i. Violation d'une obligation internationale

L'existence d'une violation d'une obligation internationale est une condition *sine qua non* pour l'adoption de contre-mesures qui, par définition, ne peuvent constituer que des réponses à un acte illicite *initial* d'un autre État et sont des voies d'exécution pour obtenir le respect des obligations internationales. Plusieurs règles du droit international pourraient être violées en fonction de la nature et des effets d'une cyberattaque : elles peuvent aller de violations du *jus contra bellum* ou du *jus in bello* à des violations moins graves de la souveraineté d'un État, en passant par la violation de principes tels que le principe de non-intervention ou le droit des peuples à disposer d'eux-mêmes (130). Il est impossible, dans l'espace limité dont nous disposons ici, d'entrer dans une analyse détaillée de tous les *scenarii* et de toutes les normes qui pourraient être violées par une cyberattaque. Nous nous limiterons donc ici à trois observations.

(129) La nature du « préjudice » subi par « l'État lésé » dépend ainsi des exigences de la règle primaire violée par l'État responsable. Comme l'a soulignée la CDI : « On a parfois dit que la responsabilité internationale ne peut être engagée par le comportement d'un État qui manque à ses obligations que s'il existe un autre élément, en particulier celui du « dommage » causé à un autre État. Mais la nécessité de tenir compte de tels éléments dépend du contenu de l'obligation primaire, et il n'y a pas de règle générale à cet égard ». *ACDI 2001*, *supra* note 19, p. 37, §9.

(130) Une ingérence grave dans le processus électoral d'un pays dont résulterait un résultat faussé pourrait, par exemple, être considérée comme une violation de ce principe. Rappelons que, selon le codification de ce principe par la Déclaration relative aux principes du droit international touchant les relations amicales entre les États adoptée par l'Assemblée générale des Nations Unies en 1970 : « En vertu du principe de l'égalité de droits des peuples et de leur droit à disposer d'eux-mêmes, principe consacré dans la Charte des Nations Unies, tous les peuples ont le droit de déterminer leur statut politique, en toute liberté et sans ingérence extérieure… ».

En premier lieu, un examen des textes du droit international et de la doctrine révèle les incertitudes qui existent quant à la distinction entre le principe de non-intervention et le principe de non-ingérence dans les affaires internes d'un pays. On pourrait penser que le premier se réfère à la protection du *territoire* de l'État, de son *dominium*, et que sa violation impliquerait donc la réalisation d'opérations matérielles en territoire étranger ; tandis que le second renverrait à une interférence, sans l'autorisation de l'État, dans la sphère de l'exercice de ses compétences nationales, de ses pouvoirs souverains et affecterait donc l'*imperium* de l'État (131). Pourtant, cette distinction s'émousse souvent dans la pratique. Ainsi, par exemple, la fameuse *Déclaration relative aux principes du droit international touchant les relations amicales entre les États* adoptée par l'Assemblée générale des Nations Unies en 1970, énonce le principe selon lequel :

> « Aucun État ni groupe d'États n'a le droit d'intervenir, directement ou indirectement, pour quelque raison que ce soit, dans les affaires intérieures ou extérieures d'un autre État. En conséquence, non seulement l'intervention armée, mais aussi toute autre forme d'ingérence ou toute menace, dirigées contre la personnalité d'un État ou contre ses éléments politiques, économiques et culturels, sont contraires au droit international » (132).

La Cour internationale de justice, quant à elle, a souligné dans son arrêt de 1986 dans l'affaire des *Activités militaires au Nicaragua* que :

> « L'intervention interdite doit donc porter sur des matières à propos desquelles le principe de souveraineté des États permet à chacun d'entre eux de se décider librement. Il en est ainsi du choix du système politique, économique, social et culturel, et de la formulation des relations extérieures. L'intervention est illicite lorsqu'à propos de ces choix, qui doivent demeurer libres, elle utilise des moyens de contrainte. Cet élément de contrainte, constitutif de l'intervention prohibée et formant son essence même, est particulièrement évident dans le cas d'une intervention utilisant la force, soit sous la forme directe d'une action militaire soit sous celle, indirecte, du soutien à des activités armées subversives ou terroristes à l'intérieur d'un autre État » (133).

Des études plus approfondies devraient sans doute être menées en doctrine pour mieux définir le contenu de ces principes et pour identifier à partir de quel moment ces principes pourraient être considérés comme violés dans l'hypothèse d'une cyberattaque. Ainsi, par exemple, il n'existe aucun doute sur le fait qu'une cyberattaque qui manipule les résultats électoraux dans un pays pourrait constituer une violation du principe de non-ingérence (134). Il est plus compliqué, néanmoins, de définir à partir de quel moment le simple vol de messages électroniques de certaines figures politiques et leur diffusion dans des médias ou leur

(131) Voir, à cet égard, Jean Combacau et Serge Sur, *Droit international public*, Paris, Montchrestien, 5e édition, 2001, p. 260 et Pierre-Marie Dupuy et Yann Kerbrat, *Droit international public*, Paris, Dalloz, 12e édition, 2014, p. 130.

(132) Selon le texte du « principe relatif au devoir de ne pas intervenir dans les affaires relevant de la compétence nationale d'un État, conformément à la Charte » de la A/RES 2625 (XXV) du 24 octobre 1970.

(133) CIJ, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci*, Arrêt du 27 juin 1986, *Rec. 1986*, p. 108, §205.

(134) Voir à cet égard le discours de Brian Egan (*US State Department Legal Adviser*), « International Law and Stability in Cyberspace », 10 novembre 2016 (www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf).

publication sur internet pourraient être considérés comme une violation du même principe [135].

En deuxième lieu, il est intéressant de noter la position du *Manuel de Tallinn 2.0* qui a essayé de déterminer dans quelles circonstances une cyberattaque pourrait constituer une violation de la souveraineté d'un État. Selon les experts invités à participer à ce *Manuel* :

> « *The precise legal character of remote cyber operations that manifest on a State's territory is somewhat unsettled in international law. […] First, most of the Experts agreed that cyber operations constitute a violation of sovereignty in the event they result in physical damage or injury […]. Second, the Experts agreed that, in addition to physical damage, the remote causation of loss of functionality of cyber infrastructure located in another State sometimes constitutes a violation of sovereignty, although no consensus could be achieved as to the precise threshold at which this is so […]. There was full agreement that a cyber operation necessitating repair or replacement of physical components of cyber infrastructure amounts to a violation because such consequences are akin to physical damage or injury. […] Third, no consensus could be achieved as to whether, and if so, when, a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty* » [136].

Le *Manuel de Tallinn 2.0* a aussi considéré que « *Although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so* » [137]. D'autres auteurs ont par contre considéré que le cyber-espionnage constitue une violation du principe de non-ingérence dans les affaires internes des États [138].

Notre troisième et dernière observation concerne la violation de l'obligation de diligence due qui est particulièrement pertinente par rapport à notre problématique liée à des cyberattaques conduites par des acteurs privés. Comme nous l'avons vu en effet dans la première partie, les États ont, en vertu de leur souveraineté, l'obligation de ne pas laisser utiliser leur territoire aux fins d'actes contraires aux droits d'autres États. Si les États ont (ou auraient dû avoir) connaissance d'une cyberattaque lancée par des acteurs privés depuis leur territoire et ne font rien pour l'empêcher, ils pourraient violer leur obligation de *due diligence* autorisant l'État lésé à adopter contre eux (et les acteurs privés sur leur sol) des contre-mesures, y compris des mesures de *hack-back*, jusqu'à ce que l'État responsable adopte les mesures nécessaires pour mettre fin à la cyberattaque.

II. Attribuable à un État

Pour qu'un État puisse adopter des contre-mesures encore faut-il que la violation du droit international par action (par exemple une cyberattaque) ou

(135) Dans le discours précité, Brian Egan concluait que : « *For increased transparency, States need to do more work to clarify how the international law on non-intervention applies to States activities in cyberspace* ».

(136) *Manuel de Tallinn 2.0*, *supra* note 12, analyse sous la « *Rule 4 – Violation of sovereignty* », §10-14.

(137) *Ibid.*, *Rule 32*.

(138) Voir Russell Buchan, « Cyber Espionage and International Law » *in* Nicholas Tsagourias et R. *Buchan* (dir.), *Research Handbook on International Law and Cyberspace*, Edward Elgar, 2015, p. 168-189.

omission (par exemple manquement à l'obligation de diligence due) soit attribuable à l'État à l'encontre duquel les contre-mesures sont adoptées. L'attribution apparaît ainsi comme une condition fondamentale pour l'adoption de contre-mesures justifiées sur la base du droit international. Ceci nous amène de nouveau à trois observations.

La première concerne les **mécanismes d'attribution**. Il convient en effet de distinguer, même si les deux opérations sont très liées, l'identification des attaquants en tant qu'opération technique liée à la criminalistique (ce que l'on appelle en anglais les « *cyber forensics* ») de l'attribution en tant qu'opération légale. Le droit international prévoit, en effet, des mécanismes très précis qui permettent d'attribuer, sous certaines conditions strictes, le comportement des acteurs privés à des États. Ces mécanismes sont analysés *infra* dans la Partie III (3C).

La deuxième observation concerne les **difficultés en matière d'attribution** du point de vue technique précité des *cyber forensics*. Jusqu'à une époque récente, l'attribution des attaques dans le cyberespace était considérée comme particulièrement difficile. Malgré les progrès accomplis et les efforts de certains de présenter l'attribution comme un problème désormais résolu, des difficultés redoutables demeurent. Ces difficultés sont dues à une multitude de facteurs dont, notamment l'absence de capacités techniques suffisantes (le problème de « *forensic capacity* ») dans plusieurs pays ; le recours à des techniques de dissimulation (« *spoofing* ») particulièrement sophistiquées utilisées par les *hackers* pour faire croire que l'attaque a été lancée par quelqu'un d'autre et le manque, souvent, de temps suffisant pour établir avec certitude l'origine de l'attaque avant l'adoption de contre-mesures qui prennent souvent la forme de *hack-back*. La complexité et les limites de l'attribution sont souvent exprimées par plusieurs États. Tout récemment, le Président américain lui-même s'est prononcé sur le sujet soulignant que « *unless you catch "hackers" in the act, it is very hard to determine who was doing the hacking* » ou encore que « *hacking is a very hard thing to prove* » [(139)].

Pour résoudre le problème de l'attribution sur le plan international, certains États ont proposé au sein du GGE la création d'un mécanisme international d'attribution qui devrait disposer de l'expertise technique nécessaire pour procéder à des attributions fiables et indépendantes. Néanmoins, d'autres États s'y opposent, considérant que le processus d'attribution comprend des considérations non seulement techniques et juridiques mais aussi politiques, qui font partie de l'ADN même de la sécurité nationale des États. Ces pays ont aussi exprimé leurs doutes quant à la capacité d'un organe international de remplir efficacement ce rôle considérant que sa création pourrait même s'avérer contre-productive. En conclusion, ils considèrent que le processus d'attribution, du point de vue à la fois technique et juridique, devrait rester l'apanage des États eux-mêmes.

(139) Voir Kristen Eichensehr, « Trump's Dangerous Attribution Message on Russian Hacking—and How to Counter It », *Just Security*, 10 janvier 2017 (www.justsecurity.org/36161/trumps-dangerous-attribution-message-and-counter/).

La troisième et dernière observation concerne la question de **la preuve nécessaire à apporter en matière d'attribution** avant l'adoption de contre-mesures. Il s'agit d'une question capitale qui a donné lieu à beaucoup d'échanges entre les États à la fois au sein du GGE et en dehors de celui-ci – y compris en relation avec certaines accusations de cyberattaques.

Le droit international positif semble pourtant assez clair à cet égard : il n'exige pas des États d'apporter la preuve de leur allégation concernant l'existence d'une violation du droit international par un autre État avant l'adoption de contre-mesures envers ce dernier. Il s'agit ici d'un domaine où le vieil adage *Nemo iudex in causa sua* (140) ne s'applique pas. En l'absence, dans l'ordre juridique international, d'une instance centralisée automatiquement compétente pour apprécier les faits et pour interpréter les règles qui sont applicables aux États, ce pouvoir est souvent laissé aux États y compris en matière de contre-mesures (141). Comme l'avait souligné en 1978 un Tribunal arbitral dans une affaire phare en matière de contre-mesures qui opposait les États-Unis à la France :

> « Dans l'état actuel du droit international général, abstraction faite des engagements spécifiques découlant de traités particuliers et notamment des mécanismes institués dans le cadre des organisations internationales, chaque État apprécie pour lui-même sa situation juridique au regard des autres États » (142).

La Commission du droit international de l'ONU a codifié cette règle dans son projet sur la responsabilité internationale des États. Selon la CDI :

> « Un État qui prend des contre-mesures le fait à ses propres risques, si sa perception de la question de l'illicéité se révèle mal fondée. Un État qui recourt à des contre-mesures en fonction d'une appréciation unilatérale de la situation le fait à ses propres risques et peut encourir une responsabilité à raison de son propre comportement illicite dans l'hypothèse d'une appréciation inexacte » (143).

Ceci signifie donc qu'un État n'a pas l'obligation juridique de produire des preuves relatives à l'attribution d'une cyberattaque avant d'adopter des contre-mesures contre l'État accusé d'être à l'origine de celle-ci. Si, en revanche, il s'avère ultérieurement que l'État lésé s'est trompé en matière d'attribution, les contre-mesures ne seront pas justifiées sur la base du droit international et sa responsabilité internationale sera engagée avec une obligation de réparation du préjudice subi par l'État injustement accusé d'être à l'origine de la cyberattaque. Il faut ajouter, à cet égard, que l'existence d'une croyance raisonnable, compte tenu des circonstances, ou d'une bonne foi de l'État auteur des contre-mesures ne sera pas suffisante pour exonérer sa responsabilité s'il s'avère que cet État s'est, malgré tout, trompé en matière d'attribution.

---

(140) « Nul n'est juge en sa propre cause ».

(141) *Cf.* Linos A. Sicilianos, *Les réactions décentralisées à l'illicite*, Paris, LGDJ, 1990, p. 31.

(142) *Affaire concernant l'accord relatif aux services aériens du 27 mars 1946 entre les États-Unis d'Amérique et la France*, Sentence arbitrale du 9 décembre 1978, *RSA*, vol. XVIII, §81.

(143) *ACDI 2001*, *supra* note 19, p. 139, §3.

Si donc, en son état actuel, le droit positif ne semble pas *exiger* des États d'apporter la preuve de leurs allégations en matière de cyberattaques, sur le plan politique et de légitimation des contre-mesures auprès de l'opinion publique mondiale, les États pourraient avoir intérêt à présenter certains éléments de preuve. La quantité et la qualité de ces preuves devraient d'ailleurs être proportionnelles à l'ampleur et à la gravité des contre-mesures. C'est dans ce sens que le GGE de l'ONU a souligné, dans son rapport de 2015, que « les accusations d'organiser et d'exécuter des actes illicites portées contre des États devaient être étayées » (144).

b) Conditions d'exercice

Si le droit international autorise, dans les conditions précitées, le recours à des contre-mesures et à des mécanismes de « justice privée », il ne s'agit pas pour autant d'un retour à la loi de la jungle. L'ordre juridique international encadre très strictement l'exercice des contre-mesures en imposant toute une série de conditions qui montrent que ces « voies d'exécution » dont disposent les États doivent être utilisées de façon prudente, afin d'éviter les abus et de ne pas mettre en danger la stabilité et la sécurité internationales. Sans entrer dans le détail de ces conditions, analysées dans d'autres études (145), nous soulignerons rapidement certaines d'entre elles pour les besoins de notre analyse.

• **Conditions liées à l'objectif des contre-mesures.** L'État lésé ne peut prendre de contre-mesures à l'encontre de l'État responsable du fait internationalement illicite que pour amener cet État à s'acquitter des obligations de cessation ou de réparation qui lui incombent en vertu du droit international. Les contre-mesures n'ont donc pas une fonction punitive et ne devraient pas être considérées comme une expression de la loi du talion. Il s'agit, au contraire, de voies d'exécution dont le seul objectif doit être de faire respecter le droit international par l'État qui l'a violé en premier. Les contre-mesures doivent dès lors être réversibles (146) et cesser « dès que l'État responsable s'est acquitté des obligations qui lui incombent » en vertu du droit international (147).

• **Les contre-mesures doivent toujours être pacifiques.** La Commission du droit international de l'ONU a codifié la règle selon laquelle les contre-mesures « ne peuvent porter aucune atteinte à l'obligation de ne pas recourir à la menace ou à l'emploi de la force telle qu'elle est énoncée dans la Charte des Nations Unies » (148). Cette règle, codifiée aussi dans d'autres instruments importants du

(144) *GGE 2015*, *supra* note 2, §28 (f).

(145) Voir, entre autres, le commentaire de la *ACDI 2001*, *supra* note 19, p. 79-80 et 137-149 et les études de Denis Alland, *Justice privée et ordre juridique international*, Paris, Pedone, 1994, 503 p. et L.A. Sicilianos (*supra* note 141). Voir aussi le *Manuel de Tallinn 2.0*, *supra* note 12, *rules 20-25*.

(146) Selon l'article 49 §3 du projet de la CDI sur la responsabilité : « Les contre-mesures doivent, autant que possible, être prises d'une manière qui permette la reprise de l'exécution des obligations en question ».

(147) *Ibid.*, article 53.

(148) *Ibid.*, article 50.

droit international [149], exclut la possibilité de recourir à des contre-mesures militaires ou de réagir par des mesures de *hack-back* qui pourraient être considérées comme une violation de la prohibition de la menace ou de l'emploi de la force en droit international [150]. Ceci pose, bien entendu, la question de savoir à partir de quand une action précise peut être considérée comme franchissant le « seuil » de l'existence d'un recours prohibé à la force. Il s'agit d'un grand débat relatif au *jus ad bellum* qui a fait l'objet de longues études dans la doctrine [151] que nous ne pouvons malheureusement pas analyser ici. Il convient néanmoins de citer une récente étude de Marco Roscini qui propose une définition large des cyber-opérations susceptibles d'être qualifiées comme une violation de l'article 2 §4 de la Charte relatif à la prohibition de la menace et du recours à la force. Selon la conclusion de cet auteur :

> « *Those worried that, by qualifying seriously disruptive cyber operations as a use of force, the risk of inter-State conflicts will increase should be reassured: indeed, a use of force, in itself, is not sufficient to entitle the victim State to react in self-defence, unless it is serious enough to amount to an "armed attack". Apart from the stigma attached to it, then, the only consequence of qualifying seriously disruptive cyber operations as a use of force is that they could not be undertaken in countermeasure, which certainly is a welcome result, considering the severe negative impact that they might have on the public order of today's digitally reliant societies* » [152].

• **Les contre-mesures ne peuvent pas violer certaines autres obligations importantes des États.** Selon la règle codifiée par l'article 50 du projet de la CDI sur la responsabilité des États, les contre-mesures ne peuvent pas non plus porter atteinte aux obligations relatives à la protection des droits fondamentaux de l'homme, aux obligations de caractère humanitaire excluant les représailles ainsi qu'aux obligations découlant de normes impératives du droit international général. Cette règle est particulièrement importante car elle interdit l'utilisation de contre-mesures qui pourraient affecter, de manière directe ou indirecte, les obligations des États relatives aux droits humains qui ne sont pas, en principe, soumises au principe de réciprocité en vertu du droit international.

• **Les contre-mesures doivent respecter le principe de proportionnalité.** Selon l'article 51 du projet de la CDI : « Les contre-mesures doivent être proportionnelles au préjudice subi, compte tenu de la gravité du fait internationalement illicite et des droits en cause ». Contrairement aux mesures de rétorsion où, comme nous l'avons vu, le principe de proportionnalité n'est pas pertinent, ici il joue un rôle fondamental. L'idée générale est que l'adoption de contre-mesures, qui est autorisée pour « corriger » un déséquilibre créé par l'acte illicite initial d'un autre État et obliger cet État à « retrouver le chemin » de la légalité internationale, ne

(149) Voir par exemple la *Déclaration relative aux principes du droit international touchant les relations amicales et la coopération entre les États* de 1970 selon laquelle : « Les États ont le devoir de s'abstenir d'actes de représailles impliquant l'emploi de la force », *op. cit.*

(150) L'hypothèse de la légitime défense est bien entendu distincte et examinée *infra* Partie II (2B).

(151) Voir surtout Olivier Corten, *Le droit contre la guerre*, Paris, Pedone, 2014, p. 67-194.

(152) Marco Roscini, « Cyber Operations as a Use of Force », *in* N. Tsagourias et R. Buchan (dir.), *op. cit.*, p. 250.

doit pas créer un nouveau déséquilibre ou aboutir à des résultats inéquitables. Le respect du principe de proportionnalité doit être apprécié au cas par cas en tenant compte « non seulement de l'élément purement "quantitatif" du préjudice subi mais [aussi] de facteurs "qualitatifs" comme l'importance de l'intérêt protégé par la règle violée et la gravité de la violation » (153). En revanche, le principe de proportionnalité n'impose pas à l'État lésé de répondre « en nature » en adoptant des contre-mesures dans le même domaine que les mesures initiales. Il laisse au contraire une large discrétion à cet égard aux États aussi longtemps que leur réponse ne se révèle pas excessive par rapport à l'acte qui l'a motivé.

• **Conditions procédurales (sommation, notification, procédure juridictionnelle en cours).** Le droit international impose aussi toute une série de conditions procédurales codifiées par l'article 52 du projet de la CDI. Avant d'adopter des contre-mesures, l'État lésé doit demander à l'État responsable, de s'acquitter des obligations qui lui incombent en vertu du droit international, puis notifier à l'État responsable la décision de prendre des contre-mesures et offrir de négocier avec cet État. L'État lésé peut, néanmoins, prendre les contre-mesures urgentes qui sont nécessaires pour préserver ses droits. Par ailleurs, et dans une logique de respect des mécanismes juridictionnels de règlement des différends, des contre-mesures ne peuvent être prises et, si elles sont déjà prises, doivent être suspendues sans retard indu si le différend est en instance devant une cour ou un tribunal habilité à rendre des décisions obligatoires pour les parties. En d'autres termes, là où le caractère « décentralisé » du système international est nuancé par l'existence d'un mécanisme obligatoire de règlement des différends, là où la justice institutionnelle s'est substituée à la « justice privée », la logique unilatérale des contre-mesures n'a plus de justification ni de raison d'être.

B) Légitime défense en cas d'agression armée

Contrairement aux contre-mesures qui, comme nous l'avons vu, ne peuvent pas impliquer le recours à la force armée, la légitime défense autorise les États à recourir à la force afin de riposter à une agression armée dirigée contre eux. La perspective d'invoquer la légitime défense en riposte à une cyberattaque a largement mobilisé la doctrine internationale et plusieurs études ont été publiées à cet égard pour examiner la question sous l'angle du *jus ad bellum* et du *jus in bello* (154). Pourtant, force est de constater que le débat sur ces questions a, pour l'instant, une dimension surtout théorique : jamais jusqu'ici un État n'a accusé officiellement, à notre connaissance, un autre État de mener contre lui une cyberattaque constituant un « acte d'agression » ; jamais un État n'a saisi le Conseil de sécurité d'une

(153) *ACDI 2001*, *supra* note 19, p. 145, §6.

(154) Voir surtout : M. Roscini, *Cyber Operations and the Use of Force in International Law*, New York, Oxford University Press, 2014 ; M. Schmitt (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.* ; et plusieurs études *in* N. Tsagourias et R. Buchan (dir.), *op. cit.*

telle question ; et jamais un État n'a invoqué l'article 51 de la Charte pour riposter à une cyberattaque dont il se considérait être la victime.

Le débat a donc largement un caractère prospectif et il existe, peut-être, une disproportion entre l'intérêt de la doctrine pour les questions de *jus ad bellum* et *jus in bello* relatives aux cyberattaques et la pratique qui montre que les réactions à des cyberattaques relèvent presque exclusivement pour l'instant du « droit de la paix » et des catégories que nous avons examinées dans le reste de cette étude. Pourtant, compte tenu des prédictions de Cassandre selon lesquelles l'espace numérique pourrait devenir rapidement un lieu de confrontation armée entre les États et donner lieu à des « *cyber Pearl Harbor* » (155), on peut aisément comprendre l'anticipation du milieu académique. On peut aussi comprendre pourquoi plusieurs États ou organisations internationales (156) se sont penchées sur ces questions en élaborant des stratégies nationales en matière de cyberdéfense ou des doctrines internationales pour envisager différentes hypothèses possibles.

Tenant compte de ces considérations et aussi de l'ampleur des études publiées sur la « cyber-guerre », nous nous limiterons ici à quelques observations rapides en examinant les conditions de déclenchement (a) et les conditions d'exercice (b) de la légitime défense en riposte à une cyberattaque.

a) Condition de déclenchement : l'existence d'une agression armée

Pour qu'un État puisse invoquer la légitime défense pour répondre par des moyens militaires (ou assimilés) à une cyberattaque il faut que cet État soit la victime d'une « agression armée ». Selon, en effet, les termes de l'article 51 de la Charte des Nations Unies :

> « Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. Les mesures prises par des Membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité et n'affectent en rien le pouvoir et le devoir qu'a le Conseil, en vertu de la présente Charte, d'agir à tout moment de la manière qu'il juge nécessaire pour maintenir la paix et la sécurité internationales ».

Il convient de remarquer, à cet égard, que la Charte des Nations Unies présente la légitime défense comme un « droit naturel ». Il s'agit en réalité d'une *exception* au principe général de l'interdiction du recours à la force (157).

(155) Selon la phrase célèbre de l'ancien ministre de la Défense américain Leon Panetta. Voir Elisabeth BUMILLER et Thom SHANKER, « Panetta Warns of Dire Threat of Cyberattack », *NY Times*, 12 octobre 2012.

(156) Voir par exemple la Déclaration du Sommet du Pays de Galles de l'Otan, adoptée en 2014, par laquelle les pays membres de l'Otan ont adopté leur « Politique de cyberdéfense renforcée », ont affirmé « dès lors que la cyberdéfense relève de la tâche fondamentale de l'Otan qu'est la défense collective » et ont souligné qu'il reviendrait au Conseil de l'Atlantique Nord de décider, au cas par cas, des circonstances d'une invocation de l'article 5 à la suite d'une cyberattaque » (§72) (www.nato.int/cps/en/natohq/official_texts_112964.htm).

(157) Pour une analyse voir T. CHRISTAKIS et K. BANNELIER, « La légitime défense en tant que "circonstance excluant l'illicéité" » *in* Rahim KHERAD (dir.), *Légitimes défenses*, Paris, LGDJ, 2007, p. 233-256.

La conséquence juridique est qu'il appartient à l'État qui invoque ce « droit » d'exception de prouver la réunion des conditions nécessaires pour son existence. Le fardeau de la preuve appartient donc à celui qui se prévaut d'une situation de légitime défense.

Pour qu'un État puisse invoquer la légitime défense, il faut qu'il soit victime d'une **agression « armée »**. Certes, cette agression armée peut prendre des formes diverses. Au-delà des hypothèses classiques, comme l'invasion ou le bombardement du territoire d'un État, il existe d'autres hypothèses, comme l'attaque de la marine ou de l'aviation d'un État, l'envoi de forces paramilitaires, de mercenaires, etc. Il convient de souligner que la nature des armes utilisées importe peu : une agression peut être perpétrée par des armes conventionnelles, des armes de destruction massive, voire des **armes « par destination »** comme l'utilisation des forces de la nature (détournement d'un fleuve, irruption provoquée d'un volcan, etc.) à des fins hostiles. De ce point de vue, il n'existe aucun doute sur le fait qu'une agression armée peut être perpétrée en utilisant des moyens numériques, à condition que les effets d'une telle « cyberattaque » soient similaires à ceux qui résultent de l'utilisation d'armes classiques.

Ceci nous amène à un autre critère qui est celui de la **gravité** : pour être qualifiée « d'agression » (et permettre donc une action en légitime défense) une attaque doit avoir une certaine gravité. Un recours limité à la force donc, comme un incident de frontière (une patrouille militaire qui tire sur une autre patrouille), constitue certes une violation de l'article 2 §4 de la Charte, engageant la responsabilité internationale de son auteur mais ne constitue pas forcément une « agression » et ne permet donc pas à l'autre État d'invoquer la légitime défense. La Cour internationale de justice a eu l'occasion de souligner ce point à plusieurs reprises, par exemple dans l'affaire des *Activités militaires au Nicaragua* (en 1986), où elle a souligné qu'« il y a lieu de distinguer entre les formes les plus graves de l'emploi de la force (celles qui constituent une agression armée) et d'autres modalités moins brutales ». L'idée est d'éviter le risque d'escalade qui pourrait exister si les États entreprenaient trop facilement des actions militaires en légitime défense pour répondre à des incidents mineurs. En conclusion, une cyberattaque qui aurait des effets limités sur le territoire de l'État victime pourrait constituer une violation du droit international sans pour autant être considérée comme une « agression armée » donnant la possibilité à l'État victime d'invoquer la légitime défense.

Une autre question fondamentale est de savoir **qui peut commettre** une agression. On accepte traditionnellement en droit international que seul un État peut commettre une agression contre un autre État. Or, depuis surtout les attentats du 11 septembre 2001, plusieurs auteurs ont soutenu que des groupes *infra*-étatiques pourraient aussi commettre une « agression armée » au sens de l'article 51 et que cette notion devrait couvrir toute personne susceptible de lancer une attaque d'une certaine gravité, quelle que soit sa qualité. La légitime défense pourrait donc, selon cette théorie, être exercée non seulement à l'encontre d'autres États,

mais aussi contre des groupes *infra*-étatiques comme des groupes terroristes (dont *Al-Qaïda* ou *Daesh*). L'acceptation d'une telle théorie n'est pas sans problème. Le problème majeur est, bien sûr, le fait que ces groupes n'ont pas d'assise territoriale propre et se trouvent sur le territoire d'États qui, parfois, n'ont pas la possibilité de s'en débarrasser. Or, toute action militaire contre ces groupes sans le consentement de l'État sur le territoire où ils se trouvent pourrait être considérée comme une violation de la souveraineté de cet État, voire comme un acte d'agression.

Le débat prend une dimension nouvelle dans le cadre d'une réaction à des cyberattaques qui pourraient être lancées par des acteurs privés. Pourrait-on accepter, par exemple, que le fait que des acteurs non-étatiques lancent une cyberattaque importante contre le territoire d'un État A depuis le territoire d'un État B, donne automatiquement à l'État A le droit de bombarder l'État B au titre de la « légitime défense » ? Quelles seraient les possibilités de riposte de l'État B dans une telle hypothèse, surtout s'il ignorait la présence des terroristes sur son territoire ou n'avait pas les moyens de les neutraliser ? C'est pour cette raison (et d'autres) que la Cour internationale de justice a adopté une démarche prudente en refusant l'application de la légitime défense en dehors des relations interétatiques. Ainsi, dans son avis consultatif du 9 juillet 2004 concernant les *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, la Cour a souligné que : « L'article 51 de la Charte reconnaît […] l'existence d'un droit naturel de légitime défense *en cas d'agression armée par un État contre un autre État* ». Malgré cette position de la Cour et le soutien ferme d'un grand nombre de pays (y compris le Mouvement des non-alignés, composé de 117 États, qui a souligné à plusieurs reprises ces dernières années que l'article 51 de la Charte ne devrait « ni être réécrit ni faire l'objet d'une nouvelle interprétation »), le débat continue à faire rage en droit international. Tous s'accordent néanmoins pour reconnaître que le droit positif accepte l'hypothèse d'une « agression indirecte » dans les cas où l'attaque armée commise par un groupe non-étatique est considérée comme une « agression » indirectement commise par un État, autorisant de ce fait à l'État victime de cette attaque d'invoquer la légitime défense pour déclencher une riposte militaire contre l'État qui a commis « l'agression » indirecte (158).

Last but not least, un autre débat doctrinal fait rage depuis quelques années : il concerne la question de savoir si un État pourrait, malgré l'énoncé clair de l'article 51 de la Charte, invoquer la légitime défense sans la présence effective d'une « agression armée ». Plus précisément, certains auteurs considèrent que le droit international reconnaît aujourd'hui la théorie de la « légitime défense préemptive », selon laquelle un État peut répondre à une menace d'agression imminente, tandis que d'autres sont allés jusqu'à soutenir la « légitime défense préventive », selon laquelle un État pourrait réagir face à ce qu'il considère être une menace

(158) Pour identifier dans quels cas l'action d'un acteur non-étatique pourrait être attribué à un État voir, entre autres, *infra* Partie III (3C).

lointaine, non encore concrétisée. Le *Manuel de Tallinn 1* a ainsi accepté la théorie de la « légitime défense préemptive » en matière de cyberattaques (159). Pourtant, une analyse approfondie de l'état actuel du droit positif semble montrer que celui-ci n'accepte ni la « légitime défense préventive » ni la « légitime défense préemptive » (160). La prudence s'impose donc dans un domaine où les risques d'abus et de déstabilisation du système international sont très importants.

b) Conditions d'exercice

Le respect des principes de nécessité et de proportionnalité. Comme l'a souligné la CIJ dans son avis consultatif rendu le 8 juillet 1996 dans l'affaire de la Menace ou de l'emploi d'armes nucléaires : « La soumission de l'exercice du droit de légitime défense aux conditions de nécessité et de proportionnalité est une règle du droit international coutumier ». On considère, traditionnellement, que les exigences de la « nécessité » et de la « proportionnalité » de l'action menée en légitime défense ne sont que les deux faces d'une même médaille. L'action militaire en légitime défense ne peut, en effet, être justifiée que s'il s'agit d'une mesure destinée à mettre fin à une agression armée, « nécessaire et proportionnelle » dans la mesure où l'État ne peut pas atteindre ce résultat (mettre fin à l'agression) par un comportement différent n'impliquant pas l'emploi de la force armée ou pouvant se limiter à un emploi plus restreint de cette force. Il va de soi que ce critère de proportionnalité pose des questions très difficiles et « techniques » que nous ne pouvons pas ici analyser (161). Mais le point fondamental est que, comme en matière de contre-mesures, la légitime défense ne doit viser qu'à repousser l'acte d'agression sans provoquer un nouveau déséquilibre.

La subordination à l'action du Conseil de sécurité. Selon l'article 51 de la Charte, les États ont une obligation procédurale : informer le Conseil des actions militaires en légitime défense. Le manquement à cette obligation de notification n'entraîne pas l'illicéité de l'action militaire en légitime défense en tant que telle (car une agression reste une agression) ; mais il constitue, une violation de la Charte et pourrait, d'ailleurs, avoir d'autres conséquences, lourdes pour son auteur. Ainsi, la Cour internationale de justice a considéré à plusieurs reprises que le fait qu'un État n'informe pas le Conseil de sécurité de ses actions militaires sur le territoire d'un autre État, pouvait être considéré comme un indice du fait que cet État ne se considèrait pas comme agissant en légitime défense. Parallèlement, l'article 51 indique que la légitime défense est un droit « subordonné » à l'action du Conseil de sécurité. On retrouve ici la vision « multilatéraliste » des rédacteurs

(159) Voir *Manuel de Tallinn 1*, *supra* note 12, « *Rule 15: The right to use force in self-defence arises if a cyber armed attack occurs or is imminent* ».

(160) Voir surtout O. Corten, *Le droit contre la guerre*, *op. cit*, p. 662-716 et T. Christakis, « Existe-t-il un droit de légitime défense en cas de simple "menace" ? Une réponse au "groupe de personnalités de haut niveau" de l'ONU » *in* SFDI, *Les métamorphoses de la sécurité collective*, Paris, Pedone, 2005, p. 197-222.

(161) Voir O. Corten, *Le droit contre la guerre*, *op. cit.*, p. 772-800.

de la Charte qui voulaient « bannir » autant que possible le recours unilatéral à la force dans les relations internationales : l'action unilatérale en légitime défense n'est considérée comme « nécessaire » (et n'est donc justifiée) qu'en l'absence de mesures appropriées de sécurité collective. Comme nous l'avons dit en introduction jamais, à notre connaissance, un État n'a saisi le Conseil de sécurité considérant qu'il est victime d'une agression armée du fait d'une « cyberattaque ». L'hypothèse reste donc théorique pour l'instant.

PARTIE III. *Hack-back*, « cyberdéfense active » et le besoin d'un système international ordonné

Introduction : le rôle important des acteurs privés en cas de cyberattaque

A) Défense passive

B) Attribution des cyberattaques

C)* hack-back *et « cyberdéfense active »

1. Arguments en faveur et contre le *hack-back*

***A) Intérêt et avantages du* hack-back**

B) Inconvénients et risques

2. Le *hack-back* « sauvage » : les acteurs privés peuvent-ils déclencher unilatéralement des mesures cyber-offensives ?

A) L'inexistence d'un « droit de* hack-back *» en droit international

B) Une violation du droit international ?

C) Le* hack-back *en tant que violation du droit interne

3. Le *hack-back* « encadré » : les États peuvent-ils s'appuyer sur des acteurs privés pour conduire des contre-attaques ?

A) Une coopération entre les acteurs publics et privés pour répondre aux cyberattaques ?

B) Le cas des Entreprises militaires et de sécurité privées (EMSP)

C) La responsabilité internationale des États peut-elle être engagée du fait de mesures de* hack-back *conduites par des acteurs privés ?

III. *Hack-back*, « cyberdéfense active » et le besoin d'un système international ordonné

Introduction : le rôle important des acteurs privés en réponse aux cyberattaques

Les entreprises du secteur privé spécialisées en matière de cybersécurité jouent un rôle de plus en plus important en matière de prévention et de réaction aux cyberattaques et ceci au moins à trois niveaux : défense passive (A), attribution des cyberattaques (B), *hack-back* et autres activités de « cyberdéfense active » (C).

A) Défense passive

Elles interviennent, tout d'abord, dans une logique de défense passive (162) afin de protéger les systèmes d'information et les données de leurs clients qui sont tantôt des personnes morales de droit privé, tantôt des institutions de droit public, tantôt des personnes physiques. Elles développent alors des systèmes de pare-feu et des dispositifs anti-intrusion et aident aussi leurs clients à surveiller leurs réseaux, mettre à jour des logiciels, évaluer les risques, détecter et corriger des vulnérabilités et, de façon plus générale, à adopter des politiques efficaces d'hygiène et de sécurité informatique.

B) Attribution des cyberattaques

Un deuxième domaine où des entreprises du numérique interviennent de façon croissante est celui de l'attribution des cyberattaques. Cette fonction prend deux formes principales.

a) En juin 2012, Google annonçait que désormais il avertirait ses usagers en cas de piratage par des États. Google a ainsi expliqué que si une intrusion des comptes de ses usagers était soupçonnée ces derniers recevraient le message suivant : « ***Warning:*** *We believe state-sponsored attackers may be attempting to compromise your account or computer. Protect yourself now* » (163). De manière similaire, Facebook annonçait en octobre 2015 qu'il enverrait une notification à ses utilisateurs s'il estimait que leur compte avait été piraté par une personne soupçonnée

(162) Ce terme renvoie de façon générale aux « *Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative* ». Ministère américain de la Défense, *Dictionary of Military and Associated Terms, Joint Publication 1-02*, novembre 2010 (modifié en février 2016), p. 181 (www.dtic.mil/doctrine/new_pubs/jp1_02.pdf).

(163) Voir Eric Grosse, « Security Warnings for Suspected State-Sponsored Attacks », 5 juin 2012 (https://security.googleblog.com/2012/06/security-warnings-for-suspected-state.html).

de travailler pour une force gouvernementale (164). Yahoo (165) et Microsoft (166) ont suivi en décembre 2015, alors que Twitter, sans annoncer une politique similaire, a averti plusieurs activistes politiques d'intrusions similaires (167). Toutes ces compagnies technologiques ont accompagné leurs annonces de la précision selon laquelle « pour protéger l'intégrité de leurs méthodes et de leurs processus » elles ne « pourront pas expliquer comment elles attribuent certaines attaques aux *hackers* suspectés » mais que la notification aura lieu « seulement dans les situations où les preuves recoupent fortement leurs soupçons » (168). L'objectif affiché de ces notifications est que la personne piratée change son mot de passe et mette en place des mesures de sécurité.

b) La deuxième grande fonction en matière d'attribution concerne certaines entreprises spécifiquement spécialisées dans ce domaine qui offrent leurs services à des clients privés ou publics. C'est ainsi, par exemple, que des entreprises de cybersécurité comme FireEye, Novetta, Mandiant ou CrowdStrike ont été particulièrement actives ces dernières années dans ce domaine accusant des gouvernements étrangers de se cacher derrière certaines cyberattaques importantes, allant de plusieurs cas de vol de la propriété intellectuelle et de cyber-espionnage industriel (169) au piratage du Parti démocrate lors des élections américaines de 2016 (170).

Ce rôle croissant des entreprises privées en matière d'attribution des cyberattaques soulève plusieurs questions politiques et juridiques. Pour la première fois peut-être dans l'histoire du droit international, l'imputation d'un fait à l'État (aux conséquences importantes en matière de réaction et de responsabilité) est assumée principalement par des acteurs privés en lieu et place des acteurs publics traditionnels, à savoir les États victimes. On peut d'ailleurs imaginer que cette « attribution privée » pourrait, dans certains cas, être encouragée par des États réticents, pour différentes raisons, à assumer eux-mêmes ce rôle. Mais ce « partenariat » occulte et

(164) Alex Stamos, « Notifications for Targeted Attacks », Facebook, 17 octobre 2015 (www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766/).

(165) Bob Lord, « Notifying Our Users of Attacks by Suspected State-Sponsored Actors », Yahoo, 21 décembre 2015 (https://yahoo-security.tumblr.com/post/135674131435/notifying-our-users-of-attacks-by-suspected).

(166) Scott Charney, « Additional steps to help keep your personal information secure », Microsoft, 30 décembre 2015 (https://blogs.microsoft.com/on-the-issues/2015/12/30/additional-steps-to-help-keep-your-personal-information-secure/).

(167) Voir Bethany Horne, « Twitter 'leaving us in the dark' over state hacking claims, activists say », *The Guardian*, 4 février 2016 (www.theguardian.com/technology/2016/feb/04/twitter-leaving-us-in-the-dark-over-state-hacking-claims-activists-say).

(168) Selon la phrase utilisée par Facebook. Voir aussi l'avertissement de Google : « *You might ask how we know this activity is state-sponsored. We can't go into the details without giving away information that would be helpful to these bad actors, but our detailed analysis—as well as victim reports—strongly suggest the involvement of states or groups that are state-sponsored* ».

(169) Pour plusieurs exemples voir K. Eichensehr, « The Private Frontline in Cybersecurity Offense and Defense », *Just Security*, 30 octobre 2014 (http://justsecurity.org/16907/private-frontline-cybersecurity-offense-defense/) ou K. Eichensehr, « Public-Private Cybersecurity », *Texas Law Review* n° 95, 2017, p. 19-23.

(170) Voir par exemple Ellen Nakashima, « Cybersecurity firm finds evidence that Russian military unit was behind DNC hack », *The Washington Post*, 22 décembre 2016 (www.washingtonpost.com/).

informel en matière d'attribution est, comme il a été justement remarqué, fragile et même dangereux [171] : les motivations des compagnies privées de cybersécurité (guidées par leurs intérêts commerciaux et la recherche de gains et se faisant d'ailleurs une belle publicité en attribuant des attaques à des États puissants) ne sont pas nécessairement les mêmes que celles d'un État qui doit protéger sa sécurité nationale, ses personnes morales et physiques. L'action intempestive d'une entreprise privée mal coordonnée avec l'État pourrait avoir des répercussions négatives sur sa politique étrangère et créer des tensions avec l'État accusé par la compagnie privée. Quant aux méthodes et techniques utilisées, elles pourraient nécessiter un contrôle étroit de la part de l'État pour vérifier la pertinence de l'attribution.

C) Hack-back *et « cyberdéfense active »*

Sans négliger les questions importantes posées par le rôle du secteur privé en matière d'attribution, c'est sur un troisième domaine d'intervention du secteur privé en matière de cybersécurité que nous nous concentrerons, celui des mesures offensives adoptées pour contrer une cyberattaque, atténuer ses effets et prévenir sa répétition. La pratique du « *hack-back* » est fondée sur l'idée que « *the best defense is a good offense* ».

Le terme de « *hack-back* », ou « *hacking back* » ou encore « *reverse hacking* », ne connaît pas vraiment de définition officielle et pratiquement aucune organisation internationale ne s'est jusqu'à présent véritablement penchée sur cette question capitale mais hautement sensible. Ce terme, qui pourrait être traduit en français par « contre-piratage », « piratage en retour » ou encore « contre-fouiner » [172], décrit une activité aisément compréhensible : le fait, pour la victime d'une cyberattaque, de riposter contre son auteur. Le terme « *hack-back* indique ainsi que la riposte à une cyberattaque peut utiliser des techniques pratiquement aussi variées que l'attaque (« *hacking* ») elle-même [173].

Toutefois, pour éviter de qualifier la victime qui réagit à une attaque de « *hacker* » (en « retour » certes, mais « *hacker* » quand même) on a tendance à

(171) K. Eichensehr, « Public-Private Cybersecurity », *op. cit.*, p. 23.

(172) Il est à noter que la Délégation générale à la langue française et aux langues de France du ministère de la Culture et de la Communication, conjointement avec la Commission générale de terminologie et l'Académie française, propose comme traduction française pour le nom « *hacker* » le mot « fouineur » (voir par exemple www.gouvernement.fr/top-10-des-mots-d-internet-que-vous-allez-oser-dire-en-francais). Si on suivait cette proposition, il faudrait ici traduire « *hacking-back* » par « contre-fouiner ». Pour des raisons de commodité et pour éviter les confusions nous allons utiliser ici le terme anglais « *hack-back* ».

(173) Comme l'avait déjà écrit Renee Albersheim en 1999 : « *reverse hacking involves striking back at a hacker. A hacker is someone who through various technical means gains access to a computer system without authorization. With a reverse hack, a system administrator identifies the hacker as he enters the system, and sends a response back in kind. The purpose is to prevent damage to the administrator's system, while damaging the attacker's system in the hope that this will deter the hacker from attempting to try again* ». R. Albersheim, « The Legal Implications of Corporate Reverse Hacking », *Preventive Law Reporter*, vol. 18, été 1999, p. 8.

préférer l'emploi d'un euphémisme, celui de « cyberdéfense active ». Ce néologisme (174) permet non seulement d'éviter l'utilisation de termes pouvant avoir une connotation péjorative pour qualifier la réaction de la victime, mais il permet aussi d'apporter un fort degré de légitimation à la réaction de la victime en renvoyant de manière implicite au concept juridique de la « légitime défense ». Par ailleurs, cette expression occulte le caractère offensif des mesures adoptées : il ne s'agit pas d'une contre-offensive mais d'une « défense active ». Évidemment, tout cela ne va pas sans rappeler la fameuse réponse que Talleyrand avait donnée alors qu'on lui demandait de définir le terme « non-intervention » : « C'est un mot métaphysique et politique qui signifie à peu près la même chose qu'intervention », avait-il répondu.

La lecture de la littérature consacrée à ce domaine montre que l'expression « cyberdéfense active » est utilisée pour décrire des activités variées qui vont de la « défense passive » décrite plus haut (installer et *activer* un pare-feu ou un anti-virus pourrait en effet être qualifié de « cyberdéfense *active* ») à certaines techniques particulièrement agressives comme la destruction des réseaux, systèmes ou données de l'adversaire, en passant par d'autres mesures telles que la déconnexion, l'inactivation de *botnets*, la suspension temporaire de la fonctionnalité d'un système ou de l'accès aux données, etc. Certaines techniques sont d'ailleurs difficiles à situer précisément entre les deux extrémités (passives/offensives) du spectre des cyberdéfenses possibles. Il en va ainsi, par exemple, avec les fameux « pots de miel » (« *honeypots* ») destinés à attirer des adversaires déclarés ou potentiels pour les identifier et éventuellement les neutraliser (175). Ces pots de miel ont pour fonction principale d'attirer les pirates vers un espace précis afin de les démasquer mais ils peuvent aussi permettre de surveiller le système de l'adversaire afin de mieux anticiper et prévenir des attaques futures. Dans une logique plus agressive, les « pots de miel » pourraient aussi être utilisés pour introduire dans le système de l'adversaire des capacités cyber-offensives susceptibles de voler ou détruire des données, suspendre le fonctionnement des réseaux ou provoquer un dommage irréversible à ses systèmes informatiques.

Pour les besoins de cette étude, nous préférons donc ne pas utiliser ce terme polysémique de « cyberdéfense active » et nous utiliserons le terme de « *hack-back* » afin de nous concentrer sur les techniques de riposte offensive. Nous présenterons

(174) Si ce terme est relativement nouveau dans le contexte cyber, le terme « défense active » avait déjà été utilisé (non sans soulever des controverses) dans le contexte de la guerre conventionnelle dès 1974. Le ministère américain de la Défense, dans le *Dictionary of Military and Associated Terms*, définit la « défense active » comme « *the employment of limited offensive action and counterattacks to deny a contested area or position to the enemy* ». Pour l'histoire de ce terme et sa transposition dans le domaine cyber voir Robert M. Lee, « The Sliding Scale of Cyber Security », *SANS Analyst White Paper*, SANS Institute InfoSec Reading Room, 2015, p. 9-11 (www.sans.org/readingroom/whitepapers/analyst/sliding-scale-cyber-security-36240) et « Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats », *Project Report*, George Washington University Center for Cyber and Homeland Security, octobre 2016, p. 6-8 (https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf).

(175) Voir par exemple DELL, « Les Hackers dans le piège du pot de miel », *La revue de l'IT* (www.dell.com/learn/fr/fr/frbsdt1/campaigns/revueit-securite-hackers-honeypot-piege-pot-miel).

tout d'abord les arguments qui sont généralement avancés pour soutenir le *hack-back* tout en montrant les risques et inconvénients de cette pratique (1). Nous procéderons ensuite à une analyse du droit international qui permet de distinguer le *hack-back* « sauvage » et non contrôlé, pratiqué de façon unilatérale par le secteur privé, qui ne trouve aucun appui en droit international (2) du *hack-back* « encadré », entrepris sous l'impulsion et le contrôle étroit de l'État, qui, tout en posant certaines difficultés, peut être admis en droit international (3).

1. Arguments en faveur et contre le *hack-back*

Plusieurs arguments ont été mobilisés pour soutenir le *hack-back* (A) mais les risques et inconvénients de cette pratique sont nombreux (B).

A) Intérêt et avantages du hack-back

Au moins six arguments ont été avancés [(176)] pour vanter les vertus du *hack-back*.

a) Le hack-back pourrait remédier aux insuffisances de l'action gouvernementale

L'un des arguments phares avancés en faveur du *hack-back* est que les gouvernements ne sont pas en mesure de protéger efficacement les personnes morales et physiques contre les cyberattaques. L'action gouvernementale, décrite comme lente et semée d'embûches, n'offrirait *in fine* que peu de garanties aux victimes. Le *hack-back* permettrait donc d'éviter les lenteurs d'un pouvoir exécutif et juridictionnel parfois peu enclin ou capable d'agir dans l'espace numérique. Comme le notait Jan Messerschmidt :

> « *Hackbacks avoid some of the most troublesome challenges of traditional remedies, including "lengthy prosecutions, thorny jurisdictional matters, technologically unsophisticated juries, and slow courts" which are unhelpful when viruses and worms can propagate at remarkable speeds. Traditional law enforcement typically lacks the resources or the expertise to adequately respond to cyber attacks, and is largely ineffective in cases of cross-border intrusions* » [(177)].

Sur le plan éthique, l'incapacité de l'État d'agir de façon efficace pour protéger les personnes morales et physiques contre les cyberattaques, ouvrirait la voie à une dérogation au « contrat social » qui avait transféré à l'État souverain le « monopole de la contrainte légitime » :

(176) Parmi les *policy papers* qui prennent la défense du *hack-back* voir par exemple Irving Lachow, « Active Cyber Defense: a Framework for Policymakers », *Center for a New American Security*, 22 février 2013 (www.cnas.org/publications/policy-briefs/active-cyber-defense-a-framework-for-policymakers) et Patrick Lin, « Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies », *A Policy Paper on Cybersecurity*, *Ethics+Emerging Sciences Group*, 26 septembre 2016 (http://ethics.calpoly.edu/hackingback.pdf).

(177) J.E. Messerschmidt, « Hacback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm », *Columbia Journal of Transnational Law*, vol. 52, n° 1, 2013, p. 293. Voir aussi Neal Katyal, « Community Self-Help », *Journal of Law, Economics and Policy*, n° 1, 2005, p. 60.

« *[I]f there is a social contract to swap our natural executive powers for collective security—a reasonable arrangement—it seems premised on the ability of the state to live up to its purpose of protecting us. If the state fails in this duty with respect to a particular threat, the entire social contract is not necessarily voided, but the state's monopoly on violence could be apportioned back to citizens to defend ourselves* » (178).

b) Le hack-back serait plus rapide et efficace

Ce deuxième argument s'inscrit dans la continuité du premier : les cyberattaques nécessiteraient une réponse immédiate afin de contrer efficacement l'adversaire. Mieux encore, elles appelleraient en amont un travail d'anticipation passant par le développement de leurres permettant de tracer les activités des pirates dans le système de l'entreprise, d'attribuer l'attaque et de prévenir, par le biais de techniques de cyberdéfense active de nouvelles attaques. Se contenter d'une approche purement « réactive » de l'État signifierait donc laisser l'initiative à l'adversaire. Par ailleurs, compte tenu de l'expertise technique et de la puissance des grands acteurs du numérique (Google, Microsoft, Apple etc.) et des compagnies spécialisées en cybersécurité, les réponses privées pourraient s'avérer plus efficaces que les réponses publiques. On se souvient d'ailleurs que le « *hack-back* » a été popularisée par la réponse immédiate de Google à la cyberattaque baptisée par McAfee « *Opération Aurora* ». Fin 2009, Google avait réalisé qu'elle était victime d'une cyberattaque importante et sophistiquée. Elle avait alors considéré qu'une riposte immédiate était indispensable pour éviter le vol et les modifications de codes sources, identifier les pirates et mettre fin à l'opération. La contre-attaque lui a permis d'établir qu'une trentaine d'autres entreprises, principalement américaines, étaient visées par l'opération – et de leur communiquer, ainsi qu'aux forces de l'ordre, des informations à cet égard (179).

Ce besoin d'auto-protection rapide serait d'autant plus important que le développement de l'« internet des objets » (*Internet of Things – IoT)* qui s'accompagne de la mise sur le marché de milliards d'objets connectés (180) pouvant être mobilisés dans le cadre de cyberattaques rend une réaction gouvernementale rapide de plus en plus compliquée.

c) Le hack-back *aurait un effet dissuasif important*

L'effet dissuasif du *hack-back* a souvent été plaidé par ses partisans. Dans un rapport célèbre publié en mai 2013, la *Commission on the Theft of American Intellectual Property* recommandait au gouvernement et au Congrès américains de

(178) P. Lin, « Ethics of Hacking Back: Six Arguments from Armed Conflict to Zombies », *op. cit.*, p. 8.

(179) Voir Kim Zetter, « Google Hack Attack Was Ultra Sophisticated, New Details Show », *Wired*, 14 janvier 2010 (www.wired.com/2010/01/operation-aurora/).

(180) Les estimations sur le nombre des objects qui seront connectés à l'*Internet of Things* d'ici 2020 varient de 26 milliards à un chiffre incroyable de 212 Mds ! Voir Michael Miller, *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World*, Indianapolis, Que Publishing, p. 12.

donner la possibilité aux entreprises américaines de riposter aux cyberattaques dans une logique de « *threat-based deterrence* ». Selon la Commission :

> « *Effective security concepts against targeted attacks must be based on the reality that a perfect defense against intrusion is impossible. The security concept of threat-based deterrence is designed to introduce countermeasures against targeted hackers to the point that they decide it is no longer worth making the attacks in the first place* » (181).

L'idée est qu'une réaction rapide et musclée par le secteur privé pourrait faire augmenter de manière significative les risques et les coûts pour les pirates et les pousser à renoncer à de futures cyberattaques. Si un *hacker* potentiel sait qu'une compagnie comme Google va contre-attaquer (182) et qu'il y aura des conséquences graves pour lui, il serait logique de s'abstenir. Des analogies avec la dissuasion nucléaire ont même été opérées. Pourtant, il existe une grande différence de contexte entre les deux situations (183) et, comme nous le verrons, l'effet dissuasif du *hack-back* est loin d'être assuré dans certains cas.

d) Le hack-back *permettrait aux entreprises de ne pas dévoiler leurs vulnérabilités*

Les entreprises pourraient se montrer réticentes à l'idée de coopérer avec l'État et pourraient de ce fait préférer assurer elles-mêmes leur défense, passive ou active.

Elles pourraient en effet craindre qu'un appel à l'État rende publique leurs failles de sécurité et autres vulnérabilités. Ceci pourrait affecter négativement la réputation de l'entreprise (désignée, par exemple, comme incapable de protéger les données de ses clients), impacter la valeur de l'action de l'entreprise en bourse (184) (ou celle de ses obligations) ou encore être utilisé par des concurrents (185).

De façon plus générale, les compagnies privées pourraient aussi ne pas souhaiter que les services de l'État accèdent à leurs systèmes, à leurs données et celles de leurs clients. Les révélations de Snowden ont montré l'ampleur de la surveillance de masse entreprise par les services secrets de certains États et la multiplication des lois de surveillance à travers le monde n'apaise pas ces craintes. Sur un plan institutionnel, une solution pourrait être une séparation organique au sein des États

(181) The Commission on the Theft of American Intellectual Property, *The IP Commission Report*, mai 2013, p. 80 (www.ipcommission.org/).

(182) Comme cela a été écrit dans un *blog* technologique après le *hack-back* de Google lors de l'*opération Aurora* : « *it's pretty awesome: If you hack Google, they will haek your ass right back* ». Cité par J.E. Messerschmidt, *supra* note 177, p. 277.

(183) Entre autres choses, la dissuasion nucléaire n'impliquait qu'un nombre très limité d'acteurs étatiques, connus et se menaçant d'une « destruction mutuelle assurée » (*MAD*) en cas d'attaque nucléaire. Rien de tel dans le cyberespace où les auteurs potentiels et les victimes de cyberattaques sont innombrables.

(184) À titre d'exemple, l'action de Gemalto a dégringolé de 9 % après les révélations selon lesquelles la *NSA*, l'agence de sécurité nationale américaine, et son homologue britannique, le *GCHQ*, auraient dérobé les clés de cryptage du premier fabricant mondial de cartes *SIM*. Voir « L'action chute après le piratage par la *NSA* de ses clés de cryptage *SIM* », *Les Échos*, 20 février 2015 (https://investir.lesechos.fr/actions/actualites/l-action-chute-apres-le-piratage-par-la-nsa-de-ses-cles-de-cryptage-sim-1033016.php).

(185) Pour une analyse voir J.E. Messerschmidt, *supra* note 177, p. 293-294.

entre les activités de renseignement et de cybersécurité. L'exemple de la France pourrait être utile à cet égard car l'agence nationale de cybersécurité, l'ANSSI [186], est placée en dehors de la communauté du renseignement. Ceci permet de favoriser la coopération de l'ANSSI avec les entreprises privées et les autres administrations, d'ordinaire moins enclines à coopérer avec les services de renseignement, tout en favorisant une gestion responsable des vulnérabilités informatiques.

e) Le hack-back *permettrait de résoudre des problèmes délicats d'extraterritorialité*

Un autre avantage du *hack-back* serait qu'il permettrait d'éviter des questions délicates d'extraterritorialité. Comment, en effet, un État pourrait-il exercer sa protection à l'égard de personnes morales (ou physiques) situées à l'étranger, victimes de cyberattaques ? Certes, en vertu de sa compétence personnelle reconnue par le droit international, l'État peut agir pour la protection de ses nationaux à l'étranger, mais une telle action peut se heurter à l'exercice de la compétence territoriale de l'État sur lequel se trouvent ces personnes. Inversement, comment un État pourrait-il assurer la protection des compagnies étrangères qui se trouvent sur son territoire et quelles difficultés pourraient émerger à cet égard (y compris en ce qui concerne les risques de cyber-espionnage industriel et les objectifs de confidentialité et de discrétion évoqués *supra*). Le *hack-back* permettrait d'éviter ces difficultés en donnant à ces entreprises la possibilité de se défendre elles-mêmes contre les cyberattaques sans avoir à ouvrir leurs systèmes informatiques aux États.

f) Le hack-back *serait bon pour les affaires et pour la recherche*

Enfin, le *hack-back* serait riche d'un énorme potentiel en termes de croissance pour l'industrie spécialisée dans la cyberdéfense active. Compte tenu de l'ampleur des menaces, le marché de la cybersécurité est particulièrement lucratif. Malgré les doutes qui persistent à propos de la légalité des activités de *hack-back*, les compagnies proposant des outils de cyberdéfense active se multiplient, qu'il s'agisse d'entreprises spécialisées en matière de cybersécurité ou de grands acteurs industriels qui développent des activités dans ce domaine pour ne pas manquer ce qu'ils considèrent comme « *a vast private-sector market emerging for cybersecurity solutions* » [187].

B) Inconvénients et risques

Le *hack-back* comporte différents risques : risques pour le système international et sa stabilité, risques pour les États, risques aussi pour les entreprises. Nous présenterons ici dix de ces principaux risques.

(186) Agence nationale de la sécurité des systèmes d'information (www.ssi.gouv.fr/).

(187) Voir Loren Thompson, « Lockheed Martin Moves To Dominate Cyber Defense of Electric Grid & Energy Complex », *Forbes*, 14 mars 2014 (www.forbes.com/sites/lorenthompson/2014/03/14/lockheed-martin-moves-to-dominate-cyber-defense-of-electric-grid-energy-complex/).

a) Risques d'escalade

L'utilisation par des acteurs privés de techniques cyber-offensives contre des acteurs non-étatiques qui se situent sur le territoire d'un autre État, voire contre l'État lui-même, pourrait entraîner une rapide escalade, transformant un événement relativement isolé initialement en une véritable crise internationale. L'État étranger visé par l'attaque (ou qui souhaiterait défendre ses nationaux) pourrait riposter en dénonçant l'attribution de la cyberattaque initiale comme erronée ou en dénonçant les mesures de *hack-back* comme étant ni nécessaires ni proportionnées compte tenu des circonstances. Cette riposte pourrait elle-même générer une contre-riposte de l'autre État qui pourrait souhaiter défendre son entreprise doublement victime à ses yeux. Le *hack-back* conduirait ainsi à enfermer les États dans un dangereux cercle vicieux de contre-réactions. Suivant un autre scénario, des États tiers dont les personnes morales ou physiques seraient les victimes collatérales de mesures de *hack-back* pourraient aussi décider d'agir contre l'auteur du *hack-back*.

De telles situations seraient évidemment en totale contradiction avec les buts du droit international contemporain qui propose aux États différents mécanismes de règlement pacifique de leurs différends (ou de ceux affectant leurs nationaux et leurs biens). Comme montré dans les Parties I et II, la réaction normale en cas de cyberattaque devrait être de s'adresser à l'État d'où émane l'attaque en lui demandant d'agir d'urgence pour mettre fin à celle-ci conformément à son obligation de diligence due. La coopération (y compris dans sa dimension pénale), le développement d'opérations conjointes et le recours aux mécanismes de règlement pacifique des différends devraient être privilégiés. À supposer même que ces mécanismes s'avèrent impossibles ou impraticables compte tenu des circonstances (par exemple en cas d'urgence), le droit international a confié aux États la tâche de réagir en utilisant les moyens décrits dans la Partie II. Laisser les entreprises « se faire justice elles-mêmes » avec les risques d'escalade que cela comporte pourrait aboutir à une augmentation spectaculaire des menaces pour la sécurité internationale.

b) Risques de déstabilisation

Ces risques sécuritaires pourraient facilement déstabiliser le système international. Si le *hack-back* est autorisé par un État et pratiqué par ses entreprises, il est très probable que d'autres États (voire tous les États) suivront cette voie. Le droit international étant fondé sur le principe de réciprocité, une telle voie devrait inévitablement aboutir à une symétrie juridique entre les entreprises des différents États. Le *hack-back* ne pourra pas juridiquement être réservé aux entreprises de certains pays, il pourra théoriquement être exercé par n'importe quelle entreprise située dans n'importe quel pays du monde. Quand on connaît les difficultés rencontrées par le droit international pour arriver à ériger des normes de coexistence pacifique entre moins de 200 États, on n'ose à peine imaginer ce qui pourrait se

produire si l'on donnait licence aux quelque 200 millions d'entreprises existantes de par le monde de lancer des attaques transfrontières en pratiquant le *hack-back*…

c) Risques pour l'autorité de l'État

Au-delà de l'ordre international, l'ordre interne pourrait lui-même être menacé. Accepter l'idée selon laquelle « les États ne sont pas capables de garantir la sécurité dans le cyberespace », que le « contrat social » est donc brisé et que le monopole de la violence légitime de l'État est ainsi remis en cause (voir *supra*) pourrait s'avérer dangereux. L'ordre juridique étatique est fondé sur l'idée d'une substitution de la justice institutionnelle à la justice privée qui prévalait à « l'état de nature » avant la création des sociétés civilisées (188). Remettre en cause l'adage « nul ne peut se faire justice à soi-même » serait autoriser des comportements anti-sociaux susceptibles de semer le désordre. Certes, les États pourraient théoriquement éviter une érosion de leur pouvoir de régulation et d'exécution en interdisant le *hack-back* « interne » tout en autorisant le « *hack-back* » transnational. L'aveu d'impuissance de l'État face aux cyberattaques transfrontières et son abdication à cet égard n'enverraient pas moins un message désastreux pour l'autorité de l'État et sa capacité à exercer ses fonctions régaliennes face aux nouvelles menaces.

d) Risques pour la conduite de la politique étrangère

Une action de *hack-back* intempestive ou mal coordonnée et entreprise sans concertation avec les autorités publiques, pourrait générer des tensions diplomatiques et compliquer la conduite de la politique étrangère d'un pays. Ceci est particulièrement évident lorsque des compagnies privées de cybersécurité attribuent publiquement une cyberattaque à un État étranger. Des auteurs ont par exemple fait remarquer que la publication du rapport Mandiant en février 2013 « *set off a bomb in one of the most delicate and thorny areas of US foreign policy* » (189) et que « *the decision to launch the bomb came from a private company marketing its services, not from the government agencies charged with diplomacy, national defense, or intelligence* » (190).

e) Risques pour le renseignement et la lutte contre la criminalité

Des risques similaires pourraient apparaître dans d'autres domaines de l'activité de l'État. Les actions autonomes d'un acteur privé à l'encontre d'un *hacker* pourraient par exemple mettre en péril des opérations menées contre la même cible par les agents de renseignement d'un État. De même, des actions de *hack-back* destinées à effacer des données volées par le *hacker* pourraient détruire

(188) « et chacun avant les loix étant seul juge et vengeur des offenses qu'il avoit reçues… » écrivait J.-J. Rousseau, *Discours sur l'origine et les fondements de l'inégalité parmi les hommes*, 1754, p. 96.

(189) Shane Harris, *@WAR: The Rise of the Military-Internet Complex*, Harvest Books, 2014, p. 206.

(190) K. Eichensehr, « Public-Private Cybersecurity », *op. cit.*, p. 23.

des preuves nécessaires pour engager des poursuites judiciaires et entraver de ce fait les activités des forces de l'ordre. Pire encore, le *hack-back* pourrait devenir une excuse permettant à des cybercriminels de justifier des actes malveillants. Aujourd'hui, en effet, la prohibition des activités de *hacking* par les ordres juridiques internes (voir *infra* Partie III 2C) permet de clairement distinguer les *victimes* des *auteurs* d'une cyberattaque. Autoriser le *hack-back* signifierait brouiller cette distinction : les auteurs de cyberattaques pouvant alors prétendre qu'ils ne font que répondre à des attaques initiales, les prévenir, protéger les victimes, réunir des preuves ou encore établir une attribution. La lutte contre la cyber-criminalité pourrait ainsi devenir plus complexe.

f) Risques de dommages collatéraux

Des tiers innocents pourraient aussi devenir victimes d'activités de *hack-back*. Ceci pourrait, tout d'abord, se produire à la suite **d'erreurs d'attribution**. Le risque est d'autant plus important que l'action de *hack-back* pourrait être lancée sans prendre le temps nécessaire pour procéder à l'attribution avec une relative certitude (191). L'expérience des Entreprises militaires et de sécurité privées (EMSP) qui sera évoquée ultérieurement montre que des agents de sécurité privés sous-entraînés et/ou trop zélés peuvent agir de façon intempestive voire abusive. Le risque de dommages collatéraux découle aussi de la nature de certaines cyber-attaques. Dans le cadre d'une attaque par déni de service (*DDoS*) par exemple des ordinateurs « zombies » peuvent être utilisés à l'insu de leurs propriétaires par des pirates. La mise hors-service de *botnets* lors d'une opération de *hack-back* pourrait alors affecter des parties innocentes.

g) Risques liés à la cyberdéfense active « automatique »

Les risques précités sont d'autant plus importants que la cyberdéfense active est de plus en plus « automatisée ». Afin de répondre de façon plus efficace aux cyberattaques et s'adapter à la complexité croissante des moyens utilisés, la cyber-défense active a recours à l'apprentissage automatique (*machine learning*) et à l'intelligence artificielle. Ceci augmente l'adaptabilité, la réactivité, la précision et *in fine* l'effectivité du *hack-back* mais aussi les risques d'erreur en cas de mauvaise conception et programmation du système ou en cas de manipulation de celui-ci par un acte malveillant extérieur (192).

h) Risques d'un « retour de manivelle »

Les entreprises qui pratiquent le *hack-back* pourraient être confrontées à un « retour de manivelle ». Si des géants comme Google ou Microsoft ont sans doute

(191) Voir P. Lin, *supra* note 178.

(192) Voir par exemple Ian Goodfellow, « Deep Learning Adversarial Examples – Clarifying Misconceptions », *KD Nuggets*, juillet 2015 (www.kdnuggets.com/2015/07/deep-learning-adversarial-examples-misconceptions.html).

peu de choses à craindre, des PME qui se lancent dans des contre-attaques contre des pirates puissants (liés, par exemple, à l'appareil de certains États) pourraient être écrasés par la contre-offensive du *hacker*. Agir donc en concertation avec leur État pourrait s'avérer être une sage décision.

i) Risques d'une cyberdéfense active élitiste ou hypocrite

Cette dernière remarque pourrait être prolongée en mettant en exergue l'inégalité entre les quelque grands acteurs du numérique et l'univers de millions de PME à travers le monde. Ces dernières pourraient ne pas avoir les moyens financiers pour se procurer des outils efficaces de cyberdéfense active ni d'ailleurs les ressources humaines compétentes pour les utiliser. Une proportion infime d'entreprises disposerait alors de la capacité technique et des compétences requises pour riposter de façon efficace et relativement sûre. Pire encore, une autorisation générale du *hack-back* pourrait conduire à des dérives mafieuses de la part d'acteurs peu scrupuleux de la cybersécurité qui lanceraient des attaques contre des PME dépourvues d'outils de cyberdéfense active afin de leur vendre leur « protection ». *Last but not least*, le *hack-back* pourrait aisément devenir un prétexte pour légitimer le cyber-espionnage industriel ou nuire aux concurrents.

j) Un effet dissuasif contestable

L'effet dissuasif supposé du *hack-back* rencontre d'importantes limites. Certes, la crainte d'une riposte robuste pourrait éventuellement dissuader des pirates, isolés motivés par l'appât du gain, mais elle n'aura probablement aucun effet (autre que la nécessité d'une meilleure préparation ou dissimulation) à l'égard de terroristes ou d'autres acteurs ayant des motifs idéologiques comme des *hackers* « patriotiques » ou politiques en lien avec des intérêts étatiques.

2. Le hack-back *« sauvage » : les acteurs privés peuvent-ils déclencher unilatéralement des mesures cyber-offensives ?*

Il convient maintenant de procéder à une analyse du droit positif afin d'examiner la compatibilité du *hack-back* avec le droit existant. Nous nous concentrerons sur ce que nous appelons ici le *hack-back* « sauvage », afin de décrire des cyber-ripostes non contrôlées, pratiquées de façon unilatérale et autonome par le secteur privé, que nous comparerons à ce que nous appellerons plus tard un *hack-back* « sage », entrepris sous l'impulsion et le contrôle étroit de l'État. Nous verrons, tout d'abord, que le droit international ne reconnaît aucun droit de *hack-back* « sauvage » (A). Ceci ne signifie pas forcément qu'une opération privée de *hack-back* viole le droit international en tant que tel (B) mais elle constitue, le plus souvent, une violation du droit interne du pays visé exposant alors son auteur à des risques juridiques considérables (C).

A) L'inexistence d'un « droit de hack-back » en droit international

En droit international, les acteurs non-étatiques, qu'il s'agisse d'individus, de minorités nationales ou encore d'entreprises, peuvent bénéficier de droits. Encore faut-il que les créateurs du droit international, les États, leur reconnaissent de tels droits dans des traités internationaux ou à travers d'autres modes classiques de formation du droit international (notamment la voie coutumière et les actes unilatéraux des organisations internationales investies par les États d'un pouvoir normatif). Or, une analyse du droit international positif montre clairement qu'il n'existe aucun droit de « *hack-back* » au profit d'acteurs privés.

D'une part, force est de constater qu'il n'existe aucune règle spécifique et expresse élaborée par les États pour reconnaître un tel droit. Les rares traités internationaux qui existent dans ce domaine n'expriment rien qui pourrait être interprété comme favorisant la pratique du *hack-back*. Au contraire même, ils appellent souvent les États à lutter contre la cybercriminalité, comme la Convention de Budapest de 2001 qui demande aux États, comme nous le verrons, d'ériger en infraction pénale les atteintes à l'intégrité des systèmes informatiques. Quant aux instruments de *soft law*, tels que les règles agréées dans le cadre du GGE, loin de favoriser les actions unilatérales des acteurs non-étatiques, ils demandent aux États de « veiller à ce que des acteurs non-étatiques n'utilisent pas leur territoire pour commettre » des « faits internationalement illicites à l'aide des technologies de l'information et des communications » [(193)].

D'autre part, comme nous le verrons, les règles générales du droit international qui s'appliquent également en matière de cybersécurité ne peuvent en aucun cas être interprétées comme conférant aux acteurs non-étatiques un droit de *hack-back*.

Il est tout d'abord **impossible pour ces acteurs de s'appuyer sur la théorie des contre-mesures**, analysée en détail dans la Partie II. Les contre-mesures ne peuvent être adoptées que par *des États lésés* [(194)] *contre d'autres États* en suivant les conditions strictes déjà analysées. Ce sont donc les États qui, selon la logique du droit international, ont qualité pour agir en adoptant des contre-mesures en réaction au fait internationalement illicite commis par un autre État qui affecte leurs droits ou ceux de leurs ressortissants. Les États ont, en effet, sur la base du droit international, un droit non seulement de protéger leur territoire et leur souveraineté mais aussi d'exercer leur protection en faveur de toute personne physique ou morale à l'égard de laquelle ils bénéficient d'une compétence, en commençant par

(193) *GGE 2015*, *supra* note 2, p. 15.

(194) Les organisations internationales, en tant que sujets du droit international, ont aussi qualité pour adopter des contre-mesures sous certaines conditions. Voir les articles 22 et 51 à 57 du Projet d'articles sur la responsabilité des organisations internationales adopté par la Commission du droit international de l'ONU en 2011 (http://legal.un.org/ilc/texts/instruments/french/draft_articles/9_11_2011.pdf).

leurs nationaux [195]. Ils ont, à cet égard, un titre de réaction pour adopter toutes les mesures autorisées par le droit international, y compris les contre-mesures. Ce titre n'existe pas en principe pour les personnes privées. Comme l'a bien résumé un auteur : « aussi loin que l'on puisse remonter dans l'histoire, le droit de représailles a toujours été un droit public, un droit souverain et régalien » [196]. Certes, comme nous le verrons (*infra* Partie III, 3), les États pourraient dans certaines circonstances concéder de façon expresse à des acteurs privés la possibilité d'exercer des contre-mesures, mais ceci implique un acte express, un contrôle étroit de l'État et le risque pour celui-ci d'engager sa responsabilité, les réactions ainsi adoptées étant considérées comme des faits de l'État lui-même.

De la même manière, **il est impossible pour les acteurs privés de s'appuyer sur la théorie de « légitime défense »** en droit international. Il faut, à cet égard, clairement écarter toute confusion possible qui pourrait découler de l'utilisation du terme de « cyberdéfense » (active ou d'ailleurs passive). Le concept de légitime défense en droit international, tel que codifié aussi par l'article 51 de la Charte des Nations Unies, renvoie à quelque chose de très précis : une agression armée commise contre un État. La légitime défense d'ailleurs ne peut être invoquée que par les États victimes. Un individu, une entreprise, un acteur privé quelconque ne peut, du point de vue du droit international, ni être victime d'une « agression armée » ni invoquer le droit de légitime défense consacré par l'article 51 de la Charte. Ces dernières années, beaucoup d'encre a coulé dans la doctrine du droit international pour savoir si, au-delà des États, des acteurs non-étatiques (et surtout des groupes terroristes tels que *Al-Qaïda* ou *Daesh*) pourraient aussi commettre une agression armée contre un État (et ceci alors que, selon la position traditionnelle de la Cour internationale de justice, une agression ne peut être commise que par un État contre un autre État) [197]. Mais quel que soit l'intérêt de ce débat, il n'a jamais été avancé dans la doctrine que ces acteurs pourraient être *victimes* d'une agression armée leur donnant la possibilité d'invoquer la « légitime défense » pour lancer des attaques contre d'autres États.

Les acteurs privés ne peuvent pas non plus s'appuyer sur certains autres mécanismes d'autoprotection reconnus par le droit international, tels que le « droit de poursuite ». Ce droit important en matière de droit de la mer est codifié par l'article 111 de la Convention des Nations Unies sur le droit de la mer de 1982 (Convention de Montego Bay). Selon cet article, un État côtier a le droit, sous certaines conditions, de poursuivre un navire étranger qui se trouve dans sa zone maritime lorsqu'il a de sérieuses raisons de penser que ce navire a contrevenu à ses lois et règlements. La poursuite peut continuer de façon ininterrompue

(195) Voir aussi le mécanisme dit de « protection diplomatique » en droit international.

(196) D. ALLAND, *Justice privée et ordre juridique international*, *op. cit.*, p. 316.

(197) Ainsi, dans son avis consultatif du 9 juillet 2004 concernant les Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé, la Cour a souligné que : « L'article 51 de la Charte reconnaît […] l'existence d'un droit naturel de légitime défense en cas d'agression armée par un État contre un autre État ».

jusqu'à ce que le navire entre dans la mer territoriale d'un autre État. Il pourrait être tentant de s'inspirer de cette vieille règle du droit de la mer et songer à la conception d'un « droit de cyber-poursuite ». Mais comme le « droit de poursuite » classique, son extension dans le cyberespace ne devrait, en principe, être réservé qu'aux autorités étatiques. Ainsi, l'article 111 de la Convention de Montego Bay souligne que « le droit de poursuite ne peut être exercé que par des navires de guerre ou des aéronefs militaires ou d'autres navires ou aéronefs qui portent des marques extérieures indiquant clairement qu'ils sont affectés à un service public et qui sont autorisés à cet effet ».

Enfin, les acteurs privés **ne peuvent pas s'appuyer sur les droits de l'homme pour exercer des mesures de *hack-back*.** Certes, il est vrai que certains instruments relatifs à la protection des droits de l'homme (tels que la Convention européenne des droits de l'homme) consacrent des droits importants tels que le droit à la vie ou la protection de la propriété privée. Mais à aucun moment ils n'investissent les particuliers d'un droit de « se faire justice eux-mêmes » pour les protéger. La logique des conventions internationales de protection des droits de l'homme est que *ce sont les États qui doivent agir* pour garantir ces droits en protégeant leurs bénéficiaires tant des atteintes portées par les organes de l'État que des atteintes portées par les acteurs privés eux-mêmes dont l'État a connaissance ou aurait dû avoir connaissance (théorie des obligations positives). Une fois encore, il est impossible d'effacer l'État de l'équation droit d'action, de protection et de réaction.

Il convient d'ajouter que **les acteurs privés ne peuvent pas non plus bien entendu s'appuyer sur le concept de légitime défense de droit interne** pour lancer de telles attaques transfrontalières. Au-delà du fait que dans plusieurs ordres juridiques nationaux il sera difficile d'invoquer la « légitime défense » pour riposter à une cyberattaque, une telle possibilité ne changerait rien du point de vue du droit international. En d'autres termes, à supposer même qu'un droit de *hack-back* soit reconnu dans certains ordres juridiques (ce qui ne semble pas être le cas pour l'instant comme nous le verrons), ceci ne signifierait nullement l'existence d'un tel droit dans l'ordre juridique international qui est un ordre distinct. Selon la règle codifiée par la Commission de droit international de l'ONU : « La qualification du fait de l'État comme internationalement illicite relève du droit international. Une telle qualification n'est pas affectée par la qualification du même fait comme licite par le droit interne » [(198)].

B) Une violation du droit international ?

Nous avons vu que le droit international ne confère pas aux acteurs privés un « droit de *hack-back* ». Cela ne signifie pas pour autant qu'une opération de

(198) *ACDI 2001*, *supra* note 19, article 3.

hack-back lancée par des acteurs privés serait automatiquement une « violation » du droit international. Il peut parfaitement arriver que l'ordre juridique international ne reconnaisse pas, au profit d'une personne physique ou morale, un « droit » de faire quelque chose sans pour autant considérer que cette action est « prohibée » par le droit international. Cette situation résulte souvent de la volonté de laisser les États décider librement de certaines questions qui relèvent de leur « domaine réservé ».

La question de savoir si le « *hack-back* » entrepris par des acteurs privés constitue une violation du droit international a, comme nous le verrons, relativement peu d'intérêt pratique. Il convient néanmoins d'examiner rapidement cette question et de remarquer que, probablement, le droit international n'interdit pas en tant que tel, pour l'instant, un *hack-back* « privé ».

Certes, une action de *hack-back* conduite par un État pourrait, dans certaines circonstances constituer une violation de la souveraineté d'un autre État, voire une violation des principes de non-ingérence et de non-intervention. Mais, normalement, seuls les États peuvent violer ces principes. Un acteur privé, dont les actions ne sont pas imputables à un État, ne peut pas violer le principe de non-ingérence (199). Ceci ne signifie pas pour autant que le comportement de l'acteur privé se situe dans un *vacuum* juridique. Ce comportement pourrait, en effet, constituer, comme nous le verrons, une violation du droit interne de cet État, exposant l'acteur privé à des poursuites. Par ailleurs, le fait que l'État dont relève l'acteur privé ne prenne pas les mesures nécessaires pour faire cesser le *hack-back* qui cause, de façon non justifiée par le droit international, des dommages à un autre État, pourrait constituer une violation de son obligation de diligence due (*supra* Partie I), exposant cet État à des contre-mesures de la part de l'État victime. Il en va de même, bien entendu, si les actes de *hack-back* de l'acteur privé peuvent, d'une façon ou d'une autre, être attribués à l'État (200). On retombe alors dans une logique « interétatique » classique où les réactions décrites dans la Partie II sont applicables.

On pourrait se demander, par ailleurs, si le *hack-back* pourrait être considéré comme un « crime international » directement prohibé par le droit international. Le droit international peut en effet ériger certaines infractions imputables à des individus agissant à titre purement privé en « crimes internationaux » permettant l'engagement de leur responsabilité pénale internationale. Ceci a été

(199) Position adoptée aussi par *Manuel de Tallinn 2.0*, *supra* note 12, *Rule 33*, §1 et 2 : « *[I]nternational law by and large does not regulate cyber operations conducted by non-State actors, such as private individuals or companies. The International Group of Experts agreed that cyber operations conducted by non-State actors that are not attributable to States do not violate the sovereignty of the State into which they are launched, constitute intervention or amount to a use of force because these breaches can be committed only by States* ». Paradoxalement, alors que les experts ont reconnu unanimement dans ce passage que les acteurs non-étatiques ne peuvent pas violer le principe de l'interdiction du recours à la force, une majorité d'entre eux considère ultérieurement (*Rule 71*, §18-19) que ces mêmes acteurs non-étatiques pourraient néanmoins commettre une agression, y compris par des moyens cyber.

(200) Voir *infra* Partie III (3C).

fait, par exemple, avec les actes de piraterie en haute mer, la traite d'esclaves, la piraterie aérienne ou encore le trafic de stupéfiants ou certains actes de terrorisme international. La création d'un nouveau « crime international » nécessite néanmoins l'adoption de conventions spécifiques à cet égard ou une reconnaissance claire par la communauté internationale des États. Comme l'a remarqué Ellen S. Podgor, « *membership in the exclusive club of international crimes is limited* » (201).

Or, il n'est pas certain que les cyberattaques aient franchi ce pas en tant que telles (202). Des instruments contre la cybercriminalité ont certes été adoptés, le plus fameux d'entre eux étant la Convention de Budapest sur la cybercriminalité de 2001 du Conseil de l'Europe, aujourd'hui ratifié par 52 États. Cette convention demande aux États d'adopter « les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à [leur] droit interne », toute une série de comportements y compris les atteintes à l'intégrité des données ou à l'intégrité de systèmes informatiques (203). La Convention de Budapest n'érige pas expressément la cybercriminalité en « crime international » mais cet appel aux États de l'ériger en infraction pénale dans leurs ordres internes, d'harmoniser leurs législations et de coopérer pour la combattre s'inscrit clairement dans la logique d'une internationalisation de cette infraction. Les appels en faveur de l'adoption d'une convention universelle contre la cybercriminalité n'ont néanmoins pas encore abouti (204). Par ailleurs, à supposer même que le « *hacking* » puisse être considéré comme une infraction internationale, ceci ne devrait pas être automatiquement le cas du « *hack-back* » qui répond à une logique différente.

Même si le « *hack-back* » privé n'est pas un « crime international », l'importance d'une telle conclusion, ne doit ni être exagérée, ni prêter à confusion. En effet, les juridictions pénales internationales telles que la Cour pénale internationale n'ont de toute façon aucune compétence à cet égard. La véritable question qui se pose sur un plan pratique est de savoir comment la loi pénale nationale s'applique dans ce domaine et quels sont les risques de poursuites nationales à l'encontre d'un auteur de *hack-back*.

(201) E.S. Podgor, « Cybercrime: National, Transnational or International? », *Wayne Law Review*, vol. 50, n° 97, 2004, p. 104.

(202) Il va de soi en revanche qu'une cyberattaque pourrait devenir l'instrument pour commettre un crime international (par exemple une attaque contre des civils constitutive d'un crime de guerre).

(203) Voir : « Article 4 - Atteinte à l'intégrité des données 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques. 2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux ». « Article 5 - Atteinte à l'intégrité du système : Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques ».

(204) Voir Jonathan Clough, « A World of Difference: The Budapest Convention on Cybercrime and The Challenges of Harmonisation », *Monash University Law Review*, vol. 40, n° 3, 2014, p. 725-729.

C) Le hack-back *en tant que violation du droit interne*

Agissant de façon spontanée ou sous l'impulsion d'instruments comme la Convention de Budapest sur la cybercriminalité de 2001, de très nombreux pays ont légiféré contre la cybercriminalité en érigeant en infraction pénale les atteintes à l'intégrité des données ou à l'intégrité de systèmes informatiques. Une analyse récente a montré, par exemple, que tous les pays du G8 ont adopté des lois à cet égard prévoyant des amendes et/ou des peines de prison en cas de violation (205). Aucune d'entre elles ne semble autoriser le *hack-back* privé (206). Aucune ne l'interdit de façon expresse non plus, mais il est normal de penser que le même régime qui interdit le « *hacking* » interdit aussi en principe le « *hacking back* » – à moins que certaines exceptions ou excuses légales classiques (comme la légitime défense ou la nécessité) (207) puissent le justifier (208). Dans certains pays par ailleurs, des dispositions législatives encadrent expressément la riposte aux cyberattaques réservant ce droit à l'État ou aux personnes autorisées par celui-ci. En France, par exemple, la pratique est encadrée par l'article 21 de la Loi de programmation militaire (LPM) de 2013, qui prévoit que ce sont des agents habilités de l'État qui sont autorisés à prendre de telles mesures pour caractériser une attaque et/ou en neutraliser les effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque (209).

(205) Voir Paul Rosenzweig, « International Law and Private Actor Active Cyber Defensive Measures », *Stanford Journal of International Law*, vol. 50, 2014, p. 742-745.

(206) Il faut noter, néanmoins, qu'une proposition de loi présentée (mais pas encore adoptée) aux États-Unis le 23 février 2017 vise à légaliser pour la première fois certains actes de *hack-back*. Il s'agit de l'*Active Cyber Defense Certainty* (ou *ACDC*) *Act*, qui vise à amender la section 1030 du *Computer Fraud and Abuse Act* afin d'autoriser les victimes d'une cyberattaque de « *access without authorization the computer of the attacker […] to gather information in order to establish attribution of criminal activity to share with law enforcement or to disrupt continued unauthorized activity against the victim's own network* ». Par contre cette proposition d'amendement n'autorise pas les victimes d'une cyberattaque à détruire les informations qui se trouvent dans l'ordinateur de l'attaquant, de causer des dommages physiques à une autre personne ou de constituer une menace pour la santé ou la sécurité publique. Pour le texte, voir sur le site du *Congressman* Tom Graves (https://tomgraves.house.gov/uploadedfiles/discussion_draft_ac-dc_act.pdf).

(207) Il convient à cet égard de noter que le paragraphe 38 du Rapport explicatif de la Convention de Budapest stipule que : « Les infractions énumérées ont un trait particulier, à savoir que leurs auteurs doivent expressément agir "sans droit". Cette expression rend compte du fait que le comportement décrit n'est pas toujours punissable en soi, mais peut être légal ou justifié non seulement par des exceptions légales classiques (consentement, légitime défense ou nécessité), mais dans les cas où d'autres principes ou intérêts excluent toute responsabilité pénale ». Le rapport n'envisage pas, néanmoins, l'hypothèse d'un *hack-back* privé. Il souligne, par contre, que « la Convention ne concerne pas, par conséquent, les comportements conformes aux compétences gouvernementales légales (par exemple, lorsque le gouvernement de la Partie concernée agit dans un but de maintien de l'ordre public, de protection de la sécurité nationale ou dans le cadre d'une instruction pénale) ». Voir le *Rapport explicatif de la Convention sur la cybercriminalité* (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ccea4).

(208) À noter néanmoins qu'aucune de ces lois ne semble prévoir une atténuation de la responsabilité spécifique au *hack-back*.

(209) Selon les articles L. 2321-1 et L. 2321-2 du chapitre I^{er} du titre II du livre III de la 2^{e} partie du Code de la Défense : Art. L. 2321-1. « Dans le cadre de la stratégie de sécurité nationale et de la politique de défense, le Premier ministre définit la politique et coordonne l'action gouvernementale en matière de sécurité et de défense des systèmes d'information. Il dispose à cette fin de l'autorité nationale de sécurité des systèmes d'information qui assure la fonction d'autorité nationale de défense des systèmes d'information ». « Art. L. 2321-2. Pour répondre à une attaque informatique qui vise les systèmes d'information affectant le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation, les services de l'État peuvent, dans les conditions fixées par le Premier ministre, procéder aux opérations techniques nécessaires à la caractérisation de l'attaque et à la neutralisation de ses effets en accédant aux systèmes d'information qui sont à l'origine de l'attaque ». C'est nous qui soulignons.

Un acteur privé qui conduit une opération de *hack-back* ayant des conséquences transnationales pourrait ainsi violer le droit interne de plusieurs États : de l'État depuis lequel il agit et de l'État ou des États où le *hack-back* provoque des dommages. Si tous ces pays interdisent de façon absolue l'accès non autorisé aux systèmes informatiques et les atteintes à l'intégrité de ces systèmes et des données opérées par le *hack-back*, des poursuites pourraient être engagées. À supposer même que l'État national de l'auteur du *hack-back* ne souhaite pas agir contre lui, cette personne pourrait ne pas être à l'abri d'une action judiciaire. Le ou les pays affectés pourraient en effet utiliser les canaux de la coopération pénale et de l'entraide judiciaire contre lui. Ils pourraient émettre des mandats d'arrêt et des demandes d'extradition réclamant l'arrestation et l'extradition du suspect (exactement de la même façon qu'ils le font parfois avec un « *hacker* » tout court). L'auteur du *hack-back* pourrait ainsi se trouver pris dans le filet de la coopération internationale contre le cybercrime favorisée par des instruments comme la Convention de Budapest. En bref, comme l'a écrit James A. Lewis : « *Anyone who engages in retaliation probably should avoid international trips* » [(210)].

Jusqu'à présent, nous n'avons pas eu connaissance de poursuites contre des auteurs de *hack-back*. Ceci est probablement dû à plusieurs raisons. D'une part, tant les auteurs de telles pratiques que les pirates visés par le *hack-back* pourraient préférer ne pas en faire la publicité pour éviter, précisément, les risques de poursuites. D'autre part, dans la plupart des cas qui ont été publics et ont été médiatisés, le *hack-back* a eu lieu le plus souvent en coordination avec l'État [(211)] ou sur la base d'une autorisation délivrée par le Juge national [(212)] – ce qui signifie qu'on se situe plutôt dans la logique d'un *hack-back* « encadré » entrepris sous l'impulsion ou avec le consentement de l'État.

3. Le *hack-back* « encadré » : les États peuvent-ils s'appuyer sur des acteurs privés pour conduire des contre-attaques ?

Un *hack-back* « sauvage » conduit de façon unilatérale par des acteurs privés soulève donc de nombreuses difficultés juridiques. Dans ce contexte, il convient alors de se demander dans quelle mesure un *hack-back* qui serait entrepris après autorisation de l'État et en concertation avec ses autorités pourrait être considéré comme plus « sage » et soulever moins de difficultés juridiques. Cette question nous invite à réfléchir aux perspectives et aux formes possibles d'une coopération entre les acteurs publics et privés pour répondre aux cyberattaques (A). L'expérience des Entreprises militaires et de sécurité privées permet à cet égard de

(210) J.A. Lewis, « Private Retaliation in Cyberspace », *Center for Strategic and International Studies*, 22 mai 2013 (www.csis.org/analysis/private-retaliation-cyberspace).

(211) Voir par exemple *BBC*, « FBI and Microsoft take down $500m-theft botnet Citadel », juin 2013 (www.bbc.com/news/technology-22795074).

(212) Voir par ex. Robert Lemos, « Microsoft Can Retain Control of Zeus Botnet Under Federal Court Order », *eWeek*, décembre 2012 (www.eweek.com/security/microsoft-can-retain-control-of-zeus-botnet-under-federal-court-order).

dresser un parallèle intéressant (B). De façon plus générale, l'idée d'un *hack-back* « sage » nous renvoie à la question fondamentale de l'engagement de la responsabilité internationale des États du fait de la conduite des acteurs privés (C).

A) Une coopération entre les acteurs publics et privés pour répondre aux cyberattaques ?

La réponse à la question « les États peuvent-ils s'appuyer sur des acteurs privés pour faire du *hack-back* ? » est en principe très simple : oui. Oui, mais seulement si la riposte respecte les conditions de réaction à une cyberattaque analysées *supra* (Partie II). Ainsi, par exemple, le fait qu'une mesure de *hack-back* soit conduite directement par un État ou par une entité privée autorisée par cet État ne change rien à la licéité de cette action si celle-ci constitue une contre-mesure légitime. Nous avons donc ici un changement profond de logique et de régime juridique par rapport à un *hack-back* « sauvage » déclenché de façon unilatérale par une entreprise. Dans le *hack-back* « sauvage », l'entreprise est un « *lonesome cowboy* » qui « se fait lui-même justice » dans une sorte de *Far-West* numérique sans foi ni loi. En revanche, dans le *hack-back* « sage », c'est l'État qui agit, délégant si nécessaire certaines de ses compétences en matière d'exécution à des entreprises. Il ne s'agit plus de l'état de nature où tout acteur privé serait « juge de sa propre cause » mais d'un univers ordonné où l'État maintient et assure son rôle de garant de la protection et de l'exécution du droit.

Si la délégation de pouvoirs d'une autorité publique à une autorité privée est un mécanisme bien connu des systèmes juridiques, son application dans le domaine de la sûreté et de la sécurité nationale peut poser des difficultés parfois redoutables. L'ancienne pratique de l'octroi par les souverains de « lettre de marques » à des corsaires permettant à ces derniers de pratiquer la course et d'exercer, au nom de l'État, un droit de représailles constitue à cet égard un bon exemple. Une lettre de marque ou lettre de course était en effet un document émanant d'un souverain permettant à un capitaine de rechercher, attaquer, saisir et détruire dans les eaux territoriales, internationales ou étrangères les navires d'une Nation adverse de laquelle on avait reçu offense. La pratique était strictement réglementée (en France, par exemple, par l'Ordonnance de la Marine de Colbert de 1681). Pourtant, cette pratique a posé de tels problèmes dans la conduite des relations internationales que la « course » a été finalement abolie en 1856 par la Déclaration de Paris.

Pourrait-on envisager aujourd'hui la résurgence de cette pratique sous la forme de « corsaires numériques » [(213)] ? Pour répondre à cette question, il semble nécessaire d'envisager plusieurs situations possibles.

(213) Terme préférable à celui de « mercenaire numérique ». Le terme « mercenaire » renvoie en effet une définition très précise en droit international qui désigne un individu qui s'enrôle volontairement dans des forces armées combattantes d'un État belligérant dont il n'est pas le ressortissant afin d'obtenir un profit personnel, notamment d'ordre financier. En

Un premier scénario pourrait être celui où un État sollicite une ou plusieurs entreprises privées à propos d'une cyberattaque précise à laquelle l'État souhaite riposter de la façon la plus efficace. Un tel *hack-back*, déclenché sous le contrôle étroit de l'État, ne semble poser aucune difficulté de principe et pourrait être compatible avec le droit international si les conditions évoquées *supra* (Partie II) sont respectées. Il en irait de même dans l'hypothèse où des entreprises solliciteraient et obtiendraient l'accord et l'aide de l'État pour répondre à une cyberattaque précise. La pratique offre effectivement plusieurs exemples de telles situations [(214)] qui ne peuvent pas être assimilées à l'ancienne pratique de la « course ».

Un deuxième scénario pourrait être ce que certains auteurs ont appelé la « cyberdéfense active certifiée ». Selon ce scénario, un État pourrait autoriser « *a limited number of certified private entities to work with government to take active defense measures focused on attribution, initially to protect critical information within the defense industrial base* » [(215)]. À la différence du premier scénario (où il s'agit de répondre de façon *ad hoc* à une cyberattaque), l'État établirait en amont une sorte de « partenariat public/privé » avec des entreprises désignées pour répondre plus efficacement aux cyberattaques. Dans la mesure où l'État garderait un contrôle étroit des activités de ces acteurs privés, contrôle d'autant plus étroit que le nombre de ces acteurs serait limité, ce scénario ne semble pas poser de difficultés juridiques insurmontables. Une telle solution permettrait d'ailleurs de concevoir un cadre juridique précis des relations « public/privé » en matière de cybersécurité, trop souvent développées *de facto* et de manière désordonnée. Ce faisant, elle permettrait que les valeurs de l'état de droit comme la transparence, l'accès au juge, la responsabilité ou la protection de la vie privée soient respectées [(216)]. Un tel cadre juridique serait par définition encadré par un contrôle et une vigilance de l'État sur les activités de ses partenaires privés, ce qui permettrait d'éviter un grand nombre d'inconvénients associés au *hack-back* analysés *supra* (Partie III 1B).

Beaucoup plus problématique pourrait être par contre un troisième scénario où l'État donnerait « carte blanche » à l'ensemble des entreprises pour pratiquer le *hack-back* sur la base d'une auto-appréciation de la nécessité d'agir. Le *hack-back* dans une telle situation ne serait plus vraiment « sage », redeviendrait « sauvage » rendant un contrôle efficace et étroit par l'État pratiquement impossible. Le développement de myriades de « corsaires numériques » se considérant habilités par

tant que tel il est principalement utilisé dans une situation de conflit armé. Il convient toutefois de noter que la Convention internationale contre le recrutement, l'utilisation, le financement et l'instruction des mercenaires du 4 décembre 1989 prévoit une extension du terme en dehors d'une situation de conflit armé mais cette extension semble être très difficilement applicable en cas d'un *hack-back*. Selon l'article 1 (2) de cette convention : « Le terme "mercenaire" s'entend également, dans toute autre situation, de toute personne : a) Qui est spécialement recrutée dans le pays ou à l'étranger pour prendre part à un acte concerté de violence visant à : i) Renverser un gouvernement ou, de quelque autre manière, porter atteinte à l'ordre constitutionnel d'un État ; ou ii) Porter atteinte à l'intégrité territoriale d'un État ».

(214) Voir notes 211 et 212.

(215) Franklin D. Kramer et Melanie J. Teplinsky, « Cybersecurity and Tailored Deterrence », *Atlantic Council Issue Brief*, décembre 2013, p. 2 et 6-7 (www.atlanticcouncil.org/publications/issue-briefs/cybersecurity-and-tailored-deterrence).

(216) Voir à cet égard l'étude récente de K. Eichensehr, « Public-Private Cybersecurity », *op. cit.*, p. 1-64.

l'État à exercer un droit de représailles, pourrait susciter de vives tensions internationales brandissant le spectre de l'escalade de la violence et de la déstabilisation des États déjà évoqué (Partie III 1B).

B) Le cas des Entreprises militaires et de sécurité privées (EMSP)

Un parallèle s'impose ici avec l'attitude des États à l'égard des EMSP, sujet amplement débattu en droit international ces dernières années.

Pour de nombreuses raisons (multiplication des opérations extérieures depuis la fin de la guerre froide, réduction des effectifs des armées, fin de la conscription, développement du concept « zéro mort », gestion par les États-Unis et leurs alliés des conséquences de l'invasion de l'Irak en 2003, lutte contre la piraterie maritime, etc.), le recours aux EMSP s'est largement développé au cours de ces deux dernières décennies. On dénombre aujourd'hui pas moins d'une centaine d'EMSP à travers le monde comptant près de 200 000 employés pour un volume commercial estimé à 100 milliards de dollars [(217)]. Parallèlement à leur développement, les missions confiées aux EMSP se sont largement diversifiées. Ces missions vont désormais des services de conseil, d'assistance tactique, de formation et d'entraînement des forces de police et forces armées régulières, à la protection et la surveillance des personnes en passant par la sécurisation des zones sensibles, les opérations de renseignement, de ravitaillement et d'aide logistique aux troupes.

Le recours à ces EMSP, souvent considéré par les États comme utile, permet de satisfaire des besoins auxquels les forces armées des États ne veulent plus – ou ne peuvent plus – répondre. La lutte contre la piraterie maritime constitue un exemple consensuel de recours au EMSP et ceci malgré les importantes difficultés rencontrées. Le phénomène de la piraterie aux larges des côtes de l'Afrique de l'Est et surtout de la Somalie, a en effet pris une dimension particulièrement inquiétante à partir de la seconde moitié des années 2000. Entre 2008 et 2009, le nombre des attaques par des pirates dans la zone avait ainsi augmenté de 300 % et ceci en dépit du développement progressif d'opérations navales conjointes entre les États dans le cadre d'une impressionnante coopération internationale [(218)]. Bien que d'une utilité incontestable, les opérations navales étatiques ont toutefois montré leurs limites dans l'éradication du phénomène. Face à cette situation, les États ont progressivement autorisé les navires battant pavillon national à embarquer des membres armés d'EMSP. Cette mesure, combinée à des opérations navales étatiques de plus en plus efficaces et à d'autres facteurs, a conduit à une réduction spectaculaire à la fois du nombre des attaques réussies mais aussi du nombre des attaques elles-mêmes.

(217) Selon l'ouvrage à paraître de Thierry Garcia, *Les entreprises militaires et de sécurité privées appréhendées par le droit*, Mare & Martin, mai 2017.

(218) *Cf.* David Axe, « Why the Somali Pirates are Winning », *The Guardian*, 9 avril 2009 (www.theguardian.com/commentisfree/cifamerica/2009/apr/09/piracy-somalia-alabama-us-navy).

Malgré leur utilité dans certains cadres opérationnels précis, les activités des EMSP ont pourtant souvent été au cœur d'importantes controverses. Dans le cadre de différents théâtres d'opérations, plusieurs rapports ont ainsi dévoilé des pratiques abusives de la part de membres de EMSP, voire des violations des droits de l'homme ou du droit humanitaire. L'affaire concernant des employés de la société Blackwater (aujourd'hui Academi), accusés d'avoir tué quatorze personnes dans une fusillade à Bagdad, le 16 septembre 2007 et finalement condamnés à de lourdes peines d'emprisonnement en 2015, a été sans doute la plus médiatisée. Même dans le domaine de la lutte contre la piraterie maritime, des rapports ont dénoncé des membres d'EMSP sous-entraînés et trop zélés tuant sans distinction des pêcheurs innocents considérés de façon erronée comme des pirates.

Une étude récente soutient que, malgré la volonté des États de réglementer strictement les EMSP, les droits internes, souvent hésitants et surtout très diversifiés, s'avèrent insuffisants pour encadrer de façon efficace les activités des EMSP et de leurs membres. Quant au droit international positif, à la fois dans sa dimension régionale et universelle, il s'avère inadapté et ineffectif. La *soft law* prolifère alors que l'autorégulation, prônée par les EMSP, a conduit à l'adoption de codes de conduite privés dont les limites sont soulignées dans cette étude (219).

Les difficultés rencontrées par les États ayant recourt à des EMSP dans des domaines où, pourtant, le contrôle est beaucoup plus aisé que celui de la cybersécurité, ne militent guère en faveur d'une « carte blanche » octroyée au secteur privé en matière de *hack-back*. Les États connaissent d'ailleurs les risques de voir leur responsabilité engagée du fait des activités de ces personnes privées.

C) La responsabilité internationale des États peut-elle être engagée du fait de mesures de hack-back *conduites par des acteurs privés ?*

En droit international, les États sont responsables des actes (y compris les cyber-actes) de leurs agents et ceci même si ces agents agissent *ultra vires* (220). En revanche, en règle générale, le comportement de personnes ou d'entités privées, n'est pas attribuable à l'État d'après le droit international. Des circonstances peuvent cependant survenir où un tel comportement est néanmoins attribuable à l'État parce qu'il existe une relation de fait entre la personne ou l'entité ayant ce comportement et l'État. Par ailleurs, une violation du principe de diligence due analysé *supra* (Partie I), peut aussi engager la responsabilité de l'État.

(219) T. Garcia, *supra* note 217.

(220) Selon l'article 7 des *Articles de la CDI sur la Responsabilité internationale* des États adoptés en 2001 : « Le comportement d'un organe de l'État ou d'une personne ou entité habilitée à l'exercice de prérogatives de puissance publique est considéré comme un fait de l'État d'après le droit international si cet organe, cette personne ou cette entité agit en cette qualité, même s'il outrepasse sa compétence ou contrevient à ses instructions ». ACDI 2001, *supra* note 19.

a) L'État est responsable s'il habilite des acteurs privés à exercer des prérogatives de puissance publique

Selon l'article 5 du projet de la CDI sur la Responsabilité internationale des États adoptée en 2001 :

> « Le comportement d'une personne ou entité qui n'est pas un organe de l'État au titre de l'article 4, mais qui est habilitée par le droit de cet État à exercer des prérogatives de puissance publique, pour autant que, en l'espèce, cette personne ou entité agisse en cette qualité, est considéré comme un fait de l'État d'après le droit international ».

Ainsi, un État peut engager sa responsabilité s'il habilite une société privée « à exercer des fonctions à caractère public normalement exercées par des organes de l'État et que son comportement se rapporte à l'exercice des prérogatives de puissance publique en cause » [(221)]. Tel pourrait être le cas si l'État habilitait une ou plusieurs sociétés privées à conduire des opérations de *hack-back* qui violeraient le droit international. Dans une telle hypothèse, la responsabilité de l'État serait engagée et ceci sans même avoir besoin de démontrer que le *hack-back* s'est opéré sous le contrôle de cet État [(222)].

b) L'État est responsable si des acteurs privés agissent sur ses instructions, ses directives ou sous son contrôle

Comme analysé *supra* (partie I), l'article 8 du projet de la CDI sur la Responsabilité internationale des États dispose que :

> « Le comportement d'une personne ou d'un groupe de personnes est considéré comme un fait de l'État d'après le droit international si cette personne ou ce groupe de personnes, en adoptant ce comportement, agit en fait sur les instructions ou les directives ou sous le contrôle de cet État ».

Cet article pourrait être résumé pour les besoins de notre analyse de la façon suivante :

Tout d'abord, l'État engage sa responsabilité si, sans « habiliter » dans son droit interne une société privée à exercer des prérogatives de puissance publique (hypothèse déjà examinée *supra*), il recrute des sociétés privées à titre « d'auxiliaires », ou les incite à agir à ce titre tout en restant en dehors des structures officielles de l'État. Un exemple pourrait être celui d'un État qui « *specifically instructed an IT department within a university to carry out a Distributed Denial of Service (DDoS) attack against a designated target* » auquel cas « *the resulting operation would be attributable to the State in question* » [(223)].

(221) Commentaire de l'article 5, §2. ACDI 2001, *supra* note 19, p. 44.

(222) Selon le commentaire de la CDI : « Aux fins de l'article 5, sont visées les entités qui, dans l'exercice de la puissance publique, disposent d'un pouvoir d'appréciation et peuvent agir de manière indépendante : il n'est nul besoin de montrer que le comportement était soumis au contrôle de l'État ». (ACDI 2001, *supra* note 19, p. 45)

(223) K. Macak, « Decoding Article 8 of the International Law Commission's Article on State Responsibility: Attribution of Cyber Operations by Non-State Actors », *op. cit.*, p. 414.

De l'aveu même de la CDI, « [p]lus complexes sont les problèmes qui se posent lorsqu'il s'agit de déterminer si le comportement a été adopté « sur les directives ou sous le contrôle » de l'État. Ce comportement ne peut être attribué à l'État que si ce dernier a dirigé ou contrôlé l'opération elle-même et que le comportement objet de la plainte faisait partie intégrante de cette opération » (224). Le degré de contrôle que l'État doit avoir exercé pour que le comportement puisse lui être attribué a donné lieu à de grands débats et certaines divergences au sein de la jurisprudence internationale. La CDI a préféré conclure que « c'est au cas par cas qu'il faut déterminer si tel ou tel comportement précis se produisait ou non sous le contrôle d'un État et si la mesure dans laquelle ce comportement était contrôlé justifie que le comportement soit attribué audit État » (225). Dans tous les cas, on pourrait conclure que si une activité de *hack-back* par une société privée est conduite sous le contrôle effectif de l'État (qui surveille son déroulement) sa responsabilité peut être engagée. En revanche, si un État a simplement encouragé des acteurs privés à conduire des opérations de *hack-back* (sans pour autant contrôler leur déroulement) la responsabilité de l'État ne pourra pas être engagée sur la base de l'article 8. On pourrait, néanmoins, considérer éventuellement dans une telle hypothèse qu'un État qui a encouragé des acteurs privés à entreprendre des opérations dommageables pour des pays tiers a manqué à son obligation de diligence.

c) L'État est responsable s'il a reconnu les actions des acteurs privés comme étant les siennes

Selon l'article 11 du projet de la CDI sur la Responsabilité internationale des États :

> « Un comportement qui n'est pas attribuable à l'État selon les articles précédents est néanmoins considéré comme un fait de cet État d'après le droit international si, et dans la mesure où, cet État reconnaît et adopte ledit comportement comme sien ».

Dans la jurisprudence internationale, l'exemple souvent avancé est l'arrêt rendu par la CIJ dans l'affaire du *Personnel diplomatique et consulaire des États-Unis à Téhéran* (1980). Dans cet arrêt la Cour a clairement distingué la situation juridique créée par la prise en otages des personnels de l'ambassade des États-Unis de celle créée par le décret de l'État iranien approuvant expressément cette prise d'otages. En matière de cybersécurité un parallèle pourrait être fait avec la situation où une opération de *hack-back* entreprise initialement par une société privée agissant serait par la suite endossée par l'État lui-même.

d) L'État est responsable s'il a manqué à ses obligations de diligence

Cette situation se distingue fortement de celles décrites précédemment. Dans les situations évoquées précédemment, certaines circonstances permettent d'attribuer à un État le comportement d'une société privée : on considère alors que

(224) *ACDI 2001*, *supra* note 19, p. 49.
(225) *Ibid.*, p. 50.

ce que la société privée fait est ce que l'État fait. Si l'acte en question constitue un acte internationalement illicite, l'État doit réparer les conséquences dommageables de cet acte.

En revanche, dans l'hypothèse présente, l'acte de la société privée n'est pas attribué à l'État. La responsabilité de ce dernier ne peut être ici engagée que dans la mesure où l'État n'a pas pris les mesures nécessaires et exigées par les circonstances pour empêcher les actions transfrontalières dommageables d'une société privée. On retrouve donc ici les conséquences en termes de responsabilité de la violation des obligations exposées *supra* (Partie I) : « qui peut et n'empêche, pèche ».

Conclusion

Notre analyse a montré que le droit international compte déjà de nombreuses règles susceptibles de régir les relations entre les États ainsi qu'entre les États et les acteurs privés en cas de cyberattaque.

Nous avons ainsi montré l'utilité du concept de cyber-diligence pour prévenir les cyberattaques ou pour agir rapidement pour mettre fin à celles-ci. L'obligation de diligence due que les États doivent exercer à l'égard des acteurs non-étatiques qui opèrent depuis leur territoire (qu'il s'agisse de groupes terroristes, de cybercriminels, d'entreprises ou de simples *hackers*) découle directement de l'obligation, pour tout État, « de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États ».

Nous avons ensuite examiné le régime juridique applicable aux cyberattaques en procédant à une classification des réactions possibles à celles-ci. Nous avons procédé à une distinction entre les réactions qui sont toujours autorisées et d'autres réactions qui ne sont admissibles que si l'on peut établir qu'un État a commis, par action ou omission, un « fait internationalement illicite ». Nous avons mis l'accent sur la nécessité de la coopération internationale dans ce domaine qui devrait commencer par la démarche de l'État victime de s'adresser à l'État d'où est issue la cyberattaque pour solliciter son intervention contre les auteurs des actes malveillants. Nous avons aussi mis en garde contre toute « banalisation » des ripostes qui constituent en principe des violations du droit international mais qui sont « excusées » comme circonstances excluant l'illicéité ou la responsabilité. Ceci vaut tant pour « l'état de nécessité », dont l'invocation est rarement acceptée en pratique par les juridictions internationales, que pour les contre-mesures. Ces dernières constituent, certes, une réponse autorisée par le droit international pour riposter à une cyberattaque qui viole le droit international et qui est attribuée à un État, mais cela reste « faute de mieux ». Dans différents domaines, ces procédés de « justice privée » ont cédé leur place à des procédures institutionnelles de règlement juridictionnel des différends et à des mécanismes centralisés d'exécution. Si les contre-mesures restent un moyen important de réaction aux cyberattaques pour les États (mais pas pour les acteurs privés), il faudrait éviter toute banalisation ou prolifération de ces procédés de justice privé qui comportent des risques pour l'ordre international et qui, par définition, font la part belle aux plus puissants.

Nous avons, enfin, procédé à une étude détaillée de la problématique de la « cyberdéfense active » et du « *hack-back* » sous l'angle tant du droit international que du droit comparé. Nous avons montré les nombreux obstacles juridiques et les risques que comportent un *hack-back* déclenché unilatéralement par des acteurs

non-étatiques. Les acteurs privés auraient donc plutôt intérêt à investir dans de bonnes pratiques d'hygiène et de sécurité informatiques – plutôt que chercher à acquérir des outils offensifs. Si, malgré tout, ils sont victimes d'une cyberattaque, plutôt que de se lancer dans un *hack-back* hasardeux et risqué tant sur le plan technique que sur le plan juridique, il serait préférable qu'ils puissent notifier cette attaque à leurs autorités et leur demander d'agir afin qu'ils puissent aussi exercer leurs droits légaux contre l'auteur de la cyberattaque (à supposer que ce dernier puisse être identifié). Les États pourraient, par ailleurs, autoriser le *hack-back* et/ou s'appuyer sur des acteurs privés pour conduire des contre-attaques dans certaines circonstances, mais ceci devrait se faire sous leur contrôle étroit et pourrait engager leur responsabilité internationale.

Dire que le droit positif apporte des solutions à différents problèmes concernant la prévention des cyberattaques et les réactions à celles-ci ne signifie nullement que les États devraient se désengager. Comme nous l'avons vu tout au long de cette analyse, de très nombreuses zones grises demeurent en droit international sur des questions pourtant fondamentales – alors que de nouvelles interrogations émergent sans cesse. Il est donc impératif pour la communauté internationale de coopérer étroitement pour trouver des réponses à ces questions en utilisant tous les moyens appropriés offerts par le droit international en fonction des circonstances : adoption de nouveaux instruments obligatoires ; adoption de textes de *soft law* ; interprétation dynamique et évolutive des règles existantes, etc.

Après une période relativement longue, les États se sont saisis ces dernières années du problème de la sécurité du numérique en général et des cyberattaques en particulier. Ils négocient et coopèrent dans différents *fora* en multipliant les initiatives au sein de diverses organisations internationales : organisations à vocation universelle, tout d'abord, avec les exemples majeurs de l'ONU (où néanmoins le GGE est, pour l'instant, un organe à composition restreinte) et de l'Union internationale des télécommunications ; ou à vocation régionale ou restreinte comme l'Union européenne, le Conseil de l'Europe, l'OSCE, l'OCDE, l'Union africaine, l'Organisation de coopération de Shanghai, l'Otan, le G20 et d'autres encore.

Toutefois, le problème est que le foisonnement de ces initiatives au sein de *fora* très divers ne témoigne pas nécessairement d'une bonne gouvernance de la sécurité du numérique. Certains États ont proposé comme remède à cette dispersion la création d'une nouvelle organisation internationale spécialisée dans la sécurité du numérique qui pourrait agir de façon centralisée. Pourtant, sur la scène internationale, l'ère n'est peut-être plus vraiment à l'adoption de structures lourdes passant par des négociations chronophages de nouveaux traités constitutifs qui pourraient d'ailleurs n'être jamais ratifiés par certains États. L'ère n'est pas non plus à la création de nouvelles organisations internationales à vocation universelle dotées de pouvoirs normatifs. On observe, au contraire, une multiplication de « *fora* », « réseaux », « groupes », « agences », « comités » et autres institutions informelles qui, peut-être, ne correspondent pas vraiment à la définition classique de l'organisation

internationale, mais qui remplissent leurs fonctions avec une certaine efficacité. Comme l'a résumé un auteur : « *Alternatives to international law are created through diverse intergovernmental coordinated actions that do not involve the setting up of international organizations that are subjects of international law* » (226).

Ces observations semblent être particulièrement pertinentes dans le domaine de la cybersécurité. En l'état actuel des choses, on voit difficilement comment les États pourraient s'engager dans la création d'une organisation internationale spécialisée dans ce domaine. On voit mal aussi comment ils pourraient transférer à une telle organisation des compétences importantes en matière de cybersécurité qui sont largement perçues comme relevant du domaine de la « sécurité nationale » et de la sécurité « humaine » de leurs populations, bref de leurs pouvoirs régaliens.

Toutefois, le besoin d'une meilleure coopération et la nécessité de rationaliser les initiatives se fait cruellement sentir, tout comme le besoin de renforcer les mesures de confiance et d'assistance en direction des nombreux pays qui accusent un retard certain en matière de cybersécurité. La création d'un organe susceptible de fédérer ces actions, d'assurer le suivi des décisions mais aussi de générer des études ou encore de dispenser des formations et de promouvoir une culture d'hygiène informatique, semble indispensable. Un tel organe ne pourra toutefois être efficace que s'il est souple, ouvert et dépourvu de pouvoirs normatifs qui pourraient éveiller les craintes de nombreux États.

Un tel organe devrait d'ailleurs, impérativement, réserver une grande place aux acteurs privés en prévoyant une composition multipartite (*multi-stakeholder*) ou, au moins, la création d'un mécanisme formel d'intégration du secteur privé tel qu'un « *Corporate Partnership Board* ». À cet égard, il convient de rappeler la proposition récente avancée par Microsoft de créer un organe informel de ce type en ajoutant aux G20 un *ICT20* – c'est-à-dire les 20 plus grandes compagnies des technologies de l'information et des communications (TIC) (227). Il pourrait toutefois être plus efficace (et plus conforme à la logique interétatique du droit international – surtout dans des domaines qui touchent directement la sécurité nationale des États) de créer un organe international souple permettant aux grandes compagnies des TIC de participer à un tel « *Corporate Partnership Board* » afin de travailler avec les États et les décideurs pour trouver des solutions efficaces aux nombreux défis actuels et futurs pour la sécurité du numérique.

(226) Eyal Benvenisti, « Substituting International Law », *in* « The Move from Institutions? », *American Society of International Law Proceedings*, vol. 100, 2006, p. 289-290.

(227) Voir Microsoft, *International Cybersecurity Norms, Reducing conflict in an Internet-dependent world*, 2015, p. 18 : « *A third option could be leveraging existing frameworks, such as G20, and extending them to 20 leading ICT providers (ICT20). The G20 + ICT20 would have the advantage of being global in nature yet manageable in terms of size. An agreed-upon norms document between these stakeholders could represent a powerful contribution to a first cybersecurity norms baseline. It would also allow the 20 most developed economies to hold themselves and others accountable to the agreed-upon behaviors in cyberspace. The drawback of such a group is its lack of truly global representation and its limited input from civil society. However, creating a G20 + ICT20 and top 20 nongovernmental organizations (NGO20) could improve collaboration and improve outcomes on norms. It will not be easy to establish criteria for selecting the ICT20 and NGO20, but it is well worth the effort to address this challenge* ».

TABLE DES MATIÈRES

Préface

Avant-propos

Introduction : Sécurité de l'espace numérique et droit international

I. Cyber-diligence : un concept clef face aux actes malveillants transnationaux

Introduction

A) Le fait d'une personne privée comme fait de l'État

B) L'« obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États »

1. « Qui peut et n'empêche, pèche » : le concept de cyber-diligence

A) La souveraineté des États au cœur du concept de cyber-diligence

B) La responsabilité des États à l'égard des attaques transnationales et des dommages causés à des États tiers

C) L'utilité du concept de cyber-diligence face aux cyberattaques

2. La cyber-diligence comme norme de comportement responsable et raisonnable

A) Une obligation de comportement et non de résultat

B) Une obligation fondée sur le principe de responsabilité commune mais différenciée ?

3. Un devoir de prévenir et de réagir aux cyberattaques

A) Prévention des cyberattaques et protection des infrastructures critiques numériques

B) Notification et répression des cyberattaques

II. Comment répondre aux cyberattaques ? Le cadre général du droit international

Introduction : à la recherche d'une classification des réactions aux cyberattaques

A) La définition des cyberattaques

B) À la recherche d'un critère de classification des réactions admissibles

1. Réactions en l'absence de violation du droit international par un autre État

A) Mécanismes de coopération internationale et de règlement des différends

a) Coopération entre les États concernés

b) Recours aux organisations internationales compétentes

B) Mesures de rétorsion

C) Mécanismes exceptionnels d'autoprotection (état de nécessité, détresse, force majeure)

a) La force majeure

b) La détresse

c) L'état de nécessité

2. Réactions en cas de violation du droit international par un autre État

A) Contre-mesures pacifiques

a) Conditions de déclenchement : l'existence d'un fait internationalement illicite d'un État

I. Violation d'une obligation internationale

II. Attribuable à un État

b) Conditions d'exercice

B) Légitime défense en cas « d'agression armée »

a) Condition de déclenchement : l'existence d'une agression armée

b) Conditions d'exercice

III. *Hack-back*, « cyberdéfense active » et le besoin d'un système international ordonné

Introduction : le rôle important des acteurs privés en cas de cyberattaque

A) Défense passive

B) Attribution des cyberattaques

C)* Hack-back *et « cyberdéfense active »

1. Arguments en faveur et contre le hack-back

A) Intérêt et avantages du hack-back

a) Le hack-back *pourrait remédier aux insuffisances de l'action gouvernementale*

b) Le hack-back *serait plus rapide et efficace*

c) Le hack-back *aurait un effet dissuasif important*

d) Le hack-back *permettrait aux entreprises de ne pas dévoiler leurs vulnérabilités*

e) Le hack-back *permettrait de résoudre des problèmes délicats d'extraterritorialité*

f) Le hack-back *serait bon pour les affaires et pour la recherche*

B) Inconvénients et risques

a) Risques d'escalade
b) Risques de déstabilisation
c) Risques pour l'autorité de l'État
d) Risques pour la conduite de la politique étrangère
e) Risques pour le renseignement et la lutte contre la criminalité
f) Risques de dommages collatéraux
g) Risques liés à la cyberdéfense active « automatique »
h) Risques d'un « retour de manivelle »
i) Risques d'une cyberdéfense active élitiste ou hypocrite
j) Un effet dissuasif contestable

2. Le *hack-back* « sauvage » : les acteurs privés peuvent-ils déclencher unilatéralement des mesures cyber-offensives ?

A) L'inexistence d'un « droit de* hack-back *» en droit international

B) Une violation du droit international ?

C) Le* hack-back *en tant que violation du droit interne

3. Le *hack-back* « encadré » : les États peuvent-ils s'appuyer sur des acteurs privés pour conduire des contre-attaques ?

A) Une coopération entre les acteurs publics et privés pour répondre aux cyberattaques ?

B) Le cas des Entreprises militaires et de sécurité privées (EMSP)

C) La responsabilité internationale des États peut-elle être engagée du fait de mesures de* hack-back *conduites par des acteurs privés ?

a) L'État est responsable s'il habilite des acteurs privés à exercer des prérogatives de puissance publique
b) L'État est responsable si des acteurs privés agissent sur ses instructions, ses directives ou sous son contrôle
c) L'État est responsable s'il a reconnu les actions des acteurs privés comme étant les siennes
d) L'État est responsable s'il a manqué à ses obligations de diligence

Conclusion