REVUE BELGE DE DROIT INTERNATIONAL
2017/2 – Éditions BRUYLANT, Bruxelles

OBLIGATIONS DE DILIGENCE DANS LE CYBERESPACE : QUI A PEUR DE LA CYBER-DILIGENCE ?

PAR

Karine BANNELIER*

Résumé

« Qui peut et n'empêche, pèche ». Ce vieil adage du XVII^e^ siècle traduit bien ce que le principe de due diligence exprime au XXI^e^ siècle à l'égard des États souverains dans l'espace numérique : intervenir quand ils le savent et qu'ils le peuvent pour empêcher des actes portant atteinte aux droits d'États tiers. Principe fécond du droit international, la due diligence est aujourd'hui appelée à jouer un rôle central dans la régulation des activités numériques, la prévention et la réaction aux cyber-attaques. La hausse spectaculaire des actes de malveillance dans le cyberespace dans lesquels sont impliqués des États mais aussi des acteurs non étatiques constitue en effet une véritable menace pour la paix et la sécurité internationales. Du point de vue du droit international, le phénomène est complexe à appréhender dans la mesure où certains États entretiennent des liens plus ou moins étroits avec ces groupes non étatiques et les utilisent comme des « intermédiaires », des « proxies », pour développer des activités malveillantes contre les intérêts d'autres États. Fondé sur l'une des obligations les plus importantes des États en droit international qui est l'obligation pour tout État de ne pas utiliser ou de ne pas laisser utiliser son territoire à des fins contraires aux droits des autres États, le principe de due diligence concerne un très grand nombre d'activités qui sont menées sous le contrôle ou la juridiction des États et ceci quels que soient les acteurs impliqués. Les États ne sont donc pas seulement responsables des activités conduites par leurs organes, ils peuvent aussi être tenus responsables des activités conduites par les personnes privées. Pourtant, certains États, dans le cadre des négociations menées au sein du Groupe d'experts gouvernementaux des Nations Unies sur la cyber-sécurité mais aussi certains experts ont remis en cause l'existence même de telles obligations dans le cyberespace et le concept associé de « cyber-diligence ». Ces objections sont multiples et remettent fondamentalement en question certains éléments fondamentaux des relations entre les États. L'objectif de cet article est tout d'abord de répondre à ces objections et dissiper les malentendus qui entourent l'existence même d'une obligation de diligence dans

* Maître de Conférences-HDR en droit international public (Université Grenoble Alpes), Directrice adjointe du Cyber Security Institute. Cet article a bénéficié du support de l'Agence Nationale de la Recherche de la France dans le cadre du programme « Investissements d'avenir » (ANR-15-IDEX-02). Cet article développe une réflexion amorcée dans deux articles sur l'application du principe de due diligence dans le cyber-espace : « "Cyber Diligence": A Low Intensity Due Diligence Principle for Low Intensity Cyber-Operations? », *Baltic Yearbook of Intl Law*, 2014, et « Le standard de due diligence et la cyber-sécurité », in *Le standard de due diligence et la responsabilité internationale*, Paris, Pedone, 2018 (à paraître).

le cyberespace pour en affirmer la positivité et en analyser la nature. Il propose ensuite une étude des défis de l'application de l'obligation de diligence dans le cyberespace et ses implications concrètes tant du point de vue du comportement requis par les États que du point de vue des règles secondaires et d'engagement de leur responsabilité internationale.

Abstract

"Who can and does not prevent, sin". This old adage of the seventeenth century reflects what the principle of due diligence expresses in the twenty-first century with regard to sovereign states in the digital space: to intervene when they know and they can to prevent acts that undermine rights of third States. As a fertile principle of international law, due diligence is today called upon to play a central role in the regulation of digital activities, the prevention and reactions to cyber-attacks and the maintenance of international peace and security. The dramatic rise of cyber-attacks involving States and non-State actors constitutes today a real threat to international peace and security. From an international law perspective, the phenomenon is all the more complicated because some States have more or less close ties with these non-State groups and use them as 'intermediaries', 'proxies', to develop malicious activities against the interests of other States. Founded on one of the most important obligations of the States in international law, which is the obligation for all States not to use or allow their territory to be used for acts contrary to the rights of other States, the due diligence principle concerns a very large number of activities which are conducted under the control or jurisdiction of States and this whatever the persons involved. The States are therefore not only responsible for the activities conducted by their agents, they may also be held responsible for activities conducted by private persons when they violate their obligations of diligence. However, a few States, and also some scholars (mainly from the Anglo-Saxon world), have questioned the very existence of such obligations and the associated concept of 'cyber-diligence' used to describe in one word the obligations of due diligence in cyberspace. These objections are multiple and call into question fundamental building blocks of international relations between States. The aim of this article is, first, to respond to all these objections and dispel any misunderstandings surrounding the very existence of an obligation of diligence in cyberspace in order to clearly affirm the positiveness of the principle and to analyze its precise nature. The study then focuses on the different challenges of due diligence obligations in cyberspace. It also discusses the parameters of the due diligence standard and its practical implications both as concerns the specific obligations of States in matters of cybersecurity and as concerns the consequences of its violation in the framework of secondary rules relating to the international responsibility of States.

Introduction

« Qui peut et n'empêche, pèche »(1). L'adage d'Antoine Loysel, jurisconsulte du XVII[e] siècle célèbre pour avoir collecté les règles coutumières du

(1) A. 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*, Paris, A. L'Angelier, 1607 (https://archive.org/details/1607LoiselInstitutesCoutumieres).

Royaume de France, traduit bien ce que le principe de due diligence exprime au XXIe siècle à l'égard des États souverains dans l'espace numérique : intervenir quand ils le savent et qu'ils le peuvent pour empêcher des actes portant atteinte aux droits d'États tiers. Principe fécond du droit international, la due diligence est aujourd'hui appelée à jouer un rôle central dans la régulation des activités numériques, la prévention et la réaction aux cyber-attaques (2) et le maintien de la paix et de la sécurité internationales.

Dans son rapport de 2015, le Groupe d'experts gouvernementaux des Nations Unies sur la cyber-sécurité (GGE) (3) exprimait son inquiétude face à des « tendances préoccupantes » marquées par une hausse spectaculaire des actes de malveillance dirigés notamment contre les infrastructures vitales des États (4). Les chiffres donnent en effet le vertige. Une étude publiée récemment par l'Union européenne dénombrait ainsi, pour 2016, pas moins de 4.000 attaques de rançongiciel lancées quotidiennement à travers le monde (5). Ce phénomène s'est nettement aggravé en 2017 comme en témoignent les attaques Wannacry ou NotPetya — et ceci alors que les rançongiciels sont loin d'être les seules menaces. Ces « tendances préoccupantes » sont largement dues à une augmentation de la « surface » des actes malveillants combinée à une sophistication croissante des méthodes et à une diversification de leurs auteurs (États, 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, etc.). 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 » (6).

(2) Pour une analyse des réponses du droit international aux cyber-attaques, voy. notre étude, K. Bannelier, T. Christakis, *Cyberattaques. Prévention-réactions : rôle des États et des acteurs privés*, Paris, Les Cahiers de la Revue Défense Nationale, 2017, 90 p.

(3) Le Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique (GGE) a été constitué pour la première fois en 2004 sur la base de la Résolution de l'Assemblée générale des Nations Unies 58/32 du 8 décembre 2003 afin d'assister le Secrétaire général des Nations Unies dans son examen des risques qui pourraient se poser dans le domaine de la sécurité de l'information ainsi que des mesures de coopération qui pourraient être prises et des principes internationaux susceptibles de renforcer cette sécurité.

(4) « L'environnement informatique mondial présente 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. […] 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 »).

(5) Voy. État de l'Union 2017 : la Commission renforce sa capacité de réaction face aux cyberattaques, Fiche d'information, Bruxelles, 19 septembre 2017.

(6) GGE 2015, *op. cit.*, § 5.

Du point de vue du droit international, le phénomène est particulièrement complexe à saisir dans la mesure où certains États entretiennent des liens plus ou moins étroits avec des acteurs privés et les utilisent comme des « intermédiaires » ou des « proxies » pour développer des activités malveillantes.

Or, cette multiplication d'actes de malveillance relevant d'acteurs privés est souvent associée 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. En réalité, l'infrastructure physique qui supporte internet et les activités numériques qui s'y développent, les données qui circulent, se situent en grande partie sur le territoire des États souverains ou sous leur contrôle (7). La territorialité de l'espace numérique a d'ailleurs clairement été reconnue par les membres du GGE dans leur rapport de 2015 où ils soulignent que « la compétence territoriale des États s'applique aux infrastructures informatiques situées sur leur territoire » (8). Il est ainsi admis que cette compétence 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 (9).

Une deuxième source d'erreur est de considérer que le droit international est muet dès lors que les activités sont d'origine privée. 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 développées sur leur territoire, sous leur juridiction ou sous leur contrôle et ils peuvent, dans certaines hypothèses, être tenus responsables de ces activités.

À cet égard, le principe de due diligence pourrait jouer un rôle important dans la prévention et la réaction à ces actes malveillants et constituer même une pièce maîtresse de la régulation du cyberespace. Fondé sur l'une

(7) Comme le soulignait en effet le conseiller juridique du département d'État américain H.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, http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.

(8) GGE 2015, *op. cit.*, § 28 (a).

(9) Ceci ne signifie pas, bien entendu, que tous les problèmes sont résolus automatiquement. Les différentes techniques utilisées lors des cyberattaques (y compris l'utilisation de botnets ou les techniques de *spoofing*) peuvent limiter l'importance de cette compétence territoriale. Mais, en fonction des circonstances, cette dernière peut s'avérer importante chaque fois qu'un État *sait* que ses infrastructures sont utilisées pour lancer des cyberattaques et *dispose de moyens techniques* pour les arrêter ou en atténuer les effets.

des obligations les plus importantes des États en droit international qui est l'obligation pour tout État de ne pas utiliser ou de ne pas laisser utiliser son territoire à des fins contraires aux droits des autres États, il concerne en effet un très grand nombre d'activités qui sont menées sous le contrôle ou la juridiction des États et ceci quels que soient les acteurs impliqués. Les États ne sont donc pas seulement responsables des activités conduites par leurs organes, ils peuvent aussi être tenus responsables des activités conduites par les personnes privées.

Pourtant, aussi étonnant que cela puisse paraître, certains États, dans le cadre des négociations menées au sein du Groupe d'experts gouvernementaux des Nations Unies sur la cyber-sécurité, ont remis en cause l'existence même de telles obligations et le concept associé de « cyber-diligence » utilisé pour décrire en un mot les obligations de diligence due dans le cyberespace (10). Ces objections sont multiples et remettent fondamentalement en question certains éléments fondamentaux des relations entre les États. Elles concernent tout d'abord la *positivité* de la diligence due et contestent tantôt l'existence d'obligations de vigilance en droit international *général*, tantôt l'existence de telles obligations en dehors du domaine spécifique de la protection de l'environnement et tantôt leur existence dans le domaine particulier de la cyber-sécurité. Parallèlement, certains auteurs, principalement issus de la doctrine anglo-saxonne, dénoncent le caractère dangereux et déstabilisateur de l'application du principe de due diligence au cyberespace (11), tandis que d'autres se focalisent sur ce qui est présenté comme « l'indétermination normative » et les « lacunes » du régime juridique de la diligence due qui ne pourrait ainsi être appliquée en matière de cyber-sécurité qu'à la condition d'être précisée et clarifiée (12). D'autres enfin, comme le Manuel de Tallinn 2.0, sans remettre en cause son application au cyberespace, rejettent l'idée selon laquelle l'obligation de diligence pourrait comprendre, au-delà d'un droit de réaction, une dimension de prévention ou de répression (13).

(10) Pour ce concept et la diligence requise par les États dans le cyberespace voy. K. Bannelier, « Cyber-Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber-Operations? », *Baltic Yearbook of International Law*, vol. 14, 2014, pp. 23-39. La France a officiellement adopté ce terme comme en témoigne la *Revue Stratégique de cyberdéfense* (Secrétariat de la Défense et de la Sécurité Nationale) publiée le 12 février 2018 (voy. par ex. p. 86), disponible sur http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

(11) E. Talbot Jensen, S. Watts, « A cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer », *Texas Law Review*, vol. 95, 2017, pp. 1555-1577.

(12) Voy. à cet égard l'intervention de N. Tsagourias, « On the virtues and limitations of cyber due diligence », *Agora 12: The Defence of General Interests in Cyberspace*, 13th Annual Conference of the European Society of International Law, *Global Public Goods, Global Commons and Fundamental Values: The Responses of International Law*, Naples, 8 septembre 2017.

(13) M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, CUP, 2017, 598 p. Voy. *Infra*, nos analyses à cet égard.

Certaines de ces objections résultent peut-être de malentendus liés à une absence de théorisation suffisante du standard de diligence due (14) ainsi qu'à une confusion sur la nature des obligations de vigilance en droit international. Il est vrai que le concept de due diligence est particulièrement complexe et son application dans les différentes branches du droit international peut soulever des interrogations légitimes. Ceci est particulièrement vrai dans le domaine entièrement nouveau de la cyber-sécurité, où, du fait même de la nature du cyberespace et du caractère souvent obscur et sophistiqué des cyberattaques, les questions sont particulièrement délicates. Mais la réponse ne peut sans doute pas être de faire disparaître par magie les obligations de diligence des règles juridiques régissant le comportement responsable des États dans le cyberespace. L'échec du dernier GGE à adopter un rapport substantiel sur la façon dont les règles du droit international s'appliquent au cyberespace (15) invite au contraire les juristes à s'atteler à cet important chantier qui consiste, entre autres, à identifier un régime juridique crédible et cohérent de « cyber-diligence » qui tient compte des difficultés, notamment technologiques, inhérentes à ce domaine.

L'objectif de cet article est tout d'abord de répondre à ces objections et dissiper les malentendus qui entourent l'existence même d'une obligation de diligence dans le cyberespace pour en affirmer la positivité et en analyser la nature (I). Nous concentrerons ensuite notre étude sur les défis de l'application de l'obligation de diligence dans le cyberespace et ses implications concrètes tant du point de vue du comportement requis par les États que du point de vue des règles secondaires et d'engagement de leur responsabilité internationale (II).

I. — L'existence d'une obligation de diligence dans le cyber-espace

Malgré les différentes tentatives de la remettre en cause, l'existence en droit international positif d'un devoir de diligence due dans le cyberespace ne fait pas de doute (A). Ceci nous invite à nous interroger sur la nature de cette obligation afin d'en comprendre les tenants et les aboutissants (B).

A. — *Positivité du devoir de due diligence dans le cyberespace*

Nous nous attacherons tout d'abord à présenter les objections concernant la positivité du devoir de diligence dans le cyberespace (1), avant de

(14) Comme le remarque en effet Riccardo Pisillo Mazzeschi, le concept de due diligence a été pendant longtemps ignoré de la doctrine. Voy. R. Pisillo Mazzeschi, « Le standard de due diligence comme extension ou limite de la responsabilité internationale », in SFDI-SID, *Le standard de due diligence et la responsabilité internationale*, Paris, Pedone, à paraître.

(15) Voy. *Infra*, Partie I(C).

les réfuter et d'affirmer l'applicabilité d'une obligation de diligence dans le cyberespace et en matière de cyber-sécurité (2).

1) *Les objections au concept de cyber-diligence*

Plusieurs objections au concept de cyber-diligence ont été formulées ces dernières années par des acteurs surtout anglo-saxons.

a) *La due diligence, un simple « standard » de* soft law *?*

Selon une première objection, le standard de due diligence en droit international ne ferait partie que de la *soft law* et ne relèverait pas du droit positif. La due diligence serait peut-être une proposition normative à envisager *de lege ferenda*, mais elle ne ferait certainement pas partie de la *lex lata*. Le terme « standard » pour qualifier la diligence due en droit international serait donc particulièrement approprié car il évoquerait la *soft law* et indiquerait que la due diligence n'a pas atteint un seuil de normativité suffisant pour répondre à la définition de « norme ». La due diligence n'exprimerait que le souhait d'un comportement responsable dont les contours seraient imprécis et qui ne pourrait passer le seuil de la normativité que par une concrétisation précise et détaillée dans un traité international.

Lors des débats au sein du GGE, et alors que de nombreux États ont soutenu l'existence en droit positif d'une obligation de due diligence dans le cyberespace, quelques États ont ainsi refusé de reconnaître son applicabilité à la sécurité du numérique (16). Certains ont affirmé que le concept de « due diligence » aurait émergé de l'arrêt de la CIJ dans l'affaire du *Détroit de Corfou* et que, selon le principe de *res judicata*, il ne lierait que les États parties au litige pour cette affaire précise. Le concept de « due diligence » n'aurait donc pas fait l'objet d'une reconnaissance plus générale en droit international. Il a aussi été soutenu que l'on ne trouvait nulle part, ni dans la pratique internationale ni dans l'*opinio juris*, une preuve quelconque qui soutiendrait l'affirmation selon laquelle il existerait en droit international général une « obligation de diligence due ». Enfin, selon un dernier argument, la CIJ, dans l'affaire du *Détroit de Corfou*, n'aurait pas étayé son fameux *dictum* selon lequel chaque État a l'obligation « de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États ».

Dans la doctrine juridique, il est difficile de trouver une négation aussi radicale et complète de l'existence même d'obligations de diligence en droit

(16) L'auteur de cet article a participé à différents séminaires et réunions d'experts en matière de cyber-sécurité organisés avec des membres du GGE. Ces réunions se sont déroulées sous la règle de Chatham House, selon laquelle les participants sont libres d'utiliser les informations collectées à cette occasion, mais ne doivent révéler ni l'identité ni l'affiliation des personnes à l'origine de ces informations. C'est la raison pour laquelle, en respect de cette règle, les positions de certains États sont évoquées ici mais leur identité ne sera pas révélée.

international. À notre connaissance, les critiques adressées à la Cour internationale de justice pour base juridique insuffisante de son *dictum* dans l'affaire du *Détroit de Corfou* sont rares, à l'exception peut-être du juge Badawi Pacha qui, dans son opinion dissidente jointe à l'arrêt, avait déclaré qu'une « pareille obligation générale n'existe pas et ne peut exister » (17). Certains auteurs ont toutefois essayé de limiter la portée de la diligence due, soit en suggérant que les obligations de « *best efforts* » relèveraient davantage du domaine politique que du domaine normatif (18), soit en affirmant que les obligations de diligence n'existeraient qu'en droit international de l'environnement (comme le démontrerait le fameux arbitrage dans l'affaire de la *Fonderie du Trail*) et qu'une preuve de leur application dans d'autres domaines du droit international devrait être recherchée dans la pratique et l'*opinio juris* des États (19).

b) *Règles primaires particulières contre principe général ?*

Ces dernières considérations nous amènent à une seconde série d'objections qui concernent plus précisément l'existence d'une obligation de diligence dans le domaine du cyberespace et de la cyber-sécurité. Ces objections pourraient être résumées ainsi : une obligation de diligence ne peut découler que d'une obligation primaire spécifique consacrée de façon incontestable par une convention internationale ou une coutume clairement établie. De telles obligations existent sans doute dans certaines branches spécifiques du droit international, surtout dans le droit international de l'environnement, mais il n'existe pas de règle *générale* relative à la diligence due qui serait applicable dans *tous* les domaines, y compris donc dans celui du cyberespace. Si l'on veut donc avancer l'existence d'un standard de diligence due dans un domaine précis, il faut apporter la preuve de l'existence d'une règle primaire particulière imposant des obligations de comportement dans cette branche du droit international.

Comme nous le voyons, ces objections portent principalement sur deux points : d'une part, l'inexistence d'une obligation « générale » de diligence en droit international qui nécessiterait donc d'apporter la preuve de l'existence

(17) Opinion dissidente du juge B. Pacha, *Affaire du Détroit de Corfou*, arrêt du 4 avril 1949, *CIJ Recueil*, 1949, p. 65. Pour une analyse récente de l'ensemble de cette affaire ainsi que de la positivité et de la pertinence du *dictum* de la Cour en ce qui concerne l'« obligation, pour tout État de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États », voy. K. Bannelier, T. Christakis, S. Heathcote (eds), *The ICJ and the Evolution of International law: The enduring impact of the Corfu Channel case*, New York, Routledge, 2011 (2nd ed. 2013), 377 p.

(18) Voy., par exemple, M. Glennon, « Foreword », in R. Barnidge, *Non-State Actors and Terrorism — Applying the Law of State Responsibility and the Due Diligence Principle*, La Haye, Asser, 2008.

(19) Voy. M. N. Schmitt, « In Defense of Due Diligence in Cyberspace », *The Yale Journal Forum*, June 2015, p. 73. M.N. Schmitt ne partage néanmoins pas cette approche, considérant que : « *In international law, it is unnecessary to identify a distinct reason to apply a general principle in a particular context. On the contrary, since it is a general principle, the presumption is that the principle applies unless state practice or* opino juris *excludes it* ».

d'une règle primaire pour *chaque* branche du droit international et, d'autre part, l'inexistence d'une telle règle primaire dans le domaine du cyberespace et de la cyber-sécurité en raison de l'absence d'une convention internationale en matière de cyber-sécurité imposant de telles obligations et d'une pratique et d'une *opinio juris* encore balbutiantes dans ce domaine.

c) *Les travaux du GGE comme appui ?*

Les porteurs de ces objections pourraient peut-être essayer de s'appuyer sur les récents travaux conduits au sein du GGE. En effet, même si ce dernier a clairement introduit le concept de « cyber-diligence » en déclarant que : « Les États ne devraient pas permettre sciemment que leur territoire soit utilisé pour commettre des faits internationalement illicites à l'aide des technologies de l'information et des communications » (20), cette affirmation se situe dans la partie du rapport « Normes, règles, et principes de comportement responsable des États » qui semble, malgré son intitulé, davantage relever du domaine de la *soft law* que de celui du droit positif. En introduction de cette partie, le rapport précise en effet qu'il « propose » une série de « recommandations » pour « examen par les États concernant des normes, règles ou principes de comportement responsable des États, facultatifs, *non contraignants* et devant permettre de promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique » (21). Au-delà de ces précisions, le langage utilisé pour décrire le concept de cyber-diligence, notamment l'usage du conditionnel (« ne devraient pas », « *should not* ») plutôt que de l'indicatif (« ne doivent pas », « *shall not* »), semble encore indiquer qu'il s'agit davantage de l'expression d'une intention politique que d'une obligation juridique.

L'échec de la dernière session du GGE pourrait aussi être perçu par certains comme un indice révélateur de l'absence de consensus entre les États sur la question de l'application de l'obligation de due diligence au cyberespace. En effet, alors que le GGE avait pour mandat de faire un rapport à l'Assemblée générale sur « comment le droit international s'applique » dans le cyberespace (22), ce rapport, bien que très avancé, n'a pu finalement être adopté en juillet 2017, faute de consensus entre les États.

(20) GGE 2015, *op. cit.*, § 13(c), p. 8.

(21) *Ibid.* Nous soulignons.

(22) Dans sa résolution A/70/237 adoptée le 30 décembre 2015, l'Assemblée générale des Nations Unies avait invité le nouveau Groupe d'Experts Gouvernementaux (GGE) d'informer le Secrétaire général sur sa vision et son évaluation de plusieurs sujets liés au développement dans le domaine de l'information et de la télécommunication dans le contexte de la sécurité internationale, y compris « comment le droit international s'applique dans l'utilisation de l'information et des technologies de l'information par les États, comme les normes, les règles et les principes d'un comportement responsable des États, ainsi que des mesures pour fonder et construire la confiance ».

2) *La réfutation de ces objections : l'existence d'un devoir de diligence dans le cyberespace*

Nous allons maintenant essayer de réfuter chacune de ces objections.

a) *« Les obligations de diligence existent, nous les avons rencontrées »*

Réfutons, tout d'abord, les arguments selon lesquels les obligations de vigilance en droit international ne relèveraient que de la *soft law* et ne seraient que de simples intentions politiques dépourvues de toute normativité. « Les obligations de diligence existent, nous les avons rencontrées », pourrait-on répondre en paraphrasant Prosper Weil (23). Il ne fait aucun doute que le droit positif contemporain comporte des obligations de vigilance dans de nombreux domaines, la seule question est de savoir si ces obligations existent dans *tous* les domaines du droit international ou seulement dans certains domaines précis (et alors lesquels).

En pratique, force est de constater que les États qui ne se sont pas conformés à leurs obligations de vigilance ont été condamnés pour ces manquements, que ce soit dans le domaine de l'environnement (l'affaire de la *Fonderie du Trail* étant la plus célèbre) ; de la protection de la sécurité des États tiers (en commençant par l'arbitrage de l'*Alabama* ou l'affaire du *Détroit de Corfou*) ; de la protection des étrangers (avec un nombre impressionnant d'arbitrages et arrêts qui concernent tantôt la protection du personnel diplomatique et consulaire tantôt la protection d'individus qui ne sont pas des agents d'un État) ou encore, mais la liste est loin d'être exhaustive, de la protection des droits de l'homme (où, dans un grand nombre d'affaires, des Cours, Commissions ou Comités des droits de l'homme ont condamné des États pour manquement à leurs obligations positives (24)).

b) *L'échec des arguments sémantiques*

Les arguments sémantiques ne sont pas non plus très convaincants car le terme « standard » ne renvoie pas exclusivement à la *soft law*. Comme l'explique bien, par exemple, le *Dictionnaire de Droit International Public* : « Le mot standard *renvoie tantôt à une norme incontestée de droit international*, tantôt à des principes n'ayant pas un seuil de normativité suffisant pour répondre à la définition de "norme" » (25). À cet égard, il n'est peut-être pas très approprié d'utiliser comme *seul* qualificatif adossé à la due diligence ce « vocable d'origine anglaise dont l'utilisation en français prête souvent

(23) « Le droit international existe, je l'ai rencontré » (P. Weil, *Le droit international en quête de son identité*, RCADI, t. 237 (1992 VI), La Haye, Martinus Nijhoff, 1996, p. 47).

(24) Voy. à cet égard les analyses de R. Pisillo Mazzeschi, *Responsabilité de l'État pour violation des obligations positives relatives aux droits de l'homme*, RCADI, vol. 333, 2008, pp. 175-506.

(25) J. Salmon (dir.), *Dictionnaire de droit international public*, Bruxelles, Bruylant/AUF, 2001, p. 1049. Nous soulignons.

à confusion » — pour citer encore le même dictionnaire autorisé. À côté du terme « standard », il serait sans doute utile de parler « *d'obligations* de diligence » en droit international afin de clairement désigner l'existence en droit positif d'un *devoir* des États d'adopter un comportement requis par certaines règles primaires du droit international et d'éviter ainsi ces confusions. Même des auteurs comme Riccardo Pisillo Mazzeschi qui privilégient le terme « standard » insistent sur le fait qu'« on ne peut pas parler de *soft law* en ce qui concerne la due diligence » (26) et n'hésitent pas non plus à se référer aux « obligations de due diligence » dans leurs écrits (27).

c) *Le foisonnement de règles primaires : une présomption en faveur de l'existence d'un principe général ?*

La seconde série d'objections est sans doute plus importante. Comme nous l'avons évoqué, ces objections soulèvent en réalité deux questions qui sont liées mais distinctes : 1) peut-on considérer qu'il existe un principe général de « diligence due » qui s'appliquerait dans toutes les branches du droit international et qui imposerait donc certaines obligations de comportement dans tous les domaines (y compris donc en matière de cyber-sécurité) ? ; et 2) en cas de réponse négative, existerait-il des obligations de diligence due dans le domaine spécifique de la cyber-sécurité ? Inutile de dire que l'on pourrait théoriquement répondre par la négative à la première question, qui est plutôt d'ordre théorique et générale, tout en répondant positivement à la seconde.

Commençons donc par la première question. Il est intéressant de noter que, au-delà de certains acteurs (dont un nombre limité d'États) qui pourraient donner l'impression de vouloir réfuter, pour des considérations politiques ou autres, une applicabilité générale de la due diligence en droit international, même des observateurs neutres et attentifs ont exprimé des doutes à cet égard. Nous pensons surtout à Riccardo Pisillo Mazzeschi qui est incontestablement l'un de ceux ayant dédié à la due diligence les études les plus approfondies (28). Ainsi, dans son étude de 1992, Riccardo Pisillo Mazzeschi exclut une applicabilité générale de la due diligence et conclut que :

> « *Our research has shown that the notion of due diligence plays a role only in some normative areas of general international law, which we have identified.* [...].

(26) Voy. à cet égard R. Pisillo Mazzeschi, « Le standard de due diligence comme extension ou limite de la responsabilité internationale », *op. cit.*

(27) Voy., par exemple, R. Pisillo Mazzeschi, *Responsabilité de l'État pour violation des obligations positives relatives aux droits de l'homme*, *op. cit.*, pp. 282 et s.

(28) Au-delà des autres études déjà citées, voy. R. Pisillo Mazzeschi, « *Due Diligence* » *e responsabilità internazionale degli Stati*, Milano, 1989 ; R. Pisillo Mazzeschi, « Forms of International Responsibility for Environmental Harm », in F. Francioni & T. Scovazzi (eds), *International Responsibility for Environmental Harm*, 1991, pp. 15 et s. ; R. Pisillo Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », *German Yearbook of International Law* (t. 35), 1992, pp. 9 et s.

The "diligence" factor is present only in the content of certain international obligations » (29).

Cette conclusion appelle néanmoins quelques remarques. Tout d'abord, la liste des domaines présentés par l'auteur en 1992 comme étant « les seuls » où une obligation de diligence due existe doit sans doute être révisée aujourd'hui. Les trois domaines d'application de la due diligence présentés par Riccardo Pisillo Mazzeschi (1. Protection des étrangers et des représentants des États tiers ; 2. Sécurité des États tiers ; et 3. Protection de l'environnement) sont toujours, bien entendu, d'une grande actualité, mais ils ne sont sans doute plus les seuls. Riccardo Pisillo Mazzeschi a lui-même en 2006, dans son cours à l'Académie de droit international de La Haye, complété cette liste avec un quatrième domaine majeur, celui de la protection des droits de l'homme (30). Dans ses rapports récents sur « *Due Diligence in International Law* », l'*International Law Association* (ILA) a proposé des arguments convaincants pour ajouter d'autres domaines du droit international, comme le droit des investissements internationaux (31) ; le droit international humanitaire (32) ; le droit pénal transnational et la lutte contre la criminalité transnationale (33) ainsi que le droit de la mer (34). Sans doute pourrait-on ajouter encore d'autres domaines du droit international qui n'ont pas été mentionnés dans ces études, comme le droit de l'espace (35) ou celui de la protection des données (36).

À la lumière de cet impressionnant développement du champ d'application de la due diligence, le véritable enjeu n'est peut-être plus d'identifier les branches du droit international qui comportent des obligations de vigilance

(29) R. Pisillo Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », *op. cit.*, pp. 46 et 47. Voy. aussi p. 20 où l'auteur souligne qu'il est nécessaire de définir « *the scope of application* of diligence; that is, in which areas of rules or obligations does diligence come into play and in which areas does it not come into play ».

(30) R. Pisillo Mazzeschi, *Responsabilité de l'État pour violation des obligations positives relatives aux droits de l'homme*, *op. cit.*, passim.

(31) ILA Study Group on Due Diligence in International Law, first Report, 7 mars 2014, pp. 6 et s. (http://www.ila-hq.org/index.php/study-groups). Voy. aussi E. De Brabandere, « 'Host States' Due Diligence Obligations in International Investment Law », *Syracuse Journal of International Law and Commerce*, vol. 42-2, 2015, pp. 319 et s. ; A. De Nanteuil, *Droit international de l'investissement*, Paris, Pedone, 2014, pp. 364-366.

(32) ILA Study Group on Due Diligence in International Law, first Report, *op. cit.*, pp. 11 et s.

(33) *Ibid.*, pp. 22 et s.

(34) *Ibid.*, pp. 29 et s.

(35) L'interdiction de la militarisation des corps célestes, par exemple, ou la non-arsenalisation partielle (interdiction, par exemple, de mettre sur orbite des armes de destruction massive) de l'espace circumterrestre, comporte logiquement non seulement une obligation d'abstention mais aussi une obligation de vigilance qui est d'autant plus importante aujourd'hui que le secteur privé occupe une place fondamentale dans les activités spatiales. Voy., par ailleurs, S. Aoki, « The standard of due diligence in operating a space object », *Proceedings of the International Astronautical Congress, IAC*, vol. 14, pp. 11659-11667.

(36) Le Règlement général sur la protection des données de l'Union européenne, qui est entré en vigueur le 24 mai 2016 et qui sera applicable à partir du 25 mai 2018, comporte plusieurs obligations de vigilance pour les États.

mais plutôt celles où les obligations de vigilance sont absentes. Dans son étude précitée, Riccardo Pisillo Mazzeschi semble penser qu'il existerait de telles branches mais il ne les identifie pas. Il se pourrait, en effet, que certaines branches du droit international ne comportent que des obligations de résultat ou encore ce que Riccardo Pisillo Mazzeschi appelle des « obligations à réalisation progressive » (37). Toutefois, il est très difficile d'identifier de tels domaines et, en toute hypothèse, si de tels domaines devaient encore exister, ils constitueraient peut-être davantage l'exception que la règle.

Ne pourrait-on pas dès lors considérer, à l'instar de nombreux auteurs (38), que le concept de due diligence fait partie du droit international général et s'applique dans *toutes* les branches de ce droit — sauf si certaines règles primaires excluent son application ?

d) *Le fondement de l'obligation de diligence due :* sic utere tuo ut alienum non laedas *?*

Mais une telle conclusion se heurte à une difficulté importante. Si le concept de due diligence fait partie du droit international général, quel est alors son fondement ? La diligence due n'est pas une règle primaire autonome qui, tel un *deus ex machina*, intervient pour tout régler et tout prévenir. Le concept de due diligence ne peut que décrire une dimension précise de certaines obligations internationales en indiquant que ces obligations imposent aux États certains *devoirs de comportement* vigilant. Ainsi, par exemple, la prohibition de la torture comporte à la fois une obligation d'abstention/résultat (les agents de l'État ne doivent pas pratiquer la torture) et une obligation de vigilance (l'État doit adopter des mesures raisonnables de protection pour

(37) Voy. R. Pisillo Mazzeschi, *Responsabilité de l'État pour violation des obligations positives relatives aux droits de l'homme*, *op. cit.*, pp. 290 et s., 297 et s., et 429 et s.

(38) Voy., par exemple, A. Ouedraogo qui affirme que la due diligence « est devenue un principe général applicable même en l'absence de mention spécifique dans la règle primaire » (A. Ouedraogo, « La due diligence en droit international : de la règle de la neutralité au principe général », *Revue générale de droit*, vol. 42, n° 2, 2012, p. 644). Selon toujours cet auteur, « eu égard à la densité de la pratique étatique et de la jurisprudence arbitrale, notamment, la diligence devient une norme du droit international général » (*ibid.*, p. 657). Selon T. Koivurova, « Although the concept of due diligence remains a general one in international law, *State practice has developed more precise rules and standards as to what due diligence requires of its subjects in certain areas of international relations* » (T. Koivurova, « *Due Diligence* », *Max Planck Encyclopedia of Public International Law*, p. 1 (nous soulignons)). Selon l'*International Law Association*, il existe un « *broad principle of due diligence* » qui « *can be viewed as a default standard that is triggered in operation if no more specific elaboration of due diligence or stricter standard is in existence. Subject to specific primary rules, this general principle of due diligence remains applicable and requires active (though not easily identified) measures of due diligence by States in their own territory* ». Et le rapport de l'ILA ajoute que : « *there is no contradiction between the general standard and more specific expressions of due diligence in sub-branches of international law* » (ILA Study Group on Due Diligence in International Law, Second Report, juillet 2016, p. 4 (http://www.ila-hq.org/index.php/study-groups)). Voy. aussi M. N. Schmitt, « In Defense of Due Diligence in Cyberspace », *op. cit.*, p. 73 : « *In international law, it is unnecessary to identify a distinct reason to apply a general principle in a particular context. On the contrary, since it is a general principle, the presumption is that the principle applies unless state practice or* opinio juris *excludes it* ».

empêcher que des individus pratiquent la torture lorsqu'il a ou devrait avoir connaissance de tels actes). En d'autres termes, la due diligence qualifie ce que certaines règles primaires requièrent des États. Mais quelles seraient alors ces règles primaires imposant un devoir de diligence due en droit international général, y compris dans le cyberespace ?

On pourrait répondre que l'obligation de diligence, dans les relations entre les États (39), découle notamment de la souveraineté de ces derniers et du principe *sic utere tuo ut alienum non laedas*. La souveraineté territoriale des États implique en effet des droits mais aussi des devoirs à l'égard des États tiers. Comme le soulignait déjà Max Huber en 1925 dans 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 » (40). Quelques années plus tard, en 1928, la sentence arbitrale rendue dans l'*Affaire de l'île de Palmas* a confirmé cette position en soulignant que « 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 » (41).

Les États souverains ont donc le droit au respect de leur intégrité mais ils ont aussi en miroir de ce droit un devoir, celui de ne pas utiliser ou de ne pas laisser utiliser leur territoire d'une manière qui porterait atteinte aux droits d'un autre État et ce devoir est une obligation de due diligence. Bien avant sa fameuse transposition dans le domaine du droit international de l'environnement, une longue série d'arbitrages a appliqué cette obligation en relation avec la protection des étrangers et des représentants d'États (42). C'est ainsi que quand, en 1941, la due diligence a été appliquée pour la première fois à une affaire concernant une pollution transfrontière (*Affaire de la Fonderie du Trail*), le tribunal arbitral n'a fait qu'appliquer à ce domaine par analogie ce qu'il a qualifié de « *principle of international law* » (43). Quelques années plus

(39) Dans d'autres domaines, telle la protection des droits de l'homme ou la protection de la sécurité physique des investisseurs ou de leurs investissements, d'autres fondements devraient être recherchés bien entendu.

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

(41) *Île de Palmas, États-Unis c. Pays-Bas*, Sentence arbitrale du 4 avril 1928, *RSA*, vol. II, p. 839.

(42) Voy. à cet égard les illustrations données par R. Ago, *Quatrième rapport sur la responsabilité des États*, *ACDI*, 1972, vol. II, pp. 109-116, §§ 74-90. En relation plus spécifiquement avec la protection des représentants des États étrangers, voy. R. Ago, *Septième rapport sur la responsabilité des États, ACDI*, 1978, vol. I, Part. 1, p. 33, § 13, note 18.

(43) Selon le Tribunal arbitral dans l'*Affaire de la Fonderie du Trail* : « *As Professor Eagleton puts in (*Responsibility of States in International Law*, 1928, p. 80) : 'A State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction'. A great number of such general pronouncements by leading authorities concerning the duty of a State to respect other*

tard, la Cour internationale de justice dans l'*Affaire du Détroit de Corfou* n'a, elle non plus, pas hésité à affirmer que l'« obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États » était un principe général.

Il est par ailleurs intéressant de rappeler que la CDI, dans ses travaux sur la prévention des dommages transfrontières résultant d'activités dangereuses, travaux qui reposent largement sur le principe de due diligence, a insisté sur le fait que toute activité comportant un risque de causer un dommage transfrontière significatif entrait dans le champ de ses articles et a refusé d'établir une liste de ces activités au motif, notamment, qu'une telle liste serait rapidement dépassée en raison de la rapidité des évolutions technologiques (44).

Il semble donc que l'obligation de due diligence va bien au-delà de tel ou tel domaine spécifique du droit international ou activité et constitue un principe général du droit international qui découle de la souveraineté des États et s'applique aussi, de ce fait, au cyberespace et à la cyber-sécurité. Comme le souligne à cet égard le rapport du GGE de 2015, « la compétence territoriale des États s'applique aux infrastructures informatiques situées sur leur territoire » (45) et « [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 » (46).

e) *Obligation de due diligence et protection de la sécurité des États tiers*

Toutefois, même si quelqu'un réfutait l'application de l'obligation de diligence au cyberespace en tant que principe général du droit international, il est incontestable et incontesté que l'obligation de due diligence s'applique dans le domaine spécifique de la protection de la *sécurité des États tiers*, ce qui implique aussi logiquement leur sécurité dans le cyberespace.

L'existence d'obligations de diligence en matière de sécurité des États étrangers a été maintes fois affirmée, tant par la doctrine (47) que par la pratique diplomatique et jurisprudentielle qui, de l'affaire de l'*Alabama* (48)

States and their territory have been presented to the Tribunal. These and many others have been carefully examined. International decisions, in various matters, from the Alabama case onward, and also earlier ones, are based on the same general principle… » (*Affaire de la Fonderie du Trail, Canada c. États-Unis*, Sentence arbitrale du 11 mars 1941, *RSA*, III p. 1963).

(44) 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, Article 1, commentaire §§ 2-4, pp. 409-410.

(45) GGE 2015, *op. cit.*, § 28 (a).

(46) *Ibid.*, § 27.

(47) Voy., par exemple, R. Pisillo Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », *op. cit.*, pp. 31-36.

(48) Dans l'*Affaire de l'Alabama*, le tribunal a clairement reconnu l'applicabilité d'une obligation de diligence due et a conclu que « *the British government failed to use due diligence in the performance of its neutral obligation and especially that it omitted* […] *to take in due time any effec-*

à l'affaire *RDC c. Ouganda* (49), en passant par plusieurs autres affaires telles que celle relative au *Détroit de Corfou* (50) ou celle relative à l'*Agression contre la Légation de Roumanie à Berne* (51), n'a cessé de rappeler le devoir des États de prendre toutes les mesures raisonnables à leur disposition pour essayer d'empêcher une atteinte à la sécurité des États tiers. Ces obligations de diligence ont d'ailleurs été substantiellement renforcées dans le cadre de la lutte contre le terrorisme (52), surtout depuis le 11 septembre 2001 (53), où il a été affirmé que les États devraient aussi adopter des mesures actives afin de prévenir et réprimer les activités terroristes.

Il est donc manifeste que les États ont des obligations de diligence qui consistent à prendre toutes les mesures raisonnables à leur disposition pour empêcher que leur territoire soit utilisé pour porter atteinte à la sécurité d'autres États. Comment pourrait-on dès lors exclure le cyberespace de l'applicabilité de cette règle générale en matière de sécurité ?

Le principe de due diligence dans le cyberespace constitue pour les États un aspect essentiel de leur cyber-sécurité. C'est ainsi par exemple que les États-Unis (pourtant assez réticents à l'égard de la « cyber-diligence ») en ont fait un élément fondamental de leur stratégie internationale pour le cyberespace en reconnaissant que, selon le concept de « *Cybersecurity due diligence* »,

tive measures of prevention… » (*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 Recueil des Sentences Arbitrales*, vol. XXIX, p. 130).

(49) Voy. aussi nos développements *infra*.

(50) Affirmant que l'« obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États » était un principe général, la Cour a condamné l'Albanie car elle savait que des mines se trouvaient dans le Détroit, avait les moyens d'agir (surtout notifier aux navires britanniques la présence de ces mines) mais n'avait rien fait pour prévenir le désastre.

(51) Selon l'opinion de la Suisse dans cette affaire : « L'État doit prévenir et punir les actes qui sont dirigés de son territoire contre l'intégrité extérieure et intérieure des États étrangers » (*Annuaire Suisse de Droit International*, 1959, p. 225).

(52) Voy. par ex. G. Guillaume, *Terrorisme et droit international*, RCADI, 1989, III, vol. 215, pp. 390-398 ; ou l'article 9 de la résolution 71984, *International Terrorism*, de l'International Law Association (*Report of the Sixty-First Conference*, Paris, 1984, p. 6), selon lequel : « *A State is legally obliged to exercise due diligence to prevent the commission of acts of international terrorism within its jurisdiction* ».

(53) Le Conseil de sécurité, dans le préambule de la résolution 1373 (2001) du 28 septembre 2001, a ainsi souligné que « chaque État a le devoir de s'abstenir d'organiser et d'encourager des actes de guerre civile ou des actes de terrorisme sur le territoire d'un autre État, d'y aider ou d'y participer, ou de tolérer sur son territoire des activités organisées en vue de perpétrer de tels actes ». Parmi un grand nombre d'affirmations doctrinales, voy. par exemple : F. Dubuisson, « Vers un renforcement des obligations de diligence en matière de lutte contre le terrorisme ? », in K. Bannelier *et al.* (eds), *Le droit international face au terrorisme*, Paris, Pedone, 2002, 141-58 ; J. Kendall, P. Barron, M. Allenbaugh, « The diligence due in the era of globalised terrorism », *The International Lawyer*, 2002, vol. 36, pp. 49 et s. ; R. Barnidge, « State's due diligence obligations with regard to international Non-State terrorist organisations post-11 september 2001 : the heavy burden that States must bear », *Irist Studies in International Affairs*, 2005, vol. 16, 103-125 ; R. Barnidge, *Non-State Actors and Terrorism — Applying the Law of State Responsibility and the Due Diligence Principle*, *op. cit.*

« *States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse* » (54).

f) *Le standard de diligence due dans les travaux du GGE*

L'application de l'obligation de due diligence à la cyber-sécurité est aussi très largement soutenue par la doctrine, y compris par les Manuels de Tallinn 1.0 et 2.0 (55), mais aussi par les travaux du GGE. C'est ainsi que le rapport de 2015 a introduit le concept de « cyber-diligence » non seulement dans la partie « Normes, règles, et principes de comportement responsable des États » comme nous l'avons déjà évoqué mais aussi dans la partie « Applicabilité du droit international à l'utilisation des TIC » qui identifie les règles du droit international positif qui jouent un rôle dans la sécurité du cyberespace. Dans cette partie, le rapport y affirme que les États « devraient veiller à ce que les acteurs non étatiques n'utilisent pas leur territoire pour commettre des faits internationalement illicites à l'aide des technologies de l'information » mais aussi 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 » (56).

L'utilisation du conditionnel dans certaines parties du rapport du GGE ne vise en fait pas à exclure la positivité des obligations de diligence due en matière de cyber-sécurité mais constitue plutôt un compromis politique lié à l'opposition d'un nombre limité d'États et vise à dissiper certaines craintes quant à la nature de l'obligation de due diligence en tant qu'obligation de moyen et non de résultat. Il est à cet égard intéressant de noter la position particulièrement subtile du conseiller juridique du département d'État américain selon laquelle « *voluntary, non binding norms set out standards of expected State behavior that may, in certain circumstances, overlap with standard of behavior that are required as a matter of international law* ». (57)

L'échec du dernier GGE n'est en réalité pas dû à l'intégration du principe de due diligence (qui avait d'ailleurs été accompagnée de développements notables tels que la mise en place de protocoles de notification consensuels). Selon la France d'ailleurs, un accord avait même été trouvé entre les États concernant « l'interdiction faite aux acteurs non étatiques, dont les entreprises privées, de conduire des activités offensives dans le cyberespace pour

(54) The White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, Washington 2011, p. 10, disponible sur https://obamawhitehouse.archives.gov/sites/default/files/rssviewer/international_ strategy _for_cyberspace.pdf.

(55) M.N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, CUP, 2013, 282 p.; M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*

(56) GGE 2015, *op. cit.*, § 28 (e).

(57) B. J. Egan, « International Law and Stability in Cyberspace », Berkeley, 10 novembre 2016 (https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf).

eux-mêmes et pour le compte d'autres acteurs non étatiques » (58). L'échec est plutôt lié à des controverses plus générales sur la façon dont le droit international s'applique au cyberespace, notamment en matière de recours à la force, de droit de légitime défense et de droit international humanitaire (59). Au-delà donc du fait que la due diligence n'est pas la cause de l'échec du GGE (mais plutôt une victime collatérale), il semble que, de façon plus générale, les conséquences de l'échec du GGE ne doivent pas être surestimées sur un plan strictement juridique dans la mesure où les règles que le GGE devaient clarifier existent en droit international indépendamment de l'adoption ou non d'un tel rapport.

B. — *Nature de l'obligation de due diligence*

Nous avons vu que l'obligation qu'a tout État « de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États » s'applique dans le domaine de la cyber-sécurité et aux cyberattaques. Or, comme l'a affirmé Riccardo Pisillo Mazzeschi, « il n'y a pas de règles ou normes sur la due diligence différentes d'un secteur à l'autre du droit international » (60) — il n'y a pas de « fragmentation » de la due diligence en fonction du secteur d'application. Cette affirmation, qui semble aussi être partagée par l'ILA (61), doit toutefois être lue correctement : elle signifie que la *nature* des obligations de vigilance est la même quel que soit le domaine d'application. Ceci n'exclut toutefois pas l'existence de facteurs de variabilité qui font que l'appréciation de la conformité d'un comportement étatique à la diligence requise doit être effectuée au cas par cas en tenant compte de différents paramètres. Pour dissiper donc certains malentendus sur l'application du concept de diligence due dans le cyberespace, il est nécessaire de se pencher sur la nature de la diligence due qui impose une obligation de moyens et non de résultat aux États (1) et qui intègre certains facteurs de variabilité (2).

(58) Secrétariat de la Défense et de la Sécurité Nationale, *Revue Stratégique de cyberdéfense*, *op. cit.*, pp. 84-85.

(59) Les déclarations officielles des États membres du GGE à cet égard sont extrêmement rares. À notre connaissance seuls Cuba et les États-Unis ont publié une déclaration officielle expliquant la nature, selon eux, du désaccord ayant abouti à l'échec du GGE. Voy. à cet égard les déclarations finales du représentant de Cuba (https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf) et du représentant des États-Unis (https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm). Voy. aussi *infra*, Partie II(B).

(60) R. Pisillo Mazzeschi, « Le standard de due diligence comme extension ou limite de la responsabilité internationale », *op. cit.*, p. 6.

(61) Selon ainsi l'ILA, « *the idea that there is a common standard persists* », ILA Study Group on Due Diligence in International Law, first Report, *op. cit.*, p. 4. Comme nous l'avons déjà évoqué, l'ILA va encore plus loin en considérant qu'il existe un « principe général » de due diligence applicable partout.

1) *Une obligation de moyens et non de résultat*

Les obligations de diligence sont traditionnellement conçues comme des obligations de moyens ou dites aussi de « comportement » et non de résultat (a). De ce point de vue, la notion récente et controversée « *unable or unwilling* », qui a séduit le Manuel de Tallinn, crée une importante confusion quant à la nature des obligations de vigilance et s'avère être particulièrement dangereuse (b).

a) *Une obligation de comportement*

Le droit interne est familier de la distinction opérée entre obligations de résultat et obligations de moyens, de comportement, de prudence ou de diligence. Une *obligation de résultat* est une « obligation pour le débiteur de parvenir à un résultat déterminé [...] de telle sorte que la responsabilité du débiteur est engagée sur la seule preuve que le fait n'est pas réalisé, sauf à se justifier, s'il le peut, en prouvant que le dommage vient d'une cause étrangère » (62). L'*obligation de moyens (ou de diligence)*, en revanche, est une « obligation, pour le débiteur, non de parvenir à un résultat déterminé mais d'y appliquer ses soins et ses capacités [...] de telle sorte que la responsabilité du débiteur n'est engagée que si le créancier prouve, de la part de ce débiteur, un manquement à ses devoirs de prudence et de diligence » (63). L'exemple classique d'une obligation de résultat est l'obligation faite au transporteur de conduire le voyageur sain et sauf à destination (en utilisant, si nécessaire, un autre *moyen* de transport que celui initialement prévu). L'exemple type d'une obligation de moyens est l'obligation pour le médecin non pas de guérir son patient (ce qui peut être parfois impossible) mais de le soigner avec science et conscience.

C'est exactement cette distinction qui, malgré quelques interrogations dues à un édifice particulièrement complexe de catégorisation des obligations internationales proposé initialement par le Rapporteur de la CDI Roberto Ago (64), s'est imposée en droit international (65). Quand on parle d'obligations de diligence en droit international, on veut signifier que les États qui ont connaissance (ou ont dû avoir connaissance) d'un risque important d'atteinte aux droits d'un État tiers (ou aux droits d'un individu dans le cadre des obligations positives en matière de droits de l'homme) en raison

(62) G. Cornu, *Vocabulaire juridique*, Paris, Quadrige/PUF, 2001, p. 586.

(63) *Ibid.*

(64) Sur ce point, voy. surtout les analyses de R. Pisillo Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », *op. cit.*, pp. 10-21 ; J. Combacau, « Obligations de résultat et obligations de comportement : quelques questions et pas de réponse », in *Mélanges offerts à Paul Reuter — Le droit international : unité et diversité*, Paris, 1981, pp. 181 et s. ; et P.-M. Dupuy, « Reviewing the Difficulties of Codification : On Ago's Classification of Obligations of Means and Obligation of Result in Relation to State Responsibility », *EJIL*, 1999, pp. 371 et s.

(65) R. Pisillo Mazzeschi, *Responsabilité de l'État pour violation des obligations positives relatives aux droits de l'homme*, *op. cit.*, pp. 283 et s.

d'activités développées sur leur territoire sous leur contrôle ou juridiction, doivent prendre des mesures raisonnables pour prévenir ce risque — sans pour autant pouvoir garantir le résultat. La CDI, à l'instar de certains auteurs anglo-saxons (66), a expliqué que l'obligation de diligence consiste pour un État à adopter ses « *best efforts* » (67) en fonction des circonstances de l'espèce. Toutefois, comme l'a noté Riccardo Pisillo Mazzeschi, « l'expression "*best efforts obligations*" n'est pas très appropriée car elle amène erronément à penser qu'on se trouve à la limite entre obligation juridique et effort politique de bonnes intentions » (68). Il pourrait ainsi être préférable de dire que les États ont l'obligation de « déployer tous les moyens à leur disposition », ou « d'adopter toutes les mesures disponibles », ou « de prendre les mesures raisonnables et appropriées » ou de « faire ce que l'on peut raisonnablement attendre d'eux » au regard des circonstances (69).

Ainsi que l'a souligné la CIJ dans son arrêt de 2007 dans l'*Affaire de l'Application de la Convention pour la prévention et la répression du crime de génocide* :

> « (…) il est clair que l'obligation dont il s'agit est une obligation de comportement et non de résultat, en ce sens que l'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

(66) Voy., par exemple, S. Heathcote, selon qui l'obligation de diligence signifie que les États « *should deploy their best efforts to achieve [the] desired outcome… even if that outcome need not be ensured* » (S. Heathcote, « State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility », in K. Bannelier, T. Christakis, S. Heathcote (eds), *The ICJ and the Evolution of International law: The enduring impact of the Corfu Channel case*, *op. cit.*, p. 308).

(67) Selon la Commission du droit international, « [l']obligation de prévention s'analyse normalement comme une obligation de diligence, imposant aux États de prendre toutes les mesures raisonnables ou nécessaires pour éviter qu'un événement donné ne se produise, mais sans garantir que l'événement ne se produira pas » (*Rapport de la Commission du droit international*, Cinquante-troisième session, 2001, p. 153, § 14).

(68) R. Pisillo Mazzeschi, *Responsabilité de l'État pour violation des obligations positives relatives aux droits de l'homme*, *op. cit.*, p. 284.

(69) Comme la Cour européenne des droits de l'Homme l'a dit, pour engager la responsabilité de l'État il lui faut se convaincre que les autorités de cet État « savaient ou auraient dû 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 […] [I]l suffit au requérant de montrer que les autorités *n'ont pas fait tout ce que l'on pouvait raisonnablement attendre d'elles* pour empêcher la matérialisation d'un risque certain et immédiat pour la vie, dont elles avaient ou auraient dû avoir connaissance » (CEDH, *Osman c. Royaume-Uni*, arrêt du 28 octobre 1998-VIII, § 116).

"*due diligence*", qui appelle une appréciation *in concreto*, revêt une importance cruciale »(70).

À la lumière de ce qui précède, il semble donc impossible d'accepter l'argument avancé par certains auteurs anglo-saxons qui, pour contester l'applicabilité de la diligence due dans le cyberespace, en dénoncent ses dangers pour les États soutenant que leur responsabilité serait engagée chaque fois qu'ils ne seraient pas en mesure *d'empêcher la survenance d'un dommage* subi par un État tiers du fait d'une cyberattaque lancée ou transitant par leur territoire(71). Ces arguments résultent sans doute d'une confusion entre obligations de résultat et obligations de moyens mais ne trouvent nul appui ni dans la pratique générale comme nous l'avons vu, ni dans les travaux du GGE sur la cyber-sécurité qui indiquent, au contraire, que les États ne peuvent agir qu'en fonction de leurs capacités(72). La jurisprudence internationale offre aussi différents exemples où la responsabilité internationale d'un État n'a pas été engagée pour manquement à ses obligations de diligence, soit parce que les conditions posées par les « facteurs de variabilité » (*infra*) n'étaient pas réunies, soit parce que l'État avait pris des mesures raisonnables même si elles se sont révélées insuffisantes (l'*Affaire RDC c. Ouganda* que nous analyserons dans la section suivante est emblématique à cet égard). Cette confusion entre obligations de résultat et obligations de diligence n'est pas d'ailleurs sans rappeler la théorie « *unwilling or unable* », dont le spectre, s'il n'est pas dissipé, pourrait bouleverser profondément la catégorisation des obligations internationales.

b) *Le spectre de la théorie « unwilling or unable »*

La théorie « *unwilling or unable* », que l'on peut traduire par « qui ne veut pas *ou* qui ne peut pas », a été invoquée par les États-Unis en 2014 dans la lutte contre Daesh comme base légale justifiant leurs frappes sur le territoire syrien. Selon la position américaine, cette théorie, en association avec l'article 51 de la Charte, les autoriserait à user de la force armée sur et contre le territoire de la Syrie sans son consentement dans la mesure où la Syrie ne veut

(70) CIJ, *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, § 430.

(71) E. Talbot Jensen, S. Watts, « A cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer », *op. cit.*, p. 1568 (« *If however, an obligation of cyber due diligence is recognized, as the territorial State, State C could* be responsible for failing its duty to stop harm *emanating from its territory. If State A informs State C early of the harm and State C, aware that its cyber infrastructure is being used to harm State A,* does not terminate *the cyber incitements, State C is in breach of its due diligence obligation. State C's breach of due diligence constitutes an independent internationally wrongful act and State A may* [...] *resort to countermeasures against State C* » [nous soulignons]).

(72) Dans l'un des derniers projets de rapport du GGE de 2017, on peut ainsi lire (sous la norme agréée « *States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs* ») la précision selon laquelle les États devraient « *within their capacity, take all reasonable steps, to cause these activities to cease* ».

pas *ou* ne peut pas empêcher des groupes terroristes de lancer des attaques depuis son territoire (73).

Lorsque les États-Unis ont invoqué cette théorie, l'idée n'était pas d'imputer les attaques de ces groupes terroristes à la Syrie pour pouvoir invoquer un droit de légitime défense interétatique tel que prévu par la Charte. En effet, le gouvernement syrien n'était en principe accusé ni de soutenir, ni de contrôler, ni même d'ailleurs de tolérer ou de rester passif à l'égard des activités des groupes terroristes. Au contraire, il les combattait, mais il était clair que, en dépit de ses efforts, il n'était pas capable de les éradiquer. Selon donc le raisonnement américain, le fait que la Syrie était objectivement incapable justifiait qu'un État tiers puisse bombarder son territoire sans son consentement.

Comme on le sait, cette théorie soulève de nombreux problèmes, notamment parce qu'elle n'est soutenue par aucun instrument juridique ni par aucun cas d'espèce (74) et on peut donc se demander dans quelle mesure celle-ci pourrait trouver appui sur le principe de due diligence.

En effet, même si les États-Unis n'ont pas invoqué une violation de l'obligation de diligence, la théorie « *unwilling or unable* » pourrait être conçue comme découlant de l'obligation pour les États de ne pas laisser sciemment leur territoire être utilisé à des fins d'actes contraires au droit d'autres États. Le « *unwilling* » pourrait ainsi renvoyer à la situation où un État ne veut pas, en connaissance de cause, prendre les mesures nécessaires pour prévenir ou faire cesser des attaques terroristes lancées depuis son territoire. Quelles que soient les conséquences attachées à la violation de cette obligation de moyens (75), nous sommes bien ici dans une logique classique de diligence due.

Toutefois, cette théorie semble aussi aller plus loin que l'obligation de due diligence dans la mesure où, même si un État *veut* lutter, prend toutes les mesures raisonnables dont il dispose pour éradiquer de tels groupes mais n'y

(73) Lettre datée du 23 septembre 2014, adressée au Secrétaire général par la Représentante permanente des États-Unis d'Amérique auprès de l'Organisation des Nations Unies, S/2014/695, 23 septembre 2014.

(74) Voy. O. Corten, « The 'Unwilling or Unable' Test: Has it Been and Could it be, Accepted? », *Leiden JIL*, 29, 2016, pp. 777-799.

(75) Si un manquement à l'obligation de diligence constitue incontestablement une violation du droit international, cette violation n'autorise pas pour autant automatiquement (et sans violation de l'article 2, § 4, de la Charte) le recours à la force armée. Voy., à cet égard, l'Appel contre une invocation abusive de la légitime défense pour faire face au défi du terrorisme, signée en septembre 2016 par plus de 300 experts en droit international (http://cdi.ulb.ac.be/wp-content/uploads/2016/06/Contre-une-invocation-abusive-de-la-legitime-defense.pdf). On peut aussi à ce titre remarquer que la situation était à peu près analogue dans l'*Affaire du Détroit de Corfou*. L'*Operation Retail*, à savoir le déminage forcé opéré par le Royaume-Uni, a été considéré comme une violation du droit international et ceci alors que l'Albanie avait elle-même violé le droit international et le principe de diligence due. La Cour n'a pas accepté l'idée de l'existence d'un droit de *self-help* dans ce domaine autorisant le Royaume Uni à opérer un déminage forcé des eaux albanaises.

arrive pas, il peut faire l'objet d'une intervention militaire non consentie. Le « *unable* » semble ainsi exprimer une *obligation de résultat* peu compatible avec l'approche traditionnelle des obligations de diligence comme obligations de moyen.

On se souvient à cet égard que, dans l'*Affaire des activités armées sur le territoire du Congo*, l'Ouganda affirmait, en se fondant notamment sur l'arrêt du *Détroit de Corfou*, qu'il était en état de légitime défense car la République démocratique du Congo (RDC) avait violé son obligation de *vigilance* en laissant des groupes armés conduire des attaques transfrontières. La Cour a parfaitement accepté l'existence d'une telle obligation de *vigilance* dans ce domaine mais elle a par contre refusé de considérer que l'incapacité dans laquelle se trouvait la RDC de mettre fin à ces attaques constituait une violation de cette obligation. Si un État prend des mesures raisonnables en son pouvoir pour empêcher ces attaques mais échoue, il ne peut pas être tenu responsable d'une violation de l'obligation de due diligence, ni d'ailleurs de l'article 2, § 4, de la Charte et les États victimes ne peuvent se fonder sur le droit de légitime défense de l'article 51 (76).

La théorie « *unwilling or unable* » a pourtant été invoquée par les États-Unis pour soutenir leurs frappes contre Daesh en Syrie et quelques États, certes peu nombreux, ont plutôt bien accueilli cette théorie comme d'ailleurs aussi certains auteurs. Toutefois, plus nombreux sont ceux qui n'ont pas souhaité épouser cette théorie, manifestant leur inquiétude à l'égard de ce qu'ils estiment être une remise en cause fondamentale du système de sécurité collective (77). Selon ses détracteurs, la théorie « *unwilling or unable* » serait dangereuse car elle autoriserait un État à lancer une campagne militaire contre le territoire d'un autre État au motif subjectif que l'État en question serait incapable de mettre fin aux activités d'un groupe terroriste.

On pourrait toutefois craindre que cette théorie soit utilisée comme une « super » obligation de due diligence dans le cyberespace. En effet, au cours de la même année 2014, les États-Unis ont fait parvenir au GGE des Nations Unies un rapport concernant notamment l'application du droit international dans le cyberspace. Dans ce rapport, les États-Unis affirment que : « *State facing an imminent or actual attack by a non-State actor in or through cyberspace (…) may act without consent (…) if the territorial State is unwilling or unable to stop or prevent the actual or imminent armed attack launched in or through cyberspace* » (78). Certes, les États-Unis n'ont pas opéré dans ce rapport de lien direct entre la théorie « *unable or unwilling* » et l'obligation

(76) *Activités armées sur le territoire du Congo* (*République démocratique du Congo c. Ouganda*), arrêt du 19 décembre 2005, *CIJ Recueil*, 2005, §§ 297-302.

(77) Pour une illustration récente des positions en faveur et contre cette théorie, voy. les différents articles présentés dans le dossier « Self-Defence Against Non-State Actors : Impulses from the Max Planck Trialogues on the Law of Peace and War », *ZaöRV/HJIL*, vol. 77(1), 2017, pp. 1-95.

(78) Voy. US Department of State, *Digest of United States Practice in International Law*, 2014, p. 735 (https://www.state.gov/s/l/2014/).

de diligence. Toutefois, le Manuel de Tallinn 1.0 publié l'année d'avant et qui, selon ses auteurs, se fonderait sur le droit international coutumier, n'a pas hésité à faire ouvertement ce lien sur la base d'une lecture croisée de la théorie « *unable or unwilling* » et l'obligation de diligence à laquelle renvoie la règle 5 du Manuel. Ainsi, selon le Manuel de Tallinn, « *self-defence against a cyber armed attack (…) is permissible when the territorial State is unable (e.g because of it lacks of technology) or unwilling to take effective actions to repress the relevant elements of the cyber-armed attack. In particular, (…)* States have a duty to ensure their territory is not used for acts contrary to international law (Rule 5) ». (79) Il est vrai que le Manuel de Tallinn est une œuvre doctrinale d'experts indépendants, mais il est vrai aussi que le processus de Tallinn est très ouvertement soutenu par les États-Unis, comme en témoigne notamment le discours du conseiller juridique au département d'État américain H.H. Koh, même s'il affirme ne pas partager toutes les conclusions du Manuel (80). La « juxtaposition » de ces textes, affirmant l'un et l'autre se fonder sur le droit international positif, pourrait donc susciter certaines inquiétudes quant à l'interprétation de l'obligation de diligence en droit positif. À cet égard, le Directeur du Manuel de Tallinn, M. Schmitt, n'a pas hésité à écrire que : « *The relative congruency between the US Government's views, as reflected in the Koh speech, and those of the International Group of Experts* [*of the Tallinn Manual*] *is striking. This confluence of a state's expression of* opinio juris *with a work constituting "the teachings of the most highly qualified publicists of the various nations" significantly enhances the persuasiveness of common conclusions* » (81).

Quoi qu'il en soit, il reste très clair que la due diligence exprime, en droit international, une obligation de moyens et non de résultat. Si un État prend toutes les mesures raisonnables à sa disposition mais est incapable de prévenir ou de faire cesser une activité numérique qui cause des dommages à un État tiers, il ne peut pas être considéré comme ayant violé son obligation de diligence. La théorie « *unwilling or unable* » n'a donc aucune place dans l'interprétation des obligations de diligence des États en matière de cybersécurité et ceci quels que soient par ailleurs les débats entourant cette théorie et ses éventuels autres fondements juridiques. Il convient d'ailleurs de rappeler que la majorité des partisans de cette théorie ont essayé de la lier à l'élément de « nécessité » dans l'exercice de la légitime défense et non pas

(79) M.N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, pp. 60-61. La Règle 5 du Manuel de Tallinn intitulée « *Control of Cyber infrastructure* » est exprimée de la manière suivante : « *A State shall not knowingly allow the cyber infrastructures located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States* » (p. 26).

(80) H.H. Koh, *International Law in Cyberspace*, *op. cit.*, p. 6 (www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf).

(81) M.N. Schmitt, « International Law in Cyberspace: The Koh Speech and the Tallinn Manual Juxtaposed », *Harvard International Law Journal*, vol. 54, 2012, p. 15.

à une interprétation extensive des obligations de diligence des États. Cette conception extensive de la légitime défense a suscité, comme nous l'avons déjà évoqué, la crainte chez certains membres du GGE que la régulation du cyberespace ne soit utilisée par des États puissants comme un fondement juridique les autorisant à recourir unilatéralement à la force en cas de menace ou d'atteinte à la cyber-sécurité résultant de la défaillance de certains États. À cet égard, la déclaration du représentant de Cuba du 23 juin 2017 illustre bien cette controverse et ces craintes (82).

2) *Une obligation ayant une nature objective mais fondée sur des facteurs à contenu variable*

Les obligations de diligence due renvoient à un standard objectif de comportement et non à la démonstration d'une « faute » ou d'une intention délictueuse de l'État (a). Elles font certes appel à certains facteurs « à géométrie variable » mais qui peuvent néanmoins être déterminés par des méthodes et critères rationnels (b).

a) *Une obligation de nature objective (indifférence de l'intention délictueuse de l'État)*

Il est communément accepté que l'obligation de diligence a une nature objective dans le sens où elle fait appel à une appréciation à vocation objective. Il n'est ainsi guère nécessaire de démontrer que l'État avait *l'intention de nuire* à un autre État, il suffit d'établir que l'État n'a rien fait pour que les droits d'un autre État ne soient pas enfreints, alors qu'il savait et qu'il aurait pu agir en ce sens. Comme le souligne Riccardo Pisillo Mazzeschi, « *what counts is not the subjective attitude of fault on the part of the individuals acting as State organs, but the breach of an* objective standard *of conduct by the State* considered as a whole » (83). L'Institut de droit international avait

(82) « *We regret that it was not possible to reach a consensus in this Group to submit substantive recommendations to the UN General Assembly. I must register our serious concern over the pretension of some, reflected in paragraph 34 of the draft final report, to convert cyberspace into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs. We consider unacceptable the formulations contained in the draft, aimed to establish equivalence between the malicious use of ICTs and the concept of "armed attack" as provided for in Article 51 of the Charter, which attempts to justify the alleged applicability in this context of the right to self-defense. To establish as a precedent this dangerous reinterpretation of the norms of international law and the Charter of the United Nations would be a fatal blow to the collective security and peacekeeping architecture established in the Charter of the United Nations. The "Law of the jungle" cannot be imposed, in which the interest of the most powerful States would always prevail to the detriment of the most vulnerable* » (Declaration by M. Rodriguez, Representative of Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, New York, 23 juin 2017, *op. cit.*).

(83) R. Pisillo Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », *op. cit.*, p. 42.

d'ailleurs déjà indiqué de façon indirecte ce caractère « objectif » de la due diligence lors de sa session de Lausanne de 1927 en déclarant que « [l]'État n'est responsable, en ce qui concerne les faits dommageables commis par des particuliers, que lorsque le dommage résulte du fait qu'il aurait omis de prendre les mesures auxquelles, d'après les circonstances, il convenait normalement de recourir pour prévenir ou réprimer de tels faits » (84). Les obligations de diligence renvoient donc « à un standard objectif de comportement, et non à la démonstration, au demeurant fort hypothétique, d'une intention délictueuse » de l'État (85). Ce standard est un standard international (« due diligence ») et non national (*diligentia quam in suis*), comme l'a bien montré Riccardo Pisillo Mazzeschi (86) ou encore l'ILA (87).

b) *Une obligation à texture ouverte fondée sur des facteurs à contenu variable*

L'affirmation selon laquelle les obligations de diligence renvoient à un standard objectif de comportement n'est pas remise en cause par le fait que le concept de *diligence due* appelle à une appréciation du caractère « raisonnable » du comportement étatique, évalué à la lumière d'un certain nombre de facteurs à contenu variable, que nous analyserons en détail dans la partie II.

Il est vrai que les notions de « raisonnable », de « due diligence » et les « facteurs de variabilité » de cette dernière (*infra*) semblent relever de ce que Herbert Hart avait qualifié de « *open texture of legal language* » ou de « *fringe of vagueness in legal rules* » (88). Selon Hart, à côté des normes claires et précises (« *determinate rules* ») qui ne nécessitent aucune intervention ultérieure, il existe dans tous les ordres juridiques des normes imprécises, vagues et dont la « texture » reste très ouverte. Ces dernières doivent faire l'objet d'une application au cas par cas et il appartient aux organes d'application du droit, en commençant par les juridictions, de préciser progressivement le contenu de ces normes. Ces normes dont la « texture est ouverte » ne vont pas sans rappeler ce que l'on a appelé opportunément dans la doctrine juridique francophone

(84) IDI, Responsabilité internationale des États à raison des dommages causés sur leur territoire à la personne et aux biens des étrangers (article 3), Session de Lausanne, 1927, *Annuaire de l'IDI*, 1927, vol. 33-III, pp. 330-335.

(85) O. Corten, *Le droit contre la guerre*, 2e éd., Paris, Pedone, 2014, p. 317. Voy. aussi O. Corten, « La complicité dans le droit de la responsabilité internationale : un concept inutile ? », *AFDI*, 2011, pp. 76 et s.

(86) R. Pisillo Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », *op. cit.*, pp. 41 et s.

(87) Selon ainsi l'ILA, « *Even if the content of due diligence is very general, it is clear that its requirements are defined at the level of international, rather than national, law* » (ILA Study Group on Due Diligence in International Law, Second Report, *op. cit.*, p. 6).

(88) Voy. H. Hart, *The Concept of Law*, Oxford, Clarendon Press, 1961, p. 132. Selon ce dernier, « *The open texture of law means that there are, indeed, areas of conduct where much must be left to be developed by courts or officials striking a balance, in the light of circumstances, between competing interests which vary in weight from case to case* ».

les « notions à contenu variable », c'est-à-dire des notions « dont la dénomination, le signifiant, restent constants, mais dont le domaine, le champ, le signifié sont mouvants, évoluent, plus spécialement en fonction de facteurs spatio-temporels » (89). Comme l'a résumé Chaim Perelman :

> « Tenant compte de la variété infinie des circonstances, du fait qu'il n'est pas capable de tout prévoir et de tout régler avec précision, admettant que des règles rigides s'appliquent malaisément à des situations changeantes, le législateur peut délibérément introduire dans le texte de la loi des notions à contenu variable, flou, indéterminé, telles que [...] le *raisonnable*, [...], en laissant au juge le soin de les préciser dans chaque cas d'espèce » (90).

Certains auteurs, qui essaient de repousser l'applicabilité du standard de diligence en matière de cyber-sécurité, se sont parfois référés à « l'indétermination normative » de la due diligence en droit international pour suggérer qu'elle ne pourrait être appliquée au cyberespace que si elle devenait beaucoup plus précise (91). Il nous semble toutefois qu'une telle proposition méconnaît la nature même de la diligence due qui est par définition un concept flexible, élastique et relatif. Comme l'a excellemment montré Riccardo Pisillo Mazzeschi, le degré de diligence qu'un État doit observer dépend largement des *circonstances particulières* de chaque cas d'espèce (92). Essayer de tout « définir », « déterminer » et « préciser » d'avance avant d'appliquer des obligations de diligence due dans un système juridique serait détruire la flexibilité inhérente à ce concept et sa force. Les juridictions internationales qui ont appliqué pour la toute première fois le concept dans des domaines entièrement nouveaux (la neutralité en 1872, l'environnement en 1941, la protection de la sécurité des États tiers en 1949, les droits de l'homme plus tard...) n'ont pas été arrêtées par « l'indéterminisme normatif » des obligations de diligence qui, par ailleurs, leur confèrent un pouvoir d'appréciation important.

Ainsi que l'a par ailleurs bien montré Olivier Corten, des notions comme le « raisonnable » qui sont centrales dans l'appréciation du respect des obligations de diligence et qui peuvent, *prima facie*, donner l'impression d'un subjectivisme débridé, sont en réalité susceptibles de faire l'objet d'une détermination par des méthodes et critères rationnels. L'étude minutieuse de plusieurs centaines de décisions rendues par des juridictions internationales l'amène effectivement à considérer que, en pratique, la notion du « raison-

(89) R. Legros, « Les notions à contenu variable en droit pénal », in C. Perelman, R. Vander Elst (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 1984, p. 21. Voy. A. Ouedraogo, « La due diligence en droit international : de la règle de la neutralité au principe général », *op. cit.*, p. 644.

(90) C. Perelman, « Les notions à contenu variable en droit, essai de synthèse », in C. Perelman, R. Vander Elst (dir.), *Les notions à contenu variable en droit*, *op. cit.*, p. 365.

(91) N. Tsagourias, « On the virtues and limitations of cyber due diligence », *op. cit.*

(92) R. Pisillo Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », *op. cit.*, p. 44. L'auteur va jusqu'à ajouter que « *In this sense, the flexibility of the due diligence concept does not allow more precise rules* ».

nable » est souvent utilisée pour sanctionner un écart par rapport à un standard général de comportement par le biais de notions comme la nécessité et la proportionnalité (93). Sera « déraisonnable » un comportement qu'un État ne pourra justifier au regard d'objectifs admis comme légitimes, en établissant un lien de causalité suffisant entre ceux-ci et celui-là (94). Mais, au-delà de toute une série de critères d'application, l'appréciation du caractère « raisonnable » d'un comportement va dépendre nécessairement des circonstances de chaque cas d'espèce, ce que la CIJ a appelé, comme nous l'avons vu, la nécessité d'une « appréciation *in concreto* ». Pour pouvoir procéder à cette appréciation, le juge va s'appuyer, à chaque fois, sur une série de « facteurs de variabilité » dont nous allons essayer maintenant d'esquisser les contours d'application dans le cyberespace.

II. — Les défis de l'application de l'obligation de due diligence dans le cyberspace

La due diligence n'est pas une norme indéterminée mais une obligation objective de comportement qui implique certains « facteurs de variabilité ». Cela signifie principalement, comme l'a souligné la Cour internationale de justice dans l'*Affaire de l'Application de la convention pour la prévention et la répression du crime de génocide*, que le manquement à l'obligation de diligence ne doit pas s'apprécier de façon abstraite et que « plusieurs paramètres entrent en ligne de compte quand il s'agit d'apprécier si un État s'est correctement acquitté de l'obligation en cause » (95). Il convient donc d'identifier ces paramètres, ces « facteurs de variabilité » qui donnent à l'obligation de due diligence la flexibilité et la plasticité nécessaires à son effectivité en s'interrogeant sur les spécificités de leur application et de leur interprétation dans le cyberespace (A). Cette analyse nous permettra ainsi de mieux cerner les implications de la due diligence tant en ce qui concerne les obligations des États que leur responsabilité dans le cyberespace (B).

A. — *Les facteurs de variabilité*

Examinons successivement les quatre principaux facteurs de variabilité qui permettent, dans chaque cas d'espèce, de déterminer comment s'appliquent les obligations de diligence.

(93) Voy., par exemple, O. Corten, *L'utilisation du « raisonnable » par le juge international*, Bruxelles, Bruylant, 1997, pp. 520-525 et 594-601.

(94) Voy. « Raisonnable », in J. Salmon (dir.), *Dictionnaire de droit international public*, *op. cit.*, pp. 923-924 et O. Corten, « Motif légitime et lien de causalité suffisant : un modèle d'interprétation rationnel du raisonnable », *AFDI*, 1998, pp. 187-208.

(95) *Application de la convention pour la prévention et la répression du crime de génocide*, préc., p. 43, § 430.

1) *La connaissance*

La connaissance est un élément clé sans lequel il ne peut y avoir d'obligation de diligence due qui mérite toutefois plusieurs observations.

a) *Connaissance et « raisonnable »*

Alors que la connaissance est un élément essentiel de l'obligation de due diligence, très peu d'études lui ont été consacrées. Dans l'*Affaire du Détroit de Corfou*, la Cour a pourtant bien souligné que les États ont l'obligation de ne pas laisser sciemment (« *knowingly* » dans la version anglaise) leur territoire être utilisé à des fins contraires aux droits d'autres États. C'est parce que le mouillage du champ de mines « n'a[vait] pas pu échapper à la connaissance du Gouvernement albanais » (96) que la Cour a finalement jugé que l'Albanie avait violé ses obligations en ne prenant aucune mesure pour prévenir l'accident. De la même manière, dans l'*Affaires des otages à Téhéran*, la Cour internationale de justice a engagé la responsabilité de l'Iran après avoir conclu que les autorité iraniennes « b. étaient pleinement conscientes, du fait des appels à 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 » (97). Les obligations de prévention et de cessation sont ainsi étroitement liées à la connaissance par les États de la situation.

Dans l'espace numérique, l'élément de connaissance peut toutefois soulever certaines interrogations et être source d'inquiétudes (98). En effet, la rapidité et la furtivité des activités qui s'y développent mais aussi leur caractère essentiellement privé, rendent difficile cette connaissance, *a fortiori* lorsque ces activités ne font que transiter par les infrastructures numériques d'un État. Ces craintes peuvent par ailleurs être alimentées par des positions relativement exigeantes concernant la connaissance comme par exemple celle du juge Alvarez dans son opinion individuelle jointe à l'arrêt du *Détroit de Corfou* où il estime que la connaissance « ce n'est pas une présomption, ce n'est pas une hypothèse : c'est la conséquence de la souveraineté » et que si un État « prétend qu'il n'a pas eu connaissance de ces actes, notamment par suite de circonstances que sa vigilance ne pouvait déceler (…) il doit le prouver » (99).

En réalité toutefois, l'obligation de due diligence n'implique pas que les États sachent tout ce qui se passe sur leur territoire ou sous leur contrôle. 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

(96) *Affaire du Détroit de Corfou*, préc., p. 22.

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

(98) Voy. N. Tsagourias, « On the virtues and limitations of cyber due diligence », *op. cit.*

(99) Opinion individuelle du juge A. Alvarez, *Affaire du Détroit de Corfou*, préc., p. 44.

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 » (100). Comme nous l'avons déjà évoqué, toutes les juridictions internationales et tous les organes internationaux qui ont eu à interpréter et à appliquer le principe de due diligence affirment que le degré de vigilance attendu est celui « d'un bon gouvernement », 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 » aux États (101).

Le fait que l'obligation de diligence n'implique pas des États une connaissance et un contrôle territorial absolu dans le monde physique est évidemment tout aussi valable dans le monde numérique. Il semblerait ainsi raisonnable que l'on puisse estimer qu'un État peut sans doute avoir des difficultés à connaître les activités qui se développent dans les infrastructures numériques privées même lorsqu'elles se développent sur son territoire.

b) *Connaissance constructive*

Cette connaissance peut donc varier d'un État à l'autre en fonction des circonstances de l'espèce. Peut-on toutefois admettre la notion de « connaissance constructive » ? Peut-on, dans certaines circonstances, considérer qu'un État « devait savoir », « aurait dû savoir », voire même « devrait chercher à savoir » ce qui se passe dans les infrastructures numériques ? Le Manuel de Tallinn 1.0 s'est montré hésitant à cet égard, considérant que le Groupe d'experts « *could not achieve consensus as whether this rule applies if the respective State has only constructive ("should have known") knowledge… if it fails to use due care* » (102).

Pourtant, la jurisprudence internationale donne des indications très claires à cet égard. La Cour internationale de justice dans l'*Affaire du Détroit de Corfou* a ainsi affirmé qu'« un État, sur le territoire duquel s'est produit un acte contraire au droit international, peut être invité à s'en expliquer (…) 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 » (103).

De façon encore plus explicite dans l'*Affaire Application de la Convention pour la prévention et la répression du crime de génocide*, la Cour internationale de justice a estimé qu'« un État peut être considéré comme ayant violé son

(100) *Affaire du Détroit de Corfou*, arrêt du 4 avril 1949, préc., p. 18.

(101) CEDH, *Affaire Osman c. Royaume-Uni*, préc., § 116.

(102) M.N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, *op. cit.*, p. 28, § 11.

(103) *Affaire du Détroit de Corfou*, préc., p. 18.

obligation de prévention même s'il n'avait pas acquis la certitude, au moment où il aurait dû agir mais s'en est abstenu, qu'un génocide était sur le point, ou en train, d'être commis : il suffit, pour que sa responsabilité internationale soit susceptible d'être engagée à ce titre, qu'il ait eu connaissance, *ou eût dû normalement avoir connaissance*, de l'existence d'un risque sérieux de commission d'actes de génocide » (104). En 2017, le Manuel de Tallinn 2.0 est d'ailleurs revenu sur cette question pour finalement reconnaître que la connaissance constructive faisait partie de l'obligation de diligence (105).

Il est vrai que cette connaissance constructive peut ensuite être difficile à déduire *in concreto*. Dans l'*Affaire du Détroit de Corfou*, la Cour a ainsi estimé que l'Albanie ne pouvait pas ne pas savoir car l'Albanie « n'a pas cessé d'exercer une vigilance très attentive sur les eaux du Détroit » (106), voire même « d'exercer une surveillance jalouse » (107). De même pourrait-on estimer que les États qui développent une surveillance active de leurs infrastructures numériques devraient connaître certains actes malveillants ou attaques qui sont lancées depuis leurs infrastructures numériques. Mais il ne s'agit évidemment que d'une supposition qui devrait être corroborée par d'autres éléments.

c) *Connaissance et notification*

Pourrait-on cependant considérer qu'un État ne peut pas ne pas savoir lorsqu'il a été informé par des tiers que des activités malveillantes ou des cyber-attaques sont lancées depuis son territoire, ses infrastructures ou y transitent ? Dans le cyberespace, la notification peut en effet constituer un moyen intéressant pour porter à la connaissance d'un État une cyberattaque lancée ou transitant par son territoire alors qu'il l'ignore. Ce processus de notification peut toutefois soulever certaines interrogations et appeler des précisions. Ceux qui notifient, à savoir le plus souvent les États directement victimes des cyber-attaques, doivent-ils, par exemple, apporter certains éléments permettant d'accréditer cette notification ? Pour garantir cette notification ne devrait-on pas confier cette mission à des organismes indépendants ? Il s'agit là de questions importantes qui ont été débattues au sein du GGE des Nations Unies et pour lesquelles des propositions ont été faites mais qui n'ont finalement pas pu adopter faute de consensus, comme on le sait, lors de l'adoption du rapport final (108).

(104) *Application de la Convention pour la prévention et la répression du crime de génocide*, préc., § 432.

(105) M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, p. 41.

(106) *Affaire du Détroit de Corfou*, préc., p. 18.

(107) *Ibid.*, p. 19.

(108) Parmi les dernières versions du rapport final, on peut ainsi lire sous la norme agréée de 2015 « *States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs* », les précisions suivantes destinées à aider les États à mettre en œuvre cette norme : « — *An*

d) *Connaissance, surveillance diligente et droits de l'homme*

Quoi qu'il en soit, si dans certains cas il est sans doute possible de considérer qu'un État « ne peut pas ne pas avoir su », notamment, comme l'a dit la Cour, lorsque l'État exerce une « étroite surveillance » (109) pendant la période des actes en question, doit-on aller plus loin et considérer que l'obligation de diligence implique aussi de la part des États au nom de leurs « *best efforts* » une obligation de chercher à acquérir cette connaissance et donc une obligation de surveillance ? Les États, au titre de l'obligation de diligence, doivent-il surveiller les activités qui se développent sur leur territoire ou sous leur contrôle ? Ont-ils l'obligation de surveiller les infrastructures numériques ? Le Manuel de Tallinn 2.0 a répondu à cette question par la négative mais en esquivant un peu le problème puisqu'il a estimé que l'obligation de diligence n'impliquait pas une obligation de prendre des mesures préventives et donc ne pouvait impliquer une obligation de contrôle (110). En réalité (voy. nos développements *infra*), la prévention est au cœur de l'obligation de diligence et la question de la surveillance ne peut ainsi être esquivée.

Dans son opinion individuelle jointe à l'arrêt du *Détroit de Corfou*, le juge Alvarez a affirmé que : « Tout État est tenu d'exercer une surveillance diligente sur son territoire » (111). La relation étroite entre connaissance et surveillance au titre de l'obligation de diligence a aussi été abordée par le juge international dans d'autres affaires, notamment en relation avec la protection internationale des droits de l'homme et la protection de l'environnement. Dans l'*Affaire Usines de pâte à papier sur le fleuve Uruguay*, la Cour internationale de justice a 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 » (112).

Cette affirmation et cette jurisprudence appellent toutefois certaines remarques. En effet, si l'on considère que l'obligation de diligence est une obligation de moyens et non de résultat, il faut sans doute en déduire que les moyens sont en principe laissés à l'appréciation des États : on ne saurait imposer aux États des obligations spécifiques de surveillance sans glisser vers une obligation de résultat. Par ailleurs, cette surveillance peut être modu-

official notification from one State to another State should be regarded as providing the notified State with actual knowledge of the alleged activity. (…) — *The notified State should acknowledge receipt of the request via the relevant national point of contact; If the States knows the malicious activity is transiting through its territory and is able to identify the State from which it is originating, it may choose to notify that States* (…). *Since all States do not yet have the national structures and mechanisms in place to send or respond to notifications* (…) *the Group recommends that States* (…) *encourage international and regional organizations to consider facilitating the development of such tools and measures*».

(109) *Affaire du Détroit de Corfou*, préc., p. 19.

(110) M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, pp. 41-42.

(111) Opinion individuelle de M. A. Alvarez, préc., p. 44.

(112) *Usines de pâte à papier sur le fleuve Uruguay* (*Argentine c. Uruguay*), arrêt du 20 février 2010, *Recueil CIJ*, 2010, § 197.

lée en fonction de certains paramètres, comme par exemple les risques que comporte une activité donnée et la capacité des États. Ainsi que le soulignait le juge Alvarez, la « surveillance dépend des moyens dont dispose chaque État » (113).

Si les États doivent sans doute exercer un contrôle sur les activités qui se développent sur leur territoire, il convient toutefois de s'interroger sur l'articulation entre les mesures de *surveillance* que les États pourraient adopter dans le cadre de leur obligation de due diligence et d'autres obligations internationales, notamment en matière de protection des droits de l'homme. Au nom de l'obligation de diligence n'y a-t-il pas un risque que les États développent des mesures de *surveillance* portant atteinte au droit à la vie privée et à la protection des données personnelles (114) ? En réalité, il va de soi que l'obligation de diligence ne peut servir de cheval de Troie pour éroder les libertés fondamentales. Il convient en effet de rappeler que la Cour internationale de justice dans l'*Affaire Application de la Convention pour la prévention et la répression du crime de génocide* a souligné que « chaque État ne peut déployer son action que dans les limites de ce que lui permet la légalité internationale » (115).

Dans le cyberespace, il semble d'ailleurs exister un consensus concernant le respect par les États de leurs obligations en matière de protection des droits de l'homme, comme en témoignent les nombreuses déclarations adoptées dans différents fora (116) et les rapports successifs du GGE des Nations Unies. Dans le rapport de 2013, le GGE affirme ainsi que : « Les actions entreprises

(113) Opinion individuelle de M. A. Alvarez, préc., p. 44.

(114) Voy. à cet égard le discours de B. J. Egan, « International Law and Stability in Cyberspace », *op. cit.*, qui souligne que « *Some States invoke the concept of State sovereignty as a justification for excessive regulation of online content, includig censorship and access restrictions, often undertaken in the name of counterterrorism or countering violent extremism* ».

(115) *Application de la convention pour la prévention et la répression du crime de génocide*, préc., § 430.

(116) Voy., par exemple, « Chair's Statment », Global Conference on Cyberspace 2015, 16-17 avril 2015, La Haye (https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf) ; Déclaration du G7 de Lucca du 11 avril 2017 (« *We also reaffirm that the same rights that people have offline must also be protected online and reaffirm the applicability of international human rights law in cyberspace, including the UN Charter, customary international law and relevant treaties* »), *G7 Declaration on Responsible States Behavior in Cyberspace*, Lucca, 11 avril 2017, http://securityaffairs.co/wordpress/57932/cyber-warfare-2/g7-declaration-responsible-states-behavior-cyberspace.html ; Déclaration du G7 de Ise-Ishma, (« *We strongly support an accessible, open, interoperable, reliable and secure cyberspace as one essential foundation for economic growth and prosperity. This also enhances the common values of the G7, such as freedom, democracy and respect for privacy and human rights* »), *G7 Ise-Shima Leaders' Declaration — G7 Ise-Shima Summit*, 26-27 May 2016, (http://www.mofa.go.jp/files/000160266.pdf) ; Déclaration du G20 de Hambourg du 7 juillet 2017, *Leaders' Statement on Countering Terrorism*, http://europa.eu/rapid/press-release_STATEMENT-17-1955_en.htm ; voy. aussi le préambule de l'*Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on cooperation in the Field of International Information Security* du 16 juin 2009 ou encore le *Code de conduite international pour la sécurité de l'information* (Annexe à la lettre datée du 9 janvier 2015 adressée au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie,

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 »(117) et dans le rapport de 2015, les membres du GGE rappellent cette exigence 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 »(118).

L'obligation de diligence s'inscrit ainsi dans le cadre de la légalité internationale et n'autorise donc pas les États à l'invoquer pour adopter des mesures qui seraient contraires à leurs engagements conventionnels ou coutumiers en matière de protection des droits de l'homme.

2) *La capacité*

Le standard de due diligence nécessite une prise en compte des capacités et pouvoirs des États — ce qui ne met pas pour autant en cause l'unicité du régime juridique.

a) *Une diligence proportionnée aux moyens ?*

Tous les États ne disposent pas des mêmes capacités pour prévenir les utilisations malveillantes des infrastructures numériques situées sur leur territoire, sous leur juridiction ou sous leur contrôle. Dans son rapport de 2015, le GGE souligne ainsi que « certains États ne disposent peut-être pas de capacités financières suffisantes pour protéger leurs réseaux informatiques »

du Kazakhstan, du Kirghizistan, de l'Ouzbékistan et du Tadjikistan auprès de l'Organisation des Nations Unies), A/69/723, 13 janvier 2015.

(117) 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 (ci-après GGE 2013).

(118) GGE 2015, *op. cit.*, § 13 (e). La résolution *Le droit à la vie privée à l'ère du numérique* (Res. A/68/167, 18 décembre 2013) exprime en effet bien les attentes dans ce cadre. Cette résolution invite les États à :« b) À prendre des mesures pour faire cesser les violations de ces droits et à créer des conditions qui permettent de les prévenir, notamment en veillant à ce que la législation nationale applicable soit conforme aux obligations que leur impose le droit international des droits de l'homme ; c) À revoir leurs procédures, leurs pratiques et leur législation relatives à la surveillance et à l'interception des communications, et à la collecte de données personnelles, notamment à grande échelle, afin de défendre le droit à la vie privée en veillant à respecter pleinement toutes leurs obligations au regard du droit international ; d) À créer des mécanismes nationaux de contrôle indépendants efficaces qui puissent assurer la transparence de la surveillance et de l'interception des communications et de la collecte de données personnelles qu'ils effectuent, le cas échéant, et veiller à ce qu'ils en répondent, ou à les maintenir en place s'ils existent déjà ».

et que ce manque de capacité non seulement peut les rendre vulnérables mais peut aussi faire d'eux « sans qu'il(s) le sache(nt), un refuge pour des individus malintentionnés » (119). Les différences de capacités entre les États, tant financières que technologiques, sont, il est vrai, particulièrement criantes dans l'espace numérique à tel point que l'on peut parler d'une véritable fracture numérique entre les pays développés et les pays en développement, notamment les pays les moins avancés (120). Cette situation peut être source d'incertitude pour les États qui connaissent un véritable déficit d'expertise et de moyens dans le numérique et qui, de ce fait, pourraient craindre que l'obligation de due diligence leur impose un fardeau trop lourd et les expose trop facilement aux réactions d'États tiers.

Cette préoccupation, quoi que légitime, ne doit toutefois pas être surestimée. En effet, la capacité est un facteur de variabilité largement admis par le juge international lorsqu'il interprète et applique l'obligation de diligence. Dans l'*Affaire de l'Alabama* déjà, les États-Unis avaient défini la due diligence comme : « Une diligence proportionnée à l'importance du sujet, à la dignité et à la force du pouvoir qui l'exerce » (121). Dans l'*Affaire Application de la Convention pour la prévention et la répression du crime de génocide*, la Cour internationale de justice a aussi estimé que le premier paramètre qui permet de déterminer si un État s'est acquitté de son obligation de due diligence est « évidemment la capacité, qui varie grandement d'un État à l'autre » (122).

b) *Critères de capacité*

Plusieurs critères peuvent être retenus pour évaluer la capacité d'un État à l'égard de ses obligations de diligence dans l'espace numérique. Dans ses travaux sur la prévention des dommages transfrontières résultant d'activités dangereuses, la Commission du droit international des Nations Unies a ainsi 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 » (123). La Commission explique ainsi 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

(119) GGE 2015, A/70/174, 22 juillet 2015, § 19.

(120) Voy. à cet égard, Conférence des Nations Unies sur le Commerce et le Développement, *Déclaration ministérielle du Groupe des 77 et de la Chine à la quatorzième session de la Conférence*, TD/507, 19 juillet 2016.

(121) *Affaire de l'Alabama*, Sentence de 1872, RAI, Paris, Pedone, 1923, t. II, pp. 814-815.

(122) *Application de la convention pour la prévention et la répression du crime de génocide*, préc., § 430.

(123) 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, nº 2, 2001, Article 3, commentaire § 13, p. 424.

très élaborés est différent de celui attendu d'États moins bien lotis »(124). Il ne s'agit évidemment là que d'exemples et d'autres critères pourraient sans doute être pris en compte dans le cyberspace, notamment les connaissances scientifiques et les capacités technologiques des États.

c) *Asymétrie des moyens mais unicité du standard*

Une question importante qui demeure toutefois est de savoir, pour reprendre les mots du Professeur Riccardo Pissilo Mazzeschi, si le « standard de la due diligence peut être plus bas pour les États en voie de développement ou pour les États qui possèdent des capacités limités »(125) ? C'est ce que semble suggérer T. Koivurova selon qui, « *Due diligence does not require similar measures from all States, as lack of economic and technological capacity may mitigate the attendant obligations for developing countries* »(126). Pourrait-on alors emprunter au droit international de l'environnement la notion de « responsabilité commune mais différenciée » pour désigner ce facteur de variabilité relatif aux capacités des États dans l'espace numérique ? L'obligation serait différenciée dans la mesure où les États ont des capacités différentes, mais elle serait commune car, comme l'a dit le GGE dans son rapport de 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 »(127). Si l'analogie avec la notion de « responsabilité commune mais différenciée » du droit international de l'environnement est sans doute intéressante pour indiquer les différences de capacité tout en soulignant l'intérêt de l'ensemble de la communauté internationale à l'application de l'obligation de due diligence, elle doit néanmoins être précisée. Il ne s'agit pas en effet, comme semble le suggérer T. Koivurova, de reconnaître l'existence de deux ou plusieurs régimes de due diligence comportant des obligations distinctes en fonction des capacités des États. Ainsi que l'a démontré R. Pissilo Mazzeschi l'obligation de due diligence est « un standard international »(128) et la capacité des États n'est qu'un facteur de variabilité qui permet l'application de la due diligence à des situations différentes. Par ailleurs, il convient de rappeler que, quelles que soient ces inégalités en termes de capacité, les États sont souverains et, comme l'a justement souligné la CDI, « une certaine vigilance est censée être exercée dans l'utilisation des

(124) *Ibid.*, § 17, pp. 425-426.

(125) R. Pisillo Mazzeschi, « Le standard de due diligence comme extension ou limite de la responsabilité internationale », *op. cit.*

(126) T. Koivurova, « Due Diligence », *op. cit.*, § 19.

(127) GGE 2013, *op. cit.*, § 10.

(128) R. Pisillo Mazzeschi, « Le standard de due diligence comme extension ou limite de la responsabilité internationale », *op. cit.*

infrastructures et la surveillance des activités dangereuses sur le territoire de l'État, ce qui est un attribut naturel de tout gouvernement »(129).

3) *Le risque*

Dans son projet d'articles sur la prévention des dommages transfrontières résultant d'activités dangereuses, la CDI note que : « Le degré de diligence par rapport auquel le comportement de l'État d'origine devrait être apprécié est celui qui est généralement considéré comme approprié et proportionné au degré de risque de dommages transfrontières dans le cas dont il s'agit. Par exemple, les activités qui peuvent être considérées comme comportant un risque exceptionnellement élevé exigent de la part de l'État qu'il mette beaucoup plus de soin à élaborer les principes d'action et beaucoup plus de vigueur à les appliquer »(130). Cette variabilité dans l'obligation de diligence en fonction de l'importance du risque(131) semble aussi avoir été admise par le juge international. En 2011, dans son avis consultatif sur les *Responsabilités et obligations des États dans le cadre d'activités menées dans la Zone*, le tribunal du droit de la mer a ainsi estimé que « [c]ette notion peut également changer en fonction des risques encourus par l'activité »(132) et que « [l]e niveau de diligence requise doit être plus rigoureux pour les activités les plus risquées »(133).

Le développement spectaculaire des actes de malveillance dans l'espace numérique et leur impact sur l'économie et la sécurité mondiales placent peut-être les activités numériques parmi les activités à haut risque(134). Pourrait-on toutefois aller jusqu'à considérer que, au regard de l'importance de ce risque, les États doivent aussi respecter certaines obligations spécifiques ? Dans l'*Affaire Usines de pâte à papier sur le fleuve Uruguay*, la Cour a estimé que l'étude d'impact faisait partie de l'obligation de diligence. Selon elle, « on ne pourrait considérer qu'une partie s'est acquittée de son obligation de diligence, et du devoir de vigilance et de prévention que cette obligation implique, dès lors que, prévoyant de réaliser un ouvrage suffisamment important pour affecter le régime du fleuve ou la qualité de ses eaux, elle n'aurait pas procédé à une évaluation de l'impact sur l'environnement permettant

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

(130) *Ibid.*, § 11, p. 424.

(131) Le risque étant défini par la CDI comme « la probabilité qu'un accident se produise » (*ibid.*, p. 416).

(132) Responsabilités et obligations des États dans le cadre d'activités menées dans la Zone, avis consultatif, 1er février 2011, *TIDM Recueil*, 2011, § 117.

(133) *Ibid.*

(134) Selon ainsi le Groupe d'experts des Nations Unies, « Le risque que les technologies de l'information et des communications soient utilisées à des fins terroristes (…) notamment contre des systèmes qui utilisent ces technologies ou contre des infrastructures qui en dépendent augmente. Si l'on ne s'attaque pas à ce problème, il pourrait menacer la paix et la sécurité internationales » (GGE 2015, *op. cit.*, § 6).

d'apprécier les effets éventuels de son projet »(135). Il convient toutefois d'être prudent à l'égard d'une telle généralisation et de son application dans le cyberespace. En effet, l'obligation d'étude d'impact pourrait être perçue comme une obligation de résultat et nécessiter donc d'être prévue dans les règles primaires(136).

4) *Le dommage*

Tout risque de dommage n'est pas forcément couvert par l'obligation de diligence, le dommage doit en effet atteindre un certain seuil de gravité(137) et c'est d'ailleurs l'effet combiné du risque et du dommage qui, selon la CDI, doit permettre d'évaluer le degré de vigilance que les États doivent apporter à une activité donnée(138). Toutefois, force est de constater l'incertitude qui entoure le seuil de gravité du dommage tant la pratique semble fluctuante pour qualifier le dommage(139). Le terme « significatif » semble toutefois recueillir un certain consensus, il a été retenu par la CDI dans l'article 1er du projet sur la prévention des dommages transfrontières résultant d'activités dangereuses(140) ainsi que dans différents travaux consacrés à la due diligence(141) et jugements(142). Il n'en demeure pas moins que le terme « significatif » n'est lui-même pas sans ambiguïté, comme l'a d'ailleurs reconnu la

(135) *Usines de pâte à papier sur le fleuve Uruguay*, préc., § 204.

(136) Il convient toutefois de relever que la CDI, sans parler d'étude d'impact, estime toutefois que l'obligation de prévention prévue à l'article 3 « ne saurait viser les seules activités déjà dûment réputées comporter un tel risque. Elle s'entend aussi de l'obligation de prendre des mesures appropriées pour déterminer les activités qui comportent un tel risque, et cette obligation est de caractère continu » (CDI, Projet d'articles sur la prévention des dommages transfrontières résultant d'activités dangereuses et commentaires y relatifs, *op. cit.*, § 5, p. 421).

(137) CDI, Projet d'articles sur la prévention des dommages transfrontières résultant d'activités dangereuses et commentaires y relatifs, *op. cit.*, pp. 23 et s.

(138) Selon ainsi la CDI, « Aux fins des présents articles, l'expression "risque de causer un dommage transfrontière significatif" renvoie à l'effet combiné de la probabilité qu'un accident se produise et de l'ampleur de l'impact dommageable ainsi causé. Aussi est-ce l'effet combiné du "risque" et du "dommage" qui détermine le seuil » (*ibid.*, pp. 417-418).

(139) Selon ainsi la CDI, « L'idée de seuil est présente dans la sentence rendue dans l'affaire de la *Fonderie de Trail* où sont employés les mots "*serious consequences*" (conséquences graves), de même que dans celle rendue dans l'affaire du *Lac Lanoux*, qui s'est appuyée sur le concept rendu par "gravement" ("*seriously*"). On a aussi utilisé les termes "important", "sensible" ou "significatif" (comme équivalents du mot "*significant*"), ainsi que les termes "grave" ou "substantiel", pour exprimer le seuil dans un certain nombre de conventions. L'adjectif anglais « "*significant*" a également été employé dans d'autres instruments juridiques et dans des textes de loi nationaux » (*ibid.*, Commentaire art. 2, § 6, p. 419). On pourrait d'ailleurs ajouter à cette liste d'exemples l'*Affaire du Fleuve San José* où la CIJ parle de « dommages transfrontières importants » (*Certaines activités menées par le Nicaragua dans la région frontalière* (*Costa Rica c. Nicaragua*) & *Construction d'une route au Costa Rica le long du fleuve San Juan* (*Nicaragua c. Costa Rica*), arrêt du 16 décembre 2015, *Rec. CIJ*, 2015, § 153).

(140) CDI, Projet d'articles sur la prévention des dommages transfrontières résultant d'activités dangereuses et commentaires y relatifs, *op. cit.*, art. 1, p. 409.

(141) Voy. à cet égard, ILA, Study Group on Due Diligence in International Law, *op. cit.*, p. 26.

(142) Responsabilités et obligations des États dans le cadre d'activités menées dans la Zone, *op. cit.*, § 116.

CDI elle-même (143). Quoi qu'il en soit, ce qui importe ici, c'est de constater que le degré de vigilance attendu d'un État varie en fonction de la gravité du dommage que l'on peut raisonnablement prévoir. Ainsi selon la CDI, « [p]lus le risque de dommage *inacceptable* est élevé, plus l'obligation de vigilance pour le prévenir serait importante » (144) et c'est donc l'ampleur du dommage potentiel combiné à l'importance du risque qui permet d'évaluer le degré de vigilance que les États doivent porter à une activité donnée (145).

Ni le seuil ni le degré de gravité du dommage n'ont toutefois fait l'objet d'une attention particulière dans les rapports du GGE des Nations Unies sur la cyber-sécurité. Ces derniers évoquent de façon assez vague « l'éventualité de dommages » pour les biens, l'économie et les ressortissants des États mais sans les caractériser davantage (146). Les travaux menés sur la cyber-sécurité, au sein du GGE comme dans d'autres instances internationales, montrent que l'attention s'est jusqu'à présent plutôt portée sur l'importance de certains biens pour les États et la communauté internationale et les effets que leur destruction pourrait avoir pour ces derniers. Les expressions « infrastructures critiques », « infrastructures essentielles », « opérateurs de services essentiels » ou encore « opérateurs d'importance vitale » sont fréquemment utilisées pour désigner des installations, des équipements ou des biens dont « la destruction ou l'indisponibilité obéreraient gravement le potentiel militaire, la force économique, la sécurité voire la capacité de survie d'un État ou mettraient en danger sa population » (147). Dans son rapport de 2015, le GGE souligne ainsi que « [l]es États devraient prendre les mesures appropriées pour protéger leurs infrastructures essentielles des risques liés aux technologies de l'information et des télécommunications » (148) et qu'« [u]n État ne devrait pas mener ou soutenir sciemment une activité informatique qui est contraire aux obligations qu'il a contractées en vertu du droit international et qui endommage intentionnellement une infrastructure essentielle ou qui compromet l'utilisation et le fonctionnement d'une infrastructure essentielle pour fournir des services au public » (149) (voy. aussi *infra* nos développements).

(143) « Le terme "significatif" n'est pas sans ambiguïté et il faut se prononcer dans chaque cas d'espèce. Il implique davantage des considérations d'ordre factuel qu'une décision juridique. Il doit être entendu que « significatif » est plus que « détectable », mais sans nécessairement atteindre le niveau de « grave » ou « substantiel ». Le dommage doit se solder par un effet préjudiciable réel sur des choses telles que la santé de l'homme, l'industrie, les biens, l'environnement ou l'agriculture dans d'autres États. Ces effets préjudiciables doivent pouvoir être mesurés à l'aide de critères factuels et objectifs » (Projet d'articles sur la prévention des dommages transfrontières résultant d'activités dangereuses et commentaires y relatifs, *op. cit.*, p. 417).

(144) *Ibid.*, p. 426.

(145) *Ibid.*, p. 416.

(146) GGE 2015, *op. cit.*, § 7.

(147) Commission d'enrichissement de la langue française, *Vocabulaire de la défense : cyberdéfense*, *JORF*, 19 septembre 2017.

(148) GGE 2015, *op. cit.*, § 13 (g).

(149) *Ibid.*, § 13 (f).

B. — *Les implications pratiques de l'obligation de due diligence dans le cyberespace*

Nous avons vu que selon le principe de due diligence les États ont l'obligation de prendre les mesures raisonnables afin de faire en sorte que leur territoire ou les espaces sous leur contrôle ou juridictions ne soient pas utilisés à des fins contraires aux droits d'autres États et que l'appréciation de la conformité du comportement de l'État avec cette obligation ne peut se faire qu'au cas par cas en tenant compte des « facteurs de variabilité ». Il convient maintenant, d'examiner les implications pratiques de ce principe aussi bien en ce qui concerne les obligations des États en matière de cyber-sécurité (1) qu'en ce qui concerne les conséquences de sa violation dans le cadre des règles secondaires relatives à la responsabilité internationale des États (2).

1) *Implications au niveau du comportement requis par les États en matière de cyber-sécurité*

Même si l'obligation de diligence implique une appréciation de nature objective tout en renvoyant à des notions (comme le « raisonnable ») et des critères déjà utilisés et précisés dans d'autres domaines du droit international, son application concrète dans l'espace numérique nécessite sans doute des recherches pluridisciplinaires approfondies. Nous ne sommes en effet qu'au début de la réflexion et, contrairement à d'autres domaines du droit international, aucune décision de justice internationale n'est encore venue éclairer les nombreuses questions et zones d'ombre qui demeurent.

Il semble toutefois admis que l'obligation de due diligence impose à un État, qui a connaissance d'activités malveillantes développées depuis son territoire contre un État tiers, de prendre les mesures raisonnables pour mettre fin à ces activités. De ce point de vue, la due diligence comporte donc une obligation d'agir en vue de faire *cesser* les activités qui portent atteinte aux droits d'États tiers. Toutefois, certaines questions importantes demeurent : la due diligence implique-t-elle une obligation de notification voire de coopération (a) ? Implique-t-elle aussi une obligation de prévention et de répression (b) ? En cas de réponse positive, existe-t-il une obligation d'adopter des mesures en amont (c) ? Et finalement, dans la mesure où les obligations de diligence sont par définition des obligations de moyen, existe-t-il parallèlement à celles-ci certaines obligations de résultat fonctionnellement nécessaires à la réalisation des obligations de diligence (d) ?

a) *Une obligation de notification voire de coopération ?*

Existe-t-il des moyens spécifiques que l'État devrait utiliser dans le cadre de la réaction à une cyberattaque ? Plus précisément, existe-t-il une obligation de *notification* à l'égard de l'État victime d'une cyberattaque, voire une obligation de *coopération* avec celui-ci ?

Dans l'*Affaire du Détroit de Corfou*, la CIJ a interprété l'obligation de diligence requise par les autorités albanaises comme impliquant l'obligation de « 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 »(150). Or, alors que l'Albanie connaissait ou aurait dû connaitre la présence de ces mines, elle n'a « ni notifié l'existence du champ de mines ni averti les navires de guerre britanniques du danger vers lequel ils avançaient »(151). Pourrait-on en déduire que la CIJ a considéré qu'il existait, dans le cadre de la diligence due, une obligation de notification vis-à-vis de l'État tiers qui est victime ou qui risque d'être victime d'une activité informatique ?

Une certaine prudence s'impose à cet égard. Affirmer qu'il existerait toujours « une obligation de notification » dont la violation entrainerait automatiquement la responsabilité d'un État signifierait que nous serions là devant une obligation de *résultat*. Or, comme nous l'avons longuement montré, les obligations de diligence ne sont, par définition, que des obligations de *comportement*. Les États ont donc le choix des moyens pour essayer de mettre fin au risque connu pour la sécurité de l'État tiers et la notification, voire la coopération avec l'État tiers, sont sans doute des moyens privilégiés mais ils ne sont pas les seuls. Si l'État adopte d'autres mesures pour prévenir la cyberattaque et/ou mettre fin à celle-ci, la notification pourrait ne pas être nécessaire.

Ceci étant dit, dans certaines situations la notification pourrait être *le seul moyen* de prévenir la survenance du dommage ou d'en atténuer les conséquences. Dans l'*Affaire du Détroit de Corfou*, par exemple, compte tenu des circonstances de l'affaire et de ce que la Cour a appelé une « extrême limite de temps », la notification au Royaume-Uni apparaissait comme pratiquement le seul moyen disponible(152). On voit donc que, sans nécessairement constituer une obligation autonome, la notification pourrait paraître comme pratiquement incontournable dans certains cas et ceci d'autant plus qu'une telle notification semble être à la portée de tous les États indépendamment de leur « capacité »(153). Compte tenu de la nature de l'espace numérique et du caractère potentiellement dévastateur des cyberattaques, les États

(150) *Affaire du Détroit de Corfou*, préc., p. 22.

(151) *Ibid.*

(152) Pourtant, comme l'a conclu la Cour : « rien ne fut tenté par les autorités albanaises pour prévenir le désastre. Ces graves omissions engagent la responsabilité internationale de l'Albanie » (*ibid.*, p. 23).

(153) Certaines circonstances exceptionnelles, telles qu'une situation de force majeure ou d'état de nécessité, pourraient néanmoins excuser l'absence de notification. On pourrait aussi penser que certains États puissent souhaiter éviter de dévoiler les moyens technologiques qui leur ont permis de détecter une cyberattaque — mais dans ce cas, peut-être qu'un calcul de nécessité et de proportionnalité pourrait entrer dans l'équation de l'appréciation du caractère « raisonnable » de l'absence de notification en tenant compte de l'importance des dommages causés par la cyberattaque.

devraient sans doute utiliser largement la *notification*, faute de quoi on pourrait conclure qu'ils n'ont pas pris les mesures « raisonnables » à leur disposition pour prévenir/cesser la cyberattaque. Quant à la *coopération* entre les États, si elle apparaît comme très souhaitable elle pourrait être moins impérative que la notification. Au regard de certaines difficultés de coopération inhérentes au cyberespace (y compris celle de ne pas dévoiler à des tiers la situation technologique d'un État en matière de cyber-sécurité) ou des relations parfois compliquées entre les États, la coopération pourrait en effet s'avérer beaucoup plus difficile qu'une notification qui, comme il a été souligné, est à la disposition de tous. Il convient toutefois de relever que, pour certains États, le principe de due diligence doit jouer un rôle moteur dans le développement de la coopération volontaire entre les États. C'est ainsi que selon la France, le « principe de "cyberdiligence" pourrait notamment permettre de renforcer la coopération opérationnelle volontaire entre les États, essentielle en vue de protéger certaines infrastructures critiques et de répondre à des cyberattaques majeures, notamment lorsque celles-ci transitent via un État tiers » (154).

b) *Une obligation de prévention voire de répression ?*

La deuxième question est de savoir si le devoir de diligence va au-delà de l'obligation de prendre des mesures en vue d'arrêter une cyberattaque en cours. Le Manuel de Tallinn 2.0 rejette en effet l'idée selon laquelle l'obligation de diligence comprend une dimension de prévention (155) ou de répression (156). Deux observations peuvent être faites à cet égard.

Tout d'abord, il faut noter qu'il n'existe aucun obstacle « structurel » ou théorique à ce que les obligations de diligence comprennent une dimension autre que l'action en vue de la *cessation* d'une atteinte aux droits d'un État tiers. Au contraire, toutes les études autorisées du standard de due diligence en droit international montrent que ce standard comporte à la fois une dimension de *prévention*, de *cessation* et, parfois même d'*enquête* et de *répression* (157). Comme le note Riccardo Pisillo Mazzeschi : « *diligence does not apply to the State's obligation to possess a minimum apparatus for protection*

(154) Secrétariat de la Défense et de la Sécurité Nationale, *Revue Stratégique de cyberdéfense*, *op. cit.*, p. 86.

(155) M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, voy. pp. 44 et s., où il est par exemple dit que : « *the Experts rejected the argument that the due diligence obligation requires preventive measures* » (§ 13) car « *the obligation is limited to taking feasible measures to terminate the operations* » (§ 21).

(156) *Ibid.*, p. 48 (§ 21) : « *Nor is there any obligation under the due diligence principle for the State to prosecute those engaging in the underlying cyber operations* ».

(157) Dans l'*Affaire du Détroit de Corfou*, la Cour avait ainsi reproché à l'Albanie, que « 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 » (préc., pp. 19-20).

but only to the obligation to use *this apparatus in activities of* prevention *and in some activities involving* punishment » (158). La jurisprudence internationale, que ce soit celle des Tribunaux arbitraux (159), de la CIJ (160) ou des organes de protection des droits de l'homme (161), regorge d'exemples où le devoir de prévention (ou encore de poursuites) a été clairement et expressément affirmé en relation avec des obligations de diligence (162). Dans ce contexte, on voit mal comment le standard de diligence en matière de cyber-sécurité devrait subitement être amputé de ces deux volets.

Le Manuel de Tallinn 2.0, tout en repoussant fermement le concept de « prévention », semble toutefois l'admettre implicitement dans au moins deux hypothèses. Tout d'abord, en soulignant que « [*the principle of due diligence*] *also applies to specific cyber operations that have not yet been launched, but with respect to which material steps to execute the operation are being taken and a reasonable State would conclude it will be carried out* » (163) ; ensuite, en reconnaissant qu'il existe une obligation de prévention dans une situation « *in which a State foresees with reasonable certainty that cyber infrastructure*

(158) R. Pisillo Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », *op. cit.*, p. 46 (nous soulignons). Voy. aussi par exemple p. 27 : « *the due diligence concept certainly comes into play with regard to the State's duty* to use *its apparatus for purposes of prevention. This is confirmed by a very wide international practice, which covers the whole sector of so-called State responsibility for acts of private persons* ».

(159) Dans l'*Affaire de* l'*Alabama*, par exemple, 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* [...] *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 their execution was not practicable* » (*Réclamations des États-Unis d'Amérique contre la Grande-Bretagne relatives à l'Alabama*, préc., p. 130 [nous soulignons]).

(160) 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 » (préc., p. 23 — nous soulignons). 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 » (*Affaire des activités armées sur le territoire du Congo*, préc., § 179 — nous soulignons). Dans l'*Affaire du Génocide*, la Cour parle, là aussi clairement, d'une obligation pour l'État « de mettre en œuvre les mesures de *prévention* du génocide qui étaient à sa portée » (préc., § 430 — nous soulignons).

(161) Parmi les très nombreux arrêts de la CEDH, voy., par exemple, l'affirmation de prendre des mesures de prévention pour réduire des phénomènes de pollutions nuisibles à la vie privée des personnes dans des affaires aussi célèbres que *López Ostra c. Espagne*, arrêt du 9 décembre 1994 ; ou *Hatton et autres c. Royaume-Uni*, arrêt du 2 octobre 2001.

(162) Voy. aussi à cet égard les travaux de la CDI sur la prévention des dommages transfrontières résultant d'activités dangereuses où la CDI qualifie de « principe général » fondé sur l'obligation de prévenir des dommages transfrontières significatifs (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, Article 3, commentaire §§ 1 et s., pp. 420-421).

(163) M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, *op. cit.*, p. 43, § 3.

on its territory, having previously been so used, will again be employed for harmful cyber operations directed at another State » (164). On glisse donc ici de l'affirmation selon laquelle l'obligation d'agir n'existe que dans une logique de *cessation* d'un acte en cours vers la reconnaissance d'une obligation de diligence pour *prévenir* des risques sérieux.

Il est donc bien difficile d'effacer la prévention de l'équation de la *due diligence* tant elle fait partie de l'ADN même des obligations de diligence (qui incluent, mais ne se limitent pas à, cette dimension). Il convient par ailleurs de rappeler que le manquement à une obligation de « prévention » ne peut être apprécié que *in concreto*, en tenant compte notamment de la connaissance et de la gravité du *risque* et de la capacité raisonnable de l'État d'adopter des mesures en vue de prévenir ce risque. Tout cela fait partie des « facteurs de variabilité » examinés précédemment. Soutenir qu'il ne doit pas y avoir d'obligation de prévention dans le cyberespace, car cela « imposerait un fardeau insupportable aux États » en matière de développement de mesures effectives de cyberdéfense, n'a pas vraiment de sens du point de vue de la théorie de la diligence due car l'obligation d'agir pour prévenir ne commence que *si* un risque grave pour les droits d'un autre État existe. En d'autres termes, la seule boussole est celle de la règle primaire qui impose la diligence requise, à savoir l'« obligation, pour tout État, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres États ». L'obligation d'adopter des mesures raisonnables existe *chaque fois* qu'un risque d'atteinte grave aux droits d'un autre État est avéré et connu — et pas seulement si une action hostile est déjà déclenchée (165).

c) *Une obligation d'adopter des mesures en amont ?*

Ce qui semble en réalité préoccuper les rédacteurs du Manuel de Tallinn 2.0 est une question conceptuellement *distincte*, bien que complémentaire et très liée à celle de la diligence due : existe-t-il des obligations positives d'adopter des mesures afin d'être capable de faire face effectivement aux cyberattaques ? Existe-t-il une obligation pour les États de prendre des mesures concrètes, législatives, administratives, techniques, pour prévenir l'utilisation des infrastructures numériques à des fins malveillantes contre d'autres États ? Il s'agit d'une question complexe dont l'analyse pourrait nous amener bien loin. Dans le cadre limité de cet article, nous nous cantonnerons à quelques brèves observations.

Premièrement, cette question est, bien que très complémentaire, *distincte* de celle du contenu des obligations de *diligence*. Quand on pose les questions

(164) *Ibid.*, p. 46, §§ 14-15.

(165) Il s'agit bien, d'ailleurs, d'une obligation de prévention en cas de risque avéré (ou qui aurait dû être raisonnablement connu de la part d'un État agissant de bonne foi, comme dans l'affaire du *Détroit de Corfou*) — et non pas d'une obligation de *précaution* pour des risques aléatoires et non avérés.

de savoir si les États ont l'obligation de légiférer en matière de cyber-sécurité, de protéger leurs infrastructures critiques ou d'interdire l'acquisition par des acteurs privés d'armes ou techniques cyber-offensives ou le commerce des vulnérabilités « zero-days » (à savoir les vulnérabilités non corrigées), il s'agit là de questions relatives à l'existence de certaines obligations de *résultat*. Or, comme nous l'avons vu, les obligations de diligence ne sont, par définition, que des obligations de *moyens*. Si on estimait par exemple que les États ont l'obligation « d'interdire la commercialisation de techniques cyber-offensives », dont la violation engagerait en tant que telle la responsabilité de l'État, nous ne serions plus dans le cadre des obligations de *diligence* mais plutôt dans le cadre d'obligations de *résultat*.

Or, pour que de telles obligations de résultat puissent exister deux voies sont possibles. D'une part, l'adoption de règles primaires spécifiques imposant de telles obligations de résultat, comme par exemple une obligation d'adopter des mesures législatives spécifiques. L'exemple le plus connu dans ce domaine est la Convention de Budapest de 2001 du Conseil de l'Europe sur la cybercriminalité, ratifiée par 56 États, dont le principal objectif, énoncé dès son préambule, est de mettre en place « une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée… ». De telles obligations de résultat vont alors se combiner avec les obligations de moyens prévues soit par le droit international général, soit par des règles primaires spécifiques. D'autre part, et c'est un point sur lequel nous allons maintenant nous tourner, on peut se demander si certaines obligations de résultat ne seraient pas fonctionnellement nécessaires à la mise en œuvre des obligations de diligence.

d) *Des obligations de résultat fonctionnellement nécessaires à la réalisation des obligations de diligence ?*

Existerait-il donc certaines obligations de résultat qui, tout en étant distinctes des obligations de diligence, seraient *fonctionnellement nécessaires* à la réalisation de celles-ci ? Comme le montre ainsi Riccardo Pisillo Mazzeschi, dans le domaine de la protection des droits de l'homme, il existe certaines obligations positives de *résultat*, qui ne font pas partie des obligations de diligence mais qui sont fonctionnellement nécessaires pour atteindre le but général du respect de ces droits — par exemple l'obligation de se doter d'une législation qui respecte et sauvegarde les droit de l'homme, de disposer d'un appareil adéquat de prévention des violations des droits de l'homme et d'enquête (166). L'émergence de telles obligations positives de *résultat* liées aux obligations de diligence dans le domaine du cyberespace devrait toutefois résulter de la volonté de la communauté des États, exprimée soit par la voie

(166) Voy. R. Pisillo Mazzeschi, *Responsabilité de l'État pour violation des obligations positives relatives aux droits de l'homme*, *op. cit.*, pp. 311 et s.

conventionnelle soit par la voie coutumière. C'est ainsi, par exemple, que la protection des infrastructures critiques constitue aujourd'hui un aspect essentiel de la sécurité de l'espace numérique. Les travaux conduits par l'Assemblée générale des Nations Unies sur la cyber-sécurité et la protection des infrastructures critiques (167), les travaux de l'OSCE sur cette même question dans le cadre de ses mesures de confiance (168), ou encore les travaux de l'OCDE (169), de l'Union européenne (170), de l'Union africaine (171) et de l'Organisation de coopération de Shanghai (172) montrent qu'il existe une préoccupation commune des États afin d'élaborer des standards 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… » (173). La résolution 2341 adoptée à l'unanimité le 13 février 2017 par le Conseil de sécurité de l'ONU sur la protection des infrastructures critiques contre les attaques terroristes et notamment contre les cyber-attaques démontre aussi à quel point la communauté internationale est préoccupée par la nécessité de protéger ces infrastructures d'importance vitale et de développer une coopération internationale dans ce domaine entre les États mais aussi avec le secteur privé qui est tout aussi concerné par ces questions.

2) *Implications pour les règles secondaires de la responsabilité internationale*

La violation dans le cyberespace de l'obligation de moyen de ne pas laisser sciemment son territoire être utilisé à des fins contraires aux droits d'États

(167) Dans sa résolution 64/211 du 21 décembre 2009 intitulée Création d'une culture mondiale de la cyber-sécurité et évaluation des efforts nationaux visant à protéger les infrastructures essentielles, l'Assemblée générale des Nations Unies a ainsi proposé aux États une « Méthode d'auto-évaluation volontaire des efforts nationaux » qui incite les États à développer des mesures de protection de leurs infrastructures numériques critiques.

(168) Voy., par exemple, OSCE, *Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, Décision nº 1201, 10 mars 2016.

(169) Voy., 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 June 2008.

(170) Voy. notamment à cet égard la directive (UE) 2016/1148 du Parlement européen et du Conseil 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.

(171) Convention de l'Union africaine sur la cyber-sécurité et la protection des données à caractère personnel du 27 juin 2014, disponible sur https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf.

(172) 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, disponible sur http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf (traduction non officielle en anglais disponible sur http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf).

(173) GGE 2015, *op. cit.*, § 13.

tiers pourrait constituer un acte illicite international engageant la responsabilité de l'État. À cet égard, il est intéressant de remarquer que, alors que l'attribution constitue l'un des problèmes les plus épineux pour engager de la responsabilité des États dans le cyberespace, ce problème d'attribution est contourné lorsqu'il s'agit d'engager cette responsabilité sur le fondement de l'obligation de due diligence (a). Ceci ne signifie toutefois pas que la responsabilité dans ce domaine est plus « facile » ni plus « étendue » car, comme nous allons le voir, l'engagement de la responsabilité d'un État pour violation de ses obligations de due diligence pourrait parfois devenir une véritable *probatio diabolica* (b).

a) *Un contournement opportun du problème majeur de l'attribution*

Il est bien connu que l'attribution d'une cyberattaque, comme opération juridique mais surtout comme opération technique liée à la criminalistique (ce que l'on appelle en anglais les « *cyber forensics* »), est particulièrement complexe et laborieuse. Ces difficultés sont dues à une multitude de facteurs dont le manque de capacités techniques suffisantes dans de nombreux pays (le problème de « *forensic capacity* ») ainsi que le recours à des techniques de dissimulation (« *spoofing* ») particulièrement sophistiquées qui sont utilisées par les hackeurs pour faire croire que l'attaque a été lancée par quelqu'un d'autre. 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 » pour développer des activités malveillantes contre les intérêts d'autres États. Dans l'espace numérique, le recours à des personnes privées sous la forme de « *proxies* » est en effet une pratique largement utilisée par certains États qui cherchent ainsi à développer différentes opérations de manière clandestine (174). 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 (175). Dans son Rapport de 2015, le GGE a réitéré avec force cette affirmation en soulignant que « [l]es États (…) 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 » (176).

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

(175) GGE 2013, *op. cit.*, § 23.

(176) GGE 2015, *op. cit.*, § 28 (e).

Malgré ces appels, l'attribution aux États des actes des personnes privées reste une opération très complexe dans le cyberespace. Il est rare 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 (177). 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 » (178). 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 » (179).

L'application dans l'espace numérique du standard de diligence due permet de contourner en grande partie ces difficultés, sans, bien entendu, les résoudre. Établir qu'un État a violé ses obligations de diligence n'implique en effet pas nécessairement *l'attribution* de la cyberattaque à cet État en utilisant les mécanismes classiques d'imputation. Il est en fait relativement indifférent que l'activité en question ait été commise par un organe de l'État, un agent agissant *ultra vires* ou en dehors de ses fonctions, un « *proxy* », un intermédiaire, un groupe de « hackers patriotiques », des terroristes, la mafia, des cybercriminels ou encore une entreprise voulant tirer un avantage concurrentiel. La seule chose qui importe pour la due diligence c'est de savoir si les éléments constitutifs de sa violation sont présents et ceci quel que soit l'auteur de l'attaque : l'État savait-il ou aurait-il dû savoir que ses infrastructures étaient utilisées pour lancer une cyberattaque causant un dommage d'une certaine gravité à un autre État ? A-t-il manqué à son obligation de prendre les mesures raisonnables dont il disposait pour prévenir le dommage ? Si la réponse à ces questions est positive, la responsabilité de

(177) Voy. notamment sur cette question, M. Schmitt, L. Vihul, « Proxy Wars in Cyber Space: The Evolving International Law of Attribution », (2014) I *Fletcher Security Review* 55, pp. 55-73 ; K. 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 and Security Law*, 2016, vol. 21, n° 3, pp. 405-428.

(178) GGE 2015, *op. cit.*, § 28 (f).

(179) *Ibid.*

l'État pourrait être engagée quel que soit l'auteur des actes (180). La situation juridique de la Russie dans le cadre de l'attaque contre le parti démocrate durant les élections présidentielles américaines est ainsi intéressante à rappeler. En effet, la Russie a été ouvertement accusée par les États-Unis d'avoir dirigé cette opération (181). De nombreuses études et déclarations ont estimé que ces attaques avaient été lancées par différents groupes russes et au mois de février 2018, le procureur spécial chargé de superviser l'enquête sur de possibles ingérences du gouvernement russe dans cette affaire a mis en accusation plusieurs ressortissants et sociétés russes (182).

Pendant longtemps, la Russie a nié toute implication de groupes russes dans cette attaque. Toutefois, en juin 2017, à l'occasion du Forum économique de St Petersbourg, le Président Poutine a reconnu que des hackers russes avaient pu théoriquement participer à cette attaque tout en déclinant toute responsabilité de la Russie à l'égard de ce qu'il a qualifié de « hackers patriotiques » (183). Du point de vue de l'obligation de due diligence on comprend que l'argument du Président Poutine n'est pas convaincant et que, sans même avoir à démontrer le lien entre le gouvernement russe et ces hackers, la responsabilité de la Russie pourrait être engagée si l'on arrivait à prouver que la Russie savait et pouvait empêcher ou faire cesser ces attaques.

Bien entendu, cela ne signifie pas que les nombreuses difficultés techniques relatives à l'origine et au mode opératoire des cyberattaques disparaissent comme par miracle. Pour démontrer l'existence d'une violation de l'obligation de diligence, des preuves techniques sont nécessaires, y compris celles permettant de démontrer que la cyberattaque émane bien du territoire de

(180) Selon ainsi la *Revue Stratégique de Cyberdéfense* de la France, « Un État qui n'aurait pas rempli cette obligation (de moyens) pourrait ainsi, dans certains cas engager sa responsabilité et être l'objet de contre-mesures par l'État victime, même s'il n'est pas le commanditaire. Pour faire jouer cette hypothèse, il convient néanmoins de notifier au préalable à l'État que ses infrastructures sont utilisées à des fins malveillantes (critère de connaissance) et d'assurer que l'État n'a pas rempli son obligation (de moyens) de faire cesser l'attaque. Une telle situation pourrait par exemple se caractériser par le silence complet d'un État saisi d'une requête d'assistance, ou le refus de coopérer en vue de résoudre l'incident ou de mettre un terme à l'attaque » (Secrétariat de la Défense et de la Sécurité Nationale, *Revue Stratégique de cyberdéfense*, *op. cit.*, pp. 83-84). Il va de soi que si l'opération ultérieure d'attribution conclut que la cyberattaque est imputable à l'État lui-même, la nature de la responsabilité pourrait changer passant d'un simple manquement à une obligation d'agir afin de prévenir à un manquement au devoir d'abstention. Les conséquences en termes de responsabilité et de réparation pourraient alors être plus importantes.

(181) US Homeland Security, *Joint Statment from the Homeland Security and Office of the Director of National Intelligence on Election Security*, 7 octobre, disponible sur https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

(182) « 13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign », *The New York Times*, 16 février 2018, disponible sur https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html.

(183) « Présidentielles : Poutine reconnaît de possibles piratages russes pour mieux dédouaner le Kremlin », *Numerama*, 2 juin 2017, disponible sur https://www.numerama.com/politique/263638-presidentielles-poutine-reconnait-de-possibles-piratages-russes-pour-mieux-dedouaner-le-kremlin.html.

l'État en question (ou y a transité) et que ce dernier avait (ou aurait dû) avoir connaissance de cette situation, disposait des moyens raisonnables pour y mettre fin (ou au moins en atténuer les conséquences) et n'a rien fait à cet égard. Ces difficultés technico-juridiques, combinées à d'autres difficultés inhérentes même à la nature de la diligence due, pourraient rendre la preuve de la violation d'une telle obligation de vigilance dans le cyberespace particulièrement difficile.

b) *Un engagement plus difficile de la responsabilité internationale*

Certains détracteurs ont soutenu que l'existence d'obligations de diligence dans le cyberespace pourrait « déstabiliser brutalement » le droit international en favorisant l'adoption de contremesures et une escalade dans l'engagement de la responsabilité internationale des États. Selon par exemple, deux auteurs :

> « *In short, by presenting more opportunities for more State to allege more breaches of international law, due diligence potentially increases the frequency of States' resort to contermeasures and their accompanying potentially destabilizing effects* » (184).

Cette position semble néanmoins discutable. En effet, l'existence d'obligations de diligence en matière de cyber-sécurité n'affecte pas, en tant que telle, le régime juridique des contremesures en droit international et par ailleurs, contrairement à ce qui est soutenu, l'engagement de la responsabilité des États pour manquement à leurs obligations de diligence dans le cyberespace est loin d'être aisé et se heurte même à des difficultés redoutables.

Il convient tout d'abord de souligner que le droit international positif 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 contre ce dernier. Il s'agit ici d'un domaine où le vieil adage *nemo iudex in causa sua* 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. (185) Comme l'avait souligné en 1978 un Tribunal Arbitral dans une affaire 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 ». (186)

(184) E. Talbot Jensen, S. Watts, « A cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer », *op. cit.*, p. 1577.

(185) Voy. L.A. Sicilianos, *Les réactions décentralisées à l'illicite*, Paris, LGDJ, 1990, p. 31.

(186) *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.

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 » (187).

Ceci signifie donc qu'un État n'a pas *l'obligation juridique* (188) de démontrer qu'un autre État a violé le droit international (par action ou omission) avant d'adopter des contre-mesures contre un autre État accusé d'être lié à une cyberattaque (189). On peut logiquement penser qu'un État qui subit des dommages graves du fait d'une cyberattaque lancée depuis le territoire d'un autre État *va réagir de toute façon* et par divers moyens pour mettre fin à la cyberattaque et en atténuer les conséquences. En d'autres termes, ce qui va le motiver pour réagir et protéger ses intérêts n'est pas une réflexion théorique sur la *nature* des obligations existantes en droit international dans ce domaine (dont il n'a même pas à démontrer la violation), mais plutôt l'existence de la situation factuelle : la cyberattaque dommageable. Par ailleurs, et pour aller plus loin, si l'État n'est pas informé du cadre juridique dans lequel il peut réagir, on pourrait craindre le pire. L'État pourrait, par exemple, essayer de s'appuyer sur la théorie controversée « *unwilling or unable* » considérant que l'incapacité d'un État de mettre fin aux cyberattaques, combinée à la gravité des dommages, l'autorise à invoquer la légitime défense et recourir à la force. L'explication du régime juridique dans lequel il intervient et du fait que l'obligation de diligence est une obligation de comportement et non de résultat pourrait alors s'avérer utile pour limiter l'ampleur des réactions et les encadrer.

Loin de « déstabiliser » le droit international, l'affirmation de l'existence d'obligations de diligence dans le cyberespace pouvait s'avérer salvatrice pour « responsabiliser » les États (en leur faisant prendre conscience de leurs devoirs découlant de leur souveraineté et de l'impératif de coexistence pacifique) sans pour autant multiplier, comme le craignent certains, les cas d'engagement de leur responsabilité internationale. Comme l'a bien expliqué Riccardo Pisillo Mazzeschi (190), l'engagement de la responsabilité d'un État pour manquement à ses obligations de diligence est particulièrement

(187) Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, *Rapport de la Commission du droit international*, Cinquante-troisième session, A/56/10, supplément n° 10, p. 355, § 3.

(188) Néanmoins, 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.

(189) Voy. à cet égard nos analyses, K. Bannelier, T. Christakis, *Cyberattaques. Prévention-réactions : rôle des États et des acteurs privés*, *op. cit.*, pp. 49-50.

(190) Voy. par exemple R. Pisillo Mazzeschi, « The Due Diligence Rule and the Nature of the International Responsibility of States », *op. cit.*, p. 50.

difficile. Alors que pour les obligations de résultat il suffit de démontrer que le résultat n'a pas été atteint (et que ce manquement est attribuable à l'État), les obligations de diligence exigent une opération très complexe consistant à établir que : 1) l'État avait connaissance d'une cyberattaque lancée ou transitant par son territoire ; 2) qu'il avait aussi connaissance que cette attaque causait des dommages importants au territoire d'un État tiers ; 3) qu'il avait la capacité, compte tenu aussi des circonstances, d'adopter des mesures efficaces pour mettre fin à cette cyberattaque et/ou en atténuer les effets ; 4) et que le comportement qu'il a adopté (inaction complète ou action limitée) était en inadéquation avec celui que l'on pourrait raisonnablement attendre de lui (191). Cette démonstration, en tenant compte aussi des difficultés techniques inhérentes au cyberespace mentionnées *supra*, pourrait être extrêmement difficile à réaliser.

En conclusion, il semble que l'application du principe de diligence due en matière de cyber-sécurité n'aura pas les conséquences graves prédites pas certains. La « cyber-diligence » n'a pas pour fonction de conduire à un régime « aggravé » de responsabilité internationale. Son objectif est plutôt de sensibiliser les États à propos de la nécessité d'agir en matière de sécurité du numérique dans une optique qui vise, après tout, à promouvoir la sécurité internationale et la sécurité humaine.

Conclusion

Le concept de cyber-diligence a un rôle important à jouer en matière de cyber-sécurité en contribuant à l'émergence d'un comportement responsable des États dans le cyberespace à travers l'affirmation de leur responsabilité première de vigilance pour les activités situées sur leur territoire et conduites tant par des personnes publiques que par des acteurs privés. Il instaure ainsi un standard de comportement raisonnable et responsable des États pour prévenir et mettre fin, en cas de connaissance et de capacité, aux cyberattaques lancées depuis leur territoire ou sous leur contrôle contre les infrastructures, les entreprises et les particuliers d'autres États.

Du point de vue du droit international, le concept de cyber-diligence présente deux attraits majeurs. Tout d'abord, il peut permettre, comme nous l'avons analysé (II(2a)), de *« contourner » en partie le problème majeur de l'attribution*. Il pourrait aussi permettre de résoudre celui de la *qualification juridique d'une cyberattaque* et la question existentielle de savoir si celle-ci constitue ou non un « acte illicite international ». La pratique en matière de

(191) C'est ainsi par exemple que la France dans ses « options de réponse aux attaques informatiques » reconnaît expressément la possibilité pour un État suspecté de se disculper en rapportant « les mesures qu'il aurait prises en matière de cyber-diligence » (Secrétariat de la Défense et de la Sécurité Nationale, *Revue Stratégique de cyberdéfense*, *op. cit.*, p. 161).

cyberattaques montre, en effet, qu'il est parfois difficile de qualifier d'« acte illicite international » une cyberattaque lancée depuis un État, soit parce qu'il est très difficile d'attribuer celle-ci à celui-ci, soit parce qu'il est difficile de déterminer avec précision la norme violée, soit pour les deux raisons à la fois. Après l'attaque contre Sony en 2014, le président Obama a par exemple refusé de se référer à une norme de droit international, préférant simplement la décrire comme un acte de « cyber-vandalisme » (192), terme qui ne signifie rien de spécifique du point de vue du droit international. De manière similaire, lors du piratage du parti démocrate lors des élections américaines de 2016, le Président Obama n'a pas parlé directement d'une violation du droit international mais de « *violation of established international norms of behavior* » (193), expression qui, si on y regarde de plus près, pourrait ne pas nécessairement désigner une violation du droit international. Le concept de cyber-diligence pourrait donc permettre de résoudre ces difficultés : au lieu de mettre l'accent sur la qualification juridique d'une cyberattaque, ce concept permet de se focaliser sur *ce qui aurait pu être fait* par un État, et sur *ce que l'État n'a pas fait*. Ainsi, sans avoir à chercher si la cyberattaque en question est ou non « le fait d'un État », et sans avoir à chercher quelle *norme précise* a été violée (non-ingérence ? non-intervention ? autre ?), on pourrait se focaliser sur le fait que l'État *savait* qu'une cyberattaque était lancée depuis son territoire et ses infrastructures, *avait les moyens d'agir* pour empêcher cette cyberattaque ou en atténuer les effets, et pourtant n'a rien fait à cet égard. Pour revenir au point de départ de cet article : « Qui peut et n'empêche, pèche ».

Depuis la publication d'une première étude sur l'existence d'obligations de diligence dans le cyberespace (194), l'auteur a pu suivre les évolutions de ce débat au sein de différents fora internationaux. Ces débats montrent qu'il existe une volonté d'un grand nombre d'États de consacrer le standard de diligence due comme un pilier central de l'édifice du droit international de la cyber-sécurité comme en témoigne notamment la *Revue stratégique de Cyberdéfense* récemment publiée par la France. Toutefois, un nombre limité d'États, ainsi qu'une partie de la doctrine anglo-saxonne, le combattent tandis que certains pays en développement craignent que celui-ci, combiné à des théories hasardeuses telles que la théorie « *unwilling or unable* », pourrait les exposer à de douloureuses aventures.

Un auteur remarquait récemment que « *States are not generally fond of the due diligence principle because it places some amount of Responsibility on them* » (195). Nous espérons que cet article aura permis de repousser l'essentiel

(192) Voy. http://edition.cnn.com/2014/12/21/politics/obama-north-koreas-hack-not-war-but-cyber-vandalism/index.html.

(193) *Cf.* http://edition.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-white-house/index.html.

(194) *Supra*, note 11.

(195) E. Talbot Jensen, « The Tallinn Manual 2.0: Highlights ans Insights », J. Reuben Clark Law School, Brigham Young University, Research Paper, n° 17-10, p. 11.

de ces objections et démontré certaines contradictions inhérentes à leurs discours — tel que le refus de l'existence d'une obligation de diligence en matière de cyberattaque et l'affirmation paradoxale dans le même temps, d'un droit de recours à la force sur la base de la théorie « *unwilling or unable* ». Nous espérons aussi que cette étude pourra dissiper certains malentendus quant au « fardeau » que pourrait faire peser la due diligence sur les États, notamment les plus faibles. Mais, bien sûr, tous les problèmes sont loin d'être résolus, le chantier dans ce domaine reste immense et de nombreuses recherches, réflexions et échanges sont encore nécessaires pour construire un régime juridique convaincant et acceptable par tous.