Articles

—

L'espionnage en temps de paix en droit international public

IÑAKI NAVARRETE

Résumé

Avec la récente affaire d'espionnage *Timor-Leste c Australie* portée devant la Cour internationale de justice, les opérations de cyberespionnage telle GhostNet ou encore la mise sur écoute d'Angela Merkel, déterminer le statut de l'espionnage en temps de paix (ETP) est devenu un enjeu pressant. Or, celui-ci ne fait l'objet d'aucune définition et encadrement précis en droit international. La doctrine demeure quant à elle plutôt silencieuse. Face à cette situation, il est nécessaire de déterminer la légalité de l'ETP par un examen poussé des notions classiques du droit international public. C'est ce que la présente contribution tente de réaliser.

Mots-clés: espionnage en temps de paix; *Timor-Leste c Australie*; droit à la non-ingérence dans les communications; égalité souveraine; cyberespionnage.

Abstract

With the *Timor-Leste v Australia* spying scandal before the International Court of Justice, cyber espionage operations like GhostNet and the wiretapping of German chancellor Angela Merkel, legal questions on the legality of peacetime espionage arise. Peacetime espionage, however, is almost completely unregulated by international law and has no agreed upon legal definition. Scholarly work on this matter is scarce. Against this background, there is critical need for an in-depth public international law assessment of peacetime espionage. This article analyzes this very issue and examines the legality of peacetime espionage in light of classical notions of public international law.

Keywords: peacetime espionage; *Timor-Leste v Australia*; right of non-interference in communications; sovereign equality; cyber espionage.

Iñaki Navarrete (BCL/LLB, 2016) Faculté de droit de l'université McGill. Le présent texte est inspiré, pour partie, et a été bonifié s'agissant des droits de la personne, par ma participation au concours de procès simulé en droit international Charles-Rousseau 2015. Je tiens à cet égard à remercier le professeur René Provost, Sarah Berger Richardson et Alex O'Reilly, des mentors d'exception, ainsi que Pierrick Rouat, pour leurs précieux commentaires et suggestions sur les versions antérieures de ce texte. Toutes les erreurs sont les miennes.

Vol. 53 [2015], doi:10.1017/cyl.2016.16

Introduction

Les États s'espionnent les uns et les autres; mais ils le savent tous. Au cours des dernières années, plusieurs affaires d'espionnage intéressant le droit international ont montré le caractère universel et omniprésent de cette activité conduite par les États, depuis la mise sur écoute d'Angela Merkel par l'agence américaine NSA mise à jour par les révélations Snowden,[1] jusqu'au cyberespionnage industriel chinois des entreprises américaines,[2] en passant par l'écoute d'un arbitre par la Croatie dans un différend terrestre et maritime l'opposant à la Slovénie.[3] Mais autant les États aiment à cacher leurs secrets et intrigues en réprimant l'espionnage dans leurs ordres juridiques internes, autant la question de la légalité de l'espionnage en temps de paix (ETP) n'est pas tranchée en droit international. Cette situation peut sembler paradoxale. Pour certains auteurs, l'ETP serait un fait internationalement illicite, car il impliquerait par définition une violation de la souveraineté territoriale. Pour d'autres, les actes d'espionnage ne seraient pas interdits en droit international, et participeraient tout au plus des actes inamicaux entre États. Selon nous, la prise en compte de la pluralité des formes de l'ETP conduit à une image beaucoup plus nuancée: l'ETP est une activité *a priori* licite, s'autorisant du principe de liberté des États, que des règles hétérogènes prohibent dans certains cas bien précis.

Écrire sur le statut l'espionnage en droit international, c'est donc forcément faire sourciller. Pour les juristes, sa principale caractéristique est justement d'être un phénomène "extralégal."[4] À l'exception du droit international humanitaire (DIH), aucun corps de règles ne traite directement de la légalité de l'espionnage — c'est-à-dire, du caractère conforme de l'espionnage au droit international.[5] Même le droit diplomatique, dont les missions diplomatiques peuvent pourtant être de vrais "nids d'espions,"

[1] Nicolas Barotte, "En Allemagne, le scandale de la NSA empoisonne Merkel depuis deux ans" (24 juin 2015) *LeFigaro.fr*, en ligne: <http://www.lefigaro.fr/international/2015/06/24/01003-20150624ARTFIG00126-en-allemagne-le-scandale-de-la-nsa-empoisonne-merkel-depuis-deux-ans.php>.

[2] Le Monde, "Le FBI accuse la Chine de cyberespionage à grande échelle" (10 juin 2014) *LeMonde.fr*, en ligne: <http://www.lemonde.fr/international/article/2014/10/06/le-fbi-accuse-la-chine-de-cyberespionnage_4500894_3210.html>.

[3] Arman Sarvarian & Rudy Baker, "Arbitration between Croatia and Slovenia: Leaks, Wiretaps, Scandal" (28 juillet 2015) *EJIL: Talk!*, en ligne: <http://www.ejiltalk.org/arbitration-between-croatia-and-slovenia-leaks-wiretaps-scandal/#more-13476>.

[4] John Kish, *International Law and espionnage*, Cambridge, Martinus Nijhoff Publishers, 1995 à la p 83.

[5] Jean Salmon, dir, *Dictionnaire de droit international public*, Bruxelles, Bruylant, 2001 à la p 554.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

ne traite de l'espionnage qu'indirectement, toujours en tournant autour du pot.[6] L'ETP apparait alors comme une notion sans réelle portée juridique, destinée à se maintenir dans les interstices des relations interétatiques. Telle une forêt vierge et dense, le droit de l'espionnage résiste à l'appréhension. Reste qu'il est grand temps de réexaminer la question de l'ETP, de défricher, pour ainsi dire, cette province "si touffue, si encombrée d'éléments complexes"[7] du droit international.

On peut constater deux faits importants qui précipitent une telle entreprise. En premier lieu, le renseignement est porteur de vives tensions entre les États, qui s'avèrent être plus marquées dans un contexte de lutte contre le terrorisme. Ayant d'abord constitué une pratique refoulée, les États ont institutionnalisé et utilisé leurs services de renseignement ouvertement dès la seconde moitié du XXe siècle.[8] Et quoique le renseignement présente une importance grandissante sur les relations interétatiques depuis les événements du 11 septembre 2001, notamment au sein des forums multilatéraux tels les Nations-Unies,[9] la notion demeure indéfinie. En second lieu, la récente affaire des *Questions concernant la saisie et la détention de certains documents et données (Timor-Leste c Australie)* vient jeter un éclairage nouveau sur l'espionnage avec des questions tout à fait nouvelles en droit international public (DIP).[10] L'affaire présenterait un droit qui n'a pas de précédent, et qui traite d'un problème que la doctrine classique n'a jamais considéré, pour la simple raison qu'aucun État n'a protesté formellement dans le passé. Il s'agit du droit à la non-ingérence dans les communications qu'entretiennent les États avec leurs avocats, un droit qui pourrait prohiber une facette de l'espionnage de communications privilégiées.

Ces deux faits nous invitent à reconsidérer le statut de l'espionnage par un examen poussé des notions classiques du DIP. À ce titre, plusieurs interrogations restent en suspens. Peut-on dégager une définition juridique de l'ETP? Celui-ci constitue-t-il une activité contraire au droit international? Si non, qu'en est-il de certaines de ses incarnations, tel le cyberespionnage? Qu'en est-il de la cyber reconnaissance? Un État peut-il intercepter les communications d'un autre État avec ses conseillers juridiques? L'ambition principale des présentes sera de tenter de répondre à ces questions. Pour ce faire et examiner le contenu de la notion d'ETP, le texte

[6] Kish, *supra* note 4 à la p 8.

[7] Cohen-Jonathan Gérard & Robert Kovar, "L'espionnage en temps de paix" (1960) 6 AFDI 239 à la p 240.

[8] Simon Chesterman, "The Spy Who Came in from the Cold War: Intelligence and International Law" (2006) 27 Mich J Int'l L 1071 à la p 29.

[9] *Ibid.*

[10] *Questions concernant la saisie et la détention de certains documents et données (Timor-Leste c Australie)*, Ordonnance du 3 mars 2014 [2014] CIJ [*Affaire Timor-Leste c Australie*].

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

privilégie une approche positiviste. Ce recours se justifie parce que l'étude du statut de ces formes d'espionnage, en droit positif, demeure à entreprendre dans la littérature.

Le texte abordera le statut de l'espionnage en temps de paix à travers quatre parties distinctes. Il faut, pour préciser l'analyse, commencer par interroger la notion même d'espionnage en droit. La première partie est consacrée à l'étude de la notion d'espionnage, que nous tenterons de débroussailler à partir des références discrètes qui émaillent le DIP général et de quelques précisions techniques. La deuxième partie traite du principe de liberté du *Lotus* qui pose que les actes non prohibés par le droit international, dont l'espionnage, sont licites. Ce principe constituera le point d'ancrage de notre étude. Cet échelon de compréhension atteint, la troisième partie tente de déterminer la licéité de l'ETP au regard de trois branches majeures du DIP: la souveraineté étatique, les droits de la personne et le droit diplomatique. Enfin, dans la quatrième et dernière partie nous tenterons de déterminer la licéité de l'espionnage à l'aune des nouveaux droits allégués par le Timor-Leste dans l'affaire *Timor-Leste c Australie*.

L'impact des nouvelles normes sur l'espionnage seront alors discutées, et les difficultés, en termes de détermination du statut, exposées. Dans cette optique, cette étude nous conduira à mettre en évidence une légalité à géométrie variable, non exempte de contradictions. Si la légalité du cyberespionnage et de la cyber reconnaissance semble s'affirmer au regard des normes émergentes du DIP, nous montrerons qu'un droit à la non-ingérence dans les communications entre un État et ses avocats émerge du principe d'égalité souveraine et du principe de règlement pacifique des différends. L'espionnage des communications d'un État et ses avocats par un autre État serait illicite quand ceux-ci sont engagés dans le règlement d'un différend international.

L'espionnage en temps de paix: une notion à l'épreuve du droit

Notre travail de défrichage s'amorce par la quête d'une définition. Il n'existe, en DIP, aucun consensus autour d'une définition conventionnelle de l'ETP, en raison de la diversité des modalités de celui-ci et des enjeux politiques d'une telle définition. Cette absence même de référence juridique explicite indique que les États n'ont pas souhaité s'imposer de contraintes, fussent-elles réciproques, en la matière.[11] Il reste néanmoins possible d'esquisser une définition de l'ETP à partir des références discrètes présentes en temps de paix et du DIH. Il conviendra ensuite de préciser l'aspect technique de cette notion.

[11] Olivier Forcade & Sébastien Laurent, *Secrets d'État: pouvoirs et renseignent dans le monde contemporain*, Paris, Armand Colin, 2005 à la p 66.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

DES RÉFÉRENCES JURIDIQUES DISCRÈTES EN TEMPS DE PAIX

À notre connaissance, seules trois références obliques et ponctuelles à l'espionnage existent en temps de paix. Nous tenterons d'en tirer des éléments de définition constitutifs de l'espionnage. Les auteurs qui ont cherché la nature juridique de l'ETP se sont jusqu'ici inspiré de l'ordre juridique interne des États vu le caractère bancal de ces références.[12] D'après nous, cependant, seule la référence aux outils du DIP et du DIH permettra de dégager une définition satisfaisant toute la rigueur de l'analyse que requiert la détermination du statut de l'espionnage.

Une première référence se trouve en droit diplomatique pour les activités des agents diplomatiques (une sphère importante d'espionnage) se trouvant dans l'État d'accueil. Les agents diplomatiques jouissent de plusieurs immunités et exercent plusieurs fonctions. L'article 3(1)(d) de la *Convention de Vienne sur les relations diplomatiques* (*CVRD*) précise très clairement que l'une des fonctions de ces agents est de "s'informer par tous les moyens *licites* des conditions et de l'évolution des événements" dans l'État d'accueil. Ainsi, il appert qu'une "définition par omission existe sur l'espionnage en droit international — mais uniquement s'agissant de l'espionnage par les agents diplomatiques — soit celle d'informations recueillies par des moyens illicites."[13] Le droit diplomatique ne va pas beaucoup plus loin que cela. D'ailleurs, c'est un lieu commun d'indiquer que les agents diplomatiques se livrant à l'espionnage par des moyens illicites et découverts par l'État d'accueil sont promptement déclarés *persona non grata* pour "activité non conforme au statut diplomatique." Les États se gardent de parler d'espionnage.

Une seconde référence discrète existe dans le droit de la mer avec la notion de passage inoffensif des navires dans la mer territoriale. Contrairement au droit international aérien qui oblige tout aéronef d'un État étranger à obtenir l'autorisation préalable de l'État survolé, le droit de la mer accorde à tout navire de guerre un droit de passage inoffensif dans la mer territoriale d'un État tiers.[14] D'après l'article 19(2)(c) de la *Convention de Montego Bay* de 1982, le fait, pour un navire, de se livrer "à la collecte de renseignements au détriment de la défense ou de la sécurité de l'État côtier" constitue une conduite constitutive d'un passage non inoffensif qui viole le droit international.[15] On remarquera que le droit de la mer reste le plus discret possible sur la notion d'ETP. Comme l'indique un auteur, la convention n'interdit la collecte de renseignement que pour enlever

[12] Gérard & Kovar, *supra* note 7 à la p 240.

[13] *Ibid* à la p 67.

[14] Fabien Lafouasse, "L'espionnage en droit international" (2001) 47 AFDI 63 à la p 69.

[15] *Convention des Nations Unies sur le droit de la mer*, 10 décembre 1982, 1834 RTNU 4.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

son caractère "innocent" au passage dans la mer territoriale; elle ne dit rien quant à la légalité ou la définition juridique de l'espionnage.[16] L'État victime d'une violation de ses eaux territoriales aux fins de collecte de renseignement pourra ainsi seulement exiger que ce navire quitte ses eaux territoriales[17] en alléguant une violation territoriale. Comme en diplomatie, de tels incidents se règlent par une approche politique qui semble se payer de mots.

Cette impression est confirmée par les travaux préparatoires de l'article 19(2)(c). Lors des débats préparatoires de 1973 sur la convention, les iles Fidji présentèrent un projet d'articles qui énumérait une liste d'activités susceptibles d'êtres considérées comme portant atteinte à la paix, au bon ordre ou à la sécurité de l'État riverain, parmi lesquelles se trouvaient à l'alinéa (f) les "actes d'espionnage."[18] Il est intéressant de constater que l'expression "actes d'espionnage" fut gommée de la version finale de la *Convention de Montego Bay*. Cela tient certainement au fait que l'expression "collecte de renseignement" apparait plus neutre. On remarquera en outre que l'expression est certainement plus large que l'expression stricte "espionnage", dans la mesure où elle couvre tant les activités clandestines (telles que l'interception de communications) que les activités non clandestines (telles que l'utilisation de jumelles sur le pont d'un navire).[19] Cette seconde référence ne permet donc pas, à elle seule, de mieux cerner la notion d'ETP.

Une dernière référence à l'espionnage existe enfin en matière de lutte antiterroriste avec le concept de renseignements. Les évènements du 11 septembre 2001, ainsi que les attaques ultérieures perpétrées à Madrid, Londres, Bali, Amsterdam et plus récemment les attentats de novembre 2015 à Paris, ont fait ressortir l'importance de lutter contre le terrorisme à l'échelle internationale. À la suite des attentats du 11 septembre 2001, le Conseil de sécurité adopta ainsi à l'unanimité la résolution 3173,[20] qui oblige tous les États à "trouver des moyens d'intensifier et d'accélérer l'échange d'informations opérationnelles"[21] et "d'échanger des renseignements conformément au droit international et national" afin de prévenir

[16] Michel Voelckel, "Raison d'État en droit de la mer: quelques constats et commentaires" (2002) tome VII, ADM à la p 275.

[17] Carlos Espaliú Berdud, *Le passage inoffensif des navires de guerre étrangers dans la mer territoriale*, Bruxelles, Bruylant, 2007 à la p 42.

[18] *Ibid* à la p 42.

[19] Fabien Lafouasse, *L'espionnage dans le droit international*, Paris, Nouveau Monde, 2012 à la p 279.

[20] Résolution 3173, Doc off CS NU, 4385^{e} sess (2001) art 2b)-3a); Résolution 1269, Doc off CS NU, 4053^{e} sess (1999).

[21] *Ibid* art 2(3).

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

les actes de terrorisme.[22] Encore une fois, la définition du renseignement (tout comme celle du terrorisme) fut gommée de la résolution. Assurément, une résolution aussi exceptionnelle ne put d'ailleurs être adoptée qu'à cause des circonstances tragiques dans laquelle elle s'inscrivait, et précisément parce qu'elle se garde bien de définir des concepts aussi controversés.[23] Cette tactique législative se perçoit également en droit pénal international[24] et dans certains traités économiques multilatéraux[25] qui font référence au droit des États de refuser de fournir ces renseignements dont la divulgation serait contraire à la sécurité nationale.[26] Nous constatons ainsi que si le DIP emploie parfois la notion de renseignements, c'est uniquement pour en laisser le contenu à l'initiative des États.[27]

Partant, ces trois références obliques à l'espionnage renforcent l'idée selon laquelle les États font tout leur possible pour résoudre politiquement plutôt que juridiquement les conflits surgissant de l'ETP. Ils suivent en ce sens une "stratégie d'évitement."[28] Cette stratégie d'évitement consiste à contourner toute résolution juridique d'un différend né d'un acte d'espionnage en le rattachant à des normes tirées d'autres branches du DIP (droit de la mer, droit aérien, droit diplomatique, etc.), qui n'ont pourtant avec ce dernier qu'un rapport lointain.[29] Plus encore, les États évitent d'entamer tout débat juridique sur l'espionnage afin d'empêcher la formation d'*opinio juris*. Ils caractérisent l'espionnage par des euphémismes ("passage non inoffensif", "activité non conforme au statut diplomatique") qui n'emportent aucune qualification juridique. Il faudra garder ce fait en mémoire au moment d'étudier la licéité de l'ETP.

Bref, concept très fuyant, c'est sciemment que les États n'ont pas défini l'ETP en droit conventionnel. L'espoir a toujours été déçu de dégager une

[22] *Ibid* art 3(1).

[23] Simon Chesterman, *Shared Secrets: Intelligence and Collective Security*, Sydney, Lowy Institute for International Policy, 2006 à la p 55.

[24] On retrouve ce même phénomène de protection des secrets d'État en droit pénal international. Comme l'indique Sipowo: "C'est ce qu'évoque explicitement l'article 72 du *Statut de Rome* en faisant nommément référence aux 'renseignements touchant la sécurité nationale' … Très peu d'instruments multilatéraux évoquent aussi explicitement la sécurité nationale par la protection de secrets des renseignements" dans Alain-Guy Tachou Sipowo, *La Cour pénale internationale et le secret: de l'atténuation de la confidentialité au nom de l'impératif d'effectivité*, thèse de doctorat en droit, Université Laval, 2014 [non publiée] à la p 211.

[25] *Ibid* à la p 211.

[26] *Ibid* à la p 212.

[27] Lafouasse AFDI, *supra* note 14 à la p 96.

[28] Lafouasse, *supra* note 19 à la p 309.

[29] Leslie Edmonson, "Espionage in Transnational Law" (1971) 5:2 Vand J Transnat'l L 434 à la p 446.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

définition à partir de ces seules références, raison pour laquelle nous nous tournons à présent vers le droit international humanitaire.

LE CONCEPT D'ESPIONNAGE EN TEMPS DE CONFLITS ARMÉS

Le droit international humanitaire (DIH) est bien plus clair. Malgré l'absence de pratique étatique contemporaine pour étayer notre analyse,[30] deux types de sources du DIH contribuent à fouiller le concept d'espionnage: d'une part, les conventions internationales, et d'autre part, les manuels de guerre, dont le récent Manuel de Tallinn. Une précision d'ordre méthodologique s'impose. Il faudra se garder de transposer directement au temps de paix, *mutatis mutandis*, la définition juridique de l'espion du DIH.[31] En effet, la comparaison des deux espionnages est incorrecte au plan méthodologique pour plusieurs raisons. Contrairement au temps de paix, l'espionnage en temps de conflits armés est licite et fortement encadré par des règles issues de nombreuses conventions, et ce depuis la seconde moitié du XIXe siècle. Qui plus est, la définition de l'espion du DIH fait appel à des notions particulières,[32] telles que les "zones d'opération militaire" ou "l'ennemi" qui sont des notions étrangères à l'ETP.[33] Sans parler du fait que la définition de l'espion en DIH date d'un autre siècle, ce qui nous amènera à étudier le récent Manuel de Tallinn.

L'acte d'espionnage perpétré au cours d'un conflit armé est assimilé à une ruse de guerre, soit à un acte licite de combat.[34] La plus ancienne définition codifiée de l'espion est formulée à l'article 88 du code Lieber de 1863 comme "une personne qui, en secret, déguisée ou sous une fausse identité, recherche des renseignements avec l'intention de les communiquer à l'ennemi."[35] De même, l'article 29 du *Règlement de La Haye de*

[30] Voir Marco Sassòli, Antoine Bouvier & Anne Quintin, *Un droit dans la guerre?*, 2e éd, CICR, 2012 à la p 1052; voir également Jean-Marie Henckaerts & Louise Doswald-Beck, *Customary International Humanitarian Law*, Cambridge, Cambridge University Press, ICRC, 2005 à la p 2561.

[31] Gérard & Kovar, *supra* note 7 à la p 242.

[32] *Ibid* à la p 243.

[33] Moins utile toutefois est la notion de "zone d'opération d'un belligérant." Ce critère *ratione loci* s'étend essentiellement à tout territoire contrôlé par la partie adverse, ou, autrement dit, du coté ennemi de la ligne de front, comme l'indiqua plus tard l'article 46(2) du *Protocole additionnel I*. Le parallèle avec le droit de la guerre montre ici ses limites, d'autant que cette définition de 1907 est depuis longtemps périmée: elle a été élaborée sans pouvoir envisager, par exemple, des nouveaux moyens comme le cyberespionnage. Évidemment, l'ETP obéit à un tout autre type de division territoriale, soit l'espace national et les espaces internationaux. Le conflit armé transcende cette distinction pour suivre les principaux lieux d'hostilités. Cet élément n'est donc pas recevable en temps de paix.

[34] Lafouasse, *supra* note 19 à la p 47.

[35] *Ibid* à la p 46.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

1907 donne une définition conventionnelle de l'espionnage en temps de guerre sur un mode restrictif et négatif.[36] Ainsi:

> Ne peut être considéré comme espion *que* l'individu qui, *agissant clandestinement ou sous de faux prétextes*, recueille ou cherche à recueillir des informations dans *la zone d'opérations d'un belligérant, avec l'intention de les communiquer à la Partie adverse.*
>
> Ainsi les militaires *non déguisés* qui ont pénétré dans la zone d'opérations de l'armée ennemie, à l'effet de recueillir des informations, *ne sont pas considérés comme espions*. De même, *ne sont pas considérés comme espions*: les militaires et les non militaires, accomplissant *ouvertement* leur mission, chargés de transmettre des dépêches destinées, soit à leur propre armée, soit à l'armée ennemie. À cette catégorie appartiennent également les individus envoyés en ballon pour transmettre les dépêches, et, en général, pour entretenir les communications entre les diverses parties d'une armée ou d'un territoire (nous soulignons).[37]

L'article 29(1) circonscrit le concept d'espion autour de son mode opératoire, soit le fait d'agir *clandestinement* ou *sous de faux prétextes* dans une zone d'opération. L'article 29(2) vise quant à lui à protéger certaines catégories de personnes afin qu'elles ne soient pas considérées comme des espions.[38] Les critères qui résultent de cette définition, par un raisonnement *a contrario*, sont: (1) le mode opératoire, clandestin ou sous de faux prétextes; et (2) l'élément personnel, à savoir que l'espionnage s'effectue au détriment de l'État sur la zone militaire duquel l'espionnage à lieu. En revanche, le *Règlement de La Haye*, les autres conventions, tout comme les manuels militaires, ne précisent pas ce que signifie le concept "d'informations" — soit l'objet de l'espionnage. Par suite, ce critère est subjectif puisqu'il laisse aux États parties au conflit le soin de déterminer quelles sont les informations visées par la disposition.[39] Mode opératoire clandestin ou sous de faux prétextes, élément personnel et objet: ces trois critères sont recevables en temps de paix. D'ailleurs, l'article 46(2) du *Premier Protocole additionnel aux Conventions de Genève* confirme la pertinence de l'élément de clandestinité:

> Un membre des forces armées d'une Partie au conflit qui recueille ou cherche à recueillir, pour le compte de cette Partie, des renseignements dans un territoire contrôlé par une Partie adverse *ne sera pas considéré comme se livrant à des*

[36] Kish, *supra* note 4 à la p 133.

[37] *Convention (IV) concernant les lois et coutumes de la guerre sur terre, Annexe: Règlement concernant les lois et coutumes de la guerre sur terre — Section II — des hostilités, Chapitre II des espions*, La Haye, 18 octobre 1907, art 29.

[38] Lafouasse, *supra* note 19 à la p 47; Kish, *supra* note 4 à la p 144.

[39] *Ibid* à la p 48.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

activités d'espionnage si, ce faisant, il est revêtu de l'uniforme de ses forces armées (nous soulignons).[40]

Au-delà de ces conventions internationales d'antan, les manuels de guerre contemporains nous guident dans la définition du concept d'ETP.[41] Le Manuel de Tallinn en particulier, un guide rédigé en 2013 par un groupe d'experts mandatés par l'OTAN, constitue un développement intéressant pour définir l'espionnage. Le Manuel propose une transposition du DIH que nous venons d'examiner aux nouveaux cyberconflits, son but étant d'apporter "un certain niveau de clarté aux difficultés juridiques complexes entourant les cyberopérations, avec une attention particulière à celles relatives au *jus ad bellum* et au *jus in bello*."[42] Dans ce cadre, les experts ont pu aborder le concept juridique d'espionnage, en soulignant qu'il n'était pas défini en temps de paix.[43] Le Manuel élabore néanmoins une définition opérationnelle du cyberespionnage à partir de l'article 29 du *Règlement de La Haye*. Le cyberespionnage y est défini de manière étroite comme "any act undertaken clandestinely or under false pretences that uses cyber capabilities to gather or attempt to gather information with the intention of communicating it to the opposing party."[44] Deux critères sont ici mis en exergue: le mode opératoire, clandestin ou sous de faux prétexte, et l'élément personnel. La majorité des experts étaient en outre d'avis que l'objet du cyberespionnage (soit la nature des informations recueillies, militaires ou non) n'avait aucune incidence sur qualification du cyberespionnage.

Christopher Yoo constate un fait plus révélateur encore: le Manuel distingue clairement le cyberespionnage au sens strict d'autres activités, comme le *computer network exploitation* (CNE) et la cyber reconnaissance, qui sont conduites *hors* du territoire de l'ennemi.[45] Celles-ci se définissent comme "the use of cyberspace capabilities to obtain information about enemy activities" depuis le *territoire national*.[46] Pour les experts, ces activités ne sont même pas du cyberespionnage, car l'espionnage implique par définition une intrusion sur le territoire de l'État belligérant. Aux fins de notre

[40] *Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux*, 8 juin 1977, ICAO Doc [*Protocole I*].

[41] Sassòli, *supra* note 30 à la 1054.

[42] Michael N Schmitt, dir, *Tallinn Manual on the International Law Applicable to Cyber-Warfare*, Cambridge, Cambridge University Press, 2013 à la p 18.

[43] *Ibid* à la p 18.

[44] *Ibid* à la p 159.

[45] Christopher Yoo, "Cyber Espionage or Cyber War?: International Law, Domestic Law and Self-Protective Measures" (2015) 15:3 U PA L Rev 1 à la p 26.

[46] *Ibid* à la p 12.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

analyse, le critère *ratione loci* indiqué ici est crucial. Recevable en temps de paix, il rappelle l'importance d'une distinction entre l'espace national et les espaces internationaux.

En somme, le droit international est presque entièrement silencieux sur l'ETP, les États procédant à une véritable stratégie d'évitement. Par contraste, l'espionnage est bien défini en DIH. Combinant les définitions retenues par le DIH avec les éléments soulevés en temps de paix, on peut esquisser les grands traits d'une définition juridique de l'ETP de la manière suivante: il s'agit de l'acte par lequel un État recueille (ou cherche à recueillir), pour son bénéfice et au détriment d'un autre État, des renseignements (de tout ordre), en opérant de manière clandestine ou sous de faux prétextes, sur le territoire ou non du second. Nous adoptons donc une définition large du concept. Cette définition nous permettra, tout au long de cette recherche, de situer l'espionnage parmi d'autres pratiques distinctes afin d'en déterminer la licéité. Pour plus de clarté, concentrons-nous pour finir sur l'aspect technique du concept.

TYPOLOGIE DES MOYENS ET TYPOLOGIE GÉOGRAPHIQUE

Il importe, à l'orée de ce texte, de comprendre "que la circulation de l'information et du renseignement est au premier chef une question d'ordre technique."[47] La technologie est en effet l'un des principaux moteurs de la révolution des services de renseignements du XX^e^ siècle.[48] La discipline du *signals intelligence* est née avec l'avènement de la radio peu avant la Première Guerre mondiale, alors que celle de l'*imagery intelligence* ("imint") a été propulsée peu après par l'invention des aéronefs. En ce début XXI^e^ siècle, nous mesurons encore les effets de la révolution informatique et de la révolution Internet sur les services de renseignements, l'*open source* offrant d'innombrables informations perméables à la collecte massive.[49] Logiquement, nous devrons donc intégrer régulièrement cette dimension technique des moyens de collecte du renseignement dans notre étude sur la licéité de l'espionnage.

Sur le plan des moyens, il nous faut distinguer entre deux moyens principaux de collecte d'information, soit: (1) l'interception des signaux par divers moyens d'écoute ("sigint," comme l'abrègent les services secrets) et (2) la collecte de renseignements effectuée par des agents des services de renseignements ("humint"). La part *sigint* du renseignement ne cesse de croitre depuis Internet et les agences recueillent aujourd'hui la majorité

[47] Forcade, *supra* note 11 à la p 42.

[48] Wesley K Wark, "Learning to Live with Intelligence" dans Wesley K Wark, dir, *Twenty-First Century Intelligence*, New York, Routledge, 2005 à la p 2.

[49] *Ibid* à la p 3.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

de leurs renseignements par cette voie.[50] À titre d'illustration, il est apparu que certains États pouvaient piger dans les câbles subaquatiques par où transitent la majorité des communications internationales à l'aide de sous-marins,[51] alors que ces câbles avaient longtemps semblé hors d'atteinte de telles interférences. Vu cette prédominance du *sigint* dans la pratique actuelle des États, nous concentrerons l'essentiel de notre étude sur ces nouvelles formes d'espionnage que sont l'interception des télécommunications et le cyberespionnage.

À travers les pages qui précèdent, il est aussi apparu que le *lieu* de l'interception des communications constitue un critère crucial. Reprenant ici la typologie géographique élaborée par Craig Forcese, on distinguera schématiquement trois types d'espionnage:[52] (1) l'espionnage territorial, qui se réalise entièrement sur le territoire de l'État-espion; (2) l'espionnage extraterritorial, qui désigne l'espionnage se réalisant depuis le territoire national de l'État-espion, mais dans lequel la collecte de l'information s'opère en tout ou en partie sur le territoire de l'État victime; et, enfin, (3) l'espionnage transnational, pour désigner l'espionnage dans lequel l'interception de l'information se réalise hors du territoire de l'État victime d'où provient l'information. Rendons dès maintenant cette typologie géographique un peu plus concrète.

Premièrement, l'espionnage peut être simplement *territorial*, dans lequel cas il se déroule entièrement sur le territoire de l'État-espion. Un bon exemple se présente à travers l'espionnage par l'État d'accueil des diplomates étrangers qui se trouvent sur son territoire. Deuxièmement, l'espionnage peut être *extraterritorial*. Dans ce cas de figure, l'État-espion ne limite pas l'espionnage à son seul territoire, mais procède à des collectes de données sur le territoire d'autres États au risque de voir sa responsabilité internationale engagée. Le fait, pour un État, de mobiliser des espions sur le territoire de l'État victime, constitue un exemple d'espionnage extraterritorial. Il en va de même lorsque l'État-espion emploie des bâtiments-espion (navire d'État, sous-marin, chalutier, etc.) ou des aéronefs-espion. Tous ces cas comportent une forme d'extraterritorialité, ce qui pose le problème de leur légalité au regard du DIP. Quoiqu'on puisse s'attendre à une réponse uniforme, nous montrerons plus loin qu'en fonction des moyens employés, l'espionnage extraterritorial possède une licéité à géométrie variable.

Troisièmement, l'espionnage *transnational* se réalise sur le territoire même de l'État-espion ou dans les espaces internationaux s'agissant d'information provenant de l'État victime. L'espionnage transnational

[50] *Ibid* à la p 43.

[51] Duncan Campbell, *Surveillance électronique planétaire*, Paris, Allia, 2001 à la p 54.

[52] Sur cette typologie, voir Craig Forcese, "Spies without Borders: International Law and Intelligence Collection" (2011) 5:179 J Nat'l Sec L & Pol'y 179 à la p 205.

prend naturellement la forme de *sigint*, au sens où des communications peuvent être interceptées d'un peu partout. À cet égard, le réseau baptisé Échelon constitue assurément l'exemple le plus connu d'espionnage *sigint* transnational.[53] Ce système multilatéral serait exploité par les États-Unis, en collaboration avec la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande, en vertu d'un accord secret appelé UKUSA signé à la fin des années 1940.[54] Bien qu'on dispose de peu d'information sur Échelon, celui-ci serait en mesure d'intercepter toutes les communications par satellites et de les filtrer grâce à des ordinateurs très puissants, par l'utilisation de mots-clefs prédéfinis et des techniques de reconnaissance vocale.[55] L'interception de ces communications se réaliserait donc vraisemblablement dans l'espace extra-atmosphérique ou dans le territoire de l'État-espion, un fait que les concepts territoriaux du DIP peinent à accommoder. Nous reviendrons sur ce point dans la troisième partie de l'article.

Le Tableau 1 ci-dessous résume les présents développements techniques. En nous situant dans la perspective esquissée dans cette première Partie, nous sommes mieux équipés pour déterminer la licéité d'un acte aussi diffus et protéiforme que l'espionnage. Comme nous le montrerons à l'instant dans la Partie II, le principe du *Lotus* constitue le point d'ancrage de la présente étude; c'est à celui-ci que nous reviendrons toujours.

Le principe du *lotus:* de la liberté des états de s'espionner

Ce qui n'est pas formellement interdit est juridiquement permis.[56] C'est dans un *dictum* fort célèbre rendu par la Cour permanente de Justice internationale (CPJI) dans *l'Affaire du "Lotus"* que fut posé le principe de liberté des États.[57] Cette liberté d'agir en dehors de toute règle préétablie est le principe fondamental du droit international. Il revient donc aux États non contents des actes d'un autre État de démontrer que celui-ci a consenti à ce que sa liberté soit tronquée ou qu'une règle prohibitive limite ces actes.[58]

[53] Campbell, *supra* note 51 à la p 21.

[54] Suisse, Chambres fédérales, Délégation des commissions de gestion, *Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports* (projet "Onyx") (10 novembre 2003) à la p 1386 [*Projet "Onyx"*].

[55] *Ibid* à la p 1385.

[56] Louis Cavaré, *Le droit international public positif*, Paris, Pedone, 1966; Stefan Talmon, "Kosovo: The ICJ Opinion — What Next ?" (2010) University of Oxford Document de travail, en ligne: <http://users.ox.ac.uk/~sann2029/ChathamH_kosovo_ICJ_Paper.pdf>.

[57] *Affaire du "Lotus" (France c Turquie)* (1927), CPJI (sér. A) nº 10 [*Affaire du"Lotus"*].

[58] Ashley Deeks, "An International Legal Framework for Surveillance" (2014) 55:2 Va J Intl L 292 à la p 301, en ligne: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490700##>; J. Stone, "Legal Problems of Espionage in Conditions of Modern Conflict" dans R.J. Stanger, *Essays on Espionage and International Law* à la p 33.

Tableau 1: Typologie géographique de l'espionnage de Forcese

Moyens	Territorial	Extraterritorial	Transnational
HUMINT	Collecte de renseignements par un agent étatique qui prend place sur le territoire national de l'État-espion	Collecte de renseignements par un agent étatique qui prend place sur le territoire de l'État victime	Collecte de renseignements par un agent étatique dans lequel la source des renseignements (mais non l'agent) se trouve sur le territoire de l'État victime
SIGINT	Interception de signaux ou communications transmises par divers moyens (émissions radio, câbles, courriers électroniques, etc.) et dans lequel tant le lieu d'origine que le lieu d'interception est le *territoire national* de l'État-espion	Interception de signaux ou communications transmises par divers moyens (émissions radio, câbles, courriers électroniques, etc.) et dans lequel tant le lieu d'origine que le lieu d'interception *est le territoire de l'État victime*	Interception de signaux ou communications transmises par divers moyens (émissions radio, câbles, courriers électroniques, etc.), dans lequel le lieu d'origine (*mais non celui l'interception*) est le territoire de l'État victime

La CPJI soutint en ce sens que les États restent libres "d'adopter les principes qu'ils jugent les meilleurs est les plus convenables."[59] Bien que le principe du *Lotus* ait pu être vivement critiqué par la doctrine[60] et par certains juges comme étant le reflet d'une conception ancienne et vieillie du droit international, le principe demeure d'actualité. Réaffirmé à plusieurs reprises dans la jurisprudence de la CIJ,[61] ce principe prend tout son rôle lorsqu'il n'existe pas de normes internationales régissant un pan des activités étatiques.[62] Puisque le droit international ne prohibe

[59] *Affaire du "Lotus," supra* note 57 à la p 19.

[60] Alain Pellet, "Lotus que de sottises on profère en ton nom: remarques sur le concept de souveraineté dans la jurisprudence de la Cour mondiale" dans *Mélanges en l'honneur de J.-P. Puissochet: L'État souverain dans le monde d'aujourd'hui*, Paris, Pedone, 2008 à la p 216.

[61] Voir notamment *Affaires du Sud-Ouest Africain (Éthiopie c Afrique du Sud), (Libéria c Afrique du Sud)*, 2e phase, [1996] CIJ rec au para 54 [*Affaires du Sud-Ouest Africain*]; *Affaire des Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c États-Unis d'Amérique)*, [1986] CIJ rec 392 au para 269 [*Affaire Nicaragua c États-Unis*].

[62] Deeks, *supra* note 58 a la p 36.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

pas la propagande, les opérations psychologiques ou les pressions économiques,[63] ces activités sont *a priori* licites.

Le principe du *Lotus* constituera naturellement le cadre de référence de cette étude sur l'ETP. Tel que nous l'avons démontré dans la Partie I de ce texte, l'absence même de référence au concept d'ETP montre que les États ne souhaitent pas s'imposer de contraintes conventionnelles en la matière.[64] L'espionnage ne parvient pas au demeurant à se loger dans la coutume ou dans la jurisprudence internationale; c'est ce que nous constaterons ici.

Il est généralement admis que l'existence d'une règle coutumière implique la réunion de deux éléments: un élément matériel qui consiste dans la répétition prolongée et constante d'une pratique, et un élément psychologique (*opinio juris*) qui consiste dans la croyance au caractère obligatoire de cette pratique par les États.[65] D'aucun soutiennent ainsi que l'espionnage possède une légalité coutumière du fait sa pratique longue et constante, à laquelle s'ajoute l'existence de services de renseignements jouant aujourd'hui une fonction étatique légitime au grand jour.[66] D'après nous, on ne peut compter pour rien cette pratique puisqu'elle ne s'accompagne généralement d'aucune manifestation d'*opinio juris* qui permettrait de valider la thèse de la coutume. Bien au contraire, "[s]tates regularly condemn spying conducted against them. And when they spy, they do so covertly — in part for effectiveness reasons but also in part to avoid condemnation and embarrassment."[67] Ce constat, Chesterman l'exprime éloquemment en faisant une revue de la pratique étatique: "[S]tate practice and *opinio juris* appear to run in opposite directions."[68]

[63] Schmitt, *supra* note 42 à la p 52.

[64] Geoffrey B Demarest, "Espionage in International Law" (1996) 24 Denv J Int'l L & Pol'y 321; Jordan J Paust, "Can You Hear Me Now?: Private Communication, National Security, and the Human Rights Disconnect" (2015) 15:2 Chicago J Int'l L 612 à la p 647; Roger D Scott, "Territorially Intrusive Intelligence Collection and International Law" (1999) 46 AFL Rev 217 à la p 224; A John Radsan, "The Unresoldved Equation of Espionage and International Law" (2007) 28 Mich J Int'l L 595 à la p 603.

[65] *Affaires du Plateau continental de la Mer du Nord (République fédérale d'Allemagne/Danemark; République fédérale d'Allemagne/Pays-Bas)*, [1969] CIJ Rec 3 au para 77; *Plateau continental (Jamahiriya arabe libyenne/Malte)*, [1985] CIJ Rec 13 à la p 30.

[66] Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013 à la p 438.

[67] Voir Craig Forcese, "The Federal Court's Prescience: Spying and International Law" (21 novembre 2013) *National Security Law* (blogue), en ligne: <http://craigforcese.squarespace.com/national-security-law-blog/2013/11/21/the-federal-courts-prescience-spying-and-international-law.html>.

[68] Chesterman, *supra* note 8 à la 1072.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

L'espionnage est donc une activité éminemment politique à l'épreuve du droit coutumier.

Cela explique certainement que la CIJ n'ait guère pris position sur la question de sa licéité, bien qu'elle en ait eu l'occasion à plusieurs reprises. Dans l'affaire des *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c États-Unis d'Amérique)*, le Nicaragua s'est plaint du passage d'aéronefs-espions américains dans son espace aérien aux fins de renseignement.[69] La CIJ s'est pourtant cantonnée à la violation de la souveraineté aérienne:[70] à aucun moment le sujet de la licéité de l'espionnage n'a-t-il été effleuré. De même dans l'affaire du *Personnel diplomatique et consulaire des Etats-Unis à Téhéran (Etats-Unis c Iran)*, le ministre des Affaires étrangères de l'Iran s'est référé aux pratiques d'espionnage menées par les diplomates américains sur leur territoire pour tenter de justifier le saccage de l'ambassade américaine.[71] La question de l'espionnage fut, encore une fois, contournée. Plus nettement, la CIJ aurait pu avoir à se prononcer sur l'espionnage dans l'affaire *Timor-Leste c Australie*, mais l'affaire ne fut jamais étudiée au fond, le Timor-Leste et l'Australie ayant convenu de rechercher un règlement à l'amiable.

L'espionnage est ainsi un sujet épineux à l'égard duquel la CIJ se montre très réticente. Sur ce point, l'attitude apaisante et la prudence évasive d'un avocat du Timor-Leste, Sir Elihu Lauterpacht, lors des représentations orales pour l'indication de mesures provisoires, sont très révélatrices:

> May I begin with a few words of reassurance — and I hope comfort — despite the circumstances surrounding the present case, *this is not a case about spying and espionage. The Court will not have to pronounce on such activities generally.* Rather, the case is a relatively simple one. One state has taken the property of another, and should be required to give it back, untouched and without delay (nous soulignons).[72]

Ce passage en dit long sur la manière dont se matérialise l'espionnage devant la CIJ: la Cour semble épouser la stratégie d'évitement des États. Mais que faut-il voir exactement dans cette attitude? La prudence observée ici par la CIJ mérite d'être expliquée plutôt que décriée. Insistons que la CIJ se trouve devant une stratégie d'évitement étatique où les références conventionnelles discrètes et *l'opinio juris* portant sur l'espionnage

[69] *Affaire Nicaragua c États-Unis*, *supra* note 61 au para 21.

[70] *Ibid* au para 91, 251 et 252.

[71] *Affaire relative au personnel diplomatique et consulaire des États-Unis à Téhéran (États-Unis d'Amérique c Iran)*, [1980] CIJ rec au para 85 [*Affaire Téhéran*].

[72] *Questions concernant la saisie et la détention de certains documents et données (Timor-Leste c Australie)*, Ordonnance du 3 mars 2014 [2014] CIJ, Exposé oral de Sir Elihu Lauterpacht à la p 16.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

laissent très peu de manœuvre aux juges, qui doivent se cantonner aux sources du droit énumérées à l'article 38 du *Statut de la Cour internationale de Justice* (*Statut de la CIJ*). La possibilité de créativité judiciaire peut difficilement s'exprimer dans ce contexte d'ETP. Sauf rare exception, on s'aperçoit d'ailleurs que les tribunaux nationaux et organisations internationales, telle l'Organisation mondiale du commerce (OMC), suivent cette même ligne de conduite.[73]

À cet égard, il devient urgent de faire une remarque. Il nous apparait incorrect d'un point de vue doctrinal de parler d'ambigüité créative (*creative ambiguity*), comme le font certains auteurs,[74] pour désigner la stratégie d'évitement des États en matière d'espionnage. En règle générale, la formulation d'une ambigüité créative dans les traités internationaux et les résolutions du Conseil de Sécurité des Nations Unies vise justement la nécessité de dépasser l'impasse momentanée d'une négociation, pour permettre une interprétation dynamique des textes et un rôle accru reconnu au juge dans le futur.[75] Or, nous avons montré dans la première partie que les références discrètes à l'espionnage se concrétisent par des termes neutres, des euphémismes juridiques, dont le contenu est laissé à la seule discrétion des États.[76] La politique du silence ne permet pas de développer des normes prohibitives ou permissives incrémentales, quoiqu'elle autorise l'ETP. La Cour Européenne des droits de l'Homme a d'ailleurs reconnu dans sa jurisprudence la légitimité de cette politique de "non-confirmation et de non-dénégation" des États.[77] Dans ce sens, le principe du *Lotus* constituera indiscutablement la trame de fond de notre étude sur le statut de l'ETP.

Le statut de l'espionnage en temps de paix

Dans le cadre des développements qui suivent, nous souhaitons voir quelles règles prohibent l'espionnage. Si l'on veut établir un portrait complet de la question, trois branches distinctes du DIP doivent être abordées tour à tour: la souveraineté étatique; les droits humains; et le droit diplomatique.

[73] Dapo Akande, "International Adjudication on National Security Issues: What Role for the WTO" (2003) 43 VA J Int'l L 365 à la p 369.

[74] Voir par exemple Craig Forcese, "Creative Ambiguity: International Law's Distant Relationship with Peactime Spying" (14 novembre 2013) *Just Security* (blogue) en ligne: <http://www.justsecurity.org/3168/guest-post-creative-ambiguity-international-laws-distant-relationship-peacetime-spying/>.

[75] Sipowo, *supra* note 24 à la p 28.

[76] Notons par ailleurs que la CIJ elle-même préfère à l'expression "espionnage" des termes tels que: "abus de fonction," "acivités illicites des membres de missions diplomatiques ou consulaires" ou encore l'expression "ce genre d'activité"; voir notamment *Affaire Téhéran*, *supra* note 71 au para 82–87.

[77] *Kennedy c Royaume Uni*, n°26839/05, [2010] CEDH (Sér A) 1 au para 187 [*Affaire Kennedy*].

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

Avant d'entamer cette analyse, une difficulté inhérente à cette recherche doit être soulevée, soit celle de comprendre que les règles qui pourraient prohiber l'espionnage ne sont pas encore toutes cristallisées. Le juriste espère une réponse claire, non équivoque et précise cependant que certaines règles que nous étudierons sont en émergence et floues. C'est là — et à chaque fois le DIP sera silencieux — que le principe du *Lotus* interviendra. En l'absence de règles prohibitives, nous pourrons conclure que l'ETP est licite en vertu de la liberté des États.

LA SOUVERAINETÉ ÉTATIQUE: UN REMPART IMPÉNÉTRABLE?

Nous exposerons à présent comment la souveraineté étatique prohibe l'espionnage. Pour ce faire, nous examinerons quatre aspects distincts que couvre la souveraineté étatique. Il s'agit de la souveraineté territoriale; de l'interdiction du recours à la force; du principe de non-intervention dans les affaires intérieures; et enfin de l'exercice territorial de la compétence étatique. Agissant d'ordinaire comme un véritable rempart, le château de la souveraineté est une notion protéiforme qui signifie que l'État n'est soumis à aucun autre État. Nous montrerons cependant que face à l'espionnage, la souveraineté est loin d'être un rempart impénétrable.

L'espionnage comme atteinte à la souveraineté territoriale des États

Le statut de l'espionnage en temps de paix dépend d'abord du régime de l'espace dans lequel, ou partir duquel, il s'effectue. Le territoire national — y compris le territoire terrestre, maritime et aérien — constitue un véritable titre de compétence pour les diverses manifestations étatiques. L'État possède un droit exclusif qu'il exerce sur toute personne ou fait dans l'aire territoriale qui lui est propre.[78] De ce fait même, les frontières d'un État sont inviolables et aucune puissance étrangère ne peut s'introduire physiquement sur son territoire national sans le consentement de ce dernier.[79] Par contraste, les espaces internationaux — soit la haute mer, l'espace aérien international et l'espace extra-atmosphérique — échappent par définition à la souveraineté des États. Les États sont libres d'y mener toutes sortes d'activités pourvu que celles-ci ne soient pas nuisibles aux autres États, y compris, donc, de se livrer à l'espionnage.[80] Une *summa divisio* peut ainsi être établie entre (1) les actes d'espionnage qui

[78] Salmon, *supra* note 5 à la p 1046.

[79] Maurice Arbour, *Droit international public*, 6e éd, Cowansville, Yvon Blais, 2012 à la p 327.

[80] Lafouasse, *supra* note 19 à la p 36.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

font appel à des moyens intrusifs entrainant une "violation collatérale"[81] de l'intégrité territoriale de l'État victime d'une part; et (2) d'autre part, les actes d'espionnage qui n'entrainent aucune violation collatérale, car se déployant à partir du territoire même de l'État-espion ou à partir d'espaces internationaux.[82]

En se situant dans la *summa divisio* qui vient d'être esquissée, nous sommes naturellement amenés à étudier l'ETP selon sa mise en œuvre dans différends espaces physiques. Pour certains auteurs du XX^{e} siècle, l'ETP serait forcément illicite puisqu'il s'accompagnerait toujours d'une violation collatérale de l'intégrité territoriale.[83] Les progrès techniques ont toutefois fait mentir cette conception. L'âge d'or des espions à la James Bond, envoyés sur le territoire des États, est dépassé. Les progrès ont fait franchir à l'espionnage des étapes fondamentales qui, depuis l'espionnage dans la haute mer à l'espionnage satellitaire, se jouent des limites frontalières.[84]

Pour Olivier Forcade, nous assistons ainsi depuis les années 1960 à une véritable "déterritorialisation" des espaces d'espionnage.[85] Dans le cadre de notre étude, nous n'aborderons donc pas les violations "classiques" de la souveraineté territoriale que constitue l'envoi d'un espion, l'intrusion de l'espace aérien par un aéronef-espion ou encore l'intrusion de la mer territoriale par un navire-espion. Celles-ci ont déjà été documentées ailleurs par la doctrine. Ayant le futur et ses possibles développements à l'esprit, nous croyons plus pertinent de dresser l'état des lieux de l'ETP déployé dans deux espaces: l'espace extra-atmosphérique et le cyberespace. C'est là que se soulèvent aujourd'hui les questions difficiles. Nous suggérons que l'ETP est licite dans ces deux cas, le droit étant à la remorque de la technologie.

[81] Nous employons le terme "violation collatérale" puisqu'il faut s'abstenir de confondre la fin et les moyens. Il existe bien une violation d'une obligation internationale ainsi qu'un préjudice pour lesquels réparation peut être demandée pour atteinte à l'intégrité territoriale — mais il s'agit là d'une violation collatérale distincte de l'acte d'espionnage. Autrement dit, l'espionnage n'est pas un délit international (la fin recherchée), c'est l'entrée non autorisée sur le territoire d'un État étranger (les moyens utilisés), pour des motifs de reconnaissance, qui en est un. Par exemple, s'il y a violation de l'espace aérien aux fins d'espionnage, c'est bien cette violation de l'espace aérien qui est illicite et dont les États peuvent se plaindre, mais non la fin recherchée. Voir notamment Lafouasse, *supra* note 19 à la p 27.

[82] *Ibid* à la p 28.

[83] Pour un exemple de cette discussion, voir Oliver J. Lissitzyn, "Electronic Reconnaissance from the High Seas and International Law" (1970) Naval War College R 563.

[84] Forcade, *supra* note 11 à la p 67.

[85] *Ibid.*

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

Un acte d'espionnage licite dans l'espace extra-atmosphérique

L'espace extra-atmosphérique constitue un espace international dans lequel règne le principe de libre utilisation. L'article I.2 du *Traité de l'espace* édicte le principe selon lequel les États sont libres de mener toutes sortes d'activités spatiales, pourvu qu'elles soient pacifiques.[86] Il suit que les États sont libres de se livrer à l'espionnage par des interceptions satellitaires ou de se livrer à de l'observation satellitaire prospective (*imint*), cette dernière apparaissant d'ailleurs aujourd'hui comme une activité licite au statut coutumier sur lequel nous ne nous attarderons pas.[87] (Il existe en effet depuis le début des années 1960 une longue pratique d'observation spatiale militaire et une opinion acceptant sa légalité[88]). Puisque le *sigint* est présentement l'une des principales sources d'informations pour les agences de renseignement, concentrons-nous plutôt sur l'exploration radio ou renseignement électronique discursif.

Plusieurs États disposent de systèmes nationaux et multilatéraux d'interception, composés de stations d'écoutes au sol et de satellites-espions pour capter les télécommunications qui transitent par satellites (*comsat* — une branche du *sigint*). La NSA américaine intercepterait ainsi un million de conversations satellites par demi-heure avec le système Échelon, dont dix seraient finalement retenues par les analystes pour rapport.[89] D'autres pays disposent de tels systèmes, dont la Suisse avec le système Onyx,[90] le Royaume-Uni, la Russie, l'Espagne, la Chine, le Danemark, les Pays-Bas, l'Allemagne, l'Inde ou la Suède.[91]

Quoique cela soit contesté par certains auteurs,[92] il est généralement admis que la localisation matérielle de ces interceptions git dans les faisceaux d'ondes descendants ("downlinks") que les satellites renvoient vers

[86] Arbour, *supra* note 79 à la p 458; *Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes* (annexe de la résolution 2222 (XXI) de l'Assemblée générale), 19 décembre 1966, RTNU art 1 [*Traité de l'Espace*]; Laurence Ravillon, "Espace extra-atmosphérique" dans Hugues Fulchiron *JurisClasseur Droit International*, LexisNexis, 2009, Fasc 141–20 au para 10; Armel Kerrest, "Espace extra-atmosphérique — Cadre juridique de droit public" dans Hugues Fulchiron, *Juris Classeur Droit International*, LexisNexis, 2009, Fasc 141–10 au para 22.

[87] Voir notamment Ilias I Kuskuvelis, "La légalité coutumière de l'observation spatiale militaire" (1990) 3 Rev fr dr aérien 297.

[88] *Ibid.*

[89] *Projet "Onyx," supra* note 54 à la p 1396.

[90] *Ibid* à la p 1408.

[91] *Ibid* à la p 1387.

[92] Dimitri Yernault, "De la fiction à la réalité: le programme d'espionnage électronique global 'Échelon' et la responsabilité internationale des États au regard de la Convention Européenne des Droits de l'Homme" (2001) 1 RBDI 138 à la p 167.

la Terre.[93] Cette forme d'espionnage transnational n'atteint donc pas l'intégrité territoriale des États. La Cour Européenne des droits de l'Homme (CourEDH) le confirme d'ailleurs dans l'affaire *Weber et Saravia c Allemagne*.[94] Dans cette affaire, les requérants disaient avoir été frappés de mesures d'interceptions par le gouvernement allemand alors qu'ils se trouvaient en Uruguay. Selon eux, l'interception des télécommunications opérées par l'intermédiaire de relais satellites ou hertziens portait atteinte à la souveraineté territoriale de cet État ainsi qu'à leur droit à la vie privée. Rappelant la localisation matérielle de l'interception, la CourEDH rejeta en ces termes l'argument des requérants:

> Des signaux émis depuis des pays étrangers étaient surveillés par des sites d'interception situés sur le sol allemand et les données recueillies étaient utilisées en Allemagne. Cela étant, la Cour estime que *les requérants n'ont pas démontré, par des indices concordants, que les autorités, en adoptant et en appliquant les mesures de surveillance stratégique, aient procédé à des activités attentatoires à la souveraineté territoriale d'États étrangers*, telle qu'elle est protégée par le droit international public (nous soulignons).[95]

Cette conclusion n'a rien d'étonnant lorsqu'on considère l'aspect technique en présence. L'interception des communications transitant par satellites s'opère souvent au moyen d'antennes paraboliques situées sur le territoire national de l'État-espion. Ces antennes captent les faisceaux d'ondes descendants renvoyés vers la Terre par les satellites. Les faisceaux d'ondes, loin d'être focalisés sur une zone géographique précise, débordent sur de grandes zones d'empreintes ("footprint") représentant parfois jusqu'à 50% de la surface terrestre s'ils ne sont pas concentrés.[96] Une seule station de réception peut ainsi suffire pour capter passivement les communications de toute l'Europe.

Un acte d'espionnage licite dans le cyberespace

Les services de renseignement ont pour règle absolue de s'adapter constamment au progrès croissant de la technologie. Le cyberespace constitue à cet égard l'espace le plus récent dans lequel évolue l'ETP: on parle alors de *cyberespionnage* et de *cyber reconnaissance*. Pour mémoire, le cyberespionnage, tel que définit par le Manuel de Tallinn, consiste en "any act undertaken

[93] Jean Treccani, "Internet: investigations transnationales et atteintes à la souveraineté" dans *L'individu face aux nouvelles technologies: surveillance, identification et suivi. Actes du Colloque international des 10 et 11 novembre 2004 à Lausanne*, Genève, Schulthess, 2005, 93 à la p 123.

[94] *Weber et Saravia c Allemagne*, n° 54934/00, [2006] CEDH 1 au para 31 [*Affaire Weber*].

[95] *Ibid* au para 88.

[96] *Projet "Onyx," supra* note 54 à la p 1391.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

clandestinely or under false pretences that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party [within] the territory controlled by [the] party."[97] De son côté, aucune définition juridique de la cyber reconnaissance (ou CNE) n'existe en DIP. C'est plutôt un concept doctrinal et militaire, qui s'entend du "use of cyberspace capabilities to obtain information about enemy activities, information resources, or system capabilities [from beyond enemy territory]."[98] Or, l'actualité est émaillée d'affaires de cyberespionnage et cyber reconnaissance qui méritent notre attention.

Songeons à *GhostNet*, un système de piratage et de cyber espionnage chinois révélé par l'Université de Toronto en 2009, qui a contaminé des milliers d'ordinateurs.[99] Le tiers des ordinateurs touchés faisaient partie de ministères des Affaires étrangères ou d'ambassades, à l'instar des bureaux du Dalaï-lama, qui auraient été des sympathisants de la cause tibétaine.[100] En juin 2012, un imposant logiciel malveillant nommé *Flame*, permettant d'intercepter des courriels ou d'enregistrer des conversations en ligne, est découvert au Proche-Orient.[101] Il aurait lui aussi infecté des milliers d'ordinateurs dans une série de pays de la région israélo-palestinienne, ainsi que l'Iran. Quoique la paternité de *Flame* reste inconnue, le virus semble, de par sa sophistication, avoir été développé par un État.[102] Cinq ans ont été nécessaires ne serait ce que pour le repérer. Face à cette pratique étatique grandissante, tirer au clair la légalité ce type d'activité au regard de la souveraineté territoriale vaut la peine. Poser cette question est d'autant plus important qu'elle ébranle les conceptions classiques du DIP centrées sur le territoire et les ressources naturelles.

Une fois encore, c'est le statut du cyberespace qui déterminera le statut du cyberespionnage. De deux choses l'une: soit le cyberespace est considéré comme un espace international qui échappe par définition à la souveraineté des États, soit le cyberespace se rattache partiellement ou totalement au territoire national, dans lequel cas le cyberespionnage

[97] Schmitt, *supra* note 42 à la p 159.

[98] *Ibid.*

[99] Georg Kerschischnig, *Cyberthreats and International Law*, Hague, Eleven International Publishing, 2012 à la p 171.

[100] Tyler Moore, "Introducing the Economics of Cybersecurity: Principles and Policy Options" dans Committee on Deterring Cyberattacks dir, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, Nadtional Academies Press, 2010 à la p 5.

[101] Johann-Christoph Woltag, *Cyber Warfare: Military Cross-border Computer Network Operations under International Law*, Cambridge, Intersentia, 2014 à la p 41.

[102] Yves Eude, "Flame, un virus espion d'État" (2012) *Le Monde*, en ligne: <http://www.lemonde.fr/technologies/article/2012/06/20/flame-un-virus-espion-d-etat_1721182_651865.html>.

pourrait de fait entrainer une "violation collatérale" de l'intégrité territoriale.[103] Or, le cyberespace suscite une confusion mentale quant à sa géographie, d'autant que les données interceptées transitent par plusieurs États avant de se rendre à leur destination finale. Certains ont ainsi argumenté que le cyberespace constitue un espace international ou encore une nouvelle dimension spatiale si unique qu'elle justifie l'application de règles particulières du DIP.[104] Force est toutefois d'admettre que le cyberespace dépend de réseaux informatiques se trouvant bel et bien sur le territoire d'un État.[105] Nous nous rangeons donc ici avec ceux qui considèrent que la souveraineté territoriale s'applique au cyberespace.[106]

Au vu de ce qui précède, il ne fait pas de doute que le *cyberespionnage*, dans son acception stricte du Manuel de Tallinn, viole l'intégrité territoriale des États victimes. Envoyer un agent sur le territoire d'un État pour qu'il y collecte des informations sur un ordinateur ou un serveur protégé d'un *air gap* (c'est-à-dire un réseau isolé physiquement, rendant le piratage informatique à distance impossible) viole le droit international.[107] Un tel acte viole l'intégrité territoriale de manière évidente, au même titre qu'une violation de l'espace aérien par un aéronef-espion.

Moins patente, en revanche, est l'illicéité de la cyber reconnaissance ou CNE. Transnationales par définition, ces formes d'espionnage ne semblent pas violer directement ledit principe par une intrusion sur le territoire national. Nous le concevons bien: à vrai dire, ne serait-il pas illusoire de suggérer que la cyber reconnaissance constitue une violation de la souveraineté territoriale, au même titre (pour tabler sur le même exemple) qu'une violation de l'espace aérien par un aéronef-espion? Nous le croyons. Et pourtant, il n'en manque pas certains pour souligner que, d'un point de vue objectif, "une action sur le clavier ici produit des effets bien réels à l'étranger. La frappe du clavier induit un influx électrique transmis à la machine distante, laquelle induit à son tour un influx électrique en réponse à l'ordinateur requérant."[108] La question de l'atteinte matérielle à l'intégrité territoriale est, là encore, technique. Reconnaissons donc que des effets tangibles existent, à commencer par les mouvements mécaniques "subtils" sur les supports de données distants, au moment où ces données sont copiées et transférées

[103] Lafouasse, *supra* note 19 à la p 161.

[104] Jonathan Bourguignon, "La recherche de preuves informatiques et l'excercice extraterritorial des compétences de l'Etat" dans *Internet et le droit international*, Paris, Editions A Pedone, 2014, 357 à la p 396.

[105] *Ibid* à la p 362.

[106] Schmitt, *supra* note 42 à la p 115.

[107] *Ibid.*

[108] Treccani, *supra* note 93 à la p 94.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

à l'État-espion.[109] D'après nous, toutefois, les effets tangibles qui résultent de la cyber reconnaissance n'atteignent pas le seuil minimal requis pour constituer une atteinte à l'intégrité territoriale, particulièrement lorsqu'on les mesure à la pratique antérieure des États.[110]

Un argument se met en place ici: appelons le l'argument *de minimis*. On trouvera dans les activités de télédétection et d'observation satellitaire un parallèle fécond à l'aune duquel mesuré l'argument *de minimis*.[111] À cet égard, les États emploient dans l'espace extra-atmosphérique deux grands types de satellites aux fins d'observation satellitaire. Dans un premier cas de figure, les satellites présentent une technologie optique *passive*. Cette technologie reçoit les rayonnements électromagnétiques ayant quitté le territoire de l'État observé pour synthétiser une image.[112] En d'autres mots, cette technologie n'envoie pas activement de rayons vers le sol, mais ne fait qu'enregistrer des rayonnements émis naturellement depuis le territoire d'un État. Elle n'est guère problématique au plan juridique.

Un second cas de figure plus problématique se présente toutefois dans la technologie *active*, qui émet vers le sol de l'État observé des ondes radar sous forme d'impulsions brèves dont les échos sont enregistrés.[113] Ces ondes radars n'interfèrent pas matériellement avec le territoire, mais on dira que, d'un point de vue objectif, la technologie active produit bien des *effets subtils sur le territoire de l'État observé*, comme c'est le cas pour la cyber reconnaissance, des ondes radar étant *émises* vers le sol. Pourtant, il est clair que la souveraineté territoriale des États ainsi observés n'est nullement troublée par la technologie des satellites, qu'elle soit passive

[109] Nicolai Seitz, "Transborder Search: A New Perspective in Law Enforcement" (2005) 7:2 Yale JL & Tech 25 à la p 36.

[110] Seitz, *supra* note 109 aborde la question en matière de saisies transnationales et offre un point de vue contraire: "[*The view*] which holds that transborder searches are merely a low-intensity encroachment, is not convincing either. The existence of norms, expressed by statutes such as § 202 of the German criminal code or § 271 of the Swiss criminal code, which address transborder searches, already demonstrates that transborder searches are perceived to be an encroachment of high intensity. The de minimis level beneath which the vonBriehl/Ehlscheid view would apparently like to locate transborder searches is certainly exceeded" à la p 43. Notons cependant qu'on ne peut tirer aucune inference de l'existence de lois nationales sur l'accès transfrontière aux données pour déterminer l'*opinio juris* des États.

[111] Pour une approche similaire au cyberspace fondée sur le raisonnement par analogie, voir Kristen E Eichensehr, "The Cyber-Law of Nations" (2014) 103 Geo LJ 317 à la p 342; voir également Sean P Kanuck "Information Warfare: New Challenges for Public International Law" (1996) 37 Harv Int'l LJ 243 à la p 279.

[112] Jana Kristin Hettling, *Satellite Imagery for Verification and Enforcement of Public International Law*, Munich, Heymanns, 2008 à la p 22.

[113] *Ibid.*

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

ou active.[114] Aucun État n'a jamais protesté l'observation de son territoire par des satellites sous le seul prétexte que ces technologies violeraient *per se* la souveraineté territoriale, sans autre forme de bris collatérale de la souveraineté aérienne. Les États ne s'émeuvent tout simplement pas face à ces réalités techniques. Ils indiquent par là la légalité de ces observations.

À partir de là, il est concevable de solliciter l'idée que les effets subtils produits par la cyber reconnaissance sur le territoire de l'État victime n'équivalent pas à une violation de l'intégrité territoriale. On soutiendra certes que la cyber reconnaissance présente une dimension cinétique plus invasive que la télédétection active, dès lors qu'elle entraine un traitement de données et le bris de barrières virtuelles.[115] L'argument est plausible. À notre avis cependant, le parallèle avec la télédétection vient confirmer la stérilité de cantonner le débat autour des seuls effets qu'un clavier peut produire sur le territoire de l'État victime de cyber reconnaissance. Le critère déterminant est ultimement l'opinion des États. Comme le note Ziolkowski, un mémoire juridique averti du Département de la Défense des États-Unis met le doigt sur ce problème délicat:

> An unauthorized electronic intrusion in another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to physical trespass into a nation's territory, *but such issues have yet to be addressed in the international community* (nous soulignons).[116]

Faute de consensus, la cyber reconnaissance doit présentement être présumée licite en vertu du *Lotus*. De la pratique étatique, il ressort que la cyber reconnaissance n'est pas plus une violation de l'intégrité territoriale que la télédétection depuis l'espace extra-atmosphérique. À titre d'illustration, les États-Unis n'ont jamais formellement protesté contre la cyber reconnaissance industrielle intensive de ses compagnies par la Chine, alors que

[114] *Ibid.*

[115] Nous reconnaissons ici la position d'un des évaluateurs anonymes de ce texte — et le remercions au passage — selon laquelle la cyber reconnaissance est une technique d'espionnage vraisemblablement plus invasive que l'espionnage par télédétection active. Si l'argument est plausible, il est important de reconnaitre que la télédétection active implique elle aussi plusieurs étapes. Comme l'exprime Hettling, *supra* note 113 à la p 12: "[I]t is important to understand that remotely sensed data is not created with one *click*, like a photograph, but that different stages of development need to be distinguished. In particular, it needs to be divided between the raw/primary data that is recorded by the sensor, the processed data that is being built at the ground stations and the interpreted/analyzed data which is the end product and ready to fulfill the purpose of gaining certain information."

[116] Ziolkowski, *supra* note 66 à la p 458.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

ces actes ont entrainé des répercussions économiques majeures.[117] Les États suivent leur traditionnelle stratégie d'évitement.

L'espionnage comme recours illicite à la force

Peu de principes ont joué un rôle aussi fondamental en droit international contemporain que le principe de l'interdiction du recours à la force. Et pourtant le rôle que ce principe peut jouer en matière d'espionnage est forcément nul. L'article 2(4) de la *Charte des NU* prévoit une interdiction coutumière du recours à la menace et l'emploi de la force armée par les États dans leurs relations internationales. L'emploi de la force armée peut revêtir différentes formes, allant de l'agression armée à la simple menace d'utilisation de la force.[118] Une agression armée se dit ainsi d'une attaque déclenchée par un État agissant le premier contre un autre État.[119]

La prohibition de tout usage de la force se limite à la force armée proprement dite et ne saurait inclure, par exemple, l'usage de la force économique[120] ou l'usage de la force morale comme le souhaitaient certains États à la conférence de San Francisco.[121] Or, comme nous l'avons défini plus tôt, l'espionnage est un acte clandestin de collecte de renseignement qui n'entraine, en lui-même, aucun dommage matériel à l'État victime. Tout au plus, un espionnage massif pourrait entrainer des dommages économiques indirects. Face à telle définition, de toute évidence, l'espionnage ne saurait constituer un recours à la force et encore moins une agression armée au sens de la *Charte des NU*.

Il faut néanmoins admettre qu'en périodes turbulentes l'ETP a de tout temps fait naitre ce qu'on pourrait appeler une "dangereuse ambigüité" avec le recours à la force. Le potentiel d'information est un potentiel d'action. Du point de vue de l'État victime, l'espionnage sert à préparer des opérations militaires et va jusqu'à se confondre avec elles. Ceci ressort clairement dès la guerre froide avec l'utilisation des premiers aéronefs-espions. L'affaire U-2 en est la meilleure illustration. Le 1er mai 1960, un aéronef américain U-2, spécialement aménagé pour des missions de

[117] Benedikt Pirker, "Territorial Sovereignty and Integrity and the Challenges of Cyberspace" dans Katharina Ziolkowski, dir, *Peacetime Regime for State Activities in Cyberspace: International law, International Relations and Diplomacy*, Tallinn, NATO CCD COE Publication, 2013, 189 à la p 202; Pour un point de vue contraire quant à l'opinion des États sur le cyberespionnage, voir Russell Buchan, "Cyber Espionage and International Law" dans *Research Handbook on International Law and Cyberspace*, Elgar, 2005 à la p 184.

[118] Arbour, *supra* note 79 à la p 351.

[119] Salmon, *supra* note 5 à la p 657.

[120] *Ibid.*

[121] Jean-Pierre Cot, Alain Pellet et Mathias Forteau, dir, *La Charte des Nations Unis: Commentaire article par article*, 3e éd, Paris, Economica, 2005 à la p 443.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

renseignements aériens à haute altitude, survola le territoire soviétique et fut abattu par la défense antiaérienne soviétique.[122] Pour l'URSS, l'absence d'intention belliqueuse de l'aéronef n'était pas forcément apparente, celui-ci pouvant bien transporter des bombes.[123] Les juristes soviétiques qualifièrent d'ailleurs un temps l'ETP d'acte d'agression pour justifier la réplique soviétique, avant que Khrouchtchev ne concède qu'il ne s'agissait pas d'un "act of true aggression and war."[124] Cette brève perspective historique voudrait simplement suggérer la subjectivité de la confusion; mais ce type de confusion dans la qualification juridique n'est pas que l'apanage du passé.

Aujourd'hui, ce problème de confusion se pose d'une tout autre manière et bien plus délicat lorsque la cyber reconnaissance se confond à la cyberattaque. Cette ambigüité découle de ce que sur un plan technique, les moyens déployés par la cyber reconnaissance sont les mêmes qui précèdent une cyber attaque, en ce qu'ils permettent d'exposer le talon d'Achille d'une infrastructure informatique.[125] Pour cette raison, l'État victime se trouve "in the difficult situation of having to estimate whether an activity is still a matter of [spying] or is already forming into an intrusion or attack, and has to gauge the response appropriately."[126]

En pratique toutefois, deux éléments nous permettent de distinguer cyber reconnaissance et cyberattaque. D'une part, l'élément de clandestinité ou sous de faux prétextes. Comme le notent Rattray et Healey, alors que ceux qui conduisent des actes d'espionnage font de leur mieux pour dissimuler leurs activités, ceux qui participent à une cyberattaque passent moins de temps à brouiller les pistes.[127] Par exemple, l'attaque des "hackers patriotes" chinois contre les États-Unis en 2001, ou encore l'attaque de l'Estonie par la Russie en 2007, ont été biens moins subtiles que la cyber reconnaissance déployée par le groupe derrière *GhostNet*.[128] D'autre part, l'élément de la pratique étatique. La cyber reconnaissance est si courante que les États victimes ne protestent que très rarement, contrairement à ce

[122] Lafouasse, *supra* note 19 à la p 249.

[123] Spencer M Beresford, "Surveillance Aircraft and Satellites: A Problem of International Law" (1960) J Air L & Com 27 à la p 114.

[124] *Ibid* à la p 115.

[125] Kerschischnig, *supra* note 99 à la p 172. Voir également Heather Harrison Dinniss, *Cyber Warfare and the Law of War*, Cambrige, Cambridge University Press, 2012 à la p 156.

[126] Kerschischnig, *supra* note 99 à la p 173.

[127] Gregory Rattray & Jason Healey, "Categorizing and Understand Offensive Cyber Capabilities and Their Use" dans Committee on Deterring Cyberattacks, dir, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, Nadtional Academies Press, 2010 à la p 83.

[128] *Ibid.*

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

qui se passerait pour les cyberattaques.[129] Encore une fois, c'est parce que la cyber reconnaissance constitue tout au plus une collecte de renseignements, opérant clandestinement et ne causant aucun dommage matériel à l'État victime.[130] Le Manuel de Tallinn le corrobore à sa Règle 66(a).[131] Passé et présent concourent donc à démontrer l'absence d'identité entre l'ETP et le recours à la force. La confusion se dissipe ici.

L'espionnage comme atteinte au principe de non-intervention

Le principe de non-intervention est reconnu depuis fort longtemps. Découlant du principe d'égalité souveraine des États, il comporte l'obligation fondamentale des États de ne pas s'ingérer dans les affaires intérieures d'un autre État et s'applique également à toute menace d'une telle intervention.[132] À l'occasion de l'arrêt *Nicaragua c États-Unis*, la CIJ a d'ailleurs noté qu'il s'agissait d'un principe coutumier.[133] Il y a intervention illicite lorsque deux éléments sont réunis: (1) l'intervention porte sur des matières à propos desquelles le principe de souveraineté des États leur permet de décider librement (le "domaine réservé"); et (2) l'intervention prend la forme de moyens de contrainte d'ordre politique, économique ou militaire ("l'élément de contrainte").[134] D'emblée, on peut douter que l'espionnage présente l'élément de contrainte. Comme nous l'avons déjà remarqué dans la Partie I de ce texte, l'espionnage se présente d'abord comme une activité de collecte de renseignements exempte de toute coercition à laquelle les États consentent sur le fondement de la réciprocité.[135] D'un point de vue pratique, la réussite de l'espionnage passe par des moyens clandestins qui ne contraignent pas l'État espionné a adopté une ligne de conduite particulière.

L'absence de l'élément de contrainte ressort d'ailleurs clairement de l'affaire des *Activités militaires et paramilitaires au Nicaragua et contre celui-ci*

[129] *Ibid.*

[130] Ziolkowski, *supra* note 66 à la p 452. Voir également Jason Barkham, "Information Warfare and International Law on the Use of Force" (2002) 34 NYU Int'l L & Pol 57 à la p 89; Bradley A Thayer & Brian M Mazanec, *Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace*, Londre, Palgrave MacMillan, 2015 à la p 7; Oona A Hathaway et al, "The Law of Cyber Attack" (2012) 100 Cal L Rev 817 à la p 829.

[131] Schmitt, *supra* note 42 à la p 192. Qui dit: "Cyber espionage and other forms of information gathering directed at an adversary during an armed conflict do not violate the law of armed conflict."

[132] *Conférence sur la sécurité et la coopération en Europe, Acte final d'Helsinki*, 1 aout 1975 à la p 3.

[133] *Affaire Nicaragua c États-Unis*, *supra* note 61 au para 202.

[134] Juanita Westmoreland-Traoré, "Droit humanitaire et droit d'intervention," Journées mexicaines de l'Association Henri Capitant présenté à Mexico et Oaxaca, 18 au 25 mai 2002 à la p 161.

[135] Lafouasse, *supra* note 19 à la p 226.

(Nicaragua c États-Unis), où le Nicaragua ne reprocha nullement aux États-Unis de faire preuve d'ingérence dans ses affaires intérieures, en dépit d'un espionnage américain volumineux réalisé par des moyens divers[136]. Lors des plaidoiries, un représentant nicaraguayen, réfutant toute agression de son pays contre les États voisins soutenus par les États-Unis, remarqua ainsi:

> Maintenant, je mentionnerai seulement le fait évident que les États-Unis *disposent de bases, de stations radars, d'avions-espions, de navires-espions*, des forces armées du Salvador et du Honduras pour effectuer des manœuvres en Amérique centrale impliquant des milliers de soldats; et, avec tout cela, en presque quatre ans, ils n'ont pas été capables de prouver la moindre affaire de trafic d'armes du Nicaragua au Salvador par exemple (nous soulignons).[137]

Tel que l'indique Lafouasse, ce passage montre que l'agent du Nicaragua ne reproche, en aucune façon, au gouvernement américain de faire preuve d'ingérence dans les affaires intérieures de son pays en employant des dispositifs d'espionnage.[138] Tout au plus y a-t-il violation collatérale de l'intégrité territoriale par les aéronefs et navires-espions. Plus près de nous, le Comité d'experts du Manuel de Tallinn arrive à la même conclusion en prenant le cas du cyberespionnage. Surtout: "[m]ere intrusion into another State's systems does not violate the non-intervention principle … this holds true even where such intrusion requires the breaching of protective virtual barriers (e.g. the breaching of firewalls or the cracking of passwords)."[139]

D'aucuns prétendent toutefois que l'espionnage *économique* viole le principe de non-intervention.[140] Ceci tiendrait à deux arguments. D'une part, l'espionnage économique se distinguerait de l'espionnage traditionnel par l'absence de toute réciprocité entre les États. L'espionnage économique servirait à garantir les intérêts égoïstes de l'État-espion au risque de déstabiliser économiquement les États victimes, à l'inverse de l'espionnage traditionnel qui assure un équilibre des forces.[141] C'est la distinction entre l'objet économique et l'objet politique de l'espionnage. D'autre part, l'espionnage économique comporterait un élément de contrainte en ce qu'il

[136] *Ibid* à la p 228.

[137] *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci, Exposé oral de M. Arguello Gomez* CIJ à la p 11.

[138] Lafouasse, *supra* note 19 à la p 226.

[139] Schmitt, *supra* note 42 à la p 47.

[140] Christina Parajon Skinner, "An International Law Response to Economic Cyber Espionage" (2014) 46:4 Conn L Rev 1165 à la p 1168.

[141] *Ibid.*

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

pourrait bien causer des dommages économiques considérables forçant l'État victime à adopter une nouvelle ligne de conduite.[142] L'exemple de l'espionnage massif par la Chine des compagnies américaines est avancé par les tenants de cette position.[143]

Cette position prête flanc à la critique. L'argument le plus immédiat qui vient s'opposer à une telle lecture expansive du principe de non-intervention est que ce sont bien les *moyens* employés qui doivent être coercitif *per se*, ce qui est différent de la *nature* de l'information collectée. De plus, le domaine réservé d'un État s'entend du "domaine d'activités dans lequel l'État, n'étant pas lié par le droit international, jouit d'une compétence totalement discrétionnaire."[144] À l'ère de la globalisation et de l'interdépendance économique, il semble difficile d'avancer que les États jouissent d'une compétence totalement discrétionnaire sur leurs décisions économiques.[145] D'autant que l'assistance humanitaire, la cessation de l'aide économique ou un embargo économique ne constituent même pas des ingérences en droit international.[146] En définitive, le principe de non-intervention ne prohibe pas l'espionnage, quelle que soit la nature de l'information collectée.[147]

L'espionnage comme exercice extraterritorial illicite de la compétence d'exécution

Un dernier corolaire du principe d'égalité souveraine des États et de la souveraineté attire notre attention: celui de l'exercice territorial de la compétence. La compétence territoriale constitue le pouvoir juridique

[142] Catherine Lotrionte, "Countering State-Sponsered Cyber Economic Espionage under International Law" (2014) 40 NCJ Int'l L Rev 443 à la p 503.

[143] Ziolkowski, *supra* note 66 à la 238.

[144] Salmon, *supra* note 5 à la p 356.

[145] Ziolkowski, *supra* note 66 à la 238.

[146] *Affaire Nicaragua c États-Unis*, *supra* note 61 au para 112.

[147] C'est pourquoi plusieurs auteurs de doctrine ont cherché, sans succès, à se tourner vers des instruments conventionnels pour prohiber l'espionnage économique. L'*Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce* (*ADPIC*) est ainsi invoqué par ces auteurs. Certes, l'article 39(1) de cet instrument oblige les États parties à assurer une protection, strictement nationale, contre la concurrence déloyale en protégeant les "renseignements non divulgués" des personnes physiques et morales. En revanche, l'*ADPIC* ne dit rien quant à l'espionnage dans les rapports entre États. En réalité, les États, tout comme l'Organisation mondiale du commerce, n'ont nullement voulu réguler l'espionnage économique malgré une préoccupation croissante face à cette activité. Voir Ziolkowski, *supra* note 66 à la p 436; voir généralement sur ce sujet Gerald O'Hara, "Cyber-Espionage: A Growing Threat to the American Economy" (2010) 19 CommLaw Conspectus 241; David P Fidler, "Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies" (2014) 17:10 Insights, en ligne: <www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving>.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

exclusif reconnu par le droit international à un État de soumettre les personnes, biens et activités sur son territoire à *son* ordre juridique.[148] À cet égard, on distingue traditionnellement deux types de compétence.[149] La *compétence normative* s'entend du pouvoir d'un État d'édicter des lois nationales.[150] La *compétence d'exécution* s'entend quant à elle du pouvoir d'un État de donner effets à ces lois sur son territoire, par un acte de police ou de sanction officielle.[151] Si l'exercice extraterritorial d'une compétence normative est tout à fait admis en DIP depuis l'affaire du "*Lotus*" (par exemple, les États criminalisent souvent des actes criminels commis à l'étranger, dont l'espionnage[152]), tel n'est pas le cas de l'exercice extraterritorial de la compétence d'exécution. Faute de consentement de l'État tiers concerné, le fait d'exercer une compétence d'exécution de manière extraterritoriale constitue un exercice de compétence qui viole le droit international.

Nous parlerons en ce sens *d'actes de puissance illicites*. De tels actes violent le droit international parce qu'en exerçant des actes de sanction ou de police sur le territoire d'un État tiers, l'État qui exerce sa compétence entre "en compétition" avec la compétence exclusive de ce dernier. La pratique offre plusieurs exemples de tels actes illicites. Le fait pour un État d'envoyer des enquêteurs sur le territoire d'un État tiers pour contrôler des questions fiscales constitue assurément un acte de puissance illicite.[153] Vu sous cet angle, nous pouvons nous demander si ces actes d'espionnage étudiés plus tôt, qui ne violent pas collatéralement l'intégrité territoriale, *peuvent néanmoins constituer des actes de puissance illicites en droit international*. À cet escient, la légalité de l'espionnage est à rechercher dans deux directions. En premier lieu, celle de la cyber reconnaissance, à une époque d'incertitude quant aux règles (dont la compétence d'exécution) qui irradient le cyberespace. En deuxième lieu, celle des interceptions transnationales des télécommunications.

Une cyber reconnaissance licite au prise avec une coutume émergente

Voyons, dans un premier temps, la cyber reconnaissance. Il nous semble que, pour élucider la question du statut de cette forme d'espionnage, il peut être utilement fait appel aux traités internationaux relatifs à la

[148] Salmon, *supra* note 5 à la p 210.

[149] Ian Brownlie, *Principles of Public International Law*, 6e éd, New York, Oxford University Press, 2003 à la p 297.

[150] Salmon, *supra* note 5 à la p 345.

[151] *Ibid.*

[152] Monika B Krizek, "The Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice" (1988) 6 BU Int'l L J 337 à la p 352.

[153] Bourguignon, *supra* note 104 à la p 362.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

coopération entre États en matière de saisies et perquisitions sur des systèmes informatiques se trouvant à l'étranger[154] pour déterminer, du même coup, le statut de la cyber reconnaissance. Cette dernière présente en effet une similarité frappante avec les perquisitions et saisies extraterritoriales. Il arrive fréquemment que des agents de police collectent des informations situées dans un ordinateur exploité sur le territoire d'un autre État, et ce sans jamais quitter leurs bureaux nationaux, tout comme les services de renseignements le feraient pour espionner. C'est ici qu'entre en jeu la *Convention sur la cybercriminalité* (ou *Convention de Budapest*), le premier traité international sur les infractions pénales commises via l'Internet et autres réseaux informatiques.[155] Ce traité multilatéral, développé par le Conseil de l'Europe et ouvert aux signatures à tous les États depuis 2001, compte aujourd'hui 50 États signataires et 47 États parties.[156]

La convention cherchait justement à établir un fondement juridique clair pour permettre les perquisitions extraterritoriales sur les systèmes informatiques se trouvant à l'étranger. Pour ce faire, celle-ci organise un dispositif de coopération et d'entraide en matière de cybercriminalité.[157] Une pièce centrale de ce dispositif est l'article 32 de la convention. Celui-ci prévoit deux hypothèses dans lesquelles l'accès transfrontière aux données situées dans un ordinateur exploité sur un autre État est permis, sans qu'il soit nécessaire de recourir aux mécanismes classiques d'entraide.[158] Une Partie peut ainsi, sans l'autorisation d'une autre Partie:

- accéder à des données informatiques stockées *accessibles au public (source ouverte)*, quelle que soit la localisation géographique de ces données; ou
- accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques *stockées situées dans un autre État*, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique (nous soulignons).[159]

L'article 32(a) appelle alors une première remarque applicable à la cyber reconnaissance. Constatons une différence de traitement juridique remarquable des actes de puissance illicites selon la nature des renseignements,

[154] Voir John H Currie, *Public International Law*, 2e éd, Toronto, Irwin Law, 2008 à la p 333.

[155] *Convention sur la Cybercriminalité*, STCE n° 185, *RTNU*, vol. 2296, n° 40916, 167.

[156] Krizek, *supra* note 152 à la p 122.

[157] *Convention sur la cybercriminalité: Rapport explicatif*, Conseil de l'Europe 23 novembre 2001, n°185 à la p 25 [*Rapport explicatif*].

[158] *Ibid.*

[159] *Ibid* art 32.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

soit entre données *ouvertes* et *fermées*. Les données sont dites *ouvertes* ou en "accès libre" lorsque toute personne peut y accéder sans entraves techniques[160] (à l'instar des données publiées sur des sites internet comme Facebook, Twitter ou Instagram, à moins que l'accès nécessite un mot de passe ou une inscription). Accéder aux données ouvertes est autorisé, quel que soit le lieu de stockage des données ou la localisation de l'hébergeur du site web, sans préavis ou avis subséquent.

Or, le rapport explicatif de la convention précise bien que le Comité d'experts n'a réglé dans l'article 32(a) que ces accès unilatéraux considérés par les États comme unanimement admissibles en droit international.[161] Dit autrement, le Comité considéra que l'accès aux données ouvertes n'était pas un acte de puissance illicite. L'examen de la pratique des États, qui ne prennent jamais ombrage de l'accès non autorisé aux données ouvertes, pointe ici vers l'existence d'une coutume autorisant cet accès. Comme l'exprime Nicolai Seitz, "the examination of data in generally accessible Internet sources within the framework of a sovereign activity has been and is practiced daily [by States]."[162] Pour cette raison, nous croyons que l'article 32(a) codifie une coutume qui existait depuis relativement longtemps au moment où le Comité élabora la convention.[163] Partant de là, les États jouissent d'une liberté coutumière de collecter des données ouvertes, que ce soit pour une perquisition dans le cadre d'une enquête … ou encore pour se livrer à la cyber reconnaissance! On s'explique assez bien cette licéité.

L'article 32(b) appelle une seconde remarque plus délicate. La disposition est remarquable en ce qu'elle autorise les actes de puissance, sans préavis ni avis subséquent à l'État concerné — et ce, *pour des données non publiques*, c'est-à-dire des informations protégées ou fermées.[164] Comme nous l'avons déjà souligné, un État ne peut exercer des actes de puissance à moins que l'État visé l'y autorise ou encore, nous dit l'affaire du "*Lotus*", que des "règles permissives découlant du droit international coutumier ou d'une convention"[165] permettent ces empiètements. Dans ce sens, l'article 32(b) constitue précisément une règle permissive découlant d'une convention[166] et faisant exception au principe de souveraineté étatique.

[160] Bourguignon, *supra* note 104 à la p 369.

[161] *Rapport explicatif*, *supra* note 157 au para 293; Bourguignon, *supra* note 104 à la p 368.

[162] Seitz, *supra* note 109 à la p 38.

[163] Treccani, *supra* note 93 à la p 96.

[164] *Ibid.*

[165] *Affaire du "Lotus,"* *supra* note 57 à la p 19.

[166] Bourguignon, *supra* note 104 à la p 365.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

L'épineuse question qui est alors soulevée est de savoir si, à l'image de l'article 32(a), on peut conclure que l'article 32(b) reflète la coutume internationale? Nous ne le croyons pas. Les divergences d'opinions sur l'accès transfrontière aux données fermées n'ont pas permis au Comité d'experts d'atteindre un consensus.[167] Ce régime dérogatoire semble ainsi réservé aux seuls États parties de la *Convention de Budapest*, de sorte que cette disposition ne reflète pas une coutume internationale reconnue.[168] Au demeurant, le fait qu'un tel accès soit conditionnel à l'obtention d'un consentement légal et volontaire met bien en exergue que ces empiètements incommodent les États. En ajoutant ce critère à l'article 32(b), les États récalcitrants atténuent chez eux l'exercice de puissance des États étrangers ou en retirent le caractère illicite.[169] Avec tout cela, on vient à penser qu'une norme coutumière émergente est peut-être en train de voir le jour, qui pourrait prohiber la cyber reconnaissance des données fermées dans le futur.[170] Mais à moins que cette norme ne se consolide, la cyber reconnaissance est présumée licite en vertu du *Lotus*.

Des interceptions transnationales licites dans l'espace extra-atmosphérique

Voyons, dans un deuxième temps, les interceptions transnationales des télécommunications. Rappelons qu'est transnational l'espionnage dont l'interception se réalise *hors* du territoire de l'État victime d'où proviennent les communications. Comme nous l'avons mentionné précédemment, une trentaine d'États posséderaient divers systèmes d'interception, dont certains sont en mesure de capter les transmissions et transferts de données écrites et vocales qui transitent par satellites. Dans ces cas, l'interception a lieu dans l'espace extra-atmosphérique où sont situés les satellites de communication ou à partir du territoire de l'État-espion. Guère appréhendés par le principe de souveraineté territoriale, peut-on dire de ces formes d'espionnage qu'elles sont des actes de puissance illicites? Il faut répondre par la négative, quelque soit la nature des communications. On remarquera sur ce point que la *Convention de Budapest* avance un cadre de coopération uniquement pour ces données qui sont "stockées situées dans un autre État" (selon la formule boiteuse en français, "stored computer data located in another Party" en anglais). Autrement dit, la convention ne dit rien quant aux données interceptées *hors* du territoire de l'État tiers. L'espionnage transnational n'emporterait donc pas d'acte de puissance illicite.

[167] *Rapport explicatif*, *supra* note 157 au para 293.

[168] *Ibid.*

[169] *Ibid* au para 293.

[170] Seitz, *supra* note 109 à la p 45.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

L'affaire *X(Re)* de la Cour fédérale du Canada, l'une des rares décisions judiciaires nationales traitant du statut de l'ETP en droit international,[171] soutient cette analyse. Au centre de cette récente affaire gisait une demande d'autorisation par le *Service canadien du renseignement de sécurité* pour l'interception de communications et la collecte de renseignements provenant de l'étranger *depuis le Canada*.[172] Le principe de souveraineté territoriale n'était donc pas atteint *per se* par l'interception et la collecte réalisée au Canada, mais la Cour fédérale devait quand même considérer s'il s'agissait d'un acte de puissance illicite en droit international. À cet égard, la Cour soutint avec justesse que "ce qui est proposé dans le mandat en l'espèce n'est pas l'application de lois canadiennes à l'étranger, mais plutôt l'exercice au Canada d'une compétence relative à la protection de la sécurité du pays."[173] Aussi la Cour fédérale autorisa-t-elle ces interceptions jugées compatibles au droit international.

En conclusion, l'enseignement plus général qui peut être tiré de cette partie et de la décision *X(Re)*, est que la norme de l'exercice territorial de la compétence d'exécution ne parvient pas, en son état actuel, à prohiber la cyber reconnaissance ou l'interception transnationale des communications, même si une norme coutumière émergente pourrait prohiber ces pratiques pour les informations fermées dans le futur.

À ce stade de l'analyse, nous avons également dégagé les prohibitions, peu nombreuses, de l'espionnage qui naissent de la souveraineté étatique et de ses corolaires. Penchons-nous à présent sur ces règles prohibitives qui émergent d'une seconde branche du DIP: les droits de la personne. Plus particulièrement, nous montrerons que le droit à la vie privée garanti par le *Pacte international relatif aux droits civils et politiques* (*PIDCP*) n'offre qu'une protection virtuelle aux victimes de surveillance massive, cependant que la *Convention européenne des droits de l'homme* (*CEDH*) offre une protection plus expansive et robuste.

LE DROIT À LA VIE PRIVÉE ET LA SURVEILLANCE MASSIVE

Les droits de la personne peuvent-ils empêcher un État d'espionner les citoyens d'autres États? La surveillance massive est-elle licite? Il y a eu lieu de s'interroger suite au récent émoi provoqué par les pratiques de surveillance massive menée par la NSA américaine, qui a poussé l'Assemblée générale des Nations Unies à adopter, en décembre 2013, la résolution

[171] Craig Forcese, "Triple Vision Accountability and the Outsourcing of CSIS Intercepts" (6 décembre 2013) *National Security Law* (blogue), en ligne: <http://craigforcese.squarespace.com/national-security-law-blog/2013/12/6/triple-vision-accountability-and-the-outsourcing-of-csis-int.html>.

[172] *X (Re)*, 2009 CF 1058, [2010] 1 RCF 460 au para 40 [*Affaire X (Re)*].

[173] *Ibid* au para 66.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

68/167 sur le droit à la vie privée à l'ère du numérique.[174] Cette résolution vient condamner "la surveillance ou l'interception de communication, y compris en dehors du territoire national, ainsi que la collecte des données personnelles, notamment à grande échelle."[175] Les questions ci-dessus se révèlent d'autant plus aigües qu'à l'occasion des débats entourant la résolution, plusieurs États sont sortis de leur politique de silence habituelle pour condamner sévèrement les actes d'espionnage de la NSA. Ainsi d'après le représentant de l'Indonésie, "extraterritorial surveillance … must be carried out in strict compliance with international law."[176] De même, un autre représentant déclarait que "the mass extraterritorial surveillance … carried out by the United States of America [was a] violation of the … human right to privacy."[177] Dans les faits, l'espionnage bafoue sans aucun doute le droit à la vie privée; cela ne signifie pas *ipso facto* que la surveillance massive est illicite en DIP. Ces scandales retentissants rendent donc importante la tâche de circonscrire le droit à la vie privée et d'en préciser les liens avec l'espionnage.

C'est ce que nous tenterons de faire ici en nous penchant sur le *PIDCP*, et incidemment sur la *CEDH*. Dans chaque cas, les développements suivants répondent à deux questions distinctes. Au premier chef, une question de seuil d'applicabilité, celle de savoir si les personnes visées par des interceptions transnationales sont sous le contrôle de l'État-espion au sens de ces conventions. Autrement, ces conventions sont inapplicables. Une question de fond redouble la première, celle de savoir comment la protection juridique du droit à la vie privée, telle qu'elle est consacrée aujourd'hui, prohibe l'espionnage transnational. Si c'est bien le DIP général que nous ciblons dans ce texte, le parallèle avec la *CEDH* nous permettra d'appréhender comment la CourEDH condamne les systèmes de surveillance massive.

La protection virtuelle offerte par le PIDCP

Nous verrons à présent que le *PIDCP* offre une protection virtuelle aux victimes de surveillance massive. La première question qui nous interpelle est celle de l'applicabilité du *PIDCP*. Les personnes concernées par les interceptions transnationales doivent se trouver sous le contrôle de l'État-espion afin que le *PIDCP* soit applicable. L'article 2(1) du *PIDCP* établit que les États parties s'engagent uniquement à respecter et à garantir le

[174] AGNU, *Le droit à la vie privée à l'ère du numérique*, A/RES/68/167, adoptée le 18 décembre 2013.

[175] *Ibid* au para 15.

[176] Draft resolution, A/C.3/68/L45/rev1; *The Right to Privacy in the Digital*, A/C3/68/SR.51, Agenda Item 69: Promotion and Protection of Human Rights à la p 7.

[177] *Ibid* à la p 6.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

droit à la vie privée des individus se trouvant "sur leur territoire *et* relevant de leur compétence." Cette clause de compétence reçoit d'ordinaire une interprétation restrictive. Effectivement, l'article 31(1) de la *Convention de Vienne sur le droit des traités* commande que l'interprétation du *PIDCP* se fasse "suivant le sens ordinaire à attribuer aux termes du traité."[178] D'après les tenants de l'interprétation restrictive, dont les États-Unis jusqu'à très récemment, le sens ordinaire de deux conditions reliées par la conjonction "et" est que les obligations étatiques naissent seulement lorsque les deux conditions sont réunies: le test serait donc cumulatif.[179] Des États ont ainsi traditionnellement nié l'application extraterritoriale du *PIDCP*. Ils n'auraient pas à garantir le droit à la vie privée des individus se trouvant hors de leur territoire.

Cette interprétation restrictive fait aujourd'hui l'objet de vives critiques. Le Comité des droits de l'homme des Nations Unies (CDH) estime dans son Observation générale n° 31 que le test est conjonctif. Les droits reconnus dans le *PIDCP* doivent être respectés et garantis "même si l'individu ne se trouve pas sur [le territoire de l'État]"[180] puisque la jouissance des droits reconnues dans le *PIDCP* devrait être accordée aux "personnes qui se trouveraient sur le territoire de l'État parti ou qui relèveraient de sa compétence," nous dit le CDH.[181] Le CDH est allé dans cette même direction dans l'affaire *Lopez-Burgos c Uruguay* en reconnaissant que l'Uruguay avait compétence sur M. Lopez Burgos, qui, bien que situé sur le sol de l'Argentine, avait été kidnappé, abusé, et enlevé du pays par les services secrets uruguayens avant d'être soumis à la torture.[182] D'ailleurs, le CDH n'a pas hésité, lors du dernier examen périodique des États-Unis, et dans l'approche audacieuse qu'on lui connait, à exhorter ledit État à prendre toutes les mesures nécessaires pour que ses activités de surveillance extraterritoriales soient conformes au *PIDCP*, et ce "indépendamment de l'emplacement des personnes dont les communications sont sous surveillance directe."[183]

[178] *Convention de Vienne sur le droit des traités*, 29 mai 1969, 1155 RTNU 331 [*Convention de Vienne*].

[179] Ilina Georgieva, "The Right of Privacy under Fire: Foreign Surveillance under the NSA and the GCHQ and Its Compabtibility with Art. 17 ICCPR and Art. 8 ECHR" (2015) 31:80 Utrecht J Int'l & Euro L 105 à la p 108.

[180] Comité DH (HRC), *La nature de l'obligation juridique générale imposée aux États parties au Pacte*, Observation générale No 31 (Article 2), 80ème session, CCPR/C/21/Rev.1/Add 13, 29 mars 2004, au para 10.

[181] *Ibid.*

[182] *Sergio Ruben Lopez Burgos c Uruguay*, (1981) comm n° R.12/52, 29, A/36/40 (1981) à la p 176.

[183] Comité DH (HRC), *Concluding Observations on the Fourth Periodic Report of the United States of America*, CCPR/C/USA/CO/4 (23 avril 2014) para 22, en ligne: <http://www.state.gov/documents/organization/235641.pdf>.

Quant à elle, la CIJ estime dans son avis sur les *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé* qu'une personne relève de la compétence d'un État lorsque cette personne est soumise à son "contrôle effectif", dans un contexte où l'État avait un contrôle militaire du territoire où se trouvaient des individus.[184] La CIJ impulse donc un test conjonctif. On constate ainsi que l'interprétation traditionnelle n'a plus préséance de nos jours; une nouvelle interprétation de la clause de compétence, bien que toujours contestée, s'est greffée au paysage juridique moderne.

Ces considérations nous conduisent à nous demander si, vu l'interprétation moderne de la clause de compétence du *PIDCP*, les personnes victimes de surveillance massive par un État étranger sont sous le "contrôle effectif" de celui-ci. Après tout, l'État exerce bien une sorte de compétence d'exécution en recueillant leurs données. Séduisant à première vue, ce concept du contrôle ne saurait être soutenu sérieusement sans ignorer d'importantes réalités techniques. Par définition, les interceptions transnationales portent sur des individus sur lesquels l'État n'exerce aucun contrôle *territorial* ou *physique*[185]

On peut s'en convaincre en s'appuyant sur deux exemples. D'abord, l'exemple des télécommunications opérées par l'intermédiaire de relais satellites de l'affaire *Weber*. Là, des signaux émis depuis des pays étrangers étaient surveillés par des sites d'interceptions situés sur le sol de l'Allemagne, et les données recueillies, utilisées sur le sol allemand.[186] N'apparaitrait-il pas extrêmement contestable d'affirmer que les personnes dont les signaux ont été captés se trouvent sous le contrôle *territorial* de l'Allemagne? On peut s'en convaincre d'abondant avec l'exemple du système PRISM de la NSA qui recueille des données dans le cyberespace. Remarquons, avec Ilina Georgieva, que "the implantation of tiny radio transmitters in most of the computers produced in the US grants the NSA the capacity to gain control over computers not connected to the Internet. Considering also that much of the Internet traffic is routed through the U.S., makes the picture complete — *physical* control [of individuals] does not play a role at all."[187] À la lumière de ces deux exemples, le test du contrôle effectif se révèle ainsi être un legs juridique dépassé par la technique moderne.

[184] *Conséquences juridiques de l'édification d'un mur dans le Territoire palestinien occupé*, Avis consultatif, [2004] CIJ rec 136.

[185] Craig Forcese, "Square Peg, Round Hole: International Human Rights and Transnational Spying" (18 octobre 2013) *National Security Law* (blogue), en ligne: <http://craigforcese.squarespace.com/national-security-law-blog/2013/10/18/square-peg-round-hole-international-human-rights-and-transna.html>.

[186] *Affaire Weber*, *supra* note 94 au para 31.

[187] Georgieva, *supra* note 179 à la p 113.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

Marko Milanovic suggère à cet égard d'adopter un nouveau test du contrôle *virtuel* des données.[188] Il importe de cette manière de distinguer ce dernier critère des deux autres critères du contrôle effectif qui brillent dans la jurisprudence.[189] Premièrement, *l'affaire du Mur* présente une forme de contrôle *territorial* sur les individus: c'est parce que les individus se trouvaient sur un territoire contrôlé par les forces militaires de l'État que celui-ci devait garantir leurs droits.[190] Deuxièmement, l'affaire *Lopez-Burgos* présente une forme de contrôle *personnel:* dans un contexte de détention et d'interrogation en Argentine, l'Uruguay exerçait littéralement un contrôle physique sur l'individu torturé.[191]

Or, comme nous l'avons vu, le droit à la vie privée s'accommode mal de ces deux premiers critères. La surveillance massive réalisée à l'instigation des États concrétise plutôt une nouvelle et troisième forme de contrôle; un contrôle *virtuel*. C'est un critère sans précédent en DIP qui ne trouve aucun soutènement dans la jurisprudence.[192] Il résulte que l'application du *PIDCP* achoppe en l'espèce dès l'étape de l'applicabilité, laissant les États sans recours. En dernière analyse, même si le *PIDCP* était applicable, il resterait encore à déterminer si les interceptions sont arbitraires ou illégales au sens du *PIDCP*, en se rappelant bien sûr le droit à la vie privée demeure l'un des droits les plus contestés du DIP.[193]

La protection concrète offerte par la CEDH

La jurisprudence de la CourEDH contient certaines des élaborations les plus importantes du droit international en matière de droit à la vie privée et de surveillance massive. Pour Yernault, la *CEDH* serait même à l'heure actuelle le "moyen juridique le plus complet"[194] pour affronter les dangers des systèmes de surveillance transnationaux. Aussi mérite-t-elle d'être étudiée plus avant et comparée avec le *PIDCP*, d'autant que la *CEDH* s'applique à plusieurs États des "cinq yeux," qui possèdent les systèmes d'interception les plus considérables. Pour ne point appesantir l'analyse, soulignons trois aspects saillants.

[188] Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015) 56:1 Harvard Intl J 82 à la p 111; voir également Peter Margulies, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism" (2014) 82 Fordham L Rev 2137 à la p 2145.

[189] Milanovic, *supra* note 188 à la p 111.

[190] *Ibid* à la p 112.

[191] *Ibid* à la p 114.

[192] Georgieva, *supra* note 179 à la p 113.

[193] Forcese, *supra* note 185.

[194] Yernault, *supra* note 92 à la p 140.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

En premier lieu, la jurisprudence de la *CEDH* s'accommode mieux du test du contrôle virtuel des données au stade du seuil d'applicabilité. La différence textuelle majeure avec le *PIDCP* est que la *CEDH* commande aux États de garantir les droits des personnes se trouvant dans leur *juridiction*, chose qui, malgré quelques remous,[195] autorise une application extraterritoriale de la *CEDH*. Aucune mention n'est faite du *territoire*. La CourEDH a eu l'opportunité de se pencher sur la question de la portée extraterritoriale de la *CEDH* dans au moins deux affaires.[196] Dans l'affaire *Weber* étudiée plus haut, les requérants alléguaient avoir été victimes d'interceptions de leurs télécommunications par le *Bundesnachrichtendienst* sur le sol allemand alors qu'ils résidaient en Uruguay. Quoique le gouvernement allemand excipa que ces derniers ne relevaient pas de la juridiction allemande au sens de l'article 1 *CEDH*,[197] la CourEDH fit peu de cas de cet argument au motif que la requête était de toute façon inadmissible.[198] Similairement dans *Liberty et autres c Royaume-Uni*, ni le gouvernement ni la Cour ne prirent position sur la question de la portée extraterritoriale de la *CEDH*, qui fut acceptée tacitement.

S'ajoute à cela, en deuxième lieu, une notion de "victime" innovante. Dès l'affaire *Kennedy*, la réception des affaires de surveillance secrètes à la CourEDH s'opère depuis une approche extensive de la notion de "victime."[199] D'ordinaire, la jurisprudence constante de la CourEDH commande que le requérant ou la requérante remplisse un certain nombre d'exigences, dont celle d'être une victime au sens de la convention. Une personne ne saurait se plaindre *in abstracto* d'une législation qui n'aura pas donné lieu à une violation concrète de ses droits.[200] La Cour déroge sensiblement à cette approche ordinaire du statut de victime dans les cas de surveillance secrète. Dans ces cas, la simple existence d'une législation permettant des mesures de surveillance, couplée à l'absence de recours au niveau national pour contester ces mesures, suffit pour obtenir le statut de victime au sens de l'article 8 (droit à la vie privée). Bref, il suffit d'être une victime potentielle de la législation incriminée pour saisir la *CEDH* en matière de surveillance massive.

[195] Voir Article 1 *CEDH*; voir notamment *Affaire Al-Skeini et autres c. Royaume-Uni*, [2011] n° 55721/07 (Sér A); Marko Milanovic, "Al-Skeini and Al-Jedda in Starsbourg" (2005) 23:1 Eur J Int'l L 121, en ligne: <http://ejil.oxfordjournals.org/content/23/1/121.full#sec-2> (l'affaire Al-Skeini provoqua de véritables remous lorsque la CourEDH rejeta l'approche de la *House of Lords* en matière d'extraterritorialité).

[196] Milanovic, *supra* note 188 à la p 58.

[197] *Affaire Weber*, *supra* note 94 au para 66.

[198] *Ibid* au para 72.

[199] *Affaire Kennedy*, *supra* note 77 au para 120.

[200] *Roman Zakharov c Russie*, n° 47143/06, [2015] CEDH (Sér A) 1 au para 164 [*Affaire Roman Zakharov*].

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

La CourEDH justifie cette approche sous prétexte que le caractère secret des mesures de surveillance des États conduit souvent à ce que ces mesures soient complètement inattaquables en pratique en l'absence de recours internes effectifs. Cette position fut récemment réaffirmée dans *Roman Zakharov c Russie*.[201] Dans cette affaire, le requérant, M. Zakharov, alléguait que le système d'interception secrète des communications de téléphonie mobile SORM en Russie avait emporté violation de son droit au respect de sa privée et de sa correspondance.[202] Dans un jugement fouillé, la CourEDH considéra qu'eu égard au défaut de recours internes effectifs, M. Zakharov n'avait pas à prouver fut-ce qu'il était au risque de voir ses communications interceptées. La simple existence de la loi constituait *per se* une ingérence dans son droit à la vie privée. On se trouve ainsi face à une jurisprudence strasbourgeoise "résolument évolutive"[203] en matière d'ingérences dans la vie privée perpétrées au moyen des nouveaux systèmes d'interception.

Quoique positive dans ces effets, d'aucuns déplorent l'activisme judiciaire de la CourEDH. Comme l'exprime le juge concordant Dedov dans *Roman Zakharov c Russie*, l'examen *in abstracto* des mesures de surveillance est problématique en ce qu'il conduit la Cour à produire des expertises, et non des arrêts, approche qui compromet son impartialité et neutralité aux yeux des États.[204] D'autres soulignent que la jurisprudence de la CourEDH en matière de surveillance massive s'harmonise mal avec les normes du DIP et du DIH.[205] Reste que cette approche nous parait de bon aloi. Il n'est pas difficile de saisir pourquoi la CourEDH défend avec tant de vigueur le droit à la vie privée, son action s'inscrivant dans un contexte de scandales retentissants (que ce soit dans l'affaire *Kennedy*, *Klass*, ou encore *Roman Zakharov*[206]) et menaces nouvelles redoutables qui pèsent sur ce droit. Les menaces sont redoutables parce que la Cour doit livrer de véritable bras de fers contre les États; avec *Roman Zakharov c Russie*, la réponse préventive de la Russie n'a pas tardé, loin de là. Trois jours avant le jugement, le 1er décembre 2015, la Douma russe vota en procédure accélérée une loi instaurant la primauté de la constitution russe sur les décisions de la CourEDH, ainsi que la faculté de rendre ses décisions inopérantes.[207]

[201] *Ibid* au para 169.

[202] *Ibid* au para 8.

[203] Yernault, *supra* 92 à la p 168.

[204] *Affaire Roman Zakharo, supra* note 200 à la p 94 (opinion concordante du juge Dedov).

[205] Milanovic, *supra* 188 à la p 2156.

[206] *Affaire Roman Zakharo, supra* note 200 à la p 89 (opinion concordante du juge Dedov).

[207] Voir Global Voices, "La Russie s'isole des institutions internationales de défense des droits de l'homme pour mieux étendre la surveillance" (19 décembre 2015), *Global Voices* (blogue), en ligne: <https://fr.globalvoices.org/2015/12/19/193151/>.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

La Russie prétend ainsi faire totale abstraction d'un jugement qui compromettait son système SORM.

En troisième lieu, malgré cette approche favorable aux victimes potentielles d'interceptions, n'allons pas croire que la CourEDH condamne les programmes de surveillance tous azimuts. La CourEDH fait au contraire preuve de nuance. À la deuxième étape de l'analyse, la CourEDH doit déterminer si l'ingérence dans la vie privée est justifiée au regard de l'article 8(2) de la *CEDH*, car prévue par la loi, poursuivant un but légitime et nécessaire dans une société démocratique. Des garanties adéquates et effectives doivent exister contre les abus puisque les systèmes de surveillances risquent de saper la démocratie au motif de la défendre. Crucialement, la CourEDH prit acte dès l'affaire *Klass* du fait que l'existence des systèmes de surveillance est "devant une situation exceptionnelle, telle la lutte contre le terrorisme ou l'espionnage extérieur, nécessaire dans une société démocratique."[208] Elle reconnait d'abondant que l'expression "sécurité nationale" est suffisamment précise et prévisible au sens de l'article 8.[209] De fait, la CourEDH valida plusieurs programmes de surveillance dans sa jurisprudence pour autant qu'ils offrent certaines garanties. Dans l'affaire *Weber*, les mesures de surveillance fondées sur la loi furent validées, car ni la manière dont les mesures de surveillance avaient été prises ni leurs ampleurs n'auraient été excessives.[210] Si dans *Liberty et autres*, la CourEDH avait conclu au manque de clarté des dispositions d'une loi sur les interceptions des communications, le régime qui succéda à cette loi dans *Kennedy* décrivait avec suffisamment de clarté les procédures applicables à la délivrance et le fonctionnement des mandats d'interception.[211]

Pour conclure, ces développements récents de la CourEDH donnent espoir pour une croissance expansive et incrémentale du droit à la vie privée en droit international, même si, réalistement, il est peu concevable qu'un État saisisse un jour les juridictions internationales telles la CIJ contre un État tiers pour violation de l'obligation de respect du droit à la vie privée de ses citoyens, les preuves relatives aux systèmes secrets d'interceptions étant difficile à réunir, pour ne pas dire impossible. La conclusion — peut-être cynique — qui s'impose est que les États tolèrent l'espionnage transnational au détriment de la vie privée de leurs citoyens.[212]

[208] *Klass et autres c Allemagne*, n° 5029/71, [1978] CEDH (Sér A) 1.

[209] *Ibid.*

[210] *Affaire Weber*, *supra* note 94 au para 118.

[211] *Affaire Kennedy*, *supra* note 77 au para 169.

[212] Il faut plus que de simples allégations ou déclarations, la CIJ doit avoir une base permettant de se former une opinion judiciaire; voir par exemple *Affaire Téhéran*, *supra* note 71 au para 82.

Une telle conclusion s'inscrit naturellement dans la lignée des instruments conventionnels protégeant le droit à la vie privée. L'article 37(1) de la *Constitution de l'Union International des Télécommunications* (*Constitution de l'UIT*) de 1892 prévoyait par exemple d'ores et déjà que les États parties doivent prendre toutes les mesures possibles "pour faire respecter le secret des correspondances internationales"[213] … à moins que les États souhaitent écarter cette obligation pour assurer l'application de leurs législations nationales.[214] Une anecdote pleine d'ironie, rapportée par Duncan Campbell, un journaliste anglais célèbre pour avoir révélé à l'opinion l'existence du réseau Échelon dans les années 2000, met en évidence le sérieux accordé à cette convention.[215] Ainsi, durant les années 1980, les opérateurs qui pénétraient le Building 600 (une base d'écoute de l'US Air Force en Angleterre) passaient un tourniquet et ne présentaient leur badge que pour se retrouver nez à nez avec une plaisanterie propre au *sigint*: une copie de la *Constitution de l'UIT*, laquelle les opérateurs s'apprêtaient à violer, était placardée au mur pour rappeler à tous l'importance du secret des correspondances.

L'ESPIONNAGE DIPLOMATIQUE: ÉROSION NORMATIVE ET DOUBLE DISCOURS

L'espionnage s'est toujours donné carrière aux côtés de la diplomatie, cependant que le droit diplomatique contient les seules règles prohibitives à l'ETP. C'est pourquoi la prise en compte de cette troisième et dernière branche du DIP est d'une grande importance. Deux cas de figure focalisent l'attention: l'espionnage territorial des agents diplomatiques par l'État d'accueil, puis l'espionnage extraterritorial réalisé par ces agents diplomatiques dispersés à l'étranger.

L'espionnage territorial par l'État d'accueil

Le premier cas de figure concerne l'espionnage des agents diplomatiques par l'État d'accueil. Les agents diplomatiques et consulaires jouissent d'un certain nombre de privilèges et d'immunités conventionnelles qui limitent sérieusement, en théorie du moins, la pratique de l'espionnage. D'abord, la personne de l'agent diplomatique est inviolable,[216] c'est-à-dire qu'elle ne peut être soumise à aucune forme d'arrestation ou détention.[217]

[213] *Constitution de l'Union Internationale des Télécommunications*, 22 Décembre 1992, UIT, *Recueil des textes fondamentaux de l'union internationale des télécommunications adoptés par la conférence de plénipotentiaires*, 2011, art 37.1 [*Constitution UIT*].

[214] *Ibid* art 37.2

[215] Campbell, *supra* note 51 à la p 118.

[216] *Convention de Vienne sur les relations diplomatiques*, 18 Avril 1961, RTNU, vol. 500, n° 7310, à la p 96, art 29 [*CVRD*].

[217] Arbour, *supra* note 79 à la p 479.

De même, les locaux,[218] les archives et documents "à tout moment et en quelque lieu qu'ils se trouvent,"[219] ainsi que la correspondance officielle,[220] sont inviolables. Conséquemment, l'État d'accueil ne saurait se livrer à de l'espionnage sur son propre territoire (ni même à de l'espionnage transnational) sans violer la CVRD et voir sa responsabilité internationale engagée. De nombreux auteurs s'accordent par ailleurs pour dire que les chefs d'État bénéficient, où qu'ils se trouvent, des mêmes immunités et privilèges en droit coutumier.[221] En se greffant à son objet même, cet ensemble de règles conventionnelles et coutumières pourraient circonscrire sérieusement l'ETP.

Dans les faits, toutefois, ces immunités et privilèges n'ont pas l'envergure nécessaire pour écarter les États de pratiques absolument contraires à la convention — loin s'en faut. L'espionnage territorial des diplomates étrangers semble être une activité de routine largement tolérée par les États.[222] L'examen du *Foreign Intelligence Surveillance Act* (*FISA*) en 1978 par le Congrès des États-Unis l'illustre parfaitement.[223] Il est piquant de noter qu'à l'époque le Congrès s'inquiétait du fait que la *FISA* — une loi encadrant l'utilisation de moyens de surveillance électronique — puisse autoriser la surveillance des enceintes diplomatiques situées aux États-Unis et conduise à violer la *CVRD*.[224] L'affaire fit controverse, mais elle ne fit pas long feu. L'affaire s'éteint lorsque la branche exécutive fournit au Congrès une liste — très longue — des États qui avaient pu espionner les enceintes diplomatiques américaines à l'étranger dans le passé. La loi fut aussitôt adoptée.

Cet exemple est topique de la réalité. Les États ignorent superbement la *CVRD* par un ETP routinier directement contraire à leurs obligations internationales, cependant qu'aucune *opinio juris* n'indique que les immunités attachées aux biens et communications diplomatiques soient des legs juridiques obsolètes inapplicables aujourd'hui.[225] Sur ce point, on retiendra avec profit l'observation pénétrante de Reisman: "[States presumably have concluded] that the need for and value of intelligence gained by

[218] *CVRD*, *supra* note 216 art 22.

[219] *Ibid* art 24.

[220] *Ibid* art 27(1).

[221] Arbour, *supra* note 79 à la p 224; *Mandat d'arrêt du 11 avril 2000 (République démocratique du Congo c Belgique)*, arrêt [2000] CIJ rec 3 à la p 19 et 43.

[222] Eileen Denza, *Diplomatic Law. Commentary on the Vienna Convention on Diplomatic Relations*, New York, Oxford University Press, 2008 à la p 223.

[223] Forcese, *supra* note 52 à la p 197.

[224] *Ibid.*

[225] Denza, *supra* note 222 à la p 224.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

electronic surveillance outweighs the incremental erosion of the norm upholding the inviolability of diplomatic premises and their communications."[226] D'autant que cette érosion est peu couteuses pour les États; la responsabilité engagée par de tels actes se règle exclusivement suivant le régime dégradé de responsabilité de la *CVRD*.

L'espionnage extraterritorial par les agents diplomatiques

Le second cas de figure concerne l'espionnage extraterritorial commis par les agents diplomatiques à l'encontre de l'État d'accueil. Espionnage et diplomatie sont toujours allés de pair. Dès le XIXe siècle, les États ont introduit l'usage de joindre un ou plusieurs attachés militaires à leurs missions diplomatiques, ceux-ci se transformant fréquemment par la suite en centre d'espionnage et d'intrigue.[227] Les agents diplomatiques recevaient d'ailleurs autrefois le titre "d'honorables espions," au temps où les institutions de renseignement n'existaient pas. La pratique persiste assurément aujourd'hui.

La *CVRD* reconnait la fonction d'information des diplomates à son article 3(1)(d). Elle précise que la mission diplomatique peut «[s]'informer par tous les moyens licites des conditions et de l'évolution d'événements dans l'État accréditaire et faire rapport à ce sujet au gouvernement de l'État accréditant." Déterminer si l'ETP est licite en l'espèce, c'est déterminer le sens juridique précis du qualificatif "par tous les moyens licites." Or, cette condition de licéité des moyens est l'une des dispositions les plus ambigües et contestées de la *CVRD*.[228] D'après Pancracio et certains auteurs, la disposition renvoie au droit interne de l'État accréditaire. La condition des moyens devrait s'entendre selon eux "au sens large pour inclure tant le contenu de certaines informations que le procédé utilisé pour y accéder."[229] L'article 3(1)(d) interdirait ainsi aux diplomates l'acte d'espionnage portant sur des sources fermées, donc protégées par l'État accréditaire dans son droit interne. La fonction d'information serait circonscrite aux sources *ouvertes*. Pancracio dépasse la lettre du traité pour se rattacher à l'esprit du traité.

On ne perçoit pas ces arguments. Nous sommes plutôt d'accord avec Kish,[230] pour qui la condition de licéité des moyens doit être entendue comme faisant référence à la *CVRD* en vertu du principe de primauté du

[226] W Michael Reisman, "The Plainiff's Dilemma: Illegally Obtained Evidence and Admissibility in International Adjudication" (1982) 76 Am J Int'l L 737 à la p 752.

[227] Philippe Cahier, *Le Droit diplomatique contemporain*, Librairie Droz, 1964 à la p 73.

[228] Kish, *supra* note 4 à la p 54.

[229] Jean-Paul Pancracio, *Droit et institutions diplomatiques*, Paris, Pedone, 2007 à la p 175.

[230] Kish, *supra* note 4 à la p 55.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

droit international avancé dans le préambule.[231] D'autres éléments corroborent cette interprétation. Si l'article 3(1)(d) faisait référence au droit interne des États accréditaires, on se trouverait face à un régime éminemment complexe où la permissibilité de certaines collectes de renseignement varierait d'État en État. Une telle variation dans l'exercice de la fonction diplomatique d'information serrait contraire au principe de réciprocité reconnu à l'article 47(2)(a) de la *CVRD*. De plus, suivant la Commission du droit international, le membre de phrase "des conditions et de l'évolution d'événements" de l'article 3(1)(d) couvre tout ce qui meut le pays accréditaire en profondeur et qui pourrait intéresser l'État accréditant.[232] Le tout est défini de manière suffisamment large pour qu'aucune prohibition portant sur *l'objet* (ceci inclut les sources fermées) du renseignement n'entrave la fonction de collecte d'information.[233] L'article 3(1)(d) porte ainsi bien sur les moyens employés. Cette conclusion surprend-elle?

Quoi d'étonnant pourtant, nous avons déjà vu que l'espionnage diplomatique territorial est abondement pratiqué et toléré. De même ici, tous les États jouent tour à tour le rôle d'État accréditant et accréditaire, ce qui assure un traitement réciproque des agents diplomatiques exerçant leurs fonctions d'information. Le diplomate-espion observe autant qu'il est observé. Rappelons qu'au terme de la *CVRD*, l'État accréditaire dispose précisément de nombreux outils pour contrôler la fonction de renseignement,[234] que soit en déterminant l'effectif de la mission,[235] en refusant l'accès à certains des fonctionnaires,[236] en refusant l'installation d'un poste émetteur radio,[237] ou, plus crucialement, en expulsant des diplomates à sa discrétion.[238] Chaque État se voit ainsi compensé d'une possible intrusion dans sa sécurité nationale par le bénéfice que représente des sources d'informations chez les autres États.[239] Du reste, admettons que la plupart des informations dont peut avoir besoin un gouvernement au regard des activités d'un État accréditaire sont réalistement ouvertes: "[R]evue de presse écrite et audiovisuelle, entretiens avec l'attaché de presse … dépouillement

[231] Qui dit: "Affirmant que les règles du droit international coutumier doivent continuer à régir les questions qui n'ont pas été expressément réglées dans les dispositions de la présente Convention."

[232] Forcese, *supra* note 52 à la p 200.

[233] Kish, *supra* note 4 à la p 55.

[234] Chesterman, *supra* note 8 à la p 1088.

[235] *CVRD*, *supra* note 216 art 11(1).

[236] *Ibid* art 11(2).

[237] *Ibid* art 27(1).

[238] *Ibid* art 9.

[239] *Ibid*.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

de revues spécialisées [et] colloques scientifiques sont très riches en renseignements… parfois mêmes classifiés."[240]

Concluons avec un dernier point de controverse. La question des immunités des chefs d'États a pu surgir dans les allégations d'espionnage des communications de la chancelière allemande Angela Merkel et de la présidente brésilienne Dilma Rousseff à l'encontre de la NSA. Les téléphones personnels des deux chefs d'État auraient en effet été mis sur écoute depuis les ambassades américaines,[241] ce qui violerait leurs immunités coutumières. Pour Russel Buchan, un tel espionnage violerait même le principe de non-intervention et mettrait à mal l'ordre et la sécurité internationale.[242] L'histoire récente nous montre nonobstant que l'illégalité de cette pratique n'est pas aussi manifeste qu'il n'y parait. Signalons que les deux chefs d'État se sont bien abstenus, en bout de ligne,[243] de qualifier cette écoute de fait internationalement illicite. La déclaration de Merkel joue sur la grammaire et l'illustre éloquemment: "Spying between friends, that's just not done."[244] C'est là un membre de phrase qui se drape de la même fonction atténuante l'égard de l'ETP identifiée précédemment au seuil de ce texte, pointant vers l'acte inamical, non vers le fait internationalement illicite. Le double discours est une constante.

Au terme de cette troisième Partie, nous avons pu étudier des normes du droit diplomatiques qui prohibent clairement l'ETP en s'attardant sur son objet et sur ses moyens. Nous avons aussi constaté que les normes sont une chose, et leur application en est souvent une autre. La Partie IV qui suit, abordant deux droits inédits allégués par le Timor-Leste, veux souligner qu'une dernière prohibition à l'espionnage, prometteuse cette fois, peut être dégagée en DIP.

[240] Pancracio, *supra* note 229 à la p 178.

[241] Frédéric Lemaitre, "Angela Merkel espionnée par la NSA" (2013) *Le Monde*, en ligne: <http://www.lemonde.fr/international/article/2013/10/24/angela-merkel-espionnee-par-la-nsa_3502360_3210.html>.

[242] Buchan, *supra* note 117 à la p 178.

[243] Rousseff a d'abord qualifié l'espionnage d'acte contraire au droit international, avant de se rétracter et d'employer les euphémismes habituels. Voir notamment Julian Borger, "Brazilian President: US Surveillance a 'Breach of International Law" (2014) *The Guardian*, en ligne: <http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance>; comparer Jenna McLaughlin, "Brazilian President Dilma Rousseff's Flip-Flop on NSA Spying" (2015) *The Intercept* (blogue), en ligne: <https://theintercept.com/2015/06/29/brazilian-president-dilma-rousseffs-flip-flop-nsa-spying/>.

[244] Alex Spillius, "Angela Merkel: Spying between Friends Is Unacceptable" (24 octobre 2013) *The Telegraph*, en ligne: <http://www.telegraph.co.uk/news/worldnews/europe/germany/10402570/Angela-Merkel-spying-between-friends-is unacceptable.html>.

Tendances récentes: de nouvelles limites à l'espionnage?

Que signifient les principes fondamentaux de l'égalité souveraine, de la bonne foi et le secret professionnel des avocats pour le processus de règlement pacifique des différends et pour le statut de l'ETP? Telle est la question que nous souhaitons maintenant élucider. Nous mettrons d'abord en contexte nos interrogations en présentant l'affaire *Timor-Leste c Australie* qui les soulevait. Par la suite, nous présenterons, dans un premier temps, le droit à la confidentialité des communications avec les avocats et conseillers juridiques découlant du secret professionnel comme principe général du droit, puis dans un second temps, nous évaluerons le droit à la non-ingérence dans ces communications, découlant du principe d'égalité souveraine. Nous montrerons que seul ce dernier droit prohibe l'espionnage.

L'affaire *Timor-Leste c Australie*

Il est exceptionnel qu'une affaire d'espionnage donne naissance à un contentieux entre États. C'est pourquoi nous prenons le temps de l'exposer ici. Le 3 mars 2014, la CIJ indiqua des mesures conservatoires dans l'affaire des *Questions concernant la saisie et la détention de certains documents et données* (*Timor-Leste c Australie*),[245] une affaire qui pose des questions nouvelles en matière d'espionnage. La dispute nait du fait que, le 3 décembre 2013, des documents et des données furent saisis par des agents du service de renseignement de l'Australie dans les locaux professionnels d'un conseil juridique du Timor-Leste à Narrabundah (territoire de la capitale australienne), M. Bernard Collaery, en vertu d'un mandat délivré sur la base de l'article 25 de l'*Australian Security Organisation Act*.[246] L'Australie invoqua la sécurité d'État. Selon le Timor-Leste, les éléments saisis comprenaient des documents et données confidentiels se rapportant à un arbitrage entre ce dernier et l'Australie sur le gisement de gaz "Greater Sunrise" devant la Cour Permanente d'Arbitrage (CPA), en vertu du *Traité sur la mer de Timor*.[247] Quoique ces procédures parallèles devant la CPA soulèvent des questions intéressantes quant aux conséquences de l'espionnage sur la validité des traités, elles n'irradient pas immédiatement la

[245] *Affaire Timor-Leste c Australie, supra* note 10 à la p 16.

[246] *Ibid* au para 22.

[247] *Ibid* au para 24. Cette procédure devant la CPA concerne des allégations distinctes de celles portées devant la CIJ, selon lesquelles le Timor-Leste cherche à voir déclaré nul ou non-contraignant le *Traité sur la mer de Timor* au motif que l'Australie aurait placé les locaux de ce dernier sous écoute électronique.

question de sa licéité.[248] Notre analyse se concentrera donc sur les mesures conservatoires indiquées par la CIJ.

Les mesures conservatoires font parties de l'arsenal des États dans leurs conflits politiques.[249] Obtenir des mesures conservatoires, c'est pour le demandeur obtenir dès le départ une victoire morale et juridique pesante sur l'État adverse. C'est ce que le Timor-Leste parvint à obtenir dans le cas présent, qui constitue la plus récente escarmouche d'un long duel entre "David et Goliath" au sujet du partage des revenus du pétrole et gaz issus de la mer qui sépare les deux pays. Le Timor-Leste demanda avec succès à la CIJ d'indiquer des mesures conservatoires contre l'Australie, notamment qu'elle lui remette les documents et données saisis et cesse toute interception des communications avec ses avocats et conseillers juridiques.[250] Pour y arriver, le Timor-Leste s'appuya sur des droits jamais évoqués auparavant en DIP, ce qui n'empêcha pas les médias d'annoncer en grande pompe que la CIJ avait reconnu les nouveaux droits du Timor-Leste et ordonner à l'Australie de "cesser d'espionner son voisin."[251]

La victoire du Timor-Leste n'est pas aussi éclatante que le laissent croire les médias. Dans sa requête, celui-ci déclara vouloir protéger *deux* droits. D'une part son droit à l'inviolabilité et l'immunité des biens saisis, et d'autre part, son droit à la non-ingérence dans les communications privilégiées ou le secret professionnel.[252] Dans un certain flou artistique, entretenu ou non, on ne saurait dire, le Timor-Leste fusionna en un seul concept juridique les deux derniers éléments (le droit à la non-ingérence et le secret professionnel) dans son mémoire.[253] Il s'agit pourtant là de deux droits distincts. Le droit à la non-ingérence découlerait d'un principe général du droit international, soit un principe propre aux relations internationales. Le secret professionnel, quant à lui, serait un droit dérivé des législations internes des États s'appliquant par analogie aux relations internationales,

[248] Kate Mitchell & Dapo Akande, "Espionage & Good Faith in Treaty Negociations: East Timor v Australia" (20 janvier 2014) *EJIIL:Talk!* (blogue), en ligne: <http://www.ejiltalk.org/author/mitchellakande/>; voir également Sarah Heathcote, "Explainer: Australia and Timor Leste in the Hague" (5 décembre 2013) *The Conversation* (blogue), en ligne: <http://theconversation.com/explainer-australia-and-timor-leste-in-the-hague-21215>.

[249] Terry D Gill, "*Litigation Strategy at the International Court: A Case Study of the Nicaragua v. Unite States Dispute*," Leiden, Martinus Nijhoff Publishers, 1989 à la p 86.

[250] *Affaire Timor-Leste c Australie*, *supra* note 10 au para 5.

[251] AFPQC2, "La CIJ ordonne à l'Australie de cesser d'espionner le Timor oriental" (3 mars 2014) *TheHuffingtonPost.ca — Québec*, en ligne: <http://quebec.huffingtonpost.ca/2014/03/03/la-cij-ordonne–laustra_n_4891237.html>.

[252] *Questions Relating to the Seizure and Detention of Certain Documents and Data*, "Mémoire du Timor-Leste" (28 avril 2014), [2013] CIJ Mémoires (vol 1) au para 6.2 [*Mémoire du Timor-Leste*].

[253] *Questions Relating to the Seizure and Detention of Certain Documents and Data*, "Contre-Mémoire de l'Australie" (28 juillet 2014), [2013] CIJ Mémoires (vol 1) à la p 53 [*Contre-Mémoire*].

donc un principe général du droit (PGD). D'emblée, une distinction s'impose entre deux droits aux portées potentiellement différentes.

Ceci n'a pas échappé à la CIJ, pour qui le Timor-Leste avance trois droits distincts: (1) le droit à la non-ingérence dans les communications avec les conseillers juridiques; (2) le droit au secret professionnel des États avec leurs conseillers comme principe général du droit; et (3) le droit à l'inviolabilité et l'immunité des biens saisis.[254] Au moment d'indiquer des mesures provisoires, la CIJ doit s'assurer que les droits allégués sont à tout le moins plausibles, c'est-à-dire qu'il est réalistement permis de penser que, lorsqu'elle se prononcera sur le fond de l'affaire, la Cour reconnaitra leur existence et leur applicabilité. La CIJ conclut ici qu'un droit à la non-ingérence des communications était plausible, mais ne se prononça pas explicitement sur la plausibilité d'un secret professionnel comme principe général du droit.[255] La Cour ne tira aucune conclusion quant au troisième droit à l'inviolabilité et l'immunité des biens saisis.

Une question se pose alors: les deux droits retenus par la CIJ prohibent-ils l'espionnage des communications d'un autre État avec ses conseillers juridiques? Cette question est loin d'être académique. La pratique étatique est riche d'actes d'espionnage des communications privilégiées d'un État tiers avec ses avocats et conseillers juridiques. Par exemple, l'affaire des *Essais nucléaires (Australie c France, Nouvelle-Zélande c France)*[256] en 1975 ou encore l'affaire *Buraimi Oasis (Arabie saoudite c Royaume-Uni)*[257] en 1965 auraient été entachées par des actes d'espionnage. Pas plus tard qu'en septembre 2015, l'arbitrage relatif au différend terrestre et maritime entre la Croatie et la Slovénie devant la CPA se trouva perturbé (la sentence n'est pour cette raison toujours pas rendue) par une affaire d'écoutes ayant révélé le contenu d'échanges téléphoniques entre un arbitre slovène et un agent.[258] Les services secrets croates auraient mis sur écoute l'arbitre slovène, ce qui leur a valu d'être accusés d'espionnage.[259] Or, la licéité de ces actes d'espionnage reste encore indéterminée en DIP. Puisque la CIJ n'a pu régler la question de l'existence des droits allégués — le Timor-Leste et l'Australie ayant convenu de régler à l'amiable leur différend le 15 mai 2015 — la question mérite d'être étudiée pour déterminer si, dans

[254] *Affaire Timor-Leste c Australie, supra* note 10 au para 24.

[255] *Ibid* au para 28.

[256] Christopher D Baker, "Tolerance of International Espionage: A Functional Approach" (2003) 19:5 Am U Intl L Rev 1091, Part III; Mélanie Dubuy, "Chronique de jurisprudence internationale" (1 octobre 2015) *Sentilnelle Droit International* (blogue) en ligne: <http://www.sentinelle-droit-international.fr/?q=content/cij-ordonnance-du-22-avril-2015-questions-concernant-la-saisietimor-leste-c-australie>.

[257] *Ibid.*

[258] *Ibid.*

[259] *Ibid.*

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

le futur, les États victimes de cette forme d'espionnage pourront braver l'audace des États-espions.

LE SECRET PROFESSIONNEL DES AVOCATS ET CONSEILLERS JURIDIQUES

Explorons d'abord la première hypothèse avancée par le Timor-Leste, selon laquelle le secret professionnel des avocats et conseillers constituerait un PGD applicable aux relations interétatiques. L'article 38(1)(c) du *Statut de la CIJ* mentionne les principes généraux de droit reconnus par les nations comme étant l'une des sources subsidiaires du droit international.[260] Elle permet à la Cour de déduire des principes communs à partir des systèmes juridiques nationaux, qui sont ensuite appliqués au domaine des relations internationales. Une fois définis par la Cour, ces PGD deviennent opposables aux États sans l'expression formelle de leur volonté. Pour cette raison, la CIJ a rarement eu recours aux PGD sans détour. Ce sont surtout les domaines moins controversés de la preuve, de la procédure et de l'administration de la justice qui ont servi de terrain privilégié pour la déduction de PGD.[261] Aussi, la question de savoir si un PGD limitait d'une quelconque manière l'espionnage avait été jusqu'à ce jour plutôt théorique.[262] L'interrogation qu'appelle l'affaire *Timor-Leste c Australie* est de savoir si on peut déduire des systèmes internes un secret professionnel transposable aux relations internationales à même de prohiber l'espionnage.

Résoudre cette interrogation nous amène à dire un mot sur la méthode de détermination d'un PGD. L'existence d'un PGD est conditionnée par la réunion de plusieurs éléments de preuve. Quoique cette méthode fasse l'objet de débats et de nombreux malentendus, celle-ci a été habilement résumée par le Juge Tanaka dans *l'affaire du Sud-ouest africain*: "[L]es principes généraux sont censés être des principes de droit privé dégagés grâce

[260] Jean-Yves De Cara, "Les principes généraux de droit au sens de l'article 38 du statut de la Cour Internationale de Justice" dans *Les principes généraux du droit*, Bruxelles, Bruylant, 2005.

[261] Brownlie, *supra* note 149 à la p 18.

[262] Certains ont soutenu, à tort, que l'illégalité de l'espionnage au plan interne équivalait à son illicéité sur le plan international. Comme nous l'avons déjà souligné, les États disposent depuis longtemps de lois internes prohibant l'espionnage, soit en assimilant l'espionnage à de la trahison, soit en criminalisant l'espionnage lui-même. Cette situation a parfois contribuée à ce que l'espionnage soit perçu comme une activité illicite en droit international. Pourtant, élever cette prohibition interne au rang de principe de droit international au titre de l'article 38(1)(c) du *Statut de la CIJ* est inadmissible. Premièrement, cette prohibition interne ménage la responsabilité criminelle individuelle des ressortissants nationaux et des étrangers. Deuxièmement, cette prohibition interne ne constitue pas un principe du droit domestique à même d'être traduit dans les relations interétatiques, contrairement, par exemple, aux principes traditionnels de bonne foi ou encore d'enrichissement injustifié.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

à la méthode de droit comparé et applicables par analogie à des questions de droit international."[263] Cette méthode implique essentiellement trois étapes: (*a*) identifier des règles communes aux ordres juridiques internes (droits "civil," romano-germanique, *common law*, etc.); (*b*) dépouiller ces règles communes des particularités nationales pour les ramener à leurs aspects généraux;[264] et, enfin, (*c*) s'assurer que le principe ainsi dégagé soit "transposable" aux conditions particulières de la vie internationale.[265] La méthode de détermination est un véritable parcours à obstacles, mais, selon le Juge dissident Callinan, le secret professionnel des avocats et conseillers avait l'envergure nécessaire pour franchir cette épreuve.[266] Étudions dès à présent ces trois étapes.

Le secret professionnel des avocats en droit interne

Le secret professionnel des avocats et conseillers juridiques semble franchir (laborieusement) la première étape de la méthode Tanaka. Comme l'indique le Timor-Leste dans son mémoire,[267] de nombreuses législations nationales reconnaissent le secret professionnel, auxquelles s'ajouterait une jurisprudence abondante de plusieurs cours arbitrales,[268] ainsi que celle de la Cour de justice de l'Union européenne[269] et de la CourEDH.[270]

[263] *Affaires du Sud-Ouest Africain*, *supra* note 61 au para 88.

[264] Voir notamment Michael D Nolan & Frédéric Gilles Sourgens, "Issues of Proof of General Principles of Law in International Arbitration" (2009) 3:4–5 World Arb & Mediation Rev 505.

[265] *Ibid.*

[266] *Questions concernant la saisie et la détention de certains documents et données (Timor-Leste c Australie)*, Ordonnance du 3 mars 2014 [2014] CIJ, juge Callinan, dissident, au para 4. Le Juge Callinan n'est pas le seul à considérer que le soutènement du secret en droit international se trouve dans les principes généraux de droit. Bien avant lui, Paul Reuter soutint que "c'est dans les principes généraux du droit, et particulièrement du droit interne, qu'un interprète ira puiser les éléments qui doivent lui permettre de construire une protection du secret" dans Paul Reuter, "Le droit au secret et les institutions internationales" (1956) 2 AFDI 46 à la p 58.

[267] *Mémoire du Timor-Leste, supra* note 252 au para 6.2.

[268] *Dr Horst Reineccius et al c Bank for International Settlements* (CPA), Procedural Order No 6, 11 Juin 2002, à la p 10, en ligne: <http://www.pca- cpa.org/showfile.asp?fil_id=405>; cité dans *Vito G Gallo c Government of Canada* (PCA-NAFTA), Procedural Order No 3, 8 avril 2009, au para 49, en ligne: <http://www.naftalaw.org/Disputes/Canada/Gallo/Gallo-Canada-Order3.pdf>; voir aussi *Libananco Holdings Co Limited c Republic of Turkey*, ICSID No ARB/06/8, Decision on Preliminary Issues, 23 Juin 2008.

[269] Voir par exemple *AM & S Europe Limited c Commission des Communautés européennes*, n°155/79 [1982] CEDH au para 18, en ligne: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:61979CJ0155&from=EN>.

[270] Voir par exemple *Niemietz c Allemagne* n°13710/88 [1993] 16 CEDH 97 au para 37.

En réalité, et tel que l'allègue l'Australie, cette jurisprudence ne saurait servir de raccourci puisqu'aucune ne se prononce de front sur l'existence d'un secret professionnel au sens de l'article 38(1)(c) du *Statut de la CIJ*.[271] Il faut plutôt s'en remettre à la législation des principaux systèmes juridiques du monde. À partir de là, on constate que le secret professionnel des législations nationales présente deux composantes distinctes: (1) une obligation de se taire à laquelle est tenu l'avocat ou le dépositaire du secret; ainsi (2) qu'un droit au silence de ce dernier.[272] Le secret professionnel en droit interne se situe donc principalement au plan d'une relation interindividuelle,[273] dont l'objectif est de préserver la stratégie de la défense de la divulgation à ses accusateurs. En dépit de cela, suivant le Timor-Leste, un tel secret professionnel protègerait *contre* les interceptions d'un *tiers* — l'Australie.

Cette conception affronte une difficulté d'ordre conceptuelle. On s'apercevra que le Timor-Leste s'appuie vraisemblablement sur une conception juridique du secret professionnel qui trouve son soutènement, *non dans les législations nationales*, mais dans la jurisprudence de la CourEDH. Certes la CourEDH a reconnu un secret professionnel de manière indirecte (aucun article de la *CEDH* ne garantissant ce droit), comme un aspect du droit à la vie privée (article 8) et du droit à un procès équitable (article 6).[274] Mais, non seulement les États n'ont pas de droit à la vie privée en droit international comparable à celui reconnu aux individus par les droits de la personne,[275] nous avons vu au surplus que les règles communes aux ordres juridiques internes élaborent un secret professionnel juridiquement distinct. Ce secret professionnel est bien éloigné du droit à la vie privée et du droit au procès équitable de la CourEDH, qui protègent *contre* l'interception et l'enregistrement, *par un tiers*, des communications entre un client et son avocat.

En somme, nous pouvons concevoir qu'un secret professionnel des avocats et conseillers franchisse la première étape de la détermination d'un PGD, mais celui-ci protègerait contre la divulgation *par les avocats* et ne saurait se réclamer de la jurisprudence de la CourEDH, qui protège contre l'immixtion *par les tiers*. Déjà donc, la reconnaissance du secret professionnel ne se fait pas sans écueils.

[271] *Contre mémoire*, *supra* note 253 au para 4.32.

[272] Jean Louis-Beaudoin, *Secret professionnel et droit au secret dans le droit de la preuve*, Paris, Librairie Générale, 1965 à la p 3.

[273] Dean Spielmann, "Le secret professionnel de l'avocat dans la jurisprudence de la Cour européenne des droits de l'homme" dans Georges-Albert Dal, dir, *Le secret professionnel de l'avocat dans la jurisprudence européenne*, Bruxelles, Larcier, 2011 à la p 27.

[274] *Ibid* à la p 40.

[275] Léopold Peyrefitte, *Droit de l'espace*, Paris, Dalloz, 1993 à la p 274.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

Les exceptions au secret professionnel en droit interne

Des difficultés plus importantes surgissent à la seconde étape. Lorsqu'on rapporte le droit interne à ses aspects les plus généraux, il se dégage des principaux systèmes juridiques du monde diverses entorses juridiques au secret avocat-client qui chahutent l'analyse. Par exemple, le secret est mis en échec "lorsque la partie qui l'invoque n'est pas en mesure de démontrer l'existence d'un intérêt à protéger, lorsqu'il empêche le jury d'avoir accès à une information susceptible d'innocenter l'accusé, ou encore lorsque l'avis juridique est recherché par le client pour commettre un crime ou une fraude."[276] Deux thèses s'affrontaient donc inévitablement quant à la portée des limites du secret professionnel. Le Timor-Leste avançait ce que nous appelerons une "thèse absolutiste."[277] Pour ce dernier, le secret professionnel dérivé des législations nationales ne connaitrait aucune exception en DIP. L'Australie contesta ce point en soutenant une thèse "relativiste."[278] D'après elle, si le secret professionnel devait être reconnu comme PGD, ce qu'elle nie, l'exception de crime ou fraude devrait également être reconnue et s'appliquer aux faits d'espèce, la saisie des documents ayant été effectuée à des fins de sécurité nationale.[279]

Des thèses en présence, la thèse australienne nous apparait plus convaincante pour deux motifs. Le premier motif est que non seulement la thèse absolutiste du secret professionnel du Timor-Leste ne trouve pas d'équivalent dans les systèmes juridiques internes,[280] mais qu'elle serait bien isolée de la pratique des tribunaux *ad hoc* de l'ONU qui admettent l'exception de crime ou fraude.[281] L'exception est par ailleurs reconnue dans de nombreux pays.[282] Le second motif est que même si l'on devait, comme l'enjoint le Timor-Leste, solliciter la conception du secret professionnel qui brille dans la jurisprudence de la CourEDH, cette conception suppose quand même un secret professionnel susceptible de restrictions, le droit à la vie privée n'étant pas un droit absolu.[283]

Au bout du compte, on s'aperçoit que dépouiller les règles nationales est un chemin semé d'embuches. Le secret professionnel soulève plus de questions qu'il n'apporte de réponses. Aussi n'est-il pas surprenant, comme l'exprime Tully, que "[s]uch challenging questions were neatly

[276] Sipowo, *supra* note 24 à la p 91.

[277] Notre expression.

[278] *Contre mémoire*, *supra* note 253 au para 4.44.

[279] *Ibid.*

[280] *Ibid* au para 4.36.

[281] Sipowo, *supra* note 24 à la p 87ss.

[282] *Contre mémoire*, *supra* note 253 au para 4.44.

[283] Sipowo, *supra* note 24 à la p 93.

sidestepped by the ICJ."[284] Il faut insister sur ce point: les PGD se donnent davantage carrière sur les terrains solides et consensuels des relations internationales; plus difficilement sur les terrains mouvants et changeants que sont l'espionnage et la sécurité nationale.

Les obstacles de transposition du secret professionnel

L'analyse qui précède permet d'entrevoir les difficultés auxquelles aurait été confrontée la CIJ à la première et à la seconde étape de la méthode Tanaka, eut-elle étudié la question au fond. Mais c'est à la troisième étape — celle de la transposition aux relations internationales — que le bât blesse le plus. Certaines difficultés sont fatales à la reconnaissance du secret professionnel.

D'abord, contrairement aux tribunaux nationaux qui sont l'émanation des États, la CIJ, dont la compétence est consensuelle, peut difficilement étudier tous les aspects du secret professionnel, spécialement s'il met en jeu une exception pour sécurité nationale. À un niveau plus abstrait, on dira que les tribunaux nationaux et internationaux sont de natures distinctes. La structure des premiers est horizontale, celle des seconds, verticale.[285] Bien plus, au terme de l'article 49 de son *Statut*, la CIJ n'a pas le pouvoir d'exiger un témoignage ou la production de preuve. La Cour peut seulement prendre acte du refus d'un État. Or, la pratique révèle que les États refusent selon leur gré de produire les éléments de preuve touchant à leur sécurité nationale.

L'affaire du *Détroit de Corfou* l'illustre bien. En 1949, le Royaume-Uni refusa de produire certains documents cruciaux intitulés "XCU" (signifiant "Exercice Corfu") en excipant le secret naval.[286] L'Albanie avançait dans son contre-mémoire que les équipages des navires britanniques s'étaient livré à de l'espionnage constitutif d'un passage non inoffensif sur sa mer territoriale en violation du droit international. Le Royaume-Uni répliqua qu'il n'avait jamais donné l'ordre à ses navires d'espionner les côtes albaniennes, tout en refusant de produire la pièce XCU. La CIJ ne put que prendre acte de ce refus et finit par rendre un jugement en faveur du Royaume-Uni.[287] Rendus publics des décennies plus tard, les documents XCU confirmèrent ce que tous suspectaient: le Royaume-Uni avait

[284] Stephen Tully, "Legal Professional Privilege and National Security" (2014) 24:26 Bar News NSW 24 à la p 25.

[285] Gernot Biehler, *Procedures in International Law*, Dublin, Springer, 2008 à la p 38.

[286] *Affaire du Détroit de Corfou*, [1949] CIJ rec 4 à la p 32.

[287] Kenneth J Keith, "Naval Secrets, Public Interest Immunity and Open Justice" dans Karine Bannelier, Theodore Christakis et Sarah Heathcote, dir, *The ICJ and the Evolution of International: The Enduring Impact of the Corfu Channel Case*, New York, Routledge, 2012 à la p 125.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

bien donné l'ordre à ses navires d'espionner.[288] Comme l'étaye cette illustration, la CIJ doit ainsi parfois supporter la mauvaise foi des États.[289]

Dans un même ordre d'idées, les exceptions au secret professionnel évoquées par l'Australie posent d'importantes difficultés de transposition devant la CIJ. Cette dernière évita la question dans son ordonnance de mesures provisoires. Seul le Juge Cançado Trindade, dans son opinion individuelle, aborda le point de savoir si une juridiction internationale comme la CIJ dispose des outils requis pour se prononcer en faveur d'allégations de sécurité nationale. Illustrant ses propos avec la Cour pénale Internationale (CPI) et la Cour interaméricaine des droits de l'homme (CIDH), le Juge Cançado Trindade suggéra qu'aujourd'hui les "juridictions internationales savent de toute façon comment traiter les éléments confidentiels … et [que] les préoccupations de sécurité nationale … ne sauraient le faire oublier."[290] En réalité, ces parallèles avec la CPI et la CIDH ne sont pas des plus fructueux.

D'une part, très peu de règles encadrent la production des éléments probatoires devant la CIJ, contrairement à ces deux juridictions internationales,[291] cependant qu'aucune règle n'existe pour maintenir le secret de la preuve. La CIJ peut certes prononcer un huit clos si des motifs graves et clairs militent en ce sens, mais ceci est rare en pratique.[292] D'autre part, s'agissant des atteintes aux droits humains ou aux violations du droit pénal international, l'obligation des États de coopérer avec les juridictions internationales telles la CPI et la CIDH s'explique par le fait qu'un refus systématique, de communiquer des documents pour des raisons de sécurité, compromettrait l'objet et le but même de ces juridictions.[293] À l'inverse, il nous faut reconnaitre que la nature consensuelle de la compétence de la CIJ l'amène à une certaine déférence de la souveraineté étatique, chose

[288] *Ibid* à la p 136.

[289] De même dans l'affaire du *Personnel diplomatique et consulaire des États-Unis à Téhéran (États-Unis c Iran)*, la CIJ posa une question à un agent américain à laquelle il refusa de répondre. Comme dans l'*Affaire du Détroit de Corfou*, la CIJ prit simplement acte du refus sans en tirer aucune inférence. De même, en 2005, la Serbie refusa de produire des documents classés secrets militaires et la CIJ prit acte du refus dans l'affaire *Application de la Convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c Serbie-et-Monténégro)*, arrêt, [2007] CIJ rec 47 au para 204–05.

[290] *Questions concernant la saisie et la détention de certains documents et données (Timor-Leste c Australie)*, Ordonnance du 3 mars 2014 [2014] CIJ, au para 40 (juge Cançado Trindade, dissident) [*Questions concernant la saisie et la détention*, Cançado Trindade].

[291] Géraldine Giraudeau, *Les différends territoriaux devant le juge international*, Leiden, Boston, Martinus Nijhoff Publishers 2013 à la p 413.

[292] Robert Kolb, *La Cour international de Justice*, Paris, A. Pedone, 2013 à la p 1028.

[293] *Questions concernant la saisie et la détention*, Cançado Trindade, *supra* note 290 au para 39.

[294] Sipowo, *supra* note 24 à la p 384.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

qui ne trouve aucune correspondance dans la pratique des mécanismes régionaux des droits humains ou de la CPI.[294] Prudente, la CIJ s'efface sur ce point.

Un dernier obstacle se profile à l'horizon. Dans le paragraphe opératif de son ordonnance, on s'apercevra que la CIJ emploie l'expression "ingérer" plutôt que l'expression "intercepter" (qu'employait le Timor-Leste dans sa requête en mesures provisoires en demandant que "[l]'Australie donne l'assurance qu'elle n'interceptera pas ni ne fera intercepter les communications entre le Timor-Leste et ses conseillers juridiques").[295] L'emploi du terme "ingérer," suivant un commentateur, "has introduced a considerable degree of ambiguity into a potentially very significant operative paragraph of the order."[296] C'est d'après nous tout l'inverse. Le choix de cette expression est révélatrice de la conception de la CIJ. Ce terme révèle non seulement la préférence de celle-ci pour la notion de droit à la non-ingérence dans les communications privilégiées, mais suggère plus fondamentalement un dernier obstacle de transposition du secret professionnel préconisé par le Timor-Leste: le *lieu* de l'interception des communications. En effet, l'expression technique "interception" est hautement problématique, l'interception d'une communication ayant lieu, pour certains États, là où celle-ci est *captée*, alors qu'elle a lieu pour d'autres là où la communication est *écoutée* pour la première fois.[297] Avec cette expression, la CIJ est confrontée à l'hétérogénéité de la législation en vigueur au sein des États. Par conséquent, la CIJ n'est absolument pas aidée par la législation interne des États dans sa démarche de détermination du secret professionnel.

Somme toute, le DIP s'accommode mal du secret professionnel des avocats et conseillers juridiques, la CIJ n'étant elle-même pas aiguillée des procédures spécifiques pour régler la question. Ce PGD ne franchit donc pas les étapes de la méthode Tanaka. Les obstacles de transposition que nous avons arpentés sont en effet trop abondants pour ne pas instiller cette conclusion. Poursuivons alors en évoquant le second droit retenu par la CIJ, celui du droit à la non-ingérence dans les communications avec les conseillers juridiques.

LE DROIT À LA NON-INGÉRENCE DANS LES COMMUNICATIONS

Le principe de l'égalité souveraine des États représente le principe constitutionnel de base du droit international. D'après ce principe, les États,

[295] *Affaire Timor-Leste c Australie*, *supra* note 10 au para 5.

[296] Rain Liivoja, "*Timor-Leste v Australia*: Provisional Observations" (6 mars 2014) *EJIL: Talk!* (blogue), en ligne: <http://www.ejiltalk.org/timor-leste-v-australia-provisional-observations>.

[297] Sur ce point, voir par exemple la comparaison entre le droit canadien et américain dans l'*Affaire X (Re)*, *supra* note 172.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

petits ou grands, ont tous une vocation identique à jouir des droits à propos desquels il est établi qu'ils sont égaux.[298] Si le principe de l'égalité souveraine s'incarne dans diverses concrétisations (ses deux corolaires les plus importants étant le principe de non-intervention et de non-ingérence), nous avons déjà conclu dans la Partie II que celles-ci ne sauraient prohiber l'espionnage à elles seules.[299] La question qui se pose alors est si, de ce principe, peut quand même se détacher une règle précise venant prohiber l'espionnage en conférant un droit aux États de communiquer de manière confidentielle avec leurs conseillers juridiques au sujet de questions faisant l'objet d'une procédure arbitrale ou contentieuse.

Comme l'on noté certains,[300] dont le Juge dissident Greenwood,[301] il semble douteux de dériver un droit aussi spécifique d'un principe large comme celui de l'égalité souveraine. Prenant en considération cette situation, la CIJ interpréta en ces termes le droit allégué par le Timor-Leste:

> [C]e droit allégué pourrait être inféré du principe de l'égalité souveraine des États, l'un des principes fondamentaux de l'ordre juridique international qui trouve son expression au paragraphe 1 de l'article 2 de la Charte des Nations Unies. *Plus spécifiquement, il convient de préserver l'égalité des parties lorsque celles-ci se sont engagées, conformément au paragraphe 3 de l'article 2 de la Charte, dans le règlement, par des moyens pacifiques, d'un différend international* (nous soulignons).[302]

Ce passage est très clair. L'interprétation combinée de deux principes, l'égalité des parties (un corolaire de l'égalité souveraine) et le principe de règlement pacifique des différends, garantissent un droit à la non-ingérence dans les communications avec les conseillers juridiques.[303] Conçu ensemble, le tout représent un socle solide pour ériger un nouveau droit prohibant l'espionnage dans le paysage juridique international. Examinons-le en détail maintenant.

Le principe d'égalité des parties est un principe autonome de la procédure judiciaire. Il domine la procédure en exigeant que "des opportunités égales soient données aux parties pour faire des actes de procédures

[298] Salmon, *supra* note 5 à la p 419.

[299] *Ibid.*

[300] Cecily Rose, "The Protection of Communications between States and Their Counsel in International Dispute Settlement" (2014) 73:2 CL Rev 231 à la p 234.

[301] *Questions concernant la saisie et la détention de certains documents et données (Timor-Leste c Australie)*, Ordonnance du 3 mars 2014 [2014] CIJ, au para 12 (juge Greenwood, dissident) [*Questions concernant la saisie et la détention*, Greenwood].

[302] *Affaire Timor-Leste c Australie*, *supra* note 10 au para 27.

[303] Voir Matthew Coleman & Thomas Innes, "ICJ Order on Timor-Leste's Request for Provisional Measures against Australia and Its Implications on Investor-State Arbitration" (2014) Practical Law, en ligne: <http://ca.practicallaw.com/8-560-5608?q=&qp=&qo=&qe=>.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

et que les modalités de procédures soient égales pour elles."[304] De fait, les parties doivent notamment avoir le même temps pour présenter leurs pièces écrites; avoir le même nombre de pièces (mémoire, contre-mémoire, etc.); pouvoir apporter le même nombre d'arguments.[305] Pour sa part, l'article 2(3) de la *Charte des NU* pose le principe fondamental de règlement pacifique des différends. En vertu de ce principe coutumier, les États ont une obligation de conduite,[306] celle de régler leurs différends internationaux par des moyens pacifiques de telle manière que la paix et la sécurité internationales, ainsi que la justice, ne soient pas mises en danger. Si l'égalité des parties est le fondement du droit à la non-ingérence, le principe de règlement pacifique des différends agit comme l'empreinte pour la monaie: il en dessine la portée, en précise la forme et la valeur.

La célèbre affaire *Barcelona Traction* consacre ce fondement juridique, pour prendre un exemple très simple.[307] Dans ce cas, la Belgique ne s'était désistée que pour prendre connaissance des arguments de l'Espagne et ensuite ressaisir la Cour, ce qui lui aurait permis d'affiner ses requêtes en meilleure connaissance de cause.[308] Aussi l'Espagne s'opposa-t-elle à la recevabilité de la demande: elle allégua avoir subi un désavantage indu. Selon elle, "cette connaissance préalable de la Belgique lui assurait une espèce de pièce de procédure de plus, mettant ainsi en souffrance le principe de l'égalité des parties."[309] Mais la CIJ jugea cette souffrance bénigne. En effet, même dans l'instance ordinaire, la Belgique aurait pu modifier ses conclusions pour prendre en compte les arguments espagnols. De surcroit, l'Espagne continuait de pouvoir faire valoir toutes les exceptions préliminaires lors de la seconde instance. Par suite, la Cour jugea que le principe d'égalité des parties n'était pas atteint. On comprend que la CIJ n'interviendra pas lorsqu'un désavantage n'impose aucune souffrance véritable à l'autre partie. La question est alors soulevée de savoir si l'espionnage de communications privilégiées constitue, pour l'État victime, un net désavantage susceptible de mettre en souffrance le principe d'égalité des parties.

Il ne faut pas en douter: la réponse est positive et les faits de l'affaire *Timor-Leste- c Australie* l'illustrent bien. Ceci ressort tant des opinions

[304] Kolb, *supra* note 292 à la p 1161.

[305] *Ibid* à la p 1164.

[306] Bruno Simma avec la collaboration de Herman Mosler, Albrecht Randelzhofer et Christian Tomuschat, *The Charter of United Nations: A Commentary*, New York, Oxford University Press, 2002 à la p 106.

[307] *Affaire Barcelona Traction and Power Company, Limited (Belgique c Espagne) (Nouvelle requête: 1962)*, arrêt [1970] CIJ rec 3 à la p 20.

[308] Kolb, *supra* note 292 à la p 1167.

[309] *Ibid.*

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

individuelles des Juges que de l'attitude de la CIJ elle-même. À titre d'exemple, le Juge Greenwood considère qu'il est parfaitement compréhensible que le Timor-Leste redoute la perquisition effectuée dans les locaux de ses conseillers, celle-ci ayant donné "de manière pour le moins inéquitable, un net avantage dans le cadre de la procédure d'arbitrage et d'une éventuelle négociation à venir avec le Timor-Leste au sujet de la mer de Timor."[310] On vient à penser qu'il est probable que les documents et données saisis se rapportent à la stratégie juridique du Timor-Leste, "incluant les avis de ses conseils, des analyses juridiques de sa position ainsi que des instructions données à ses conseils et experts en géologie et questions maritimes."[311] Plus loin, le Juge Greenwood parle d'un "avantage on ne peut plus inéquitable."[312]

Plus concrètement, l'attitude désapprobatrice de la CIJ confirme que la saisie des documents et données fut considérée franchement inéquitable. On sait qu'une condition clé pour l'indication de mesures conservatoires est l'existence d'une menace de préjudice irréparable à la substance des droits invoqués par le défendeur.[313] En l'espèce, c'est le risque que soit compromise la position du Timor-Leste dans le cadre de l'arbitrage et d'éventuelles futures négociations qui s'est révélé déterminant pour la Cour.[314] Or, les faits révèlent nettement que l'Australie avait déjà pris avec son *Solicitor-General* un engagement écrit supplémentaire en date du 21 janvier 2014 pour protéger la position du Timor-Leste, qui couvrait la possibilité que les éléments saisis soient divulgués.[315] Les éléments étaient sous scellés et la CIJ le savait. Celle-ci, bien qu'elle dise n'avoir aucune raison de penser que l'engagement écrit ne serait pas respecté par l'Australie,[316] considéra néanmoins qu'un risque important subsistait que les éléments saisis soient divulgués et indiqua les mesures provisoires. Le fait que la CIJ ait indiqué les mesures provisoires, en dépit de la présence de cet engagement écrit supplémentaire (chose qui n'a pas d'équivalent dans le passé[317]) en dit long: la saisie était un acte peu ordinaire.

Une telle conclusion ne surprend pas. Songeons que la fonction même de la CIJ serait compromise par l'espionnage des communications d'un État avec ses conseillers. La CIJ est tenue, en tant que corps judiciaire,

[310] *Questions concernant la saisie et la détention*, Greenwood, *supra* note 301 au para 10.

[311] *Affaire Timor-Leste c Australie*, *supra* note 10 au para 33.

[312] *Ibid* au para 27.

[313] Kolb, *supra* note 292 à la p 648.

[314] *Affaire Timor-Leste c Australie*, *supra* note 10 au para 42.

[315] *Questions concernant la saisie et la détention*, Greenwood, *supra* note 301 au para 27.

[316] *Affaire Timor-Leste c Australie*, *supra* note 10 au para 44.

[317] Voir notamment *Questions concernant l'obligation de poursuivre ou d'extrader (Belgique c Sénégal)*, [2012] CIJ rec à la p 8.

dans la procédure consultative comme dans celle contentieuse, d'inscrire ses actions dans le principe de la bonne administration de la justice.[318] Ce principe exige notamment que la Cour mette en balance les intérêts contradictoires pour maintenir en tout temps l'égalité procédurale des parties.[319] La CIJ invoque d'ailleurs régulièrement les deux principes côte à côte pour pallier à des contextes d'inégalité. Dans l'affaire relative aux *Jugements du tribunal administration de l'Organisation internationale du travail sur requêtes contre l'UNESCO* (1956) la CIJ dira que "le principe de l'égalité entre les parties découle des exigences de la bonne administration de la justice."[320] Il n'y aurait donc rien de surprenant à ce que l'espionnage d'espèce constitue un net désavantage mettant en souffrance le principe d'égalité et la bonne administration de la justice, l'Australie ayant vraisemblablement prit connaissance de l'argumentation du Timor-Leste. La CIJ ne peut y rester indifférente.

Notre analyse révèle donc l'existence d'une nouvelle prohibition à l'espionnage: le droit à la non-ingérence dans les communications d'un État avec ses conseillers juridiques. Tel que défini par la CIJ, ce droit à la non-ingérence dans les communications est cantonné à un contexte précis: celui où les États se sont engagés au règlement d'un différend international par des moyens pacifiques. Le droit s'attache au surplus à l'*objet* de l'espionnage (les communications privilégiées), non les *moyens* employés pour le réaliser. L'espionnage de communications privilégiées se veut ainsi prohibé et ce peu importe le lieu d'ingérence par l'État-espion. La prohibition de l'ETP privilégie donc un critère contextuel et un élément portant sur l'objet du renseignement. Cela étant, faut-il, pour conclure notre analyse, accorder beaucoup de sérieux aux contre-arguments avancés par l'Australie pour contester l'existence de ce droit ou en tempérer la portée? D'après nous, l'argument fondé sur le parallèle avec le droit diplomatique[321]

[318] Kolb, *supra* note 292 à la p 1169.

[319] *Ibid* à la p 1170.

[320] *Jugement du Tribunal administratif de l'O.I.T. sur requêtes contre l'UNESCO*, Avis consultatif [1956] CIJ rec à la p 77.

[321] L'Australie établit un parallèle avec le droit diplomatique qui doit être rejeté. Elle avançait le fait que les agents diplomatiques ne peuvent abuser de leurs privilèges et immunités (par exemple, celui de l'inviolabilité de la valise diplomatique, qui ne peut être ouverte) pour commettre des actes criminels (par exemple, transporter dans cette valise des armes ou des produits de contrebande). Par ailleurs, l'Australie soutint qu'un droit à la non-ingérence dans les communications confidentielles devrait être limité lorsqu'il vise la fraude, la commission d'infractions pénales, etc. Ce parallèle avec le droit diplomatique n'est pas convaincant. Lors de l'élaboration de la *CVRD*, diverses propositions ont été faites tendant à limiter l'inviolabilité de la valise diplomatique afin de parer à ses utilisations abusives. Elles furent toutes rejetées, les États préférant assurer la confidentialité de leurs propres valises. De plus, la proposition de l'Australie pour un droit relatif pose un problème logique. Il n'y a aucun moyen de savoir si la communication

de même que l'argument fondé sur la compétence territoriale[322] ne sont pas dirimants au droit allégué par le Timor-Leste, d'autant que la CIJ a conclu de sa plausibilité.

Récapitulons. Cette dernière partie de notre étude confirme l'existence d'un (nouveau) droit à la non-ingérence des communications entre un État et ses conseillers juridiques, dérivé du principe d'égalité souveraine combiné au principe de règlement pacifique des différends. Ce droit s'appliquerait dès que les États sont engagés, en vertu de l'article 2(3) de la *Charte des NU*, dans le règlement pacifique d'un différend. L'État qui entreprend de régler pacifiquement un différend qui l'oppose à un autre État par voie d'arbitrage ou de négociations peut s'attendre à mener procédures et négociations sans que l'autre partie ne s'ingère dans son argumentation.

Conclusion

Les règles du DIP n'apportent pas de réponse simple au statut de l'ETP. Si les formes d'espionnage sont nombreuses, réglées chacune par des normes spécifiques, il s'en faut cependant beaucoup que leur ensemble se laisse soumettre à des réductions simples: on se trouve devant un casse-tête en apparence hétérogène. Aux fins de résumer ce texte sur la licéité de l'ETP, nous procédons dans le Tableau 2 ci-dessous, et en fonction de chaque zone géographique, au rappel des différentes conclusions auxquelles nous sommes parvenus. Ce tableau vient compléter le travail amorcé par d'autres avant nous.[323]

Malgré toutes ces variations dans le statut de l'ETP, un principe fondamental a été confirmé dans ce texte. L'espionnage est licite en vertu du *Lotus* en l'absence de (rares) prohibitions contraires. L'affirmation parait provocatrice. Elle échappe pourtant à toute controverse en ce qu'elle reflète la volonté des États qui n'ont pas souhaité s'imposer de limites réciproques en la matière. L'espionnage constitue alors tout au plus un

privilégiée dans laquelle s'ingèrera un État en est une visée par les exceptions *avant* de l'avoir intercepté. Le droit diplomatique illustre ce point, puisque la mission diplomatique a le droit de communiquer librement avec les autorités de son État par tous les moyens utiles selon l'article 27(1) *CVRD*. Ce droit de libre communication est inviolable et ne connait aucune exception. En ce sens, le parallèle avec le droit diplomatique tend à renforcer, plutôt qu'à infirmer, la position du Timor-Leste sur l'existence d'un droit absolu.

[322] L'Australie invoqua le principe bien établi selon lequel un État peut exercer sa compétence d'exécution sur son propre territoire, et que les immunités (qui constituent une dérogation à ce principe) ont toutes été codifiées jusqu'à présent. Selon nous cet argument n'est pas fatal: on sait que les principes non codifiés abondent en droit international.

[323] Forcese, *supra* note 52 à la p 209.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

Tableau 2: Statut de l'espionnage en temps de paix

Règle(s)	Territorial	Extraterritorial	Transnational
Principe de souveraineté territoriale	Inapplicable	Applicable, prohibant l'espionnage entrainant une violation collatérale	Inapplicable
Principe de l'interdiction de l'emploi de la force	Inapplicable, car l'espionnage n'est pas une activité agressive	Inapplicable, car l'espionnage n'est pas une activité agressive	Inapplicable, car l'espionnage n'est pas une activité agressive
Principe de non-intervention dans les affaires intérieures	Inapplicable vu l'absence de l'élément de coercition	Inapplicable vu l'absence de l'élément de coercition	Inapplicable vu l'absence de l'élément de coercition
Exercice illicite de la compétence d'exécution	Inapplicable	Applicable, limitant le cyberespionnage commis par un agent au sol	Inapplicable, ne limitant pas la cyber reconnaissance ni les interceptions transnationales
Passage inoffensif de la *Convention de Montego Bay*(Article 19)	Applicable, limitant la "collecte de renseignement," les "recherches" et "perturbations" des systèmes de communication	Inapplicable	Inapplicable
Limitations découlant de l'*ADPIC* (Article 39)	Inapplicable	Inapplicable	Inapplicable
Limitations découlant de la *Constitution de l'UIT* (Article 37)	Applicable, mais l'exception de législation nationale autorise les interceptions	Applicable, mais l'exception de législation nationale autorise les interceptions	Applicable, mais l'exception de législation nationale autorise les interceptions

Continued

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

Tableau 2: *Continued*

Règle(s)	Territorial	Extraterritorial	Transnational
Limitations découlant du *PIDCP* (Article 17)	Applicable, limitant la capacité de l'État d' espionner ses citoyens	Applicable, lorsque l'individu est dans le contrôle effectif de l'État	Inapplicable, car l'individu est hors du contrôle effectif de l'État
Limitations découlant de la *CEDH* (Article 8)	Applicable, limitant la capacité de l'État d'espionner ses citoyens	Applicable, limitant la capacité de l'État d'espionner les citoyens étrangers	Applicable, limitant la capacité de l'État d'espionner les citoyens étrangers
Immunités et privilèges diplomatiques	Applicable, limitant la capacité de l'État d'accueil d'espionner les agents diplomatiques étrangers	Applicable, permettant la collecte d'informations, par les agents diplomatiques, réalisée par des "moyens licites"	Applicable, limitant la capacité d'un État d'intercepter les communications des agents diplomatiques avec un État tiers
Droit à la non-ingérence dans les communications avec les avocats et conseillers juridiques	Applicable, limitant toute ingérence dans les communications, documents et données	Applicable, limitant toute ingérence dans les communications, documents et données	Applicable, limitant toute ingérence dans les communications, documents et données

acte inamical, c'est-à-dire un acte d'un État à l'égard d'un autre État, qui sans être contraire au DIP, peut constituer aux yeux de l'État victime un manquement aux bonnes relations.[324] Julius Stone, l'un des premiers juristes à s'être penché sur la question du statut de l'espionnage, met habilement en relief cette conclusion: "the espionage situation is, ladies and gentlemen, like some situations that occasionally arise between friends and even, I understand, between husband and wife, when one of them does the sort of thing about which it isn't really any use for them to talk."[325]

[324] Salmon, *supra* note 5 à la p 28.

[325] Stone, *supra* note 58 à la p 39.

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press

Notre bilan semble lui donner raison. L'activité est licite, mais "flirte" avec l'illicite et baigne dans un silence singulier. C'est d'ailleurs à propos des nouvelles formes d'espionnage — cyberespionnage, cyber reconnaissance, interception transnationale — que ce phénomène est marqué de la manière la plus claire. Plus de cinquante ans plus tard, les propos de l'éminent juriste n'ont pas vieilli d'une ride.

Au-delà du flirt avec l'illicite, quelques rares formes d'espionnage sont prohibées en l'état actuel du droit international. C'est le cas de l'espionnage par un État des communications d'un autre État avec ses avocats et conseillers juridiques, lorsque ceux-ci sont engagés dans le règlement pacifique d'un différend international. Certes, la CIJ a prescrit la radiation de l'affaire *Timor-Leste c Australie* et ne statuera pas le fond pour confirmer l'existence d'un droit à la non-ingérence.[326] Mais on trouvera une preuve additionnelle de l'existence de ce droit dans la conduite de l'Australie, qui restitua, le 12 mai 2015, les documents et données qu'elle avait saisis le 3 décembre 2013.[327] Par lettre du 2 juin 2015, le Timor-Leste s'est dit satisfait de cette restitution. Satisfait, surtout, "que l'Australie reconnaisse [implicitement] que ses actes avaient constitué une violation des droits souverains du Timor-Leste."[328] Sans surprise, l'Australie nia. Elle répliqua que cette restitution des éléments en cause ne témoignait que de sa détermination à régler pacifiquement le différend en prenant une initiative positive et constructive pour y mettre fin, ajoutant "qu'aucune autre conclusion ne devait être tirée des actes de l'Australie."[329]

Aucun pouvoir ne consent à rien pour rien. Tout comme le Timor-Leste, nous croyons qu'il faut voir dans ce geste curieux une reconnaissance implicite par l'Australie que ses actes avaient bien constitué une violation du droit du Timor-Leste à la non-ingérence dans les communications entretenues avec ses conseillers juridiques. L'affaire *Timor-Leste c Australie* lève donc le voile sur un pan inattendu de l'espionnage … La province touffue et morcelée qu'est le droit de l'espionnage n'a certainement pas fini de retenir l'attention des juristes!

[326] Dubuy, *supra* note 256. Elle s'exprime également sur le point de savoir si les actes de l'Australie constituent une reconnaissance de l'atteinte à la souveraineté du Timor-Leste.

[327] *Questions concernant la saisie et la détention de certains documents et données (Timor-Leste c Australie)*, "Communiqué de presse" (12 juin 2015) CIJ, en ligne: <http://www.icj-cij.org/docket/files/156/18693.pdf>.

[328] *Ibid.*

[329] *Ibid.*

https://doi.org/10.1017/cyl.2016.16 Published online by Cambridge University Press