« les droits maritime et de l'espace peuvent-ils inspirer un droit du cyberespace ? »

CEIS

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la Compagnie Européenne d'Intelligence Stratégique cette étude sur le thème : « les droits maritime et de l'espace peuvent-ils inspirer un droit du cyberespace ? », sous le numéro de marché 2013 105 008 8823.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la défense

Délégation aux Affaires Stratégiques

Sous-direction Politique et Prospective de Défense

14 rue St Dominique

75700 PARIS SP 07

Le cyberespace tient aujourd'hui une place croissante dans nos vies quotidiennes. Pilier de l'économie et créateur d'emploi, il est aussi un espace d'expression des droits et libertés fondamentaux. Il supporte de nombreuses fonctions critiques étatiques. Il est désormais un espace stratégique, et sa maîtrise est l'enjeu de ces dernières années.

Source de litiges en matière de gouvernance internationale, il est également en proie à une militarisation croissante, et le théâtre de nombreux conflits et actes cybercriminels. Autant d'éléments faisant du cyberespace un espace devant être protégé. Mais sous quelle forme ?

Ce régime de protection ne pourrait-il pas s'inspirer de ceux élaborés pour les espaces communs tels que la mer ou l'espace ? « Les droits maritime et de l'espace peuvent-ils inspirer un droit du cyberespace ? »

1.1. L'entrelacement des espaces

D'une part, il faut souligner que « l'espace est une réalité tangible, malgré les moyens les plus modernes de mobilité, tandis que le cyberespace reste intangible pour la plupart de ses utilisateurs ».[1] Les équipements physiques ancrent toutefois le cyberespace dans l'espace terrestre, donc géographique. Les câbles sous-marins sont au cœur des espaces maritimes, et les satellites au sein de l'espace extra-atmosphérique. Ce qui traduit un véritable entrelacement du cyberespace et des espaces préexistants. La conséquence directe est l'application de dispositions juridiques du droit de la mer et du droit de l'espace à la couche physique, tangible, du cyberespace.

1.2. Une analogie surtout fonctionnelle

D'autre part, par ses usages et la sémantique associée, le cyberespace est souvent perçu comme un espace à part entière. Il est même considéré comme le 5ème champ de bataille, après la terre, l'air, la mer et l'espace, selon le Livre blanc sur la défense et la sécurité nationale de 2008[2]. Mais une analyse juridique stricte ainsi que l'observation de sa réalité physique rappellent que le cyberespace n'est peut-être pas un « espace » au sens strict du terme. Mais si les trois sujets de droit mer, espace et cyberespace ne sont pas comparables par leur essence (sujets naturels et sujet artificiel), l'analogie permet de déceler des similitudes fonctionnelles et stratégiques.

Elle se traduit par l'existence de flux plus ou moins contrôlés, de voies stratégiques et moins stratégiques, de raccourcis (et d'enclavement). Ainsi, cette analogie se traduit par la possible transposition de certains mécanismes : mécanisme de responsabilité, de réparation, mais aussi d'un statut global pour le cyberespace et de ses corollaires : principe d'utilisation pacifique, de libre accès, etc.

Au-delà de ces principes, c'est la logique d'aménagement de la souveraineté étatique proposée par le droit de la mer qui retient l'attention. Ce droit choisit de morceler la problématique en graduant la portée et l'effectivité de la souveraineté des Etats. Transposé au cyberespace, domaine artificiel, cela équivaut à graduer et donc limiter la portée de la propriété privée en sanctuarisant certaines infrastructures.

---

[1] Kavé Salamatian et Jérémy Robine, « Peut-on penser une cybergéographie ? », in « Cyberespace : enjeux géopolitiques », *Herodote*, n°152-153, 2014.

[2] Livre blanc sur la Défense et la Sécurité nationale, France, 2008

1.3. Un droit à créer *ex nihilo*

Le principal apport de cette étude est que l'analogie ne suffit pas ; elle rappelle la nécessité de créer un droit et des mécanismes propres au cyberespace, à l'image des mécanismes de responsabilité créés spécifiquement pour les activités menées dans l'espace et sur la mer. De ce constat, découlent de nombreuses idées de mécanismes originaux :

- Créer un statut propre au cyberespace : le statut d'espace international coutumier ;
- Systématiser un faisceau de domaines de compétence étatique et donc juridictionnelle propres au cyberespace (adresses IP, DNS et noms de domaine, data centers, etc.)
- Sanctuariser certaines infrastructures essentielles du cyberespace afin de préserver le milieu ;
- Assortir cette sanctuarisation de la création d'un statut *ad hoc* pour leurs opérateurs, sur le modèle incitatif de la délégation de service public.

Un traité international devrait en effet, pour préserver la sécurité de ces infrastructures, s'assurer de : la continuité du service, la non-discrimination dans l'accès à ce service, ou encore la primauté de l'intérêt collectif en cas de travaux ;

- S'inspirer du droit fluvial en adoptant un mécanisme de droit de regard pour les Etats dépendants, à l'égard de l'Etat maîtrisant une infrastructure critique pour plusieurs Etats : la communauté de droit et d'intérêt.

L'analogie du fleuve international et du statut des Etats en aval et en amont est en effet très pertinente au regard des infrastructures critiques d'Internet et de la dépendance de certains Etats enclavés à leur égard ;

- Renforcer la régulation économique, en raison de la place croissante des entreprises du numérique au sein de la gouvernance Internet.

Cette dynamique a touché le droit de l'espace qui tend aujourd'hui, de plus en plus, à intégrer cette dimension économique. La privatisation croissante des activités spatiales a relégué les Etats au second rang, face aux opérateurs privés (lanceurs, fabricants de matériel, satellites, etc.). Une situation qui tend à se rapprocher de celle du cyberespace.

Ces idées, bien qu'originales, se heurtent à une gouvernance aujourd'hui paralysée par une logique de blocs, et l'absence de consensus à l'échelle internationale. C'est pourquoi toute réforme et toute démarche créatrice en droit international ne pourra se faire que par l'adoption de mesures de « soft law ». A cet égard, l'exemple du code ISPS propre au droit de la mer est structurant.

Sommaire

3ème partie : Recommandations

Annexes

Introduction

Contexte

Le cyberespace tient aujourd'hui une place croissante dans nos vies quotidiennes. Pilier de l'économie et créateur d'emploi, il est aussi un espace d'expression des droits et libertés fondamentaux. Il supporte de nombreuses fonctions critiques étatiques. Il est désormais un espace stratégique, et sa maîtrise est l'enjeu de ces dernières années. Source de litiges en matière de gouvernance internationale, il est également en proie à une militarisation croissante, et le théâtre de nombreux conflits et actes cybercriminels. Autant d'éléments faisant du cyberespace un espace devant être protégé. Mais sous quelle forme ?

Ce régime de protection ne pourrait-il pas s'inspirer de ceux élaborés pour les espaces communs tels que la mer ou l'espace ? « Les droits maritime et de l'espace peuvent-ils inspirer un droit du cyberespace ? »

L'idée est séduisante, car les régimes relatifs au droit de l'espace et au droit maritime ont en effet déjà fait leur preuve en matière de stabilité internationale. Mais son application est soumise à la qualification du cyberespace comme espace à part entière, qualification loin d'être acquise.

Objectifs

L'étude a pour objectif de faire une analyse de l'analogie juridique entre les différents espaces.

L'étude propose également quelques clés en vue de l'élaboration d'un régime juridique du cyberespace, en distinguant les mesures pouvant être inspirées par les droits de la mer et de l'espace, de celles devant être élaborées spécifiquement pour le cyberespace. Dans cette étude, CEIS distingue les mesures juridiques de fond des mesures procédurales. Les droits de la mer et de l'espace démontreront surtout qu'ils ont été construits et rédigés pour leur domaine, ex nihilo, en s'adaptant aux réalités des espaces respectifs.

Dans une démarche créatrice, et s'inspirant de cette dynamique issue des droits de la mer et de l'espace, CEIS propose enfin des pistes originales d'évolution du droit du cyberespace.

1ère partie : Analogie des espaces

1. Les sujets de l'analogie

1.1. Les espaces maritimes et l'espace extra-atmosphérique

L'espace désigne les zones de l'Univers situées au-delà des atmosphères et des corps célestes.

Le droit de la mer regroupe l'ensemble des dispositions propres à l'usage des espaces maritimes, (« les étendues d'eau salée, en communication libre et naturelle ») par les sujets du droit international, les États. Les espaces maritimes définis par le droit de la mer sont : les eaux intérieures, la mer territoriale, la zone contiguë, la zone économique exclusive, plateau continental, la haute mer, les détroits et canaux internationaux.

Les espaces maritimes se caractérisent par la dimension stratégique de leurs accès (militaire, géopolitique, économique), de l'omniprésence de flux de circulation de marchandises et de personnes, mais aussi par la nécessité d'aménager les relations entre les différents acteurs y opérant : les Etats, mais également les acteurs privés (armateurs).

1.2. Le cyberespace

1.2.1. Définitions

Plusieurs définitions peuvent être envisagées selon un angle technique et physique, cognitif et sémantique, stratégique ou encore juridique. L'étude confrontera ces définitions afin d'aboutir au descriptif le plus exhaustif et pluridisciplinaire envisageable.

L'ANSSI définit le cyberespace comme un « espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées ». Dans cette définition orientée vers l'aspect technique, l'Internet physique n'est perçu que comme le support d'un espace de communication[3].

Le Concept d'emploi des forces du CICDE considère quant à lui que le cyberespace est « le réseau planétaire qui relie virtuellement les activités humaines grâce à l'interconnexion des ordinateurs et permet la circulation et l'échange rapides d'informations ».[4]

[3] ANSSI, « Stratégie de la France pour la Défense et sécurité des systèmes d'information », 15 février 2011.
[4] CICDE, Concept d'emploi des forces, CIA 01, 15 janvier 2010.

Dans une démarche stratégique, le département de la défense américain qualifie le cyberespace de « global common », à l'image de l'espace, des eaux internationales et de l'espace aérien. Le cyberespace est donc considéré comme un espace accessible à tous mais détenu par personne, une ressource à laquelle tous les Etats ont un droit d'accès légal. Dans cette définition, le « global common » peut être de consistance géographique ou virtuelle.[5]

Dans ces définitions, Internet n'est qu'une composante du cyberespace. Une logique qui se retrouve dans les démarches de schématisation et de décomposition du cyberespace en couches ou strates.

1.2.2. La géographie de l'Internet et l'entrelacement des espaces

Par ses usages et la sémantique associée, le cyberespace est souvent perçu comme un espace à part entière. Il est même considéré comme le 5ème champ de bataille, après la terre, l'air, la mer et l'espace, selon le Livre blanc sur la défense et la sécurité nationale de 2008. Mais une analyse juridique stricte ainsi que l'observation de sa réalité physique rappellent que le cyberespace n'est peut-être pas un « espace » au sens strict du terme.

1.2.2.1. Le cyberespace est-il un espace ?

L'espace est la propriété particulière d'un objet qui fait que celui-ci occupe une certaine étendue, un certain volume au sein d'une étendue, d'un volume nécessairement plus grand que lui, et qui peut être mesuré. On en déduit que l'espace dispose des caractéristiques suivantes : un lieu, une surface (distance), un volume, un accès. Appliqué au cyberespace, les composantes sont les suivantes :

- Un lieu : localisation géographique des infrastructures physiques.
- Une surface : datacenters, périphériques de stockage.
- Un volume : étendue des données échangées.
- Un accès : Internet.

De plus, Plusieurs éléments témoignent de cette perception du cyberespace comme étant un espace à part entière. Qu'il s'agisse de la Déclaration d'indépendance du cyberespace[6] ou de la sémantique très imagée (surfer, naviguer, espace, plage, flux, etc.), le cyberespace se présente comme un « espace mental partagé » (amorcé par le téléphone), et vient bousculer la vision de l'espace classique : notions de temps, d'éloignement physique, d'ubiquité, d'instantanéité, d'avatar, etc.

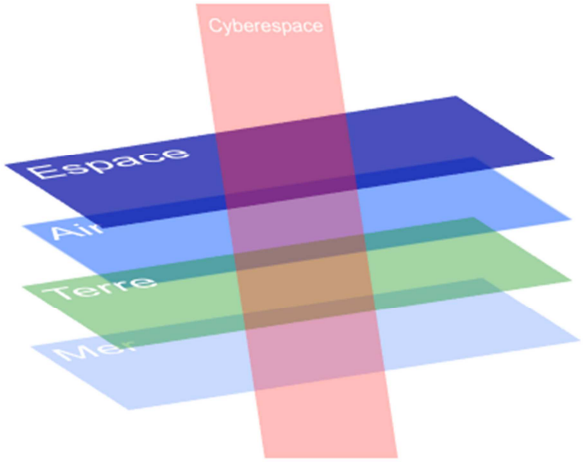
Il faut également noter le même glissement sémantique de la part d'analystes et du monde judiciaire. Voir : Arrêt du 15 novembre 2011, la Cour d'Appel de Besançon considère un « mur » Facebook comme un « espace » public. Est-ce un début d'élargissement de la terminologie ? Rappelons que la notion d' « espace public » est apparue au cours des années 1960, à la suite des travaux de J. Habermas (1962), et qu'au départ, elle s'entendait davantage d'un espace « abstrait et changeant, prenant la forme du rassemblement qui le fait naître ». Ce n'est qu'à partir des années 1970 que le glissement sémantique s'opérera, pour désigner principalement les espaces matériels.

1.2.2.2. Une géographie propre

Mais ces caractéristiques ne suffisent pas à qualifier le cyberespace d' « espace ». En effet, « l'analogie avec l'espace terrestre est [...] discutable. L'espace est une réalité tangible, malgré les moyens les plus modernes

[5] Department of Defense, National Defense Strategy of the United States of America (Washington, DC: Office of the Secretary of Defense, 2008), 13.
[6] John Perry Barlow, Déclaration d'indépendance du cyberespace, Davos, 8 février 1996

de mobilité, tandis que le cyberespace reste intangible pour la plupart de ses utilisateurs ».[7] Les équipements physiques ancrent toutefois le cyberespace dans l'espace terrestre, donc géographique. Les câbles sous-marins sont au cœur des espaces maritimes, et les satellites au sein de l'espace extra-atmosphérique. Ce qui traduit un véritable entrelacement du cyberespace et des espaces préexistants.



Le cyberespace, un domaine enraciné au sein d'autres espaces

De plus, la dimension sociale qui s'y rattache permet d'observer un solide rapport d'appropriation de la part des internautes. Formations de communautés, identification d'espaces « privés », espaces de communication qui sont décorrellés des infrastructures physiques d'Internet… sont autant d'indices pouvant évoquer l'émergence d'une géographie d'un nouveau genre.

L'émergence de la notion de « balkanisation » du cyberespace évoque également l'existence d'une géographie propre, la notion de « frontières » étant au cœur du concept. Les frontières, dans leurs définitions classiques, sont entendues comme une ligne séparant des espaces territoriaux où s'exercent deux souverainetés différentes, cette ligne étant « formée par la succession des points extrêmes du domaine de validité spatiale des normes de l'ordre juridique d'un Etat »[8]. Le terme de « balkanisation » sous-entend que des groupes d'êtres humains s'opposeraient, conduisant ainsi au morcellement du territoire sur lequel ils étaient auparavant tous réunis. Il s'agirait peut être plus de parler de fragmentation, qui ferait référence au morcellement du territoire et des populations, mais aussi de l'accès aux services, à l'information, au Web de manière générale. Mais le terme de « balkanisation » suppose l'existence de frontières. Et l'existence de celles-ci dans le cyberespace n'est pas quelque chose d'acquis. Car si pour les gouvernements, il semble logique qu'ils aient le pouvoir d'exercer une gouvernance sur « leur » cyberespace, pour d'autres, à l'image de John Perry BARLOW dans sa Déclaration d'indépendance du cyberespace, ce dernier se situe hors des frontières et donc du contrôle des Etats. Cette dernière conception s'appuie sur le fait que les concepts avancés par les Etats sont basés sur la matière alors que le cyberespace serait quant à lui immatériel. Ainsi, s'il est perçu de façon similaire et en partage certaines caractéristiques, le cyberespace ne présente pas les mêmes particularités que les espaces traditionnels (terrestre, maritime et aérien). Mieux encore, il offre la possibilité aux Etats d'« étendre » leurs territoires, de repousser leurs frontières et par là même leur souveraineté. Le corpus législatif américain étend ainsi le principe de compétence territoriale par une sorte d'extraterritorialité dont bénéficient les Etats-Unis sur le territoire d'un autre Etat dès lors que l'entreprise est de droit américain ou lorsque les données d'une entreprise étrangères sont stockées sur le territoire américain. Cette extraterritorialité accordée par le droit américain se trouve renforcée par l'aspect « physique

[7] Kavé Salamatian et Jérémy Robine, Peut-on penser une cybergéographie ? – Hérodote, « Cyberespace : enjeux géopolitiques ».
[8] Tribunal arbitral, affaire de la frontière maritime entre le Sénégal et le Guinée Bissau, RGDIP 1990, p. 253.

» du cyberespace : les serveurs DNS et de stockage de données sont majoritairement localisés sur le continent américain. La maîtrise du système d'adressage ainsi que la maîtrise des données offertes par les géants Facebook, Apple, Google ou encore Amazon viennent compléter cette suprématie.

L'étude révèle que l'analogie est limitée quant aux caractéristiques réelles des sujets de comparaison. Le cyberespace n'est pas un espace au sens du Droit des Espaces, mais un média de communication et d'échange riche et dense, associé à une dimension cognitive nouvelle. L'analogie reste toutefois viable sur les usages et la dimension cognitive. Si le cyberespace n'est pas un espace au sens juridique du terme, il se caractérise par l'émergence d'un espace au sens économique et social.

1.2.3. La logique des 3 couches

Le cyberespace peut être représenté en trois couches : la couche physique, logique, et cognitive[9].

<table>
<tr><th colspan="2">Composants</th><th>Strates</th><th></th><th></th></tr>
<tr><td colspan="2">Culture (langue, politique, éthique, liberté, etc.)
Identités réelles - humanité</td><td rowspan="4">Couche cognitive et humaine</td><td rowspan="13">C
Y
B
E
R
E
S
P
A
C
E</td><td rowspan="13">G
O
U
V
E
R
N
A
N
C
E</td></tr>
<tr><td rowspan="2">Usages</td><td>Communication, recherche, réseaux sociaux, loisirs, partage de connaissance, commerce, économie, diplomatie…</td></tr>
<tr><td>Mais aussi désinformation, propagande, conflits, renseignement…</td></tr>
<tr><td colspan="2">Perception/cognitif – Informations – Sémantique (sens des informations, diffusion, visualisation) - Identités numériques (pseudonymat)</td></tr>
<tr><td colspan="2">Contenus, données</td><td rowspan="4">Couche logique ou logicielle</td></tr>
<tr><td colspan="2">Applications d'Internet (Web, Mail, partage de fichiers, messagerie instantanée)</td></tr>
<tr><td colspan="2">Systèmes d'exploitation et autres applications – softwares/programmes</td></tr>
<tr><td colspan="2">Protocole de communication/transport/adressage</td></tr>
<tr><td colspan="2">Machines : terminaux, périphériques et objets connectés</td><td rowspan="3">Couche physique</td></tr>
<tr><td colspan="2">Infrastructures, serveurs et connectivité (câbles sous-marins, réseaux sans-fil, datacenters, routeurs)</td></tr>
<tr><td colspan="2">Enracinement géographique (conséquences stratégiques, politiques,</td></tr>
</table>

[9] Ce tableau s'inspire notamment des conceptions suivantes : Characterizing cyberspace : past, present and future http://web.mit.edu/ecir/pdf/clark-cyberspace.pdf ; Cyberspace Operations Concept Capability Plan 2016-2028 http://www.fas.org/irp/doddir/army/pam525-7-8.pdf ; Olivier KEMP - Stratégie du cyberespace http://www.diploweb.com/Strategie-du-cyberespace.html ; Cyberspace domain : a warfighting substantiated operational environement imperative, by Colonel Olen L. Kelley, United States Army
Il représente toutefois une perception propre du cyberespace et de ses composants, d'un point de vue stratégique.

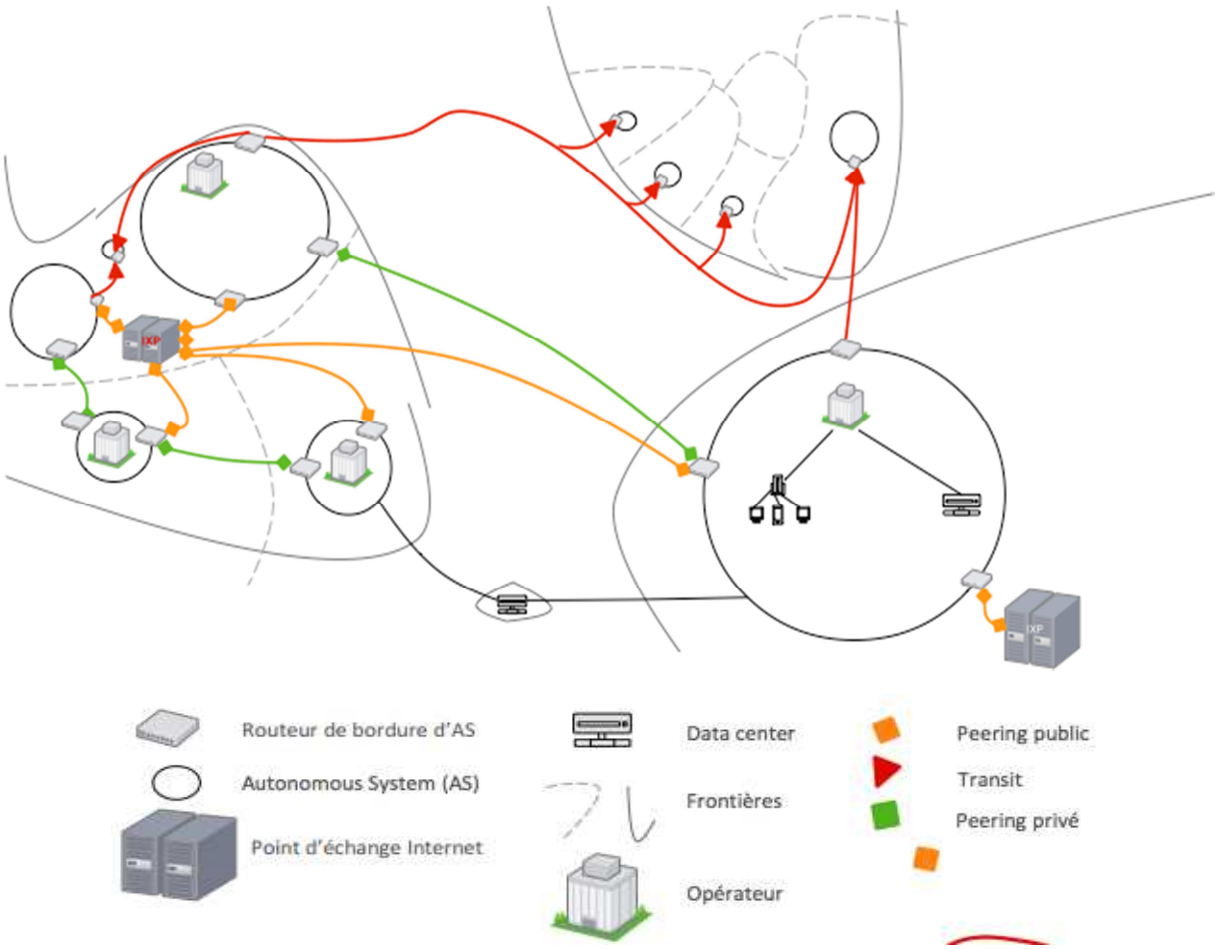
juridiques…)			

Une quatrième couche peut être observée : la couche de command & control. Elle comprend l'ensemble des protocoles de communication, transport et adressage. [Voir Bloch]

1.2.4. Décomposition du cyberespace

Des éléments précités, il est possible de décomposer plus en détail les composantes du cyberespace. Cette démarche est structurante. Elle permet tant de comprendre le cyberespace dans sa globalité, que dans sa diversité (infrastructures, acteurs, perceptions et intérêts). Diversité ayant un impact fort sur les notions de réglementation, d'harmonisation, de gouvernance et de conflit.

Le schéma ci-dessous positionne quelques éléments structurants de la couche dite « physique » du cyberespace.



Classification en couches et par acteurs :

Humains Législateur et politique - Etat	Couche cognitive	« L'esprit et l'intellection des internautes, organisés par la sémantique et la syntaxe des interfaces d'accès à la couche logique » (Laurent Bloch, 2014)										
		Culture										
		Usages										
		Services		Sites, services divers (e-commerce, réseaux sociaux)								
IETF CDN Moteurs de recherche Entreprises de services	Couche logique	Données		Logiciels		Applications					Services techniques	
						Web (http/html/URL)	Mail	FTP	SSH	Chat	CDN	Moteurs de recherche
IETF RIR IANA ICANN	Couche commande et contrôle (C&C)[10]	Protocoles de communication, transports et adressage										
		Application		DNS	BGP	P2P	Etc.					
		Transport		TCP	UDP							
		Réseau		IP			MPLS					
Géographie de l'Internet[11] Acteurs télécom Constructeurs Etats (UIT)	Couche physique	Liaisons physiques				Data centers	Routeurs et AS (ensemble de routeurs)				Terminaux	
		Câbles		Satellites	Autres							
		Peering public/ dorsales	transit		Ondes hertziennes		Privés (box)	IXP[12]	Routeurs de bordure d'AS		Ordinateurs, smartphones, tablettes, consoles	
	Milieu	Terre/mer	Terre/mer	Espace		Terre	Terre	Terre	Terre			

[10] Représentation inspirée du modèle OSI, Open Systems Interconnection

[11] Gilles Puel et Charlotte Ullmann, « Les nœuds et les liens du réseau Internet : approche géographique, économique, et technique », 2005 http://halshs.archives-ouvertes.fr/docs/00/10/98/91/PDF/puel_ullmannV3gp.pdf

[12] Il s'agit de locaux techniques où les opérateurs s'entendent pour interconnecter leurs réseaux. Leurs emplacements sont d'importance cruciale et les États ne peuvent pas s'en désintéresser. Il y a dès lors une possibilité théorique de couper Internet en fermant ces NAPs. Par exemple, au moment de la révolte égyptienne au printemps 2011, les autorités du Caire décidèrent de fermer les dits sites.

2. Analogie et superpositions

Quels sont les points communs et les points de comparaison viables entre espace extra-atmosphérique, espace maritime et cyberespace ? Quelles sont les limites de cette analogie ?

2.1. Analogie des espaces

L'analogie avec les espaces maritimes est extrêmement fructueuse. Mais force est de constater qu'il y a autant d'analogies que d'experts. Les océans sont-ils comparables aux Autonomous systems ou aux câbles de fibre optique ? Ces câbles sont-ils plutôt l'équivalent de détroits et autres passages stratégiques ? Il est toutefois possible d'opter pour les subdivisions ci-dessous :

Un Etat est un espace délimité par des frontières, se caractérisant par un « intérieur » et un « extérieur » régis par des règles différentes, sous le contrôle d'une autorité unique. C'est l'analogie la plus pertinente pour l'**Autonomous System** (ou AS), ce dernier se définissant comme « un ensemble de réseaux informatiques IP intégrés à Internet et dont la politique de routage interne (routes à choisir en priorité, filtrage des annonces) est cohérente », et « généralement sous le contrôle d'une entité/organisation unique »[13] (un fournisseur d'accès à Internet, une entreprise, etc.).

Les eaux intérieures et immédiatement adjacentes au territoire (ports, baies, criques) peuvent, par conséquent, être assimilées aux limites d'AS caractérisées par un **routeur de bordure d'AS**. Le routeur de bordure joue en effet le rôle de frontière entre l'intérieur d'un AS et l'extérieur (obéissant à un autre protocole : BGP). Le routeur de bordure d'AS maîtrise donc les deux protocoles : interne et externe à l'AS.

La mer territoriale est un espace maritime sur lequel l'Etat exerce sa souveraineté la plus importante. Elle peut donc être assimilée aux **câbles de transit**, considérés à l'échelle de la connexion mondiale comme non stratégiques, ou stratégiques pour une petite quantité d'Etats.

Les détroits et canaux sont, eux, plus stratégiques, à l'image des **câbles de fibre optique de *peering*** entre AS de tier 1 ou tier 2, ou câbles liant deux points d'échange Internet (ou IXP). Véritables autoroutes, ces câbles de fibre optique permettent une connexion de point à point, et sont assimilables de ce fait aux voies stratégiques menant aux grands océans, telles que les canaux ou détroits. L'analogie est d'autant plus pertinente qu'elle rejoint également l'idée selon laquelle ces détroits ou canaux ne sont que des voies permettant d'atteindre un point plus rapidement, mais ne représentent pas l'unique chemin permettant d'atteindre ce point. De la même manière, le fonctionnement d'Internet qui privilégie la route la plus rapide par défaut, se caractérise par la possibilité, en cas d'indisponibilité de la route la plus courte, d'en emprunter d'autres. La seule différence tiendra au facteur temps (des semaines sur l'eau, des millisecondes dans le cyberespace).

La fragmentation des données caractérisant le **cloud computing** rejoint la notion d'**eaux archipélagiques,** connexe à celle de « discontinuité territoriale ». Discontinuité qui caractérise aussi un empire colonial, ou un Etat fragmenté (exemple : Etats-Unis et Alaska).

[13] Définition issue de Wikipedia.

La question des points d'échange Internet souligne toutefois la difficile transposition du statut de la haute mer. L'équivalent de la haute mer pourrait en effet être le point d'échange Internet (ou IXP). Ce point d'échange connecte entre eux plusieurs AS, par le biais de routes stratégiques que sont les câbles. Ils constituent de véritables points d'intersection. Deux océans (IXP) seront liés entre eux par des détroits ou canaux stratégiques que sont les câbles de fibre optique.

2.1.1. Tableau récapitulatif

	Mer	Cyber
Milieu	Océan	Points d'échange Internet
	Passages stratégiques : océans	Câble de peering
	Mer territoriale	Câble de transit
	Détroits, canaux	Câbles optiques
	Etat doté de frontières	AS
	Territoire	Data center
	Port, baies, criques	Routeur de bordure d'AS
	Ile	Territoire isolé numériquement
	Archipel	Cloud computing
	Fond des mers	Web profond
Utilisateurs	Individus	Individus
	Entreprises	Entreprises
	Etats (militaires)	Etats (militaires)
Véhicules et transport	Cargo	Paquets de données
	Container	Données
	Navires	Flux de données, protocoles de transport
	Immatriculation, pavillon	Adresse IP
Hub	Bases navales	Internet Exchange Point (IXP)
	Haute mer	

2.2. L'analogie sur la dimension stratégique : des domaines stratégiques d'expression de puissance

L'analogie peut également faire abstraction des composantes matérielles des sujets de droit (où l'analogie peut se révéler très faible en raison des différences intrinsèques des sujets), pour se concentrer sur les fonctions stratégiques des éléments observés.

Comme la haute mer, l'espace extra-atmosphérique ou encore l'espace aérien, le cyberespace est devenu un enjeu d'hégémonie pour les Etats. Dès le 19ème siècle, la haute mer était vue par certains auteurs comme un espace public mondial hautement stratégique. Alfred Thayer Mahan[14], officier de marine américain, considérait en effet que les cinq éléments constitutifs de la supériorité britannique étaient basés sur leur usage habile de la haute mer (commerce extérieur, une marine marchande abondante, une marine de guerre protégeant les voies maritimes, un empire colonial conséquent et un réseau étendu de bases navales). Enjeu de puissance désormais incontournable, la haute mer devait être investie par les Etats-Unis afin qu'ils affirment leur puissance à l'échelle internationale. A l'inverse, une mauvaise appréhension de cet espace mettrait en péril cette puissance.

Dans une certaine mesure, ce raisonnement peut être appliqué au cyberespace[15]. Support et moteur de l'économie mondial, espace d'exercice des libertés fondamentales, nouvel enjeu militaire et de conflits, cet espace numérique est aujourd'hui un critère de puissance incontournable. Il est devenu l'espace à maîtriser ; en témoignent les moyens colossaux investis par les Etats en ce sens.

A l'image de la conquête de l'espace, ainsi que de la maîtrise de plus en plus importante de la mer (via la portée croissante des armes), motivées par une montée en puissance technologique, le cyberespace est aujourd'hui en proie à de nombreuses convoitises. La singularité de la constitution du cyberespace inverse toutefois les raisonnements. Approprié par la société civile et les activités économiques, le cyberespace est aujourd'hui un domaine d'expression des libertés fondamentales et de développement économique. La dynamique de militarisation, mais aussi la montée en puissance de la lutte contre la cybercriminalité traduisent la volonté des Etats de reprendre la main sur ce domaine. L'omniprésence d'Internet fait de cet outil un vecteur et une cible de choix lors de conflits internationaux. La singularité de la démarche de création du domaine artificiel qu'est le cyberespace se traduit également par l'ultra-domination de certains acteurs, économiques ou étatiques, à l'image des GAFAM (Google, Amazon, Facebook, Apple, Microsoft) sur la couche logique et cognitive, mais aussi sur la couche physique (convergence et maîtrise des câbles).

Ainsi, si la conquête des domaines ne s'est pas réalisée selon la même logique, des problématiques similaires d'ordonnancement de la gouvernance entre les différents acteurs et leurs intérêts divergeants se posent. La volonté de protéger les plus faibles en leur garantissant un accès, tout en contenant les plus forts, se pose de plus en plus. Des problématiques proches de celles de préservation du milieu et de garanties d'accès aux ressources naturelles et aux espaces stratégiques.

[14] Alfred Thayer Mahan, The Influence of Sea Power Upon History, 1660–1783 (New York: Dover Publications, Inc., 1987.
[15] Voir en ce sens : « Les Global Commons et l'Internet à la lumière d'Alfred Mahan », Laurent Bloch, 2011.

Conclusion partielle

Si les trois sujets de droit ne sont pas comparables par leur essence (sujets naturels et sujet artificiel), l'analogie permet de déceler des similitudes fonctionnelles et stratégiques entre composantes. Elle se traduit par l'existence de flux plus ou moins contrôlés, de voies stratégiques et moins stratégiques, de raccourcis (et d'enclavement), d'axes clés, mais aussi de zones plus ou moins communes aux différents acteurs. C'est cette analogie fonctionnelle qui rythmera l'étude, notamment l'exercice de transposition des différentes dispositions juridiques préexistantes.

2ème partie : Transposition et étude d'adéquation

Le cyberespace soulève de nombreux défis : hétérogénéité des législations, prolifération des paradis numériques, circulation et protection des données, neutralité du net, etc. Un droit du cyberespace aura pour objectif de répondre avec efficacité à ces problématiques, afin d'atteindre l'objectif de stabilité et de sécurité internationale. Par conséquent, l'analogie (notamment quant aux usages stratégiques) doit déboucher sur la proposition de mesures applicables et adéquates aux spécificités et aux principaux enjeux du cyberespace. Certaines règles et autres grands principes élaborés dans le cadre du droit de l'espace[16] et du droit de la mer ont, pour leur part, contribué (bien que contestés) à la stabilité internationale sur ces domaines. Ils peuvent inspirer un droit du cyberespace. D'autres s'appliquent déjà au cyberespace en raison de l'entrelacement des trois domaines.

1. Etat des lieux des dispositions du droit de la mer et du droit de l'espace étant directement applicables au cyberespace

Le droit de la mer et le droit de l'espace proposent chacun un régime juridique de protection de certaines infrastructures de télécommunication propres à leurs milieux. Ces dispositions vont, par ricochet, venir encadrer juridiquement – et donc protéger – une partie de la couche physique du cyberespace.

1.1. Le droit de l'espace

Le droit de l'espace trouve ses sources dans le droit international issu de l'Organisation des Nations unies, notamment quant au régime de fréquences des orbites élaboré dans le cadre de l'UIT (Union Internationale des Télécommunications), mais aussi dans quelques directives européennes. Les principaux textes sont le Traité de l'espace (1967) et les conventions sur la responsabilité (1972) et l'immatriculation (1974). Le droit de l'espace liste les principes ci-après. Ceux-ci sont directement applicables au cyberespace, en ce qu'ils protègent certaines infrastructures participant à la couche physique du cyberespace.

1.1.1. Le principe de non-agression dans l'espace

Source
Traité de l'espace : « Article III

[16] Ces grands principes se retrouvent dans la « Déclaration des principes juridiques régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique » http://www.unoosa.org/oosa/fr/SpaceLaw/gares/html/gares_18_1962.html

Les activités des États parties au Traité relatives à l'exploration et à l'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, doivent s'effectuer conformément au droit international, y compris la Charte des Nations Unies, en vue de maintenir la paix et la sécurité internationales et de favoriser la coopération et la compréhension internationales. »

Commentaire

Avant d'être une source d'inspiration pour un droit du cyberespace, le principe de non-agression dans l'espace a pour première finalité de protéger l'intégrité des infrastructures de télécommunication, dont certaines participent à Internet, composante essentielle du cyberespace.

Ce principe trouve sa source dans l'obligation faite, dans le cadre du droit de l'espace, d'être conforme aux principes du droit international, notamment en respectant le principe de non-agression présenté par la Charte des Nations unies.

Champ d'application

Il peut s'appliquer dans un futur droit du cyberespace, et constitue la première brique du régime protecteur des infrastructures physiques du cyberespace présentes dans l'espace extra-atmosphérique.

1.1.2. Le principe de non-interférence avec les activités des autres Etats

Source

Traité de l'espace :

« Article I :

« L'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, peut être exploré et utilisé librement par tous les États sans aucune discrimination, dans des conditions d'égalité et conformément au droit international, toutes les régions des corps célestes devant être librement accessibles. »

Commentaire et champ d'application

Il peut s'appliquer dans un futur droit du cyberespace, en ce qu'il impose aux Etats de ne pas empêcher leurs homologues de se doter d'infrastructures.

1.1.3. Le principe de l'utilisation pacifique

Source

Traité de l'espace :

« Article IV:

« Les États parties au Traité s'engagent à ne mettre sur orbite autour de la Terre aucun objet porteur d'armes nucléaires ou de tout autre type d'armes de destruction massive, à ne pas installer de telles armes sur des corps célestes et à ne pas placer de telles armes, de toute autre manière, dans l'espace extra-atmosphérique.

Tous les États parties au Traité utiliseront la Lune et les autres corps célestes exclusivement à des fins pacifiques. Sont interdits sur les corps célestes l'aménagement de bases et installations militaires et de

fortifications, les essais d'armes de tous types et l'exécution de manœuvres militaires. »

Commentaire

L'utilisation pacifique de l'espace impose une utilisation pacifique des objets en orbite, dont font partie les infrastructures d'Internet.

La question se pose toutefois, pour le second paragraphe de l'article IV, de la définition de la notion d' « armes de tous types ». Cette notion englobe-t-elle, *in extenso*, la notion de cyberarme ?

Cette question, en suspens, élargirait considérablement le champ d'application du texte.

Champ d'application

Ces dispositions s'appliquent aux infrastructures d'Internet. Elles ont pour finalité d'assurer leur protection, en les tenant éloignées de tout conflit international.

1.1.4. Le principe de responsabilité de l'Etat de lancement pour dommage

Sources

Traité de l'espace :

« Article VI :

« Les États parties au Traité ont la **responsabilité internationale des activités** nationales dans l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, qu'elles soient entreprises par des organismes gouvernementaux ou par des entités non gouvernementales, et de veiller à ce que les activités nationales soient poursuivies conformément aux dispositions énoncées dans le présent Traité.»

« Article VII :

« Tout État partie au Traité qui procède ou fait procéder au lancement d'un objet dans l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, et tout État partie dont le territoire ou les installations servent au lancement d'un objet, est responsable du point de vue international des dommages causés par ledit objet ou par ses éléments constitutifs [...] »

Commentaire

Le principe de responsabilité internationale vient renforcer les obligations précédemment listées, en aménageant un recours pour les victimes.

Champ d'application

Il est tout à fait envisageable qu'un Etat victime d'une coupure de son réseau en raison d'une activité malveillante ou d'un accident de la responsabilité d'un tiers, puisse enclencher ce mécanisme à des fins de réparation.

1.2. Le droit de la mer

Les dispositions du droit de la mer applicables au cyberespace, et plus précisément à ses infrastructures physiques sous-marines, sont répertoriées dans convention des Nations unies sur le droit de la mer (1982) et la convention internationale relative à la protection des câbles sous-marins, signée à Paris le 14 mars 1884.

« Les câbles sous-marins sont des fils ou faisceau de fils ou de fibres optiques, isolés et étanches, servant à transporter des biens immatériels (de l'énergie, des informations) »[17]. Ils assurent 95 % des télécommunications internationales et constituent le principal vecteur d'Internet.

Sources
Convention internationale relative à la protection des câbles sous-marins : « Article 2 : « La rupture ou la détérioration d'un câble sous-marin, faite volontairement ou par négligence coupable, et qui pourrait avoir pour résultat d'interrompre ou d'entraver, en tout ou partie, les communications télégraphiques est punissable, sans préjudice de l'action civile en dommages-intérêts ». « Article 4 : Le propriétaire d'un câble qui, par la pose ou la réparation de ce câble, cause la rupture ou la détérioration d'un autre câble doit supporter les frais de la réparation [...] ». Ces textes ont été intégrés dans la convention des Nations unies sur le droit de la mer (ou Convention de Montego Bay) aux articles 113 et suivants.
Commentaire
La convention internationale relative à la protection des câbles sous-marins sanctionne la dégradation volontaire « ou par négligence coupable » de câbles.
Champ d'application
Ces textes peuvent s'appliquer en cas de dégradation volontaire de la couche physique du cyberespace en mer. La détérioration de câbles peut être un mode d'action privilégié en cas de conflit international, afin d'isoler numériquement un Etat. L'inverse est toutefois plus courant : les tentatives d'isolation d'un territoire viennent souvent de l'intérieur, les grandes puissances du cyberespace cherchant, au contraire, à développer les points de connexion à des fins d'influence.

[17] « Le régime international des câbles sous-marins », Savadogo Louis, Journal du Droit International Clunet, 2013
http://documentation.outre-mer.gouv.fr/Record.htm?idlist=1&record=19123486124919416689

2. Analyse des dispositions du droit de la mer et du droit de l'espace pouvant inspirer un droit du cyberespace

Si le droit de l'espace est extrêmement riche en principes généraux pouvant être appliqués au cyberespace, le droit maritime intègre pour sa part la notion d'aménagement de la souveraineté, notion clé que l'on retrouvera par la suite. C'est un juste équilibre de ces deux grands axes qu'il conviendrait d'adopter pour le cyberespace, selon que l'on veuille règlementer sa couche logique, de commande et contrôle, physique ou cognitive.

2.1. L'influence des textes préliminaires

Un droit du cyberespace devrait être innovant, en raison de la remise en cause, par l'innovation technologique constante, des processus multilatéraux traditionnels, et du manque de consensus sur la question à l'échelle internationale.

2.1.1. Un indispensable effort de définitions : l'importance de partager des définitions communes et l'importance de les influencer

La convention « Responsabilité et dommages des objets spatiaux » apporte des éléments de définition essentiels à la compréhension du texte. Sont ainsi définis : le dommage, le lancement, l'Etat de lancement.

Exemple de définition en droit de l'Espace :

Convention responsabilité et dommages des objets spatiaux, article 1 : « Le terme « dommage » désigne la perte de vies humaines, les lésions corporelles ou autres atteintes à la santé, ou la perte de biens d'État ou de personnes, physiques ou morales, ou de biens d'organisations internationales intergouvernementales, ou les dommages causés auxdits biens ».

Un droit du cyberespace devrait avoir pour tâche première de tenter de définir ce qu'est le cyberespace et, surtout, ce qu'est une cyberarme ainsi qu'une cyberattaque. Le tout en prenant garde à ne pas s'attacher à une quelconque technologie, et à identifier des définitions suffisamment intemporelles pour assurer la pérennité du texte adopté, de technologies en technologies. Les textes 323-1 du Code pénal français en sont un bon exemple, l'expression « système de traitement automatisé de données » s'adaptant *a priori* à toute évolution technologique.

Focus : la question de la définition de la cyberarme cristallise les oppositions

Une cyberarme peut être définie comme un programme informatique malveillant dont la finalité est de pénétrer les réseaux informatiques adverses pour compromettre ou saboter son système d'information ou un sous-ensemble de celui-ci. Une cyberarme ne peut néanmoins pas être simplement définie par sa seule complexité. D'autres programmes malveillants comme les RAT (Remote Administration Tool) ou les logiciels permettant de coordonner et lancer des attaques par déni de service distribué peuvent être également qualifiés de cyberarmes. Il faut également souligner le caractère dual d'une arme informatique. En effet, un seul et même programme informatique peut être à la fois être développé et utilisé à des fins défensives ou

offensives, et dans un contexte militaire ou civil. Certains auteurs comme Thomas Rid et Peter McBurney proposent également une classification[18] des cyberarmes en deux grandes catégories :

- Les armes informatiques génériques à faible potentiel. Elles sont simples d'utilisation, facilement disponibles mais leurs impacts restent limités (par exemple, des malwares basiques, des outils DDoS, etc.)
- Les armes informatiques sur-mesure à haut potentiel. Elles sont comparées à des armes « intelligentes ». Très sophistiquées, elles nécessitent une phase spécifique de renseignement sur les systèmes ciblés, des investissements importants en matière de R&D et un temps de développement élevé (par exemple, Stuxnet ou Duqu[19]).

A cela, s'ajoute la question de la nature armée ou non d'un outil de surveillance de masse exploité à des fins répressives.

La définition du dommage en matière cyber est également primordiale : envisage-t-on une vision restrictive de dommages faits uniquement à l'intégrité de données piratées et au bon fonctionnement d'un ordinateur (machine à machine), ou uniquement aux pertes de vies humaines, etc. ? Ou envisage-t-on une vision extensive, à l'image de la définition donnée par la convention responsabilité et dommages des objets spatiaux ?

Le partage de définitions et de concepts communs reste un pas indispensable à une coopération effective. Pour un Etat, réussir à imposer sa définition reste un acte d'influence habile.

2.1.2. Le préambule, outil d'influence

Le préambule d'un texte international est loin d'être inutile. Bien que souvent sous-estimé, il pose un contexte et une dynamique propre aux Etats en influençant l'adoption. Volonté de porter un message positif d'espoir, d'alerter sur une problématique contemporaine ou d'avertir et de dissuader les non-adoptants… le préambule n'est pas à négliger.

Souhaitant replacer le texte dans un contexte global, le préambule du *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*[20] (ci-après « Traité de l'espace »)[21] propose un rappel de généralités, visant à affirmer symboliquement certains principes généraux. Il réaffirme l'importance de la coopération internationale et du « règne du droit » ; « se félicite » de la conclusion du traité ; « exprime l'espoir » d'une forte adhésion des Etats au traité.

Les mêmes éléments peuvent être envisagés dans le préambule d'un éventuel traité portant sur le cyberespace. Il paraitra en effet non superflu de rappeler la volonté première des gouvernements dépositaires du texte initial : appliquer le droit, préserver la paix, préserver et protéger le cyberespace comme étant une innovation, voire une révolution technologique d'intérêt capital pour l'humanité, et trouver le consensus.

[18] http://www.tandfonline.com/doi/full/10.1080/03071847.2012.664354#tabModule
[19] Pour en savoir plus : http://www.numerama.com/magazine/20466-le-virus-duqu-detecte-par-un-outil-open-source.html
[20] 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 , consultable : http://www.unoosa.org/oosa/fr/SpaceLaw/gares/html/gares_21_2222.html

[21] Ce document, initialement conclu entre les trois pays que sont l'Union Soviétique, les Etats-Unis et le Royaume-Uni en 1967, a par la suite été ratifié par de nombreux autres Etats. Il prévoie quelques dispositions méritant le détour.

Traité de l'espace, préambule : « *S'inspirant* des vastes perspectives qui s'offrent à l'humanité du fait de la découverte de l'espace extra-atmosphérique par l'homme, [...] ».

Le préambule d'un traité sur le cyberespace ne fera pas l'économie de la mention de la vitesse de l'innovation, et des changements prévus à moyen et long terme (Internet des objets, nanotechnologies, Web 4.0.

Ce même texte pourra, à l'inverse, emprunter une tonalité plus belliqueuse, ou encore aborder plus en détails les réels enjeux ayant poussé à l'adoption d'un texte, selon la volonté réelle des gouvernements dépositaires.

Le préambule de la convention des Nations unies sur le droit de la mer (ci-après « Convention de Montego Bay ») va en ce dernier sens. Ses premières lignes laissent supposer une préalable mésentente, la nécessité de régler des différends.

2.2. La qualification du domaine comme patrimoine commun de l'Humanité

2.2.1. Source

Le droit de la mer et le droit de l'espace présentent tous deux la particularité de tenter de règlementer les usages sur des espaces physiques, préexistants et naturels. Et tous deux ont, dans leurs principaux textes, identifié tout ou partie de ces espaces comme étant des patrimoines communs de l'Humanité.

Ce que le droit de la mer prévoit :

Convention de Montego Bay, préambule : « Souhaitant développer, par la Convention, les principes contenus dans la résolution 2749 (XXV) du 17 décembre 1970, dans laquelle l'Assemblée générale des Nations Unies a déclaré solennellement, notamment, que la zone du fond des mers et des océans, ainsi que de leur sous-sol, au-delà des limites de la juridiction nationale et les ressources de cette zone sont le patrimoine commun de l'humanité et que l'exploration et l'exploitation de la zone se feront dans l'intérêt de l'humanité tout entière, indépendamment de la situation géographique des Etats,

Ce que le droit de l'espace prévoit :

Accord régissant les activités des États sur la Lune et les autres corps célestes, art. 11 : « La Lune et ses ressources naturelles constituent le patrimoine commun de l'humanité »

2.2.2. Problématiques adressées

Transposer ces dispositions au cyberespace a pour finalité d'adresser les problématiques suivantes : reconnaître l'intérêt public et international global « supérieur aux intérêts nationaux ou privés » du cyberespace, la nature transfrontalière qui le caractérise ; mais aussi le fait qu'Internet constitue une ressource « abondante de force créatrice » désormais en proie à la cybercriminalité et à la militarisation

croissante[22].

2.2.3. Exemple de transposition

« Le cyberespace, dans ses composantes physiques, logiques et cognitives, présente un intérêt public et international global supérieur aux intérêts nationaux ou privés. Il est le patrimoine commun de l'Humanité ».

2.2.4. Commentaires

Une analogie faible

Le cyberespace, créé de toutes pièces par l'Homme et dont les infrastructures physiques sont régies par la propriété privée et les rapports contractuels, tient difficilement l'analogie sur le plan structurel.

La possibilité de qualifier Internet de « patrimoine commun appartenant à toute l'humanité (ci-après « PCH »), sans que quiconque puisse en revendiquer un usage exclusif » a toutefois bel et bien été évoquée dans le rapport intitulé « Internet : pour une gouvernance ouverte et équitable » du Conseil économique, social et environnemental.

Il est vrai qu'Internet et, plus globalement le cyberespace présente un intérêt public et international global « supérieur aux intérêts nationaux ou privés », une nature transfrontalière qui le caractérise, et constitue une ressource « abondante de force créatrice » désormais en proie à la cybercriminalité et à sa militarisation croissante. Protéger cet actif en lui appliquant le qualificatif de PCH semble alors pertinent.

Une telle reconnaissance aurait tout d'abord une portée principalement symbolique. Elle aurait les faveurs de la société civile sans pour autant contraindre fermement les autres acteurs de la gouvernance du cyberespace. Cette reconnaissance pourrait également être plus ferme et être assortie de mesures strictes, menant à l'établissement d'une gouvernance multi-acteurs. La reconnaissance de l'intérêt commun aurait également comme conséquence l'émergence d'autres principes (non-appropriation, libre-accès, libre-circulation, l'usage pacifique…) qui, adaptés au cyberespace, pourraient adresser les problématiques relatives à la neutralité du net, la fracture numérique, la militarisation, etc.

Une définition floue

Il n'existe pas de définition unique de la notion de « patrimoine commun de l'Humanité ». L'expression a été utilisée pour la première fois à propos des grands fonds marins en 1958. Le professeur de droit international belge Jean Salmon le définit comme un « espace de biens appartenant à l'humanité toute entière et, partant, soustraits à l'appropriation exclusive des Etats ». Ont été qualifiées de patrimoine commun de l'humanité : la Zone (en vertu de l'article 136 la Convention sur le Droit de la mer du 30 avril 1982[23] modifiée en 1994) et la Lune (Traité de l'espace). D'autres espaces font aujourd'hui débat : l'Antarctique, le spectre des fréquences radioélectriques ou encore la biosphère.

Bien que non reconnue en droit positif, la qualification de PCH influence fortement les différentes dispositions d'un traité international. Cette qualification a un impact direct majeur car elle impose l'application des trois principes suivants : la protection des intérêts de l'humanité (utilisation efficace et

[22] « Internet : pour une gouvernance ouverte et équitable », Nathalie CHICHE, Conseil économique, social et environnemental http://www.lecese.fr/travaux-publies/internet-pour-une-gouvernance-ouverte-et-equitable
[23] Voir également : Résolution 2749 (XXV) de l'Assemblée Générale des Nations Unies, 1970.

rationnelle, lutte contre pollution, etc.) ; l'usage pacifique ; et surtout le principe de « non-appropriation ».

Ces principes, corolaires de la qualification de PCH, peuvent êtres affirmés un à un de façon distincte. Il est ainsi possible, tout en évitant la qualification de PCH, d'affirmer la viabilité de certains principes. Mais la qualification du cyberespace comme patrimoine commun de l'humanité est-elle envisageable ? Si comme vu ci-dessus, la transposition des deux premiers principes est tout à fait possible, celui de la « non-appropriation » du cyberespace se heurte à des réalités bien plus complexes.

Conclusion

Plusieurs options sont envisageables pour cette transposition. La première est de qualifier le cyberespace comme patrimoine commun de l'humanité. La seconde est de créer un statut *ad hoc* pour le cyberespace, un statut « à la carte » en raison du flou entourant la notion de patrimoine commun de l'humanité, afin d'écarter certaines contraintes liées à cette qualification. Enfin, toujours dans une logique de transposition partielle, il est envisageable de ne sanctuariser qu'une partie du cyberespace (exemple : la couche C&C).

2.3. La non-appropriation des espaces, un principe éloigné de la réalité du cyberespace

2.3.1. Source

Ce que le droit de l'espace prévoit :

Traité de l'espace, art. 2 : « L'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, **ne peut faire l'objet d'appropriation nationale** par proclamation de souveraineté, ni par voie d'utilisation ou d'occupation, ni par aucun autre moyen. »

Le principe de non-appropriation est affirmé par le traité de l'Espace en son article 2, par l'Accord régissant les activités des États sur la Lune et les autres corps célestes dans son art. 11 § 2 (La Lune ne peut faire l'objet d'aucune appropriation nationale par proclamation de souveraineté, ni par voie d'utilisation ou d'occupation, ni par aucun autre moyen. »).

L'Accord régissant les activités des États sur la Lune et les autres corps célestes dans son art. 11 § 3 « Ni la surface ni le sous-sol de la Lune, ni une partie quelconque de celle-ci ou les ressources naturelles qui s'y trouvent, ne peuvent devenir la propriété d'États, d'organisations internationales intergouvernementales ou non gouvernementales, d'organisations nationales ou d'entités gouvernementales, ou de personnes physiques. »

Cette non-appropriation ne se retrouve en droit de la mer qu'à propos de la « zone du fond des mers et des océans, ainsi que de leur sous-sol »[24], qualifiés de patrimoine commun de l'humanité (ci-après PCH).

[24] Convention de Montego Bay, préambule.

2.3.2. Commentaires

La réalité du cyberespace est très éloignée de ces concepts. Sa nature artificielle se caractérise par une forte présence de la propriété privée, notamment quant à ses infrastructures physiques. Les data centers et autres câbles transocéaniques sont la propriété d'opérateurs privés ou de consortiums, et sont régis par des accords et contrats. Chaque terminal (ordinateur, smartphone…), une fois connecté, fait partie du cyberespace, tout en appartenant à un particulier. La multiplicité des acteurs ainsi que la nature artificielle du cyberespace excluent donc l'application du principe de non-appropriation au cyberespace dans sa globalité. Or, ce principe est l'un des principaux corrolaires de la qualification de patrimoine commun de l'Humanité.

Si la qualification du cyberespace de patrimoine commun de l'Humanité semble inconcevable en l'état, plusieurs observateurs s'accordent à reconnaître qu'il serait possible de consacrer l'intérêt commun de façon partielle, d'autres strates du cyberespace telle que la couche dite de Commande et contrôle (rassemblant les fonctions DNS, BGP, les tables et protocoles de routage et les logiciels qui les implémentent[25]). Ainsi, à l'image de la Zone ou de la Lune qui ne sont que des parties de leur domaine respectif, cet ensemble de protocoles et de standards serait préservé dans l'intérêt commun de l'Humanité.

La seconde possibilité est d'imaginer un statut *ad hoc*, spécifique au cyberespace. L'absence de définition figée du patrimoine commun de l'Humanité n'exclut pas la création d'un statut dédié, reconnaissant un principe global d'intérêt commun au cyberespace, tout en reconnaissant un aménagement de la souveraineté des Etats et de la propriété privée sur ces éléments.

2.4. La consécration d'un droit d'accès de tous les Etats

2.4.1. Source

Traité de l'espace, préambule :

« *Reconnaissant* l'intérêt que présente pour **l'humanité tout entière** le progrès de l'exploration et de l'utilisation de l'espace extra-atmosphérique à des fins pacifiques, […] » ;

« Estimant que l'exploration et l'utilisation de l'espace extra-atmosphérique devraient s'effectuer **pour le bien de tous les peuples, quel que soit le stade de leur développement économique ou scientifique**, […] ».

Traité de l'espace, art. 1, § 1 : « L'exploration et l'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, doivent se faire **pour le bien et dans l'intérêt de tous les pays**, quel que soit le **stade de leur développement économique ou scientifique**; elles sont l'apanage de l'humanité tout entière. »

Traité de l'espace, art. 1, § 2 : « L'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, **peut être exploré et utilisé librement par tous les États sans aucune discrimination**, dans des conditions

[25] FGI, atelier cyberstratégie, Laurent Bloch.

d'égalité et conformément au droit international, toutes les régions des corps célestes devant être librement accessibles. »

Traité de l'espace, art. 12 : « Toutes les stations et installations, tout le matériel et tous les véhicules spatiaux se trouvant sur la Lune ou sur d'autres corps célestes seront **accessibles, dans des conditions de réciprocité, aux représentants des autres États** au Traité. Ces représentants notifieront au préalable toute visite projetée, de façon que les consultations voulues puissent avoir lieu et que le maximum de précautions puissent être prises pour assurer la sécurité et éviter de gêner les opérations normales sur les lieux de l'installation à visiter. »

Convention de Montego Bay :

« Considérant que la réalisation de ces objectifs contribuera à la mise en place d'un **ordre économique international juste et équitable** dans lequel il serait tenu compte des intérêts et besoins de l'humanité tout entière et, en particulier, des intérêts et besoins spécifiques des **pays en développement, qu'ils soient côtiers ou sans littoral**, [...] ».

2.4.2. Problématiques adressées

La transposition de ces dispositions adresse les problématiques suivantes :

- Libre circulation des données entre les pays,
- Libre accès/usage au réseau,
- Lutte contre la fracture numérique à l'échelle nationale et internationale.

2.4.3. Exemple de transposition

« Reconnaissant l'intérêt que présente pour l'humanité toute entière le progrès de l'accès à Internet et son impact sur le développement économique, social, scientifique [...]

Reconnaissant le droit fondamental pour tous les Etats, sans aucune discrimination, de disposer d'un accès à Internet dans des conditions respectueuses des dispositions internationales ».

2.4.4. Commentaires

Transposés, ces textes peuvent avoir un impact fort, par la reconnaissance d'un droit pour tous les Etats d'accéder à Internet.

Il s'agirait d'affirmer dans un texte à portée internationale la volonté à court terme de mettre fin à la fracture numérique, d'étendre le réseau jusqu'aux pays en développement et de permettre aux pays enclavés numériquement d'accéder à Internet à moindre coûts. L'impact d'une telle disposition serait une possible réforme du système actuel d'accords de *peering*, mais surtout de *transit* entre opérateurs dits tier 1 et tier 3.

Dans un contexte où il est reconnu qu'Internet accentue le développement économique d'un pays, porter une telle disposition permet à l'Etat la proposant de se positionner en *leader* d'une volonté de généraliser l'accès à Internet vers les Etats en difficulté, les Etats aux populations muselées. Il s'agit là d'un **texte à forte portée diplomatique** (« diplomatie 2.0 »).

La seconde conséquence de la proposition d'un tel texte est, pour l'Etat le portant, de bénéficier, d'initier à l'aide de ses opérateurs nationaux, l'équipement des pays en développement en question, et ainsi de s'assurer une **maîtrise des infrastructures physiques de ces pays souvent à fort potentiel à moyen et long terme**. La mention de la notion de développement « scientifique » au-delà du simple développement « économique » permet également d'envisager le transfert de technologies et, par conséquent, une **maîtrise logicielle** considérable.

Le corolaire d'une telle mesure est l'affirmation d'un « libre passage » sur certains points de connexion clés, à l'image du droit de passage « inoffensif » prévu par l'article 19 de la convention de Montego Bay. On parle alors de **libre transit par la haute mer pour les Etats enclavés**. Ces mesures participent d'une sorte d'aménagement de la souveraineté des Etats et de la propriété privée des opérateurs détenteurs de la couche physique du cyberespace (voir développements ci-dessous).

2.5. La préservation du milieu

2.5.1. Source

Traité de l'espace, art. 9 : « [...] Les États parties au Traité effectueront l'étude de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, et procéderont à leur exploration de manière à **éviter les effets préjudiciables de leur contamination ainsi que les modifications nocives du milieu terrestre résultant de l'introduction de substances extraterrestres** et, en cas de besoin, ils prendront les mesures appropriées à cette fin. »

2.5.2. Commentaires

Le principe de préservation du milieu marin et la lutte contre la pollution peuvent être transposés au cyberespace. Ce dernier étant « pollué » par une quantité astronomique de *spam*, courriels indésirables dépassant de loin la quantité globale de courriels légitimes.

Les attaques contre le protocole BGP peuvent également être visées par le texte.

2.6. Le principe d'usage pacifique

2.6.1. Source

Traité de l'espace, préambule : « *Désireux* de contribuer au développement d'une large coopération internationale en ce qui concerne les aspects scientifiques aussi bien que juridiques de l'exploration et de l'utilisation de l'espace extra-atmosphérique à des fins pacifiques, [...] ».

Traité de l'espace, art. 3 : « Les activités des États parties au Traité relatives à l'exploration et à l'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, doivent s'effectuer **conformément au droit international**, y compris la Charte des Nations Unies, en vue de **maintenir la paix et la**

sécurité internationales et de favoriser la coopération et la compréhension internationales. »

Convention de Montego Bay : « Reconnaissant qu'il est souhaitable d'établir, au moyen de la Convention, compte dûment tenu de la souveraineté de tous les Etats, un ordre juridique pour les mers et les océans qui facilite les communications internationales et favorise les utilisations pacifiques des mers et des océans, l'utilisation équitable et efficace de leurs ressources, la conservation de leurs ressources biologiques et l'étude, la protection et la préservation du milieu marin, [...] ».

2.6.2. Problématiques adressées

La transposition de ces dispositions adresse les problématiques suivantes :

- Principe d'usage pacifique et encadrement de l'usage de la force dans le cyberespace ;
- Maitrise de la cybercriminalité ;
- Fondement juridique d'un mécanisme de responsabilité internationale et lutte contre les paradis numériques.

2.6.3. Exemple de transposition

« Les Etats s'engagent, afin de maintenir la paix et la sécurité internationale, afin de préserver le cyberespace comme patrimoine commun de l'Humanité/bien public mondial/héritage de l'Humanité, à un usage pacifique du réseau dans toutes ses composantes ».

2.6.4. Commentaires

La notion d'utilisation pacifique d'un espace dispose d'une portée principalement symbolique et encourage à ne pas mener d'action agressive. Si le traité de l'espace évoque une « coopération » sur la question de l'usage pacifique de l'espace extra-atmosphérique, la convention de Montego Bay se contente d'un ordre juridique « [favorisant] les utilisations pacifiques des mers et des océans ».

La question de l'affirmation « noir sur blanc » de l'impérative utilisation du cyberespace à des fins pacifiques présente un double enjeu. Le premier est d'arriver par-là à contraindre tout ennemi éventuel à peser la portée de ses actes offensifs dans le cyberespace, surtout si celui-ci a déjà quelques faits d'armes à son actif. Le second est, pour le pays porteur de la disposition, de ne pas limiter son propre champ d'action.

Ceci étant dit, l'affirmation de l'utilisation pacifique du cyberespace légitime bel et bien toute action visant à « pacifier », donc à mieux observer et maîtriser le cyberespace, mais aussi à intervenir en cas d'acte international illicite ou d'agression de la part d'un Etat. De plus, l'utilisation pacifique n'empêche certainement pas l'usage de la dissuasion. Un tel texte permet ainsi à l'Etat porteur d'influencer en son sens la coopération internationale. C'est la question de la distinction entre « usage pacifique » et « usage exclusivement pacifique ». Le droit de l'espace prévoit en effet dans un second temps un usage « exclusivement pacifique » des corps célestes, portant l'interdiction de l'« aménagement », de l'« installation » et d'« essais » d'outils militaires. Cette notion ne doit pas être confondue avec celle d' « usage pacifique ».

Traité de l'espace, art. 4, § 1 : Les États parties au Traité s'engagent à ne mettre sur orbite autour de la Terre aucun objet porteur d'armes nucléaires ou de tout autre type d'armes de destruction massive, à ne pas

installer de telles armes sur des corps célestes et à ne pas placer de telles armes, de toute autre manière, dans l'espace extra-atmosphérique.

Traité de l'espace, art. 4, § 2 : Sont interdits sur les corps célestes l'aménagement de bases et installations militaires et de fortifications, les essais d'armes de tous types et l'exécution de manouvres militaires.

Ainsi, si prôner un usage pacifique par le biais d'une obligation positive peut être un outil majeur d'influence, une limitation excessive des possibilités d'installation d'outils militaires ou d'essais de cyberarmes dans le cyberespace serait extrêmement contraignante. Un tel texte viendrait même contredire les derniers éléments abordés dans la récente loi de programmation militaire. Cette notion est reprise par l'art. 3 § 4 de l'Accord régissant les activités des États sur la Lune et les autres corps célestes.

2.7. L'aménagement de la souveraineté étatique

2.7.1. Sources

La question de la souveraineté est facilement délimitée en droit de l'Espace, entre les corps célestes et les objets spatiaux. C'est ainsi que l'article 12 de l'Accord régissant les activités des États sur la Lune et les autres corps célestes dispose que « les États parties conservent la juridiction ou le contrôle sur leur personnel, ainsi que sur leurs véhicules, matériel, stations, installations et équipements spatiaux se trouvant sur la Lune » et que « la présence sur la Lune desdits véhicules, matériel, stations, installations et équipements ne modifie pas les droits de propriété les concernant ». L'article 11 du même accord précise bien que « la Lune ne peut faire l'objet d'aucune appropriation nationale par proclamation de souveraineté, ni par voie d'utilisation ou d'occupation, ni par aucun autre moyen. »

La question est bien plus complexe en droit maritime, véritable droit « des » espaces maritimes.

Dans les deux cas toutefois, la question de la non-appropriation n'est pas traitée de façon uniforme : c'est un véritable aménagement de la souveraineté qui est prévu, aménagement dont peu s'inspirer un droit du cyberespace.

2.7.2. Problématiques adressées

La transposition de ces dispositions adresse les problématiques suivantes :

- Difficile agencement des acteurs dans un domaine foncièrement multi-acteur ;
- Restriction de l'hégémonie de certains acteurs ;
- Restriction de la liberté de certains acteurs privés responsables d'infrastructures critiques du cyberespace.

2.7.3. Exemples de transpositions et commentaires

La transposition de régime d'aménagement de la souveraineté étatique du droit de la mer, se traduit par l'aménagement de la propriété privée. La logique est en effet inversée, le cyberespace étant un domaine

artificiel principalement composé d'infrastructures privées.

La transposition impose de reprendre les termes de l'analogie déjà réalisée.

- Souveraineté pleine et entière :

La souveraineté pleine et entière se caractérise par l'absence de contraintes spécifiques. Ainsi, au sein d'un Autonomous system, l'opérateur ou l'entreprise responsable ne serait contraint par aucune disposition spécifique, hormis les diligences quant à la sécurité de ses infrastructures.

- Souveraineté aménagée :

L'équivalent d'une souveraineté aménagée dans le cyberespace se caractériserait par l'adjonction d'obligations nouvelles aux détenteurs de ces éléments stratégiques et d'intérêt commun : obligation de respecter la « libre circulation », obligation de préserver l'intégrité et le bon fonctionnement (entretien), etc.

Il est important de noter que certains canaux, même s'ils relèvent de la souveraineté du territoire duquel ils ont été creusés, sont soumis à un régime conventionnel qui garantit la libre navigation de tous les navires. Le régime du Canal de Suez est par exemple défini par la Convention de Constantinople de 1888[26], convention multilatérale. Le régime du Canal de Panama est fixé par une convention bilatérale entre les Etats-Unis et le Panama (1974 puis 1977).

- *La question des points d'échange Internet et l'impossible transposition du statut de la haute mer*

Pour cette dernière catégorie, le régime juridique applicable peut être celui de la zone contigüe, du plateau continental, ou de la zone économique exclusive. Impossible en effet d'aller plus loin dans l'analogie qui imposerait d'associer l'IXP à un espace international comme la haute mer échappant à toute emprise de souveraineté, et serait alors bien éloigné de la réalité du régime juridique de ces points d'échange Internet.

Le respect de ce régime de souveraineté aménagée serait assuré et contrôlé par une autorité indépendante, à l'image de l'Autorité des Fonds Marins (voir développements ci-dessous).

2.7.4. Commentaires

Une telle réforme ne peut se faire sans l'intégration des opérateurs et principaux consortiums à la réflexion. L'émergence de contraintes ne pourra faire consensus, qu'en cas de compensation par l'incitation à entretenir des infrastructures stratégiques (incitations financières, etc.).

2.8. L'application territoriale de la loi et la notion de juridiction

2.8.1. Sources

La question de l'immatriculation des objets lancés dans l'espace extra-atmosphérique fait l'objet d'une convention éponyme.

[26] Voir également : déclaration unilatérale de l'Egypte (1957), nationalisation du canal, Traité de Washington de 1979.

Traité de l'espace, art. 8 : « L'État partie au Traité sur le **registre** duquel est inscrit un objet lancé dans l'espace extra-atmosphérique **conservera sous sa juridiction et son contrôle ledit objet** [...]. »

En droit de la mer, chaque navire est associé à un pavillon (nationalité). L'Etat du pavillon peut exercer un contrôle sur le navire à tout moment (art. 92 à 94). Il y a également **juridiction exclusive**.

2.8.2. Problématiques adressées

La détermination de la loi applicable dans le cyberespace reste aujourd'hui un défi majeur à relever. La transposition de ces dispositions adresse les problématiques suivantes :

- Déterminer l'Etat compétent en cas de conflit : la transposition de ces mécanismes de détermination de la loi applicable (juridiction compétente) aurait ici pour finalité de simplifier la tâche des acteurs judiciaires, confrontés à la difficile identification de la loi applicable en cybercriminalité ;
- Constituer un point d'ancrage pour le mécanisme d'engagement de la responsabilité des Etats.

2.8.3. Exemples de transpositions

- L'immatriculation des objets spatiaux et l'immatriculation d'un navire (pavillon) correspondent théoriquement à **l'adresse IP d'origine** d'un paquet de données ;
- Le registre central de l'immatriculation des objets spatiaux et le numéro IMO (pour International Maritime Organization) correspondent à la **fonction IANA**, composante de l'ICANN et à l'action des **RIR** (registres Internet régionaux, réunis dans la Number Resource Organisation (NRO)), fonctionnant sur le RFC 2050[27] développé par l'IETF[28].

2.8.4. Commentaires

Une transposition inopérante

La transposition de ces dispositions est extrêmement complexe. En effet, il n'existe pas d'équivalent strict à la notion d'immatriculation. L'adresse IP, n'étant qu'une mention du départ et de l'arrivée d'un paquet à des fins de routage, n'est pas propre ou unique à chaque paquet.

De plus, en raison de la facilité avec laquelle il est possible de s'attribuer une adresse IP de son choix dans le monde (VPN, *spoofing*, etc.), ce texte serait complètement ineffectif et inapplicable.

Enfin, en cas de cyberattaque, la transposition pure et simple de ce texte permet à l'attaquant de faire primer la législation du pays d'où il ferait partir l'attaque, au détriment de celle de l'Etat de la victime. Un tel mécanisme encouragerait le développement et l'usage de paradis numériques. L'adresse IP ne peut donc être le seul outil déterminant la loi applicable.

Vers un Schengen du numérique ?

[27] RFC 2050, consultable : http://tools.ietf.org/html/rfc2050
[28] IETF : https://www.ietf.org/iesg/

La question de la détermination de la loi applicable sur Internet, notamment en cas d'infractions, rejoint celle des poursuites et des investigations portant sur des infractions aux éléments constitutifs distribués sur Internet[29] (instigation, préparation, mise en œuvre, diffusion, et impact), sur des juridictions distinctes. Il s'agit d'une situation proche de la situation actuelle en France: le parquet compétent pour la poursuite d'une infraction est, par défaut, celui du lieu de commission de cette infraction par son auteur. Mais le droit actuel est bien plus complet : le parquet compétent peut également être celui du lieu de constatation de l'infraction par la victime, ou celui du lieu d'hébergement des données (localisation du data center).

Les dispositions relatives à l'espace Schengen sont un bon exemple de coopération en matière d'investigations au-delà des frontières de forces de police nationales. Les contrôles aux frontières supprimés ont permis d'améliorer la coopération à travers la mise en œuvre du SIS (Système d'information Schengen).

Sont ainsi prévus :

- Le droit d'observation transfrontalière (article 40) ;
- Le droit de poursuite (article 41).

D'autres modèles de « juridictions » ou « territoires numériques »

Bertrand de La Chapelle[30] identifie pour sa part deux nouveaux modèles de « juridictions numériques » envisageables.

La juridiction du domaine Web (DNS) : Partant du principe que le cyberespace est organisé en domaines, *via* le Domain Name System, et que chaque domaine voit s'appliquer le droit de l'Etat correspondant, c'est le nom de domaine qui déterminerait la loi applicable. Passer d'un site web en .com à un site en .fr équivaut ainsi à franchir une « frontière numérique ».

La juridiction de l'entreprise fournissant un service d'hébergement : Cette seconde vision consacrerait l'importance des conditions générales d'utilisation des plateformes Web telles que Google ou Facebook, comme textes de référence. Ces plateformes constitueraient ainsi de nouveaux « territoires numériques ».

Cette vision va dans le sens d'une nouvelle géographie, propre au cyberespace. Cette nouvelle géographie rejoindrait les conclusions relatives à l'indépendance concrète des AS et aux résultats de l'analogie de ces AS aux Etats côtiers. Cette nouvelle géographie serait en réalité complémentaire des règles traditionnelles de désignation de la loi applicable.

Vers une compétence rationae cyber

C'est un modèle de compétence juridictionnelle *ad hoc* qu'il faut créer pour le cyberespace. Ce modèle sera développé dans les « Recommandations ».

[29] Voir la notion d'infraction pluri localisée. A cet égard, la jurisprudence a développé des critères de qualification de compétence.
[30] Directeur du projet « Internet & juridiction » à l'Académie diplomatique internationale et membre du directoire de l'ICANN.

2.9. La mise en œuvre de la responsabilité des Etats

2.9.1. Principe général

2.9.1.1.Sources

La question des dommages collatéraux causés par les objets dont l'Etat à la maîtrise fait l'objet de longs développements en droit de l'Espace. Le traité de l'espace aborde déjà largement le sujet en ces articles 6 à 8. Le droit de l'espace dispose toutefois d'une convention dédiée, portant « sur la responsabilité internationale pour les dommages causés par des objets spatiaux » (ci-après « convention responsabilité et dommages des objets spatiaux »).

2.9.1.2.Problématiques adressées

La question de l'attribution d'une cyberattaque en droit international est quant à elle une problématique récurrente. L'aborder dans un droit du cyberespace permettrait de faire, d'abord, un état des lieux des méthodes dont nous disposons pour identifier un cyberattaquant et, ensuite, pour les Etats de s'accorder sur un mécanisme de mise en œuvre de la responsabilité des différents acteurs ayant contribué à une cyberattaque.

2.9.2. La responsabilité de l'Etat pour les activités d'une entité étatique ou non-étatique

2.9.2.1.Sources

L'auteur pourra être une entité étatique ou non-étatique (mais pouvant être contrôlée par l'Etat), et sera identifié soit par revendication, soit par le faisceau d'indice révélé lors d'une investigation. (Ces éléments sont évoqués dans les articles 6 et 7 du Traité de l'Espace et sont à reprendre dans un droit du cyberespace) ;

La responsabilité de l'Etat pour les entités étatiques et non-étatiques :

Traité de l'espace, art. 6 : « Les États parties au Traité ont la **responsabilité internationale des activités nationales** dans l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, **qu'elles soient entreprises par des organismes gouvernementaux ou par des entités non gouvernementales**, et de veiller à ce que les activités nationales soient poursuivies conformément aux dispositions énoncées dans le présent Traité. Les activités des entités non gouvernementales dans l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, doivent faire l'objet d'une autorisation et d'une surveillance continue de la part de l'État approprié partie au Traité. »

L'auteur pourra également être l'Etat instigateur [...]

Traité de l'espace, art. 7 : « Tout État partie au Traité qui **procède** *(auteur)* **ou fait procéder** *(instigateur)* au lancement d'un objet dans l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, [...] » (confirmé par l'article 1, § c), i de la Convention responsabilité et dommages des objets spatiaux).

[...] à condition que sa requête ait un rapport de causalité direct avec les faits et les dommages qui en découlent.

Convention responsabilité et dommages des objets spatiaux, article 3 : « En cas de dommage causé, ailleurs

qu'à la surface de la Terre, à un objet spatial d'un État de lancement ou à des personnes ou à des biens se trouvant à bord d'un tel objet spatial, par un objet spatial d'un autre État de lancement, ce dernier État n'est responsable que si le dommage est imputable à sa faute ou à la faute des personnes dont il doit répondre. »

Notons que la convention responsabilité et dommages des objets spatiaux, prévoit en ses articles 4 et 5 un mécanisme de **responsabilité solidaire** pour des Etats ayant agi de concert.

2.9.2.2.Commentaires

Il s'agit-là de mesures à transposer dans le cadre d'un traité international sur le cyberespace. Ces mesures seraient la conséquence directe du principe général d'**utilisation pacifique du cyberespace**. Le non-respect de ces mesures constituerait un acte internationalement illicite.

En effet, selon l'article 2 du projet d'articles sur la responsabilité de l'Etat pour fait internationalement illicite[31] (Nations Unies), « il y a fait internationalement illicite de l'Etat lorsqu'un comportement consistant en une action ou une omission : est attribuable à l'Etat en vertu du droit international ; et constitue une violation d'une obligation internationale de l'Etat. »

2.9.3. La responsabilité de l'Etat négligeant

2.9.3.1.Sources

Traité de l'espace, art. 7 : « […] et tout État partie dont **le territoire ou les installations servent au lancement d'un objet**, est **responsable du point de vue international des dommages causés par ledit objet** *(négligeant, ou mettant délibérément ses infrastructures à disposition)* ou par ses éléments constitutifs, sur la Terre, dans l'atmosphère ou dans l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, à un autre État partie au Traité ou aux personnes physiques ou morales qui relèvent de cet autre État » (confirmé par l'article 1, § c), ii de la Convention responsabilité et dommages des objets spatiaux).

Exemple d'exclusion de responsabilité :

Convention responsabilité et dommages des objets spatiaux, article 6 : « Sous réserve des dispositions du paragraphe 2 du présent article, un État de lancement est exonéré de la responsabilité absolue dans la mesure où il établit que le dommage résulte, en totalité ou en partie, d'une faute lourde ou d'un acte ou d'une omission commis dans l'intention de provoquer un dommage, de la part d'un État demandeur ou des personnes physiques ou morales que ce dernier État représente. »

2.9.3.2.Problématiques adressées

Une telle disposition s'inscrirait dans le droit fil d'une volonté commune à l'échelle internationale de lutter contre les « Paradis numériques », ces Etats laxistes quant à l'existence d'une législation contre la cybercriminalité, sa mise en œuvre par des autorités judiciaires compétentes, ainsi que son application par les intermédiaires techniques sous sa juridiction (hébergeurs *bulletproof*).

Le respect et la mise en œuvre de diligences exonèreraient par présomption simple (donc contestable) l'Etat par lequel aurait transité une cyberattaque. A l'inverse, l'Etat laxiste se verrait sanctionné pour négligence caractérisée. Objectif de cette disposition : responsabiliser les Etats quant à l'hygiène informatique à tenir ; améliorer la cybersécurité à l'échelle internationale ; lutter contre les paradis numériques.

[31] Consultable : http://legal.un.org/ilc/texts/instruments/francais/commentaires/9_6_2001_francais.pdf

2.9.3.3.Exemples de transpositions

Le texte viendrait affirmer, dans un premier temps, une liste de diligences à laquelle devront s'astreindre les Etats signataires (disposer d'un régime juridique relatif à la lutte contre la cybercriminalité, encourager les entreprises et les particuliers à une « hygiène informatique », appliquer sévèrement les textes quant à la responsabilité des intermédiaires techniques…).

Il est en effet possible d'envisager un mécanisme supplétif de mise en œuvre de la responsabilité de l'Etat qui aura mis délibérément ou non, ses infrastructures à disposition d'un cyberattaquant. De telles dispositions sont citées dans l'article 7 du traité de l'espace.

Est visé l'Etat négligeant ayant contribué, par son manque de diligence ou parce qu'il met délibérément ses infrastructures à disposition, à la perpétration d'une cyberattaque.

2.10. Les dispositions de règlement des conflits et de prévention

2.10.1. Sources

Si la Cour internationale de justice (qui est « l'organe judiciaire principal des Nations unies » selon l'article 92 de la Charte des Nations unies) a normalement compétence générale pour les conflits juridiques entre Etats, la création du Tribunal International du droit de la mer (TIDM) empiète largement sur ses prérogatives. Le Tribunal instruit et juge les différends auxquels pourraient donner lieu l'interprétation et l'application de la Convention de Montego Bay. Son champ de compétence est complémentaire de celui de l'Autorité internationale des fonds marins, limitée, comme son nom l'indique, aux différends portant sur les fonds marins.

L'Organisation maritime internationale tient pour sa part un rôle préventif. C'est une institution spécifique des Nations unies dédiée à l'amélioration de la coopération entre Etats, l'adoption de norme, la prévention de la pollution en milieu marin, etc. Elle se compose de plusieurs sous-comités thématiques : sécurité marine, juridique, coopération technique, etc.

En droit de l'espace, les conflits se règlent soit par la voie diplomatique, soit par l'établissement d'une Commission de règlement des demandes[32]. Les conflits seront, sinon, réglés par la Cour internationale de justice.

2.10.2. Transposition

Le choix des institutions de règlement des conflits dépendra largement du véhicule juridique choisi par les Etats pour un droit du cyberespace.

Les Etats peuvent, en matière cyber, rédiger des clauses compromissoires indiquant que les litiges relatifs à tel ou tel accord bilatéral ou multilatéral seront réglés par la CIJ. Ils peuvent également soumettre tout

[32] Convention sur la responsabilité internationale pour les dommages causés par des objets spatiaux.

différend à la Cour, dans un mécanisme très proche de celui de l'arbitrage.

En cas d'adoption d'un traité international dans le cadre de l'Organisation des Nations Unies, un tribunal *ad hoc* pourra être créé. Il empiétera alors sur les compétences initiales de la CIJ.

Les Etats pourront, enfin, opter pour l'arbitrage.

La création d'une institution similaire à l'OMI composée de plusieurs sous-comités s'inscrirait dans le cadre d'une réforme en profondeur de la gouvernance Internet.

2.11. La gouvernance originale prévue par le droit de l'espace

En droit de l'espace, les organisations internationales ont un statut spécifique leur permettant d'adhérer à certaines dispositions, bien qu'elles soient excluent, *a priori*, les textes étant réservés aux Etats. En tant que « parties acceptantes », elles peuvent accepter les dispositions pertinentes à leur égard et devenir titulaires de droits et d'obligations vis-à-vis des autres parties au traité.

Ce modèle est intéressant en matière cyber : il est possible de s'en inspirer pour intégrer les autres acteurs et parties prenantes du cyberespace à la rédaction et l'adoption d'un traité international.

3ème partie : Recommandations

Des travaux réalisés, émergent quelques pistes juridiques.

1. Le cyberespace : un espace international coutumier

Le cyberespace dispose bien d'un caractère « international ». Selon A. de la Pradelle, l'espace international se définit comme un lieu de compétences concurrentes, « allergique » à la souveraineté qui est une compétence exclusive, de même qu'à l'appropriation privée. Cette définition évoque bien les caractéristiques et les problématiques relatives au cyberespace.

Pour être international, un espace a besoin d'un traité international qui le désigne comme tel. Si le cyberespace ne bénéficie pas encore d'un traité, il présente des caractéristiques en faisant un objet du droit international, de fait :

- Il n'y a pas de *dominium* étatique, l'appropriation exclusive du cyberespace étant impossible. Il est donc possible d'en déduire que le cyberspace n'est pas un espace national.[33]
- Mais il existe bien plusieurs *imperium*, c'est-à-dire des compétences territoriales et matérielles d'un côté, ou personnelles de l'autre. Le raisonnement par strates est ainsi applicable pour la couche physique et la couche des usages. Comme on le verra, cette compétence est juridictionnelle, mais a aussi un impact sur le champ de responsabilité pouvant en découler.

Le droit international étant un droit coutumier, il est possible de considérer le cyberespace comme un espace international coutumier.

2. Les conséquences de cette qualification sur les compétences juridictionnelles : vers une compétence rationae cyber ?

« A un droit international jusque-là très largement fondé sur des références territoriales (souveraineté, nationalisme maritime) ou rattachées à la territorialité (« la terre domine la mer »), est en train de se substituer un droit international qui trouve de plus en plus son fondement dans la prise en compte, imposée par une sorte de nécessité, du régime des activités humaines, quels que soient les lieux où celles-ci s'exercent. Ce phénomène est devenu dominant dans les secteurs concernés par les technologies de pointe, ou leurs conséquences : exploration et utilisations du cosmos, communications, pollutions etc. »

Lavenue J.-J., Observations sur l'évolution du droit international, p. 411

[33] Est-il possible de graduer, nuancer cette affirmation en distinguant au sein des infrastructures physiques les infrastructures plus ou moins indépendantes ?

2.1. La nécessité de créer des critères de compétence ex nihilo

Comme vu précédemment, des compétences d'ordre « matériel » ont été définies, *ex nihilo*, pour les Etats en droit de l'espace extra-atmosphérique par exemple. La question de l'immatriculation des objets lancés dans l'espace extra-atmosphérique fait d'ailleurs l'objet d'une convention éponyme.

Traité de l'espace, art. 8 : « L'État partie au Traité sur le registre duquel est inscrit un objet lancé dans l'espace extra-atmosphérique conservera sous sa juridiction et son contrôle ledit objet [...]. »

Ces modalités de définition de la compétence juridictionnelle ne sont pas naturelles, mais bien identifiées selon les spécificités des activités des Etats, et du milieu correspondant. C'est ainsi qu'en droit de la mer, chaque navire est associé à un pavillon (nationalité). L'Etat du pavillon peut exercer un contrôle sur le navire à tout moment (art. 92 à 94). Il y a également juridiction exclusive.

2.2. La question de l'extraterritorialité

Le principe de droit international public d'extraterritorialité revient pour un pays à laisser s'exercer l'autorité d'un Etat étranger ou d'une organisation internationale sur une partie de son territoire propre. Contrairement à une idée reçue, les ambassades ne bénéficient d'ailleurs pas de ce statut mais simplement d'une immunité diplomatique. Par extension, l'extraterritorialité permet aux navires d'être considérés, en matière de droit applicable, comme relevant de leur territoire d'origine dès lors qu'ils se trouvent dans les eaux internationales.

La difficulté dans la sphère numérique est l'ubiquité des données stockées dans le cloud. Les données sont alors impossibles à localiser, ce qui constitue un « redoutable obstacle à la répartition des compétences entre les différents systèmes de droit simultanément applicables »[34]. Le principe général est que la liberté contractuelle prime : c'est donc la loi des parties qui prévaut. Celles-ci peuvent choisir la juridiction compétente et le droit applicable qui régiront en totalité ou en partie leurs rapports.

Au sein de l'Union européenne, deux règlements, dits Rome I et Bruxelles I, fixent le cadre des conflits de loi lorsque les parties n'en décident pas elles-mêmes.

- Le règlement Bruxelles I pose comme principe, susceptible de dérogations, que la juridiction compétente est celle de l'Etat membre dans lequel le défendeur a son domicile, quelle que soit sa nationalité.
- Le règlement Rome I, pour sa part, fixe comme droit applicable, à défaut de choix des parties, la loi du pays dans lequel le prestataire a sa résidence habituelle.

A l'exception des dispositions contractuelles, aucune disposition n'existe cependant pour le traitement, la conservation et la protection de la confidentialité des informations stockées dans le Cloud. Or l'on sait que la relation avec les prestataires de Cloud est en général asymétrique et se traduit généralement par l'adhésion à des contrats standards, en ligne, qui excluent toute possibilité pour le client de modifier les dispositions contractuelles prévues.

[34] Colloque « Le cloud computing », http://www.cil.cnrs.fr/CIL/IMG/pdf/cloud_computing_11_octobre_2013_181013.pdf

A l'instar des navires en haute mer, il serait donc intéressant d'envisager une sorte d'extraterritorialité : les données, lorsqu'elles se trouvent en dehors du territoire national, qu'elles soient en transit, ou qu'elles y soient stockées, seraient soumises à la législation du pays émetteur, à défaut de dispositions contractuelles contraires.

Il convient enfin d'éviter toute disposition obligeant systématiquement à une relocalisation des données, à l'exception de données particulièrement sensibles. Une telle disposition, si elle peut avoir des avantages au plan de la régulation économique et d'une politique industrielle en faveur du développement d'une offre nationale, ne peut constituer une solution sur le long terme. Il s'agirait-là d'un des premiers jalons de la construction d'une compétence spécifique à la problématique cyber.

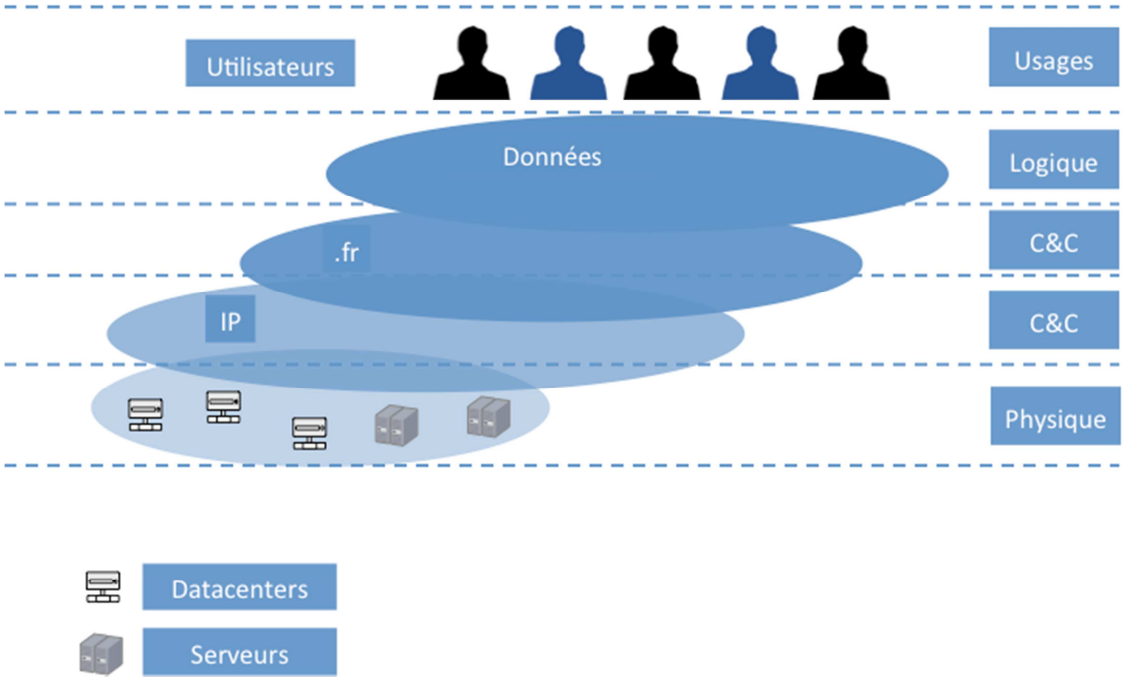
2.3. Une compétence *rationae cyber*

Transposer le mécanisme de compétence matérielle pour le cyberespace impliquerait la création de critères pouvant être qualifiés de ***rationae « cyber »***. Il s'agit de critères de compétence « embarquée », liés à des fonctions, objets ou données propres au mécanisme d'Internet sur lesquels l'Etat pourrait exercer *légitimement* sa compétence. Ce nouveau « champ de compétence cyber » implique par exemple de faire de l'adresse IP, du nom de domaine et du DNS, des critères de compétence à part entière.

Théoriquement, ces compétences sont chacune exclusives et aisément identifiables. A titre d'exemple, l'Etat français dispose d'une compétence de type *ratione personae*[35] (liée aux utilisateurs d'Internet concernés). Mais on peut également considérer que l'Etat français dispose d'une compétence sur l'extension .fr. Il est également possible de reconnaître une compétence sur une plage d'adresses IP, dès lors que celle-ci est attribuée géographiquement. Enfin, l'Etat français dispose d'une compétence pleine et entière sur les infrastructures physiques présentes sur son territoire (*ratione loci*).

Ce « système » à part entière de compétences est à préciser et à définir entre Etats.

[35] Compétence personnelle de certaines juridictions de connaître des infractions suivant la qualité personnelle du délinquant.

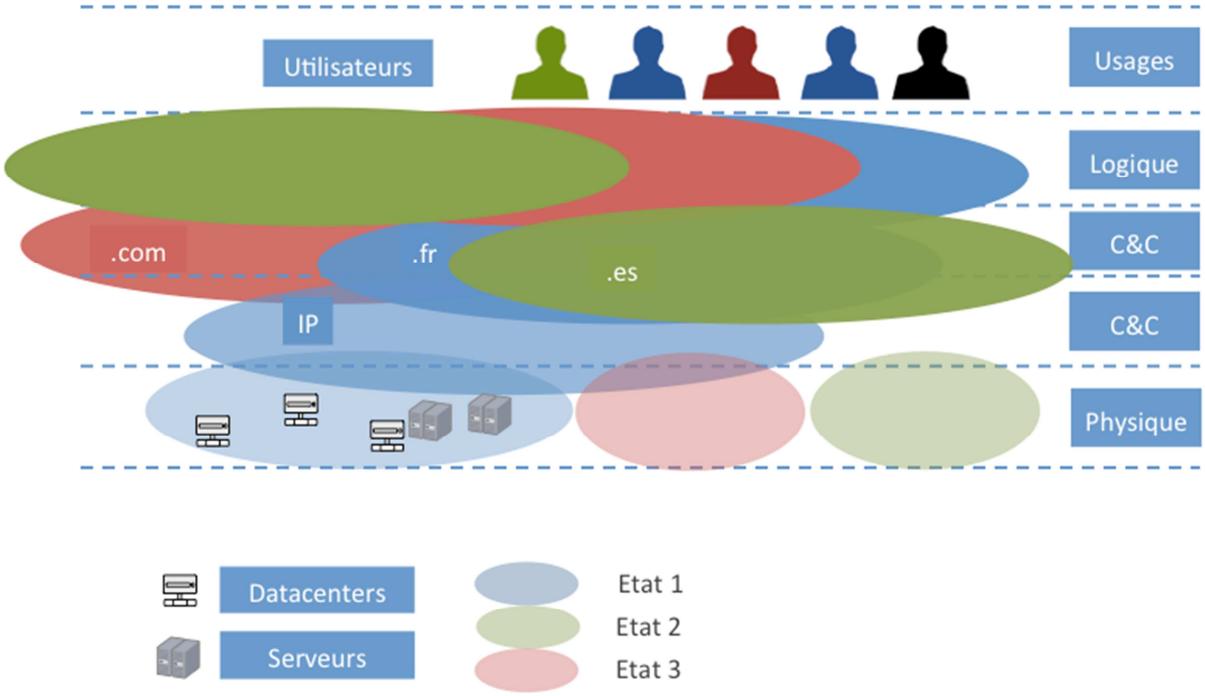


Champ de compétence d'un Etat sur Internet

A ce faisceau de compétences « cyber » peut s'ajouter le critère de l'entreprise de service. Ce critère correspond en réalité au contrat liant une entreprise de service sur Internet à un Internaute.

Si ces critères sont, pris un à un, exclusifs, ils restent pourtant concurrents de ceux des autres Etats en raison d'une superposition permanente de ces fonctionnalités en raison du fonctionnement même d'Internet. Ce qui entraîne une superposition des compétences juridictionnelles. A l'image des espaces maritimes : la compétence d'un Etat n'est pas exclusivement territoriale, et dans le même espace, plusieurs compétences peuvent s'exercer[36].

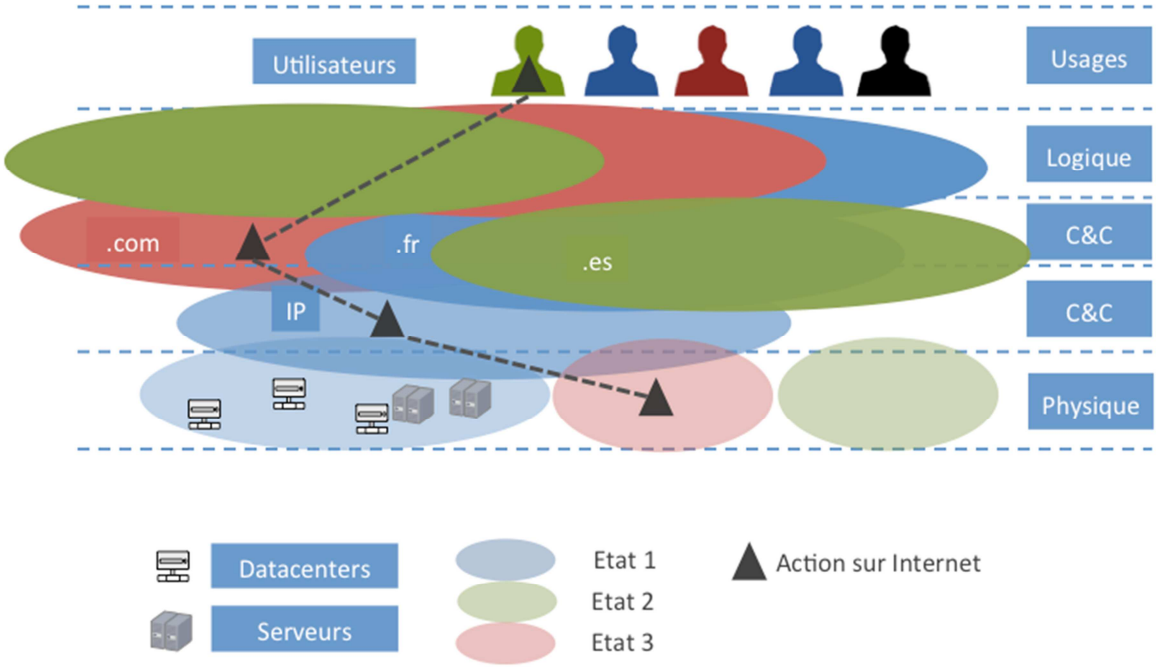
[36] Lavenue J. http://rbdi.bruylant.be/public/modele/rbdi/content/files/RBDI%201996/RBDI%201996-2/Etudes/RBDI%201996.2%20-%20pp.%20409%20%C3%A0%20452%20-%20Jean-Jacques%20Lavenue.pdf



Superposition des champs de compétence de plusieurs Etats sur Internet

Ces développements rejoignent la problématique de l'infraction plurilocalisée. La situation n'est donc pas nouvelle. Exemple : une infraction réalisée par un individu de nationalité A dans un Etat C, et son complice, un individu de nationalité B logeant dans un Etat D, ayant des conséquences dans les Etats E, F et G. Les compétences sont toutes propres aux Etats listés. Tous peuvent invoquer leur compétence juridictionnelle *rationae personae, materiae* ou *loci*. Des mécanismes de coopération existent (extraditions, commissions rogatoires internationales, etc.).

Ces développements, adaptés à la matière cyber, donneraient l'exemple suivant : un individu de nationalité A, résidant dans un Etat B, commet une infraction sur un site d'extension gérée par un Etat C (.c), utilisant l'adresse IP d'un autonomous system localisé dans un Etat D, passant par un serveur localisé dans l'Etat E. Ici, les Etats A à E sont tous compétents, selon des critères nouveaux que sont la plage d'adresse IP et l'extension du nom de domaine.



Représentation d'une action sur Internet, plurilocalisée en ce qu'elle s'éparpille sur les différentes couches du cyberespace

Les critères *ratione cyber* viendraient compléter et systématiser les critères déjà identifiés par la jurisprudence :

- *Ratione loci* (localisation des serveurs ou datacenters) ;
- Les dispositions contractuelles ;
- *Ratione personae* (données à caractère personnel).

Une question subsiste, celle de la compétence des Etats sur les données. Si les données à caractère personnel bénéficient déjà d'un tel dispositif, force est de constater que le système mériterait d'être élargi. Quid, en effet, du cas des données rattachées à une entreprise ? Ces données, bien que n'étant pas « à caractère personnel », peuvent déclencher la compétence de l'Etat de la nationalité de leur titulaire.

Fonder un critère de compétence juridictionnelle sur un paquet de données implique de pouvoir taguer, ou identifier ce paquet, à l'image d'une immatriculation. Cette immatriculation devrait être fiable, attribuée par un processus reconnu par les Etats. Ce système s'éloigne du fonctionnement même d'Internet. Il s'agirait donc, comme évoqué ci-dessus, de consacrer une compétence relative au pays de l'émetteur des données, par défaut.

Les développements ci-dessus consacrent l'existence d'un *imperium* étatique. A l'image de la Haute mer, où les Etats peuvent exercer leurs compétences sans pour autant pouvoir y clamer une quelconque souveraineté, l'Etat reste compétent dans le cyberespace, sans bénéficier d'une exclusivité. Qualifier le cyberespace d'entité ou d'espace international n'annule donc pas la compétence étatique. Il souligne simplement la coexistence et la concurrence de ces compétences, consacrant une approche **fonctionnelle** de ces compétences.

Selon Daillier et Pellet, le régime des espaces est la juxtaposition de régimes juridiques très divers. Ces régimes vont, par une **approche fonctionnelle (et non territoriale) de la souveraineté**, organiser, *en les limitant,* les compétences étatiques pouvant s'y exercer.

Ce système a pour conséquence directe de reconnaître aux Etats une souveraineté sur les différents critères énoncés (noms de domaine, etc.). Les débats animant la question du pouvoir des Etats sur leur extension Internet, par exemple, sont à cet égard essentiels. Une réforme en ce sens impliquerait donc de concéder aux Etats le plein pouvoir sur leurs noms de domaine, tout en les responsabilisant à ce sujet. Les Etats seraient alors contraints de mieux contrôler leurs noms de domaine.

Une telle réforme va dans le sens des efforts déjà initiés par l'ICANN, afin de rapprocher les populations et les Etats de la gestion de leurs noms de domaine par la création de bureaux locaux.

3. La préservation du milieu par la sanctuarisation de certaines infrastructures critiques

Le réseau fonctionne grâce à quelques ressources clés que sont :

- Le système de routage : les routeurs de bordure d'AS et le protocole BGP
- Le système de transport de paquets : MPLS et IP
- Le système DNS : serveurs racine et réplications Anycast.

Les opérateurs publics ou privés gérant ces ressources devraient également être soumis à un ensemble de règles de sécurité, comme le sont les opérateurs d'installations portuaire au titre du code ISPS. Ces opérateurs ont en effet obligation de définir un plan de sûreté recensant les moyens de sécurité mis en place. Un agrément est ensuite délivré en France pour les installations portuaires.

Un opérateur non « habilité » ne pourrait donc pas se connecter au réseau et verrait donc ses activités décliner rapidement.

3.1. La criticité de certaines infrastructures physiques

La protection des infrastructures physiques, équipements réseau, points d'échange internet et datacenterd, est également importante. Là aussi, les opérateurs devraient être tenus de respecter le code de bonne conduite et recevoir un agrément sur présentation de leur politique de sécurité. L'auditabilité de leur dispositif serait également imposée.

L'architecture d'Internet trouve son fondement dans quelques infrastructures physiques clés. Ces infrastructures physiques permettent aux fournisseurs d'accès à Internet et autres opérateurs de se connecter au réseau et d'accéder à Internet. S'il est communément admis que la suppression ou l'altération d'un élément du cyberespace ne suffit pas à « casser Internet », il est toutefois possible de déconnecter des zones géographiques entières en s'attaquant à des points clés de l'infrastructure physique d'Internet. L'un de ces points clé est le « Point d'échange Internet ». Le point d'échange Internet (ou Internet eXchange Point) est une infrastructure physique permettant aux différents fournisseurs d'accès Internet d'échanger du trafic Internet entre leurs *autonomous systems* grâce à des accords mutuels dits de *peering*.

Ces points d'échange Internet sont gérés par des prestataires de service Internet.

3.2. Le fondement juridique de l'aménagement de la propriété privée

C'est ici qu'intervient l'un des apports principaux de l'analogie entre les droits de la mer, de l'espace et le cyberespace.

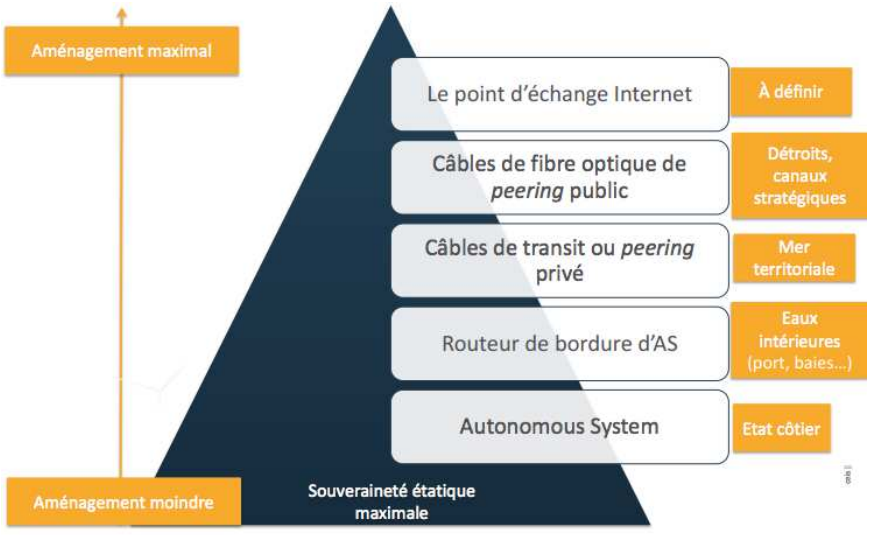
La question de la souveraineté est facilement délimitée en droit de l'Espace, entre les corps célestes et les objets spatiaux. C'est ainsi que l'article 12 de l'Accord régissant les activités des États sur la Lune et les autres corps célestes de dispose que « les États parties conservent la juridiction ou le contrôle sur leur personnel, ainsi que sur leurs véhicules, matériel, stations, installations et équipements spatiaux se trouvant sur la Lune » et que « la présence sur la Lune desdits véhicules, matériel, stations, installations et équipements ne modifie pas les droits de propriété les concernant », l'article 11 du même accord précise bien que « la Lune ne peut faire l'objet d'aucune appropriation nationale par proclamation de souveraineté, ni par voie d'utilisation ou d'occupation, ni par aucun autre moyen. »

La question est bien plus complexe en droit maritime, véritable droit « des » espaces maritimes. Dans les deux cas toutefois, la question de la non-appropriation n'est pas traitée de façon uniforme : c'est un véritable aménagement de la souveraineté qui est prévu, aménagement dont peu s'inspirer un droit du cyberespace.

Il est possible d'envisager une transposition de cet aménagement en se fondant, non sur la proximité ou l'éloignement de l'infrastructure avec la frontière ou côte d'un Etat, mais sur le caractère plus ou moins stratégique de l'infrastructure au sein du réseau, et la dépendance plus ou moins importante des autres Etats à son égard.

Ainsi, plus une infrastructure est importante pour le bon fonctionnement du réseau, et plus il y a d'Etats dépendants de cette infrastructure pour leur connexion Internet, plus cette infrastructure peut faire l'objet d'une propriété privée aménagée d'un côté, et d'une souveraineté aménagée de l'autre.

Ce régime juridique peut être reproduit pour toutes les infrastructures physiques : la gestion des câbles transocéaniques, les équipements réseau et datacenter.



Exemple d'analogie

La propriété privée pourra être encadrée par un système à la délégation de service public. La souveraineté étatique le sera par la création de « communauté de droits et d'intérêts des Etats riverains ».

3.3. La responsabilisation de leurs opérateurs par l'encadrement sur le modèle de la délégation de service public

La gestion de ces points d'échange est une activité d'intérêt général. Un traité international devrait, pour préserver la sécurité de ces infrastructures, s'assurer de : la continuité du service, la non-discrimination dans l'accès à ce service, la primauté de l'intérêt collectif en cas de travaux, etc. Autant de principes évoquant la notion de service public (l'analogie avec les droits de la mer et de l'espace n'ayant pas donné satisfaction en l'espèce).

Une transposition partielle et choisie du régime juridique de la délégation de service public permettrait d'encadrer et de valoriser la mission des prestataires gérant les points d'échange Internet.

En France, le service public repose sur trois principes :

- La continuité. Ce principe impose que le service soit assuré régulièrement, sans retard et sans discontinuité gênante pour l'usager. Ce principe peut être rapproché de la notion de résilience des infrastructures critiques d'Internet.
- La mutabilité. Ce principe rappelle la nécessaire adaptation des services publics à l'évolution des besoins collectifs et aux exigences de l'intérêt général. Un tel principe pourrait être transposé dans un traité global du cyberespace. Objectif : rappeler au prestataire gérant l'infrastructure que celle-ci doit évoluer continuellement.
- L'égalité. Ce principe souligne l'importance de l'égal accès, de l'absence de discrimination dans l'accès des usagers à un service.

Ces trois principes peuvent constituer les bases d'un régime juridique contraignant, mais aussi valorisant, de gestion d'infrastructure critiques d'Internet. A ces principes, doivent être rajoutés d'autres éléments tels que la sécurité (physique et logique). La sécurité de ces infrastructures critiques devant être encadrée selon l'état de l'art.

Assimilés à des délégataires d'une prestation de service public, les entreprises telles que Telehouse seraient à la fois contraintes, mais aussi aidées dans la gestion de ces infrastructures. L'Etat accueillant le point d'échange Internet serait, lui aussi, responsable de la bonne exécution de ces principes.

3.4. L'aménagement de l'exercice des compétences étatiques au sein d'une « communauté de droits et d'intérêt »

L'aménagement des compétences étatiques pouvant s'exercer dans le cyberespace peut se raccrocher à une analogie entre droit maritime et cyberespace et, plus précisément, entre fleuve et routes ou carrefours stratégiques d'Internet. Un fleuve est un cours d'eau traversant plusieurs Etats. Ces Etats bénéficient d'une

souveraineté indiscutable sur leur territoire. Mais ils partagent ce fleuve et peuvent, par exemple, exploiter l'eau à diverses fins plus ou moins critiques d'approvisionnement en eau potable, de génération d'électricité, etc. Le fleuve possède sa propre réalité et « suit son cours », sans se préoccuper des frontières souveraines des Etats. C'est ainsi qu'une action d'un Etat sur le fleuve (l'assèchement d'un fleuve en amont) a des répercussions importantes sur le reste du fleuve, notamment hors des frontières de l'Etat en question (en aval). L'analogie est ici très pertinente avec les « routes » et « carrefours » d'Internet que sont les infrastructures physiques suivantes : points d'échange Internet, câbles, etc. L'Etat disposant d'un point d'échange Internet sur son territoire devrait, en théorie, pouvoir agir à sa guise sur de point d'échange. Or, toute destruction ou tout débranchement aurait un impact critique sur tous les Etats « en aval » du point d'échange Internet, les privant d'une connexion peut-être indispensable pour leur économie et leu administration. La comparaison avec le droit international fluvial basée sur la distinction entre Etat d'amont et Etat d'aval souligne une véritable interdépendance des Etats (cf. affaire du Lac Laroux[37]).

En somme, les ramifications hors du territoire national d'un fleuve présent sur ce territoire national, permettent une limitation de la souveraineté. Les fleuves internationaux sont régis par des « communauté de droits et d'intérêts des Etats riverains ». Un régime juridique pouvant être transposé au cyberespace.

> *« Le droit international fluvial repose actuellement, tant en ce qui concerne la navigation que les autres utilisations, sur des conventions particulières très nombreuses, tantôt bilatérales, tantôt multilatérales, concernant des fleuves et cours d'eau déterminés, tandis que le contenu du droit général en ce domaine est devenu extrêmement limité.*
>
> *Comme d'autres branches du droit international, le droit fluvial est aujourd'hui caractérisé par la prédominance du droit conventionnel résultant de traités et d'accords spéciaux, sur le droit coutumier général, et, en conséquence, par la diversité des situations juridiques fondées sur ces traités et accords spéciaux. »*
>
> Hubert THIERRY,
>
> Professeur à l'université de Paris-X, « Les fleuves internationaux, objets de droit »

Les conséquences d'un tel dispositif peuvent être majeures :

- Sur le règlement des conflits : cela permettra de mettre en œuvre des processus de négociations et d'arbitrage ;
- Sur la protection de certaines infrastructures critiques (Etat hôte équivalant à l'Etat d'amont du fleuve, et l'Etat transitant par cette infrastructure étant l'Etat d'aval du fleuve). Si l'Etat d'amont bénéficie d'une pleine souveraineté sur l'infrastructure physique présente sur son territoire, l'Etat d'aval doit bénéficier d'un droit de regard si cela touche ses intérêts nationaux.

Cette communauté d'intérêt peut donc être reprise en matière de gouvernance du cyberespace et, plus précisément, à des fins d'aménagement de l'exercice des compétences étatiques sur Internet.

La notion d'Etat « voisin » sur Internet

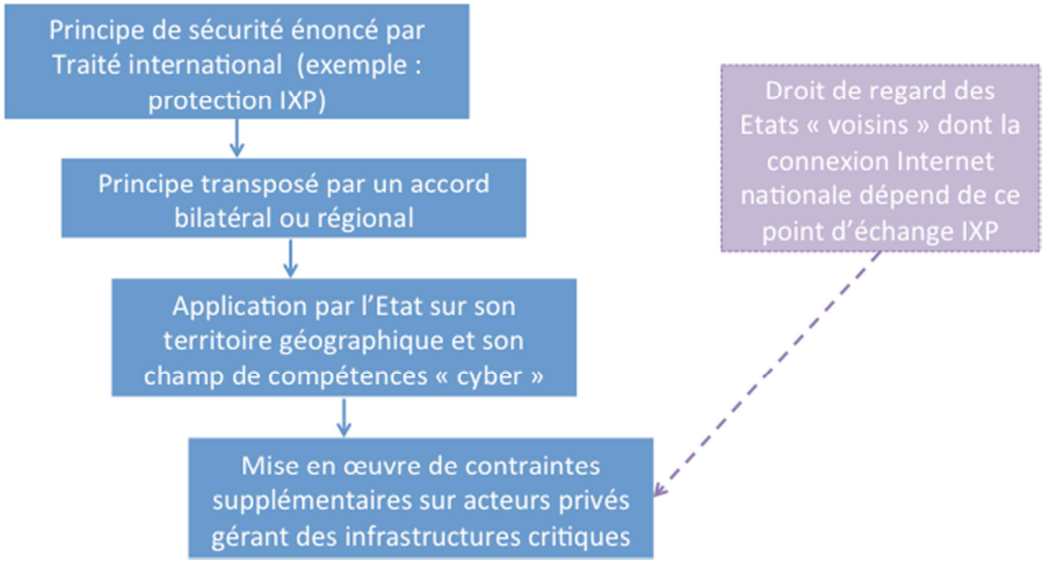
Sur Internet, la notion de proximité de deux Etats ne se décide plus selon la distance les séparant, mais selon des règles nouvelles encadrant le déplacement des données sur Internet. Ainsi, un Etat A, même s'il est

[37] Références jurisprudentielles évoquées dans : « Les aspects internationaux des contrats conclus et exécutés dans l'espace virtuel», sous la direction du Prof. P. Mayer, Université de Paris I Panthéon-Sorbonne, 2001

éloigné géographiquement, pourra être considéré comme plus « proche » sur le réseau d'un Etat B, en raison d'une meilleure connectivité reliant ces deux Etats.

Les critères de définition de ce « voisinage » pourraient être le partage de l'usage d'infrastructures critiques d'Internet telles que les points d'échange Internet, ou des data centers. L'existence d'accords de *peering* privé constituant un critère de proximité majeur.

A l'image de l'Etat « aval » d'un fleuve, bénéficiant d'un droit de regard sur les activités de l'Etat « amont » sur le fleuve (en dépit de la souveraineté territoriale pleine et entière exercée par l'Etat amont), les Etats « voisins » sur Internet peuvent constituer des communautés d'intérêt, et bénéficier d'un droit de regard sur les activités d'un Etat gérant, par exemple, un point d'échange Internet sur son territoire.



Mécanisme de mise en œuvre du dispositif présenté

Ce mécanisme implique l'existence d'un traité ou accord international constituant le fondement juridique d'obligations nouvelles, et consacrant la dimension internationale du cyberespace. Ces obligations peuvent être transposées au sein d'instruments juridiques régionaux ou locaux, afin de s'assurer de leur application. La ratification de ces instruments juridiques implique le respect des dispositions par l'Etat, et le possible engagement de sa responsabilité par les autres Etats signataires et/ou « voisins ». Enfin, l'Etat bénéficie ici de moyens d'action supplémentaires, contraignant les consortiums et acteurs gérant aujourd'hui des infrastructures critiques d'Internet.

3.5. Quelles sanctions ?

3.5.1. La réparation[38]

Le doit de l'espace envisage un mécanisme intéressant d'indemnisation de la victime d'un dommage collatéral.

Convention responsabilité et dommages des objets spatiaux, article 2 : « Un État de lancement a la responsabilité absolue de verser réparation pour le dommage causé par son objet spatial à la surface de la Terre ou aux aéronefs en vol. »

Aussi, à l'inverse, « Un État qui subit un dommage ou dont des personnes physiques ou morales subissent un dommage peut présenter à un État de lancement une demande en réparation pour ledit dommage » (Convention responsabilité et dommages des objets spatiaux, art. 8 § 1). L'Etat peut également demander réparation au nom de son ressortissant ayant été victime des dommages en question (Convention responsabilité et dommages des objets spatiaux, art. 8 § 2).

De plus, « la présentation d'une demande en réparation à l'État de lancement en vertu de la présente Convention n'exige pas l'épuisement préalable des recours internes qui seraient ouverts à l'État demandeur ou aux personnes physiques ou morales dont il représente les intérêts. »[39]

Il reconnaît également la difficile évaluation de l'étendue des dommages. Ce qui n'est pas sans rappeler la difficulté que les acteurs ont aujourd'hui à évaluer l'étendue des dommages engendrés par une cyberattaque.

Convention responsabilité et dommages des objets spatiaux, article 10, § 3 : « Les délais précisés aux paragraphes 1 et 2 du présent article s'appliquent même si l'étendue du dommage n'est pas exactement connue. En pareil cas, toutefois, l'État demandeur a le droit de réviser sa demande et de présenter des pièces additionnelles au-delà du délai précisé, jusqu'à expiration d'un délai d'un an à compter du moment où l'étendue du dommage est exactement connue. »

Convention responsabilité et dommages des objets spatiaux, article 12 : « Le montant de la réparation que l'État de lancement sera tenu de payer pour le dommage en application de la présente Convention sera déterminé conformément au droit international et aux principes de justice et d'équité, de telle manière que la réparation pour le dommage soit de nature à rétablir la personne, physique ou morale, l'État ou l'organisation internationale demandeur dans la situation qui aurait existé si le dommage ne s'était pas produit. »

3.5.2. L'embargo numérique

Contrairement au blocus, mesure par laquelle un belligérant déclare l'interdiction de communication, par entrée ou par sortie, entre la haute mer et le littoral ennemi, qui est un acte de guerre, l'embargo est considéré comme un « acte inamical » lorsqu'il est décidé unilatéralement par un pays. Il peut néanmoins être décidé par la communauté internationale, via le Conseil de sécurité. Un comité de sanction est alors mis

[38] Consulter : Thierry Autret (Col RC) et Florence Esselin (Clc RC), « Prendre la mesure des cyberattaques : peut-on définir une échelle de Richter dans le Cyber ? »
[39] Convention responsabilité et dommages des objets spatiaux, article 11, § 1.

en place pour délivrer d'éventuelles exemptions en fonction du caractère de la transaction et des biens concernés.

Article 41 de la charte des Nations unies

« Le Conseil de sécurité peut décider quelles mesures n'impliquant pas l'emploi de la force armée doivent être prises pour donner effet à ses décisions, et peut inviter les membres des Nations unies à appliquer ces mesures. Celles-ci peuvent comprendre l'interruption complète ou partielle des relations économiques et des communications ferroviaires, maritimes, aériennes, postales et des autres moyens de communication, ainsi que la rupture des relations diplomatiques. »

S'il est théoriquement possible, dans le cadre de sanctions économiques et financières décidées par les Nations Unies d'imaginer un embargo affectant les communications numériques, une telle mesure semble dans la pratique peu probable et peu efficace :

- En 2012, les 47 membres du Conseil des droits de l'Homme de l'ONU, dont la Chine et Cuba, ont adopté à l'unanimité une résolution stipulant que l'accès à Internet était un droit fondamental, au même titre que les droits de l'Homme.

- Elle est techniquement compliquée à mettre en œuvre compte tenu de l'architecture d'internet et de la multiplicité des acteurs. La meilleure solution reste la technique utilisée par l'Egypte qui a en 2011 demandé à ses fournisseurs d'accès de supprimer toutes les routes BGP vers le pays. Les réseaux égyptiens sont alors devenus injoignables pour le reste du monde.

Notons d'ailleurs que c'est en général la situation inverse qui s'est produite quand des gouvernements autoritaires décident, avec plus ou moins de succès, de supprimer toute communication entre le réseau local et le reste du monde.

Soulignons enfin que le système DNS intègre déjà un mécanisme de sanction puissant avec le refus d'un nom de domaine.

Seules des mesures très ciblées semblent donc possibles.

3.5.3. Le bannissement des instances de gouvernance

Il est enfin possible d'envisager, à titre de sanction, le bannissement – même temporaire – de certains Etats réfractaires, des instances internationales de gouvernance Internet.

4. La *soft law* comme véhicule juridique consensuel pour un droit du cyberespace

4.1. L'option du traité international

Un traité international sur le cyberespace parait être, sur le fond, le meilleur véhicule juridique. Le processus d'adoption prendrait toutefois du temps et consisterait dans un premier temps à identifier un ensemble de principes généraux constituant le plus petit dénominateur commun acceptable par les Etats.

La convention de Montego Bay de 1982 est un bon exemple de cette approche progressive. Les travaux ont pris plus de 20 ans (de 1958 à 1982), mais le texte est aujourd'hui largement ratifié (seuls 17 pays n'ont pas signé le texte et 20 pays ne l'ont toujours pas ratifié, dont les Etats-Unis) et appliqué par la quasi-totalité des Etats.

La position des Etats-Unis mérite d'être soulignée : malgré le soutien de l'administration américaine, la ratification a plusieurs fois échoué au Sénat en raison de l'hostilité de certains parlementaires qui y voient une menace pour la souveraineté territoriale des Etats-Unis et critiquent, à l'instar de John Bolton, ancien ambassadeur américain à l'ONU, la manipulation que ferait la Chine de la Convention afin d'exclure la marine de guerre américaine de la Mer de Chine méridionale. Le Department of Defense milite aujourd'hui pour sa ratification, souhaitant faire valoir les prétentions des Etats-Unis sur certaines zones se situant au large de l'Alaska à la suite de la ratification du texte par la Russie en 1997.

Cette convention cadre en matière cyber pourrait être assortie d'accords régionaux et bilatéraux.

Mais force est de constater que obstacles sont aujourd'hui trop nombreux pour espérer à court terme un tel traité. Le processus peut toutefois être engagé, en complément des initiatives[40] de *soft law,* les transformations en résultant étant toutes aussi majeures que le texte pouvant en découler.

4.2. Des freins trop nombreux à l'adoption d'un traité

4.2.1. Des évolutions juridiques tributaires des évolutions technologiques ?

4.2.1.1.La mutation et la convergence des réseaux

Le business des opérateurs de télécommunication repose sur la commercialisation de services de télécommunication. La plate-forme de production de ces services est globalement constituée de deux composantes : le réseau et le système d'information technique et commercial. Le « réseau » d'un opérateur consiste en un ensemble de sous-réseaux (réseau de transmission, réseau de commutation, réseau d'accès, réseau de signalisation, réseau intelligent, réseau de gestion), chacun ayant une fonction particulière dans le but de fournir un service au client.

Avec l'évolution des réseaux vers IP, le réseau de commutation de circuit migre petit à petit vers une nouvelle architecture appelée NGN (Next Generation Network). Cette dernière émule le comportement du réseau de commutation de circuit. Avec l'avènement des accès large bande, le réseau cœur évolué vers l'architecture IMS (IP Multimedia Sub System) qui fournit des services multimédia (téléphonie sur IP, IPTV, Présence, messagerie instantanée, etc.).

Cette convergence des réseaux vers le tout-IP aurait à terme un impact direct sur la gouvernance. L'UIT, chargée des télécommunications, verrait la fonction « téléphonie » se fondre purement et simplement sur

[40] Le label en cours de création Cloud confidence est un exemple d'initiative française en matière de soft law. Il propose une certification volontaire permettant de s'assurer que les offreurs IaaS (fourniture d'infrastructures de calcul et de stockage en ligne), PaaS (fourniture d'une plateforme de développement d'applications en ligne) et SaaS (fourniture de logiciel en ligne) respectent un certain nombre de points dans leurs conditions générales de vente. Objectif : Mettre à disposition des prestataires Cloud et des utilisateurs, un cadre de transparence centré sur la protection, la confidentialité, la sécurité des données et actifs immatériels hébergés. Cette initiative s'appuie sur la législation européenne, législation appelée à évoluer à moyen terme. Aujourd'hui, une dizaine d'offreurs installés en France et à l'étranger ont démarré le processus de certification.

Internet, via la VOIP. Cette mutation serait-elle annonciatrice d'une diminution du rôle, déjà contesté, de l'Union internationale des télécommunications (UIT) ?

4.2.2. La gouvernance Internet et la logique de blocs qui soulignent l'absence de consensus

L'approche Top-Down est celle privilégiée par les Etats qui souhaitent avoir un rôle plus important que les autres acteurs, voire être les seuls acteurs à même de prendre des décisions dans le futur modèle de gouvernance. Ce modèle propose une approche hiérarchique de la gouvernance, avec les Etats qui sont les seuls à même de prendre des décisions. L'approche Bottom-Up est au contraire le reflet d'une approche multi-acteurs de la gouvernance d'Internet, dans laquelle les Etats sont des acteurs parmi d'autres. Ces deux approches sont les deux extrêmes du débat actuel sur l'avenir de la gouvernance d'Internet. Elles constituent deux « blocs » de pays opposés dans leur conception du modèle à adopter. Même au sein des deux « blocs », les Etats ne partagent pas les mêmes conceptions sur le rôle que chaque acteur doit jouer, comme le soulignent les différentes variantes existantes de chaque approche. Ensuite, la manière dont les Etats discutent de l'avenir de la gouvernance d'Internet au sein des forums organisés par l'Union Internationale des Télécommunications (UIT) relève souvent d'une approche Top-Down, excluant les autres acteurs du processus de décision qui pourrait les concerner dans le futur. Cette critique a été formulée par les autres groupes d'acteurs qui reprochent aux Etats pourtant partisans d'une approche « Bottom-up » de la gouvernance de ne pas appliquer l'approche qu'ils défendent. Au contraire, les Etats en faveur de l'approche Top-Down tels que la Chine et la Russie tendent à ne reconnaître que les décisions prises dans des instances multilatérales et non dans des forums multi-acteurs, en cohérence avec leur approche de la gouvernance.

Cette logique de blocs souligne l'état actuel des discussions entre acteurs de la gouvernance Internet. L'absence de consensus la caractérisant rend illusoire l'adoption d'un traité sous le modèle des traités de l'espace ou de la convention de Montego Bay.

4.3. L'exemple structurant du code ISPS

4.3.1. Source

Le Code international pour la sûreté des navires et des installations portuaires[41] a été adopté le 12 décembre 2002 dans le cadre de la convention Solas (1974) (Convention internationale pour la sauvegarde de la vie humaine en mer).

4.3.2. Problématiques adressées

La transposition du texte et l'adoption d'un support juridique similaire adressent les problématiques suivantes :

- trouver un vecteur juridique pouvant déclencher le consensus ;

[41] International Ship & Port Facility Code - Code International pour la Sûreté des Navires et des Installations Portuaires, adopté le 12 décembre 2002 par la résolution 2 de la Conférence des gouvernements contractants à la Convention internationale pour la sauvegarde de la vie humaine en mer (Solas), de 1974.

- adresser les problèmes de sécurité et de stabilité internationale en matière cyber.

4.3.3. Transposition

Trouver un vecteur juridique pouvant déclencher le consensus : Il s'agit-là d'un vecteur juridique original, pouvant être exploité en matière de cybersécurité. La logique de blocs, l'absence de consensus et la rigidité actuelle de la gouvernance d'Internet freinent l'adoption à court et moyen termes d'une convention obligeante par les Etats.

Un code émergeant de l'initiative de plusieurs Etats, adopté sous le modèle du Code ISPS permettrait de rassembler le consensus nécessaire en accordant une importante liberté aux Etats signataires. La subdivision du code en une partie contraignante et une autre de simples recommandations permettrait aux Etats d'intégrer certaines dispositions sous un modèle de « *soft law* ».

Adresser les problèmes de sécurité et de stabilité internationale en matière cyber : le code ISPS présente la caractéristique de ne s'appliquer qu'à une matière précise : la lutte contre le terrorisme. Le code ne s'applique donc pas à la sécurité maritime. Il s'agit d'une piste supplémentaire dont un droit du cyberespace pourrait s'inspirer : conclure des accords sur des matières délimitées, afin de maximiser les chances d'adhésion des différents Etats.

Enfin, les mesures préconisées par le code ISPS semble facilement adaptables à la problématique « cyber » : évaluation des risques, un partage d'informations, la nomination d'un « agent de sûreté (Company Security Officer), la production d'un plan de sûreté, la préconisation d'exercices et de formation, etc. Autant de termes qui e rapprochent sémantiquement du champ lexical de la cybersécurité.

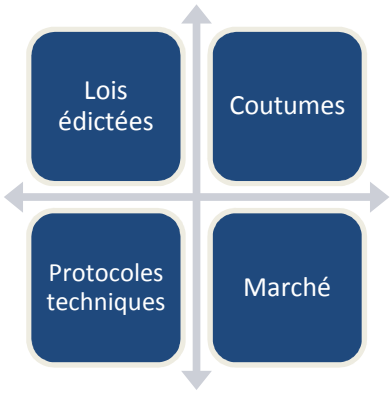
4.3.4. Commentaires

Suite aux attentats du 11 septembre 2001, la prise de conscience de la vulnérabilité des navires face aux attaques terroristes a suscité la volonté d'établir une procédure internationale sur la sûreté des installations portuaires et des navires. Les navires ont en effet un accès relativement aisé aux installations portuaires Plusieurs scénarios ont été envisagés notamment que le navire serve à transporter des terroristes, ou qu'il soit lui-même utilisé comme arme par destination.

Le code ISPS n'est obligatoire que pour les Etats décidant d'adhérer à la convention Solas. C'est un outil de prévention majeur. Il a également comme avantage de définir les rôles de chacun des acteurs sur le sujet adressé : la lutte contre le terrorisme. Son originalité est la suivante : il propose plusieurs « niveaux » de mesures : une partie de mesures obligatoires pour les signataires de la convention Solas, et une partie d'application simplement recommandée.

Le respect des dispositions du code ISPS est sanctionné par l'obtention d'une « certification de conformité au code ». L'obtention de cette certification est un gage de qualité et de fiabilité en matière de coopération internationale. Il se traduit notamment par une évaluation des risques, un partage d'informations, la nomination d'un « agent de sûreté » (Company Security Officer), la production d'un plan de sûreté, la préconisation d'exercices et de formation, etc.

4.4. Vers une régulation d'ordre économique ?



« Entre le fort et le faible, entre le riche et le pauvre, entre le maître et le serviteur, c'est la liberté qui opprime et la loi qui affranchit »

Henri Lacordaire (1802 – 1861)

La dimension économique prend une part importante au sein des débats sur la régulation du cyberespace. Nombre des rapports entre entreprises et internautes sont régis par des accords contractuels. La proposition d'un système de compétences « cyber » est en effet rapidement mise en échec par le contrat, prévalent entre les parties.

La gouvernance internet résulte en effet de 4 forces distinctes : les règles ou lois édictés par les Etats ainsi que les traités et conventions internationales qui ont une force contraignante ; les normes et coutumes que chacun respecte au nom du « vivre ensemble » ; l'architecture ou le « code », c'est-à-dire les protocoles techniques ; et, enfin, le marché et ses processus concurrentiel, sa liberté de transaction et la loi de l'offre et de la demande.

En dépit d'une montée en puissance de quelques autres acteurs sur certains segments (équipements réseaux notamment) et l'apparition d'acteurs régionaux puissants (vKontacte en Russie, RenRen, Baidu en Chine, etc.), la domination économique des Etats-Unis ne fait pas de doute sur les différents composants du réseau et surtout sa gestion quotidienne. Au point que les fameux GAFAM (Google, Amazon, Facebook, Apple, Microsoft) seraient, selon certains observateurs, devenus l'équivalent des « Compagnies des Indes » des XVII^{ième} et XVIII^{ième} siècles.

Le futur droit du cyberespace sera d'abord un droit économique visant à réguler la compétition entre acteurs privés, notamment par le biais de dispositions protégeant la concurrence. C'est l'une des pistes qui s'esquisse aujourd'hui, comme le démontrent les récents efforts visant à « démanteler » Google en Europe.

Cette dynamique a également touché le droit de l'espace, qui tend aujourd'hui, de plus en plus, à intégrer cette dimension économique. La privatisation croissante des activités spatiales a relégué les Etats au second rang, face aux opérateurs privés (lanceurs, fabricants de matériel, satellites, etc.). Une situation qui tend à se rapprocher de celle du cyberespace.

Annexes

1. Experts interrogés

- Jean-Christophe Izard, administrateur en chef des affaires maritimes, Bureau des affaires juridiques de la mer ;
- Laurent Bloch, chercheur à l'Institut Français d'Analyse stratégique ;
- Kavé Salamatian, Consultant, professeur d'informatique et de réseaux, Université de Savoie, Polytech Annecy-Chambéry ;
- Barnabé Watin-Augouard, chargé de mission sûreté maritime, Secrétariat général de la mer ;
- Philippe Achilleas, maître de conférence de Droit public, directeur de l'Institut du Droit de l'Espace et des Télécommunications ;
- Francis Bruckmann, directeur Sécurité Groupe adjoint, Orange et vice-président du CeCyf, le Centre Expert Français de Lutte contre la Cybercriminalité.

2. Bibliographie

Ouvrages généraux

- Droit international public

Jean COMBACAU, Serge SUR, *Droit international public*, Editions Montchrestien Lextenso, Collection Domat Droit public, 2012, 820 p.

Patrick DAILLIER, Mathias FORTEAU, Alain PELLET, *Droit international public*, LGDJ, 8ème éd., 2009, 1709 p.

Jean-Paul PANCRACIO, *Le droit international des espaces : air, mer, fleuves, terre, cosmos*, Editions A. Colin, Collection U. Droit, 1997, 281 p.

- Droit de l'espace

Philippe ACHILLEAS (dir.), *Droit de l'espace : télécommunication - observation - navigation - défense - exploration*, Editions Larcier, Collection Droit des technologies, 2009, 384 p.

Fernand VERGER (dir.), *L'espace, nouveau territoire*, Belin, 2002, 384 p.

Detlev WOLTER, *Common Security in Outer Space and International Law*, United Nations Publisher, 2005, 316 p.

- Droit de la mer

Ram Prakash ANAND, *Origin and development of the law of sea*, Martinus Nijhoff Publishers, 1982, 255 p.

Jean-Paul PANCRACIO, *Droit de la mer*, Dalloz, 2010, 536 p.

- Droit du cyberespace

Teresa FUENTES-CAMACHO, *Les dimensions internationales du droit du cyberespace*, Economica : UNESCO, 2000, 284 p.

- Droit des "global commons"

Alexandre-Charles KISS, *La notion de patrimoine commun de l'humanité*, Académie de Droit International de La Hay, Recueil des cours, vol. 175, Martinus Nijhoff Publishers, 1982, pp.99-256

ONU, Division des affaires maritimes et du droit de la mer, *La notion de patrimoine commun de l'humanité : historique de l'élaboration des articles 133 à 150 et 311 (6) de la convention des Nations unies sur le droit de la mer*, Editions Nations unies, 1997, 539 p.

ONU, *Global governance and governance of the global commons in the global partnership for development beyond 2015*, janvier 2013, 10 p.

Abraham M. DENMARK (dir.), *Contested commons : the future of american power in a multipolar world*, Center for a New American Security, 25 janvier 2010

Ouvrages spécialisés

Olivier KEMPF, *Introduction à la cyberstratégie*, Economica, 2012, 176 p.

Daniel VENTRE, *Cyberespace et acteurs du cyberconflits*, Editions Lavoisier, Collection Cyberconflits et cybercriminalité, 2011, 283 p.

Dictionnaire

Jean SALMON, « Recours à la force », *Dictionnaire de droit international public*, Bruylant, 2001, 1200 p.

Thèses / mémoires

Olivier DONGAR*, Le statut juridique de l'espace extra-atmosphérique*, Thèse Bordeaux IV, 2008

Raymon K. JOE, *Cyberspace and the Seas : Lessons to be Learned*, Massachusetts Institute of Techonology, septembre 1998, 119 p.

HYUN JUNG Kim, *Le principe de la liberté de la haute mer à l'époque actuelle*, Thèse Université Panthéon-Sorbonne, 2012

Véronique LESTANG, *Droit de la mer – droit de l'espace : vers un droit unitaire des espaces internationaux ?*, Thèse Université Panthéon-Sorbonne, 2001

Revues

- Droit de la mer / cyberespace

Kris E. BARCOMB, "From Sea Power to Cyber Power : Learning from the Past to Craft a Strategy for the Future", *JFQ*, Issue 69, 2nd quarter, 2013, pp.78-83

Steven M. BARNEY, "Innocent packets ? Applying navigational regimes from the law of the sea convention by analogy to the realm of cyberspace", 48 *Naval Law Review*, 2001, pp. 56-86

Mark FRAZZETTO, « A maritime model for cyberspace legal governance », *National Strategy Forum Review Blog*, 15 septembre 2011, 3 p.

Duncan B. HOLLIS, "An e-SOS for Cyberspace", *Harvard International Law Journal*, vol. 52, n°2, Eté 2011, pp.374-432

Julija KALPOKIENE, « Hostes Humani Genereise : Cyberspace, the Sea and Sovereign Control », *Baltic Journal of Law and Politics*, volume 5, n°2, 2012, pp.132-163

James G. STRADIVRIS, Elton C. PARKER III, « Sailing the cyber sea », *JFQ*, Issue 65, 2nd quarterly, 2012, pp.61-67

Aaron TURNER, Michael ASSANTE, "Freedom of the Cyber Seas", *CSO*, 10 avril 2008, 5p.

- Droit de l'espace / cyberespace

Molly MACAULEY, "Space as the canonical Global Commons", *Ressources*, Printemps 2008, pp.8-12

Larry MARTINEZ, "Is there space for the UN ? Perspectives of the UN role in the outer space and cyberspace regimes", *EPSI Perspectives*, n° 56, janvier 2012, 6 p.

Matthew MATHER, « How space and cyberspace are merging to become the primary battlefield of the 21st century », *Space Quarterly Magazine*, mars 2013

- Global commons / cyberespace

Kamlesh BAJAJ, "Cyberspace : global commons or a national asset", *Dataquest*, 15 avril 2012, pp.40-72

Kamlesh BAJAJ, « Cyberspace as global commons : challenges », *Dataquest*, 19 avril 2012, 12 p.

Ronald J. DEIBERT, "Rescuing the global cyber commons : an urgent agenda for the G8", in *The 2011 G8 Dauville Summit : New World, New Ideas*, Newdesk Media Group, 2011

Abraham M. DENMARK, "Managing the Global Commons", *The Washington Quarterly*, juillet 2010 , pp.165-182

Dan HUNTER, "Cyberspace as place, and the tragedy of the digital anticommons", *California Law Review*, vol. 91, issue 2, 2003, pp.442-519

Tara MURPHY, "Security challenges in the 21st century global commons", *Yale Journal of International Affairs*, vol. 5, Issue 2, Printemps/Eté 2010, pp.28-43

Barry R. POSEN, "Command of the Commons : the Military Foundation of U.S. Hegemony", *International Security*, vol.28, n°1, Eté 2003, pp.5-46

Mark RAYMOND, "The Internet as a global commons", in *Governing the Internet : chaos, control or consensus*, CIGI, 26 octobre 2012

Mark REDDEN, Micheal P. HUGHES, "Global commons and domain interrelationships : time for a new conceptual framwork", *Strategic Forum*, n°259, novembre 2012, 12 p.

Geral STANG, "Global commons : between cooperation and competition", *Briefs*, N°17, 8 avril 2013, pp.1-4

Paul C. STERN, "Design principles for global commons : natural ressources and emerging technologies", *International Journal of the Commons*, vol 5 n°2, 2011, pp.213-232

- Cyberespace

Bertrand BOYER, "Le cyberespace, nouveau champ pour la géopolitique ?", in François-Bernard HUYGHE (dir.), *Stratégie dans le cyberespace 2*, IRIS, 1er septembre 2012, p.9

Patrick W. FRANZESE, "Sovereignty in cyberspace : can it exist ?", *The Air Force Law Review*, vol. 64, 2009, pp.2-40

Oona A. HATHAWAY, Rebecca CROOTOF, Philip LEVITZ, Haley NIX, Aileen NOWLAN, William PERDUE, Julia SPIEGEL, « The law of cyber-attack », *California Law Review*, 2012, vol 100, n°4, pp.817-886

Eric HAZANE, "Cyberespace : définition et limite", in François-Bernard HUYGHE (dir.), *Stratégie dans le cyberespace*, IRIS, 25 janvier 2012, p.4

Mireille HILDEBRANDT, "Extraterritorial Jurisdiction to Enforce in Cyberspace. Bodin, Schmitt, Grotius in Cyberspace", *University of Toronto Law Journal*, vol. 63, n°2, 213, pp.196-224

Martin C. LIBICKI, "Cyberspace is not a warfighting domain", *I/S : A Journal of Law and Policy*, vol. 8, Issue 2, 2012, pp.321-336

Kandice McKEE, "A review of Frequently Used Cyber Analogies", *NSCI*, 22 juillet 2011, 7 p.

Darel C. MENTHE, "Jurisdiction in cyberspace : a theory of international spaces", 4 *Mich. Telecomm. Tech. L. Rev.*, 1998, pp.69-103

Joseph S. NYE Jr, "Power and national security in cyberspace", in Kristin M. LORD, Travis SHARP (dir.), *America's cyber future. Security and prosperity in the information age*, Center for a New American Security, juin 2011, pp. 7-23

Juliet M. OBERDING, Terje NORDEHAUG, "A Separate Jurisdiction for Cyberspace", *Journal of Computer-Mediated Communication*, vol. 2, Issue 1, juin 1996,

Jean POLLY, "Surfing the Internet", *Wilson Library Bulletin*, v.66, n°10, juin 1992, pp.38-42

Julie J.C.H. RYAN, Daniel J. RYAN, Eneken TIKK, « Cybersecurity regulation : using analogies to develop frameworks for regulation », Tikk, E. & Talihärm, A.-M. (Dir.*). International Cyber Security Legal and Policy Proceedings*, Tallinn CCD COE Publications, p.76-99

SHENG Li, "When does Internet denial trigger the right of armed self-defense", 38 *Yale Journal of International Law*, hiver 2013, 179-216

Eric STERNER, "Misconceptions about Conflict in Cyberspace", *George C. Marshall Institute Policy Outlook*, septembre 2012, 5p.

Daniel VENTRE, « Le cyberespace : définitions, représentations », dans *Revue Défense Nationale*, juin 2012, n°751, pp.33-38

Brett T. WILLIAMS, "Ten propositions regarding cyberspace operations", *JFQ*, Issue 61, 2nd quarter, 2011, pp.10-18

Colloques

Brett BIDDINGTON, "The Regulation of Space and cyberspace : one coin, two sides", 13th Australian Information Warfare and Security Conference, 3rd-5th December 2012, disponible sur http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1046&context=isw

Jeffrey L. CATON, "Beyond domains, beyond commons : context and theory of conflict in cyberspace", 4th International Concference on Cyber Conflict, NATO CCDCOE Publications, 2012, 11 p., disponible sur http://www.ccdcoe.org/publications/2012proceedings/3_1_Caton_BeyondDomainsBeyond%20Commons.pdf

CCDCOE, Assured Access to the Global Commons – Cyberspace Workshop, 19 octobre 2010, disponible sur http://www.act.nato.int/subpages/globalcommons-reports

Chatham House, Making the Connection : the Future of Cyber and Space, 24 janvier 2013, disponible sur http://www.chathamhouse.org/events/view/188241

Duncan B. HOLLIS, "Stewardship versus sovereignty ? International law and the apportionment of cyberspace", Cyber Dialogue 2012 - What is stewardship in cyberspace?, mars 2012, disponible sur http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_hollis.pdf

SFDI, *L'eau en droit international*, Editions Pedone, juin 2011, 408 p.

Traités

Traité sur l'Antarctique, Washington, 1er décembre 1959

Traité interdisant les essais d'armes nucléaires dans l'atmosphère, dans l'espace extra-atmosphérique et sous l'eau, Moscou, 5 août 1963

Traité sur les principes régissant les activités des Etats en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et autres corps célestes, , 1967

Traité interdisant de placer des armes nucléaires et d'autres armes de destruction massive sur le fond des mers et des océans ainsi que dans leur sous-sol, 11 février 1971

Convention sur la responsabilité internationale pour les dommages causés par des objets spatiaux, 29 novembre 1971

Convention sur l'immatriculation des objets lancés dans l'espace extra-atmosphérique, New-York, 12 décembre 1974

Protocole de 1978 relatif Convention internationale de 1973 pour la prévention de la pollution par les navires, Londres, 17 février 1978

Accord régissant les activités des Etats sur la Lune et les autres corps célestes, 5 décembre 1979

Convention des Nations Unies sur le droit de la mer, Montego Bay, 10 décembre 1982 (+ Assemblée générale des Nations unies, Accord relatif à l'application de la partie XI de la Convention des Nations unies sur le droit de la mer du 10 décembre 1982, A/RES/48/263, 17 août 1994)

Traité sur la zone dénucléarisée du Pacifique Sud, Rarotonga, 6 août 1985

Documents officiels

- Nations Unies

Déclaration des principes juridiques régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, A/RES/1962 (XVIII), 13 décembre 1963

Principes relatifs à l'utilisation de sources d'énergie nucléaire dans l'espace, A/RES/47/68, 14 décembre 1992

Déclaration sur la coopération internationale en matière d'exploration et d'utilisation de l'espace au profit et dans l'intérêt de tous les États, compte tenu en particulier des besoins des pays en développement, A/RES/51/122, 13 décembre 1996

Coopération internationale touchant les utilisations pacifiques de l'espace, A/RES/66/71, 9 décembre 2011

- Japon

Ministère de la défense, Defense of Japan 2013, 2013, pp.164-167

- Etats-Unis

Department of Defense, Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America. 2011 Redefining America's Military Leadership*, 8 février 2011, disponible sur http://www.jcs.mil//content/files/2011-02/020811084800_2011_NMS_-_08_FEB_2011.pdf

Department of Defense, US Army Training and Doctrine Command, *Cyberspace Operations Concept Capability Plan 2016-2028*, Pamphlet 525-7-8, 22 février 2010, disponible sur http://www.fas.org/irp/doddir/army/pam525-7-8.pdf

Department of Defense, Joint Operational Access Concept, 17 janvier 2012, disponible sur http://www.defense.gov/pubs/pdfs/JOAC_Jan%202012_Signed.pdf

Sites internet

Autorité Internationale des Fonds Marins : http://www.isa.org.jm/fr/home

International Mobile Satellite Organization : http://www.imso.org/default.asp

Nations Unies, Division des affaires maritimes et du droit de la mer : http://www.un.org/french/law/los/index.htm

Organisation Internationale de Télécommunications par Satellites : http://www.itso.int/

Tribunal International du Droit de la Mer : http://www.itlos.org/index.php?id=2&L=1

Blogs

CSIS : http://csis.org/blog/space-and-global-commons

Laurent BLOCH, "Les global commons et l'internet", Jade, 16 octobre 2012, disponible sur Laurent BLOCH, "Les global commons et l'internet", Jade, 16 octobre 2012


ceis