v.23

Cyber Strategy :

définir un horizon stratégique dans

l'environnement cyber

Chaire de Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales

Sébastien-Yves Laurent
Professeur des Universités

* Présentation

Sébastien-Yves Laurent est professeur des Universités à la Faculté de droit et de science politique de l'Université de Bordeaux. Il enseigne également à Sciences Po Paris, Sciences Po Bordeaux et à l'École de Guerre Économique. C'est un consultant et analyste spécialiste des enjeux de sécurité globale. Il est le fondateur de l'International Summer School Defence-Security-Cyber (DSC) (http://dsc.u-bordeaux.fr/) et le co-fondateur du groupe de travail « Mètis » (Sciences Po Paris).

Parmi ses publications récentes : *Atlas du renseignement. Géopolitique du pouvoir* (Paris, Presses de Sciences-Po, 2014) ; *Pour une véritable politique publique du renseignement* (Paris, Institut Montaigne, 2014) ; *Transformations et réformes de la sécurité en Europe* (Bordeaux, Presses universitaires de Bordeaux, 2015).

« Internet n'a pas été conçu pour être sécurisé »
(Bernard Barbier, directeur technique de la DGSE, *L'Usine nouvelle,* 12 juillet 2010*)*

* Introduction : les mots pour dire le cyber

Au seuil du travail analytique que nous entreprenons pour la chaire cyberdéfense et cybersécurité Saint-Cyr, Sogeti, Thales, il est indispensable de définir avec précision l'enjeu ici abordé, le cyberespace, tant dans un esprit de bonne méthode que parce que cette réalité est particulièrement complexe et souvent mal identifiée. Elle peut-être caractérisée de multiples façons et ceci pourrait d'ailleurs faire l'objet d'une étude en soi qui n'est cependant pas ici notre propos. Il nous faut donc partir d'une approche large et plastique.

- Le cyberespace est souvent défini comme un système de systèmes et/ou d'un réseau de réseaux d'information. Cette approche est exacte car elle explique l'architecture très particulière de cette réalité (qui cependant, de ce strict point de vue, n'est pas unique) mais en dit trop peu sur sa nature. Des systèmes de systèmes, certes plus rustiques, plus localisés, ont précédé l'Internet et le cyberespace. Or celui-ci présente une nouveauté incontestable par sa nature même. Certaines définitions étatiques peuvent constituer un point de départ, permettant de mieux cerner l'originalité du cyberespace. Ainsi, on peut lire dans la *National Military Strategy for Cyberspace Operations* des États-Unis de 2006 la définition suivante : « […] an operational domain characterized by the use of electronics and the electromagnetic spectrum to create, store, modify and exchange information via networked information systems and associated physical infrastructures »[1]. Cette approche présente le mérite d'approcher concrètement la réalité du cyber qui est faite de signaux supports d'information à portée opérationnelle.

- Il est acquis désormais que le cyberespace constituerait un espace nouveau. L'approche en termes « d'espace » s'inscrit dans un registre qui est celui de la géographie. Or, incontestablement le réseau cybernétique renvoie à une dimension spatiale. En effet, les infrastructures du réseau occupent un espace géographique (certes limité) – les câbles sous-marins, les serveurs, routeurs, *data centers*, terminaux, périphériques, objets connectés et satellites qui constituent tout le *hardware* du cyber – et l'on peut ajouter que les infrastructures couvrent une géographie à l'échelle du monde, mais l'analogie géographique est de portée peu heuristique car elle oublie le contenu et la dimension informationnelle. En revanche, il existe une géographie du cyberespace[2] au sens figuré du terme, au sens où l'entend la géopolitique constituée par des rapports de force entre les acteurs du cyber qui peuvent s'inscrire dans différents espaces.

- De façon complémentaire, le cyberespace est souvent évoqué sous forme d'une « cinquième dimension », ayant surgi après la terre, la mer, l'air et l'espace. Il est juste qu'il y a une grande part d'intangible et d'immatériel dans le cyber ; en outre le numérique est en flux et stock ; il est ubiquitaire, circulant en permanence : ces caractéristiques défient les réalités physiques des quatre autres dimensions. Le cyber

[1]. Cité dans : Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", in : Franklin D. Kramer, Stuart H. Starr, Larry Wentz (dir.), *Cyberpower and National Security*, Washington, National Defense University Press, 2009, p. 27.

[2]. Cf. "Cyberespace: enjeux géopolitiques", *Hérodote*, 1er-2e trimestre 2014, n° 152-153, 312 p.

en possède tout de même certaines caractéristiques et donc l'idée que cette autre dimension serait entièrement nouvelle n'est pas tout à fait satisfaisante, ainsi que l'illustre l'approche classique en trois couches (physique, logique, sémantique).

- Afin donc de dépasser les caractéristiques incomplètes des notions « d'espace » et de « dimension » (Kempf, 2012), on utilisera ici dans les pages qui suivent le terme d'« **environnement cyber** » qui est pour nous à la fois une réalité spatio-géographique, électro-magnétique, informationnelle et socio-politique, dernière composante qui est trop souvent négligée, alors qu'il y a là à notre sens l'un des aspects décisif de ce qui constitue son horizon stratégique. Cet environnement est par ailleurs un espace stratégique au sens propre car il recèle en son sein ce qui est constitutif du stratégique : en effet, le cyber est support de données qui ont été investies par les acteurs économiques, les États et les individus pour des raisons économiques, sécuritaires, mais aussi plus trivialement pour communiquer.

Finalement, le cyber s'inscrit entièrement dans ce que Manuel Castells a appelé en 1998 - au début de la grande expansion de l'Internet - le « paradigme de la technologie de l'information »[3]. Celui-ci est composé de cinq caractéristiques :

- les technologies de l'information agissent sur ce qui est leur matière première, dissipant l'idée d'une neutralité de la technique ;
- les effets des nouvelles technologies sont omniprésents ;
- elles se constituent et se déploient dans une « logique en réseau »
- elles sont particulièrement souples ;
- elles convergent au sein d'un même système d'information.

Le cyberespace récapitule en fait en son sein tout ce qui est constitutif de ce paradigme. On peut même aller plus loin que Castells et considérer désormais que le cyber est en fait aujourd'hui la technologie dominante de l'information et en même temps le principal environnement informationnel, ce qui n'était pas le cas lors de l'écriture de la *Société en réseaux*.

[3]. Manuel Castells, *La Société en réseaux. L'ère de l'information*, tome 1, Paris, Fayard, 1998, p. 100-108.

* Exposé de la question d'étude

L'objet de cette étude est une analyse critique et prospective des enjeux de gouvernance dans le cyber avec un focus sur la dimension de cybersécurité. Elle vise surtout à aider à la définition d'un horizon stratégique pour les acteurs étatiques et privés dans ce que l'on a fait le choix d'appeler l'environnement cyber (cf. *supra*).

Très souvent les études et expertises sur le cyber privilégient soit le point de vue ou la situation des acteurs régaliens, soit ceux des acteurs privés, à commencer par les acteurs économiques du numérique. La Cyber Strategy privilégie la plupart du temps les acteurs sécuritaires[4] (défense, police, protection des « infrastructures critiques ») en essayant de développer les intuitions de la stratégie militaire et en les appliquant au « cyberespace » : ceci a donné lieu à de très solides travaux, notamment en France (Kempf, 2012). On peut signaler aussi une réflexion plus théorique dans le cadre de travaux de recherche et s'inscrivant dans une perspective de sécurité (Ventre, 2014).

Afin de n'être pas redondants avec ces travaux de référence, on a fait le choix d'une approche différente, panoramique permettant de **rassembler dans la même analyse les acteurs régaliens et les acteurs privés, en posant bien leurs spécificités mais en considérant la façon dont ils sont confrontés à des enjeux** souvent **assez proches**. Ces deux grandes catégories d'acteurs sont en fait plongés dans le même environnement cyber avec des objectifs différents et des contraintes variées tout en utilisant des moyens souvent proches (voire identiques sur le plan technique). On fera donc ici de la « **comprehensive analysis** », soit de l'approche globale et transversale en resituant les questions technologiques dans leur environnement socio-politique. Ainsi qu'on le démontrera, le cyber étant une réalité profondément socio-technique, il nous paraît d'autant plus naturel de procéder de la sorte. Le travail sera complété par une approche prospective (4^{e} partie de l'étude) en s'inspirant de la méthode d'« horizon scanning » britannique. Par ailleurs on utilisera tout au long de ce travail la distinction classique depuis 2010 de l'environnement cyber en trois couches.

[4]. Ce terme sera employé dans cette étude dans un sens totalement neutre.

* Executive Summary :

L'objet de cette étude est une analyse critique et prospective des enjeux de gouvernance dans les trois couches du cyber avec un focus particulier sur la dimension de cybersécurité.

* Elle vise ainsi à aider à la définition d'un horizon stratégique pour les acteurs étatiques et privés.

* On a fait ici le choix d'une approche de *comprehensive analysis* permettant de rassembler dans la même analyse les acteurs régaliens et les acteurs privés et en resituant la problématique de la cybersécurité et des différentes gouvernances dans leur environnement normatif et économique.

* L'horizon stratégique fixé dans cette étude repose sur l'identification de 2 caractéristiques durables de long terme, de 10 invariants et de 5 facteurs d'incertitudes qui permettent de bâtir 3 scénarios. L'ensemble du travail s'appuie sur 20 tableaux, graphes et cartes.

* Il est bâti en 4 parties :

1. La construction progressive du cyberespace par ses structures et ses usages
2. L'état actuel de l'environnement cyber
3. Un environnement cyber fait d'incertitudes multiples
4. L'horizon stratégique : des avenirs à géométrie variable.

* Malgré l'arrivée tardive des Etats dans un environnement cyber qui n'a pas été conçu pour eux, on assiste à de multiples balkanisations. Cette caractéristique explique l'importance du principe de gouvernance multistakeholder qui est très dominante dans l'environnement. Celui-ci est faiblement régulé avec la large dominance d'un *soft law* technique sur le *hard law*. Au total, on conclut à une gouvernance relativement forte des couches physiques et logicielles par rapport à une gouvernance de la couche sémantique qui est très faible. De ce point de vue l'Europe est un isolat, favorable aux Internautes mais un espace de forte contrainte juridique pour les acteurs économiques du numérique. L'environnement est caractérisé par des visions très antagonistes entre les grandes et principales moyennes puissances sur ce que doit être le cyberespace de demain.

* Pour les acteurs étatiques et non-étatiques, mettre en œuvre une stratégie dans le cyber suppose de comprendre :

- (1) la transversalité de l'environnement car le cyber innerve tout et de ne pas le limiter à sa dimension la plus visible qui est l'aspect informationnel ;

- (2) les caractéristiques et les ressorts de la gouvernance *multi-stakeholder* où acteurs publics et privés doivent tenir compte de leur caractéristiques respectives et de leurs contraintes spécifiques ;

- (3) l'idéologie à l'œuvre dans le réseau mondial qui sert encore à mobiliser les différents acteurs ;

- (4) la composante socio-politique de l'environnement cyber qui a des effets majeurs, que ce soit sur un plan technologique ou économique.

* En fait, il n'y a pas d'autonomie du cyber par rapport aux autres aspects stratégiques. L'environnement cyber participe désormais d'une approche globale de la stratégie. Les acteurs économiques et régaliens s'affrontent dans l'environnement cyber dans le cadre de leurs rapports de forces généraux. Cet environnement particulier est devenu un terrain privilégié : il est particulièrement attractif car il permet de créer des dommages et des préjudices de façon discrète sans possibilité d'attribution. De ce point de vue, on peut estimer que l'environnement cyber est désormais le terrain majeur d'affrontement indirect. L'in-attribution favorise les stratégies indirectes pour tous les acteurs ayant un certain seuil (bas) de maîtrise technologique. Le développement de l'environnement cyber est d'une certaine façon un égalisateur relatif de puissance.

1. La construction progressive du cyberespace par ses structures et ses usages

1.1. Les deux âges de la cybersphère

Afin de dégager un horizon stratégique dans l'environnement cyber, il importe de comprendre que le cyberespace comprend une dimension publique qui est l'espace d'usage des internautes et une dimension moins publique (mais qui n'est pas close pour autant) qui créé et administre les trois couches. C'est ce que l'on pourrait appeler l'espace de gestion de l'environnement cyber et que, par commodité, on dénommera ici la « cybersphère ».

1.1.1. Des structures techniques *bottom-up*

Avec l'extension du réseau numérique des États-Unis au reste du monde à la croisée des années 1980 et des années 1990, la communauté des informaticiens réseaux et des spécialistes des télécommunications s'est dotée d'organismes techniques et opérationnels internationaux qui ont eu la charge - et l'ont encore – de développer l'Internet mondial. Quatre organisations que l'on peut regrouper selon leur fonction en **trois ensembles** sont au cœur du réseau, y assurent le développement de la couche physique et surtout de la couche logicielle. Ils constituent le coeur de la cybersphère. Ces organisations sont principalement nées aux États-Unis[5], mais avec une vocation extérieure et pour certaines ont adopté une structure internationale dans les années 1990.

- Le **premier ensemble** est constitué de deux organisations, l'IETF et l'ISOC. L'IETF (Internet Engineering Task Force) a été créée en 1986 pour développer les protocoles de l'Internet. Elle est organisée en plus de 100 groupes de travail, actifs dans 7 domaines (Applications area, General area, Internet area, Operations and Management area, Routing area, Security area, Transport area)[6]. Seules des personnes physiques peuvent y participer, ponctuellement ou non. Les membres des sociétés ou de personnes morales peuvent également y participer, mais uniquement à titre individuel. Il n'y a pas d'adhésion à l'IETF. Le *modus operandi* est l'établissement par des processus participatifs de « Requests for Comments » (RFC), au nombre de 5000 en 2011[7]. Les RFC assurent le fonctionnement du cœur du cyberspace aujourd'hui. L'Internet Architecture Board (IAB) est l'un des comités les plus importants de l'IETF dans la mesure où il mène une réflexion prospective sur l'architecture du réseau des réseaux. Par ailleurs l'IETF peut s'appuyer sur une association de droit étatsunien à

[5]. « Nous possédons l'internet. Nous l'avons créé, développé et perfectionné à un niveau qui fait qu'ils [les pays européens] ne peuvent pas nous concurrencer » est une phrase souvent citée et attribuée à B. Obama. Nous n'avons pas réussi à en retrouver une trace *princeps*.

[6]. https://www.ietf.org/iesg/area.html

[7]. Christopher T. Mardsen, *Internet Co-Regulation. European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge, Cambridge University Press, 2011, p. 105.

vocation internationale créée en 1992, l'ISOC (Internet Society). Celle-ci a pour charge de lever des fonds au bénéfice de l'IETF à qui elle donne une structure juridique et au-delà de ce rôle très important, de promouvoir les valeurs et les principes fondateurs de l'Internet (cf. *infra* en 1.2). C'est par ailleurs l'ISOC qui édite les RFC de l'IETF.

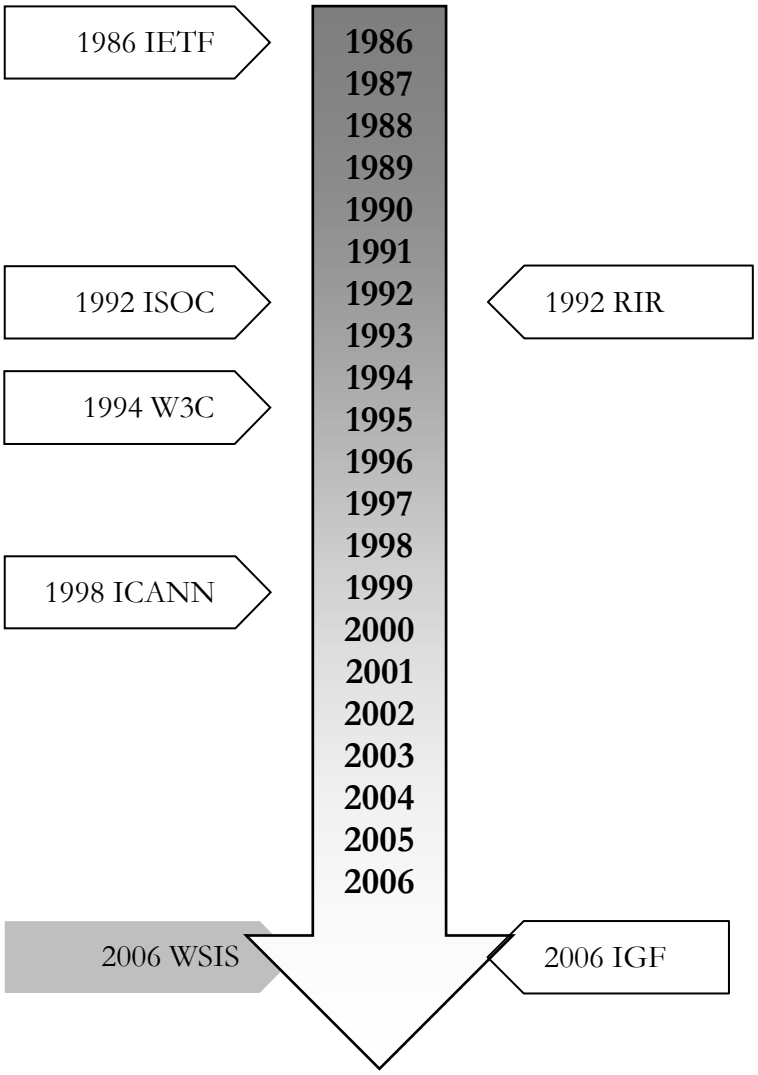
- Le **second ensemble** est chargé de développer les protocoles et d'encourager à la création de logiciels utilisables pour et sur le Web et plus généralement l'ensemble des standards du Web : c'est un organisme créé en 1994, le World Wide Web Consortium (W3C). Le W3C est une organisation à but non lucratif qui rassemble uniquement des personnes morales d'origines les plus diverses (acteurs économiques, universités et écoles…) : il compte 394 membres à l'été 2015[8].

- Enfin vient le **troisième ensemble**, l'Internet Corporation for Assigned Names and Numbers (ICANN) créée en 1998 qui assure plusieurs rôles opérationnels majeurs : le fonctionnement du système d'identification (noms de domaines et adresses IP) et la gestion des serveurs racines du DNS. C'est une association de droit californien qui a signé un MOU avec le ministère du commerce fédéral. L'organisation s'est fortement internationalisée et depuis 2010 les représentants de nationalité américaine ne sont plus majoritaires. Un an après la création de l'ICANN, l'association avait décidé la création du Governmental Advisory Committee (GAC) afin de permettre, dans un esprit *multi-stakeholder*, la représentation des États. A l'été 2015, il y avait 150 membres et 32 observateurs au sein du GAC qui est une commission seulement consultative[9], mais dont le rôle n'a cessé de croître depuis sa mise en place en 1999. Logiquement c'est l'ICANN qui gère les 5 Regional Internet Registry (RIR) mondiaux : le RIPE-NCC (« Réseaux IP Européens » – en français dans le texte - pour l'Europe et le Moyen-Orient), l'ARIN (*American Registry for Internet Numbers* pour l'Amérique du Nord), l'APNIC (*Asia Pacific Network Information Center*), le LACNIC (*Latin American and Caribbean Network Information Centre* pour l'Amérique Latine et les Caraïbes), enfin l'Afri.NIC (*African Network Information Center*).

Les quatre organisations que l'on vient d'évoquer sont historiquement les premières à être apparues et elles ont fait naître l'Internet. Situées hors du secteur marchand, elles assurent encore aujourd'hui le fonctionnement quotidien de l'Internet et du cyberespace. Elles sont toutes nées de façon spontanée sous une forme *bottom-up*, en entretenant des liens étroits entre elles. Elles sont le centre névralgique de la cybersphère, ce que nous appellerons ici par la suite le « cyberpshere core » (CC).

[8]. http://www.w3.org/Consortium/Member/List [18/07/2015]
[9]. https://gacweb.icann.org/display/gacweb/About+The+GAC [18/07/2015]

Graphe 1 : les organisations et institutions composant la Cybersphère



1.1.2. L'intervention de l'ONU : l'émergence de la question de la gouvernance de l'Internet

Jusqu'au début des années 2000, la cybersphère se limitait à ce que l'on vient de voir en 1.1.1, c'est-à-dire des structures techniques *bottom up*. Au cours de la décennie qui a suivi les Nations Unies se sont fortement engagées dans l'accompagnement du développement de l'Internet et ont contribué en deux phases (cf. le graphe 2 *infra*) à la transformation de la cybersphere.

C'est l'une des organisations spécialisées des NU, l'Union Internationale des Télécommunications (UTI-ITU) qui a mené cette transformation. Au début de la décennie, l'ITU était l'une des plus anciennes organisations internationales au monde,

fondée en 1865 à l'heure des débuts des câbles sous-marins et du télégraphe électrique international. Elle était un forum pour toutes les questions techniques posées par les télécommunications et avait de ce fait pour tâche principale d'attribuer les fréquences hertziennes et de fixer les orbites pour les satellites. L'ITU a su profiter de l'émergence de l'Internet commercial à partir du milieu des années 1990 et de son statut d'agence des NU pour organiser au cours d'une première phase (2003-2005) les deux sommets mondiaux qui ont notamment mis à l'ordre du jour la question de la gouvernance de l'Internet. Cette politique de l'ITU a eu pour toile de fond la thématique du développement de la « société de l'information ». Les NU ont ainsi confié à l'ITU le soin d'organiser les deux « sommets mondiaux de la société de l'information » (SMSI-WSIS)[10]. Le premier qui s'est tenu les 10-12 décembre 2003 à Genève a rassemblé 175 États membres de l'ITU. Une « déclaration de principes » de 67 points ainsi qu'un « plan d'action » ont été adoptés à l'issue du sommet. Pour la première fois l'Internet était qualifié de « ressource publique mondiale »/« global facility available to the public » (point 48 de la déclaration de principes). C'est dans ce même passage que la question de la gouvernance de l'Internet était abordée : « La gestion internationale de l'Internet devrait s'exercer de façon multilatérale, transparente et démocratique, avec la pleine participation des États, du secteur privé, de la société civile et des organisations internationales ». On voit la rupture potentielle que cette déclaration pouvait entraîner, par rapport à la petite cybersphère technique, seule existante à l'époque. Les signataires invitaient ensuite les NU à créer un groupe de travail sur la gouvernance de l'Internet : « […] dans le cadre d'un processus ouvert et inclusif prévoyant un mécanisme qui garantira la participation pleine et active des représentants des États […] » (point 50) en fixant par ailleurs un horizon de deux années. Le secrétaire général des Nations Unies a alors créé un Working Group on Internet Governance (WGIG) qui s'est aussitôt mis au travail, identifiant les 4 « policy areas » suivantes : « infrastructure and the management of critical Internet resources », « internet governance », « intellectual property rights » and « international trade » et « development and capacity building ». L'ITU a accompagné le travail du WGIG qui a de fait préparé le second SMSI-WSIS, tenu à Tunis les 16-18 novembre 2005. 174 pays étaient représentés à cette réunion. Confirmant les linéaments établis à Genève, son principal résultat fut la signature d'un « agenda de Tunis pour la société de l'information » comprenant 122 points. Les points 29 à 82 portaient sur la gouvernance de l'Internet[11].

La deuxième phase (cf. le graphe 2 *infra*) de la transformation de la cybersphère a débuté en 2006 et se poursuit de nos jours encore. Elle est caractérisée, après que les fondements intellectuels ont été établis lors des deux SMSI-WSIS, par la création d'un organisme dédié à la gouvernance et par la multiplication des réunions et sommets internationaux sur l'environnement cyber (cf. le graphe 2). En février et mai 2006, deux sessions de négociations ont eu lieu à Genève et ont débouché sur l'annonce le 18 juillet 2006 par le secrétaire général des Nations Unies de la création de l'Internet

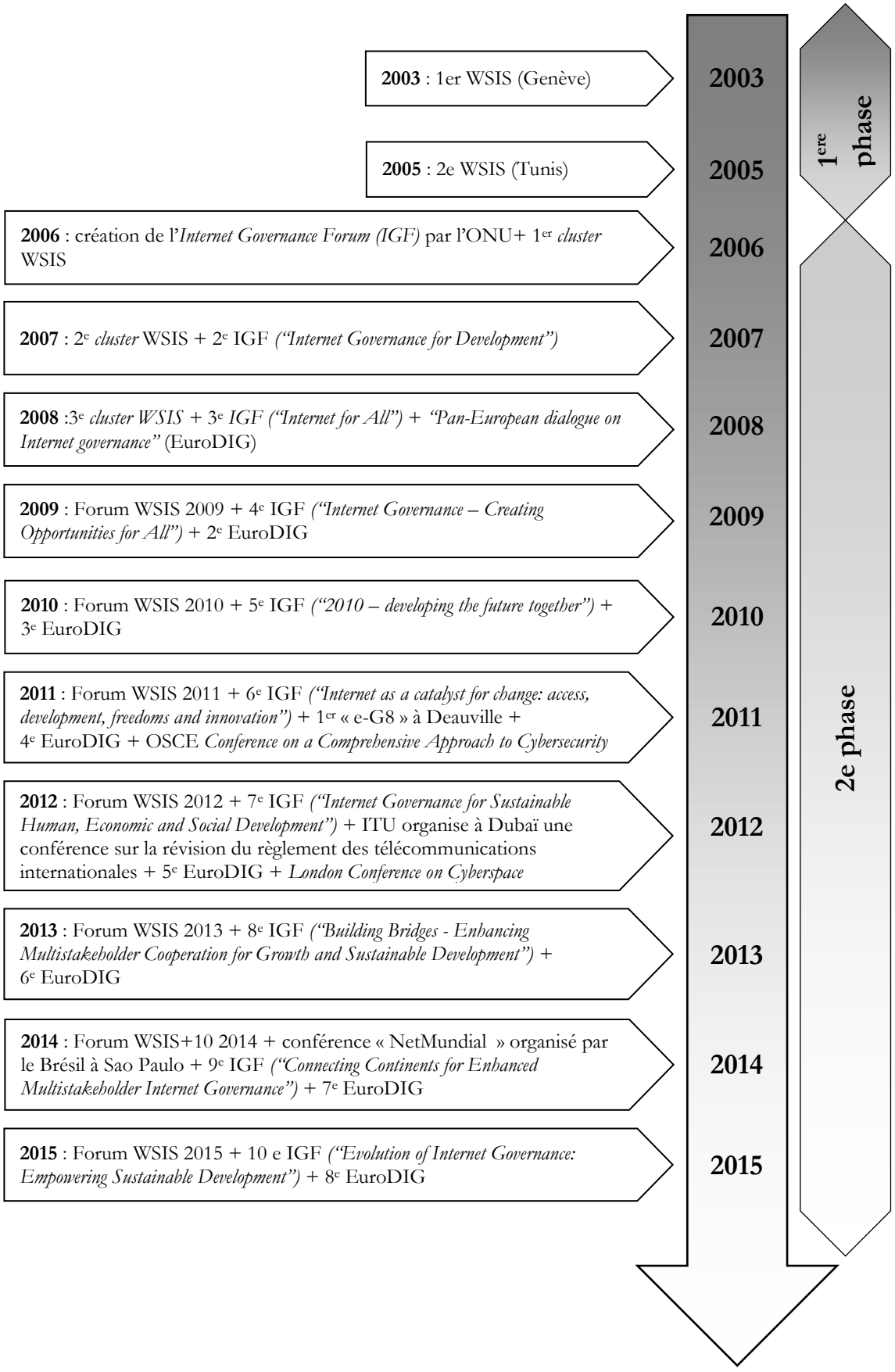
[10]. On trouvera en fin d'étude dans l'exposé détaillé des sources les différentes références précises des textes fondamentaux de ces réunions que nous citons.
[11]. On reviendra plus en détail sur ce point *infra* en 3.3.

Governance Forum (IGF), structure spécialisée des Nations Unies ayant en charge d'assurer les débats autour de la gouvernance de l'Internet. L'IGF s'inscrit entièrement dans le cadre de la pensée *multi-stakeholder*, l'un de ses comités consultatifs étant le « Multistakeholder Advisory Group » (MAG) composé de 55 membres à l'été 2015[12]. Ce MAG se réunit plusieurs fois dans l'année et prépare notamment le sommet annuel de l'IGF qui met en avant à chaque édition une thématique particulière.

Ainsi la décennie 2000 a vu la montée en puissance de l'ITU sous couvert de la mise en place de l'IGF, puis de l'animation des débats autour de la gouvernance (cf. *infra* en 2.3 et 3.3). Cependant l'ITU a été affaibli par sa propre feuille de route qui est le règlement international des télécommunications (RTI) datant de 1988, inadapté à l'ère de l'Internet. Pour faire évoluer ce cadre contraignant, l'ITU a organisé à Dubaï les 3-14 décembre 2012 un sommet (« conférence mondiale des télécommunications internationales ») dont l'objet apparent était la révision du RTI de 1988, mais avec un agenda caché, celui de la gouvernance de l'Internet. Sur les 193 États-membres de l'ITU, 151 États ont participé à la réunion. Le sommet qui s'est conclu sur un échec pour l'ITU a surtout été l'occasion de voir à quel point les positions des États s'étaient figées de façon assez antagoniste sur le devenir de l'Internet. Les États-Unis qui avaient une délégation de plus de 120 membres (dont très logiquement Google et Facebook) étaient (et demeurent) très hostiles à l'ITU dont ils contestent la volonté d'étendre son champ de compétences vers l'Internet. Les Européens ont adopté une position assez proche, alors que la Russie et la Chine plus réticentes à l'approche *multi-stakeholder* dans l'Internet, apprécient l'ITU où malgré la représentation de 700 sociétés privées de télécommunications, les États ont une action prépondérante et sont les seuls à voter. Sur les 151 États présents, 55 dont les États-Unis, la plupart des pays de l'UE (dont la France) ont refusé de signer la résolution finale de la conférence qui avait notamment le soutien de la Chine et de la Russie et qui visait à accroître le rôle de l'ITU dans la gouvernance de l'Internet.

[12]. http://www.intgovforum.org/cms/component/content/article?id=2102:mag-2015

Graphe 2 : conférences, réunions et sommets internationaux sur l'Internet (2003-2015)



2003 : 1er WSIS (Genève)

2005 : 2e WSIS (Tunis)

2006 : création de l'*Internet Governance Forum (IGF)* par l'ONU+ 1er *cluster* WSIS

2007 : 2e *cluster* WSIS + 2e IGF *("Internet Governance for Development")*

2008 :3e *cluster WSIS* + 3e *IGF ("Internet for All")* + *"Pan-European dialogue on Internet governance"* (EuroDIG)

2009 : Forum WSIS 2009 + 4e IGF *("Internet Governance – Creating Opportunities for All")* + 2e EuroDIG

2010 : Forum WSIS 2010 + 5e IGF *("2010 – developing the future together")* + 3e EuroDIG

2011 : Forum WSIS 2011 + 6e IGF *("Internet as a catalyst for change: access, development, freedoms and innovation")* + 1er « e-G8 » à Deauville + 4e EuroDIG + OSCE *Conference on a Comprehensive Approach to Cybersecurity*

2012 : Forum WSIS 2012 + 7e IGF *("Internet Governance for Sustainable Human, Economic and Social Development")* + ITU organise à Dubaï une conférence sur la révision du règlement des télécommunications internationales + 5e EuroDIG + *London Conference on Cyberspace*

2013 : Forum WSIS 2013 + 8e IGF *("Building Bridges - Enhancing Multistakeholder Cooperation for Growth and Sustainable Development")* + 6e EuroDIG

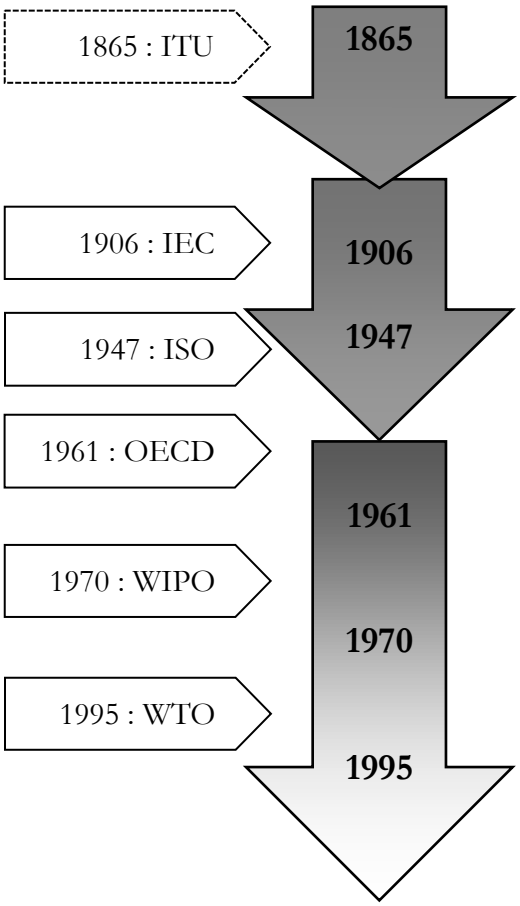
2014 : Forum WSIS+10 2014 + conférence « NetMundial » organisé par le Brésil à Sao Paulo + 9e IGF *("Connecting Continents for Enhanced Multistakeholder Internet Governance")* + 7e EuroDIG

2015 : Forum WSIS 2015 + 10 e IGF *("Evolution of Internet Governance: Empowering Sustainable Development")* + 8e EuroDIG

1.1.3. Jeux d'influence et tensions dans / autour de la cybersphère

Au cours de la 2e phase, qui caractérise à notre sens encore la situation actuelle, des organismes extérieurs ont tenté d'influer sur l'environnement cyber. On ne reviendra pas longuement sur le rôle de l'ITU que l'on vient d'évoquer et dont l'action, particulièrement ambitieuse, visait à s'imposer de façon *top down*, par le biais de certains États, sur la gouvernance. Cinq autres organismes essaient et parviennent à jouer un rôle partiel sur la cybersphère.

Graphe 3 : les organisations et institutions extérieures influant sur la Cybersphère



Ces différents organismes ont des capacités d'influence en apparence plus limitées que l'ITU. Ils ont cependant une action bien réelle, principalement en produisant des normes, des certifications et des standards (cf. tableau 1 *infra*) – du *soft law* – qui ne s'appliquent pas exclusivement à l'environnement cyber, mais qui y sont néanmoins très importantes. Le rôle des organismes dont l'action est à portée normative ne vise pas seulement à assurer un certain niveau de qualité, mais il contribue également et surtout directement à l'interopérabilité qui est un aspect central du réseau des réseaux (cf. *infra* en 1.2).

A la différence du centre névralgique de la cybersphère, ce que l'on a appelé dans le graphe 4 de synthèse le « cybersphere core » (CC), ces organisations lui sont

antérieures pour la presque totalité. Ce sont des organismes internationaux spécialisés (IEC, ISO, WIPO) ou transverses (OECD, WTO) qui ont le statut d'organisations internationales.

Tableau 1 : rôle des organisations et institutions influant sur la Cybersphère

		Pays membres en 2015	**Rôle en matière cyber-num.**
ITU	International Telecommunication Union	193	- production de normes (« Recommandations ITU-T ») - développement des infrastructures dans les PVD (par l'« ITU-D) - diffusion des bonnes pratiques y compris en cybersécurité
IEC	International Electrotechnical Commission	83	- normalisation de la sémantique électrique et électronique - normalisation de l'électrique et de l'électronique
ISO	International Organization for Standardisation	165	- normalisation en sécurité et cybersécurité
OECD	Organization for Economic Co-operation and Development	34	- diffusion des bonnes pratiques en faveur de la cybersécurité, du développement économique et du bien-être social - discussions en faveur de l'harmonisation fiscale dans le secteur du numérique
WIPO	World Intellectual Property Organization	188	- définition des droits de propriété intellectuelle (traités de 1996) - dépôt des brevets ICT
WTO	World Trade Organization	161	- définition des droits de propriété intellectuelle (TRIPS-ADPIC, 1994)

Du point de vue de leurs effets, ces différentes organisations /institutions doivent être hiérarchisées. Toutes n'ont pas la même influence sur la cybersphère.

- Depuis Dubaï, de nombreux analystes estiment que l'ITU, attachée au rôle dominant des États, plus favorable à la multilatéralité classique qu'à la gouvernance, est un organisme inadéquat et inadapté à l'environnement cyber. Les États-Unis et une partie des pays de l'Union européenne voudraient cantonner cette organisation à un rôle d'attribution des fréquences hertziennes, des orbites et des canaux satellitaires et

plus généralement à son rôle en matière de développement des infrastructures téléphoniques. Ceci est effectivement sa tâche principale depuis la fin du XIXe siècle, mais cela occulte la portée de ses compétences dans la cybersphère où son action n'est pas tout à fait négligeable. Elle joue en effet un rôle normatif méconnu, sinon des seuls spécialistes. Ainsi à l'été 2015, elle avait développé plus de 4000 normes en matière de télécommunications[13] : celles figurant dans la série Y de l'ITU sont spécifiques à l'Internet et au Cyber, mais celles de la série X les concernent également. Il reste que l'ITU est perçue également comme marginale par rapport à ce que nous appellerons ici le « cybersphere core » : des relations existent avec l'IETF et W3C, mais elles sont difficiles de l'aveu même du secrétaire général de l'ITU[14].

- L'International Electrotechnical Commission (IEC) a le même rôle normatif en matière d'équipements électriques et électroniques qui constituent une partie décisive des ordinateurs et routeurs, soit les éléments fondamentaux de la couche physique de l'environnement cyber. Sur les 97 comités techniques de l'IEC[15] plusieurs dizaines concernent des composants indispensables à l'environnement cyber.

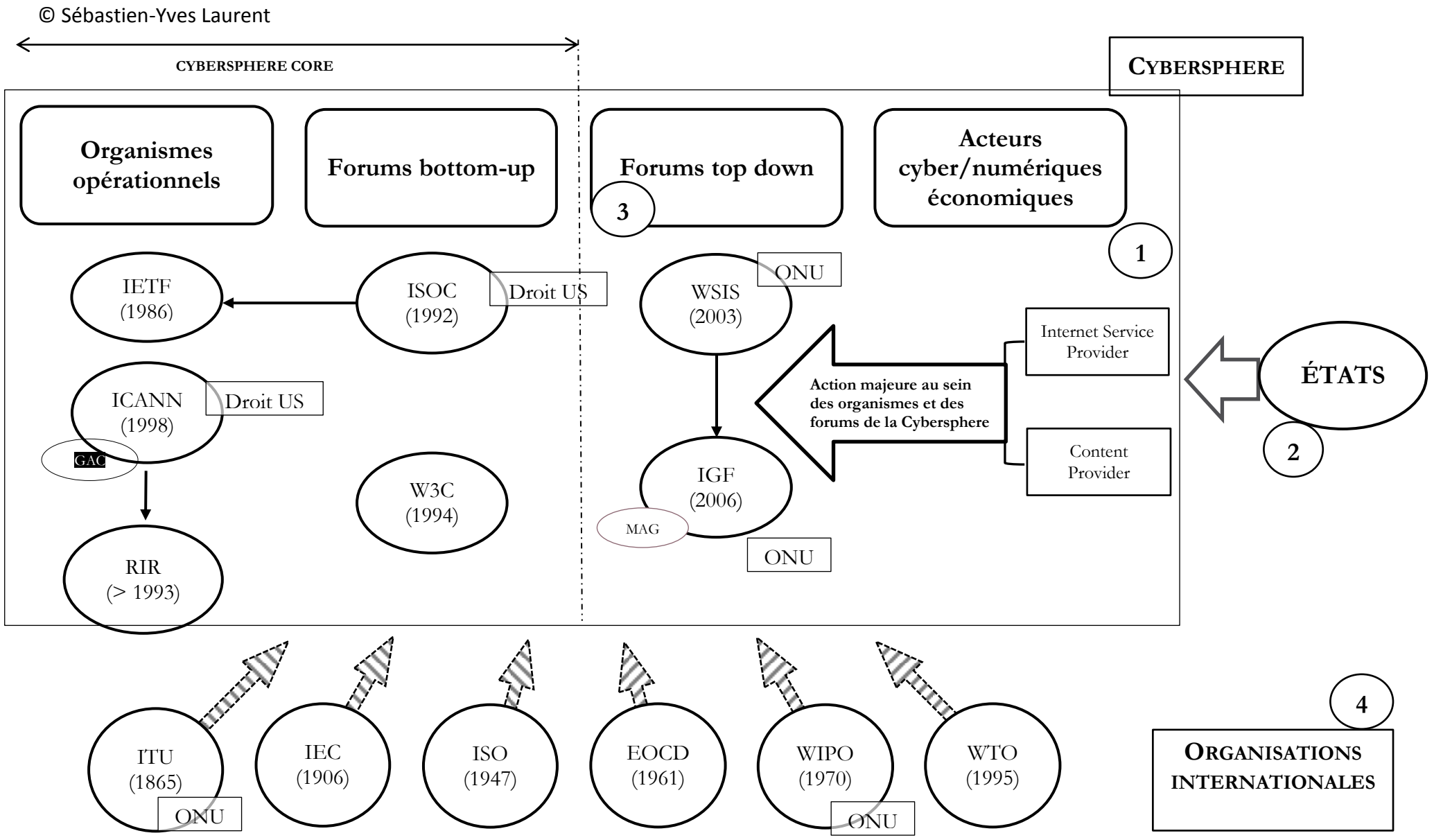
- L'organisation internationale de standardisation (ISO) est également importante dans la mesure où de nombreux processus industriels et de services ont besoin de sa certification. Actuellement un cinquième de près des 20 000 normes internationales de l'ISO concernent les technologies de l'information et de la communication[16], notamment mais pas seulement en matière de sécurité/sûreté (cf. *infra* en 3.2.).

- Enfin, l'organisation mondiale de la propriété intellectuelle (OMPI-WIPO) et l'OMC-WTO contribuent également à avoir une influence sur la cybersphère dans la mesure où ils fixent le cadre juridique des brevets et de la propriété intellectuelle. En ce qui concerne la première organisation, un tiers des brevets déposés relève du secteur ICT[17].

- Par ailleurs l'OMC-WTO s'est immiscée dès sa création dans le domaine traditionnel de l'OMPI avec l'accord TRIPS-ADPIC de 1994 qui replace une partie du DPI à portée commerciale dans l'orbite de l'OMC-WTO.

[13]. http://www.itu.int/fr/ITU-T/publications/Pages/recs.aspx
[14]. Entretien de l'auteur avec le Dr Hamadoun Touré, secrétaire général de l'UIT, 17 mars 2014.
[15]. http://www.iec.ch/dyn/www/f?p=103:6:0##ref=menu
[16]. David Fayon, *Géopolitique de l'Internet: Qui gouverne le monde ?*, Paris, Ecomonica, 2013, p. 194.
[17]. OECD, "The digital economy today", in OECD, *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, p. 35.

Graphe 4: jeux d'influences dans et autour de la Cybersphère



Le **graphe 4** synthétise de façon simplifiée les **rapports de force** aujourd'hui autour de la **cyberpshère.** Le « cybersphere core » (CC) a émergé au tournant des années 1980 et 1990 de façon autonome par rapport aux organisations et administrations nationales et internationales existant à l'époque. Une question demeure sur le CC : quelle est son autonomie ? On peut le formuler autrement : quelle est l'intensité du lien avec les États-Unis qui ont vu naître et ont accompagné les quatre organisations ? En mars 2014, les États-Unis ont annoncé qu'ils allaient abandonner au sein de l'ICANN leur tutelle sur la fonction IANA, fonction qui n'est pas aussi symbolique qu'il y paraît. Le processus est toujours en cours et devra passer par un vote du Congrès, ce qui n'est pas le moindre des obstacles. Les États-Unis ont formulé deux conditions expresses pour ce transfert : que l'administration de l'IANA ne tombe ni sous la coupe d'un seul État, ni sous celle de l'ONU…Mais le lien du CC avec les États-Unis ne touche pas seulement la fonction IANA. Un travail de recherche poussé essayant de quantifier l'influence étatsunienne au sein de l'IETF, de l'ISOC et du W3C serait nécessaire pour aller plus loin.

Ainsi que nous l'avons indiqué dans le graphe précédent, l'environnement cyber a été profondément modifié au cours de la décennie suivante sous l'effet : (1) de l'apparition des grands acteurs économiques du numérique, à commencer par les plateformes, (2) en raison de la mobilisation des États, (3) avec la mobilisation des Nations Unies, enfin (4) avec l'intérêt pour le cyber marqué par certaines organisations internationales. Les acteurs économiques ont transformé l'équilibre de l'environnement cyber en polarisant de plus en plus un système conçu sur la base d'une architecture décentralisée et ne créant des verticalités. Qui plus est, en jouant de la dimension participative du système, ils se sont investis dans les organismes opérationnels et les forums du cybersphere core en essayant de faire valoir leurs intérêts et objectifs. L'action – tardive - des États (cf. *infra* en 2.5) a également transformé la cybersphère même si l'environnement demeure assez faiblement régulé (cf. *infra* en 3.2). En l'occurrence les États ne jouent pas seulement de la règle de droit mais ont des modalités d'influence et de puissance variées. L'effet de l'irruption de l'ONU directement (organisation des SMSI-WSIS) et indirectement (par la biais de l'ITU) ne doit pas être surévalué. La création de l'IGF n'a pas eu la portée escomptée : c'est en fait devenu un forum mondial supplémentaire, certes spécialisé sur la gouvernance du cyber mais sans monopole en la matière et sans aucune capacité contraignante ou même normative, y compris en matière de *soft law*. La gouvernance réelle du cyber se fait en dehors de l'IGF. En revanche, les organisations internationales ont un rôle moins apparent mais beaucoup plus net, principalement par le biais du *soft law* dans et sur la couche logique. C'est à cette réalité politique qu'il faut confronter l'idéologie propre à l'environnement cyber.

1.2. La puissance de mobilisation des principes fondamentaux de l'Internet

L'une des caractéristiques les plus surprenantes du cyberespace aujourd'hui au regard de sa centralité est son caractère originellement non institutionnel. Par non institutionnel, on entend le fait qu'il n'est pas une création par consensus et par décision d'organisations internationales (OIT) ou d'États, à la différence de toutes les OIT qui ont été créées par des États. Il est le résultat de développements discrets aux États-Unis (cf. *infra* en 2.4) ayant abouti à créer un environnement majeur de la vie quotidienne pour les personnes physiques et les acteurs économiques. Dans le même ordre d'idées, il n'a pas fait l'objet de programmes de développement et de théorisation : c'est un environnement conçu par quelques ingénieurs et développeurs (principalement mais non exclusivement situés aux États-Unis) qui se sont entendus sur des principes techniques communs dans la couche logique sur la base d'éléments à l'époque à leur disposition dans la couche physique. Jamais ils n'ont pensé à fixer des règles dans la couche sémantique : en cela on peut considérer que l'environnement cyber a été conçu, de manière négative en quelque sorte, dans une perspective anomique. Selon l'expression célèbre du juriste Lawrence Lessig employée en 2000 dans le *Harvard Magazine* : « code is law ». Cette caractéristique est aujourd'hui de très grande portée et l'on peut même considérer que les enjeux actuels touchant à la surveillance, à la liberté d'expression, à la propriété des données, à la propriété intellectuelle….etc, tous points examinés plus avant dans la 4e partie, sont la conséquence directe du caractère exclusivement technique du réseau pendant plusieurs décennies. L'absence de théorisation du cyberespace ne s'explique pas seulement parce qu'il a été pensé et bâti par des ingénieurs, mais aussi parce que les multiples acteurs collectifs qui ont accompagné son développement (ingénieurs d'origine militaire, de sensibilité libertaire ou des universitaires) (Cardon, 2010) avaient des intérêts et des idéologies différentes. Finalement, les couches logicielle et physique ont été un plus petit dénominateur commun du cyberespace, mais aussi son unique horizon jusqu'à ce qu'un certain nombre d'institutions et d'États dans la décennie 2000 se préoccupent de fixer des règles et des normes dans la couche sémantique (cf. *infra* en 3.2).

Si l'environnement n'a pas été théorisé au sens où des règles et des normes écrites permettraient a priori d'en réguler l'usage, il a été pensé dans la mesure où des principes fondateurs communs ont été définis de façon coutumière par les différents acteurs cités plus haut. Malgré l'irruption au début des années 2000 de grands fournisseurs de contenus qui ont fortement transformé l'environnement cyber, les principes coutumiers demeurent importants à tel point que les OIT, les États et les grands acteurs économiques s'y réfèrent encore régulièrement, bien que certaines de leurs pratiques en soient la négation concrète quand ils ne les remettent pas en question… La plupart de ces principes ont également été repris lors deux SMSI-WSIS de 2003 et 2005 (cf. *supra* en 1.1.2).

On peut ainsi constater la prégnance de quatre grands principes fondamentaux (PF) :

- Le premier d'entre eux renvoie à la caractéristique fondamentale de l'Internet : il s'agit d'un réseau qui a été conçu pour être **libre et ouvert**. Tous les

utilisateurs doivent pouvoir y accéder sans restriction et avoir la possibilité de contribuer à son développement. Ceci porte de multiples conséquences et notamment le fait qu'il n'y a en apparence pas de propriété du réseau dans la couche logicielle et sémantique : tous les utilisateurs peuvent l'étendre et le modifier pour peu qu'ils utilisent les protocoles et les RFC développés par les organes techniques.

- D'autre part, l'**interopérabilité** est un PF majeur, conséquence technique du caractère ouvert de l'Internet. Tous les usagers peuvent développer des subdivisions et des extensions du réseau de réseaux à la condition qu'ils s'inscrivent dans l'architecture globale et qu'ils utilisent les protocoles adéquats. L'architecture de l'Internet hier, du cyberespace aujourd'hui est caractérisée par sa décentralisation.

- Les deux premiers PF ne sont pas discriminants, ce qui signifie que tous les usagers/utilisateurs peuvent employer l'Internet et le développer. Autrement dit, les personnes physiques et morales, les acteurs publics et privés sont tous également légitimes pour intervenir. Ceci a pour conséquence que le fonctionnement général de l'Internet repose sur un cadre ***multi-stakeholder*** qui remet principalement en cause les États, historiquement dominants dans le système international.

- Enfin le quatrième et dernier PF est la notion de « **net neutrality** » (NN) exposée par Tim Wu en 2003[18]. Selon ce principe, tous les usagers, qu'ils soient des personnes physiques ou morales doivent avoir accès à un volume égal de contenu et de données. Les *Internet Services Providers* (ISP) ne peuvent différencier les usagers afin de discriminer ce à quoi ils ont accès, que ce soit en quantité (volume) ou en qualité (contenu). Il est important de souligner qu'aux États-Unis le 26 février 2015, la Federal Communications Commission (FCC) a adopté le principe de la neutralité du Net contre la volonté de nombreux acteurs du numérique du pays (tout en reconnaissant au passage le réseau comme une « public utility »).

On peut synthétiser dans le tableau simplifié qui suit les effets des PF sur les acteurs économiques et les États.

Tableau 2 : effets des principes fondamentaux de l'Internet sur le marché et les États

PF	Effets sur le marché	Effets sur les États
liberté d'accès et ouverture	libéralisation	impossibilité de contrôler l'accès
interopérabilité	minimisation des coûts de structure et simplification	difficulté et surcoût pour développer des structures/architectures « souveraines »
cadre *multi-stakeholder*	accroissement de l'influence	dissolution de l'influence internationale
net neutrality	limitation des prix pour les ISP	difficulté de contrôler les contenus

[18]. Tim Wu, « Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and High Technology Law*, vol. 2, 2003, p. 141-178 et une solide étude critique sur cette notion : Francesca Musiani, "Neutralité de l'Internet : dépasser les scandales", *Politique étrangère*, hiver 2014-4, p. 57-68.

Comme on le voit ci-dessus, les principes fondamentaux de l'environnement cyber ont des conséquences diamétralement opposées selon que l'on considère les États ou le marché. Ceci s'explique assez aisément parce que les valeurs des PF sont en fait fondamentalement libérales. La dimension libertaire d'une partie d'entre elles rejoint dans ses conséquences la dimension libérale. La pensée - non formulée - de l'Internet est peu ou prou une pensée du marché. Incontestablement les États ne sont pas, par nature, ceux des acteurs pouvant se conformer le plus facilement au cyberespace (cf. la discussion sur ce point *infra* en 2.5) où ils sont arrivés tardivement, c'est-à-dire récemment.

Il faut nuancer cependant fortement l'effectivité des PF. Dans de nombreux États démocratiques des législations permettent de réguler la liberté d'expression et de lui fixer des limites dans le cyberespace en transposant les règles existantes. Des États non démocratiques (Chine, Iran,…) ont assuré les surcoûts de développement d'Internets « souverains » qu'ils peuvent contrôler. Enfin, la NN est encore très théorique. Elle est reconnue par la loi seulement dans de rares pays (Chili, Pérou, Pays-Bas et Slovénie). En apparence dans l'aire occidentale ce PF tend à gagner en reconnaissance officielle et normative. Ainsi au début du mois d'avril 2014, le Parlement européen a adopté le règlement 47-0190/2014 prescrivant la neutralité du Net (NN), mais ceci n'a pas de portée immédiate et concrète tant que le conseil ou la commission ne lui auront pas donné une application. Lors de la conférence de Dubaï de 2012 (cf. *supra* en 1.2) certains fournisseurs de contenus ont montré très clairement leur hostilité à la NN.

1.3. L'essor de la conflictualité dans l'environnement cyber

L'environnement cyber n'est pas resté longtemps à l'abri de diverses conflictualités. Le premier piratage de réseau informatique a eu lieu aux États-Unis en date de 1978. Six ans plus tard en Allemagne, le Chaos Computer Club attaquait avec succès un serveur de la Deutsche Bundespost, le Bildschirmtext et était parvenu à lui voler 134 000 DM. Quant au premier virus identifié, il semblerait dater de 1988, lorsque fut découvert aux États-Unis un ver ayant infecté 10 % des 60 000 ordinateurs alors connectés à l'Internet (De Nardis, 2014). Aujourd'hui l'environnement cyber est l'objet d'atteintes quotidiennes et très diverses : il est désormais un lieu courant de délinquance, de criminalité et d'affrontements de toutes sortes auxquels les individus, les personnes morales et les États sont quotidiennement confrontés. Ces mêmes types de victimes sont également les grandes catégories d'acteurs de la cybercriminalité entendue au sens large.

Par clarté, on emploiera le terme de « cyber-agression » qui couvrira pour nous ici un large spectre, allant de la délinquance individuelle aux attaques massives portées par des organisations criminelles ou des Etats. Le phénomène a pris une ampleur

considérable à l'échelle internationale à compter des années 2000[19]. Afin de disposer de quelques points de repères, on peut retenir la typologie proposée par l'analyste Myriam Dunn Cavelty du Center for Security Studies de Zürich en 2010. Celle-ci a distingué cinq grands types d'atteintes : le cyberhacktivisme, le cybercrime, le cyberespionnage, le cyberterrorisme, enfin la cyberguerre. Comme toute taxinomie, celle-ci peut être discutée, dans la mesure, par exemple où le cyberespionnage et le cyberterrorisme relèvent assurément de la cybercriminalité ou encore dans la mesure où le cyberhacktivisme peut aussi entrer dans une catégorie, large, de criminalité. Enfin la notion de cyberguerre peut être discutée (Ventre, 2014) ou réinsérée dans une catégorie plus large de cyberconflictualité. Quant au cyberterrorisme, c'est une notion qui en soi pose un véritable problème car les formes des actions terroristes dans l'environnement cyber ne nous semblent pas spécifiques par rapport au hacking. Quoi qu'il en soit, nous conserverons le terme de cyber-agression car il englobe l'ensemble des phénomènes décrits par Dunn Cavelty. D'un point de vue plus général, il serait possible de bâtir des catégories plus fines en distinguant quatre niveaux : l'auteur, le procédé, la victime ou la cible, les effets, mais ceci n'est pas du propos de cette analyse.

Il reste qu'aujourd'hui la cybercriminalité qui ne peut être sérieusement mesurée (cf. *infra*), semble être, de loin, l'atteinte la plus courante et la plus fréquente dans l'environnement cyber, notamment lorsqu'elle touche les individus. On peut en donner une définition simple, issue d'une approche juridique : « La cybercriminalité concerne l'ensemble des infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau »[20]. Cette perspective claire s'inscrit dans le cadre pénal français et ne vaut, bien évidemment, que pour lui. Il faut ajouter qu'il s'agit d'une criminalité faiblement, voire nullement cinétique. Ceci signifie qu'elle touche principalement au patrimoine informationnel des personnes physiques ou morales, ce qui se traduit en droit français par les notions d'atteinte à l'image, à la réputation ou encore à l'identité des victimes. Une autre singularité de la cybercriminalité c'est qu'elle est très souvent transfrontalière (on reviendra sur ce point en 3.2) ce qui, outre le problème majeur d'attribution, entrave fortement l'efficacité des poursuites judiciaires. Selon le colonel de gendarmerie Eric Freyssinet, il s'est développé « un véritable écosystème criminel autour du numérique »[21]. Les cyber-agressions ne sont plus seulement ponctuelles ou le fait de délinquants/criminels qui utilisent l'environnement cyber pour y commettre des infractions, mais des organisations criminelles souvent assez classiques se sont désormais spécialisées pour agir de façon exclusive dans cet environnement ou, à tout le moins, pour en faire la source principale de leurs profits. Le développement de telles pratiques doit autant à l'apparition de cet « écosystème criminel » qu'à l'affaiblissement de la sécurité, tant vis-à-vis des atteintes par des groupes criminels que par des États. Selon une étude de la société Skyhighnetworks datant d'août 2014

[19]. Eric Freyssinet, *La Cybercriminalité en mouvement*, Paris, Hermès Science Publication, "Management et informatique", 2012, p. 21.
[20]. Myriam Quéméner et Joël Ferry, *Cybercriminalité : défi mondial*, Paris, Economica, 2009, p. 2.
[21]. Eric Freyssinet, *La Cybercriminalité en mouvement*, Paris, Hermès Science Publication, "Management et informatique", 2012, p. 15.

conduite sur 2100 entreprises stockant leurs données à l'extérieur, moins de 1% respectaient le dispositif de protection des données en cours d'élaboration par l'UE, moins de 12% cryptaient et 72 % des clouds « européens » stockaient aux États-Unis. Une question demeure : quelle est l'ampleur des cyber-agressions ? Si tout un chacun, personne physique ou morale, a pu en faire l'expérience, on manque d'une évaluation fiable ou même d'un ordre de grandeur. Périodiquement, des évaluations sont rendues publiques, mais elles sont le fait de sociétés privées éditrices de solutions de cybersécurité comme Kaspersky, Symantec, McAfee ou Cisco notamment. Il y a un doute légitime sur la possibilité d'extrapoler leurs constats dans le temps comme dans l'espace.

Les cyber-agressions pratiquées par les États posent des problèmes spécifiques. L'environnement cyber brouille la distinction fondamentale du temps de paix et du temps de guerre. Dès lors, il est difficile de distinguer ce qui peut être qualifié de cybercrime ou de cyberguerre. Le problème central de la difficulté d'attribuer une attaque informatique à son auteur (qu'il soit étatique ou non) rend la question plus complexe encore. Il reste que les États ont recours aux attaques informatiques pour régler une partie de leurs différends. Selon une étude menée sur un peu plus d'une décennie, depuis 2001 sur 124 États frontaliers, 20 États ont eu recours au conflit numérique lors de 95 cyberconflits (Valeriano and Maness, 2013). On voit là l'intensité de la mobilisation des États dans l'environnement cyber qui explique probablement en partie l'intensité de la militarisation des structures étatiques cybernétiques (cf. *infra* en 2.4). C'est aussi l'indice d'une certaine banalisation de la conflictualité cybernétique qui semble être devenu un outil de conflictualité classique.

2. L'état actuel de l'environnement cyber

Le cyber est un champ de forces : il est le résultat des positions et des actions respectives des acteurs non-étatiques et étatiques mises en œuvre par eux dans l'environnement cyber. Dans la perspective de dégager des horizons à visée stratégique, il est crucial de prendre la mesure des grandes lignes de forces de cet environnement.

2.1. Les multiples balkanisations

Le terme de « balkanisation » est aujourd'hui couramment employé pour désigner l'évolution du réseau mondial vers un type de structuration de plus en plus fragmenté. Cette dé-structuration caractérisée par un cloisonnement de différents réseaux nationaux et/ou régionaux est totalement éloignée de l'idée originale de ceux qui, dans les années 1990, aux débuts de l'expansion mondiale, ont pensé un Internet global et uni, surmontant les barrières linguistiques, juridiques et politiques pour créer un réseau authentiquement mondial (cf. *supra* en 1.2.).

2.1.1. Les ambiguïtés de la vision d'un Internet unifié

Cette dernière vision s'appuyait sur une architecture composée uniquement par des flux ayant notamment pour conséquence (sinon pour objectif[22]) de dévitaliser tout ce qui dépendait et relevait de structures étatiques verticales et centralisées. Elle demeure pour autant vivace, non seulement parmi les pionniers, mais aussi parmi les acteurs économiques liés peu ou prou principalement aux États-Unis (cf. *infra* en 2.4.), ainsi que parmi des acteurs non-gouvernementaux, particulièrement chez les militants ne partageant pas tout, loin s'en faut, la vision de l'anglosphère. Il est particulièrement important de comprendre les nuances de la vision d'un Internet « uni » et de ne pas le caricaturer. En fait, l'Internet, puis le Cyberespace ont été conçus comme des systèmes réticulaires que des acteurs collectifs (libertaires, ingénieurs, sécuritaires, puis économiques) aux intérêts et idéologies différents ont investi de finalités distinctes et qu'ils ont développé tout en maintenant une interopérabilité minimale grâce aux organismes de gouvernance techniques *ad hoc* (cf. *supra* en 1.1) composant la cybersphère originelle.

Il reste qu'en 2015 la balkanisation est bien réelle : à l'image de la concurrence pure et parfaite dans la théorie néo-classique qui n'existe que dans la pensée économique, l'Internet unifié, neutre et ouvert n'existe que dans le domaine éthéré des idées et il joue en fait un véritable rôle ideal-typique. Il correspond à l'Internet des origines, celui des années 1990, aujourd'hui idéalisé. Il faut ajouter que cet Internet

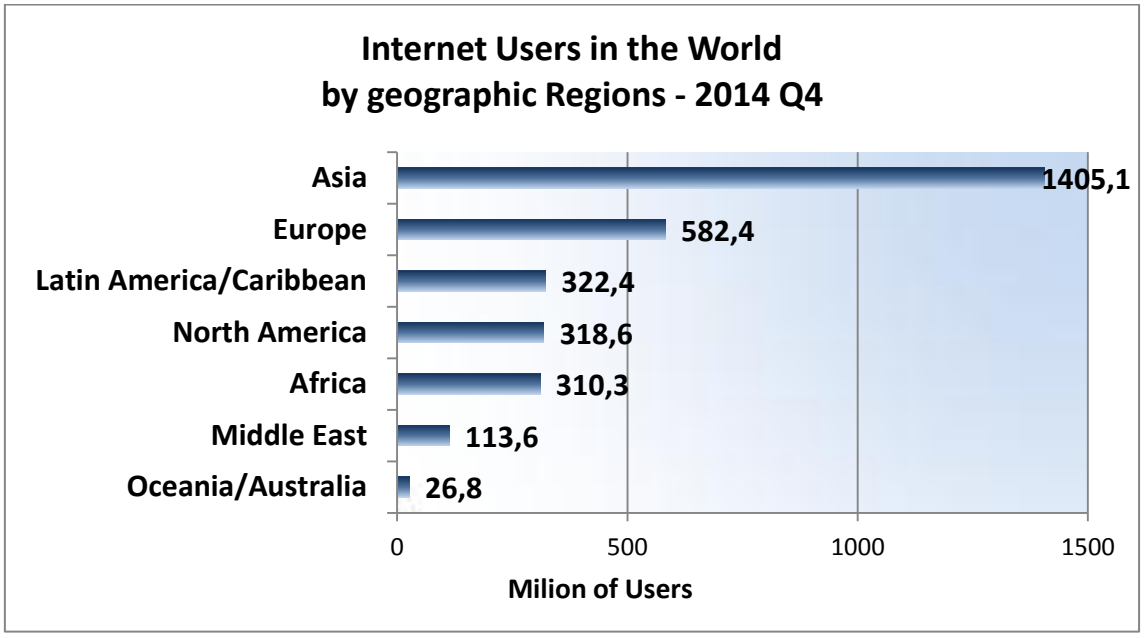
[22]. On n'abordera pas ici cette question centrale et malheureusement sous-étudiée.

était en fait principalement celui des États-Unis, à une époque où le réseau n'existait pas à l'extérieur. Dès lors, on peut se demander si l'Internet unifié à l'heure de son expansion mondiale, a un jour existé. La balkanisation n'a-t-elle pas accompagné l'expansion mondiale du réseau ? La question est d'importance car elle replacerait l'idée d'un Internet unifié dans un contexte purement idéel, loin de la réalité. Quoi qu'il en soit, à rebours de cette vision, la réalité correspond aujourd'hui à un Internet fragmenté. Le processus est en cours et il résulte des phénomènes de fragmentation très divers aussi bien *bottom-up* que *top down*.

2.1.2. La balkanisation linguistique *bottom-up* de l'Internet

Pensé depuis les États-Unis pour un monde global qui ne pouvait être qu'anglophone, l'Internet devait être nécessairement « uni » et « unifié », c'est-à-dire être un Internet utilisant des outils, notamment des moteurs de recherche, en Anglais. Or ce que l'on constate est que la part de l'Internet anglophone ne cesse de se réduire : il y a là un incontestable premier niveau de balkanisation, celle opérée sur un plan linguistique. On assiste en effet à la réduction du nombre d'internautes anglophones : ils étaient 50 % en 2001, ils n'étaient plus que 25% en 2011. Incontestablement la possibilité depuis 2005 du nommage de noms de domaines en d'autres langues que l'anglais, y compris pour des alphabets non occidentaux en pouvant utiliser des idéogrammes, a fortement joué. On voit dans le graphe suivant tiré d'Internet World Stats, l'effet en 2014 de cette évolution linguistique. Contrairement à ce que l'on croit communément, l'Internet anglophone et occidental est aujourd'hui minoritaire - compte tenu du fait qu'une partie des usagers en Europe utilise l'alphabet cyrillique. Si l'Anglais s'est imposé comme *lingua franca* dans le domaine des affaires et de la vie quotidienne, il n'a pas l'ampleur que l'on croit dans l'Internet.

Graphe 5 : nombre d'usagers de l'Internet par aires géographiques



Source: Internet World Stats – www.internetworldstats.com/stats.htm
3,079,339,857 Internet users estimated for Dec 31, 2014

Tableau 3 : part d'usagers de l'Internet par aires géographiques

Regions	users %
Asia	**45.6 %**
Europe	**18.9 %**
Latin America / Caribbean	**10.5 %**
Africa	**10.3 %**
North America	**10.1 %**
Middle East	**3.7 %**
Oceania / Australia	**0.9 %**
World total	**100.0 %**

Source : http://www.internetworldstats.com/[22/07/2015]

Cette diversité linguistique a un effet qui n'est pas seulement culturel. Il a une portée numérique et économique : en 2013, le moteur de recherche Baidu détenait 78 % du marché chinois et le moteur Yandex 60 % du marché russe[23]. Qui plus est, dans ces pays, les déclinaisons des moteurs de recherche occidentaux (Google, Yahoo…) font l'objet d'une attitude hostile des États afin d'en limiter l'implantation.

Il est nécessaire par ailleurs de se livrer à l'évaluation de l'évolution linguistique de l'Internet global. Les taux de pénétration indiqués par Internet World Stats (cf. tableau 4 et graphe 6 suivants) permettent de constater les fortes marges de progression selon les continents et les aires linguistiques. Les trois continents anglophones sont aux trois quarts pénétrés par l'Internet. L'Amérique du Nord, presque totalement anglophone (malgré la présence de près d' 1/5^{e} d'hispaniques aux États-Unis, mais qui sont en grande partie dans une situation de bilinguisme) a presque atteint son maximum. En outre, ainsi que nous l'avons écrit plus haut, l'Europe n'est que partiellement anglophone dans ses usages de l'Internet. Par ailleurs à 35 % de taux de pénétration en Asie, l'Internet sinophone a une énorme marge de croissance devant lui. Ceci va nécessairement continuer d'accroître le recul de l'Internet anglophone. Il ne faut pas oublier en outre l'importance numérique considérable de la diaspora chinoise et du *soft power* de la RPC qui a implanté des dizaines d'Instituts Confucius bien au-delà du Sud-est asiatique. L'Internet sinophone déborde très largement du seul territoire chinois. Enfin l'espace méso-américain et latino-américain a un taux de pénétration de moitié, ce qui indique une forte progression possible, soit

23. Bruno Sido et Jean-Yves Le Déaut, *Le risque numérique: en prendre conscience pour mieux le maîtriser ?*, Assemblée nationale n° 1221-Sénat n° 721, 3 juillet 2013, OPECST, p. 13.

d'un Internet hispanophone, soit d'un Internet lusophone si le sous-continent souhaite se défaire des outils étatsuniens (dits « globaux » en apparence…). Bien évidemment pour les non-anglophones *natives*, les usages de l'Internet sont fondés sur le bilinguisme. Mais ils indiquent d'ores et déjà que la domination des outils étatsuniens n'est pas absolue, loin s'en faut. D'autre part, on observe que le niveau des pratiques de bilinguisme dépend de ce qui est recherché par les Internautes. Or pour la majorité des populations, les pratiques quotidiennes d'Internet sont liées à la vie courante et donc à l'aire culturelle et linguistique dans laquelle elles se trouvent. Elles utilisent pour ce faire des moteurs de recherche et des réseaux sociaux endogènes et indépendants économiquement et en contenu, des *majors* étatsuniennes.

Certains analystes évoquent le ralentissement dans le court terme de la progression générale de l'Internet, notamment dans les régions non occidentales. Ce constat qui n'est pas faux résulte de l'échelle de temps sélectionnée : sur une période quinquennale, la progression continue à être forte sinon manifeste. Le constat de court terme s'explique principalement par les limites de l'expansion des infrastructures du réseau et de la connectivité dans les pays moins développés. Ce fait doit être fortement nuancé par les progrès continus effectués en Afrique (y compris dans le court terme) d'une part et par l'action des *majors* pour étendre la connectivité (notamment le projet « Loon » de Google depuis 2013 et le projet de web drone « Aquila » de Facebook développé depuis mars 2014) de l'autre. Les projets d'Internet spatial de certaines sociétés étatsuniennes, s'appuyant sur non plus sur la fibre optique sous-marine, mais sur le satellite permettant de contourner les faiblesses ou les interdits de certains États, laissent augurer d'une poursuite de la connectivité mondiale.

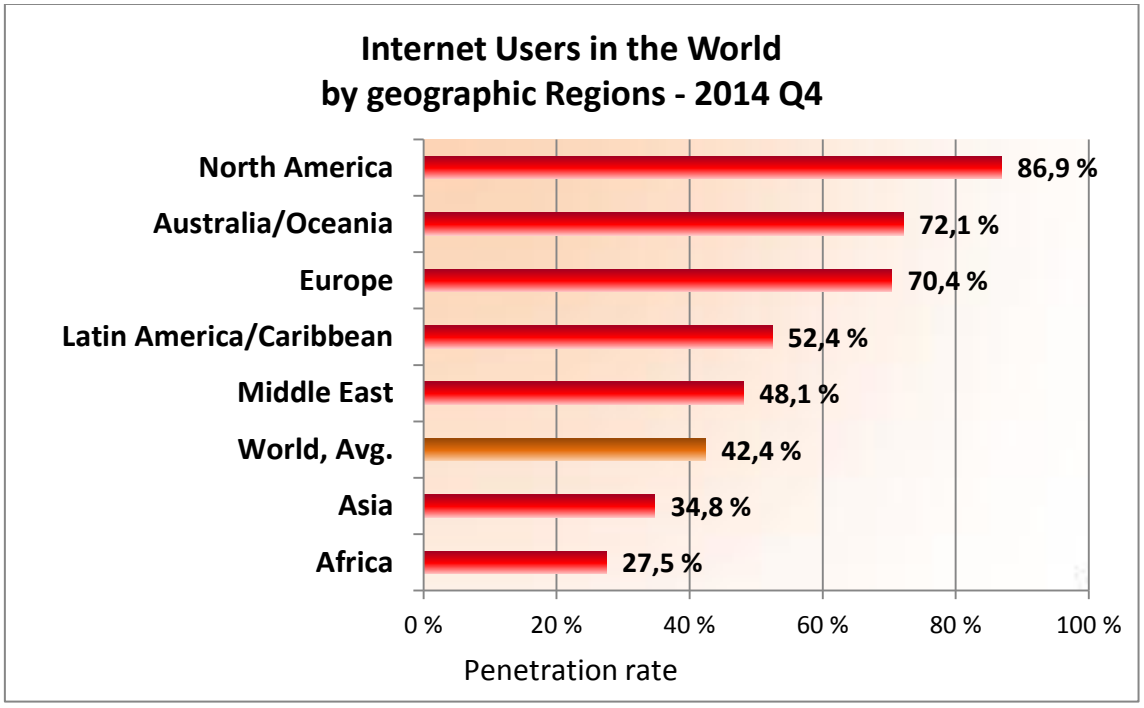
Ainsi, les usages linguistiques et culturels façonnent aussi le réseau et partant ont un impact direct sur l'architecture de son économie. Ainsi, une balkanisation linguistique *bottom up* s'opère-t-elle lentement qui est la plus structurante et durable des fragmentations du Cyberespace.

Tableau 4 : taux de pénétration de l'Internet par aires géographiques

World Regions	**Penetration (% pop)**	**Growth (2000-2015)**
North America	86.9 %	187.1 %
Oceania / Australia	72.1 %	251.6 %
Europe	70.4 %	454.2 %
Latin America / Caribbean	52.4 %	1,684.4 %
Middle East	48.1 %	3,358.6 %
Asia	34.8 %	1,129.3 %
Africa	27.5 %	6,958.2 %
World total	**42.4 %**	**753.0 %**

Source : http://www.internetworldstats.com/ [22/07/2015]

Graphe 6 : taux de pénétration de l'Internet par aires géographiques



Source: Internet World Stats – www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,264,623,793
And 3,079,339,857 estimated Internet users on Dec 31, 2014
Copyright© 2015, Miniwatts Marketing Group

2.1.3. La balkanisation *bottom-up* de l'architecture de l'Internet par concentration économique

Une deuxième forme de balkanisation *bottom-up* peut être observée lorsque l'Internet est envisagé d'un point de vue économique. Elle est le fait des acteurs économiques et industriels privés et publics qui ont la capacité de produire les éléments fondamentaux permettant de bâtir le réseau dans la couche physique. Ainsi les producteurs de tout ce qui touche au *hardware* de l'informatique et du réseau de l'Internet et du cyberespace sont *de facto* en position d'influer sur le système en termes très classiquement géostratégiques. Ce qu'il importe de relever à ce stade, ce n'est pas la structure économique oligopolistique qui est secondaire ici, mais le fait que la possession très inégale a un effet considérable sur la propriété concrète du réseau et par conséquent sur les capacités d'agir dans la couche sémantique. Les internautes ont en fait le sentiment que le réseau est libre parce qu'il est quasiment gratuit et qu'il n'y a pas d'octroi ou de péage, seul l'accès et quelques services étant payants. Ceci est une illusion car l'architecture physique du réseau est en fait très polarisée sur quelques grands acteurs privés ou publics étatsuniens, chinois et russes dans une moindre mesure.

2.1.4. La balkanisation politique *top down* de l'Internet

Créé par des acteurs privés et publics par les États-Unis pour être un outil de *soft power*, l'Internet a longtemps été ignoré par les autres États. Ceux-ci ont fait leur arrivée (et non leur « retour », terme improprement employé usuellement) tardivement, mais ils ont malgré cela fortement investi depuis le champ de l'Internet et plus largement du cyberespace (cf. *infra* en 2.5) en rattrapant en quelque sorte leur retard. Les États ont ainsi été les agents d'une fragmentation *top down* de l'Internet.

Il faut cependant distinguer la responsabilité des États à cet égard selon leur taille et leur modèle politique. Les États ayant une influence sur l'Internet sont ceux qui ont les capacités technologiques d'influer sur son architecture. Ceux d'entre eux qui ont une forme non démocratique et/ou autoritaire ont tenté, avec succès, par exemple dans le cas de la Chine ou de l'Iran, de créer des architectures propres, permettant de limiter et de contrôler l'interopérabilité du réseau de l'Internet national avec l'Internet global. L'objectif est de contrôler et au besoin de censurer l'Internet dans sa dimension d'espace informationnel. D'autres États, à régime démocratique, ont aussi contribué à balkaniser l'Internet en adoptant des normes contraignantes dans un environnement qui a été conçu à l'origine non seulement pour être ni contrôlable, ni sécurisable, ni même normalisable. Les normes contraignantes sont toutefois rares et très inégalement adoptées d'un point de vue géographique (cf. *infra* 2.3 et 3.2). D'autre part, la capacité des organisations internationales à faire respecter ces normes est faible. Mais elles dessinent tout de même deux grands ensembles d'Internet, ainsi qu'on le verra plus loin à l'aide de cartes, qui polarisent ou qui repoussent l'attractivité, laissant apparaître les structures d'une géopolitique du cyberespace.

Ainsi dans le cyberespace où l'expression la plus fréquente est celle de dé-territorialisation, des territoires numériques sont apparus principalement dans la couche sémantique. La balkanisation est donc une réalité actuelle incontestable. Rien n'indique que ce mouvement évolue à l'avenir en s'affaiblissant (cf. *infra* en 4.3).

2.2. Une domination étatsunienne multi-couches persistante

En dépit de la balkanisation évoquée plus haut, en particulier dans son volet linguistique, en dépit des progrès du cyber chinois, l'environnement cyber mondial est encore fortement polarisé par les États-Unis qui le dominent sans conteste. Cette domination s'appuie sur des ressorts technologiques et économiques et se décline dans les trois couches. Qui plus est, cette situation qui la met en surplomb est ancienne dans la mesure où l'Internet a été créé sur le territoire des États-Unis il y a une quarantaine d'années. La solidité de la domination étatsunienne tient aussi au mélange d'acteurs privés et publics du cyber qui lui confèrent une force particulière. En effet, l'environnement cyber mondial actuel est le résultat d'initiatives privées étatsuniennes développées avec l'appui et la protection de l'État fédéral qui, au tournant des années 1990 avec l'expansion mondiale du réseau, a parfaitement anticipé qu'il constituait à la fois un secteur économique propre et nouveau à portée mondiale particulièrement

innovant, mais également un outil apte à être utilisé par les autres activités économiques.

La couche physique est encore largement maîtrisée par les États-Unis. La grande majorité des serveurs racines du DNS (administré par l'ICANN) - 10 sur 13 - sont aux États-Unis. D'autre part, ce pays conserve avec les sociétés Cisco, Juniper et Alcatel-Lucent une domination sur les routeurs et notamment les routeurs cœur de réseau. Alors que plus de 90 % du trafic Internet passe par des fibres optiques sous-marines, les États-Unis qui ont constitué le réseau de *backbones* depuis leur continent ont pu faire en sorte que plus de 70 % du trafic passe par leur pays. Le reste du trafic, marginal, passe par les satellites où la domination étatsunienne est constante depuis les années 1960. Si la Russie, le Japon et l'Europe se sont mobilisés depuis, 200 satellites de communication sur les 400 qui sont actuellement en service appartiennent aux États-Unis[24]. La couche logique présente des caractéristiques analogues. Ainsi en France en 2015, 77% des logiciels utilisés quotidiennement étaient importés des États-Unis[25]. Pour ce qui est des moteurs de recherche, Google a 90 % de parts de marché dans le monde (inégalement réparties on l'a vu) et 93 % en Europe. Les fournisseurs de contenus sont issus soit des *majors* des États-Unis (GAFA qui représente une capitalisation boursière de 1 500 milliards de $ en 2015), soit des industries de l'information et de l'*entertainment* qui se sont numériseés. Ainsi dans la couche sémantique, une structure oligopolistique principalement étatsunienne s'est formée qui renforce les caractéristiques des couches physique et logique. Lors de la séance d'ouverture du premier IGF français qui s'est tenu au CESE le 10 mars 2014, l'informaticien Louis Pouzin, qui a été l'un des concepteurs des protocoles TCP/IP, a souligné que les États-Unis étaient persuadés que l'Internet leur appartenait, notamment les membres du Congrès[26]. On peut donc s'interroger sur les raisons pour lesquelles ce pays amoindrirait sa position dominante, par exemple en abandonnant la fonction IANA qui a été plusieurs fois annoncée dans le passé[27]. Peu importe qu'elle soit estimée moins stratégique qu'auparavant, le vote du Congrès sera décisif pour montrer la conception que la première puissance mondiale se fait de l'environnement cyber. Enfin la suprématie des États-Unis peut également être constatée en matière de surveillance (cf. *infra* en 4.2.5). Le réseau d'interceptions « five eyes » bâti par la NSA dès les débuts de la guerre froide donne à ce pays une capacité géographique d'interception mondiale que ni la Chine, ni la Russie ne peuvent lui contester. On sait depuis l'été 2013 que derrière un discours la justifiant pour des impératifs de sécurité (lutte contre le terrorisme), il s'agit en fait d'amasser et de traiter de la *data*, notamment pour des raisons d'espionnage économique bien classique. Dès lors on peut se demander si l'Europe n'est pas alors composée de « colonies numériques » pour reprendre l'expression employée en 2014 par la sénatrice française Catherine Morin-Desailly[28]?

[24]. Entretien de l'auteur avec le Dr Hamadoun Touré, secrétaire général de l'UIT, 17 mars 2014. Cf. également (Boulanger, 2014) qui indique une proportion plus grande encore, de 3/4.

[25]. Cf. Nicolas Brizé (ed.), *Souveraineté numérique : quels enjeux pour l'économie française ?*, Assises de la souveraineté numérique, 2015, p. 22.

[26]. 1er IGF, CESE, 10 mars 2014.

[27]. Entretien de l'auteur avec le Dr Hamadoun Touré, secrétaire général de l'UIT, 17 mars 2014.

[28]. Catherine Morin-Desailly, *Rapport d'information fait au nom de la mission commune d'information*

2.3. Le débarquement tardif mais réussi des États dans le cyberespace

Selon Milton Mueller (Mueller, 2010) l'Internet est par nature une contrainte pour les États. Son essai résume parfaitement une vision des choses couramment répandue selon laquelle tout opposant par nature les structures verticales régaliennes et la scissiparité naturelle du système de systèmes d'information qu'est l'environnement cyber, les États seraient incapables de s'y mouvoir. Les arguments de Mueller sont les suivants. C'est en premier lieu parce qu'il globalise la communication des États, la rendant plus difficile et plus coûteuse que ceux-ci ont été déstabilisés par l'Internet. D'autre part, le réseau favorise la création d'une industrie mondiale de l'information avec des capacités de stockage et de gestion des flux nouvelles auxquelles la plupart des États ont des difficultés à faire face. Par son architecture décentralisée, le cyber est d'une conception radicalement différente des États. Le cyber a suscité ses propres organisations spécifiques à distance des États. Enfin, le principe de la gouvernance internationale *multistakeholder* relativise par nature le rôle des États. On peut discuter cette analyse qui paraît aujourd'hui – en 2015 - assez datée. Car Mueller a écrit son ouvrage au moment précisément où les États arrivaient en force dans l'environnement cyber, montrant qu'ils avaient – du moins certains d'entre eux – la capacité de s'adapter à des structures et des règles qui effectivement étaient pensées en dehors d'eux.

Nous n'avons pas la place ici d'engager une longue discussion sur le moment qui a cristallisé l'arrivée des États. Il importerait pourtant que ce travail soit conduit avec précision car c'est un basculement dans le système informationnel international et dans le système international tout court. Pour certains analystes, c'est lors de la conférence de Dubaï en 2012 que les États auraient fait leur « retour ». Nous préférons le terme « d'arrivée » dans la mesure où les États ne s'étaient auparavant que très modérément intéressés à cet environnement. Le mot de « débarquement » employé dans le titre du 2.4. rend compte d'une réalité soudaine et militaire correspondant précisément à l'action d'un certain nombre d'États et que nous expliquons plus loin. Enfin, il faut garder présent à l'esprit qu'un seul État, celui des États-Unis, y était présent dès les origines de l'Internet (cf. *supra* 2.4). Pour revenir au moment d'intervention des États dans l'environnement cyber, le phénomène qui s'est cristallisé publiquement au moment de Dubaï, lui est antérieur. C'est en 2011 que les États ayant des capacités cybernétiques importantes, les États-Unis, la Grande-Bretagne, la France et l'Allemagne publient leurs stratégies nationales cyber, aboutissement de la création de structures et de financement de moyens *ad hoc* commencés à moyen terme. Si on étend l'analyse à la cybersécurité, on constate que la plupart des États de l'OCDE ont défini des politiques publiques (par ailleurs convergentes) en la matière entre 2009 et 2011 (OECD, 2012). C'est donc de la fin de la décennie 2000 qu'il faut dater le débarquement des États dans l'environnement cyber.

Finalement l'intérêt des États a été manifesté très concrètement par l'ampleur des moyens financiers et technologiques qu'ils ont consacré à l'environnement cyber.

---

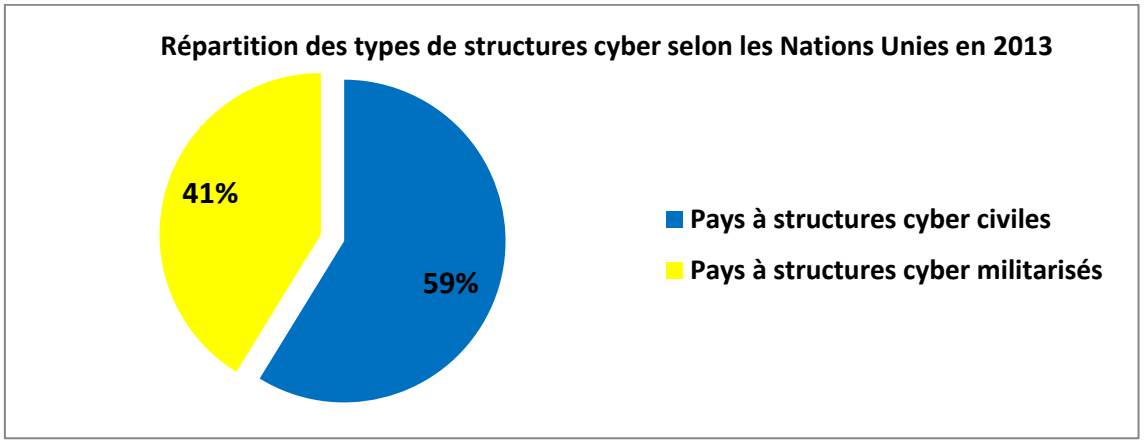
sur le « nouveau rôle et la nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », Sénat, n° 696, 8 juillet 2014, 398 p

Ainsi qu'on l'a vu en introduction la transversalité de cet environnement, sa part informationnelle en font un enjeu majeur pour les États. Mais plus fondamentalement, le cyber offre une ressource nouvelle pour certains États leur permettant d'exprimer leur influence et d'y exercer éventuellement leur puissance. Le cyber est en effet un environnement non conventionnel utilisé par les États qui ont des capacités technologiques et essaient de jouer du caractère apparemment anomique du système pour mettre en œuvre des modes d'actions irréguliers ou peu licites (cf. *infra* en 3.2 et 3.3). De ce point de vue l'absence de règles et de juridictions spécifiques est aussi de leur intérêt. Il est intéressant de noter l'implication des appareils militaires nationaux dans le cyberespace. D'après l'United Nations Institute for Disarmament Research (UNIDIR) de l'ONU, en 2012 sur 193 États, 114 avaient des programmes de cybersécurité dont 47 étaient assurés par l'autorité militaire et 67 par l'autorité civile[29]. Ceci est confirmé par exemple dans le cas français par les études ayant montré les ressorts de l'avance des militaires vis-à-vis des civils (Ocqueteau-Ventre, 2014). Ce qui frappe dans le rapport de l'UNIDIR est la proportion importante – plus de 40 % – de structures militarisées. Ceci est d'autant plus marquant qu'elles ont été mises en place dans des délais très courts.

Tableau 5 : répartition des types de structures cyber selon les Nations Unies

Pays à structures cyber civiles	67	58,77 %
Pays à structures cyber militarisés	47	41,23 %
Total	**114**	**100,00 %**

Source : UNIDIR, *The Cyber Index. International security Trends and Realities*, United Nations, New York and Geneva, 2013, 138 p.



29. UNIDIR, *The Cyber Index. International security Trends and Realities*, United Nations, New York and Geneva, 2013, p. 1.

Encart 1 : pays à structures cyber militarisées selon les Nations Unies

Afrique du Sud, Albanie, Allemagne, Argentine, Australie, Autriche, Biélorussie, Brésil, Canada, Chine, Colombie, Croatie, Cuba, Corée du Nord, Corée du Sud, Danemark, Espagne, Estonie, États-Unis, Fiji, Finlande, France, Géorgie, Grèce, Hongrie, Inde, Indonésie, Iran, Israël, Italie, Japon, Kazakhstan, Lituanie, Malaisie, Myanmar, Norvège, Pays-Bas, Pologne, Royaume-Uni, Russie, Singapour, Slovaquie, Sri Lanka, Suisse, Turquie, Ukraine, Vietnam.

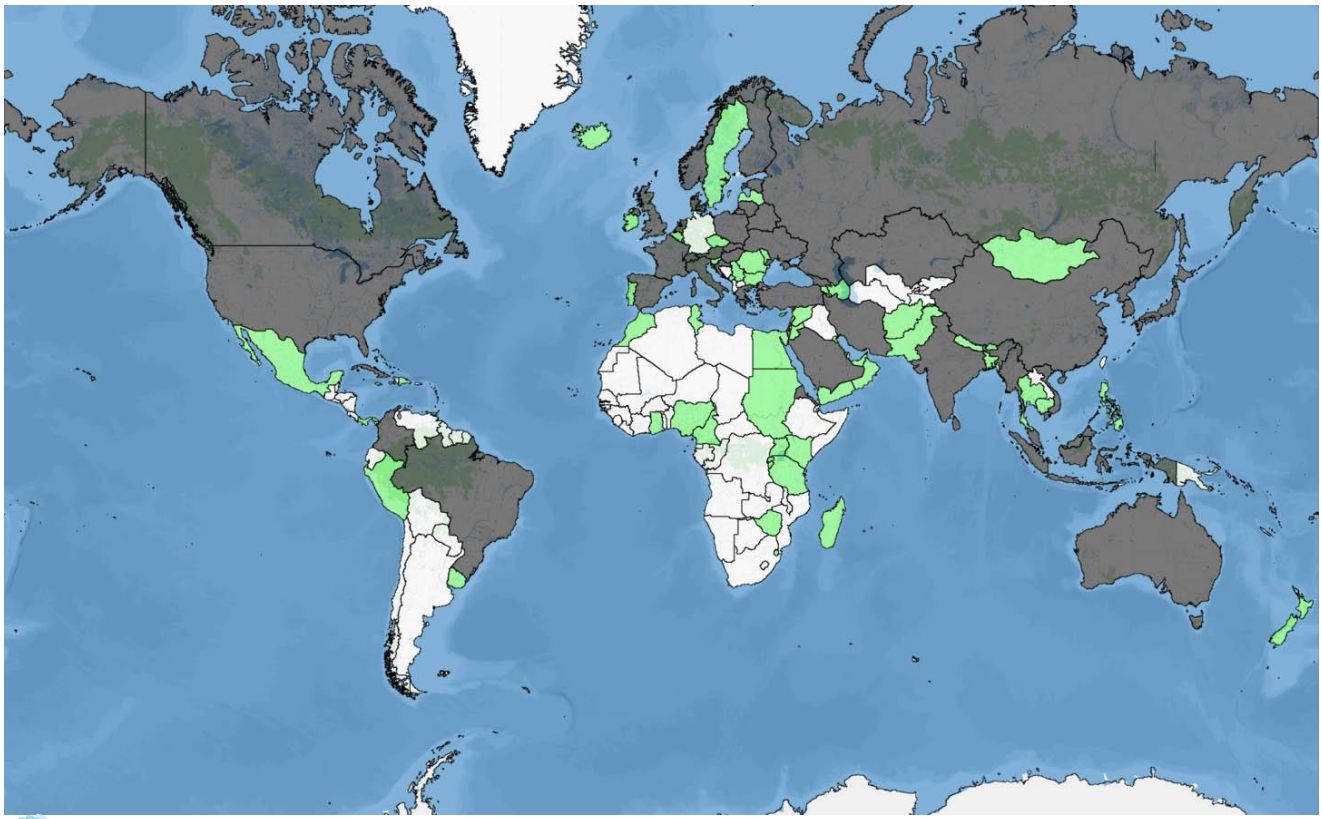
Source : UNIDIR, *The Cyber Index. International security Trends and Realities*, United Nations, New York and Geneva, 2013, p. 9-55.

Encart 2 : pays à structures cyber civiles selon les Nations Unies

Afghanistan, Antigua et Barbade, Arabie Saoudite, Arménie, Azerbaïdjan, Bangladesh, Belgique, Bhoutan, Bruneï, Bulgarie, Burundi, Cambodge, Cameroun, Chypre, Egypte, Emirats Arabes Unis, Ethiopie, Ghana, Grenade, Irlande, Islande, Jamaïque, Jordanie, Kenya, Koweït, Lettonie, Liban, Liechtenstein, Luxembourg, Madagascar, Maldives, Malte, Maroc, Maurice, Mexique, Moldavie, Mongolie, Monténégro, Népal, Nouvelle-Zélande, Nigeria, Oman, Ouganda, Pakistan, Panama, Pérou, Philippines, Portugal, Roumanie, Rwanda, Quatar, République dominicaine, République tchèque, Saint-Vincent et les Grenadines, Serbie, Slovénie, Soudan, Swaziland, Suède, Syrie, Tanzanie, Thaïlande, Trinidad et Tobago, Tunisie, Uruguay, Yémen, Zimbabwe.

Source : UNIDIR, *The Cyber Index. International security Trends and Realities*, United Nations, New York and Geneva, 2013, p. 55-90.

Carte 1 : nature des structures cyber dans le monde



N.B. : en gris foncé, les pays à structure cyber militarisées, en vert les pays à structure cyber civiles et en blanc les structures inexistantes ou aux caractéristiques non connues.

2.4. Les faux-semblants de la militarisation des structures cyber

Il faut toutefois relever que s'il y a plus de 40 % de structures militarisées, ceci ne signifie pas qu'elles ont toutes une finalité exclusivement militaire. En effet, les Etats qui ont fait le choix de la militarisation l'ont fait car les structures militaires y étaient le mieux à même d'assurer la sécurisation des SI fondamentaux, de mettre en place des systèmes résilients, en bref de protéger l'infrastructure informationnelle régalienne. Il y a en effet dans les SI une triple dimension : protectrice, défensive et offensive. Sur les 47 Etats possédant des structures cyber militarisées, seule une petite dizaine d'Etats ont des capacités offensives.

La géographie qui se dessine sur la carte est tout à fait éclairante et à vrai dire peu surprenante : les pays à structure cyber militaire qui figurent en gris foncé sont en majorité les pays du G 20 qui mènent une politique de puissance et ont les moyens technologiques de la mettre en œuvre dans l'environnement cyber.

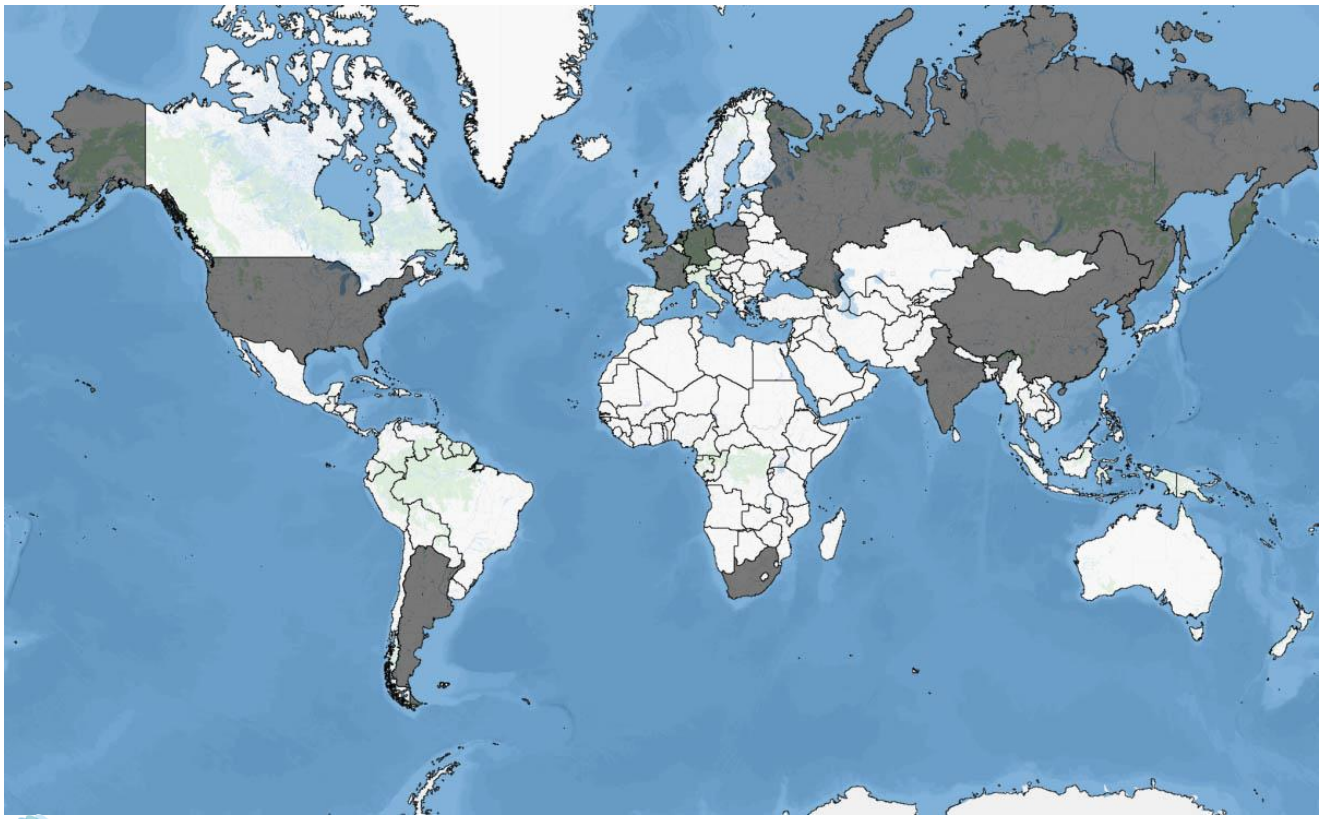
On peut compléter les observations précédentes par une représentation des pays qui ont des capacités cybernétiques offensives figurant sur la carte 2 *infra* en gris foncé. Elle s'appuie sur le rapport de l'United Nations Institute for Disarmament Research publié en 2013. Mis à part les pays permanents du Conseil de sécurité qui ont reconnu au début de la décennie 2010 qu'ils avaient ces capacités et des programmes, voire une doctrine d'emploi, les autres pays mentionnés observent une forte réserve sur le sujet, sinon une totale discrétion. Ceci ne relève pas d'une volonté de dissuasion comme on le croit souvent à tort, mais du caractère juridique encore très imprécis de l'emploi du cyber offensif : est-ce un moyen de *law enforcement* employable en dehors des frontières nationales ? est-ce un acte de guerre ? faut-il que l'acteur de l'offensif soit apparent ou secret ? Les questions ne manquent pas et pourtant l'on sait depuis l'Estonie, la Géorgie et l'Iran que des États ont déjà employé ces moyens, quitte à les sous-traiter à des acteurs non-étatiques. Il existe déjà à ce jour une liste des conflits dans lesquels la responsabilité des États peut être identifiée (Valeriano and Maness, 2013). Il reste que la liste des pays et la carte que l'on peut en tirer (cf. encart 3 et carte 2) sont à analyser avec précaution dans la mesure où l'UNIDIR s'est appuyé uniquement sur de sources ouvertes afin d'identifier les pays concernés.

Encart 3 : États ayant des capacités cyber offensives supposées selon les Nations Unies

Afrique du Sud, Allemagne, Argentine, Chine, Corée du Nord, Corée du Sud, États-Unis, France, Grande-Bretagne, Inde, Pays-Bas, Pologne, Russie.

Source : UNIDIR, *The Cyber Index. International security Trends and Realities*, United Nations, New York and Geneva, 2013, 138 p.

Carte 2 : États ayant des capacités cyber offensives dans le monde



3. Un environnement cyber fait d'incertitudes multiples

Face à l'environnement cyber les acteurs étatiques et les acteurs non étatiques sont très inégaux, du moins si l'on considère le petit nombre d'États qui ont d'authentiques capacités technologiques et financières. L'inégalité entre les deux grandes catégories d'acteurs tient au fait que les acteurs non-étatiques sont plus fortement exposés aux incertitudes structurelles de l'environnement cyber. Celles-ci sont présentes dans les trois couches. A l'heure où le discours sur la cybersécurité est envahissant, il est indispensable d'avoir conscience des fragilités structurelles de cet environnement.

3.1. De l'ignorance du réseau /dans le réseau à l'insécurité numérique

« Réseau de réseaux », cette appellation courante de l'Internet masque en fait une incertitude fondamentale sur la structure réticulaire elle-même. Il est bien évidemment impossible de dresser une cartographie générale de l'Internet, mais c'est aussi un défi pour des personnes morales et notamment pour des entreprises qui se sont lancées dans la transformation numérique. Ce défi s'accroît avec la taille de l'entreprise et avec le volume de ses données, mais il est déjà une réalité pour des structures de taille moyenne et intermédiaire. Il leur est en effet de plus en plus difficile de connaître leur réseau, que ce soit du point de vue de sa dimension, des interconnections et même de la localisation physique. Pour le seul exemple des Internet eXchange Point (IX – IXP) qui sont un aspect central dans l'architecture du système et des flux, l'incertitude est grande dans les travaux d'expertise et académique les plus sérieux : ainsi il y aurait dans le monde 357 IXP en 2011 selon (Weller-Woodcok, 2013) ou seulement une centaine en 2013 selon (De Nardis, 2014). Le facteur 3 n'ayant aucune justification sur une période de deux années, un de ces deux ordres de grandeur est manifestement faux. L'externalisation par le *cloud* des services et du stockage pour des raisons d'économie et/ou de sécurité (*sic*) a considérablement accru le problème qui est devenu un facteur absolument majeur d'incertitude pour les entreprises. Leur réseau n'est plus le leur et elles n'en ont donc plus qu'une maîtrise partielle. L'incertitude tient en partie au fait que les données ne sont stockées qu'en apparence et qu'elles circulent en fait en permanence. Les questions du dimensionnement du réseau et de la localisation des données sont des apories techniques qui exposent les personnes morales à des fragilités classiques de sécurité informatique. En effet, l'incertitude sur un réseau constitué de flux permanents rend plus fragile la confidentialité des données, leur intégrité et leur disponibilité. S'ajoute en outre une difficulté supplémentaire dans la mesure où le stockage des données sur des territoires précis les expose logiquement à la soumission au droit du territoire où est localisé le lieu de stockage. Les droits sont très inégalement protecteurs pour les données. En l'absence de droit unifié ou harmonisé

(cf. *infra* en 3.2), la balkanisation des régimes juridiques des contenus et des données produit une insécurité juridique majeure pour les personnes morales.

En outre, la numérisation de l'économie (cf. *infra* en 4.2.1.) expose les sociétés aux dangers et fragilités propres à cet environnement, principalement les *malwares* et le *hacking*. A la différence des vols et fraudes classiques, ceux qui sont opérés dans l'environnement cyber sont fondamentalement discrets. Le vol numérique étant une copie, il est difficile de constater l'atteinte au moment où elle a été effectuée. Il arrive ainsi que le constat d'une infraction soit très postérieur à sa commission, ce qui empêche d'y réagir dans une échelle de temps adaptée. Ceci a deux effets : cela peut accroître fortement le dommage et peut empêcher d'y apporter une solution adaptée (qui peut être déclassée ou inopérante lorsqu'elle est apportée très en aval de la commission). Certains *malwares* porteurs de système d'espionnage rendus particulièrement indétectables n'ont pas vocation à commettre des vols, mais simplement à observer un système ou un réseau et à pratiquer un *reporting* discret sur l'activité ou le contenu. Dans ce cas, l'infraction est bien plus grave que la seule intrusion et peut amener le dévoilement des actifs d'une société, sa stratégie ou plus généralement tous les éléments qu'elle ne souhaite pas rendre publics. Enfin, les *malwares* ont des caractéristiques qui, outre leur propre dissimulation visent aussi à dissimuler l'origine ou l'émetteur de l'intrusion et du programme. Dès lors il est difficile d'attribuer l'origine et d'engager soit des poursuites judiciaires, soit de répliquer. Ceci est une caractéristique spécifique fondamentale de l'environnement cyber.

3.2. Un environnement sans règles ?

3.2.1. L'inégale acceptation géographique de l'embryon de droit international

Un droit international spécifique à l'environnement cyber existe. Il a été discuté puis élaboré avant la très grande expansion mondiale de l'Internet et visait plutôt des infractions informatiques que des infractions liées à la circulation dans un réseau mondial. Néanmoins ce droit international s'est adapté à l'expansion cybernétique même s'il tend aujourd'hui à paraître un peu obsolète sur certains points. Il s'appuie sur deux textes signés en 1981 et 2001 dans deux configurations nettement différentes : le premier texte vise à protéger les personnes physiques à l'égard de l'utilisation de leurs données personnelles, le second a pour objet de favoriser un rapprochement entre États en matière de lutte contre la criminalité informatique.

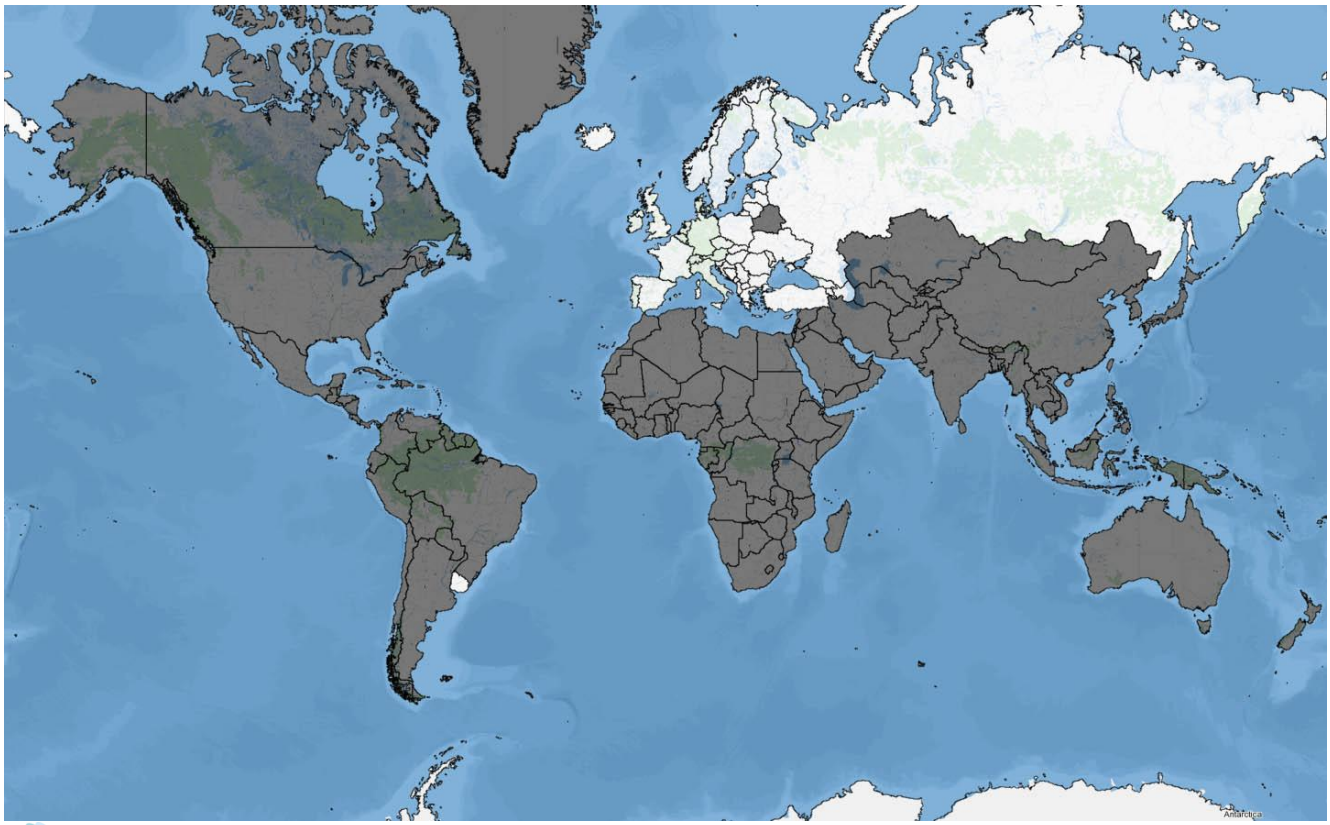
* C'est le Conseil de l'Europe qui a été la matrice de la « convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel », appelée plus souvent « convention 108 », signée en 1981. A l'époque, ce texte de 27 articles[30] s'est très fortement inspiré de la loi française « informatique et libertés » de 1978. La « convention 108 » est le seul acte international à force contraignante en matière de protection des données. Il fixe un

[30]. http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

certain nombre de principes fondamentaux en matière de protection des données (quel qu'en soit le support) des personnes physiques, celle des personnes morales relevant du droit national. La convention interdit le traitement des données sensibles (raciales, religieuses, santé…) et instaure un droit à la protection des données. Ce n'est toutefois pas un droit absolu, mais relatif qui est mis en balance avec d'autres droits. La convention 108 était et demeure le texte le plus protecteur des données personnelles existant au monde. A l'été 2015, elle avait été ratifiée par 47 pays[31] dont un seul en dehors du Conseil de l'Europe, l'Uruguay.

[31]. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=FRE

Carte 3 : pays ayant ratifié la convention 108 sur la protection des données personnelles



N.B : en blanc les pays ayant ratifié la convention 108.

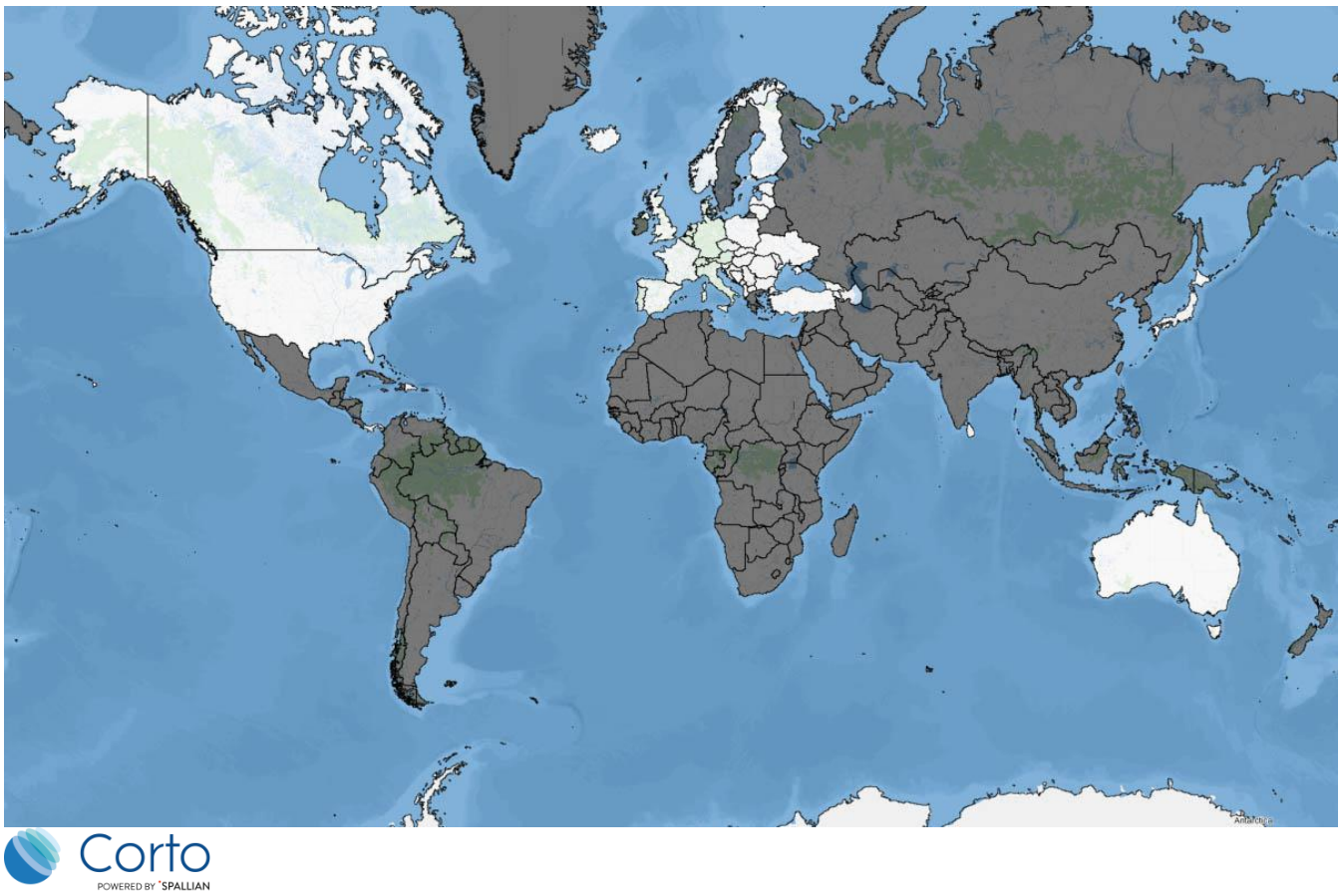
Cette géographie est très éclairante sur les zones de protection des libertés publiques en matière numérique : on peut assimiler la convention à l'Europe au sens le plus large. On y trouve tous les pays de l'Union européenne, la Scandinavie, les pays de l'ex-Yougoslavie, la Russie et certaines de ses marges (Moldavie, Géorgie et Azerbaïdjan)[32]. Le reste du monde en est totalement absent (mis à part le cas précité de l'Uruguay qui a ratifié en 2013). La carte démontre l'isolat européen et le fait que toute une partie du bloc occidental (États-Unis, Canada, Australie) a une conception moins protectrice des données personnelles numériques.

* Le second texte juridique international important en matière numérique a également été préparé sous l'égide du Conseil de l'Europe. Il a débouché sur la signature en 2001 de la « convention sur la cybercriminalité » dite « convention de Budapest » entrée en vigueur en juillet 2004. Ce texte de 48 articles visait principalement à l'harmonisation des droits pénaux en matière d'incrimination

[32]. La Turquie a signé en 1981, mais n'a jamais ratifié.

informatique et au renforcement de la coopération lors des enquêtes et des procédures judiciaires[33]. La convention de Budapest qui a montré son efficacité est aujourd'hui un outil majeur dans la lutte contre la criminalité numérique, naturellement transfrontalière. A l'été 2015, elle avait été ratifiée par 47 pays[34], dont 39 pays membres du Conseil de l'Europe, mais aussi 8 pays non-membres dont les États-Unis.

Carte 4 : pays ayant ratifié la convention de Budapest sur la cybercriminalité



N.B : en blanc les pays ayant ratifié la convention de Budapest.

A l'image de la carte représentant la ratification de la convention 108 dans le monde, celle représentant la situation de la convention de Budapest présente une forme assez tranchée. On retrouve quatre grands blocs géographiques : l'Europe, l'Amérique du Nord, le Japon et l'Australie. Si l'on resserre la focale, il faut formuler des nuances : l'Europe comprend toute l'UE (sauf la Suède) et les pays de l'ex-Yougoslavie ainsi que quelques pays d'Europe orientale (Moldavie et Ukraine), des confettis méditerranéens (Chypre et Malte) et le plateau anatolien avec une pointe

[33]. http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm
[34]. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

caucasienne (Turquie, Arménie et Azerbaïdjan). A peu de choses près, les quatre grands blocs disent une géographie qui est celle du monde développé, peu ou prou celui du G20. A contrario, les zones de non-ratification indiquent les lieux dans lesquels *de facto* le développement de la cybercriminalité peut se faire de façon relativement protégée : la Russie, l'Asie, le Moyen-Orient, l'Afrique et l'Amérique latine. On remarquera que certaines de ces zones – la Russie, l'Asie et dans une moindre mesure le Moyen-Orient – correspondent à des régions qui ont montré leur haut niveau de maîtrise des TIC.

Depuis 1981 et 2001 les discussions en vue d'améliorer le droit existant se poursuivent et un texte additionnel a été voté – en 2005 un protocole additionnel à la convention de Budapest sur « l'incrimination d'actes de nature raciste et xénophobe » –, mais le processus de modernisation de la convention 108, indispensable au regard de l'évolution permanente des TIC, lancé en 2012, a été interrompu. Par ailleurs, les ratifications ne progressent plus que très lentement : pour la convention 108, en 2013 il y avait 46 pays ayant ratifié pour 47 en 2015 et pour la convention de Budapest, 41 pays en 2014 pour 47 en 2015 mais ce texte qui est plus délicat à ratifier car il concerne du droit pénal a très probablement atteint son étiage (notamment avec les ratifications de la Pologne et du Canada en 2015). On peut en outre relever que les États-Unis l'ont ratifié en 2006 mais avec beaucoup de réserves écrites, ce qui en affaiblit l'applicabilité…

En définitive ces deux conventions internationales touchant spécifiquement à l'environnement cyber ne représentent qu'un peu plus d'un cinquième des États dans le monde, certes avec des États très puissants. Mais manquent des États tout aussi importants par leurs capacités technologiques et par leur taille (dont deux membres du Conseil de sécurité des NU, la Chine et la Russie (pour la convention de Budapest), avec des « trous noirs » géographiques qui traduisent de très importants déséquilibres mondiaux : la Russie, l'Asie, l'Afrique et l'Amérique latine demeurent des régions où le droit international ne peut entraver le développement de la cybercriminalité. Dès lors, des pôles spécialisés et des « écosystèmes » (E. Freyssinet, 2009, cf. *supra* en 1.3) de criminalité numérique s'y développent aisément. Cette situation générale affaiblit considérablement l'environnement cyber et explique en partie les **rapports de forces géo-cybernétiques**.

3.2.2. Les négociations sur un traité international peu réaliste, à l'ambition limitée

On a vu *supra* le rôle que l'ITU s'est confiée à elle-même pour l'Internet, afin notamment de concurrencer l'ONU-IGF qui avait veillé au début des années 2000 au développement de la « société de l'information » et de la « gouvernance » mondiale à cet égard. Bien que l'ITU soit depuis 1947 rattachée aux Nations Unies dont elle est désormais une organisation spécialisée, elle s'est emparée de l'enjeu cyber dans la mesure où elle est compétente en matière de télécommunications pour lesquelles elle joue un rôle de définition de normes et de standards (cf. le tableau 1 en 1.1.3.). Ainsi, elle s'est lancée à la fin des années 2000 dans une vaste réflexion internationale en vue d'aboutir à un traité spécifique pour l'environnement cyber. L'initiative s'est focalisée

autour du « Global Cybersecurity Agenda » (GCA) lancé en mai 2007 par l'organisation[35]. Il faut en premier lieu relever que les discussions sur un éventuel traité ont d'emblée été centrées sur la question de la cybersécurité qui est certes un enjeu central face à la montée des cyber-agressions mais qui laisse de côté tout ce qui a trait à la régulation générale. Il est difficile de savoir si l'ITU a préféré être prudent afin de laisser à l'IGF onusien le soin de mener une discussion plus globale, mais l'on peut observer que rien n'empêchait l'ITU malgré le RTI, vieilli, de 1988 de prendre une initiative plus ambitieuse.

Dans le cadre du GCA, une centaine de membres ont été nommés par le secrétaire général de l'ITU au sein de l' « High Level Experts Group » (HLEG), présidé par le juge norvégien Stein Schjolberg. Deux documents ont rapidement été publiés en 2008 : en août le "Chairmans Report »[36], document d'étape, puis en novembre le *Global Strategic Report*. Ce dernier rapport montre clairement les limites de la démarche du GCA dans la mesure où les 5 enjeux de négociation étaient les suivants : technical and procedural measures, legal measures, organizational structures, capacity building et international cooperation. Le HLEG entendait bien se cantonner au sujet de la cybersécurité avec une approche principalement technique. Le travail collectif s'est poursuivi et a débouché sur la publication du traité en 2009: sous le titre *A Global Treaty on Cybersecurity and Cybercrime: A Contribution for Peace, Justice and Security in Cyberspace.* Le juge Stein Schjolberg et l'universitaire Solange Ghernaouti-Hélie qui ont publié le document, ont affiché une haute ambition : dépasser la convention de Budapest qui n'était à leurs yeux qu'une convention régionale, peu ratifiée et peu mise en oeuvre[37] (cf. à ce propos….). Le texte du traité, composé de 22 articles[38] est particulièrement bref. Chaque article est une recommandation pour les États à adopter des textes de portée pénale pour chaque forme de cybercriminalité, du vol de données aux attaques massives contre les infrastructures vitales. On est immédiatement frappé par la différence avec la convention de Budapest, beaucoup plus concrète et précise. Dans les études qui accompagnent la seconde édition du traité (publiée en 2011), plusieurs études évoquent la possibilité d'un « International Criminal Court or Tribunal for Cyberspace » (ICCC). Dans l'esprit des auteurs, ce tribunal s'appuierait essentiellement sur une force coercitive, INTERPOL. Leur idée serait d'établir une subdivision du futur ICCC au centre Interpol spécialisé de Singapour qui était alors en voie de constitution pour opérer dans l'environnement cybernétique. Créé en 2014 l'INTERPOL « Global Complex for Innovation », est en fait une entité qui doit permettre de développer l'organisation internationale dans la région asiatique, de faire de la prospective en matière de « policing » et de « law enforcement », enfin de prendre en charge les questions cybernétiques. Le centre de Singapore n'est donc ni dimensionné, ni doté pour assurer la mission extrêmement ambitieuse que l'HLEG de l'ITU prévoyait de lui confier. Par ailleurs, l'ICCC, dans l'esprit de Schjolberg et Ghernaouti-Hélie, serait

[35]. Cf. Solange Ghernaouti, *Cyber Power. Crime, conflict and security in cyberspace*, Lausanne, EPFL Press, 2013, p. 407-417.
[36]. Reproduit dans : Stein Schjolberg and Solange Ghernaouti-Hélie, *A Global Treaty on Cybersecurity and Cybercrime : a Contribution for Peace, Justice and Security in Cyberspace*, 2011, p. 69-87.
[37]. *Ibid.*, p. ii.
[38]. *Ibid.*, p. 1-14.

une composante du Tribunal pénal international de La Haye[39]. Or le TPI issu de la convention de Rome n'est compétent que pour une série d'incriminations criminelles extrêmement graves (génocide, crime contre l'humanité, crimes de guerre) qui sont d'une toute autre nature que les cyber-agressions éventuellement répréhensibles dans le Traité de l'HLEG. On ajoutera que l'ITU a créé une structure dédiée à la cybersécurité « l'International Multilateral Partnership Against Cyberthreats » (IMPACT) la même année que l'HLEG. 152 pays à l'été 2015 sont membres de ce forum qui n'a pas d'autre ambition que d'être un lieu supplémentaire d'échanges de vues sans capacité à établir des mesures contraignantes.

On ne peut donc manquer d'être frappé par le caractère assez décalé de la réflexion de l'HLEG-ITU avec la réalité du système et des règles internationales. Par ailleurs, la réflexion de l'HLEG a été conduite par des experts internationaux et non des représentants des États, ce qui vidait de toute efficience ses propositions, d'autant plus qu'elles semblaient ignorer les règles du jeu international. Néanmoins, malgré ces faiblesses structurelles ce document demeure à ce jour la seule manifestation publique d'un traité dans le cyberespace. On prend ainsi la mesure de la faiblesse d'une éventuelle régulation globale dans l'environnement cyber.

3.2.3. L'improbable droit du cyberespace

On a vu *supra* que les conventions de 1981 et 2001 dessinaient une géographie d'un cyberespace régulé, mais extrêmement partiel au regard de la croissance générale de la connectivité et du nombre d'usagers (cf. *supra* en 2.1.2.). Il s'agit au fond d'un cyberespace quantitativement et géographiquement minoritaire. Demeure donc posée la question d'une régulation juridique plus large que les deux conventions régionales portées par le Conseil de l'Europe. La création d'un droit pénal international à la fin des années 1990 aurait paru comme une idée totalement irréaliste quinze ans plus tôt : il n'est donc pas interdit de réfléchir aux voies qui pourraient être suivies afin de créer un droit international spécifique à l'environnement cyber. D'un point de vue théorique et dans une perspective prospective on peut considérer qu'il pourrait exister trois types de possibilités pour parvenir à un droit du cyberespace.

* La première d'entre elles résiderait dans le fait d'extrapoler le droit régional existant en la matière, c'est-à-dire les deux conventions de 1981 et 2001. Ainsi qu'on l'a vu, rien n'interdit que des États extérieurs au Conseil de l'Europe signent et ratifient les textes qu'elle élabore. L'application de ce droit pourrait par ailleurs être contrôlé par le Comité des droits de l'homme, organisme onusien qui a la charge d'observer le respect du Pacte international relatif aux droits civils et politiques (PIDCP, 1966). Des possibilités techniques existent donc mais elles supposent un engagement politique fort de la part des États et la conscience des avantages qu'ils pourraient retirer à se lier les mains par la signature d'un nouvel accord international. Cette voie n'est donc pas la plus plausible.

[39]. *Ibid.*, p. 66.

* Une deuxième possibilité résiderait dans la construction d'un droit *sui generis* en s'inspirant des droits de l'espace et de la mer existant[40]. Il serait possible de procéder par analogies car ces textes de 1967 et 1982 qui sont appliqués sans donner lieu à un trop fort contentieux touchent à des espaces particuliers comme l'est l'Internet et garantissent une protection à certaines infrastructures physiques. Ratifié par 103 États, le traité de 1967 fonde le droit de l'espace (extra-atmosphérique). Quelques principes pourraient être extraits et appliqués au réseau : le principe de non-agression dans l'espace (article III du traité de 1967), le principe de non-interférence avec les activités des autres États (article I[er]), le principe de l'utilisation pacifique (article IV), enfin le principe de la responsabilité (civile) de l'État (articles VI et VII). Le droit de la mer (reposant sur la convention de Montego Bay de 1982, ratifiée par 162 États, mais pas par les États-Unis) pourrait être une autre source. Il a notamment en commun avec le droit de l'espace de disposer le principe de non-appropriation par un État. Ce qui est particulièrement utile par rapport à l'environnement cyber c'est que la convention de 1982 distingue plusieurs zones de mer permettant des analogies avec les différentes composantes du cyber[41]. Par ailleurs, la convention de Montego Bay a créé un « tribunal international du droit de la mer » et une « autorité internationale des fonds marins ». Le texte assure par ailleurs une protection des infrastructures, notamment des câbles sous-marins (articles 113 et 144 de la convention de 1982). On retiendra surtout des deux textes qu'ils ont inventé des aménagements à la souveraineté en définissant des espaces où l'usage est partagé d'une part ; qu'ils ont conçu ces deux espaces concernés comme un « patrimoine commun de l'humanité », ce qui présente quelque analogie avec la catégorie des « commons », assez en vogue dans une partie de la cybersphère. C'est d'ailleurs cette notion de « patrimoine commun » qui entraîne la protection de cet espace, l'usage pacifique et le principe de non-appropriation.

* Dévolu principalement à l'échange de contenus informationnels, l'environnement cyber pourrait aussi bénéficier du développement d'un droit technique, celui de la communication et des télécommunications. Les droits fondamentaux ont été définis assez tôt dans des textes anciens (Déclaration universelle des droits de l'homme, 1948 et convention de sauvegarde des droits de l'homme et des libertés fondamentales, 1950). Pour les aspects plus techniques, il s'agit du RTI de 1988. Mais la faiblesse de cette voie repose sur l'absence d'organe de contrôle et le caractère obsolète du règlement de 1988. Ainsi qu'on l'a vu *supra*, l'échec de la conférence de Dubaï en 2012 a montré l'impossibilité des États à s'entendre sur un nouveau règlement, ce qui obère à moyen terme la probabilité d'élaborer un droit de la communication et des télécommunications adapté à l'environnement cyber.

Avant de terminer on évoquera la question du traitement juridique de la conflictualité dans l'environnement cyber. Il s'agit là d'un aspect très spécifique qui ne

[40]. Cf. les préconisations du rapport de la CEIS : *Les droits maritimes et de l'espace peuvent-ils inspirer un droit du cyberespace ?*, Paris, CEIS, 2014 aux pages 41-58.
[41]. *Ibid*., l'intéressant tableau en p. 16.

peut bien évidemment fonder un droit général du cyber. Les États-Unis et les Nations-Unies ont développé une approche originale, qu'ils sont les seuls à partager, sur l'application du droit des conflits armés dans le cyberespace[42]. Ceci signifie notamment que le cyberespace est totalement intégré à leur conception du conflit et de la guerre. Mais la première puissance informationnelle au monde n'est pas parvenue à imposer ses vues et la solution du manuel de Tallinn rencontre de nombreuses oppositions notamment autour des interprétations de la Charte des Nations Unies.

La notion de « lawfare » inventée en 2001 par le général Charles Dunlap (États-Unis), caractérise très justement la bataille permanente entre les États sur les conventions juridiques internationales. Le *lawfare* caractérise essentiellement le droit des conflits armés, mais il y a un *Cyber Lawfare* qui se traduit notamment depuis 2012 (échec de Dubaï et publication du manuel de Tallinn) par un blocage des discussions multilatérales et par des initiatives unilatérales. Ceci ne peut en aucun cas fonder un droit spécifique à l'environnement cyber, ce qui est peut-être la volonté de certains acteurs étatiques et économiques. Pour dresser le bilan final de l'état du droit cyber, on peut reprendre l'expression de la juriste Eve Tourny : « un droit déclaratoire prépondérant, un droit contraignant embryonnaire »[43].

3.2.4. Les normes applicables à l'environnement cyber : un *soft law* discret

On a vu *supra* la diversité des organes producteurs de normes applicables à un titre ou à un autre à l'environnement cyber. En l'état actuel du *hard law* applicable au cyber (cf. ce qui précède immédiatement en 3.2.1. à 3.2.3.), ce sont les normes qui *de facto* assurent une régulation technique de l'environnement cyber qui peut s'apparenter à un procédé *bottom-up*. L'emploi de ce terme peut toutefois être discuté car ces normes ne sont pas issues des méthodes de travail participatives de l'IETF (cf. *supra* en 1.1.1) : elles sont principalement développées par deux organisations internationales, l'IEC et l'ISO qui sont, surtout la seconde, de grandes organisations internationales objet de batailles d'influences. Il n'est pas interdit de penser que les sociétés productrices de solutions de sécurité tentent d'influer d'une façon ou d'une autre sur l'ISO : c'est un objectif majeur pour elles. Ainsi que l'a montré le rapport de Claude Revel remis au ministre du Commerce extérieur en 2013 (Revel, 2013), il existe à l'ISO, créé il y a bientôt 70 ans, une bataille des normes qui est décisive au plan économique. Elle a relevé par exemple que 60 % des comités techniques de l'ISO étaient tenus par des Européens dont 20 % d'Allemands[44] et que les Français étaient très minoritaires dans l'organisation. Quoi qu'il en soit, l'ISO produit régulièrement des normes qui sont soit des normes de fonctionnement général, soit des normes de sécurisation. Les normes applicables au cyber sont très diverses : issues à l'origine de l'électronique et de l'informatique, elles concernaient aussi bien les composants que leur assemblage. Elles ont été étendues depuis aux

[42]. Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013, 282 p.
[43]. Eve Tourny, International Summer School DSC, Université de Bordeaux, 9 juillet 2015.
[44]. Claude Revel, *Développer une influence normative internationale stratégique pour la France*, Bercy, 31 janvier 2013, p. 29.

usages et aux processus. Il existe par exemple la norme ISO 17 799 sur la sécurité de l'information développée en 2000 et enrichie par la suite pour entrer dans la série 27 000. En effet, aujourd'hui la, plupart des normes de l'environnement cyber figurent dans le domaine de « sécurité de l'information » à quoi correspond la série ISO 27 000 subdivisée en de multiples secteurs spécialisés. Certaines de ses normes ont été développées avec l'IEC (cf. *supra* en 1.1.3.). Les finalités des normes sont aussi variées que leur périmètre : certaines sont très générales portant sur des aspects très macro de SSI, d'autres portent sur des procédés beaucoup plus précis, par exemple en cryptographie. Les normes garantissent l'interopérabilité des produits et des processus, ce qui est indispensable dans un environnement globalisé. En matière de cybersécurité où les *malwares* se disséminent très rapidement, les normes sont cruciales. De nombreuses normes sont issues de la diffusion par certains acteurs économiques de « bonnes pratiques » qu'ils peuvent ensuite faire valider plus largement par une démarche *bottom-up*, puis l'imposer plus facilement aux comités de l'ISO. En décidant de transformer en normes internationales ces bonnes pratiques, elles réussissent à imposer un standard à de futurs concurrents et valident ainsi un avantage technologique acquis. La bataille des normes est donc décisive. Il s'agit là encore d'un champ sous-étudié notamment pour l'environnement cyber.

3.3. Le règne du *multi-stakeholderism* : des « gouvernances » très éclatées

Dans l'environnement cyber les spécialistes distinguent classiquement 3 types de fonctionnement général (Brousseau, 2012) : l'**auto-régulation** qui correspond peu ou prou au fonctionnement de la cybersphère d'avant 2000 ; la **co-régulation**, qui est en fait la « gouvernance » *multi-stakeholder* (sur ses caractéristiques, cf. *infra* en 1.2) qui s'est mise en place dans la décennie 2000 et correspond à la situation actuelle ; enfin la **régulation** qui correspond à un investissement fort des États dans la cybersphère au point de vouloir en transformer l'économie générale de fonctionnement (cf. 3.2.3. et 3.2.4), jusqu'à contester le *multi-stakeholderism* qui suppose un équilibre entre acteurs étatiques et non-étatiques. Le terme de gouvernance, employé dans des sens tellement variés qu'il a perdu toute signification, doit être précisé ici car il est décisif pour comprendre ce qu'est l'environnement cyber actuel. Avant d'aborder le débat sur les définitions proposées par les acteurs de la cybersphère (cf. *infra* en 3.3.1), retenons une approche (Mueller, 2010) qui est très éclairante sur le sens réel de la gouvernance : « Thus, internet governance is the simpliest, most direct, and inclusive label for the ongoing set of disputes and deliberations over how the Internet is coordinated, managed, and shaped to reflect policies »[45]. Ce sont les trois verbes : « coordinated, managed, and shaped » qui sont le plus utiles pour notre propos et correspondent à notre sens à la réalité de ce qu'est la gouvernance que l'on va regarder maintenant plus en détail.

[45.] Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge, MIT Press, 2010, p. 9.

3.3.1. A propos des « gouvernances » dans l'environnement cyber

Il reste que les définitions officielles et institutionnelles, celles utilisées par les différents acteurs de la cybersphère doivent être observées de près. D'un point de vue général, la « gouvernance » a envahi tout le vocabulaire politique national et international et a contaminé celui des sciences sociales analytiques. La « Commission on Global Governance » (CGO) qui s'est réunie à l'initiative de l'ancien chancelier allemand Willy Brandt de 1992 à 1994 a joué un rôle fondamental dans la cristallisation d'une nouvelle façon d'appréhender le système international après la guerre froide. La commission n'a pas inventé une pratique nouvelle qui de fait s'éloignait du multilatéralisme interétatique onusien, mais est parvenue à fixer le sens d'une pratique en train de naître. On la trouve dans *Our Global Neighbourhood*, le rapport final remis par la commission en 1995: « Governance is the sum of the many ways individuals and institutions, public and private, manage their common affairs. It is a continuing process through which conflicting or diverse interests may be accommodated and co-operative action may be taken. It includes formal institutions and regimes empowered to enforce compliance, as well as informal arrangements that people and institutions either have agreed to or perceive to be in their interest"[46]. Cette approche revient en fait à dire une "governance without government » selon l'expression éponyme de James Rosenau et Ernst-Otto Czempiel en 1992. L'approche de la CGO valorise la finalité plus que les acteurs : l'accent est mis sur un mode de résolution d'intérêts différents. Cette définition n'est en rien canonique, mais elle correspond parfaitement à tout le discours sur la gouvernance qui a ensuite été développé.

Les initiatives qui ont par la suite visé à faire évoluer la cybersphère ont accommodé cette vision. Le sommet de Genève de 2003 nous paraît décisif à cet égard. On trouve en effet dans le « déclaration de principes » du SMSI au point 48 la définition suivante : « […] La gestion internationale de l'Internet devrait s'exercer de façon multilatérale, transparente et démocratique, avec la pleine participation des États, du secteur privé, de la société civile et des organisations internationales. Elle devrait assurer une répartition équitable des ressources, faciliter l'accès de tous et garantir le fonctionnement stable et sécurisé de l'Internet, dans le respect du multilinguisme ». On constate là que les principes du *multi-stakeholderism* sont fixés avec la mention des quatre acteurs principaux de l'Internet : les États, le secteur privé, la société civile et les organisations internationales (OIT). Ce qui est là nouveau par rapport aux documents prônant la gouvernance, c'est la mention du « secteur privé ». Pour le reste, la revendication de la multilatéralité n'est pas neuve, elle est propre aux initiatives onusiennes, surtout après la fin de la guerre froide et s'accorde parfaitement avec l'approche de la CGO. En son point 48, la déclaration de Genève ne reprend pas la notion de gouvernance, mais il s'agit bien pourtant de la gouvernance de l'Internet. On a vu plus haut (cf. 1.1.2) qu'à la suite de Genève, le secrétaire général des Nations Unies avait nommé un Working Group on Internet Governance (WGIG) qui avait joué un rôle majeur, tant dans la préparation du SMSI de Tunis que dans la naissance de

[46]. *Our Global Neighbourhood. The Report of the Commission on Global Governance*, Oxford University Press, 1995, p. 2.

l'IGF. Le WGIG a donné sa définition de la gouvernance : « […] development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet"[47]. Par rapport à la déclaration de Genève un an plus tôt, il s'agit là d'une intéressante variante de la définition car les OIT ne sont pas mentionnées. L'évolution est d'autant plus notable qu'elle a été élaborée par une structure onusienne. Dans la définition de l'« agenda de Tunis pour la société de l'information » qui clôt le sommet de novembre 2005, on retrouve une approche très similaire au point 34 : « […] l'élaboration et l'application par les États, le secteur privé et la société civile, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet. ». On y retrouve l'absence de mention des OIT, émanant d'une conférence organisée par….une OIT. D'une certaine façon, ce serait une gouvernance ramenée à ce qu'était la cybersphère avant l'intervention des Nations Unies. On voit là qu'il y a eu donc un fort débat interne sur le sens que devait prendre la notion de « gouvernance », à un moment où il s'agissait de la faire naître. Ce débat n'a pas été artificiel, il a commandé directement l'évolution de la cybersphère jusqu'à sa réalité aujourd'hui.

Tout au long de notre étude nous avons fait le choix d'aborder le sujet de l'environnement cyber à l'aide du séquençage en couches. Cette approche nous paraît heuristique y compris lorsqu'il est question de gouvernance. On peut à cet égard reprendre la très utile distinction de Bertrand de La Chapelle en 2012[48] qui distingue les types de gouvernance selon les couches : il a ainsi évoqué la « gouvernance de l'Internet » qui renvoie à la gouvernance des couches physique et logique et la « gouvernance sur l'Internet » qui touche à la couche sémantique. Cette distinction est très juste et permet de caractériser à notre sens toute une partie des rapports de force au sein de la cybersphère. Néanmoins, il nous paraît que l'enjeu de gouvernance se pose de plus en plus en des termes véritablement transverses au sens où toute une série d'acteurs influe sur plusieurs couches et entend jouer un rôle sur ces diverses couches. Ce sont les couches logique et sémantique qui nous paraissent être l'objet du plus fort investissement et du plus net appétit de la part de la plupart des acteurs et ce faisant qui stimulent les envies de gouvernance. On examinera donc ici trois types d'enjeux de gouvernance qui nous paraissent être les plus structurants, la gouvernance « politique » à portée générale et la gouvernance de la cybersécurité qui tend à prendre une influence de plus en plus forte. On terminera en posant la question de l'existence d'une *data* gouvernance, d'une gouvernance par les données.

[47]. Cité dans : Eric Brousseau and Meryem Marzouki, "Internet governance: old issues, new framings, uncertain implications" in: Eric Brousseau, Meryem Marzouki and Cécile Méadel (eds.), *Governance, Regulations and Powers on the Internet*, Cambridge : Cambridge University Press, 2012, p. 382.

[48]. Bertrand de La Chapelle, "Gouvernance Internet: tensions actuelles et futurs possibles", *Politique étrangère*, été 2012, n° 2, p. 249-262.

3.3.2. La gouvernance « politique » à portée générale

La gouvernance politique à portée générale que l'on ne peut que difficilement qualifier autrement, même si ces termes ne nous paraissent pas entièrement adaptés traduit finalement la volonté de trouver une gouvernance d'ensemble de la cybersphère après 2000. Elle comprend la gouvernance technique de ce que l'on a appelée au début de cette étude le « cybersphere core » (CC), mais elle la dépasse en incluant la gouvernance dans les couches logicielle et sémantique. Cette gouvernance d'ensemble est donc fondamentalement transversale.

Laura DeNardis a développé (DeNardis, 2014) une argumentation tendant à démontrer que les dispositions d'architecture technique ne sont pas neutres, mais qu'elles révèlent des arrangements de pouvoir. Selon l'expression célèbre, « architecture is politics ». Ce type de perspective bien connu dans l'étude des systèmes socio-techniques est d'autant plus convaincant depuis l'arrivée des États dans l'environnement cyber dans la décennie 2000 (cf. *supra* en 2.4.). Elle précise : « Internet governance is enacted via various routes : technical design decisions, private corporate policies, global institutions, national laws and policies, international treaties »[49]. On peut aller plus loin que DeNardis et considérer que si les dispositions techniques (dans le cadre du CC) reflètent des enjeux de pouvoir, il en va de même dans la couche logicielle et sémantique. Pour autant, il paraît important dans le cadre de cette étude de quitter le domaine trop théorique pour observer comment se concrétise cette gouvernance « politique » car l'expression est souvent employée pour qualifier des réalités assez vagues.

- Cette gouvernance nous paraît s'appuyer principalement sur deux organisations, le Multistakeholder Advisory Group (MAG) de l'IGF et le Governmental Advisory Committee (GAC) de l'ICANN (cf. le graphe 4 en 1.1.3). Le MAG de l'IGF a été créé en 2006 au même moment que l'IGF. De composition *multi-stakeholder*, il comprend 56 membres et se trouve de fait sous tutelle onusienne – au sein de l'IGF. Malgré son rôle consultatif, il joue un rôle important en pouvant infléchir l'agenda des sommets annuels de l'IGF dont la détermination est en fait entre les mains de l'ONU. Le GAC de l'ICANN est (bien) plus ancien car il a été créé en 1999 : du point de vue de la gouvernance générale, c'est une structure importante dans la mesure où tous les États y sont représentés et donc potentiellement ce peut être le lieu de mise en œuvre d'une gouvernance politique. Il ne gère qu'une partie de la couche logique.

- A ces deux structures globales, il faut ajouter depuis sa création en octobre 2008, le « Pan-European dialogue on Internet Governance » (EuroDIG) qui est une structure *multi-stakeholder* européenne dont l'objet – en liaison avec le MAG-IGF – est de contribuer à l'échelle régionale à la préparation de l'IGF. Le rôle non négligeable, quoi qu'on en dise, de l'Europe dans le développement du cyber, avec des intérêts différents de ceux des États-Unis, fait de l'EuroDIG un lieu important de délibération autour de la gouvernance politique et générale. La présidence de l'UE, la commission européenne et le Parlement jouent un rôle important au sein d'EuroDIG. On voit que la gouvernance *multi-stakeholder* domine dans les faits.

[49]. Laura DeNardis, *The Global War for Internet Governance*, New Haven-London, Yale University Press, 2014, p. 23.

- Il faut toutefois noter la volonté nettement affirmée du Brésil en 2013 d'essayer de mettre en place une autre forme de co-régulation. Cette position du Brésil était autant liée à l'indignation à la suite de la découverte que sa présidente faisait l'objet d'une surveillance de la part des États-Unis que de sa volonté de manifester à cette occasion un rôle nouveau et particulier dans le système international. C'est ainsi que ce pays a organisé les 23-24 avril 2014 le sommet Netmundial avec la volonté de trouver une position de troisième voie, entre la gouvernance multi-acteurs défendue par les États-Unis et les pays européens et la régulation étatique prônée par la Russie et la Chine. Le sommet a permis un affichage nouveau du Brésil, a donné une occasion supplémentaire de plaider pour une réforme de l'ICANN, mais en pratique le pays organisateur a échoué à rassembler une large coalition sur cette position intermédiaire (CEIS, 2014).

Malgré la diversité et la complémentarité de ces structures de gouvernance qui travaillent assez étroitement entre elles, on peut se poser la question de leur efficience. A l'image de beaucoup de structures liées à l'environnement cyber, il s'agit en fait de forums et de lieux de débat et non d'organisations opérationnelles mettant en œuvre des éléments de politiques publiques transnationales qui n'existent pas à ce jour malgré quelques intentions formulées. Néanmoins, ces structures et la notion même de gouvernance politique et générale ont une importance réelle : elles existent dans l'environnement cyber, ont une forte visibilité et représentent une polarité forte ne serait-ce que par ce que certains États leur accordent un rôle important à venir. *De facto*, elles incarnent une certaine vision du cyber entre co-régulation et régulation depuis le débarquement des États.

3.3.3. Les gouvernances de la cybersécurité

La cybersécurité est devenu un enjeu dominant depuis quelques années au point de marginaliser l'enjeu de gouvernance politique et générale. Les attaques massives contre l'Estonie en 2007 et contre la Géorgie en 2008 ont amené à une prise de conscience générale des effets informationnels - et politiques - des attaques cybernétiques massives, en l'occurrence contre des intérêts étatiques.

Mais en fait cet enjeu avait été objectivé plus tôt et au plus haut niveau. Ainsi on pouvait lire dans la « déclaration des principes » de Genève en 2003, au point 35, la nécessité de : « Renforcer le climat de confiance, notamment grâce à la sécurité de l'information et à la sécurité des réseaux, aux procédures d'authentification et à la protection de la vie privée et du consommateur est un préalable au développement de la société de l'information et à l'établissement de la confiance parmi les utilisateurs des TIC. Une culture globale de la cybersécurité doit être encouragée, développée et mise en oeuvre en coopération avec tous les partenaires et tous les organismes internationaux compétents. Ces efforts devraient être soutenus par une coopération internationale renforcée. Dans cette culture mondiale de la cybersécurité, il importe d'accroître la sécurité et d'assurer la protection des données et de la vie privée, tout en améliorant l'accès et les échanges commerciaux. Cette culture mondiale de la cybersécurité doit en outre tenir compte du niveau de développement socio-

économique des pays et respecter les aspects de la société de l'information qui sont orientées vers le développement ». Deux ans plus tard, à l'« agenda de Tunis pour la société de l'information », on pouvait constater au point 39 : « Nous cherchons à instaurer un climat de confiance et de sécurité pour l'utilisation des TIC en renforçant les bases de cette confiance. Nous réaffirmons qu'une culture mondiale de la cybersécurité doit être encouragée, développée et mise en oeuvre en collaboration avec toutes les parties prenantes comme défini par l'Assemblée générale des Nations Unies dans sa *Résolution 57/239* et par d'autres instances régionales compétentes. Cette culture suppose des actions au niveau national et une coopération internationale accrue afin de renforcer la sécurité tout en améliorant la protection de la vie privée et des informations et données à caractère personnel. La poursuite du développement d'une culture de la cybersécurité devrait renforcer l'accès et les échanges, tenir compte du niveau de développement socio-économique de chaque pays et respecter les aspects de la société de l'information qui privilégient le développement ».

Ces intentions sont demeurées au stade oratoire jusqu'aux événements d'Estonie (2007) et de Géorgie (2008). Depuis la fin de la décennie 2000, le discours public sur cet enjeu n'a cessé de prendre de l'importance au point de devenir très dominant sinon exclusif dans l'environnement cyber au cours de la décennie 2010. Il y a ainsi un danger notamment pour les États de ne plus percevoir cet environnement qu'au travers de l'insécurité (réelle) qui y règne. Cette insécurité est aussi l'une des raisons de l'affaiblissement des principes fondateurs de l'Internet.

Alors que la gouvernance politique et générale pouvait se satisfaire d'une dimension déclamatoire dans la mesure où les organismes techniques fonctionnaient et assuraient le développement et le fonctionnement du réseau, la cybersécurité était - par nature - opérationnelle. Il y ainsi une très discrète mais très opérationnelle gouvernance de la cybersécurité, c'est-à-dire une structuration au sein de la cybersphère qui assure dans un cadre *multi-stakeholder* le fonctionnement de la sécurisation de l'environnement cyber et qui passe principalement par des processus collaboratifs et coopératifs.

Le système repose principalement sur des acteurs nationaux et avant tout sur les « Computer Emergency Response Team » (CERT), ces structures de veille sécuritaire 24/24 qui sont chargées de détecter les attaques et de proposer des solutions de sécurité à court terme. Les CERT sont au nombre de 250 dans le monde (DeNardis, 2014). On se situe là à l'échelle des CERT centralisateurs, comme par exemple l'ANSSI française (composante CERT-FR), dépendant du SGDSN qui est le point de contact des différents CERT français. Les CERT ont pour mission de détecter les attaques numériques sur les réseaux et d'y apporter des solutions de court terme. Ils sont au service des acteurs publics et privés et sont apparus au cours de la décennie 2000 d'abord dans le secteur privé, puis dans le secteur public, suivant en cela l'implication des États dans l'environnement cyber. Les États se sont mobilisés et ont créé les CERT en premier lieu pour protéger les composants numériques de leurs infrastructures vitales/ressources critiques (réseaux d'énergie, de transport, etc…). Il faut ajouter aux CERT les autorités de certification assurant les opérations de chiffrement/déchiffrement par vérification et échange des clés ainsi que les autorités

en charge du routage. Ces trois types de structures assurent le cœur de la gouvernance de la cybersécurité. Ces différentes structures sont publiques mais une majorité est privée, notamment aux États-Unis : on se trouve là aussi de fait face à une situation de *multi-stakeholderism.* A la différence des autres formes de gouvernance ou de tentative d'élaborer des règles, ces structures de cybersécurité fonctionnent de façon coutumière par le biais d'accords de coopération bilatéraux fondés au mieux sur des MOU. Cette gouvernance est donc très technique, ce qui fait sa force car elle est souple, mais aussi sa faiblesse car elle peut être remise en cause à tout moment ou ne pas être effective sans être perçue comme telle. Un CERT peut ainsi refuser de signaler à un autre CERT une menace ou une attaque sans que le second ne le sache.

Au niveau supra-étatique on trouve également des organes en charge de la cybersécurité. Ils se situent principalement à l'échelle régionale. La structure la plus opérationnelle de ce point de vue est l'European Network and Information Security Agency (ENISA) créé au sein de l'UE en 2004. L'ENISA remplit le rôle d'auxiliaire des CERT défaillants des États-membres de l'UE et assure la diffusion des normes et bonnes pratiques. L'agence, bien qu'elle ait été peu dotée, ayant été mise en place précocement, a joué un rôle non négligeable dans l'UE avant 2010. Aujourd'hui, elle constitue un point de jonction entre les différents CERT, mais les pays membres de l'UE qui ont de fortes capacités technologiques n'ont pas besoin d'elle. En revanche, l'ENISA est un organisme important pour les plus petites nations de l'UE et en particulier celles qui n'ont pas le niveau technologique requis pour assurer une cybersécurité résiliente. Il joue un rôle important également dans la détermination de la stratégie de cybersécurité des institutions de l'UE et dans l'Union. L'ENISA est la plus avancée de toutes les organisations régionales mais celles-ci tendent à se développer de façon virale. L'Organisation des États Américains (OEA) a créé en 2004 un « Cybersecurity Programme » qui vise à doter les 35 pays d'Amérique du Nord et du Sud membres de l'organisation de CERT et de les faire travailler en réseau[50], les six pays membres de l'Organisation de Coopération de Shangaï (OCS) ont signé en 2009 un "Agreement on Cooperation in the Field of Information Security »[51], par ailleurs les dix pays de l'Association des nations de l'Asie du sud-est (ASEAN) se sont accordés en 2012 sur un « Statement on Cooperation in Ensuring Cyber Security »[52] et organisent depuis près de dix ans des rencontres régulières sur les questions de cybersécurité à l'échelle régionale. Il s'agit donc essentiellement de forums et d'accords en vue d'échanger des bonnes pratiques.

En revanche, au sein des organisations régionales de sécurité, les structures sont plus opérationnelles et participent de la gouvernance technique de la cybersécurité. C'est le cas du « Cooperative Cyber Defence Centre of Excellence (CCD-COE) de l'OTAN, créé en 2008 à…Tallinn où l'organisation mène une activité de recherche et de prospective en matière cyber. Le CCD-COE développe par ailleurs une expertise commune au sein des pays de l'OTAN et diffuse l'idée d'un *hard law* sécuritaire fondé sur les solutions du manuel de Tallinn. On observera que la France a rejoint cet organisme tardivement, en 2014. INTERPOL possède depuis 2014 l'

[50]. https://www.sites.oas.org/cyber/en/Pages/default.aspx
[51]. http://cis-legislation.com/document.fwx?rgn=28340
[52]. https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARFStatementCS.pdf

« Interpol Global Complex for Innovation » à Singapour avec un objectif qui n'est pas très éloigné du centre de Tallinn.

L'OSCE en tant qu'organisation pour sa part a des objectifs plus modestes[53] du type de ceux des autres organisations régionales. A l'échelle mondiale, on rappellera l'existence depuis 2008 à l'initiative de l'ITU de « l'International Multilateral Partnership Against Cyberthreats » (IMPACT, cf. 3.2.2) qui est un organisme rassemblant des acteurs publics et privés. La cybercriminalité est devenue un enjeu international très fortement objectivé : il n'est plus une organisation internationale qui n'ait un volet ou un discours (souvent peu original et innovant) en la matière. Ainsi deux organismes qui n'ont aucune capacité contraignante, l'UNODC et l'ITU ont signé en 2011 un MOU « United against Cybercrime ».

On peut ainsi constater que le cœur de la gouvernance de la cybersécurité qui est une **gouvernance technique**, est constitué par le réseau mondial des 250 CERT centralisateurs qui même acteurs publics et privés. Les autres composantes sont des forums régionaux sans aucune portée opérationnelle. Pour terminer il faut poser la question de l'ampleur des phénomènes criminels dans l'environnement cyber. Comme toute mesure de l'insécurité, l'évaluation ne tient compte que de ce qui a été mis au jour, ce qui constitue un biais majeur tendant à la sous-évaluation. Autre biais, les évaluations existantes sont le fait….des vendeurs de solutions de sécurité. Ainsi le rapport Symantec de 2013 évaluait le coût de la cybercriminalité pour 400 millions de consommateurs touchés annuellement à plus de 110 milliards de $[54]. Ce chiffre n'est qu'un ordre de grandeur probablement très fortement éloigné de la réalité, d'où l'intérêt du lancement par l'Université allemande de Münster en 2014 du projet de recherche européen (7e PCRD) « e-crime » dont l'objet est d'évaluer l'impact économique de la cybercriminalité.

La cybersécurité peut-elle se mesurer ? C'est à cette question ambitieuse que l'ITU a voulu répondre en conduisant en 2014 une étude d'amplitude mondiale qui a débouché sur la publication du rapport *Indice de cybersécurité dans le monde et profils de cyber bien-être* en avril 2015[55]. L'indice de cybersécurité dans le monde (GCI) qui est élaboré dans ce rapport tient compte de 5 critères : le cadre juridique, les mesures techniques, les structures, le renforcement des capacités et la coopération internationale. Le classement qui est ensuite réalisé ne laisse pas de surprendre. Les Etats-Unis occupent, sans *ex aequo*, la première place avec un CGI de 0,824. La France vient ….au 9 e rang après le Royaume-Uni (5), la Turquie (7) et la Slovaquie (8) avec un CGI de 0,588. S'il est toujours nécessaire d'observer sous un jour critique la méthodologie des « classements » et les intentions de ceux qui les élaborent[56], la position de la France est tout de même assez basse.

Il faut enfin noter qu'à la malveillance s'ajoute la surveillance (cf. infra en 3.3.3) pour laquelle la gouvernance est purement nationale et régalienne. Enfin, il importe de mentionner que l'on ne peut pas écarter *a priori* la question de la viabilité même de la

[53]. Elle a ainsi organisé en 2001 l' "OSCE Conference on a Comprehensive Approach to Cybersecurity".

[54]. OECD, "The digital economy today", in OECD, *Measuring the Digital Economy: A New Perspective*, Paris, OECD Publishing, 2014, p. 43.

55. ITU-UIT, *Indice de cybersécurité dans le monde et profils de cyber bien-être*, avril 2015, 531 p.

[56]. On observera tout de même que sous le timbre de l'ITU-IUT c'est une société privée, « ABI research » qui a réalisé l'étude et construit l'indicateur

cybersécurité. Selon de nombreux experts, les calculateurs quantiques - dont les plus puissants sont très rares, entre les mains de quelques États et seulement en cours de développement – pourraient fragiliser de façon radicale les solutions de sécurité fondées sur la cryptographie. Les effets économiques et politiques en seraient vertigineux…

3.3.4. Une *data governance* publique, limitée à l'Europe

Si la théorie économique peut discuter du bien-fondé du respect de la vie privée dans la mesure où l'utilisation des données liées à la *privacy* peut participer à la croissance économique voire au bien-être, par le biais de la sécurité (Rochelandet, 2010), le respect de la *privacy* est (inégalement) considéré sur un plan juridique et politique comme un élément fondamental des valeurs libérales. Relevons que le premier argument est fréquemment évoqué aujourd'hui, y compris par des juristes : pour plus de sécurité, il faudrait que les citoyens cèdent aux États de l'accès à leur données (Chesterman, 2010).

A cet égard, une forme de gouvernance particulière existe, mais se manifeste uniquement dans l'Union européenne où l'état avancé du droit en matière de protection des libertés publiques fait du continent un havre pour les données personnelles numériques des citoyens de l'UE. A ce titre, il n'est pas exagéré de parler là de *data governance*. Celle-ci s'appuie sur du *hard law* et sur des institutions chargées de le faire respecter. La définition de ces « données personnelles » est très claire dans l'article 2 de la loi 2004-801 du 6 août 2004 (modifiant la fameuse loi « informatiques et libertés » de 1978) : « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »[57]. Elle correspond peu ou prou à ce qui est le plus petit dénominateur commun dans les textes européens. Le cadre juridique de référence est constitué par quatre textes fondamentaux : la convention 108 du Conseil de l'Europe du 28 janvier 1981 (cf. *supra* en 3.2.1), la directive UE 95/46/CE du 24 octobre 1995 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », la directive communautaire n° 97/66/CE du 15 décembre 1997 « concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications », enfin la « charte des droits fondamentaux de l'Union européenne » du 7 décembre 2000. Il faut ajouter à cela la révision en cours de la directive de 1995 qui prendra la forme d'un règlement – c'est-à-dire d'application directe – dont les grandes lignes sont connues depuis janvier 2012 mais qui tarde à prendre une forme définitive. Il faut enfin ajouter les arrêts de la CEDH et les décisions de la Cour de Justice de l'Union Européenne (CJUE). Les juridictions européennes, mais aussi les juridictions nationales des pays de l'UE sont

[57] http://www.legifrance.gouv.fr/affichTexteArticle.do?idArticle=LEGIARTI000006528061&cidTexte=LEGITEXT000006068624

chargées de faire respecter ces textes. Ce n'est pas ici le lieu d'en faire l'exégèse mais l'on rappellera tout de même les principes cardinaux qui se sont dégagés au fil des ans : les notions de droit à l'oubli, de loyauté de la collecte et de droit au déréférencement (depuis la décision de la CJUE de 2014), complétées par d'autres notions secondaires mais non point marginales pour tous ceux qui ont à administrer des données personnelles. Bien d'autres dispositions complémentaires constituent un cadre protecteur pour les « données personnelles ». Elles sont une contrainte pour les États et les acteurs économiques qui collectent ces données. La gouvernance en la matière n'est pas *multi-stakeholder* : seules les juridictions nationales et européennes sont amenées à faire respecter les textes et à contraindre a priori et a posteriori ceux qui utilisent ces données. Aux côtés des juridictions existent les quasi-juridictions (dans l'esprit d'une réflexion sur la gouvernance) que sont les autorités de régulation nationale qui participent également à la *data governance*. La directive UE de 1995 a été à l'origine de la création du groupe dit de l'article 29, le G29 qui regroupe les autorités de régulation des données des pays membres de l'UE. Cet organe est consultatif mais il joue un rôle important auprès de la Commission européenne. Il faut ajouter que les révélations Snowden à l'été 2013 (cf. *infra* en 4.2.5) ont considérablement accru dans l'UE la sensibilité des opinions aux questions de protection de la *privacy* numérique. Il est évident qu'il y a eu un effet Snowden à l'origine de l'arrêt de la CJUE du 6 octobre 2015 condamnant l'accord « Safe Harbor » de 2000 en raison du caractère inadéquat de la protection des données personnelles européennes exportées et utilisées aux Etats-Unis. Cet arrêt est majeur de notre point de vue, renforçant l'isolat européen.

On observera enfin que les données des personnes morales – et notamment des entreprises – ne bénéficient pas de la même double protection juridique, nationale et européenne, que les données personnelles. Pour celles-là seul le droit national est valide. C'est incontestablement un facteur d'insécurité juridique et *in fine* de fragilité pour les acteurs économiques. Il faut noter que le paysage des données pourrait s'enrichir (et se compliquer) avec l'apparition d'une troisième catégorie de données après les données publiques et les données personnelles, les « données d'intérêt général » pour lesquelles la ministre française Axelle Lemaire plaide depuis quelque temps[58]. Cette dimension devrait être présente dans le projet de loi sur le numérique qui sera rendu public à partir de la mi-septembre 2015.

Les données sont un enjeu très fort de gouvernance dont l'importance ne va cesser de croître car l'économie numérique repose principalement sur leur utilisation d'une part et les internautes commencent à se préoccuper de ce qu'il advient des traces numériques laissées par eux, d'autre part. L'internet des objets va être dans la décennie à venir la source principale de croissances des données personnelles : on peut craindre une véritable fragilisation de ces éléments constitutifs de l'identité numérique. Dans ce contexte le rôle des instances de régulation ne va cesser de croître, principalement (exclusivement ?) en Europe. La bataille entre les GAFA et les autorités de régulation est engagée depuis quelques années : Google est en conflit avec 6 autorités de régulation sur 29. Sans surprise l'UE est le continent qui pose le

58. Cf. notamment ses déclarations au 2e forum de la gouvernance Internet (IGF), Université Paris-Descartes, 2 juin 2015.

plus de difficultés aux grandes plateformes et les données cristallisent en grande partie les conflits. Face à la marchandisation croissante des données, la réflexion théorique envisage d'en tirer les conséquences et de reconnaître aux individus un droit de propriété sur leurs données (alors que ce n'est en l'état qu'une qualité de l'individu) afin de permettre, sous certaines conditions, d'en organiser la cession en vue de l'organisation d'un marché institutionnalisé des données. L'hypothèse qui peut choquer a priori n'est pas absurde car elle permettrait de réguler ce nouveau marché, de lui apporter des protections économiques et juridiques et d'empêcher qu'elles ne soient soumises à un marché de fait clandestin quoique non illégal.

En conclusion de cette 3e partie, il faut souligner que la **gouvernance de l'Internet** est **relativement efficace et forte**. En effet, elle fonctionne parce qu'elle est souple et collaborative. Toutes les parties prenantes ayant un intérêt presque identique à y participer, elles s'y engagent et acceptent d'échanger aussi bien pour construire l'environnement cyber et le faire fonctionner que pour le défendre lorsqu'il est mis en danger.

La **gouvernance sur l'Internet** présente des caractéristiques différentes, notamment dans la couche sémantique : elle est **bien plus faible** et **géographiquement très limitée** dans la mesure où elle suppose un plus petit dénominateur commun sur les valeurs afin d'être traduite en termes juridiques.

4. L'horizon stratégique : des avenirs à géométrie variable

Aux responsables SSI qui exposent régulièrement des scénarios catastrophiques pour le réseau mondial s'opposent des analystes du cyber qui ont tendance à exposer des vues assez générales et optimistes sur le développement de l'environnement cyber. Ainsi si l'on suit Kurbalija les 5 grands enjeux à venir sont le développement du réseau, l'aspect juridique, la dimension économique, les infrastructures et la standardisation, la perspective socio-culturelle (c'est-à-dire la couche sémantique) (Kurbalija, 2013). Rien de ceci n'est faux mais cela manque singulièrement de précision. Selon le rapport français Chiche paru la même année (Chiche, 2013), il y aurait six autres enjeux : la neutralité de l'Internet, la protection des données personnelles, les cyber-attaques et la cybercriminalité, la culture partagée entre propriété intellectuelle et libre circulation gratuite des œuvres, la protection de la diversité linguistique et culturelle, enfin le « défi environnemental » - effet de la croissance du *hardware*. Cette vue nous paraît plus informée que la précédente, mais ni assez globale, ni assez précise. Toujours dans notre perspective socio-technique, on propose plutôt - sur la base de ce qui a été analysé dans les trois premières parties - de distinguer les caractéristiques durables de l'environnement cyber et les enjeux stratégiques, enfin les évolutions plus aléatoires à même de constituer les lignes de force de *scénarii* prospectifs.

4. 1. Les caractéristiques durables de l'environnement cyber

4.1.1. Le développement continu des couches physique et logique

Dans les 34 pays que compte l'OCDE, les projections de cet organisme en 2014 ont estimé que le nombre de *devices* passerait d'1,7 à 14 milliards en 2022[59]. D'autres évaluations indiquent que d'ici cinq ans (2020) il y aura 25 milliards d'objets connectés et pour d'autres cela pourrait dépasser les 200 milliards (Babinet-Vassoyan, 2015). En outre, l'*Internet of everything* n'est plus une utopie, mais un horizon où tout l'environnement matériel sera connecté, étendant plus encore la connectivité. Le *cloud* malgré des interrogations fondamentales sur la sécurité, est assuré de continuer à progresser en raison de la poursuite de la baisse du coût de stockage, passé de 56 $ par gigabyte en 1998 à 0, 05 $ en 2012, soit une diminution du coût de 40 % par an[60]. On sait par ailleurs qu'accompagnant ce développement du *hardware* et de la couche logique, les données vont continuer à croître sur trois plans : « velocity, volume, variety ». Les données seront plus nombreuses, plus variées et d'accès et de circulation plus rapides. Parce que le cyber n'est pas seulement une « dimension », ou un

[59]. OECD, "The digital economy today", in : OECD, *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, 2014, p. 26.
[60]. OECD, "The digital economy today", in : OECD, *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, 2014, p. 32.

« espace », mais qu'il est un environnement global (cf. introduction), il est assuré qu'il continuera à croître fortement. On a vu *supra* en 2.1.2. les marges de progression du réseau mondial qui sont extrêmement fortes en dehors de la seule anglosphère. Pour autant, personne ne peut faire de projections sur le rythme d'accroissement de la connectivité. Encore faut-il noter qu'il s'agit de taux de pénétration mesurés pour des équipements de base et calculés pour la connectivité de zones géographiques données. A l'heure de la multiplication des supports de raccordement au réseau, la qualité d'un espace de connexion et l'intensité de la connectivité peut croître encore, a fortiori hors de l'anglosphère. La croissance de l'environnement cyber est un horizon durable pour plusieurs décennies. Par ailleurs, cette croissance continue se fera parce que tous les acteurs privés et publics (y compris les États non démocratiques) ont des intérêts certes d'origines différents mais convergents vers la croissance générale du réseau. Il apparaît difficilement contestable que l'économie numérique croît fortement et qu'elle entraîne l'économie classique dans son sillage à moyen terme tout en contribuant, paradoxalement, dans le court terme, à son affaiblissement. Il faut toutefois garder à l'esprit la nuance majeure que le réseau pourrait croître tout en poursuivant sa balkanisation et en limitant techniquement son interopérabilité.

4.1.2. La persistance des principes fondamentaux

L'environnement cyber, paré de tous les feux de l'innovation et de l'avenir n'en demeure pas moins – déjà – également un héritage. Il ne peut se réinventer radicalement dans ses structures et dans son architecture. Ceci est particulièrement valable dans son architecture socio-politique : ni les caractéristiques de la gouvernance *multi-stakeholder*, ni les principes fondamentaux de l'Internet (cf. *supra* 1.1 et 1.2) ne nous paraissent susceptibles d'être modifiés en profondeur. La gouvernance va demeurer ce qu'elle est depuis les origines : issue du modèle étatsunien fondateur associant intérêts et structures privés et publics. Il faut d'ailleurs ajouter qu'elle est en cela emblématique de l'évolution de la « gouvernance » dans le système international sur bien d'autres enjeux. Ceci ne signifie pas cependant que dans l'environnement cyber d'autres enjeux n'apparaîtront pas (cf. *infra*), mais les structures ne seront modifiées qu'à la marge, ce qui suppose - dans une perspective stratégique - que les deux grandes catégories d'acteurs, les États et le secteur privé en prennent acte, incorporent cette dimension et apprennent mutuellement à mieux interagir dans cet environnement particulier. Il en va de même pour les principes fondamentaux qui sont d'authentiques « valeurs » socio-techniques : il importe peu qu'elles soient en partie illusoires, que la réalité du cyber s'éloigne régulièrement de ces idéaux – même s'il est nécessaire de prendre la mesure avec précision du décalage –, il faut comprendre que c'est au nom des quatre grands principes fondamentaux que le cyber conserve une forte capacité d'attraction sur les usagers, qu'il nourrit en permanence les argumentaires commerciaux et les stratégies marketing des acteurs économiques, enfin que les organisations internationales dans et autour de la cybersphère continuent à les promouvoir.

4. 2. Les enjeux stratégiques aujourd'hui et demain

4.2.1. Les effets contrastés du développement de la « nouvelle économie »

La formation d'un secteur propre - l'économie numérique - et la numérisation d'une partie de l'économie suscitent incompréhensions et critiques, rappelant les débats de la fin des années 1980 marqués par la dérégulation et l'expansion des marchés financiers. Une majorité critiquait alors les marchés et l'économie financière au nom de la défense de « l'économie réelle ». Aujourd'hui avec l'expression « d'uberisation », certains critiquent l'effet destructeur sur « l'économie réelle » de l'offre alternative par des services en ligne. Mais le numérique peut-être un adjuvant de l'économie réelle. Ainsi l'e-commerce a considérablement cru entre 2007 et 2013, les achats en ligne de la population adulte de l'OCDE passant de 31 % à 50 %. Les thuriféraires du « tout numérique » voient progressivement (et souhaitent) le remplacement progressif de l'économie réelle par l'économie numérique. Les deux cohabitent aujourd'hui mais l'économie numérique détruit incontestablement, à court terme, des emplois dans l'économie réelle tout en en créant sous une autre forme dans son secteur. Demeure le constat de son faible effet sur le marché de l'emploi: selon l'OCDE, le secteur est ainsi passé de 3,7 % de part d'emploi en 1995 à 3,8 % en 2012. S'ajoute à cela les critiques contre le rôle dominant de certaines plateformes : c'est le cas de Google qui est formellement soupçonné d'abus de position dominante par la Commission européenne depuis 2009 et directement incriminé pour l'un de ses services depuis avril 2015.

Cependant, selon l'OCDE, de 2000 à 2012, la valeur ajoutée a baissé dans tous les secteurs alors qu'elle a cru de plus de 0, 5 % dans le domaine des technologies de l'information (ICT) qui sont au cœur de l'économie numérique. Le secteur ICT est largement en tête pour les dépenses de R & D en comparaison de tous les autres secteurs économiques dans l'OCDE[61] et l'on peut parler d'un « état permanent d'innovation » selon l'expression de Gilles Babinet. Mais alors qu'ils investissent beaucoup en R & D, les plateformes et les services dominants des GAFA déposent peu de brevets. Facebook publie sa recherche assez régulièrement et ouvertement. Ceci est le signe d'un rapport assez différent de l'industrie classique à l'innovation. Il faut considérer par ailleurs que leur recherche ne va pas seulement vers le développement d'applications ou de services, mais assez souvent vers des innovations à caractère industriel - dont l'objet est de permettre d'étendre l'activité des services numériques. D'autres acteurs classiques entendent utiliser la dimension numérique pour valoriser leurs innovations : ainsi la société Tesla autorise toute personne propriétaire d'un véhicule électrique à se connecter à la plate-forme numérique de la société afin d'utiliser les services gratuitement.

Le secteur numérique présente en fait deux types d'économies qui sont juxtaposées : celle des « transactions » et celle du « partage » (Dang Nguyen-Dejean,

[61]. OECD, "The digital economy today", in : OECD, *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, 2014, p. 34.

2014), soit un secteur marchand et un secteur non-marchand. L'économie concurrentielle numérique bénéficie de puissants effets de réseau débouchant sur le rôle croissant – et dominant – des plateformes, ce qui renforce sa structuration oligopolistique. Mais dans des économies OCDE qui semblent être entrées dans une phase durable de faible croissance, quel sera l'apport au PIB de l'économie numérique ?

4.2.2. Le défi fiscal posé aux États

La seconde source d'inquiétude suscitée par l'économie numérique est le défi fiscal. Ce défi est d'autant plus net qu'il survient dans un contexte de crise générale des finances publiques dans la plupart des économies de l'OCDE et que l'économie numérique tend à détruire des emplois dans l'économie classique. Face à cette « spirale mortifère pour les économies des pays industrialisés » (Collin-Colin, 2013), en septembre 2013 un groupe de réflexion sur l'économie numérique du Comité des affaires fiscales de l'OCDE a été créé avec pour mission de rédiger un rapport d'étape pour septembre 2014. Celui-ci a paru sous le titre : *Relever les défis fiscaux posés par l'économique numérique*. Il débouchait sur un constat très net, la reconnaissance de la réalité de l'« érosion de la base d'imposition et le transfert des bénéfices » (BEPS) vers des pays plus intéressants fiscalement en raison d'un découplage entre le lieu d'exercice de consommation et le pays d'établissement (fiscal). On cite un passage de ce rapport un peu longuement mais qui est parfaitement clair sur la réalité du phénomène : « […] l'importance des actifs incorporels dans le contexte de l'économie numérique, ajoutée à la mobilité de ces actifs à des fins fiscales dans le cadre des règles fiscales existantes, offrent de larges possibilités d'érosion de la base d'imposition et de transfert de bénéfices pour ce qui concerne les impôts directs. De plus, la possibilité de centraliser les infrastructures à distance d'un marché et d'exercer de loin les activités substantielles de ventes de biens et de services sur ce marché, ainsi que la capacité croissante à exercer des activités substantielles avec un personnel minimum, ouvrent également des possibilités d'érosion de la base d'imposition et de transfert de bénéfices au moyen d'une fragmentation des activités physiques ayant pour but d'éviter l'imposition »[62]. Ce travail était assez convergent avec le rapport rendu au début de l'année 2013 par deux hauts fonctionnaires français sur la fiscalité de l'économie numérique (Collin-Colin, 2013). Les deux rapports, français et OCDE, faisaient le constat de la faiblesse des lois fiscales nationales et internationales face à la mobilité du capital, notamment dans le secteur numérique. Depuis 2013-2014, on assiste ainsi à une véritable union sacrée des États pour éviter une diminution accrue de leurs recettes fiscales, estimée de 4 à 10 % de ce rapportent les impôts sur les sociétés dans le monde. Ils ont mis en œuvre un plan d'action conduit dans le cadre du G20 et de l'OCDE et auquel ont participé des pays extérieurs à ces deux structures,

[62]. « Synthèse » in : OECD, *Relever les défis fiscaux posés par l'économie numérique*, OECD Publishing, Paris, p. 15.

signe de la préoccupation générale des États face à ce défi. Une soixantaine de pays ont participé aux travaux du BEPS, soit 25 de plus que n'en compte l'OCDE. Est ainsi apparue une volonté commune d'éviter le dumping fiscal des sociétés du secteur numérique en renforçant les coopérations et les échanges d'information, mais surtout en modifiant les conceptions fondamentales des lois fiscales qui ne sont pas adaptées à l'économie numérique et notamment à un modèle d'affaire reposant principalement sur la valeur produite par les données des utilisateurs. Quoi qu'il en soit, il est certain à moyen terme que les entreprises du numérique où qu'elles soient localisées dans les pays de l'OCDE vont au-devant d'une plus forte fiscalité. En octobre 2015, l'OCDE a rendu publics les 15 plans d'action qui seront proposés au G20 pour une adoption probable en novembre. Cette fiscalité nouvelle pourrait passer par deux moyens : en modifiant la base territoriale d'imposition d'une société et en créant un impôt sur les données, c'est-à-dire sur les utilisateurs dans la mesure où ils sont source de création de valeur (Colin-Verdier, 2013). Même si cela peut paraître *a priori* étrange, il est fort probable que les pays de l'OCDE s'acheminent également vers cette deuxième solution. Les grands acteurs du numérique n'avaient probablement pas envisagé cette réaction régalienne commune du moins dans un délai aussi rapide.

4.2.3. Le nouveau règne des données: *personnal data, big data, smart data*

On constate aujourd'hui que dans l'environnement cyber les « données » constituées par les utilisateurs l'emportent désormais en volume sur les « documents », quel qu'en soit le type (texte, son, image fixe, image mobile…etc). Le phénomène de *surge* des données est d'autant plus remarquable qu'il est très récent : c'est un basculement qui a débuté avec la décennie 2010. Cette poussée est largement due au développement du Web 2.0 et à l'expansion des réseaux sociaux. Elle est accentuée aujourd'hui par l'Internet des objets et demain le sera par l'*Internet of everything*. Le comportement des internautes est fortement accompagné par l'économie numérique qui a connu elle aussi un tournant majeur avec le 2.0. Ainsi que l'ont justement vulgarisé Colin et Verdier, l'économie numérique est fondée sur le gain tiré des utilisateurs, sur l'apport de la « multitude » (Colin-Verdier, 2013) dont les comportements traduits en données sont source de création de valeur. Ainsi sans *data*, pas d'économie profitable dans le cyberespace. Les données constituent la source principale de financement de l'économie numérique par le biais de leur utilisation à des fins prédictives ou de vente à des fins d'exploitation publicitaire, marketing et/ou de services géolocalisés. Selon l'expression, les « […] utilisateurs, bénéficiaires d'un service rendu, deviennent ainsi des quasi-collaborateurs, bénévoles, des entreprises » (Collin-Colin, 2013). Le règne des données conduit ainsi directement au règne des algorithmes qui transforment le *raw data* en *smart data*. L'intelligence ou du moins l'utilitaire n'est pas dans la *data* mais dans l'outil qui fait apparaître des corrélations et des tendances en vue de prédictions ou de recommandations. Avec ces outils mathématiques s'ouvre la voie des calculs utilisés aussi bien pour évaluer un comportement de consommateurs qu'une menace sécuritaire (la police britannique

utilise désormais le terme de social media intelligence-« Socmint »[63]). Tout le secteur numérique est totalement (quoique inégalement) dépendant des données. Or leurs usages, mais aussi leur propriété sont l'objet d'intenses débats économiques et juridiques (cf. notamment *supra* en 3.3.4 et infra en 4.2.4) qui vont prendre de l'ampleur.

4.2.4. La fragilisation de la propriété intellectuelle face au partage et à la gratuité

La gratuité offerte d'emblée sur l'Internet naissant des années 1990 a habitué les premiers internautes à considérer que tous les contenus étaient gratuits. Les services et produits rendus ensuite payants se trouvent donc aujourd'hui confrontés à un double risque : soit celui de la désaffection, ce qui est le cas d'une grande partie de la presse quotidienne qui s'est engagée, contrainte, sur la voie de la gratuité en ligne ; soit celui du piratage, devenue assez courant pour ce qui est des contenus culturels et de loisirs (musique, cinéma par exemple). Contre cela, le renforcement constant des protections techniques ne suffit pas dans la mesure où les « consommateurs » peuvent unir leurs compétences pour les casser et les rendre accessibles sur des sites de partage par téléchargement et/ou *streaming*. Il faut ajouter à cela la prégnance de la culture du partage et du collaboratif, ainsi qu'en témoigne le succès du *peer to peer,* qui fait du cyberespace un environnement hostile par nature aux inventeurs et créateurs. Dans le même temps, qu'ils s'inscrivent dans l'économie réelle ou dans l'économie numérique, ils ne peuvent plus se passer du cyber pour se faire connaître et pour vendre leurs œuvres et produits. La question cardinale est donc celle d'un biais de conception, directement responsable ensuite de l'apparition d'un environnement niant la propriété. Si les juridictions nationales tentent de faire respecter le droit de propriété dans l'environnement numérique, il reste que la nature ubiquitaire de contenus qui sont des flux et l'absence de juridiction internationale fragilise le respect de la propriété dans le cyberespace.

A côté des juridictions, l'organisation mondiale de la propriété intellectuelle (OMPI) est la structure qui permet d'assurer à la fois des échanges sur le droit de la propriété intellectuelle et de recevoir les déclarations d'enregistrement pour les marques, brevets (propriété industrielle) et créations artistiques (propriété littéraire et artistique). L'OMPI figure en surplomb des organisations régionales (par exemple, l'Office européen des brevets) et nationales qui remplissent la même fonction dans une perspective de subsidiarité. Le droit d'auteur est l'objet de deux ensembles de traités internationaux dont l'application incombe à l'OMPI. Celle-ci administre le Traité de l'OMPI sur le droit d'auteur (World Intellectual Property Organization Copyright Treaty (WIPO Copyright Treaty ou WCT), signé en 1996, entré en vigueur en 2002 et qui comprend 93 parties contractantes en 2015[64]. L'organisation a d'autre part en charge le respect du Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes (WIPO Performances and Phonograms Treaty-WPPT), signé en 1996,

[63]. Cf. David Omand, Jamie Bartlett and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)", *Intelligence and National Security*, vol. 27, n° 6, December 2012, p. 809-823.
[64]. http://www.wipo.int/treaties/fr/ShowResults.jsp?search_what=N&treaty_id=16

entré en vigueur en 2002, comprenant également 93 parties contractantes en 2015[65]. Si les caractéristiques principales de la propriété intellectuelle fixées dans la convention internationale de Berne (1886) ont été respectées et actualisées à l'heure de la forte croissance du numérique, l'application concrète des grands principes a toutefois posé des problèmes immédiats, y compris dans les pays de *common law*. Ainsi, aux États-Unis le site Napster a été condamné en 2001 par la justice californienne pour non-respect des règles relatives au copyright. Dans un ordre d'idées proche et pour les mêmes raisons, le site Megaupload a été fermé sur décision de la justice fédérale des États-Unis en 2012. Il faut enfin rappeler que certains acteurs économique du numérique sont eux-mêmes les moins respectueux du droit d'auteur : ce fut le cas de Google qui a numérisé des centaines de milliers d'ouvrages conservés dans les bibliothèques publiques pour son projet « Google books » en 2004 sans payer aucun droit aux éditeurs. Plusieurs procès ont mis un terme à cette pratique et des accords amiables ont été signés avec des éditeurs aux États-Unis et en France. Malgré les condamnations judiciaires des sites de P2P, les États éprouvent de grandes difficultés à faire adopter des législations permettant de renforcer la défense du droit d'auteur/copyright dans le cyberespace. C'est la France qui est allée le plus loin avec une loi votée en 2009 instituant l'Hadopi (Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet). La création de cette institution qui avait pour objectif de lutter contre le P2P ne respectant pas le principe du droit d'auteur a été l'occasion d'amples débats au Parlement et dans les médias. L'institution demeure aujourd'hui très vivement contestée. Aux États-Unis, le dépôt en 2011 au Congrès du projet du Stop Online Piracy Act (SOPA-PIPA) poursuivait des buts analogues aux tâches confiées à l'Hadopi, tout en ajoutant des objectifs de lutte contre la contrefaçon. Le débat qui s'est engagé[66] a été bien plus vif qu'en France car une coalition associant les *majors* de l'Internet (dont les GAFA), le chapitre anglophone de Wikipedia, les libertaires de la liberté d'expression[67] ainsi que des ultra-libéraux a permis d'arrêter le processus législatif en janvier 2012.

La vente de produits culturels en ligne n'est pas pour autant un échec comme en témoignent le succès du service Itunes d'Apple, la vente de livres électroniques sur Amazon….etc et les divers services de vidéos à la demande (VOD), mais l'état d'esprit dominant des internautes est d'accéder de façon permanente et gratuite à une offre sans cesse plus large qui, de fait, remet en cause le paiement de droits à l'auteur pour une œuvre spécifique. Fondamentalement, les effets de la culture de la gratuité ont eu pour effet que le cyberespace est devenu un environnement qui a *de facto* privilégié l'usage sur la propriété. C'est dans cet esprit que, très tôt, dès le début des années 2000, des solutions juridiques nouvelles sont apparues afin de trouver un accommodement entre le droit de propriété et le caractère viral des usages des biens et services informationnels et culturels. C'est ainsi qu'en France a été élaborée entre 2001 et 2004 la « licence globale » dont l'objectif était d'accorder un accès à un ensemble de biens/produits en échange de l'acquittement d'un droit forfaitaire. Le

[65]. http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=20
[66]. Cf. Jeanette Hofmann, "Narratives of Copyright Enforcement: The Upward Ratchet and the Sleeping Giant", *Revue française d'études américaines*, 4e trimestre 2014, n° 134, p. 64-80.
[67]. On entend par là les partisans d'une liberté d'expression sans limites.

projet était plus favorable aux internautes qu'aux auteurs, mais reconnaissait de fait l'existence d'une certaine forme de propriété. L'idée a cependant échoué lors du vote au Parlement. En 2001, le juriste étatsunien Lawrence Lessig a proposé la création de la licence « creative commons » qui a connu un certain succès dans la sphère numérique. Cette disposition, favorable aux internautes, facilite la circulation des œuvres, notamment universitaires, mais est très peu utilisée pour la gestion des œuvres culturelles solidement défendues par des sociétés de production, des éditeurs….On constate par ailleurs qu'il n'est d'ingénierie juridique qui ne soit plus favorable aux internautes qu'aux créateurs.

4.2.5. La surveillance étatique du cyber : un environnement sans confiance ?

Les déclarations d'Edward Snowden et les documents publiés par lui à compter du 6 juin 2013 ont ouvert une nouvelle ère dans l'environnement cyber. Depuis, plus personne ne peut ignorer l'intensité de la surveillance du cyber par l'anglosphère. Certes, il y a plus de dix ans le Parlement européen avait rendu public le rapport Echelon qui s'achevait par une conclusion analogue, mais publié au début du mois de septembre… 2001 il était à l'époque passé inaperçu avec les attentats aux États-Unis (Laurent, 2014). En outre avec Snowden le constat ne se fonde plus sur une enquête externe (européenne), mais sur des documents officiels et classifiés des États-Unis indiquant en outre que la surveillance s'applique à une géographie planétaire. Il y a un effet Snowden parce qu'il remet profondément en cause la confiance dans la capacité de l'Internet à assurer des échanges et des communications confidentielles. Il a de fait affaibli la position des États-Unis défendant un Internet « libre et ouvert » et la gouvernance *multi-stakeholder*, mais aussi les GAFA suspects de collaboration plus ou moins directe au système de surveillance. Les plateformes ont d'ailleurs immédiatement compris le risque pour leur crédibilité et mis en place une communication adaptée. Au lendemain du premier article sur Snowden, Mark Zuckerberg publiait le 7 juin 2013 sur sa page un communiqué condamnant très fermement les pratiques de la NSA, réaffirmant la totale indépendance de Facebook : « We will continue figthing aggressively to keep your information safe and secure. We strongly encourage all governments to be much more transparent about all programs aimed at keeping the public safe and free society we all want over the long term ». Quatre mois plus tard Facebook mettait en ligne son premier « rapport international des demandes gouvernementales » couvrant les six premiers mois de l'année 2013 en indiquant pour chaque pays, le nombre de demandes officielles, de comptes concernés et le pourcentage de réponses. Par ailleurs le 9 décembre 2013, huit sociétés de l'Internet dont Google, Apple et Facebook adressaient une lettre ouverte au Président Obama contre la surveillance et annonçant le lancement de l'initiative « Reform Government Surveillance »[68]. Quoi qu'il en soit la position officielle des États-Unis en est sortie très affaiblie. La plupart des parlements nationaux des pays libéraux et

[68]. https://www.reformgovernmentsurveillance.com/

plusieurs autorités européennes ont lancé des enquêtes parlementaires sur cette surveillance. Les « révélations » Snowden ont eu pour effet d'une part de dissiper l'illusion de la confidentialité dans l'environnement cyber et de renforcer… les offres commerciales pro-*privacy* (navigation anonyme, techniques d'anonymisation…) et de cybersécurité dans son volet de sécurisation des échanges d'autre part. Depuis l'été 2013, la science du secret qu'est la cryptographie connait pour la première fois une vaste promotion publique. Mais il est clair désormais que l'Internet « libre et ouvert » ne l'est pas seulement pour les usagers.

4. 3. Esquisse de *scenarii* d'évolution

Dans l'environnement cyber, chaque type d'acteur subit des contraintes propres et possède des latitudes d'action spécifiques. Il y a donc un environnement général, mais qui se décline différemment selon les acteurs : le cyber des États, celui des personnes morales et celui des personnes physiques sont différents. Nous n'allons pas abandonner l'approche de « comprehensive analysis » qui est la nôtre depuis le début de cette étude, mais nous allons conserver en cette fin de travail une perspective privilégiant la situation des acteurs non-étatiques et étatiques afin de conserver tout son sens à la perspective stratégique de cette étude.

Au seuil de cette partie, il nous paraît important de souligner les limites de la prospective et le fait que bien des exercices prospectifs de haut niveau, réalisés par des institutions de premier plan ont été très largement aveugles sur des évolutions pourtant structurantes. On prendra comme exemple la publication en 2003 par l'OCDE, à l'heure déjà de la grande expansion de l'Internet, du volumineux rapport *Les Risques émergents au XXIe siècle. Vers un programme d'action*, centré sur les « méga-risques ». Le travail de l'OCDE était centré d'emblée sur 5 catégories de risques : catastrophes naturelles, accidents technologiques, maladies infectieuses, terrorisme et sécurité des aliments, tout en fixant un cadre précis : la recherche des risques de forme systémique au sein de ces 5 catégories. Ce qui est frappant est la sous-estimation totale non seulement du risque cyber / numérique, mais même de la seule dimension de l'environnement cyber. Cette évaluation de l'OCDE était passée totalement à côté du cyber. On retiendra de ceci que les structures d'évaluation des risques ne sont pas paramétrées pour comprendre l'environnement cyber et moins encore son caractère transversal (cf. les définitions posées en introduction).

4.3.1. Les évolutions structurantes probables…

Au vu des éléments indiqués *supra*, on peut en 2015 considérer l'existence de dix invariants qui seront des cadres structurants de l'évolution de l'environnement cyber :

(1) En premier lieu la **baisse continue du coût de la technologie** va assurer le **développement de la couche physique** du cyber à la fois dans ses infrastructures fondamentales (fibre optique, satellites, routeurs, serveurs, *data centers*) comprenant toutes par ailleurs des technologies maîtrisées, mais aussi dans ses composants relais (multiplication des terminaux et des types de *devices*, objets connectés). Les nombreuses incertitudes autour du cadre juridique des multiples données produites par ces nouveaux types d'objets ne devraient pas beaucoup ralentir leur développement dans la mesure où l'enjeu *legal* a toujours été envisagé après le développement des technologies (numériques).

(2) Sans qu'il soit possible d'en déterminer le rythme d'évolution et la part de valeur ajoutée, **la nouvelle économie est amenée à se développer** et à continuer de bouleverser l'ensemble de l'économie, à la fois parce qu'elle l'affaiblit à court terme et parce qu'elle lui ouvre des potentialités nouvelles (développement du e-commerce pour des biens classiques, ajustement de la production à la demande…). Le fait qu'une grande partie de cette économie soit fondée sur l'illusion de la gratuité lui procure d'emblée des usagers/consommateurs en nombre. D'un point de vue global, rien ne permet de croire en la remise en cause de la **structure oligopolistique** de l'économie numérique dans la mesure où elle repose sur le principe de plateformes qui sont des agrégateurs de données très variées permettant ainsi une offre de biens et de services tout aussi diversifiés. De nouveaux acteurs apparaîtront avec des offres de meilleure qualité, à moindre prix qui seront des plateformes et des réseaux sociaux alternatifs ou plus ambitieux encore mais ils renforceront la forme de la structure, fondée essentiellement sur les données des usagers. Le type « plateforme numérique » favorise directement le développement d'une telle structuration dominant l'économie numérique.

(3) L'économie née autour des technologies du numérique valorise le règne des données. Le terme est choisi à dessein, mais peut-être parler d'***imperium* des données** serait plus juste encore. Le caractère presque global de cette économie en voie de mondialisation (on verra que la balkanisation traitée en (5) amène à nuancer l'idée de globalisation du cyber) appuyée sur les *data* déplace les terrains de concurrences. Ce qui est désormais discriminant n'est pas seulement l'ICT mais l'analyse de données et les mathématiques algorithmiques. Sur un plan mi-technique, mi-économique les grands affrontements se livreront autour de la capacité à s'emparer de grands volumes de données, à les fiabiliser, à reconstituer les séries manquantes….etc. Le fait que les économies de l'OCDE sont en passe à moyen terme de résoudre le défi fiscal en créant une imposition sur les données des utilisateurs va amener la profitabilité des entreprises du numérique à se déplacer plus encore vers l'**utilisation intensive et extensive des données**. Les données portent en elles-mêmes leur propre logique d'exploitation.

(4) La numérisation des économies à un rythme que personne ne peut évaluer est un **puissant facteur d'affaiblissement** d'une caractéristique essentielle du capitalisme, **le régime de la propriété**. Il s'agit certes de la propriété intellectuelle et non matérielle, mais elle est néanmoins porteuse d'une modification profonde des règles dans le cadre de ce que l'on peut appeler le capitalisme numérique. L'**usage l'emporte désormais sur la propriété** et l'on s'achemine vers des régimes de propriété intellectuelle numérique spécifiques dont certaines caractéristiques sont déjà esquissées.

(5) L'Internet unifié est mort… s'il a jamais existé... La croissance de l'environnement cyber se fait et se poursuivra dans des espaces linguistiques non anglophones qui entendent résister à l'anglosphère tant sur le plan culturel que sur les

plans politiques et économiques. La balkanisation est en marche et le monde se dirige vers un environnement cyber constitué de quelques **grands réseaux régionaux juxtaposés** articulés sur des grands ensembles politico-culturels **à l'interopérabilité limitée**.

(6) Le monde occidental conserve des positions très dominantes dans les nombreuses instances de gouvernance y compris les instances techniques. Par ailleurs, les **États-Unis conservent la position la plus forte** et ils n'ont **aucune raison de l'abandonner** leur situation, notamment dans le « cyberpshere core » (CC), ni de remettre en cause leur stratégie de promotion *multi-stakeholder* au détriment d'une vision alternative stato-centrée.

(7) La **gouvernance polycentrique** qui ne permet pas aux États de se positionner de façon dominante **va demeurer un principe structurant**. Les grandes organisations multilatérales, à commencer par les Nations Unies ont entériné ce principe lors de leur engagement dans la cybersphère au début de la décennie 2000.

(8) Néanmoins la cybersphère n'est pas un espace monolithique et l'on va continuer à assister au renforcement des nouvelles polarités avec un **rôle croissant des plateformes et des États au détriment des organismes techniques** du CC. Désormais ce sont les États et quelques grandes entreprises qui vont s'imposer : ce qui est discriminant ce sont les capacités technologiques de collecte et de traitement des données.

(9) « Malaise dans l'environnement cyber », c'est ainsi que l'on pourrait caractériser la situation depuis que l'on connaît l'ampleur de la surveillance. Si à l'Ouest elle est pratiquée principalement pour des raisons économiques – par l'exploitation des données, cf. (3) –, elle l'est à l'Est et au Sud-Est pour des raisons plus classiquement politiques. Le résultat de la **surveillance** est l'**affaiblissement de la confiance** parmi une partie des Internautes et surtout parmi les grands acteurs du numérique, comme en témoignent leurs déclarations publiques et leur politique de chiffrement renforcé. S'il n'apparait pas pour autant qu'elle ait eu à ce stade d'effet sur le comportement des internautes eu égard à la poursuite des volumineuses traces numériques qu'ils laissent derrière eux, elle dissipe le rêve libertaire latent dans les principes fondamentaux de l'Internet et affaiblit le discours public des *majors*.

(10) Sans être anomique, l'**environnement cyber** va demeurer **principalement régulé par du *soft law***. Le *hard law* applicable au cyber va demeurer partiel et surtout très limité géographiquement. Dans ce cadre, un droit du cyberespace est une illusion.

Tableau 6 : Synthèse : les 10 invariants de l'environnement cyber

1.	développement de la couche physique
2.	structure oligopolistique de la nouvelle économie
3.	*imperium* des données
4.	affaiblissement de la propriété

5.	balkanisation et juxtaposition des réseaux
6.	domination étatsunienne
7.	gouvernance polycentrique
8.	rôle croissant des États et des plateformes
9.	surveillance affaiblissant la confiance
10.	dominante de *soft law*, faible *hard law*

4.3.2. … et la persistance de multiples incertitudes

La tâche d'*horizon scanning* que l'on s'est fixé dans cette étude doit également tenir compte de cinq puissants facteurs d'incertitudes qui doivent être intégrés à l'élaboration des *scénarii* :

(a) le **niveau de** la **conflictualité** et plus généralement de ce que l'on a appelé ici les **cyber-agressions** est très méconnu. Il est croissant, accompagnant le développement du réseau mais il est très difficile d'imaginer son évolution à venir. La difficulté d'attribuer une attaque (voire de la caractériser pendant un certain délai) et le caractère géographiquement très limité de la portée de la convention de Budapest affaiblissent les possibilités de répression.

(b) l'état du **respect de la neutralité du net** (NN) par les opérateurs maîtrisant les flux du réseau est également une dimension en question. Certaines tensions et crises sur le réseau permettent de constater des moments temporaires de remise en cause de la NN, mais il est très difficile d'en savoir plus. Des garanties politiques sont apportées dans la sphère occidentale en faveur de la NN mais cela ne dit rien sur son respect effectif et sur l'état de la discrimination des flux. On sait par ailleurs qu'un certain nombre d'acteurs économiques importants souhaitant différencier leurs services à leurs clients sont hostiles à la NN. La croissance des flux vidéos et le refus des propriétaires d'infrastructures de financer seuls leur développement en vue de supporter la demande croissante de bande passante amène à être pessimiste sur la NN.

(c) le **statut de la donnée** sera absolument crucial à l'avenir mais il prend la forme d'un vaste point d'interrogation, **que ce soit** sur la question de sa **protection** par le *hard law* **ou** de sa **propriété.** Sur le premier point on peut faire apparaître une certaine géographie (cf. *supra* en 3.2.1), mais elle est susceptible d'évoluer. Quant au second il est aussi flou que crucial car l'appropriation par les plateformes ne peut être remise en cause sous peine d'effet massif et immédiat sur la profitabilité de l'économie numérique.

(d) la **cybersécurité** est devenu un mantra aux forts pouvoirs hypnotiques mais en fait l'on ne connaît pas du tout la durée de vie des solutions de sécurité. Bien évidemment, comme toutes les mesures de sécurité, elles doivent s'adapter en

permanence aux manifestations d'insécurité auxquelles elles sont censées répondre, mais la **question de leur viabilité de moyen terme est clairement posée** ou plutôt devrait être enfin ouvertement posée, incorporée aux standards ISO par exemple. La pression convergente et publique en 2014-2015 (manifestation d'un « effet Snowden ») de puissants États contre les *majors* prétendant au renforcement de leurs moyens de chiffrement ne diminue pas pour autant l'incertitude.

(e) il existe enfin une très forte incertitude sur l'**évolution de l'isolat européen**. Comme on l'a vu tout au long de cette étude, l'environnement cyber dans l'Union européenne se distingue de tous les autres pays, y compris des États-Unis. C'est dans l'UE que le *hard law* à portée numérique est le plus prégnant, que l'activité des plateformes est la plus contrainte et c'est en même temps une zone de forte concentration des cyber-agressions à portée économique. Mais c'est également un continent stable politiquement et économiquement qui contribue très amplement avec son demi-milliard de consommateurs au développement des *majors* et de l'économie numérique mondiale.

Tableau 7 : Synthèse : les 5 incertitudes de l'environnement cyber

1.	niveau de conflictualité
2.	effectivité de la neutralité du net
3.	protection et propriété des données
4.	viabilité temporelle de la cybersécurité
5.	isolat européen

A partir des quinze éléments des tableaux 6 et 7, il est possible de les faire évoluer afin de produire une grande variété d'évolutions et de *scénarii*. Néanmoins on ne retiendra ici que 3 cas de figure en mettant en avant ceux qui nous paraissent les plus probables à l'horizon de moyen terme, soit 5 à 10 ans. Ils sont indiqués *infra* sans qu'il y ait d'ordre ou de classement dans la façon dont ils sont énoncés.

4.3.3. Scénario A : renforcement de l'isolat européen dans le monde

Le premier cas de figure est caractérisé par la continuité dans les invariants et dans le fait que les incertitudes ne sont pas levées : les cyber-agressions demeurent au niveau actuel justifiant un recours permanent à la cybersécurité, mais sans entraver l'activité de la nouvelle économie et sans que les cyber-conflits interétatiques ne prennent une ampleur telle qu'elle la remette en question. D'un point de vue technique, la cybersécurité n'est pas remise en cause : les solutions de sécurité tentent de s'adapter aux nouvelles formes de cyber-agressions avec toujours un temps de retard. La NN demeure le principe technique dominant de référence pour les flux, même si elle n'est pas toujours respectée, ceci demeurant cependant rare. L'environnement cyber conserve donc les traits actuels que l'on vient d'énoncer et qui se prolongent. La lente balkanisation continue à s'opérer et l'isolat européen se

renforce : de plus en plus protecteur pour les données, c'est un espace géographique et juridique de plus en plus contraignant pour les plateformes qui, condamnées à des amendes, voient leur profitabilité diminuer.

4.3.4. Scénario B : généralisation de l'insécurité numérique

Il n'est pas improbable de songer à une accélération des rythmes avec une forte extension des cyber-agressions à portée économique, celles-ci couvrant les fraudes et vol de données jusqu'à l'espionnage d'origine étatique. Ceci suppose la persistance du *soft law* par refus des États de s'engager dans la voie contraignante du *hard law*. Le cadre juridique est gelé transformant *de facto* l'environnement cyber en un *far west* derrière les apparences rassurantes des multiples gouvernances. Le caractère relatif de la cybersécurité n'empêche pas ce secteur de prospérer au sein de la nouvelle économie. A l'heure du développement de l'Internet des objets et des progrès de la généralisation des connexions, la prédation des données ouvre de nouveaux champs délictuels et criminels qui sont de forme numérique mais d'application anthropique. L'intérêt de ce scénario est de montrer que des États et des manufactures criminelles numériques peuvent avoir un intérêt commun dans le caractère anomique de l'environnement cyber. Dans ce cadre la neutralité du net n'est plus que de façade, un principe fondateur aussi souvent rappelé qu'il ne correspond plus à la réalité. A la balkanisation évoquée *supra* s'ajoute une nouvelle balkanisation, technique, amenant les fournisseurs d'accès à privilégier les personnes morales sur les utilisateurs individuels. L'UE demeure un isolat normatif sans parvenir à maîtriser techniquement et judiciairement l'extension des cyber-agressions.

4.3.5. Scénario C : la victoire partielle des *majors*

On peut par ailleurs penser à la persistance d'un niveau de cyber-agression de moyenne intensité, soit parce que les structures criminelles n'ont pas les moyens de franchir un seuil supplémentaire, soit parce que les cibles potentielles prennent des mesures d'hygiène numérique et de précaution qui les tient à l'écart des intrusions les plus courantes. Seules demeurent des APT qui mobilisent de très puissants moyens criminels. Dans ce climat relativement pacifique où la nouvelle économie concentre de plus en plus la création de valeur et les résultats de l'innovation, les *majors* du numérique qui ont su minorer leurs rivalités afin de faire front commun de *lobbying*, récoltent les fruits de leur forte présence et de leur investissement dans la gouvernance *multi-stakeholder* ainsi que les résultats de leurs échanges réguliers avec les États. Ils sont parvenus à faire avaliser plusieurs principes nouveaux qui refondent l'environnement cyber : d'une part, ils ont réussi à faire reconnaître dans le *hard law* la primauté pour le numérique de l'usage sur la propriété ; par ailleurs, ils sont parvenus à faire objectiver une propriété partagée sur les données personnelles ; enfin, les données des personnes morales ont un droit de priorité sur celles des internautes, ce

qui permet aux fournisseurs d'accès d'imposer des nouveaux tarifs : la NN est défaite. Mais l'Europe a résisté à ces évolutions et les *majors* n'ont pu faire prévaloir ces innovations qu'en Amérique latine et en Afrique. Le pivot stratégique vers l'Asie engagé en 2009 se poursuit et les États-Unis qui appuient les *majors* tentent de gagner l'Asie-Pacifique à leurs vues où ils comptent des alliés solides (Australie, Japon, Philippines, Vietnam). Ils trouvent l'opposition de la Chine qui veut faire prévaloir ses propres vues. Une autre bataille - numérique - y commence.

* Conclusion ?

Cyber optimisme ou cyber pessimisme ? La question n'est pas là. Il faut avant tout une évaluation réaliste de l'environnement cyber et c'est ce que nous avons voulu faire dans cette étude *Cyber Strategy : définir un horizon stratégique dans l'environnement cyber*. Sa compréhension nécessite une perspective qui sorte de l'immédiateté, d'où une approche combinant le passé récent et des vues prospectives. Seule l'attention à ce passé récent qui construit le présent permet de prendre la mesure des caractéristiques structurantes qui vont encadrer les développements à venir.

* Il importe toutefois de rappeler un certain nombre de **caractéristiques fondamentales de la cybersécurité**.

- (1) face au caractère extensif du réseau, il est évident que le principe d'économie des moyens invite à **focaliser l'attention sur** les points particulièrement exposés que sont **les noeuds critiques** (interconnexions, *data centers*, réseaux de secours…)
- (2) face à un Internet qui « n'a pas conçu pour être sécurisé » ainsi que le déclarait en 2010 Bernard Barbier, il importe de faire désormais du **« security by design »** aussi bien dans le hard que dans la couche logicielle. Le souci de la sécurité doit exister dès la conception.

* Pour les acteurs étatiques et non-étatiques, mettre en œuvre **une stratégie dans le cyber** suppose de **comprendre** :

- (1) **la transversalité de l'environnement** car le cyber innerve tout et de ne pas le limiter à sa dimension la plus visible qui est l'aspect informationnel ;
- (2) les caractéristiques et les ressorts de **la gouvernance *multi-stakeholder*** où acteurs publics et privés doivent tenir compte de leur caractéristiques respectives et de leurs contraintes spécifiques ;
- (3) **l'idéologie** à l'œuvre, car on a vu l'influence latente des principes fondamentaux qui quoique assez largement idéaux servent encore à mobiliser les différents acteurs ;
- (4) la **composante socio-politique de l'environnement** aux effets majeurs, que ce soit sur un plan technologique ou économique.

En fait, il n'y a pas d'autonomie du cyber par rapport aux autres aspects stratégiques. L'environnement cyber participe désormais d'une approche globale de la stratégie. Les acteurs économiques et régaliens s'affrontent dans l'environnement cyber dans le cadre de leurs rapports de forces généraux. Cet environnement particulier est devenu un terrain privilégié : il est particulièrement attractif car il permet de créer des dommages et des préjudices de façon discrète sans possibilité d'attribution. De ce point de vue, on peut estimer que l'environnement cyber est désormais le terrain majeur d'affrontement indirect. L'in-attribution favorise les stratégies indirectes pour tous les acteurs ayant un certain seuil (bas) de maitrise

technologique. Le développement de l'environnement cyber est d'une certaine façon un égalisateur de puissance.

* Remerciements

- La mise en forme matérielle de cette étude doit à l'aide de M. Michel COURTY. Qu'il en soit vivement remercié.

- Mes remerciements vont également à la société SPALLIAN (http://www.spallian.com/) pour m'avoir autorisé à utiliser son logiciel de cartographie CORTO :

et tout particulièrement à MM. Guillaume FARDE et Michael VOISIN.

- Ce travail a bénéficié de l'aide de M. Clément CASTANO pour la collation des sources indiquées en fin de volume.

* Sources et bibliographie

* Sources

1. Documents fondamentaux des SMSI/WSIS de 2003 et 2005
2. Documents fondamentaux des IGF
3. Documents fondamentaux du W3C
4. Documents fondamentaux de l'IETF
5. Documents fondamentaux de l'ICANN
6. Documents fondamentaux du Governmental Advisory Committee de l'ICANN
7. Normes internationales en matière de Cybersécurité
8. Documents fondamentaux du CCD CoE Talinn et de l'ENISA
9. Documents sur le sommet de Dubaï de décembre 2012
10. Documents fondamentaux de l'IANA Stewardship Transition Coordination Group
11. Documents fondamentaux de l'ISACA
12. Textes et positions des États, gouvernements nationaux et des organisations régionales
13. Essais, textes d'intervention et pamphlets

Les sources ont été l'objet d'un travail de collation effectué par M. Clément Castano.

1. **Documents fondamentaux des SMSI/WSIS de 2003 et 2005**

(ordre chronologique)

- SMSI Genève (1ère phase – 10-12 décembre 2003) :
https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf
et reproduit également dans : Union Internationale des Télécommunications, *SMSI Documents Finals*, Genève, Suisse, 2006, 102 p. (https://www.itu.int/wsis/outcome/booklet-fr.pdf)

- WTSI Tunis (2ème phase – 16-18 novembre 2005) :
Union Internationale des Télécommunications, *SMSI Documents Finals*, Genève, Suisse, 2006, 102 p. https://www.itu.int/wsis/outcome/booklet-fr.pdf

2. **Documents fondamentaux des IGF**

(ordre chronologique)

- Internet Governance Forum, *IGF : The first two years*, Avri Doria and Wolfgang Kleinwächter & secrétariat de l'IGF, 2007, 414 p.
- Internet Governance Forum, *Proceedings of the Third Internet Governance Forum*, Hyderabad, Inde, Don MacLean, octobre 2009, 404 p.
- Internet Governance Forum, *Internet Governance : creating opportunities for all*, New-York, États-Unis, William J. Drake & The United Nations Department of Economic and Social Affairs, 2010, 554 p.
- Internet Governance Forum, *IGF 2010 - Developing the Future Together*, Nairobi, Kenya, Brian Gutterman & Publishing Services Section UNON, 2011, 348 p.
- Internet Governance Forum, *Internet as a catalyst for change: access, development, freedoms and innovation*, Naïrobi, Kenya, Brian Gutterman & Publishing Services Section UNON, 2012, 509 p.
- Internet Governance Forum, *IGF 2012 – 'Internet Governance for Sustainable Human, Economic and Social Development'*, New-York, États-Unis, Organisation des Nations Unies, 2013, 527 p.
- Internet Governance Forum, *IGF 2013—'Building Bridges–Enhancing Multistakeholder Cooperation for Growth and Sustainable Development'*, New-York, États-Unis, Organisation des Nations Unies, 2013, 553 p.

3. **Documents fondamentaux du W3C**

(ordre chronologique)

- W3C, *Membership FAQ*, Boston, États-Unis, Massachusetts Institute of Technology, 2014, http://www.w3.org/Consortium/membership-faq#who
- W3C, *Membership mission*, Boston, États-Unis, Massachusetts Institute of Technology, 2014, http://www.w3.org/Consortium/mission#vision
- W3C, *W3C process document*, Boston, États-Unis, Massachusetts Institute of Technology, 2014, http://www.w3.org/2005/10/Process-20051014/groups.html#GroupsWG

4. Documents fondamentaux de l'IETF

(ordre chronologique)

- IETF, *Le Tao de l'IETF : Guide destiné aux nouveaux participants à l'Internet Engineering Task Force*, IETF Trust, 2012, 38 p., http://www.ietf.org/tao.html.

5. Documents fondamentaux de l'ICANN

(ordre chronologique)

- ICANN, *Board of Directors' Code of Conduct*, Marina Del Rey, États-Unis, 6 mai 2012, 7 p., https://www.icann.org/resources/p./code-of-conduct-2012-05-15-en.
- ICANN, *Articles of Incorporation of Internet Corporation for Assigned Names and Numbers*, Marina Del Rey, États-Unis, 2014, 4 p., https://www.icann.org/resources/p./articles-2012-02-25-en.
- ICANN, *Règlement de l'ICANN*¸ Marina Del Rey, États-Unis, 2014, 138 p., https://www.icann.org/resources/p./bylaws-2012-02-25-fr.
- ICANN, *Conflicts of Interest Policy*, Marina Del Rey, États-Unis, 2014, https://www.icann.org/resources/p./coi-2012-02-25-en
- ICANN, *Governance Guidelines*, Marina Del Rey, États-Unis, 2014, 16 p., https://www.icann.org/resources/p./guidelines-2012-05-15-en.
- ICANN, *Final Implementation Plan for IDN ccTLD Fast Track Process*, Marina Del Rey, États-Unis, 16 novembre 2009, 59 p.
- ICANN, *Final Implementation Plan for IDN ccTLD Fast Track Process*, Marina Del Rey, États-Unis, 15 décembre 2011, 59 p.
- ICANN, *Final Implementation Plan for IDN ccTLD Fast Track Process*, Marina Del Rey, États-Unis, 4 juin 2012, 55 p.
- ICANN, *Domains Fact Sheet*, Marina Del Rey, États-Unis, 4 avril 2012, 1 page.
- ICANN, *Enabling a Multilingual Internet*, Marina Del Rey, États-Unis, 1er novembre 2013, 2 p.
- ICANN, *Summary: conflicts of interest and ethics practices review*, Marina Del Rey, États-Unis, 13 mai 2013, 5 p.
- Fadi Chehadé, « Internet : une gouvernance en mouvement », Paris, France, IFRI, 15 avril 2015, http://www.dailymotion.com/video/x2nncdy_fadi-chehade-internet-une-gouvernance-en-mouvement_news

6. Documents fondamentaux du Governmental Advisory Committee (GAC) de l'ICANN

(ordre chronologique)

- GAC, *Lignes directrices du GAC pour les réunions gouvernementales de haut niveau*, Londres, Royaume-Uni, ICANN, mars 2015, 8 p.
- GAC, *Procès-verbal de réunion*, Singapour, ICANN, 12 février 2015, 22 p.
- GAC, *Communiqué du GAC*, Singapour, ICANN, 11 février 2015, 7 p.
- GAC, *Présentation du Comité consultatif gouvernemental de l'ICANN (GAC)*, Londres, Royaume-Uni, ICANN, 2015, 13 p.
- GAC, *Procès-verbal de réunion*, Los Angeles, États-Unis, ICANN, 16 octobre 2014, 16 p.
- GAC, *Communiqué du GAC*, Los Angeles, États-Unis, ICANN, 15 octobre 2014, 10 p.

- VAIZEY (Ed), *Rapport du président sur la réunion gouvernementale de haut niveau de l'ICANN*, Londres, Royaume-Uni, Secrétariat du GAC, 23 juin 2014, 28 p.

7. Normes internationales en matière de cybersécurité (normes ISO…)

(ordre chronologique)

- BOCK (Patrick), *La norme ISA 99 progresse !*, Secur'id blog, 15 mars 2013, http://securid.novaclic.com/cyber-securite-industrielle/la-norme-isa-99-progresse.html
- HUMPHREYS (Edward J.), *La nouvelle cyberguerre*, ISO, 9 octobre 2013, http://www.iso.org/iso/fr/home/news_index/news_archive/news.htm?Refid=Ref1785
- ISA France, *Cybersécurité des installations industrielles : la norme CEI 62443 (ISA99) progresse*, 14 mars 2013, 3 p.
- ISO/CEI 27032:2012, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour la cybersécurité*, http://www.iso.org/iso/fr/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375

- ISO/IEC JTC 1/SC 27, *Techniques de sécurité des technologies de l'information*, http://www.iso.org/iso/fr/iso_technical_committee?commid=45306

8. Documents fondamentaux du CCD CoE Talinn et de l'ENISA

(ordre chronologique)

* CCDCOE

- Groupe International d'Experts, *Eléments préparatoires au manuel de Tallinn*, Cambridge, Royaume-Uni, Cambridge University Press, 2013, 215 p.
- CCDCOE, *National CyberSecurity Framework Manual*, Tallinn, Estonie, OTAN (Alexander Klimburg), 2012, 253 p.
- Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, Cambridge University Press, 2013, 282 p.

* ENISA
- ENISA, *Guide de création d'un CSIRT pas à pas,* Résultats CERT-D1 & D2 (5.1) du programme de travail 2006, Héraklion, Grèce, 2006, 90 p.
- ENISA, *Sensibilisation des organismes financiers à la sécurité de l'information*, Héraklion, Grèce, 25 novembre 2009, 54 p., https://www.enisa.europa.eu/publications/archive/is-in-financial-organisations-fr/at_download/fullReport
- ENISA, *Programme de travail 2010*, Héraklion, Grèce, 9 novembre 2009, 63 p., https://www.enisa.europa.eu/media/enisa-en-francais/news-items/fr_work-programme-2010
- ENISA, *ENISA ISACA Cyber Security Workshop – Highlights*, Berlin, Allemagne, 11 juin 2013, 7 p.

9. Documents sur le sommet de Dubaï de décembre 2012

(ordre chronologique)

- Union Internationale des Télécommunications, *Proposals received from ITU member states for the work of the conference*, Genève, Suisse, 3 décembre 2012, 5 p., http://www.itu.int/md/S12-WCIT12-121203-TD-0001/fr
- Union Internationale des Télécommunications, *Règlement des télécommunications internationales - Melbourne – 1988*, Genève, Suisse, Actes Finals de la conférence administrative mondiale télégraphique et téléphonique, 1989, 105 p., http://www.itu.int/dms_pub/itu-t/oth/3F/01/T3F010000010001PDFF.pdf
- Union Internationale des Télécommunications, *WCIT2012 Finals Acts signatories*, Genève, Suisse, 2012, 1 page, http://www.itu.int/osg/wcit-12/highlights/signatories.html
- Union Internationale des Télécommunications, *Actes Finals de la conférence mondiale des télécommunications internationales – Dubaï 2012*, Dubaï, Emirats Arabes Unis, 2012, 30 p., http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12-fr.pdf

10. Documents fondamentaux de l'IANA Stewardship Transition Coordination Group (ICG)

(ordre chronologique)

- IANA Stewardship Transition Coordination Group (ICG), *Déclaration du Groupe de coordination de la transition du rôle de supervision des fonctions IANA (ICG) à l'issue de sa première réunion*, Londres, Royaume-Uni, 18 juillet 2014, 2 p.
- IANA Stewardship Transition Coordination Group (ICG), *Charte du groupe de coordination du rôle de supervision des fonctions*, Marina Del Rey, États-Unis, 10e édition, 27 août 2014, 7 p.
- IANA Stewardship Transition Coordination Group (ICG), *Lignes directrices de l'ICG pour la prise de décisions*, Marina Del Rey, États-Unis, 17 septembre 2014, 5 p.
- IANA Stewardship Transition Coordination Group (ICG), *Proposition pour la transition de la supervision de l'IANA - Réunion et processus de finalisation*, Marina Del Rey, États-Unis, 18 décembre 2014, 4 p.
- IANA Stewardship Transition Coordination Group (ICG), *IANA Stewardship Transition Coordination Group*, Marina Del Rey, États-Unis, 7 janvier 2015, 2 p.

11. Documents fondamentaux de l'ISACA (Information Systems Audit and Control Association)

(ordre chronologique)

- ISACA, *European Cybersecurity Implementation: Overview*, Rolling Meadows, États-Unis, Cybersecurity Nexus, 2014, 26 p.
- ISACA, *European Cybersecurity Implementation: Assurance*, Rolling Meadows, États-Unis, Cybersecurity Nexus, 2014, 24 p.
- ISACA, *2013 Annual Report*, Rolling Meadows, États-Unis, 2014, 24 p.

12 Textes et positions des États, gouvernements nationaux et des organisations régionales

(ordre chronologique)

- OCDE, *Les Risques émergents au XXIe siècle. Vers un programme d'action*, Paris, OCDE, 2003, 325 p.
- Conseil européen, *Directive 2009/140/EC of the European Parliament and of the Council*, Bruxelles, Belgique, 25 novembre 2009, 33 p.
- Chantal Bernier, *Nouvelles plateformes, nouvelles mesures de protection : protéger la vie privée dans le cyberespace*, Toronto, Ontario, Commissariat à la protection de la vie privée du Canada, 23 février 2011, https://www.priv.gc.ca/media/sp-d/2011/sp-d_20110223_cb_f.asp
- Chantal Bernier, *Discussion sur l'équilibre entre la protection des renseignements personnels et l'application de la loi*, Toronto, Ontario, Commissariat à la protection de la vie privée du Canada, 28 mars 2011, https://www.priv.gc.ca/media/sp-d/2011/sp-d_20110328_cb_f.asp
- *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world,* Cabinet Office, November 2011, 43 p.

- International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World, Washington, The White House, May 2011, 25 p.
- ANSSI, *Défense et sécurité des systèmes d'information. Stratégie de la France*, Paris, ANSSI, 2011, 22 p.
- OECD, *Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national cybersecurity strategies for the Internet economy*, OECD, 2012, 116 p.
- Conseil de l'Europe, *Stratégie de gouvernance de l'Internet 2012-2015*, 15 mars 2012, 12 p.
- Pierre Collin et Nicolas Colin, *Mission d'expertise sur la fiscalité de l'économie numérique*, Ministère de l'économie et des finances, janvier 2013, 152 p.
- Claude Revel, *Développer une influence normative internationale stratégique pour la France*, Bercy, 31 janvier 2013, 101 p. Rapport remis à Nicole Bricq, ministre au Commerce extérieur.
- Commission européenne, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Joint communication to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, 7 février 2013, 20 p.
- Commission européenne, *Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, 7 février 2013, 48 p.
- Laurent Gille (dir.), *La dynamique d'Internet. Prospective 2030*, Commissariat général à la stratégie et à la prospective, Étude n° 01, mai 2013, 203 p.
- Contre-amiral Arnaud Coustillière, "La cyberdéfense: un enjeu global et une priorité stratégique pour le ministère de la défense", *Sécurité globale*, printemps 2013, p. 27-32.
- Conseil de l'Europe, *Déclaration du Comité des Ministres sur les risques présentés par le suivi numérique et les autres technologies de surveillance pour les droits fondamentaux*, 12 juin 2013, 2 p.
- *G8 Open Data Charter*, London, UK, June 2013, 10 p.
- *G8 Open Data Charter and Technical Annex*, London, UK, June 2013, 8 p., https://www.gov.uk/government/publications/open-data-charter/g8-ope
- Bruno Sido et Jean-Yves Le Déaut, *Le risque numérique: en prendre conscience pour mieux le maîtriser ?*, Assemblée nationale n° 1221-Sénat n° 721, 3 juillet 2013, OPECST, 109 p.
- Marie-Pierre Hamel et David Marguerit, *Analyse des big data. Quels usages, quels défis ?*, Commissariat général à la stratégie et à la prospective, Note d'analyse n° 8, novembre 2013, 12 p.
- Nathalie Chiche, *Internet: pour une gouvernance ouverte et équitable*, Paris, CESE-Section des affaires européennes et internationales, 11 décembre 2013, 59 p.
- *The President's Review group on Intelligence and Communications Technologies, Liberty and Security in a Changing World,* 12 December 2013, 304 p.
- *Livre blanc. Défense et sécurité nationale*, Paris, Ministère de la Défense, 2013, 160 p. Préface du Président de la République.

- OECD, « Synthèse », in OECD, *Relever les défis fiscaux posés par l'économie numérique*, OECD Publishing, Paris, p. 11-24.
http://dx.doi.org/10.1787/9789264225183-3-fr
- OECD, "The digital economy today", in OECD, *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, p. 25-47.
http://dx.doi.org/10.1787/9789264221796-5-en
- *Handbook on European data Protection Law*, Council of Europe-European Court of Human Rights, 2014, 210 p.
- *Pacte Défense Cyber:50 mesures pour changer d'échelle*, Paris, Ministère de la Défense-Dicod, 2014, 22 p.
- Philippe Lemoine, *La Nouvelle grammaire du succès. La transformation numérique de l'économie française. Rapport au gouvernement,* 2014, 37 p.
- Catherine Morin-Desailly, *Rapport d'information fait au nom de la mission commune d'information sur le « nouveau rôle et la nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet »*, Sénat, n° 696, 8 juillet 2014, 398 p.
- World Economic Forum and McKinsey Quarterly, *Risk and Responsibility in a Hyperconnected World*, January 2014, 37 p.
- Conseil de l'Europe, *Manuel de droit européen en matière de protection des données*, Strasbourg, Conseil de l'Europe, 2014, 2009 p.
- Conseil d'État, *Le numérique et les droits fondamentaux*, Paris, Documentation française, « Les rapports du Conseil d'État », 2014, 441 p.
- p fait Julia Charrié et Lionel Janin, *La Fiscalité du numérique*, France Stratégie, mars 2015, n° 26, 8 p.
- Alain Pellet, *The Independent Objector and ICANN's New Generic topLevel Domains Program*, Final Activity Report, 2015, 58 p.
- ITU-UIT, *Indice de cybersécurité dans le monde et profils de cyber bien-être*, avril 2015, 528 p.

13 Essais, textes d'intervention et pamphlets

(ordre chronologique)

- Dominique Cardon, *La démocratie Internet. Promesses et limites*, Paris, Seuil, « La République des idées », 2010, 101 p.
- Nicolas Colin et Henri Verdier, *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique*, Paris Armand Colin, 2012, 286 p.
- Eric Schmidt et Jared Cohen, *A nous d'écrire l'avenir*, Paris, Denoël, 2013, 380 p.
- Julian Assange, Jacob Appelbaum, Andy Müller-Maguhn et Jérémie Zimmermann, *Menace sur nos libertés: Comment Internet nous surveille, comment résister*, Paris, éditions Robert Laffont, 2013, 245 p.
- Viktor Mayer-Schönberger et Kenneth Cukier, *Big Data : la révolution des données et en marche*, Paris, Robert Laffont, 2014, 300 p.

* Bibliographie

(ordre chronologique)

- Pascal Griset, *Les Révolutions de la communication XIX^e^-XX^e^ siècles*, Paris, Hachette, « Carré-histoire », 1991, 255 p.
- Scott Bradner et Richard Hovey, *The Organizations Involved in the IETF Standards Process*, Cambridge, Harvard University, octobre 1996, 7 p.
- Manuel Castells, *La Société en réseaux. L'ère de l'information*, tome 1, Paris, Fayard, 1998, 671 p.
- Pierre Tabatoni (dir.), *La Protection de la vie privée dans la société d'information*, Paris, PUF, "Cahiers des sciences morales et politiques", 2000-2002, 5 tomes, 3 volumes.
- Bertrand Warusfel, "La gestion de l'Internet entre autorégulation et rivalités institutionnelles : un phénomène mondial à la recherche de son modèle de gouvernance", *Annuaire français des relations internationales*, Paris, France, 2000, 23 p.
- Tim Wu, « Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and High Technology Law*, vol. 2, 2003, p. 141-178.
- Gilles Puel et Charlotte Ullmann, « Les nœuds et les liens du réseau Internet : approche géographique, économique et technique », *L'Espace géographique, n° 2,* 2006, tome 35, p. 97-114 (www.cairn.info/revue-espace-geographique-2006-2-page-97.htm).
- Daniel Ventre, *La Guerre de l'information*, Paris, Hermès sciences publications, 2007, 282 p.
- Jeannine Gerbault (dir.), *La langue du cyberespace : de la diversité aux normes*, Paris, L'Harmattan, 2007, 298 p.
- Jeremy Malcolm, *Multi-Stakeholder Governance and the Internet Governance Forum,* Wembley, WA : Terminus Press, 2008, 641 p.
- Myriam Quéméner et Joël Ferry, *Cybercriminalité : défi mondial*, Paris, Economica, 2009, 308 p.
- Marjory S. Blumenthal and David D. Clark, "The Future of the Internet and Cyberpower", in : Franklin D. Kramer, Stuart H. Starr, Larry Wentz (dir.), *Cyberpower and National Security*, Washington, National Defense University Press, 2009, p. 206-240.
- Franklin D. Kramer and Larry K. Wentz, "Cyber Influence and International Security", in : Franklin D. Kramer, Stuart H. Starr, Larry Wentz (dir.), *Cyberpower and National Security*, Washington, National Defense University Press, 2009, p. 343-361.
- Harold Kwalwasser, "Internet Governance", in : Franklin D. Kramer, Stuart H. Starr, Larry Wentz (dir.), *Cyberpower and National Security*, Washington, National Defense University Press, 2009, p. 491-524.

- Thomas C. Wingfield, "International Law and Information Operations", in : Franklin D. Kramer, Stuart H. Starr, Larry Wentz (dir.), *Cyberpower and National Security*, Washington, National Defense University Press, 2009, p. 525-542.
- Daniel Ventre (dir.), *Cyberguerre et guerre de l'information: stratégies, règles, enjeux*, Paris, Hermès sciences publications, 2010, 319 p.
- Patrick Jacob, "La gouvernance de l'Internet du point de vue du droit international public", *Annuaire français de droit international*, 2010, LVI, p. 543-563.
- Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge, MIT Press, 2010, 313 p.
- Fabrice Rochelandet, *Economie des données personnelles et de la vie privée*, Paris, La Découverte, "Repères", 2010, 128 p.
- Simon Chesterman, "Privacy and Surveillance in the Age of Terror", *Survival*, 52-5, 2010, p. 31-46.
- Frédéric Ocqueteau et Daniel Ventre (dir.), « Contrôles et surveillances dans le cyberespace », *Problèmes politiques et sociaux*, n° 988, Septembre 2011, 121 p.
- Stein Schjolberg and Solange Ghernaouti-Hélie, *A Global Treaty on Cybersecurity and Cybercrime : a Contribution for Peace, Justice and Security in Cyberspace*, 2011, 89 p.
- Daniel Ventre, *Cyberespace et acteurs du cyberconflit*, Paris, Hermès sciences publications, 2011, 283 p.
- Nicolas Curien et Winston Maxwell, *La Neutralité d'Internet,* Paris, La Découverte, 2011, 128 p.
- Daniel Ventre, *Cyberattaque et cyberdéfense*, Paris, Hermès sciences publications, 2011, 312 p.
- Christopher T. Mardsen, *Internet Co-Regulation. European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge, Cambridge University Press, 2011, 284 p.
- Divina Frau-Meigs, Jérémie Nicey, Michael Palmer, Julia Pohle and Patricio Tupper (ed.), *From NWICO to WSIS : 30 Years of Communication Geopolitics. Actors and Flows, Structures and Divides*, Bristol, Intellect, 2012, 240 p.
- Jovan Kurbalija, *An Introduction to Internet Governance*, Geneva, Diplo Foundation, 2012 [5th ed., first : 2008], 197 p.
- Jean-Michel Salaün, *Vu, lu, su. Les architectes de l'information face à l'oligopole du Web*, Paris, La Découverte, « Cahiers libres », 2012, 152 p.
- CLUSIF, *Menaces informatiques et pratiques de sécurité en France*, 2012, CLUSIF, 110 p.
- « Histoire de l'Internet, l'Internet dans l'histoire », *Le Temps des médias*, n° 18, 2012-1, 280 p.
  dont: Paul E. Ceruzzi, "Aux origines américaines de l'Internet: projets militaires, intérêts commerciaux, désirs de communauté", *Le Temps des médias*, n° 18, 2012-1, p. 15-28.
  dont: Françoise Massit-Folléa, "La gouvernance de l'Internet. Une internationalisation inachevée", *Le Temps des médias*, n° 18, 2012-1, p. 29-40.
- "Internet, outil de puissance", *Politique étrangère*, été 2012, n° 2, p. 245-328.
  dont: Bertrand de La Chapelle, "Gouvernance Internet: tensions actuelles et futurs possibles", *Politique étrangère*, été 2012, n° 2, p. 249-262.

dont: Wolfgang Kleinwächter, "Internet, sociétés civiles et gouvernements: cohabitation ou choc des cultures ?", *Politique étrangère*, été 2012, n° 2, p. 263-276.
dont: Michel Baud, "La Cyberguerre n'aura pas lieu, mais il faut s'y préparer", *Politique étrangère*, été 2012, n° 2, p. 305-3016.
- Eric Freyssinet, *La Cybercriminalité en mouvement*, Paris, Hermès Science Publication, « Management et informatique », 2012, 256 p.
- Myriam Quéméner et Jean-Paul Pinte, *Cybersécurité des acteurs économiques. Risques, réponses stratégiques et juridiques*, Paris, Hermès sciences publications, 2012, 239 p.
- Eric Brousseau, Meryem Marzouki and Cécile Méadel (eds.), *Governance, Regulations and Powers on the Internet*, Cambridge : Cambridge University Press, 2012, 445 p.
- Olivier Kempf, *Introduction à la cyberstratégie*, Paris, Economica, 2012, 176 p.
- Benjamin Loveluck, *La Liberté par l'information. Généalogie politique du libéralisme informationnel et des formes de l'auto-organisation sur Internet*, thèse de doctorat de science politique, EHESS, 4 décembre 2012, 672 p.
- Thomas Rid, *The Cyberwar will not take place,* London, Hurst, 2013, 218 p.
- UNIDIR, *The Cyber Index. International security Trends and Realities*, United Nations, New York and Geneva, 2013, 138 p.
- David Fayon, *Géopolitique de l'Internet: Qui gouverne le monde ?*, Paris, Ecomonica, 2013, 199 p.
- Laura DeNardis, « The Emerging Field of Internet Governance », *The Oxford Handbook of Internet Studies*, Oxford, Oxford University Press, 2013, p. 555-575.
- Antoinette Rouvroy et Thomas Bern, "Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation", *Réseaux*, n° 117, 2013-1, p. 163-196.
- Solange Ghernaouti, *Cyber Power. Crime, conflict and security in cyberspace*, Lausanne, EPFL Press, 2013, 446 p.
- Dennis Weller and Bill Woodcock, "Internet Traffic Exchange: Market Developments and Policy Challenges", *OECD Digital Economy Papers*, n° 207, OECD Publishing, 2013, 99 p. (http://dx.doi.org/10.1787/5k918gpt130q-en)
- Francesca Musiani, *Nains sans géants. Architecture décentralisée et services Internet*, Paris, Presses de l'Ecole des mines, 2013, 272 p.
- Dominique Boullier, "Le « hard » du « soft » : la matérialité du réseau des réseaux", *CERISCOPE Puissance*, 2013, URL : http://ceriscope.sciences-po.fr/puissance/content/part2/le-hard-du-soft-la-materialite-du-reseau-des-reseaux [consulté le 21/06/2014]
- Brandon Valeriano and Ryan Maness, "The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011", 2013 (SSRN: http://ssrn.com/abstract=2214332 or http://dx.doi.org/10.2139/ssrn.2214332)
- Laura DeNardis, *The Global War for Internet Governance*, New Haven-London, Yale University Press, 2014, 296 p.
- Daniel Ventre (ed.), *Chinese Cybersecurity and Defense*, Hoboken, Wiley ISTE, 2014, 320 p.
- Olivier Sichel, *L'échiquier numérique américain : Quelle place pour l'Europe ?*, Paris, IFRI, « Potomac Papers », septembre 2014, 32 p.

- « Internet Governance », *Revue française d'études américaines*, 4e trimestre 2014, n° 134, 126 p. :
dont : Divina Frau-Megies, "Conducting Research on the Internet and its Governance", *Revue française d'études américaines*, 4e trimestre 2014, n° 134, p. 4-24.
dont : Julia Pohle and Luciano Morganti, "The Internet Corporation for Assigned Names and Numbers (ICANN): Origins, Stakes and Tensions", *Revue française d'études américaines*, 4e trimestre 2014, n° 134, p. 29-46.
dont : Francesca Musiani, Valérie Schafer and Hervé Le Crosnier, "Net Neutrality as an Internet Governance Issue: the Globalization of an American Debate", *Revue française d'études américaines*, 4e trimestre 2014, n° 134, p. 57-63.
dont : Jeanette Hofmann, "Narratives of Copyright Enforcement: The Upward Ratchet and the Sleeping Giant", *Revue française d'études américaines*, 4e trimestre 2014, n° 134, p. 64-80.
dont : Mathieu O'Neil, "Collaborative Internet Governance: Terms and Conditions of Analysis", *Revue française d'études américaines*, 4e trimestre 2014, n° 134, p. 98-113.
dont : Peng Hwa Angand Natalie Pang, "Globalization of the Internet, Sovereignty or Democracy: The Trilemna of the Internet Governance Forum", *Revue française d'études américaines*, 4e trimestre 2014, n° 134, p. 114-127.
- Philippe Boulanger, *Géopolitique des médias. Acteurs, rivalités et conflits*, Paris, Armand Colin, « U », 2014, 310 p.
- Sébastien Laurent, *Atlas du renseignement. Géopolitique du pouvoir,* Paris, Presses de Sciences-Po, 2014, 190 p.
- Laura DeNardis, *The Global War for Internet Governance*, New Haven-london, Yale University Press, 2014, 296 p.
- Daniel Ventre, *Impact de la cyberguerre sur les conflits armés*, thèse de doctorat en science politique sous la direction de Xavier Crettiez, Université de Versailles Saint-Quentin, 3 juin 2014, 497 p.
- Antoinette Rouvroy, « Des données sans personne : le fétichisme de la donnée à caractère personnel à l'épreuve de l'idéologie des *big data* », dans : Conseil d'État, *Le numérique et les droits fondamentaux*, Paris, Documentation française, « Les rapports du Conseil d'État », 2014, p. 407-421.
- Stéphanie Aubert et Thierry Autret, « Cybermenaces et sécurité nationale », dans Christian Vallar et Xavier Latour (dir.), L*a droit de la sécurité et de la défense en 2013*, Aix, Presses universitaires d'Aix-Marseille, 2014, p. 313-322.
- "Cyberespace: enjeux géopolitiques", *Hérodote*, 1er-2e trimestre 2014, n° 152-153, 312 p.
dont : Stéphane Frénot et Stéphane Grumbach, "Les données sociales, objets de toutes les convoitises", *Hérodote*, 1er-2e trimestre 2014, n° 152-153, p. 43-66.
- Frédéric Ocqueteau et Daniel Ventre, « D'une stratégie de cyberdéfense à un souci pour le cybercrime. Lenteurs et accélérations d'une mutation au cœur de l'État », *Revue internationale de criminologie et de police technique et scientifique*, vol. LXVII, n°3, 2014, p. 352-372.

- CEIS, *Les droits maritimes et de l'espace peuvent-ils inspirer un droit du cyberespace ?*, Paris, CEIS, 2014, 66 p.
- Didier Danet et Amaël Cattaruzza (dir.), *La Cyberdéfense. Quel territoire, quel droit ?*, Paris, Economica, 2014, 288 p.
dont : Amaël Cattaruzza, « Frontières du cyberespace. Eléments de réflexion sur la territorialisation d'Internet », Didier Danet et Amaël Cattaruzza (dir.), *La Cyberdéfense. Quel territoire, quel droit ?*, Paris, Economica, 2014, p. 21-33.
- "Internet: une gouvernance inachevée", *Politique étrangère*, hiver 2014-4 :
dont: Bernard Benhamou, "La gouvernance de l'Internet après Snowden", *Politique étrangère*, hiver 2014-4, p. 15-27.
dont : Françoise Massit-Folléa, "Internet et les errances du *multistakeholderism*", *Politique étrangère*, hiver 2014-4, p. 29-41.
dont : Francesca Musiani, "Neutralité de l'Internet : dépasser les scandales", *Politique étrangère*, hiver 2014-4, p. 57-68.
dont : Viktor Mayer-Schönberger, "La révolution Big Data", *Politique étrangère*, hiver 2014-4, p. 69-81.
- Godefroy Dang Nguyen et Sylvain Dejean, *Le Numérique. Economie du partage et des transactions*, Paris, Economica, 2014, 442 p.
- Sébastien Laurent, *Pour une véritable politique publique du renseignement*, Paris, Institut Montaigne, 2014, 96 p.
- Françoise Massit-Follé, Cécile Méadel et L. Monnoyer-Smith (dir.), *Normative Experience in Internet Politics*, Paris, Presses des Mines, 2015, 266 p.

* Liste des acronymes

- APT: Advanced Persistent Threat
- CC: Cybersphere Core
- CGO: Commission on Global Governance
- CERT: Computer Emergency Response Team
- GAC: Governmental Advisory Committee
- GCA : Global Cybersecurity Agenda
- ICANN: Internet Corporation for Assigned Names and Numbers
- IEC: International Electrotechnical Commission
- IETF: Internet Engineering Task Force
- ICCC : International Criminal Court or Tribunal for Cyberspace
- ICT: Information and Communications Technologies
- IGF: Internet Governance Forum
- ISO: International Organization for Standardisation
- ISP: Internet Services Providers
- ISOC: Internet Society
- ITU: International Telecommunication Union
- IXP: Internet eXchange Point
- MAG : Multistakeholder Advisory Group
- MOU: Memorandum of Understanding
- NN: Net Neutrality
- OECD: Organisation for Economic Co-operation and Development
- P2P: Peer-to-peer
- RFC: Requests for Comments
- RIR: Regional Internet Registry
- TRIPS: Trade Related Aspects of Intellectual Property Rights
- WGIG: Working Group on Internet Governance
- WIPO: World Intellectual Property Organization
- WSIS: World Summit on the Information Society
- WTO: World Trade Organization
- W3C: World Wide Web Consortium

* Table des graphes, tableaux, encarts, figures et cartes

* Table des matières