Rapport de recherche
ANR-14-CE28-0024-02

Programme « UTIC France-Europe »

UTIC
USAGES DES TECHNIQUES D'INTERCEPTION DE COMMUNICATIONS

Sébastien-Yves Laurent

Les gouvernances mondiales fragmentées de l'Internet

IRM
Institut de recherche Montesquieu

université de BORDEAUX

Livrable n° 8
v. 06

sebastien.laurent@u-bordeaux.fr
Université de Bordeaux

25 septembre 2019

Introduction

Ce dernier livrable du programme UTIC[1] prend pour objet les discours, les pratiques et les structures de gouvernance à l'échelle mondiale de l'Internet. Les deux premières parties sont un état des lieux diachronique de la gouvernance du réseau, bâti aux Etats-Unis (1re partie), qui s'est ensuite mondialisé, favorisant l'intervention de l'ONU avec une vision multilatéralisée de la gouvernance (2e partie). On souligne ensuite la faiblesse de la gouvernance en raison de tentatives inégalement abouties de réguler l'Internet par du *hard law*, laissant la place au règne des normes et du *soft law* (3e partie). A cela s'ajoute la forte polarisation du débat international sur le cyber par les enjeux de cybersécurité (4e partie) et l'échec d'une gouvernance globale par rapport aux idées initiales des Nations-Unies (5e partie). L'ensemble a abouti à des gouvernances mondiales fragmentées de l'Internet qui constituent l'un des traits du système international actuel (2019).

1 Le socle de l'Internet : le « cybersphere core » étatsunien

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 (IETF, ISOC, W3C, ICANN) 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 de la couche logicielle (cf. figure 3). Ces organisations ont toutes été créées aux États-Unis. Elles constituent le coeur de la cybersphère. Ayant une vocation extérieure, certaines ont adopté une structure internationale dans les années 1990. Mais février 2015, alors que la question de la réforme de l'ICANN avait été mise à l'agenda dans discussions internationales, Barack Obama a clairement rappelé:

> "We have owned the Internet. Our companies have created it, expanded it, perfected it in ways that they [les Européens] can't compete. And oftentimes what is portrayed as high-minded positions on issues sometimes is just designed to carve out some of their commercial interests"[2].

- 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)[3]. 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[4]. 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 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,

1. Nous remercions chaleureusement Daniel Ventre pour sa relecture très attentive.
2. 'http://recode.net/2015/02/15/white-house-red-chair-obama-meets-swisher/
3. https://www.ietf.org/iesg/area.html
4. Christopher T. Mardsen, *Internet Co-Regulation. European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge, Cambridge University Press, 2011, p. 105.

de promouvoir les valeurs et les principes fondateurs de l'Internet. 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 445 membres à l'été 2019[5].

- 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 (attribution des noms de domaines et d'adresses IP, soit la « fonction IANA ») 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 étatsunienne 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 2019, il y avait 178 membres et 36 observateurs au sein du GAC qui est une commission seulement consultative[6], mais dont le rôle n'a cessé de croître depuis sa mise en place en 1999. L'UE a essayé assez tôt de faire valoir un fonctionnement alternatif de l'ICANN, moins centré sur les États-Unis (Delmas in : Chatillon, 2002).

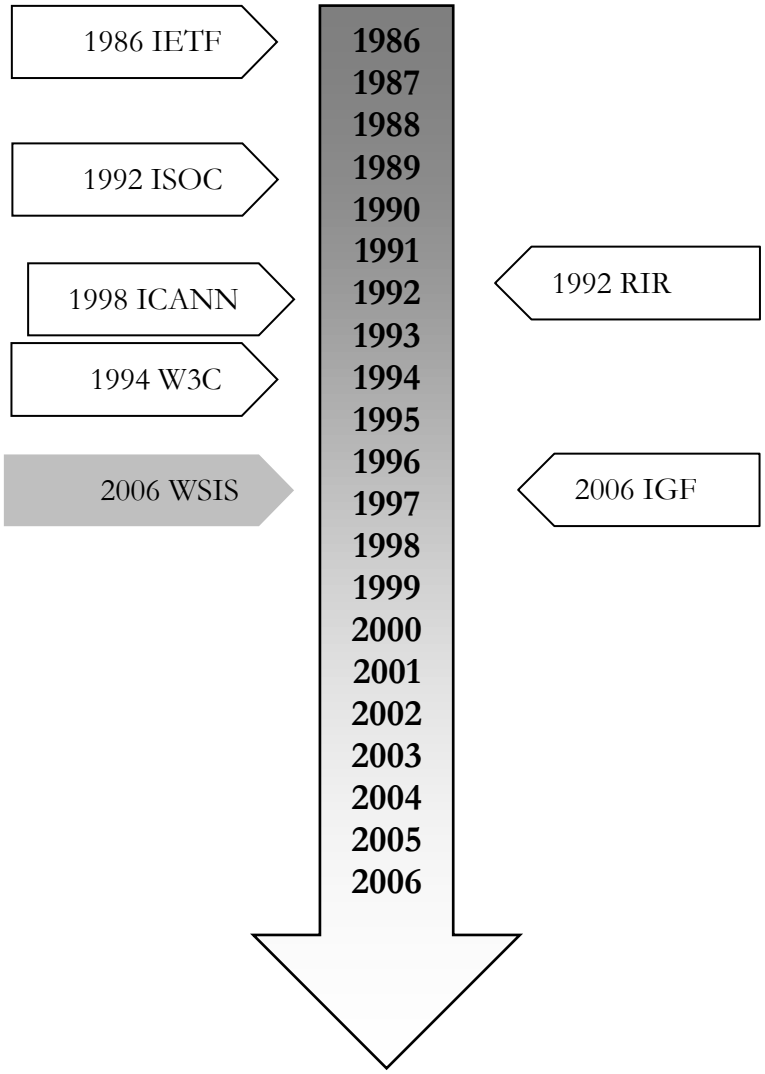
C'est donc l'ICANN qui gère les 5 Regional Internet Registry (RIR) mondiaux : le RIPE-NCC (« Réseaux IP Européens » – en français dans le texte - pour l'Europe et le Moyen-Orient), l'ARIN (*American Registry for Internet Numbers* pour l'Amérique du Nord), l'APNIC (*Asia Pacific Network Information Center*), 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 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 « par le bas », issues des communautés techniques, en entretenant des liens étroits entre elles. Elles sont le centre de la cybersphère, ce que nous appellerons ici par la suite le « cyberpshere core » (CC) (cf. figure 3).

Il faut noter la volonté nettement affirmée du Brésil en 2013 d'essayer de mettre en place une autre forme de gouvernance *multi-stakeholder*. Cette position 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).

5. http://www.w3.org/Consortium/Member/List [22/07/2015]
6. https://gac.icann.org/about/members [22/07/2019]

Figure 1 : chronologie de la Cybersphère



2 L'intervention de l'ONU et l'internationalisation de l'Internet aux origines de l'enjeu de la gouvernance

Jusqu'au début des années 2000, la cybersphère se limitait donc aux structures issues des communautés techniques. 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 à la transformation de la cybersphère.

2.1 La promotion onusienne d'un Internet comme « ressource publique mondiale »

- 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)[7].

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). Il s'agit là d'un élément de doctrine majeur pour les acteurs internationaux (États, ONG et sociétés civiles).

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 »**[8]. On voit la rupture potentielle que cette déclaration pouvait entraîner, par rapport à la petite cybersphère technique, seule existante à l'époque[9]. 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 le 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 ».

Figure 2 : les 4 « policy areas » du UN-Working Group on Internet Governance (2003-6)

1.	infrastructure and the management of critical Internet resources
2.	internet governance
3.	intellectual property rights / international trade
4.	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 (cf. *infra* en 5.1).

- La deuxième phase 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

7. 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.

8. « The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism" (https://www.itu.int/net/wsis/docs/geneva/official/dop.html)

9. On reviendra *infra* en 5.1. sur la gouvernance ?

multiplication des réunions et sommets internationaux sur l'environnement cyber. 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 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 doctrine *multi-stakeholder*, l'un de ses comités consultatifs étant le « Multistakeholder Advisory Group » (MAG) composé de 55 membres à l'été 2019[10] (nombre stable depuis plusieurs années). 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.

2.2 La minoration rapide du rôle de l'ITU

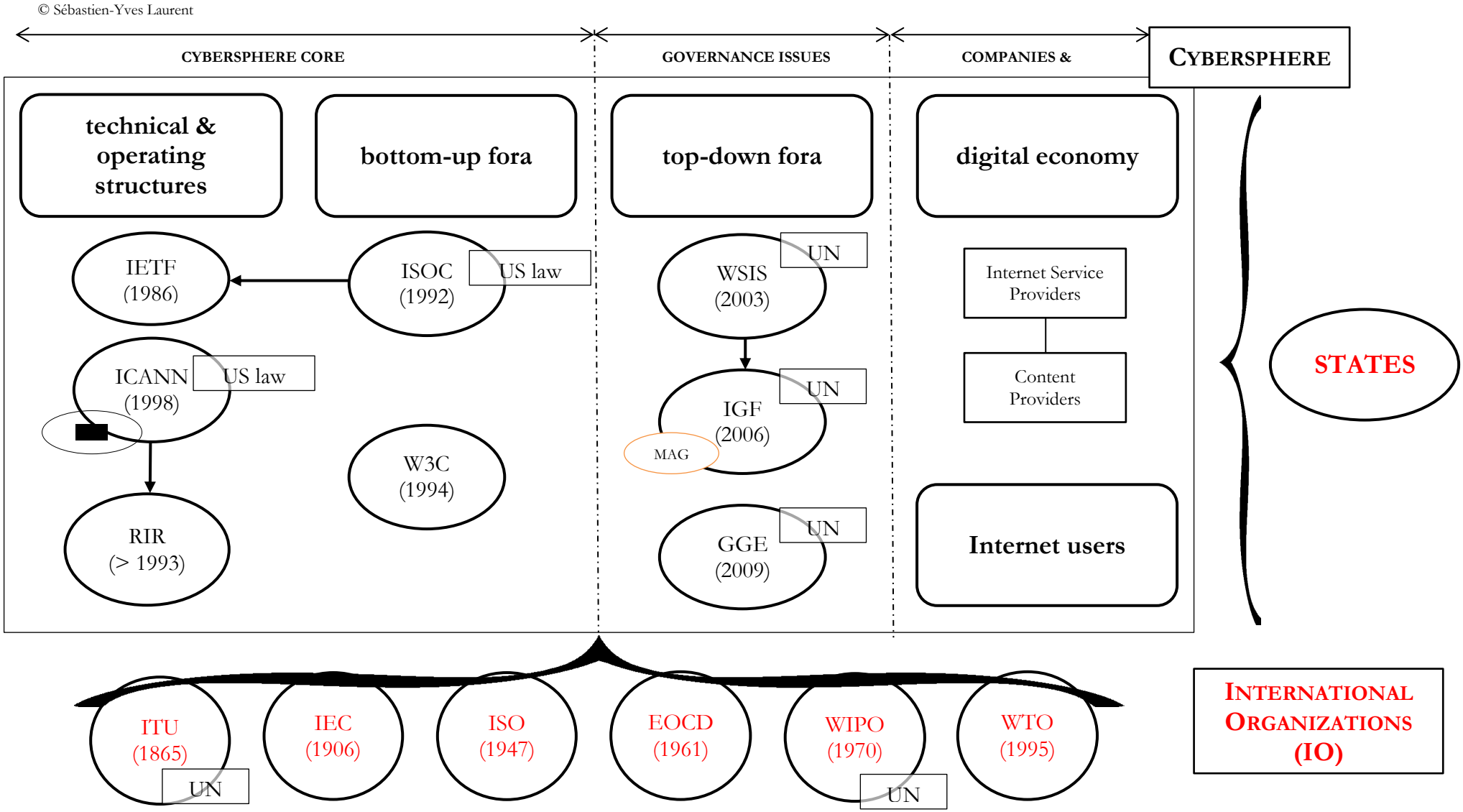
Ainsi, la décennie 2000 a vu la montée en puissance de l'ITU sous couvert de la mise en place de l'IGF, puis de l'animation des débats autour de la gouvernance. Cependant l'ITU a été affaibli par sa propre feuille de route qui est le règlement international des télécommunications (RTI) datant de 1988, inadapté à l'ère de l'Internet (Winseck, 2017).

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 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.

L'ensemble des structures actives dans l'Internet peut être représenté sur le schéma suivant.

[10]. https://www.intgovforum.org/multilingual/content/mag-2019-members [24/07/2019]

Figure 3 : organisations et institutions composant la Cybersphère



3 Un droit international pour le cyber centré sur les usages et géographiquement très inégalement ratifié

Un droit international spécifique à l'environnement cyber existe. Il est néanmoins très inégalement ratifié et se concentre sur quelques enjeux. La notion de « lawfare » inventée en 2001 par le général étatsunien Charles Dunlap qui caractérise l'affrontement entre les États sur les conventions juridiques internationales et sur les normes caractérise utilement la situation. Il existe en effet un *Cyber Lawfare* qui se traduit notamment, malgré l'existence de multiples enceintes et fora de discussions, par un blocage des discussions multilatérales et par des initiatives unilatérales. Le droit du cyber existant 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 être dépassé par l'évolution technologique. Il s'appuie uniquement sur deux textes signés en 1981 et 2001 dans deux configurations nettement différentes : le premier visait à protéger les personnes physiques à l'égard de l'utilisation de leurs données personnelles, le second avait pour objet de favoriser un rapprochement entre États en matière de lutte contre la criminalité informatique. Sur tous les autres enjeux cybernétiques (cybersécurité, cyberconflit, droit global du cyber) les discussions sont bloquées.

3.1 La précocité de la protection juridique des données personnelles en Europe

- 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 » (cf. livrable 7), appelée plus souvent « convention 108 », signée en 1981. A l'époque, ce texte de 27 articles[11] 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 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 2019, elle avait été ratifiée par 47 pays**[12] ainsi que par 8 situés en dehors du Conseil de l'Europe.

La géographie de la ratification 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)[13]. Entre 2016 et 2018 la ratification a beaucoup progressé en dehors de l'Europe (principalement en Amérique latine et en Afrique). Une projection sur une carte montre néanmoins l'isolat européen et le fait que toute une partie du bloc occidental (États-Unis, Canada, Australie) a une conception beaucoup moins protectrice des données personnelles numériques.

---

11. http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm
12. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=FRE
13. La Turquie a signé en 1981, mais n'a jamais ratifié.

A l'échelle régionale de l'Union européenne on peut relever le complément apporté en deux temps : en 1995 par la directive UE 95/46/CE, puis en 2016 par le « paquet données » composé de trois textes (cf. le livrable 7)

1. le règlement 2016/679 « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » (RGPD),
2. La directive 2016/680 « relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données »,
3. enfin, la directive 2016/681 « relative à l'utilisation des données des dossiers passagers »

3.2 Une coopération judiciaire internationale minoritaire dans le monde

- 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 informatique et au renforcement de la coopération lors des enquêtes et des procédures judiciaires[14]. 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 2019, elle avait été ratifiée par 63 pays**[15], dont 44 pays membres du Conseil de l'Europe, mais aussi 19 pays non-membres (un nombre en forte progression depuis quelques années) dont les États-Unis et Israël.

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 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 opérer 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. 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 quart des États dans le monde. En

[14]. http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm [22/07/2019]
[15]. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

suivant l'analyse suggestive de Soraya Sidani qui mesure le degré d'intégration dans le système international à l'aune de la ratification des traités internationaux, on peut constater que **les traités relatifs au cyber ne peuvent pas être des vecteurs d'intégration**[16]. 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. Cette situation générale affaiblit considérablement l'environnement cyber et influe en partie sur les rapports de forces géo-cybernétiques.

3.3 L'impossibilité d'un droit global 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. Il s'agit au fond d'un cyberespace quantitativement et géographiquement minoritaire. Il faut surtout noter que l'enjeu de régulation dépasse les seuls sujets des données personnelles et de la criminalité. Demeure donc posée la question d'une régulation juridique plus large que les deux conventions régionales portées par le Conseil de l'Europe. Les juristes spécialisés formulent trois grandes options pour bâtir un droit du cyberespace (CEIS, 2014 et SFDI, 2014).

(1) 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 (cf. *supra* en 3.1 et 3.2). Ainsi qu'on l'a vu, rien n'interdit que des États extérieurs au Conseil de l'Europe ratifient les textes qu'il élabore : c'est un phénomène en cours manifestant l'exportation des normes européennes. L'application de ce droit pourrait par ailleurs être contrôlée 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 perspective ne tient pas compte de l'état des rapports de force au sein des structures de gouvernance (cf. *infra* en 4 et 5).

(2) Une deuxième possibilité résiderait dans la construction d'un droit *sui generis* en s'inspirant des droits de l'espace et de la mer existants. 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. Par ailleurs, la

16. Soraya SIDANI, *Intégration et déviance au sein du système international*, Paris, Presses de Sciences Po, 2014, 238 p.

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. Cela renvoie par ailleurs à la définition de l'Internet (« a global facility available to the public ») adoptée lors du sommet fondateur de Genève (cf. *supra* en 2.1). 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.

(3) 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. Par ailleurs, 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.

3.4 La formation d'une doctrine juridique étatsuniene du conflit 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 peut bien évidemment fonder un droit général du cyber. Les États-Unis ont développé une approche originale, qu'ils sont les seuls à partager, sur l'application du droit des conflits armés dans le cyberespace. Pour les États-Unis, le cyberespace est totalement intégré à leur conception du conflit et de la guerre. La plupart des grandes puissances militaires ont créé des commandements militaires cyber spécifiques dans la décennie 2010. La spécificité américaine tient aux règles d'emploi brouillant les limites classiques de ce qui est cinétique et ne l'est pas et de ce qui est militaire et ne l'est pas. La doctrine a pris la forme de la publication du manuel de Tallinn en 2013 sur le droit applicable dans l'environnement cyber[17]. Quatre ans plus tard, une 2e édition a été publiée, très augmentée[18], permettant de préciser la nouvelle approche américaine. Le cœur de la doctrine américain est double : ne pas distinguer d'un point de vue juridique l'espace cinétique de l'espace cybernétique et mettre en avant la notion de légitime défense préemptive. 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, principalement de son article 51 reconnaissant le droit à la légitime défense[19]. Il faut relever qu'aucune autre puissance n'a proposé de doctrine alternative.

---

17. Michael N. SCHMITT (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge, Cambridge University Press, 2013, 282 p.

18. Michael N. SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge, Cambridge University Press, 2017, 598 p. Cf. un intéressant commentaire sous l'angle du droit international: Karine BANNELIER, " « Rien que la *lex lata* » ? Etude critique du manuel de Tallin 2.0 sur le droit international applicable aux cyber-opérations", *Annuaire français de droit international*, 2017, LXIII, p. 121-160.

19. Mais certains États comme la France reconnaissent que l'attaque contre des « infrastructures critiques » de portée « vitale » peuvent y conduire. (*Stratégie internationale de la France pour le numérique,* décembre 2017, p. 32 et SGDSN, *Revue stratégique de cyberdéfense*, 12 février 2018, p. 87).

Les Nations Unies ne partagent pas la vision extensive des États-Unis en la matière, mais ont reconnu l'existence de fait de la notion de « Cyberwar » en 2011. En effet, ils ont confié cette année à l'UNIDIR, organisme interne chargé du désarmement la tâche de conduire le programme « Perspectives on Cyber War: Legal Frameworks and Transparency and Confidence-Building"[20]. Cependant le programme a été de très brève durée, puisqu'il s'est étiré sur un an seulement, permettant toutefois plusieurs publications techniques.

3.5 L'importance du *soft law* technique

En l'état actuel du *hard law* applicable au cyber, ce sont les normes qui *de facto* assurent une régulation technique de l'environnement cyber. 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*) : 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. 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 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. 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.

4 La polarisation rapide par l'enjeu de la « cybersécurité » après 2003

Phénomène social marginal jusqu'aux années 2000, l'insécurité dans l'environnement numérique est devenue un enjeu international dominant dès le début de la décennie suivante. Permettant la naissance d'acteurs économiques privés (secteur de la sécurité informatique : éditeurs de logiciels et sociétés de conseil) et mobilisant les États, l'insécurité numérique a

[20]. http://www.unidir.org/programmes/security-and-technology/perspectives-on-cyber-war-legal-frameworks-and-transparency-and-confidence-building

profondément transformé la perception des enjeux numériques à l'échelle internationale et notamment dans les organisations internationales. Les attaques massives (de type DDoS) contre l'Estonie en 2007 et contre la Géorgie en 2008 ont facilité la fabrication d'une « prise de conscience » des effets informationnels - et politiques - des attaques cybernétiques massives contre des intérêts étatiques. Ces deux événements ont aussi été perçus à l'aune des rapports Est-Ouest et on conduit à une lecture géostratégique.

Les formes prises par l'insécurité numérique ont débouché sur la naissance d'un discours et de pratiques internationales de « cybersécurité ». Cette thématique a rapidement et discrètement polarisé l'agenda numérique international.

4.1 La conflictualité cyber et la cyber-insécurité : que caractérise-t-on ?

L'environnement cyber n'est pas resté longtemps à l'abri de divers comportements hostiles. Le premier piratage de réseau informatique a eu lieu 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 (DeNardis, 2014).

Aujourd'hui l'environnement cyber est l'objet d'atteintes quotidiennes et très diverses[21] : 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. La terminologie qui nous parait la plus adaptée est celle de « cyber-conflit » (Ventre, 2013) qui ne préjuge ni du type d'acteurs concernés, ni de la forme prise par la relation conflictuelle. On continuera donc *infra* à utiliser cette appellation.

4.2 L'inadaptation des catégories analytiques face à la cyber-insécurité : les limites de l'analogie

Les traductions de la cyber-insécurité sont désormais très diverses. Avant d'aborder la question de sa pesée quantitative (cf. *infra* en 4.4), il est nécessaire de regarder la caractérisation qualitative. Une partie de la littérature traite le sujet, mais principalement du côté des acteurs de la cybersécurité qui se contentent d'établir des nomenclatures descriptives fondées sur des analogies avec le monde cinétique (Wolf-Vallée, 2011). Dans la production critique sur le sujet, quantitativement faible, on pourrait retenir par exemple la typologie proposée par l'analyste Myriam Dunn Cavelty du Center for Security Studies de Zürich en 2010[22]. 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. Il paraît en effet que les notions d'armes numériques, de guerre numérique … sont issues de raisonnements analogiques du champ

---

21. Pour une vision en temps quasi réel, présentée par l'éditeur russe Kaspersky : https://cybermap.kaspersky.com/fr/ ou par l'entreprise étatsunienne Checkpoint : https://threatmap.checkpoint.com/ ou encore https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18160&view=map Les sites sont nombreux et ne présentent pas tous la même réalité...

22. http://www.css.ethz.ch/content/specialinterest/gess/cis/center-for-securities-studies/en/center/people/dunn-cavelty-myriam-all-publications/details.html?id=/n/o/7/1/no_71_cyberwarnr_71_cyberwar

cinétique au champ numérique et contribuent à un très fort effet de sécuritisation (Laurent, 2019). 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 sont pas spécifiques par rapport au hacking. En outre l'objectif majeur du terrorisme qu'est l'effet pscyhologique n'a pas de réalité en l'absence de forte implication cinétique. La typologie de Dunn Cavelty doit donc être écartée.

Il faut relever que les définitions juridiques sont tout aussi peu adaptées. En droit interne les infractions dans l'espace cyber sont inscrites dans les codes pénaux, mais encore sur le mode de l'analogie et en droit international (convention de Budapest[23], cf. *supra* en 3.2) le principe est le même. La dénomination de « cyber guerre » présente le même danger et c'est la raison pour laquelle on lui préfère le terme de « cyber conflit » (cf. *supra* en 4.1). On rappellera simplement que la notion de « Cyberwar » (Arquila-Ronfeldt, 1993) a été créée, puis installée en 1993 par la Rand Corporation, un *think tank* proche du Pentagone dans le but de favoriser les investissements publics et privés dans le secteur numérique. Toute la production normative des acteurs s'est inscrite à la suite, que ce soient les organisations internationales (UNIDIR, 2013) ou les doctrines stratégiques cyber publiées par les États au début de la décennie 2010[24]. Même les productions associant acteurs et académiques (Perkovich-Levite, 2017) n'échappent pas à la démarche bâtissant des analogies revendiquées avec le conflit armé, le nucléaire et le renseignement.

Afin de sortir du piège analogique, il est nécessaire de bâtir des catégories plus fines en distinguant quatre niveaux : le type, auteur, le procédé technique, la victime ou la cible, les effets et en évitant que la sémantique reprenne les catégories usuelles des champs de la force intérieure et extérieure.

4.3 Essor et banalisation de la conflictualité numérique entre les États

Les cyber-conflits pratiqués par les États posent quatre problèmes spécifiques :

- (1) L'environnement cyber brouille la distinction fondamentale du temps de paix et du temps de guerre ce qui a, entre autres, des effets juridiques importants.

- (2) L'environnement numérique érode les distinctions classiques entre le réel et le factice. La capacité à fabriquer des faux de qualité donne une ampleur sans précédent aux opérations informationnelles.

- (3) Les États utilisent des *proxies* variés, recourant à des acteurs privés. Dès lors, il est difficile de distinguer ce qui peut être qualifié de cybercrime ou de cyberguerre. On relèvera au passage que la réflexion sur la proxysation de la conflictualité est trop descriptive (Hugues, 2012 et Mumford, 2013) et qu'elle est malheureusement quasiment inexistante dans l'environnement cyber.

- (4) Enfin, le quatrième obstacle est la difficulté d'attribuer sur le plan technique une attaque informatique à son auteur (qu'il soit étatique ou non) et cela 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 – rare de ce type – 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 (Laurent, 2015). C'est aussi l'indice d'une certaine banalisation de la conflictualité cybernétique qui semble être devenu un outil de conflictualité classique entre États.

---

23. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680080f0b

24. Cf. les sources en fin de volume.

4.4 La construction sociale de l'insécurité numérique : la force du flou

La cyber-insécurité peut-elle être évaluée quantitativement ? 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 de la société Symantec de 2013 évaluait le coût de la cybercriminalité à plus de 110 milliards de $ pour 400 millions de consommateurs touchés annuellement[25]. Ce chiffre n'est qu'un ordre de grandeur probablement très fortement éloigné de la réalité, d'où l'intérêt du projet de recherche européen (7e PCRD) lancé en 2014 par l'Université allemande de Münster « e-crime », dont l'objet était d'évaluer l'impact économique de la cybercriminalité.

Quelle est la pondération entre les atteintes aux personnes physiques et celles touchant les États ? Là aussi la mesure est impossible pour les raisons évoquées plus haut et l'on ne dispose en 2019 que d'un très vaste ordre de grandeur issu d'un expert indépendant en sécurité informatique, Paolo Passeri. Selon lui, la cybercriminalité représenterait près de 80 % de l'activité violente (niveau individus) et la catégorie « cyberwarfare » (niveau États) correspondrait à moins de 4 % seulement[26].

La cybersécurité peut-elle se mesurer ? De multiples initiatives existe depuis la décennie 2010 (Ventre, 2016). 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[27]. 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 États-Unis occupent, sans *ex aequo*, la première place avec un CGI de 0,824. La France vient ….au 9e 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[28], la position de la France est de façon surprenante assez basse.

A l'image des multiples indicateurs utilisés depuis des décennies par les organisations internationales (Tiberj, 2016), les « mesures » floues de l'insécurité et de la sécurité numérique servent à accompagner des discours publics nationaux et internationaux particulièrement anxiogènes permettant d'asseoir des mesures sécuritaires et/ou des réformes structurelles. Un certain nombre d'indicateurs étant d'origine privée, ils servent à appuyer des objectifs commerciaux.

4.5 La protection des personnes physiques aux origines des notions de « confiance » et de « cybersécurité » internationales (2003-5)

Les premières manifestations collectives d'une interrogation sur la cybersécurité datent des sommets mondiaux sur la société de l'information. 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

[25]. OECD, "The digital economy today", in OECD, *Measuring the Digital Economy: A New Perspective*, Paris, OECD Publishing, 2014, p. 43.
[26]. https://www.hackmageddon.com/
[27]. ITU-UIT, *Indice de cybersécurité dans le monde et profils de cyber bien-être*, avril 2015, 531 p.
[28]. On observera que sous le timbre de l'ITU-IUT c'est une société privée, « ABI research » qui a réalisé l'étude et construit l'indicateur

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 »[29].

Deux ans plus tard, dans l'« agenda de Tunis pour la société de l'information », on pouvait constater au point 39 des termes presque identiques :

« 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 » [30].

Il est donc important de relever que les **premiers textes internationaux évoquant la « sécurité de l'information » et la « cybersécurité »** ratifiés par la presque totalité des États, **se sont focalisés sur la protection des personnes physiques en objectivant deux dimensions, la protection de la vie privée et la protection du consommateur**.

4.6 Un basculement : la mise à l'agenda international de la cybersécurité des États

Or, depuis la fin de la décennie 2000, le discours public sur la cybersécurité des États 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. Deux types de paramètres expliquent selon nous le **basculement dans la mise à l'agenda de la thématique de la cybersécurité individuelle à celle de la cybersécurité des États**. :

(1) D'une part les crises rapprochées qu'ont été les attaques numériques russes contre l'Estonie (2007) et la Géorgie (2008), habilement utilisées par l'OTAN et les États-Unis ont favorisé une « prise de conscience ».

(2) En second lieu, les grandes puissances étatiques occidentales ont fait leur irruption dans le monde numérique (Laurent, 2015), voulant limiter les effets du poids de l'idéologie libertaire et de l'architecture décentralisée qui représentaient une menace pour eux (Mueller, 2010). Leur démarche visait à mettre en place une gouvernance et une régulation internationale. Leur rôle croissant dans les organisations internationales (GAC de l'ICANN) et notamment à l'ONU (MAG de l'IGF, GGE – cf. *infra* en 4.6.2), l'adoption de stratégies nationales cyber au tout début de la décennie 2010[31] en sont les manifestations les plus apparentes et efficaces.

L'un des effets connexes dans l'évolution de l'agenda international est que la mise en avant de l'insécurité numérique des États a entraîné l'affaiblissement des principes idéologiques

[29]. C'est nous qui soulignons.
[30]. C'est nous qui soulignons.
[31]. Cf. une liste non exhaustive dans les sources de ce travail.

fondateurs de l'Internet (Cardon, 2010).

4.7 Les jeux de puissance dans la transformation de l'agenda international

4.7.1 L'initiative russe de 1998 et la naissance d'un dialogue avec les États-Unis sur la cybersécurité des États

Il faut relever que dans la foulée de la fin de la Guerre Froide, période au cours de laquelle la Russie a beaucoup réinvesti l'ONU, le pays a entrepris les premières démarches en vue de sensibiliser les États aux enjeux de sécurité liés aux technologies de l'information. En effet, en décembre 1998 la Fédération de Russie présentait une résolution (A/RES/53/70) intitulée : "Developments in the field of information and telecommunications in the context of international security". Le court texte[32] était principalement bâti autour de l'idée que ces technologies pouvaient mettre en cause la « stabilité internationale et la sécurité ». Cela situait d'emblée l'enjeu au niveau des États (et non pas des individus) et fixait - très durablement - un lien entre ces technologies et l'ordre international. La résolution fut renouvelée un an plus tard avec un contenu quasiment identique (A/RES/54/49) et le fut ensuite de façon répétée. On peut émettre l'hypothèse que l'initiative russe de 1998-9 n'est pas étrangère au fait que l'Assemblée générale des Nations Unies ait commencé à en débattre à partir de 2001 (cf. infra en 4.6.2.).

Par ailleurs l'enjeu s'est en quelque sorte bipolarisé : en effet, en octobre 2005 les États-Unis pour la première fois se manifestaient publiquement sur le sujet en votant contre la résolution russe qui avait été à nouveau déposée[33]. Sur fond d'attaques cyber réciproques, la Russie et les États-Unis ont alors engagé un dialogue bilatéral dont il n'y a qu'assez peu de traces. Il faut noter toutefois le choix que les deux pays ont fait de rendre public en 2011 une partie de leur dialogue conduit dans le cadre de l' « East-West Institute »[34]. Il portait sur l'enjeu crucial des « infrastructures critiques » qui étaient l'objet des attaques cyber réciproques. L'un des aspects essentiels fut que le deux pays se sont accordés sur la définition de ce qu'était une « cyberweapon »[35]. Le dialogue avait porté sur des aspects très opérationnels. En effet, parmi les 5 recommandations deux en particuliers témoignent de la volonté des deux États de travailler à une gouvernance bilatérale du cyber : d'une part travailler sur la possibilité de définir des zones dans l'espace cyber où le droit international humanitaire pourrait s'appliquer (recommandation 2)[36] et d'autre part sur la possibilité de définir en commun un état entre guerre et paix, qualifié par les deux États d' « other-than-war » (recommandation 5)[37].

4.7.2 La prise de relais onusienne : l'Assemblée générale et le Group of Governmental Experts (GGE)

L'un des effets de l'initiative russe aux Nations Unies a été la multilatéralisation des échanges sur le cyber. Le processus a débuté en 2001 et se poursuit encore en 2019. Deux

---

32. https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70
33. Tim MAURER, *Norm Emergence at the United Nations. An analysis of the UN's Activities regarding Cyber-Security*, Cambridge, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011, p. 22.
34. Cf. Russia-US Bilateral on critical infrastructure protection, *Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace*, January 2011, East-West Institute, 60 p.
35. *Ibid.*, p. 18.
36. *Ibid.*
37. *Ibid.*

instances onusiennes en sont le cadre, l'Assemblée générale et le Group of Governmental Experts (GGE).

La résolution AG 55/63 de l'Assemblée générale des Nations Unies (AGNU) du 22 janvier 2001 a été la première à manifester l'intérêt pour les enjeux cyber de l'ensemble des États rassemblés, avec toutefois une perspective très claire indiquée dans son intitulée : « « Combating the criminal misuse of information technologies". Cette résolution fut votée à l'identique (sous l'appelation Rés. 56/121) l'année suivante, ainsi que l'on peut le voir dans la figure 4 ci-dessous. En 2003 la 3e résolution cyber (Rés. 57/239) adoptée par l'AGNU s'appuya sur la notion de cybersécurité : « Creation of a global culture of cybersecurity ». La 4e (Rés. 58/199, en 2004) a vu la mise en avant de la notion d'infrastructure critique (« Creation of a global culture of cybersecurity and the protection of critical information infrastructures »). La 5e et dernière à avoir été adoptée (Rés. 64/211 en 2009) a insisté sur le bilan en la matière ("Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures").

Figure 4 : résolutions de l'Assemblée générale des Nations-Unies en matière de cybersécurité

		Rés. de l'AG	**Intitulé de la rés.**	
1.	**22 janv. 2001**	Rés. 55/63	**« Combating the criminal misuse of information technologies"**	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf
2.	**22 janv. 2002**	Rés. 56/121	**« Combating the criminal misuse of information technologies"**	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf
3.	**31 janv. 2003**	Rés. 57/239	**«Creation of a global culture of cybersecurity »**	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf
4.	**30 janv. 2004**	Rés. 58/199	**« Creation of a global culture of cybersecurity and the protection of critical information infrastructures »**	https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf
5.	**21 déc. 2009**	Rés. 64/211	**"Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures"**	http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211

Depuis dix ans l'AGNU ne s'est plus prononcée sur les enjeux de cybersécurité : nous faisons l'hypothèse que c'est dans le cadre de l'instance *ad hoc* et technique, le Group of Governmental Experts (GGE) que le débat sur la cybersécurité s'est déplacé (cf. *infra*). Le rôle de l'AGNU est celui d'un forum et aborde donc des sujets avec une approche large. Les résolutions citées dans la figure précédente sont extrêmement brèves et comportent des incitations très générales. En 2001, l'AGNU prescrivait 10 mesures pour lutter contre le crime dans le domaine des technologies de

l'information dans le cadre des politiques nationales des États et dans leurs pratiques internationales de coopération. En 2002, elle soulignait l'avance du conseil de l'Europe et le rôle de la convention de Budapest. Un an plus tard toutefois le texte s'était fait plus précis autour d'un véritable mot d'ordre : « Creation of a global culture of cybersecurity », la résolution comprenant une annexe détaillée en 9 points sur les aspects pratiques permettant de bâtir cette culture globale. Mais ces prescriptions traduisaient des accords faciles à obtenir.

C'est la résolution 58/32 de l'AGNU du 8 décembre 2003 qui a créé le 1er « Group of governmental experts » (GGE)[38]. Il faut relever que ces experts ont été – exclusivement – des représentants de leurs gouvernements et non du secteur privé de la « Tech » (comme cela était le cas à l'ICANN, cf. *supra* en 1) : le GGE n'a pas pris en compte les prescriptions de *multi-stakeholderism* sur l'inclusion des acteurs privés (cf. *supra* en 1. et 2.1 ; en 4.7. *infra*). Le GGE est un indice de l'arrivée des États dans la gouvernance cyber. Cet outil de gouvernance stato-centrique a été périodiquement renouvelé entre 2003 et 2017[39], mais seuls trois d'entre eux ont pu s'accorder sur un rapport commun (cf. la figure 5 ci-dessous). Ce sont les trois rapports de 2010, 2013 et 2015 que l'on va examiner maintenant.

Figure 5 : rapports des GGE

n° de GGE	**n° de rapport**	**Date Public.**	**Réf.**	**auteur (date création)**	**Membres**	**Source**
1.	**-**	2004	Pas de rapport	1er GGE (2004)	15	-
2.	**1.**	30 juillet 2010	A65/201	2e GGE (2005)	15	http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201
3.	**2.**	24 juin 2013	A68/98 *	3e GGE (2011)	15	**http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98**
4.	**3.**	22 juillet 2015	A70/174	4e GGE (2013)	20	http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
5.	**-**	2017	Pas de rapport	5e GGE (2015)		
6.				6e GGE (2018)	25	

Le 1er rapport publié en 2010 indique le plus petit dénominateur commun des 15 membres du groupe : les 5 recommandations étaient principalement bâties autour de la nécessité d'accroître les échanges de vues et les mesures de confiance entre les États[40]. Le 2e rapport du GGE publié en 2013 a débouché sur deux mesures beaucoup plus structurantes : d'une part le **principe de l'application du droit international au cyberespace (point 16)**[41] et la reconnaissance de la responsabilité des États pour les actes illégaux commis par des acteurs non–étatiques sur leur territoire (point 23) d'autre part[42]. Le 3e rapport (2015) est de loin le plus complet et précis de toute la production du GGE. La diversité des sujets abordés et les 11 recommandations illustrent un certain état de confiance entre les 20 membres. Peu de sujets techniques ont été laissés de côté : en effet le principe de cyber-diligence, la protection des droits

38. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/58/32
39. Un 6e GGE a été créé en décembre 2018.
40. https://www.un.org/ga/search/view_doc.asp?symbol=A/65/201 p. 8-9.
41. http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98, p. 8.
42. *Ibid.* Ce principe a été appelé par la suite principe de cyber-diligence (Bannelier, 2014).

humains, l'interdiction du hack back, la coopération interétatique en cas d'attaque sur les infrastructures critiques, font partie des recommandations, entre autres.

4.7.3 Le GGE, une structure oligarchique de gouvernance

La composition des GGE illustre parfaitement le rôle nouveau des États et notamment des États les plus puissants dans la gouvernance cyber. Le tableau suivant relève la composition étatique des groupes. Si 15 à 20 États figuraient, il est d'importance de relever que seuls 7 États (en rouge dans le tableau) ont fait partie des 3 GGE les plus productifs en *soft law* du cyber. Sur les 7 on constate la présence des 5 puissances permanentes du conseil de sécurité ainsi qu'une grande puissance économique et cyber - l'Allemagne – à laquelle s'ajoute l'Estonie qui est le pays d'Europe orientale de loin le plus « numérisé » par ses infrastructures et ses pratiques. On constate donc la présence d'un bloc occidental et atlantique de 5 pays ainsi que seulement deux pays non occidentaux, la Russie et la Chine. Finalement, l'action du P5 (*permanent five*) a permis de faire du GGE, c'est-à-dire une instance de gouvernance numérique, un relais de la structure oligarchique (occidentale) du système international (Badie, 2011). On remarquera que la résolution « A/RES/73/266 » du 22 décembre 2018 créant un 6e GGE avait prescrit très explicitement que la composition devait se faire « on the basis of equitable geographical distribution »[43]. Mais sur les 25 membres de ce nouveau GGE on retrouve à nouveau les P5 et l'Allemagne[44]. **Ces 6 pays sont depuis près de quinze ans le cœur de la gouvernance GGE qui est l'une des principales gouvernances de l'Internet**.

Figure 6 : composition nationale des GGE ayant débouché sur un rapport

	GGE2 (2005-10)	GGE3 (2011-13)	GGE4 (2013-15)
Argentina		*	
Australia		*	
Belarus	*	*	*
Brazil	*		*
Canada		*	
China	*	*	*
Colombia			*
Egypt		*	*
Estonia	*	*	*
France	*	*	*
Germany	*	*	*
Ghana			*
India	*	*	
Indonesia		*	
Israel	*		*
Italy	*		
Japan		*	*
Kenya			*
Malaysia			*
Mexico			*
Pakistan			*

43. https://undocs.org/A/RES/73/266 p. 3.
44. https://dig.watch/processes/un-gge#top

Qatar	*		
S. Korea	*		*
Russian Federation	*	*	*
South Africa	*		
Spain			*
UK	*	*	*
USA	*	*	*
Tot. membres	**15**	**15**	**20**

La structuration oligarchique semble être une loi d'airain pour paraphraser Roberto Michels, dans les instances internationales cyber. En effet en 2017, prenant acte du blocage au sein du GGE, deux think tanks, le Hague Centre for Strategic Studies (HCSS) et le EastWest Institute (EWI) ont décidé la création de la Global commission on the stability of cyberspace (GCSC). La nouvelle structure qui mène des discussions très poussées et de haut niveau sur les mêmes enjeux que le GGE est composée de 23 commissaires représentant divers pays mais ne représentant pas officiellement leurs États. On remarque d'emblée que les États-Unis ont près d'un tiers des commissaires alors que la Russie et la Chine n'en ont qu'un et les Pays-Bas en comptent 3.

Figure 7 : composition nationale des commissaires du GCSC

Afrique du Sud	1
Allemagne	1
Brésil	1
Chine	2
États-Unis	8
France	1
Inde	1
Israël	1
Japon	1
Malaisie	1
Nigeria	1
Pays-Bas	3
Royaume-Unis	1
Russie	1
Singapour	1
Total	**25**

4.7.4 L'échec de l'ITU dans la participation aux débats sur la gouvernance de la cybersécurité

On a vu *supra* (cf. 2. 2) 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.

Après son succès très relatif en matière de gouvernance cyber (cf. 2.2), l'ITU 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[45]. 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 sinon obsolète, 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 »[46], 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.

Figure 8 : enjeux de négociation du Global Cybersecurity Agenda (GCA, 2007-8)

1.	technical and procedural measures
2.	legal measures
3.	organizational structures
4.	capacity building
5.	international cooperation

Le HLEG entendait bien se cantonner au sujet de la cybersécurité à 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 (cf. *supra* en 3.2) qui n'était à leurs yeux qu'une convention régionale, peu ratifiée et peu mise en oeuvre[47]. Le texte du traité, composé de 22 articles 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 ne se limitant plus à une approche technique 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

45. Cf. Solange Ghernaouti, *Cyber Power. Crime, conflict and security in cyberspace*, Lausanne, EPFL Press, 2013, p. 407-417.
46. 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.
47. *Ibid.*, p. ii.

cybernétiques. Mais le centre de Singapore n'est 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 une composante du Tribunal pénal international de La Haye[48]. 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.

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 mais plus encore avec l'action des P5 dans le cadre onusien (cf. *supra* en 4.6.2 et 4.6.3). Par ailleurs, à la différence du GGE 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.

4.8 Les pratiques de cybersécurité internationale des États sont une politique

4.8.1 La « sécurité » envisagée comme l'une des « politiques publiques de l'Internet » au début des années 2000

Il est important de relever que la notion de politique publique de l'Internet a été pour la première fois employée lors des SMSI de Genève et de Tunis (cf. *infra* en 5.1). A Genève, les diplomates ont pris en considération le fait qu'il existait des politiques publiques nationales de l'Internet, mais qui créaient pour les États des droits et des responsabilités (point 49 du SMSI de Genève, 2003)[49] à l'échelle supra-étatique, ainsi qualifiée : "international Internet-related public policy issue" (point 49.a). Il était indiqué que c'était aux organisations intergouvernementales - et non aux organisations internationales – d'assurer la « coordination » des politiques publiques nationales de l'Internet (point 49.d) et aux organisations internationales des « Internet-related technical standards and relevant policies » (point 49.e).

Deux ans plus tard à Tunis l'ensemble du point 49 a été repris à l'identique dans le point 35[50]. Mais ce sommet de Tunis fut pourtant bien plus ambitieux et complet dans son approche de l'Internet comme résultat d'une politique publique que deux ans plus tôt. Au point 58, il précisait en effet que la gouvernance de l'Internet (cf. *infra* notre 5) incluait des éléments de politique publique :« It also includes other significant public policy issues such as, *inter alia*, critical Internet resources, the security and safety of the Internet […]". Enfin le point 72 par lequel il était décidé de confier au secrétaire général des NU le soin de réunir le premier Internet Governance Forum (cf. 2.3 et 5.4), prescrivait à cette future structure de discuter de « […] public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet » (72.a). L'expression de « politique publique » était donc consacrée par deux sommets internationaux, le second ayant permis – discrètement – d'inscrire la sécurité comme l'une des 5 politiques publiques de l'Internet. La mise à l'agenda par

48. *Ibid.*, p. 66.
49. https://www.itu.int/net/wsis/docs/geneva/official/dop.html
50. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

les États (cf. *supra* en 4.6) nous conduit à regarder de plus près les pratiques en la matière.

4.8.2 Le fonctionnement du réseau mondial de cybersécurité opérationnelle : les CERT

Par ailleurs, il existe une très discrète gouvernance opérationnelle de la cybersécurité. Il s'agit d'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. Il s'agit là d'un fonctionnement profondément internationalisé et pour lequel à la fois les besoins internes et externes ont été pris en compte.

Le système repose principalement sur des acteurs nationaux et avant tout sur les « Computer Emergency Response Team » (CERT), qui sont des structures de veille sécuritaire 24/24 chargées de détecter les attaques et de proposer des solutions de sécurité à court terme. Les structures 24/7 sont obligatoires (article 35) pour tous les pays ayant signé la convention de Budapest en 2001[51]. 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 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 robuste. Il joue un rôle important également dans la détermination de la stratégie de cybersécurité des institutions de l'UE et dans l'Union. En application de la directive européenne NIS de 2016, c'est à l'ENISA que revient la responsabilité d'avoir créé le réseau des CERT de l'UE, effectif en 2017[52]. 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

---

[51]. http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm [25/09/2019]
[52]. https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

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[53], 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 »[54], 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 »[55] 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 (cf. *supra* en 3.4). On observera que la France a rejoint cet organisme tardivement, en 2014. INTERPOL possède depuis 2014 l' « 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[56] 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) 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 ».

4.8.3 La cybersécurité opérationnelle, une « action publique internationale »

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 mêle acteurs publics et privés. Les autres composantes sont des forums régionaux sans aucune portée opérationnelle. L'action des CERT amène à prendre à bras-le-corps la notion de politique publique. Si l'on s'en tient à l'approche classique : « Le concept désigne les interventions d'une autorité investie de puissance publique et de légitimité gouvernementale sur un domaine spécifique de la société ou du territoire »[57]. Or, la finalité de l'action des CERT est d'avoir des effets sur le territoire national, mais ils ne peuvent y parvenir que s'ils traitent les attaques en liaison constante avec leurs partenaires étrangers. Le fait que les données ne sont pas de stocks ou des états stables mais des flux constants caractérisés par une forte mobilité a contraint les CERT à s'organiser en réseaux. Les CERT nationaux exercent une parcelle de l'autorité coercitive de l'État sur les données mais ils ne peuvent y parvenir que s'ils sont en réseau avec les autres CERT. On laissera ici de côté les effets sur la souveraineté pour se concentrer sur les formes sociales dans l'esprit de la sociologie simmelienne. Or, l'efficacité d'un CERT ne tient qu'à l'efficacité de ses partenaires ou plutôt au fait que ses partenaires acceptent de coopérer constamment avec lui. Cela revient à dire que si les acteurs étatiques font des CERT les organismes de la politique publique de cybersécurité, du point de vue de l'analyste la forte dé-territorialisation de leur action empêche d'employer la catégorie de politique publique. En revanche, on se trouve dans une

53. https://www.sites.oas.org/cyber/en/Pages/default.aspx
54. http://cis-legislation.com/document.fwx?rgn=28340
55. https://ccdcoe.org/sites/default/files/documents/ASEAN-120712-ARFStatementCS.pdf
56. Elle a ainsi organisé en 2001 l' "OSCE Conference on a Comprehensive Approach to Cybersecurity".
57. Jean-Claude THOENIG, « Politique publique », in : Laurie BOUSSAGUET, Sophie JACQUOT et Pauline RAVINET (dir.), *Dictionnaire des politiques publiques*, Paris, Presses de Sciences Po, « Références », 2006, p. 420.

situation correspondant à la définition des politiques publiques internationales, telle qu'elle a été proposée par F. Petiteville et A. Smith, soit « […] l'ensemble des programmes d'action revendiqués par des autorités publiques ayant pour objet de produire des effets dépassant le cadre d'un territoire stato-national […] »[58]. Cependant on a vu (*supra* en 4.7.2.) que le réseau des CERT comprenait des acteurs publics et privés de tailles différentes et qu'il visait à rétablir une forme d'ordre et de stabilité, soit une forme d'équilibrage. Ceci conduit plutôt à correspondre à la définition d' « action publique internationale » donnée par Charlotte Halpern, soit « […] l'ensemble des formes de régulation de l'action collective observés à l'échelle internationale et résultant de l'activité d'une pluralité d'acteurs, publics et privés, agissant conjointement dans des interdépendances multiples et à différentes échelles »[59]. A cet égard, **l'action des CERT à l'échelle mondiale en matière de cybersécurité opérationnelle** correspond en tous points à une **action publique internationale**.

5 L'échec d'une gouvernance globale

5.1 La « gouvernance » de l'Internet conçue par l'ONU (2003-5) : l'approche multi-acteurs

Le premier SMSI de Genève (2003) a fixé en son point 48 un cadre général de ce que devait être la gouvernance de l'Internet du point de vue des organisations internationales. On le cite ici in-extenso car il a durablement inscrit un principe :

> « The international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism"[60]

On voit là les principes du *multi-stakeholderism*, avec mention des quatre acteurs principaux de l'Internet : les États, le secteur privé, la société civile et les organisations internationales (OIT).

Figure 9 : les 4 composantes de la gouvernance multi-acteurs

1.	governments
2.	private sector
3.	civil society
4.	international organizations

Cette approche est directement inspirée de l'approche de la « Commission on Global Governance » (CGO) qui s'était réunie à l'initiative de l'ancien chancelier allemand Willy Brandt de 1992 à 1994 et qui a joué un rôle fondamental dans la cristallisation d'une nouvelle façon d'appréhender le système international après la guerre froide. On la trouve dans *Our Global Neighbourhood*, le rapport final remis par la commission en 1995:

---

58. Franck PETITEVILLE et Andy SMITH, « Analyser les politiques publiques internationales », *Revue française de science politique*, 2006-3, vol. 56, p. 362.
59. Charlotte HALPERN, « Politiques publiques internationales : Penser les échelles de la régulation politique », in : Dario Battistella (dir.), *Relations internationales. Bilan et perspectives*, Paris, Ellipses, 2013, p. 367.
60. https://www.itu.int/net/wsis/docs/geneva/official/dop.html

« 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"[61].

Cette approche revient en fait à prescrire 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.

La conférence de Tunis de 2005 a pleinement confirmé l'esprit de la déclaration de Genève, notamment en son point 29 qui reprenait intégralement le point 48 (cité *supra*). Mais alors que les membres du WSIS de Genève n'avaient mentionné qu'une seule fois la notion de gouvernance, les discussions du WSIS de Tunis ont permis d'apporter des précisions, notamment dans le point 34 :

« A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet"[62]

Le complément apporté par rapport à 2003 portait donc sur les « shared principles, norms, rules, decision-making procedures » ce qui signifiait clairement que la vision de la gouvernance de l'Internet ne prenait pas en compte les institutions socio-techniques existantes, celles du Cybersphere core (cf. *supra* en 1), ni même la couche des infrastructures techniques.

Avant d'aborder le débat sur les définitions proposées par les acteurs de la cybersphère, 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** »[63]. 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.

5.2 « Architecture is politics » et transversalité de la gouvernance

Les acteurs ont porté leur analyse en premier lieu sur les enjeux, sur ce qui, selon eux, était constitué comme « problème public ». De ce point de vue, les perspectives sont assez subjectives et donc différentes ainsi que le tableau ci-dessous le montre.

---

61. *Our Global Neighbourhood. The Report of the Commission on Global Governance*, Oxford University Press, 1995, p. 2.
62. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
63. Milton L. Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge, MIT Press, 2010, p. 9.

Figure 10 : les enjeux de gouvernance selon Chiche et Kurbalija.

(Chiche, 2013)						
	neutralité de l'Internet	protection des données personnelles	cyber-attaques et cybercriminalité	culture partagée entre propriété intellectuelle et libre circulation gratuite des œuvres	protection de la diversité linguistique et culturelle	défi environnemental
(Kurbalija, 2013)						
	développement (du réseau)	gouvernance juridique	gouvernance économique	gouvernance socio-culturelle	infratsructure et standaridsatrion	

Dans de précédents travaux de ce programme UTIC de l'ANR (livrables 1 et 7 notamment) le choix a été adopté d'aborder 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 faite en 2012 par le diplomate Bertrand de La Chapelle, ancien représentant français à l'ICANN 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. 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 de Mitchell Kapor « 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. Elle précise : « Internet governance is enacted via various routes : technical design decisions, private corporate policies, global institutions, national laws and policies, international treaties »[64]. Ainsi, la réalité de la gouvernance est d'être multi-couches.

5.3 Les phases de la gouvernance

Dans l'environnement cyber les économistes du contrat distinguent classiquement 3 types de fonctionnement général (Brousseau, 2012). Cette approche est très heuristique car elle correspond parfaitement aux 3 phases connues par l'environnement cyber :

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

- 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* 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, jusqu'à contester le *multi-stakeholderism* qui suppose un équilibre entre acteurs étatiques et non-étatiques.

La situation actuelle (2019) est donc celle d'une co-régulation théorique qui est de plus en plus réduite par le rôle régulateur des États et l'efficacité décroissante des organismes multi-acteurs onusiens.

5.4 Le déclin de l'idée d'une « 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 et dépassant les seuls enjeux de cybersécurité. Cette intention persiste en 2019. Elle comprend la gouvernance technique de ce que l'on a appelé 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. On peut aller plus loin que DeNardis (cf. *supra* en 5.3) 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.

Cette gouvernance est réalisée principalement par trois organisations, le Multistakeholder Advisory Group (MAG) de l'IGF, le Governmental Advisory Committee (GAC) de l'ICANN (cf. le schéma en 2.2. *supra*), ainsi que l'EuroDIG.

- (1) 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.

- (2) Le GAC de l'ICANN est 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.

- (3) A ces deux structures globales, il faut ajouter depuis sa création en octobre 2008, une structure régionale, 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 croissant de l'Europe dans le développement du cyber (avec son rôle de mieux-disant international sur les données personnelles, mais aussi les condamnations par la CJUE des GAFA), 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.

Mais malgré la diversité et la complémentarité de ces structures de gouvernance qui travaillent assez étroitement entre elles, on peut poser la question de leur efficacité. A l'image de beaucoup de structures liées à l'environnement cyber, il s'agit en fait de *fora* et de lieux de débat, non d'organisations opérationnelles. L'échec d'un droit global du cyberspace (cf. 3.3. *supra*) et la polarisation du débat et des pratiques numériques par la cybersécurité constitutive d'une action publique internationale (cf. 4 *supra*) ne donnent pas de ressource à ceux qui défendent une gouvernance politique générale. Malgré tout, 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 l'arrivée des États. Le communiqué final du G8 de Deauville (26-27 mai 2011) qui avait été précédé d'un e-sommet avec les GAFA est une parfaite illustration de la volonté de trouver un équilibre nouveau entre gouvernance multi-acteurs et intérêts de puissances des Etats. On peut en effet lire au point 20 :

> « Tout en apportant notre appui au modèle multi-acteurs qui caractérise la gouvernance de l'Internet, nous appelons toutes les parties prenantes à contribuer au renforcement de la coopération, à la fois au sein des enceintes internationales traitant de la gouvernance de l'Internet, et entre celles-ci. À cet égard, la souplesse et la transparence doivent être préservées dans la gouvernance de l'Internet pour lui permettre de s'adapter au rythme rapide des évolutions et des nouvelles utilisations technologiques et commerciales. Dans ce cadre, les États doivent jouer un rôle-clé »[65].

[65]. https://www.tresor.economie.gouv.fr/Ressources/File/334233

6 Conclusions

Malgré l'extension mondiale du réseau étatsunien avec la naissance de l'Internet commercial au milieu des années 1990, **on peut se demander si le fonctionnement pratique du réseau mondial n'est pas encore sous forte domination des Etats-Unis**. Certes, l'Internet anglophone est en net recul par rapport à l'Internet sinophone et hispanophone (Lbien aurent, 2015), mais les usages linguistiques créent une illusion d'optique dans le traitement de la gouvernance. Certes, des Etats puissants militairement et technologiquement comme la Chine et la Russie ont des visions de la gouvernance hostiles à la gouvernance multi-acteurs en défendant une approche très strictement stato-centrée. Mais ceci bénéficie en fait avant tout au *statu quo* de la gouvernance actuelle (2019) dont le fonctionnement est encore très fortement sous influence des Etats-Unis. Or, la situation actuelle est celle d'une forte fragmentation des gouvernances et d'un déclin de l'idée d'une gouvernance politique à portée générale, ce qui satisfait les intérêts des Etats-Unis. Enfin, il faut relever que la **pratique même de la gouvernance**, a fortiori en matière cyber, **ne signifie pas le déclin des Etats** (Hibou, 1996) **qui** trouvent des relais puissants et **témoignent ainsi de leur capacité de résistance** face à la nouveauté radicale ce qui fut défini comme « ressource publique mondiale ».

Acronymes et abréviations

- AGNU : Assemblée générale des Nations Unies
- CERT : Computer Emergency Response Team
- CC : Cybersphere Core
- CGO : Commission on Global Governance
- GCA : Global Cybersecurity Agenda
- GGE : Group of Governmental Experts
- HLEG : High Level Experts Group
- ICANN: Internet Corporation for Assigned Names and Numbers
- IETF : Internet Engineering Task Force
- IEC : International Electrotechnical Commission
- ISO : International Organization for Standardization
- IGF : Internet Governance Forum
- MAG : Multistakeholder Advisory Group
- W3C : World Wide Web Consortium

Sources et bibliographie

1. Sources

(ordre chronologique)

- John ARQUILLA and David RONFELDT, "Cyberwar is Coming!", *Comparative Strategy*, vol. 12, n° 2, Spring 1993, pp. 141–165.
- Commission on global governance, *Our Global Neighbourhood. The Report of the Commission on Global Governance*, Oxford University Press, 1995, 432 p.
- Philippe WOLF et Luc VALLEE (ANSSI), "Cyber-conflits, quelques clés de compréhension", *Rapport 2011 de l'INHESJ/ONDRP*, Paris, INHESJ, 2011, p. 787-802.
- *Défense et sécurité des systèmes d'information. Stratégie de la France*, Paris, ANSSI, 2011, 22 p.
- Russia-US Bilateral on critical infrastructure protection, *Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace*, January 2011, East-West Institute, 60 p.
- White House, *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World,* Washington, The White House, May 2011, 25 p.
- *The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world,* Cabinet Office, November 2011, 43 p.
- Conseil de l'Europe, *Stratégie de gouvernance de l'Internet 2012-2015*, 15 mars 2012, 12 p.
- Presidential Policy Directive/PPD-20 on US Cyber Operations Policy, 16 octobre 2012, 18 p.
- Michael N. SCHMITT (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge, Cambridge University Press, 2013, 282 p.
- SEAE, *Communication conjointe au Parlement européen, au conseil, au comité économique et social européen et au comité des régions. Stratégie de cybersécurité de l'Union Européenne : un cyberespace ouvert, sûr et sécurisé*, 7 février 2013, 21 p.
- UNIDIR, *The Cyber Index. International security Trends and Realities*, United Nations, New York and Geneva, 2013, 138 p.
- OECD, "The digital economy today", in OECD, *Measuring the Digital Economy: A New Perspective*, OECD Publishing, Paris, 2014, p. 25-47
- ITU-UIT, *Indice de cybersécurité dans le monde et profils de cyber bien-être*, avril 2015, 531 p.
- UNIDIR-CSIS, *Report of the International Security Cyber Issues Workshop Series*, 2016, 30 p. http://www.unidir.ch/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf
- *Stratégie internationale de la France pour le numérique,* décembre 2017, 34 p.
- Michael N. SCHMITT, "Grey Zones in the International Law of Cyberspace" (October 18, 2017), *Yale Journal of International Law Online;* 1-2017, 42:2, 21 p
- Michael N. SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge, Cambridge University Press, 2017, 598 p.
- SGDSN, *Revue stratégique de cyberdéfense*, 12 février 2018, 167 p.
- *National Cyber Strategy of the United States of America*, September 2018, 28 p.
- *Appel de Paris pour la confiance et la sécurité dans le cyberespace*, 12 novembre 2018, 4 p. :

- Nathalie CHICHE, *Internet: pour une gouvernance ouverte et équitable*, Paris, CESE-Section des affaires européennes et internationales, 11 décembre 2013, 59 p.

- Claude REVEL, *Développer une influence normative internationale stratégique pour la France*, Bercy, 31 janvier 2013, 101 p.

2. Bibliographie sur le cyber

(ordre chronologique)

- Georges CHATILLON (dir.), *Le Droit international de l'Internet*, Bruxelles, Bruylant, 2002, 693 p.
- Jonathan ZITTRAIN, *The Future of the Internet and How to Stop It,* Yale University Press, 2008, 352 p.
- Françoise MASSIT-FOLLEA, « La gouvernance Internet : un cas d'école pour la normativité contemporaine », *Revue Gouvernance*, 5 (1), 2008, 17 p. https://doi.org/10.7202/1039105ar
- Myriam QUEMENER et Joël FERRY, *Cybercriminalité : défi mondial*, Paris, Economica, 2009, 308 p.
- Milton L. MUELLER, *Networks and States: The Global Politics of Internet Governance*, Cambridge, MIT Press, 2010, 313 p.
- Dominique CARDON, *La démocratie Internet. Promesses et limites*, Paris, Seuil, « La République des idées », 2010, 101 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.
- 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.
- Tim MAURER, *Norm Emergence at the United Nations. An analysis of the UN's Activities regarding Cyber-Security*, Cambridge, Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011, 70 p.
https://www.belfercenter.org/sites/default/files/legacy/files/maurer-cyber-norm-dp-2011-11-final.pdf
- Christopher T. MARDSEN, *Internet Co-Regulation. European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge, Cambridge University Press, 2011, 284 p.
- Joseph NYE, "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly,* Winter 2011, p. 18-38
- Jovan KURBALIJA, *An Introduction to Internet Governance*, Geneva, Diplo Foundation, 2012 [5th ed., first : 2008], 197 p.
- Bertrand DE LA CHAPELLE, "Gouvernance Internet: tensions actuelles et futurs possibles", *Politique étrangère*, été 2012, n° 2, p. 249-262
- Michael WARNER, "Cybersecurity: a Pre-History", *Intelligence and National Security*, volume 27, n° 5, October 2012, p. 781-799.
- Loïc SIMONET, « L'usage de la force dans le cyberespace et le droit international », *Annuaire français de droit international*, vol. 58, 2012, p 117-143
- Louise ARIMATSU, « A Treaty for governing Cyber-Weapons :Potential Benefits and Practical Limitations", in : C. Czosseck R. Ottis and K. Ziolkowski, *4th International Conference on Cyber Conflict*, CCD-COE Publications, 2012, p. 91-106.
https://ccdcoe.org/publications/2012proceedings/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf
- 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.
- Global Partners and Associates, *Who governs the Internet ?*, 2012, 15 p.

- Giles KEIR, "Russia's Public Stance on Cyberspace Issues, in C. Czosseck R. Ottis and K. Ziolkowski, *4th International Conference on Cyber Conflict*, CCD-COE Publications, 2012, p. 65-66. https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf
- Eric BROUSSEAU, Meryem MARZOUKI and Cécile MÉADEL (eds.), *Governance, Regulations and Powers on the Internet*, Cambridge : Cambridge University Press, 2012, 445 p.
- Daniel VENTRE (dir.), *Cyber Conflict: Competing National Perspective*, ISTE-Wiley, 2013, 352 p.
- Joanna KULESZA, *International Internet Law*, London, Routledge, 2013, 194 p.
- Michael D. SWAINE, "Chinese Views on Cybersecurity in Foreign Relations", *China Leadership Monitor*, 42, Fall 2013.
https://www.hoover.org/research/chinese-views-cybersecurity-foreign-relations
- Laura DENARDIS, « The Emerging Field of Internet Governance », *The Oxford Handbook of Internet Studies*, Oxford, Oxford University Press, 2013, p. 555-575.
- 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 **)**
- SFDI, *Internet et le droit international*, Paris, éd. Pédone, 2014, 497 p.
- Laura DENARDIS, *The Global War for Internet Governance*, New Haven-London, Yale University Press, 2014, 296 p.
- « Internet Governance », *Revue française d'études américaines*, 4e trimestre 2014, n° 134, 126 p.
- Olivier KEMPF, *Alliances et mésalliances dans le cyberespace*, Paris, Economica, 2014, 176 p.
- Daniel VENTRE (ed.), *Chinese Cybersecurity and Defense*, London, Wiley, 2014, 320 p.
- Oriane BARAT-GINES, "Existe-t-il un droit international du cyberespace ?", *Hérodote*, 1er-2e trimestre 2014, n° 152-153, p. 201-220.
- CEIS, *Les droits maritimes et de l'espace peuvent-ils inspirer un droit du cyberespace ?*, Paris, CEIS, 2014, 66 p.
- Anne-Thida NORODOM, « Le droit international après l' « affaire Snowden » : la recherche de nouveaux équilibres », *Annuaire français de droit international*, LX, 2014, p. 731-753.
- Soraya SIDANI, *Intégration et déviance au sein du système international*, Paris, Presses de Sciences Po, 2014, 238 p.
- "Internet: une gouvernance inachevée", *Politique étrangère*, hiver 2014-4, 252 p.
- Kimberly HSU and Craig MURRAY, *China and International Law in Cyberspace*, US-China Economic and Security Review Commission, 6 May 2014.
https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf
- Benjamin MUELLER, *The Laws of War and Cyberspace. On the Need for a Treaty concerning Cyber Conflict*, The London School of Economics and Political Science, June 2014.
http://www.lse.ac.uk/ideas/research/updates/cyber
- Julien LEPOT, *Netmundial, un pas décisif dans l'évolution de la gouvernance Internet ?*, Paris, France, CEIS, décembre 2014, 52 p.
- Karine BANNELIER, « Cyber-Diligence : A Low-Intensity Due Diligence Principle for Low-Intensity Cyber-Operations », *Baltic Yearbook of International Law*, vol. 14, 2014, p. 23-39
- Kristen E. EICHENSEHR, "The Cyber-Law of Nations", *The Georgetown Law Journal*, 2015, vol. 103, p. 317-380
- Luca BELLI, "A heterostakeholder cooperation for sustainable internet policymaking". 2015. Available at
http://bibliotecadigital.fgv.br/dspace/handle/10438/17350/browse?value=Belli%2C+Luca&type=author
- "The Emergence of Contention in Global Internet Governance", Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond, Global Commission on Internet Governance, July 2015,at https://www.cigionline.org/sites/default/files/no17.pdf

- Yves AUFFRET, "Le cyberespace, catalyseur d'anarchie : approche théorique des relations internationales », *Res Militaris*, Juillet 2015
http://resmilitaris.net/ressources/10206/79/res_militaris_article_auffret_le_cyberespace__catalyseur_d_anarchie.pdf
- Paul WITHERS, "What is the utility of the Fifth Domain?", *Air Power Review*, Spring 2015, 18 (1), p. 126-150.
- Sébastien-Yves Laurent, *Cyber Strategy : définir un horizon stratégique dans un environnement cyber*, chaire de cybersécurité et de cyberdéfense Saint-Cyr/Sogeti/Thales, 2015, 92 p.
- Luca BELLI, *De la gouvernance à la régulation de l'internet*, Paris, Berger-Levrault, 2016, 336 p.
- Guillaume FLORIMOND, *Droit et Internet : de la logique internationaliste à la logique réaliste*, Paris, Mare et Martin, « Bibliothèque des thèses », 2016, 736 p.
- Séverine ARSÈNE, « Global Internet Governance in Chinese Academic Literature. Rebalancing a Hegemonic Wolrd Order?", *China Perspectives*, 2016-2, p. 25-35.
- F. MUSIANI, D. L. COGBURN, L. DENARDIS, & N. S. LEVINSON (ed.), *The turn to infrastructure in Internet governance*, Springer, 2016, 268 p.
- Hong SHEN, "China and Global Internet Governance: toward an alternative analytical framework", *Chinese Journal of Communication*, 2016, p. 1-21.
- Daniel VENTRE, *Des indices de cybersécurité pour faire du business et de la politique*, février 2016, chaire cyber-défense et cyber-sécurité, 16 p.
https://www.chaire-cyber.fr/IMG/pdf/41.pdf
- George PERKOVICH and Ariel E. LEVITE (ed.), *Understanding Cyber Conflict. 14 analogies*, Washington, Georgetown University Press, 2017, 297 p.
- Kriangsak KITTICHAISAREE, *Public International Law of Cyberspace*, Springer, "Law, Governance and Technology Series" n° 32, 2017, 376 p.
- Mark A. BARRERA, *The Achievable Multinational Cyber Treaty. Strengthening Our Nation's Critical Infrastructure*, Air Force Research Institute Papers, Perspectives on Cyber Power CPP-3, 2017, 24 p.
- Karine BANNELIER et Théodore CHRISTAKIS, *Cyberattaques. Prévention-réactions : rôle des États et des acteurs privés*, Paris, Cahiers de la Revue Défense Nationale, 2017, 90 p.
- Michael N. SCHMITT, "Grey Zones in the International Law of Cyberspace" (October 18, 2017), *Yale Journal of International Law Online;* 1-2017, 42:2, 21 p.
- Dwayne WINSECK, « The Geopolitical Economy of the Global Internet Infrastructure », *Journal of Information Policy*, vol. 7, 2017, p. 228-267.
- Jakob BUND and Patryk PAWLAK, « Minilateralism and norms in cyberspace », *Issue Alert*, European Union Institute for Security Studies, September 2017, 2 p.
- Karine BANNELIER, " « Rien que la *lex lata* » ? Etude critique du manuel de Tallin 2.0 sur le droit international applicable aux cyber-opérations", *Annuaire français de droit international*, 2017, LXIII, p. 121-160.
- Cai CUONG, « Global Cyber Governance. China's Contribution and Approach », *China Quarterly Of International Strategic Studies*, vol. 4, n° 1, 2018, p. 55-76
- Félix BLANC, « Géopolitique des câbles: une vision sous-marine de l'Internet », *Les Cahiers du CAPS*, n° 26, été-automne 2018, p. 31-49.
- James D. BOYS, "The Clinton administration's development and implementation of cybersecurity strategy (1993-2001)", *Intelligence and National Security*, vol. 33, n° 5, August 2018, p. 755-770.
- Brad BIGELOW, "The Topography of Cyberspace and Its Consequences for Operations", *2018 10th International Conference on Cyber Conflict*, NATO CCD COE Publications, 2018, p. 123-136.
- Maryline GRANGE et Anne-Thida NORODOM (dir.), *Cyberattaques et droit international. Problèmes choisis*, ¨Paris, éditions A. Pedone, 2018, 227 p.

- Sébastien-Yves LAURENT, « Les effets de la confusion des perceptions dans l'environnement numérique mondial », Forum Saint-Laurent sur la sécurité internationale, Québec (Canada), 2-3 mai 2019.

3. Bibliographie sur les RI

(ordre alphabétique)

- Raymond ARON, *Paix et guerre entre les nations*, Paris, Calmann-Lévy, « Liberté de l'esprit », 1962, 794 p.
- Bertrand BADIE, *La Diplomatie de connivence. Les dérives oligarchiques du système international*, Paris, La Découverte, 2011, 273 p.
- Karine BANNELIER, " « Rien que la *lex lata* » ? Etude critique du manuel de Tallin 2.0 sur le droit international applicable aux cyber-opérations", *Annuaire français de droit international*, 2017, LXIII, p. 121-160.
- Guillaume DEVIN et Marie-Claude SMOUTS, *Les Organisations internationales*, Paris, Armand Colin, 2011, 254 p.
- Charlotte HALPERN, « Politiques publiques internationales : Penser les échelles de la régulation politique », in : Dario BATTISTELLA, *Relations internationales. Bilan et perspectives*, Paris, Ellipses, 2013, pp. 357-376.
- Béatrice HIBOU (dir.), *La Privatisation des États*, Paris, Karthala, « Recherches internationales », 1996, 398 p.
- Geraint HUGHES, *My Enemy's Enemy: Proxy Warfare in International Politics*, Brighton, Sussex Academic Press, 2012, 241 p.
- Jean JOANA, « Faire la guerre : les politiques publiques, l'État et les conflits armés », *Critique internationale*, n° 72, juillet-septembre 2016, p. 127-145.
- Zaki LAÏDI, *La Norme sans la force*, Paris, Presses de Sciences Po, 2013 [1re éd.: 2008], 301 p.
- Xavier MATHIEU, « Souveraineté. Évolution conceptuelle d'une notion-clé », in : Dario Battistella (dir.), *Relations internationales. Bilan et perspectives*, Paris, Ellipses, 2013, pp. 195-214.
- Andrew MUMFORD, *Proxy Warfare*, Cambridge, Polity Press, 2013, 140 p.
- Franck PETITEVILLE, « Politiques internationales », in : Laurie BOUSSAGUET, Sophie JACQUOT et Pauline RAVINET (dir.), *Dictionnaire des politiques publiques*, Paris, Presses de Sciences Po, « Références », 2006, p. 437-446.
- Franck PETITEVILLE et Andy SMITH, « Analyser les politiques publiques internationales », *Revue française de science politique*, 2006-3, vol. 56, p. 357-366.
- James ROSENAU and Ernst-Otto CZEMPIEL (ed.), *Governance without Government: Order and Change in World Politics*, Cambridge University Press, 2008 [1re éd., 1992], 342 p.
- Soraya SIDANI, *Intégration et déviance au sein du système international*, Paris, Presses de Sciences Po, 2014, 238 p.
- Jean-Claude THOENIG, « Politique publique », in : Laurie BOUSSAGUET, Sophie JACQUOT et Pauline RAVINET (dir.), *Dictionnaire des politiques publiques*, Paris, Presses de Sciences Po, « Références », 2006, p. 420-427
- Vincent TIBERJ, « Chiffrer le monde. Approches quantitatives et relations internationales », in : Guillaume DEVIN (dir.), *Méthodes de recherches en relations internationales*, Paris, Presses de Sciences Po, « Relations internationales », 2016, p. 179-192

Table des matières

Table des figures