UNIVERSITE DE LILLE

FACULTE DES SCIENCES JURIDIQUES, POLITIQUES ET SOCIALES

MASTER II — DROITS ET POLITIQUES DE DEFENSE ET DE SECURITE NATIONALE

2018-2019

LA GOUVERNANCE INTERNATIONALE DE LA CYBERSECURITE

Source : https://syntec-numerique.fr/actu-informatique/projet-loi-renseignement-patriot-act-francais

Mémoire présenté et soutenu par

Adoh DJERI

SOUS LA DIRECTION DE

Vincent CATTOIR-JONVILLE

Professeur de droit public à l'Université de Lille

Dédicace

A la mémoire de mon père feu Waké DJERI qui, me convainquit de la place des études dans le monde d'aujourd'hui, avant de s'en aller prématurément. Qu'il trouve en ce travail, le respect de ses exhortations.

REMERCIEMENTS

Je ne saurai m'attribuer tout le mérite du présent mémoire. Pour son aboutissement, de nombreuses personnes m'ont apporté leur soutien, à différent niveaux et de diverses manières. S'il était un mot de témoignage de reconnaissance plus profond que le merci, il aurait été le bienvenu. A défaut donc de mieux, nous nous contentons de dire un merci sincère :

Au Professeur Vincent CATTOIR-JONVILLE**,** pour la qualité de sa direction de ce mémoire. Ses différents conseils et encouragements ainsi que les rapports de confiance qui ont existé entre nous ont été plus que déterminants à l'aboutissement de ce travail.

Au corps professoral du Master 2 Droits et politiques de défense et de sécurité nationale, pour la qualité des enseignements que nous avons reçus.

A Oukaté DJERI, mon frère et meilleur ami. J'ai la chance de partager avec lui la passion du Droit. Il m'a relu, et fait des remarques et suggestions.

A toute ma famille pour finir. A ma mère Azana AKPO, pour tous les sacrifices consentis pour mon éducation depuis le décès brutal de mon père. Puisse le tout puissant lui accorder santé et longue vie afin que je puisse un jour la combler.

SOMMAIRE

LISTE DES PRINCIPALES ABREVIATIONS

AG-NU…….. Assemblée Générale des Nations Unies

ANSSI…….. Agence Nationale de la Sécurité des Systèmes d'Information

CDI…….. Commission du Droit International

CESIN……. Club des Experts de la Sécurité de l'Information et du Numérique

CIJ…… Cour Internationale de Justice

CMTI…… Conférence Mondiale des Télécommunications

ENISA…….. Agence européenne chargée de la sécurité des réseaux et de l'information

EUROPOL.... Office européen des polices

FIFA……. Fédération Internationale de Football Association

FSSI…… Fonctionnaires de Sécurité des Systèmes d'Information

GGE……. Groupe d'Experts Gouvernementaux

ICANN …… Internet Corporation for Assigned Names and Numbers

INTERPOL...Organisation internationale de police criminelle

ISOC…….. Internet Society

NDD…….. Noms De Domaines

OEWG…….Groupe de travail à composition non limité

OIV…….. Opérateurs d'Importance Vitale

ONU…….. Organisation des Nations Unies

OTAN……. Organisation pour le Traité de l'Atlantique Nord

PESC…….. Politique Etrangère et de Sécurité Commune

PSDC…….. Politique de Défense et de Sécurité Commune

RGPD…….. Règlement Général sur la Protection des Données

SCADA…... Supervisory Control And Data Acquisition

SMSI…….. Sommet Mondial de la Société de l'Information

SRI……. Sécurité des Réseaux et des systèmes d'Informations

STAD…….. Systèmes de Traitement Automatisé de Données

TIC……. Technologies de l'Information et de la Communication

UA …….. Union africaine

UE…… Union européenne

INTRODUCTION GENERALE

« *Le cyberespace ne doit pas échapper au droit international qui peut et doit le gouverner* »

Forum mondial sur la gouvernance de l'internet
Discours du Président Emmanuel MACRON du 12/11/2018[1]

« *Nous savons que les pirates informatiques volent l'identité des personnes et s'infiltrent dans les messages privés. Nous savons que les pays étrangers et les entreprises balayent nos secrets d'entreprise. Maintenant, nos ennemis cherchent également la possibilité de saboter notre réseau électrique, nos institutions financières et nos systèmes de contrôle du trafic aérien. Nous ne pouvons regarder en arrière dans les années à venir et nous demander pourquoi nous n'avons rien fait face à de réelles menaces pour notre sécurité et notre économie*[2] » s'exclamait Barack OBAMA. Ainsi, le 12 mai 2017, une vague de cyberattaques simultanées d'envergure transnationale affectait une centaine de pays touchant des dizaines d'entreprises et d'organisations à travers le monde, dont les hôpitaux britanniques et le constructeur français Renault[3]. Les conséquences de cet acte malveillant étaient d'une gravité inouïe. Réagissant à la suite de cette cyberattaque d'envergure internationale, l'Office européen des polices « Europol » déclarait que

[1] Discours disponible sur https://www.elysee.fr/emmanuel-macron/2018/11/12/discours-du-president-de-la-republique-emmanuel-macron-lors-du-forum-sur-la-gouvernance-de-linternet-a-lunesco (consulté le 20 mai 2019).

[2] Extrait du discours du 12 février 2013 du Président américain Barack OBAMA devant le Congrès sur l'état de l'Union, en ligne sur https://www.reuters.com/article/us-obama-speech-cyber-idUSBRE91C03G20130213 (consulté le 13 mai 2019).

[3] N. ARPAGIAN, *La cybersécurité*, Nouvelle Imprimerie Laballery, 2018, p.41 ; voir aussi L. BITOUZET, *Revue trimestrielle de la gendarmerie nationale*, Limoges, SDG, 2018, p. 6 ; L. DREYFUS, « Une attaque informatique de portée mondiale crée la panique » disponible en ligne sur https://www.lemonde.fr/pixels/article/2017/05/12/des-hopitaux-anglais-perturbes-par-un-rancongiciel_5127034_4408996.html (consulté le 30 mai 2019) ;voir http://www.lefigaro.fr/secteur/high-tech/2017/05/12/32001-20170512ARTFIG00306-une-cyberattaque-d-envergure-frappe-des-hopitaux-britanniques.php (consulté le 30 mai 2019).

cette cyberattaque est « d'un niveau sans précédent »[4]. Cette vague de cyberattaques simultanées prouve à suffisance qu'Internet est un système global de réseaux informatiques interconnectés qui utilisent un protocole spécifique pour relier plusieurs milliards de terminaux dans le monde entier[5]. L'environnement ainsi créé par cette interconnexions des systèmes d'information est appelé le cyberespace[6]. Ce dernier est confronté à différentes menaces et risques qui compromettent la sécurité des Etats désormais interconnectés, des organisations, des entreprises et des personnes physiques. Ces menaces proviennent des activités illégales dont les auteurs démontrent un haut niveau de technicité tout en profitant des disparités juridiques entre les Etats[7]. Aussi, de la cybercriminalité aux attaques informatiques contre les infrastructures de types Supervisory Control And Data Acquisition (SCADA) en passant par l'espionnage, les menaces induites par l'internet sont-elles globales[8]. D'où la nécessité d'établir des solutions d'ensembles en vues d'éradiquer les cyberattaques et les conséquences qu'elles peuvent avoir sur les systèmes informatiques et d'informations des personnes et structures visées par les attaques. Les conséquences des attaques cybernétiques sont graves dans la vie des Etats[9] car elles peuvent affecter des infrastructures critiques telles que les Opérateurs d'Importance Vitale[10] (OIV) notamment les

---

[4] Voir http://www.lefigaro.fr/secteur/high-tech/2017/05/12/32001-20170512ARTFIG00306-une-cyberattaque-d-envergure-frappe-des-hopitaux-britanniques.php (consulté le 30 mai 2019).

[5] P. ACHILLEAS, W. MIKALEF, *TIC Innovation et droit international*, Paris, Pedone, 2017, p. 31.

[6] Voir A. CATTARUZZA, D. DANET, *La cyberdéfense, quelle territoire quel droit ?* , Paris, Economica, 2014, pp. 23-24.

[7] L., BITOUZET, *Revue trimestrielle de la gendarmerie nationale française*, SDG, décembre 2018, N°263, p. 1.

[8] A. DESFORGES, « La coopération internationale et bilatérale en matière de cybersécurité : enjeux et rivalités », Etude publié dans le cadre du laboratoire de l'IRSEM, p. 5, disponible sur :https://www.defense.gouv.fr/content/download/214515/2384806/file/Laboratoire%20n%C2%B016%20-%202013.pdf , (consulté le 25 mai 2019).

[9] Voir l'attaque d'EDF en 2011 : https://www.usine-digitale.fr/article/attaque-ddos-le-cas-d-edf-et-ses-consequences-juridiques.N490969 (consulté le 23 Mai 2019) ; voir aussi : A. DESFORGES, « La coopération internationale et bilatérale en matière de cybersécurité : enjeux et rivalités » disponible sur https://www.defense.gouv.fr/content/download/214515/2384806/file/Laboratoire%20n%C2%B016%20-%202013.pdf , (consulté le 25 mai 2019).

[10] Définition de l'OIV à l'article R. 1332-1 du code la défense française : Un Opérateur d'Importance Vitale:

banques, hôpitaux, ministères, médias, secteur de l'énergie[11]…. L'ampleur de la menace est telle que certains chercheurs prédisent un « Armageddon électronique » si rien n'est fait pour la juguler[12]. Cette prédiction n'est pas hasardeuse car l'on peut imaginer les conséquences qui pourraient suivre la prise de contrôle à distance du poste de commandement[13] d'une puissance nucléaire par des hackeurs[14]. En cas de survenance d'un tel scénario, les conséquences sur la sécurité nationale de l'Etat seraient importantes[15]; l'existence même de l'Etat pourrait être menacée. Une incertitude juridique plane aussi sur l'organisation et l'encadrement des réponses que les Etats doivent apporter à ces attaques cybernétiques. Ce qui met à coup sûr un frein à l'efficacité de la lutte contre la cybercriminalité. Le besoin se fait ainsi clairement ressentir de mener une étude sur : « la gouvernance internationale de la cybersécurité ». Pour la commodité du raisonnement, une précision sur la sémantique des différents termes du sujet s'invite. Controversée en doctrine parce qu'elle est un concept protéiforme qui s'inscrit dans une logique

---

1° Exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale;

2° Gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :

a) D'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;

b) Ou de mettre gravement en cause la santé ou la vie de la population.

Voir aussi https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/ (consulté le 27 mai 2019).

[11] I. CHOUKRI, « Remarques sur les Manuels de Tallinn et le droit international applicable aux cyber-opérations », disponible sur http://revel.unice.fr/psei/index.html?id=1853 (consulté le 24 Mai 2019).

[12] M. BLAINE, E. ROCHE, « Convention internationale sur l'utilisation pacifique du cyberespace », 27-3/4 / 2013, disponible sur le site https://journals.openedition.org/netcom/1449 , (consulté le 07 Mai 2019) ; voir aussi D. VENTRE, « Les évolutions de la cybersécurité : contraintes, facteurs, variables », juin 2015, p. 1 ; voir aussi D. DANET, « Collapsologie numérique », Stratégique, 2017/4, pp. 213-215, disponible en ligne sur https://www.cairn.info/revue-strategique-2017-4-page-213.htm (consulté le 21 juin 2019).

[13] Le poste de commandement est le dispositif technique qui permet de lancer une arme nucléaire et de contrôler sa progression dans l'espace.

[14] Francisation du mot anglais « hacker » qui désigne un pirate ; ici c'est un pirate informatique.

[15] D. PIALOT, « Cybersécurité dans l'énergie : pourquoi l'Europe et les Etats-Unis devraient collaborer », disponible en ligne sur https://www.latribune.fr/entreprises-finance/industrie/energie-environnement/cybersecurite-dans-l-energie-pourquoi-l-europe-et-les-etats-unis-devraient-collaborer-770489.html (consulté le 09 juin 2019).

multidimensionnelle, la « gouvernance » se définit de manière classique comme une nouvelle façon de gouverner par l'association pluraliste d'acteurs à la procédure de décision[16]. Au sens politique, c'est un néologisme qui désigne l'« art de gouverner »[17]. Soulignons néanmoins que la notion de « gouvernance » concerne autant la gestion publique que la gestion privée. Le terme est, par exemple, à la fois employé, relativement au secteur de l'entreprise ou lorsqu'il s'agit d'institutions politiques nationales, européennes ou internationales[18]. De ce fait, la « gouvernance internationale » qui fait l'objet de notre réflexion est une gouvernance qui prend en compte d'office les acteurs et les institutions de droit international. Quant à la cybersécurité dont la gouvernance représente le cœur de la présente réflexion, il faut dire d'emblée qu'elle n'a pas de définition unanimement admise en droit international[19]. Ce qui n'est pas surprenant quand on considère la conflictualité qui porte sur la question au plan international. Même la doctrine n'a pas réussi à proposer une définition qui fait l'unanimité malgré les différentes tentatives pour cerner la notion et en tracer les contours, ainsi que les efforts de standardisation menés par les instances internationales, régionales et certaines expériences nationales[20]. Une définition de la cybersécurité est contenue dans la recommandation UIT-T X.1205 portant présentation générale de la cybersécurité de l'Union Internationale des Télécommunications (UIT)[21]. Pour l'UIT : « On entend par cybersécurité, l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions

---

[16] G. OANTA, J. RIOS RODRIGUEZ, *Le droit public à l'épreuve de la gouvernance*, Perpignan, Collections Etudes, 2012, p. 298.

[17] R. ROUQUETTE, *Dictionnaire du droit administratif*, Le Moniteur, 2002.

[18] G.OANTA, J.RIOS RODRIGUEZ, *Le droit public à l'épreuve de la gouvernance*, *Op.cit.* p.7 ; voir aussi J. CHEVALLIER, « La gouvernance et le droit », in Mélange AMSELEK, Bruylant, 2005, pp. 189-207 ; disponible aussi en ligne sur https://hal.archives-ouvertes.fr/hal-01759961/document (consulté le 08 juin 2019).

[19] Voir F. AJINA, Cadre juridique de la cybersécurité dans l'espace francophone, p. 4 ; [en ligne] disponible sur http://ific.auf.org/sites/default/files/IFIC-AUF-EtudeJurid-Cybrsecurite.pdf (consulté le 29 mai 2019).

[20] *Ibidem.*

[21] L'UIT est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (TIC).

formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication et la totalité des informations transmises et/ ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de cybersécurité sont les suivants: disponibilité, intégrité,-qui peut englober l'authenticité et la non-répudiation-confidentialité »[22]. Cette définition de la cybersécurité qui est proposée par l'UIT est longue et en plusieurs temps. Ce qui ne facilite pas sa compréhension. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) de la France propose une définition plus synthétique. En effet, pour l'ANSSI, la cybersécurité est un « état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles[23] ». Quand la cybersécurité touche directement les systèmes d'information en lien avec la sécurité nationale à travers des activités militaires ou non, elle est désignée sous le vocable de « cyberdéfense[24] ». Les deux notions de cybersécurité et cyberdéfense sont donc interchangeables en fonction du contexte et de la finalité mais la cybersécurité est plus inclusive. En effet, la cybersécurité fait appel à des techniques de sécurité des systèmes

[22] Cf. Recommandation UIT- X1205 (04-2008), Présentation générale de la cybersécurité, paragraphe 3.2.5, disponible en ligne sur https://www.itu.int/rec/T-REC-X.1205-200804-I/fr (consulté le 06 juin 2019) ; voir aussi M. WATTIN-ANGOUARD, Cyberménaces et sécurité nationale, *in Le droit de la sécurité et de la défense en 2013*, Aix-en-Provence, PUAM, 2014, p. 300.

[23] Voir https://www.ssi.gouv.fr/entreprise/glossaire/c/ (consulté le 29 mai 2019) ; voir aussi M. WATTIN-ANGOUARD, « Cybermenaces et sécurité nationale », *Op. Cit.* pp. 300-301.

[24] *Ibid*. p. 301.

d'information et s'appuie sur la lutte contre la cybercriminalité et sur une mise en place d'une cyberdéfense[25]. Par souci de synthèse et de clarté, il convient de retenir la définition de l'ANSSI sans oublier l'intérêt et la portée de la définition de l'UIT. Ces précisions terminologiques étant apportées la compréhension du sujet parait plus facile. Il s'agit donc de traiter des mesures, stratégies, et actions prises sur le plan international et qui sont de nature à rendre optimale c'est-à-dire meilleure, l'administration de la cybersécurité. La cohérence et la bonne compréhension de la présente réflexion requièrent de revisiter le contexte et l'historique de cette question. En effet, le 21ème siècle voit la consécration des technologies numériques, comme la fin du Moyen-âge a vu celui de l'imprimerie. Cette révolution contemporaine est notamment liée à la structure planétaire d'Internet[26]. Cette structure de l'internet ne rime pas forcement avec la gouvernance de la règlementation et des risques que peut engendrer l'usage malveillant de l'internet. En effet le droit international ne définit pas ce qu'est une cyberattaque ni ce que l'on entend par cyberespace[27]. De même, il n'existe actuellement aucun traité international de cybersécurité réglementant le cyberespace[28]. La seule convention multilatérale de portée mondiale en vigueur qui touche partiellement la cybersécurité est la Convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 entrée en vigueur en 2004[29]. Elle est de base une convention régionale destinée à l'Europe mais certains Etats non membres du Conseil de

[25] A. CATTARUZZA, D. DANET, *La cyberdéfense : quel territoire, quel droit, Op. Cit.* p. 167.

[26] J. FERRY, M. QUEMENER, *Cybercriminalité : défi mondial*, Paris, Economica, 2009, voir préface.

[27] O. BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? », Revue Hérodote, n°152-153, 2014, p. 201 ; (Article disponible en ligne à l'adresse https://www.cairn.info/revue-herodote-2014-1-page-201.htm).

[28] *Ibid*, p. 219.

[29] Cette convention est aussi connue comme la Convention de Budapest sur la cybercriminalité ou la Convention Budapest en hommage à la capitale Hongroise qui accueilli la signature dudit traité. Voir M. QUEMENER, J-P. PINTE, *Cybersécurité des acteurs économiques: risques, réponses stratégiques et juridiques*, Paris, Lavoisier, 2013, p. 209.

l'Europe l'ont ratifiée[30]. Face à la recrudescence des cyberattaques paralysant parfois le fonctionnement de certains Etats comme ce fut le cas de l'Estonie en 2007[31], et de la Géorgie en 2009[32] des voix s'élèvent pour une appréhension du phénomène par la communauté internationale. Il convient de rappeler que l'une des premières cyberattaques médiatisées que le monde a connues a été enregistrée en Iran en 1974 avec le retardement du fonctionnement des centrifugeuses iraniennes de Bushehr par Israël. En effet, ce retardement des centrifugeuses iraniennes a été possible par une infection d'un cyber-virus que l'Etat d'Israël a lancé sur les systèmes d'information de la centrifuge. La même opération s'est répétée en 2009 avec le virus Stuxnet[33]. Récemment une vague de cyberattaques a touché 150 pays infectant plus de 300.000 ordinateurs d'un virus appelé le *ransomware Wannacry* ou *Wannacrypt*[34], un virus prenant en otages les données personnelles des systèmes informatiques attaqués[35]. Ainsi il est devenu essentiel de développer des mesures techniques et non techniques permettant aux Etats et aux entreprises de se protéger et de se défendre dans ce nouvel espace souvent considéré come le cinquième champ de conflictualité après la terre, la mer, l'air et l'espace extra-atmosphérique[36]. Cette quête d'une harmonisation des points de vue des Etats sur la cybersécurité conduira l'Organisation pour le Traité de l'Atlantique

---

[30] C'est le cas des Etats-Unis, le Canada, le Japon, l'Afrique du Sud, l'Australie, Israël.... voir la liste complète des adhésions à cette convention sur le site https://www.coe.int/fr/web/conventions/full-list/-conventions/treaty/185/signatures (consulté le 29 mai 2019).

[31] A. CATTARUZZA, D. DANET, *La cyberdéfense : quel territoire, quel droit ? Op. Cit.* p.22 ; Voir aussi J. FERRY, M. QUEMENER, *Op. Cit*. p. 93.

[32] S. KORNS, J. JOSHUA, 2009, pp. 60-76, cité par M. BLAINE, E.ROCHE, « Convention internationale sur l'utilisation pacifique du cyberespace », *Op. Cit*. Paragraphe 2.

[33] Voir « Comment le virus Stuxnet s'en est pris au programme nucléaire iranien », disponible en ligne sur www.slate.fr/story/30471/stuxnet-virus-programme-nucleaire-iranien%3famp (consulté le 31 mai 2019) ; voir aussi H.H.DINNISS, *Cyberwarfare and the Laws of War*, Cambridge University Press, 2012, p. 57.

[34] Voir G. CORNET, « Le Manuel de Tallinn ou comment le droit veut rattraper la technologie », disponible en ligne sur http://ultimaratio-blog.org/archives/8434 (consulté le 14 juin 2019).

[35] Voir « Cyberattaque mondiale Wannacry, le ransomware qui chiffre les données » disponible en ligne sur www.lexpress.fr/actualite/monde/vague-internationale-de-cyberattaques_1907798.amp.html (consulté le 31 mai 2019).

[36] O. BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? », *Op. Cit*. p. 201.

Nord (OTAN) à mettre sur pied un groupe d'expert formé d'une vingtaine d'experts de différentes nationalités pour produire un document de référence permettant l'analyse légale des cyberattaques majeures**,** c'est-à-dire pouvant être considérées comme des violations des lois sur le recours à la force et autorisant ainsi les États à exercer leur droit à l'autodéfense. Il s'agissait donc, dans un premier temps, de transposer les aspects les plus cruciaux du droit international aux activités dans le cyberespace afin de proposer un ouvrage de référence qui permettrait d'analyser les cyberattaques soit entre États souverains, soit entre États et acteurs non-étatiques, et qui pourraient justifier le déclenchement d'hostilités[37]. Cette étude accouchera du *Manuel de Tallinn*[38]. Ce manuel est novateur compte tenu de la qualité de ses propositions. Il est un outil exceptionnel pour les juristes car il représente une analyse de haut niveau des problématiques d'interprétation du droit actuel au regard des nouveaux enjeux du cyberespace[39]. En revanche, le Manuel de Tallinn n'est pas contraignant. Il ne reflète que l'analyse d'une vingtaine d'experts internationaux, non représentatifs de l'intégralité de la communauté internationale[40]. Toutefois, il convient de relever qu'une partie de la doctrine reconnait en certaines règles de ce manuel, la valeur de droit coutumier. Aussi, dans une logique de gouvernance, certaines règles du Manuel de Tallinn pourraient-elles être considérées comme du *soft-law* puisque la bonne gouvernance reviendrait à considérer les positions des différents acteurs du cyberespace y compris celles de la société civile. Face aux menaces des cyberattaques sur la sécurité des Etats chaque pays essaie, comme il peut, d'ériger des barrières techniques et réglementaires pour éradiquer la menace. Certains Etats tels que les USA, la Russie, Israël, sont aujourd'hui présentés comme des cyber-puissances en

[37] http://ultimaratio-blog.org/archives/8434 (consulté le 23 mai 2019).

[38] Il est publié en deux volumes (Le Manuel 1 et 2) et disponible pour le moment en anglais. Sa traduction en français est en cours d'élaboration.

[39] O. BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? » *Op. Cit*. p. 204.

[40] *Ibid* , p. 205.

raison de leur capacité de résistance et d'attaque dans le cyber[41]. Le caractère mondial de la menace incite les organisations supranationales tels que l'ONU et l'Union européenne à faire sienne la gouvernance de la cybersécurité. Ainsi depuis que la Fédération de Russie a soumis à l'Assemblée générale des Nations Unies (AG-NU) une proposition de résolution sur la cybersécurité-intitulé « *les progrès de la téléinformatique dans le contexte de la sécurité internationale* » -en 1998, l'ONU s'est engagée à rassembler les points de vue des Etats autour d'un idéal sécuritaire en matière cyber[42]. L'AG-NU a donc adopté le projet de résolution sans le mettre aux voix[43]. Depuis, le Secrétaire général de l'ONU présente un rapport annuel à l'Assemblée générale, qui contient les vues des États membres de l'Organisation sur la question[44]. Dans la même dynamique différents groupes d'experts ont été mis en place par l'AG-NU pour se pencher sur les problèmes et solutions liés au cyberespace. Ces groupes d'experts ont rendu différents rapports[45] qui sont restés pour l'heure lettre morte car l'AG-NU n'a pas encore adopté un instrument international juridiquement contraignant sur la cybersécurité et le cyberespace[46]. Aux Nations Unies, les Etats sont d'ailleurs divisés autour de l'idée d'avoir un instrument juridiquement contraignant sur la cybersécurité. Certains Etats à l'instar de la France préfèrent que chaque Etat s'organise individuellement d'abord avant de penser à une fédération des moyens de lutte[47]. Ces Etats privilégient-ils leur souveraineté numérique à la lutte internationale ? Il convient de souligner que la question de gouvernance internationale n'est pas nouvelle en droit international. En effet, chaque fois qu'un phénomène mine l'intérêt collectif des nations, la communauté internationale s'organise ensemble pour l'éradiquer. C'est

[41] Voir M. BLAINE, E. ROCHE, « Convention internationale sur l'utilisation pacifique du cyberespace », *Op. Cit*. Paragraphe 18.

[42] Voir https://www.un.org/disarmament/fr/informatique-et-telematique/ (consulté le 24 mai 2019).

[43] Cf. résolution A/RES/53/70 du 04 janvier 1999.

[44] Voir https://www.un.org/disarmament/fr/informatique-et-telematique/ (consulté le 24 mai 2019).

[45] Voir les différents rapports dans les résolutions de l'AG-NU : A/RES/65/201 du 30 juillet 2010 ; A/RES/66/24 du 13 décembre 2011 et A/RES/68/98 du 24 juin 2013.

[46] O. BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? », *Op. Cit*. p. 219.

[47] Voir https://www.un.org/press/fr/2018/agdsi3613.doc.htm (consulté le 26 mai 2019).

ainsi qu'on parle de gouvernance internationale de l'internet, la gouvernance internationale de l'environnement[48] ou de gouvernance internationale des mers et océans pour lutter contre la pollution des mers et mieux gérer les ressources marines[49].

Face à l'ampleur de la menace sur la sécurité informatique et des grands enjeux qui plane sur la cybersécurité à l'échelle mondiale, la question qui se pose est de savoir comment le droit international organise la gouvernance internationale de la cybersécurité. En d'autres termes, quelles sont les mécanismes, stratégies et réglementations qui sont mis en place et celles qui peuvent être instaurés pour promouvoir et assurer la sécurité des systèmes informatiques qui sont par essence interconnectés dans le monde entier ?

Au regard de cette problématique, le sujet parait très intéressant. D'un point de vue pratique le sujet n'a pas que des enjeux techniques. En effet la cybersécurité est désormais l'une des priorités des politiques de sécurité et de défense nationale. Il est donc indispensable que se développent des réflexions autour de ces enjeux[50]. Le sujet a aussi des enjeux économiques. Les entreprises font désormais de grands chiffres d'affaires sur la cybersécurité et l'on parle même de l'économie du numérique ou l'économie de la cybersécurité. En dehors des enjeux économiques, la cybersécurité pose de grands enjeux politiques notamment ceux liés à la géopolitique des Datacenters[51]. Les Datacenters constituent désormais un instrument d'influence réciproque entre les Etats et chacun a besoin de garder un contrôle sur les entreprises qui relèvent de sa nationalité. Ceci se justifie par l'immense utilité de ces immenses réservoirs de base de données contenant des

[48] P. JACOB, « La gouvernance de l'internet du point de vue du droit international public », *Annuaire Français de Droit International 2010*, Paris, CNRS Editions pp. 544-545.

[49] Voir A. MONACO, P.PROUZET, *Gouvernance des mers et des océans*, Londres, édition ISTE, 2015, 294 p.

[50] A. CATTARUZZA, D. DANET, *La cyberdéfense : quel territoire, quel droit*, *Op. Cit.* p. 7.

[51] Générique anglais désignant les centres de données (endroit physique où sont rassemblées de nombreuses machines, bien souvent des serveurs contenant des données informatiques).

centaines de serveurs des entreprises, des millions de sites web, des millions de noms de domaines[52]…. Le sujet est d'avantage intéressant compte tenu de son actualité. En effet très peu de recherches universitaires ont été menées sur les aspects internationaux de la cybersécurité. La plupart des recherches sur cette question restent partielles.

Le présent sujet reste aussi d'actualité au regard de la nouveauté et la fréquence des risques informatiques et des réponses que les Etats veulent apporter pour parer à leurs conséquences sur la vie des administrations, des entreprises et même des hommes. De ce fait, les travaux qui sont menés aux Nations Unies sur la cybersécurité peuvent occuper l'agenda des Nations Unies au cours des dix prochaines années. De son côté, l'Union européenne vient d'adopter le Règlement européen sur la cybersécurité le 12 mars 2019[53] et les prochains mois et années seront consacrés à la vulgarisation et la mise en œuvre de ce mécanisme européen de cybersécurité.

La réflexion autour du présent sujet s'inscrit dans un questionnement pluridisciplinaire d'autant plus que la cybersécurité met en exergue différentes disciplines. Mais le droit international sera longuement questionné compte tenu du caractère international de la cybersécurité. Ainsi au regard de tout ce qui précède, l'existence de quelques éléments d'une gouvernance de la cybersécurité sur le plan international semble évidente. Mais ces éléments sont insuffisants. Il est donc normal de conclure que la gouvernance internationale de la cybersécurité reste encore embryonnaire (**Partie I**) d'autant plus que les dispositions et mécanismes devant juguler les risques informatiques à l'échelle internationale n'existent pas dans bien des cas et les quelques unes qui existent sont mis en œuvre avec une certaine timidité. Cette organisation demeure néanmoins et mérite d'ailleurs d'être

[52] C'est l'exemple des capacités des Datacenters d'OVH en 2018. OVH est l'une des plus grandes entreprises française spécialisée dans les services de cloud computing. Son siège social est basé sur Roubaix dans la métropole lilloise.

[53] Voir le Règlement européen sur la cybersécurité du 12 mars 2019 en ligne sur le site http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_FR.html (consulté le 26 mai 2019).

consolidée, pour l'harmonie d'une gouvernance internationale de la cybersécurité (**Partie II**).

PARTIE I

UNE GOUVERNANCE INTERNATIONALE EMBRYONNAIRE DE LA CYBERSECURITE

La nature exogène de la cybersécurité impose aux Etats une lutte globale sur le plan international[54]. Cette exigence est justifiée par l'interconnexion des réseaux informatiques de part le monde, constituant ce que certains auteurs appellent l'écosystème numérique[55]. En effet, l'architecture technique du réseau internet est foncièrement globale et agéographique, il n'en va pas de même du système juridique international. Celui-ci repose sur des juridictions définies par les limites territoriales des Etats[56]. De ce fait, la gouvernance internationale de la cybersécurité a du plomb dans l'aile. En effet, les Etats bien que soucieux de la sécurité du cyberespace, restent jaloux de leur souveraineté numérique qui peut-selon certains Etats- leur échapper s'ils participent à des harmonisations internationales des moyens de lutte contre les cybermenaces. Cette crainte est justifiée d'autant plus que certaines cybermenaces ont une influence directe sur la sécurité nationale des Etats. Ainsi de nombreuses entraves et notamment les enjeux de souveraineté et de sécurité nationale tendent à réduire toute tentative de coopération en une collaboration a minima (**chapitre 1**). De ce fait, les Etats sont repliés sur eux même et sont perplexes quant à une véritable coopération en matière de cybersécurité. Aussi, convient-il de préciser que les quelques mécanismes supranationaux sur la cybersécurité qui existent manquent d'homogénéité (**chapitre 2**).

[54] A. DESFOGES, « La coopération internationale et bilatérale en matière de cybersécurité : enjeux et rivalités », *Op. Cit.* pp. 5- 6 ; Voir aussi A. CATTARUZZA, D. DANET, *La cyberdéfense : quel territoire, quel droit ? Op. Cit.* p. 15.

[55] P. ACHILLEAS, W. MIKALEF, *TIC Innovation et droit international*, *Op. Cit.* p. 11.

[56] B. DE LA CHAPELLE, « Gouvernance de l'internet et gouvernance sur l'internet », en ligne disponible sur https://www.lajauneetlarouge.com/gouvernance-de-linternet-et-gouvernance-sur-linternet/ (consulté le 29 mai 2019).

CHAPITRE 1

LES ENTRAVES A LA GOUVERNANCE INTERNATIONALE DE LA CYBERSECURITE

L'impact des cyberattaques sur la vie des citoyens, des entreprises et même de l'Etat a amené les gouvernants à revoir leurs politiques publiques. En effet la cybersécurité est désormais l'une des priorités de sécurité et de défense nationale[57] (**Section 1**). De ce fait, l'on est en présence d'une question qui engage l'Etat dans son attribut le plus régalien qu'est la souveraineté. Il est qu'à même surprenant de constater que les Etats ne jouissent pas pleinement de cette souveraineté en matière numérique (**Section 2**) d'autant plus que les frontières du cyberespace sont poreuses[58] et les Etats perdent de ce fait une partie de leur souveraineté numérique en raison du caractère planétaire de la chose numérique.

SECTION 1. LA PRISE EN COMPTE DE LA SECURITE INFORMATIQUE PAR LA SECURITE NATIONALE : UNE AFFIRMATION DE SOUVERAINETE DES ETATS SUR LE NUMERIQUE

L'avènement de la révolution numérique et son influence sur les nouvelles habitudes des citoyens, des entreprises et même de l'Etat, a amené les Etats à appréhender les risques qui peuvent découler de l'utilisation malveillante de l'informatique. De ce fait, les Etats ont progressivement élargi leurs politiques de sécurité nationale à la cybersécurité[59] (paragraphe 1). Cette prise en compte de la cybersécurité par la sécurité nationale est justifiée par des enjeux certains et l'objectif de protéger les systèmes d'informations des Etats (paragraphe 2).

---

[57] A. CATTARUZZA, D. DANET, *La cyberdéfense : quel territoire, quel droit ? Op. Cit.* p. 7.

[58] B. DE LA CHAPELLE, « Gouvernance de l'internet et gouvernance sur l'internet », *Op. Cit.* ; voir aussi A. DESFORGES, « Cyberespace et Internet : un réseau sans frontières ? », *CERISCOPE Frontières*, 2011, [en ligne], URL : http://ceriscope.sciences-po.fr/content/cyberespace-et-internet-un-reseau-sans-frontieres-?page=show , (consulté le 29/05/2019).

[59] Voir A.M. TALIHARM, « En quête de la cyberpaix : gérer la cyberguerre par la coopération internationale, 2013, disponible en ligne sur https://unchronicle.un.org/fr/article/en-qu-te-de-la-cyberpaix-g-rer-la-cyberguerre-par-la-coop-ration-internationale (consulté le 27 juin 2019).

Paragraphe 1 : La consécration de la cybersécurité dans les politiques de défense et de sécurité nationale des Etats

Ces dernières années ont vu une augmentation des menaces en matière de vols des données personnelles et d'infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques[60]. En effet, notre société moderne est devenue plus vulnérable d'abord par les menaces naturelles qui ont toujours existé[61] et aujourd'hui l'on compte les risques technologiques. On passe donc de la civilisation de la peine à la civilisation de la panne[62]. La cybersécurité participe à l'éradication de la panne technologique volontaire et malveillante. Ainsi face à la gravité des cybermenaces, les Etats ont intégré la cybersécurité dans leurs politiques publiques de sécurité pour mieux la gouverner[63]. C'est ainsi que la France après d'âpres législations sur la sécurité des systèmes informatiques a finalement placé la sécurité et la défense des systèmes d'information au cœur des priorités de la stratégie nationale dans le Livre blanc de 2008[64]. En effet le Livre Blanc a répertorié les grands risques technologiques que la France est susceptible de subir si une stratégie efficace n'est pas mise en place pour éradiquer les attaques cybernétiques. Et c'est la mise en application des recommandations de ce précieux mémento qui s'est matérialisé par la création par la France de l'Agence Nationale de la Sécurité des Systèmes d'Informations (ANSSI) en 2009[65]. Cet organisme a pour objectifs de :

---

[60] L. BITOUZET, *Revue de la gendarmerie nationale N° 263*, Limoges, SDG, 2018, p. 6.

[61] Les menaces naturelles qui ont toujours existé sont souvent les catastrophes naturelles (séismes, irruptions du volcan, les ouragans, les inondations….).

[62] Voir Y. LASFARGUE, « Techno-jolies, techno-folies ?, comment réussir les changements technologiques », Les éditions d'organisations, 1988.

[63] A.CATTARUZZA, D. DANET, S. TAILLAT, *La cyberdéfense, Politique de l'espace numérique*, Malakoff, Armand Colin, pp. 9-10.

[64] Le Livre Blanc , Tome 1, Paris, Odile Jacob/ La documentation Française, 2008, pp. 50-52 ; Voir aussi G. POUPARD, « La cybersécurité au cœur du nouveau Livre Blanc sur la défense et la sécurité nationale », disponible sur le site de l'ANSSI https://www.ssi.gouv.fr/publication/la-cybersecurite-au-coeur-du-nouveau-livre-blanc-sur-la-defense-et-la-securite-nationale/ (consulté le 05 juin 2019) ; WATIN-ANGOUARD, « Cybermenaces et sécurité nationale », in *Le droit de la sécurité et de la défense en 2013*, C. VALLAR et X. LATOUR(dir.), PUAM, p. 298.

[65] Cf. communiqué sanctionnant la création de l'ANSSI disponible sur le site https://www.ssi.gouv.fr/uploads/IMG/pdf/ANSSI_Communique_de_presse.pdf (consulté le 05 juin 2018).

• de détecter et réagir au plus tôt en cas d'attaque informatique, grâce à la création d'un centre opérationnel renforcé de cyberdéfense, actif 24 heures sur 24, chargé de la surveillance permanente des réseaux les plus sensibles de l'administration et de la mise en œuvre de mécanismes de défense adaptés;

• de prévenir la menace : l'agence contribuera au développement d'une offre de produits et de services de confiance pour les administrations et les acteurs économiques ;

• de jouer un rôle permanent de conseil et de soutien aux administrations et aux opérateurs d'importance vitale ;

• d'informer régulièrement les entreprises et le grand public sur les menaces et les moyens de s'en protéger, en développant une politique de communication et de sensibilisation active[66].

Certains Etats à l'instar des Etats-Unis, Israël, la Chine ou la Russie constituent ce qu'on appel aujourd'hui les cyber-puissances[67]. Ces Etats ont compris très tôt l'importance du cyber et ont développé de nombreux outils capables de faire face aux cyberattaques de grandes ampleurs et même de mener une attaque contre des entités ennemis. Pour ces cyber-puissances qui maitrisent l'arme cybernétique, la cybersécurité a dépassé les finalités civiles ; elle constitue désormais un moyen de déploiement militaire stricto sensu[68]ou une facette d'un conflit armé[69]. Ainsi les Etats-Unis font parti des premiers pays qui ont consacré l'adaptation de leur puissance militaire classique en force d'action numérique. Pour

---

[66] *Ibidem.*

[67] Voir M. BLAINE, E. ROCHE, « Convention internationale sur l'utilisation pacifique du cyberespace », *Op. Cit*. Paragraphe 16.

[68] H. H. DINNISS, *Cyber Warfare and the Laws of War, Op. Cit.*, pp. 75-76; voir aussi M. BLAINE, E. ROCHE, « Convention internationale sur l'utilisation pacifique du cyberespace », *Op. Cit*. Paragraphe 23.

[69] Ce fut le cas du conflit armé international entre la Russie et la Géorgie en 2008 à l'occasion duquel des attaques cybernétiques ont été longuement utilisées. Voir Oriane BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? », *Op. Cit*. p. 206 ; voir aussi O. ROBILLART, « La Géorgie victime de cyberattaques », disponible en ligne sur www.silicon.fr/la-georgie-victime-de-cyber-attaques-30893.html/amp (consulté le 06 juin 2019).

se faire avec brio un centre de commandement cyber a même été mis en place[70].

Eu égard à ce qui précède, l'on conviendra volontiers de la réalité de l'incorporation de la cybersécurité dans les politiques de défense et de sécurité nationale des Etats. Cette intégration de la sécurité du cyber par des politiques de sécurité et de défense des Etats est justifiée à bien d'égards.

Para 2 : Une consécration justifiée: l'objectif de protection des systèmes informatiques

Ces dernières années, les cyberattaques prennent une tournure répétitive avec des conséquences assez graves pour les structures visées par les cyberattaques. Le phénomène prend de l'ampleur assez en raison de la numérisation sans cesse croissante des services, entreprises et même des habitations des ménages. Le nombre d'attaques se compte par milliers et l'impact est significatif. Cette cybersinistralité est inquiétante (A) et justifie l'implication de la lutte contre les cyberattaques dans les priorités de sécurité nationale des Etats[71]. Ceci est nécessaire car la protection des systèmes d'information en dépend (B).

A-Une cybersinistralité inquiétante

Le taux des cyberattaques ne cesse d'augmenter dans le monde depuis quelques années. Selon une étude menée par le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN), 92% des entreprises françaises ont subi des cyberattaques en 2018[72]. Au même moment, 77% d'organisations dans le

---

[70] Voir « Cyberdéfense : le commandement cyber des Etats-Unis prend du galon », disponible sur https://www.zdnet.fr/actualites/cyberdefense-le-commandement-cyber-des-tats-unis-prend-du-galon-39840528.htm (consulté le 09 juin 2019).

[71] Marc WATTIN-ANGOUARD, « Entre sécurité et liberté, quel équilibre pour la défense et la sécurité de l'espace numérique », in *Annuaire 2018 du Droit de la sécurité et de la défense*, B. WARUSFEL et F. BAUDE (Cord.), Mare et Martin, p. 115.

[72] Voir M. ROSSIGNOL, « Sécurité de l'information », disponible en ligne sur https://www.preventica.com/actu-enbref-barometre-attaques-cybersecurite-entreprises-160119.php (consulté le 11 juin 2019).

monde ont subit une cyberattaque réussi l'année précédente[73]. La vague de cyberattaques de 2017 dénommé *ramsonware* ou *Wannacry* a fait à elle seule 200.000 victimes dans les 150 pays victimes de la vague d'attaque[74]. Deux ans auparavant, la télévision francophone internationale TV5 monde subit une cyberattaque sans précédent. Cette attaque affecta les 11 chaines de télévision du groupe TV5 monde. Pendant des heures la chaine n'avait plus de contrôle sur l'ensemble de ses chaines et les réseaux sociaux et sites internet associés à ces chaines de télévision[75]. Le but de cette cyberattaque de TV5 monde n'était pas économique contrairement à la vague de cyberattaque de 2017. Il s'agissait d'un acte de cyberterrorisme revendiqué par l'Etat islamique[76], mais après d'âpres investigations l'attaque proviendrait de cybercriminels russes[77]. Toutefois, l'histoire retiendra la vague de cyberattaques que l'Estonie a subie en 2007 comme étant la plus grave en raison de la durée des attaques et des conséquences néfastes qu'elle a eu dans la vie de ce pays. L'Estonie a tiré les leçons de cette vague de cyberattaques et a érigé de nombreux moyens techniques pour lutter contre la cybercriminalité et protéger ces systèmes informatiques (B).

B- La protection efficiente des systèmes d'informations

---

[73] Voir « Statistiques cybersécurité 2018 », disponible sur le site https://www.vaadata.com/blog/fr/statistiques-cyber-securite-2018/ (consulté le 11 juin 2019).

[74] Voir https://www.lemonde.fr/pixels/article/2017/05/14/cyberattaque-200-000-victimes-essentiellement-des-entreprises-dans-150-pays-assure-europol_5127506_4408996.html (consulté le 11 juin 2019).

[75] Voir https://www.rtbf.be/info/monde/europe/detail_tv5-monde-un-an-apres-la-cyberattaque-notre-fonctionnement-est-toujours-difficile?id=9263682 (consulté le 11 juin 2019) ; voir aussi https://www.lemonde.fr/pixels/article/2017/05/14/cyberattaque-200-000-victimes-essentiellement-des-entreprises-dans-150-pays-assure-europol_5127506_4408996.html (consulté le 11 juin 2019).

[76] *Ibidem*.

[77] Voir la réaction du Directeur Général de TV5 monde Yves BIGOT sur le site web de la chaine https://information.tv5monde.com/info/cyberattaque-de-tv5monde-s-agirait-il-de-pirates-informatiques-russes-37691 (consulté le 11 juin 2019).

Le but de la cybersécurité est la protection des systèmes d'informations des Etats et de leurs démembrements[78]. Pour ce faire, la cybersécurité fait appel à des techniques de sécurisation des systèmes d'information. Ces dernières passent par la prévention et l'anticipation sans oublier la disponibilité, l'intégrité la confidentialité et la traçabilité restent les quatre piliers de la cybersécurité[79]. Il convient de souligner que la sécurité en elle-même procède par cette dynamique d'anticipation et d'action[80]. De ce fait, le cyber emprunte à la sécurité ses attributs de bases afin d'assurer son intégrité dans l'intérêt des utilisateurs. Les Etats disposent donc d'un ensemble de référentiels en matière de sécurité pour l'ensemble de leurs services et les entreprises qui sont établies sur leur territoire. En application de ces normes et référentiels de sécurité, au sein des ministères les hauts fonctionnaires de défense et de sécurité et les fonctionnaires de sécurité des systèmes d'information (FSSI) exercent une mission de veille et d'action contre toute intrusion dans le système d'information. Dans les administrations et entreprises, un responsable de la sécurité des systèmes d'information et son équipe jouent le même rôle de veille[81]. En cas d'attaque, les responsables de la sécurité des systèmes d'information sont donc outillés pour faire face au risque. Quand le risque est d'une grande ampleur ils recourent souvent à l'expertise des services de l'Etat de type ANSSI pour gérer la crise. Ce fut le cas en 2015 avec l'attaque de la chaine internationale TV5 monde[82].

Chaque Etat essaie comme il peut de faire face aux cyberattaques à travers

---

[78] Collectivités territoriales, administrations, entreprises, etc.

[79] X. LATOUR et C. VALLAR, *Le droit de la sécurité et de la défense en 2013*, *Op. Cit.* p.297 ; voir aussi la définition de la cybersécurité selon l'UIT, disponible dans la Recommandation UIT- X1205 (04-2008), Présentation générale de la cybersécurité, paragraphe 3.2.5, disponible en ligne sur https://www.itu.int/rec/T-REC-X.1205-200804-I/fr (consulté le 11 juin 2019).

[80] P. TROUCHAUD, « La gouvernance de la cybersécurité : savoir anticiper les risques », disponible en ligne sur https://www.pwc.fr/fr/publications/cybersecurite/gouvernance-de-la-cybersecurite-savoir-anticiper-les-risques.html (consulté le 12 juin 2019).

[81] X. LATOUR et C. VALLAR, *Le droit de la sécurité et de la défense en 2013*, *Op. Cit.* 301.

[82] Voir le communiqué de presse de l'ANSSI annonçant l'attaque de TV5 monde et le soutient technique que l'ANSSI apporte à la chaine, disponible sur https://www.ssi.gouv.fr/actualite/attaque-informatique-contre-tv5-monde-lanssi-mobilisee/ (consulté le 12 juin 2019).

les différents mécanismes de cybersécurité au plan interne. Ce qui est normal et signe d'une affirmation de souveraineté. Malheureusement, les cybermenaces ne sont pas que des menaces endogènes. Elles sont de plus en plus exogènes aux Etats victimes de cyber attaques d'autant plus que les frontières du cyberespace sont poreuses voir inexistantes dans bien de cas. D'où la souveraineté numérique des Etats est limitée dans le cyberespace.

SECTION 2 : L'EVIDENTE SOUVERAINETE NUMERIQUE LIMITEE DES ETATS

La souveraineté numérique des Etats pose problème au regard de la structure planétaire d'internet[83] et du cyberespace[84]. En effet, les Etats pris individuellement ne maitrisent pas le cyberespace d'autant plus que les frontières du cyberespace sont inconsistantes voir inexistantes (Paragraphe 1). De plus une nouvelle question de territorialisation a conquis le monde numérique ces dernières années à travers le stockage des données et la délocalisation des Datacenters (Paragraphe 2).

Para 1 : L'inconsistance des frontières dans le cyberespace

L'inconsistance des frontières dans le cyberespace est encore une raison de plus qui doit pousser les Etats à faire la promotion de la gouvernance internationale de la cybersécurité. En effet, le cyberespace se caractérise par l'interconnexion des systèmes informatiques dans le monde. Cette interconnexion des systèmes informatiques entraine une dichotomie entre les frontières terrestres des Etats et leurs frontières numériques (A). Les Etats étant habitués à assurer la sécurité de

[83] J.FERRY, M. QUEMENER, *Cybercriminalité, défi mondial, Op. Cit.* Préface, p. 8.

[84] A. DESFORGES, « Cyberespace et Internet : un réseau sans frontières ? », *Op. Cit.*

leur territoire jusqu'à la limite de leurs frontières terrestres se retrouvent donc en difficulté face à un cyberespace sans frontières. Pire encore, les Etats restent dépendant les uns à l'égard des autres car leur interconnexion provient de l'intégrité des câbles sous marins que d'aucuns qualifient de bien commun mondial[85] (B).

A- L'inévitable supplantation des frontières terrestres des Etats par des frontières numériques

Le cyberespace étant une manifestation de la mondialisation suppose l'existence d'un territoire numérique sans frontières parce qu'il est le résultat d'une interconnexion de millions de systèmes informatique[86]. Les concepteurs d'internet voulaient un nouveau monde libre affranchi des sujétions des Etats et bénéficiant d'une totale indépendance[87]. Or classiquement les Etats exercent les prérogatives de leur souveraineté notamment la sécurité et la défense dans les limites de leurs territoires que sont les frontières terrestres. Dans le nouveau territoire qu'est le cyberespace la donne n'est plus la même. Dans le cyberespace, le but de la frontière ne serait pas de contrôler le territoire en soi mais de contrôler les flux (humains marchandises, capitaux, données) qui sortent et entrent sur le territoire afin d'éviter les risques informatique[88]. De ce fait, la frontière ligne est inadaptée dans le langage du cyberespace. Les frontières terrestres étant inadéquates pour

---

[85] Un bien commun est un bien considéré comme un bienfait par le plus grand nombre, et auquel chacun devrait avoir accès, comme la santé, la sécurité, l'utilisation de la terre ou encore l'accès à un logement décent… et désormais l'information, devenue cardinale dans notre monde moderne. En droit international, la notion de bien commun est entendue à la fois comme une chose qui n'appartient à personne (*res nullius*) et qui appartient à tous (*res communis*). Cette vision implique, théoriquement, un libre accès à l'objet apportant le bienfait collectif ainsi que sa préservation. *Cf.* Laurent Cordonnier, « Éclairage sur la notion de biens communs », *Alternatives économiques*, p. 3, consultable sur http://alternatives-economiques.fr/blogs/gadrey/files/laurent-bc-v2.pdf *; voir* C. MOREL, « Les câbles sous-marins : un bien commun mondial ? », Etude, 2017, p.1.

[86] Voir Amaël CATTARUZZA, D. DANET, *La cyberdéfense : quel territoire, quel droit, Op. Cit.* p. 21; voir aussi J. GRIMMELMAN, Internet Law: cases and problems, Seventh Edition, 2017, p. 56.

[87] *Ibid*. pp. 51-52 ; voir aussi J. P. BARLOW, Déclaration d'Indépendance du cyberespace, Libres enfants du savoir numérique, 2000, p. 47-48, disponible en ligne sur https://www.cairn.info/libres-enfants-du-savoir-numerique--9782841620432-page-47.htm (consulté le 13 juin 2019).

[88] Voir Amaël CATTARUZZA, « frontières du cyberespace : réalités, contournements, détournements », Cesson, 2013, disponible en ligne sur https://www.academia.edu/6630332/Les_fronti%C3%A8res_du_cyberespace (consulté le 13 juin 2019).

assurer la sécurité des systèmes d'information, les Etats recours à des stratégies de filtrages des flux d'information et d'interdiction des sites malveillants sur leurs territoires. Ces pratiques peuvent atténuer certaines formes d'atteinte à la sécurité informatique mais restent obsolètes pour luter contre le gangstérisme informatique de grande échelle qui passe par le principe même de l'interconnexion des réseaux. L'atteinte au territoire numérique d'un Etat est évidemment une violation des règles de droit international. En effet, pour la Cour Internationale de Justice (CIJ), le respect de la souveraineté territoriale est un fondement essentiel des relations entre Etats[89]. Partant de ce principe l'atteinte à la souveraineté numérique d'un Etat porterait-il atteinte à l'obligation de relations pacifique entre Etats qu'établit la charte des Nations-Unies[90] ? Encore faut-il établir le lien de causalité entre l'attaque et un Etat. Le plus souvent les cyberattaques restent anonymes. Ceci confirme la limitation de la souveraineté des Etats dans le monde numérique qui est par nature un monde globalisé nécessitant des solutions d'ensemble. En dehors des failles liées à la porosité des frontières dans le cyberespace, les Etats sont obligés de partager leur souveraineté numérique du fait même d'utiliser les câbles sous-marins principaux vecteurs de communication électronique.

B-L'interdépendance de la souveraineté numérique des Etats à travers les câbles sous-marins

L'interconnexion des systèmes d'information formant ainsi le cyberespace n'est possible qu'à travers le réseau internet. L'on assiste aujourd'hui partout dans le monde à une véritable explosion du trafic internet. Ce dernier se fait essentiellement par l'intermédiaire des câbles sous marins. Véritable canal de

[89] Affaire du Détroit de Corfou (Royaume-Uni c Albanie), CIJ Recueil 1949, 4, 35 ; voir aussi C. DOUTRIAUX, « Frontières légales et souveraineté dans le cyberespace », 2015, disponible en ligne sur http://www.chaire-cyber.fr/IMG/pdf/article_1_2_-_chaire_cyberdefense.pdf (consulté le 13 juin 2019).

[90] Article 2 paragraphe 4 de la Charte des Nations Unies, base de l'interdiction du recours à la force entre Etats.

communication électronique[91], les câbles sous marins constituent un objet de conflictualité entre Etats en raison des nombreux enjeux qui entourent leur fonctionnement[92]. En effet les câbles sous marins constituent le moyen de transit de 99% des communications électroniques tandis que les satellites de communications ne représentent que 0, 99% du trafic[93]. De ce fait les Etats et les grands groupes appelés les GAFAM (Google, Amazone, Facebook, Aplle, Microsoft) se disputent le pouvoir d'influence d'internet. En effet les câbles sous marins sont financés et poser par les GAFAM et leurs partenaires. De ce fait ils gardent une influence sur le réseau internet. Pire encore 80 % des flux des données générés par internet sont stockés à Los Angeles aux Etats-Unis dans les Datacenters des géants d'internet. Les révélations d'Edouard Snowden ont mis en évidence que la National Security Agency (NSA) des Etats-Unis espionnerait systématiquement les communications du monde entier à travers le programme PRISM[94] et l'interface de programmation des GAFAM[95]. Où est la souveraineté numérique des Etats quand un seul Etat a le pouvoir de contrôler toute les communications électroniques et téléphoniques des autres Etats ? La gouvernance internationale ne serait-elle pas le gage de la sécurité informatique et de la cybersécurité ? La raison de plus qui confirme l'intérêt de la gouvernance

[91] Environ 99% du trafic internet se fait par les câbles marins. Le reste du trafic internet (environ 0,99%) se fait par les satellites de télécommunications ; voir les dessous des cartes câbles sous marins la guerre invisible disponible sur https://www.youtube.com/watch?v=RSC0ft-hdRk (consulté le 13 juin 2019).

[92] Voir l'analyse de la Marine nationale française à propos des enjeux autour des câbles sous marins, disponible en ligne sur https://www.colsbleus.fr/articles/11160 (consulté le 14 juin 2019).

[93] Voir le dessous des cartes « les câbles sous marins », disponible en ligne sur https://www.youtube.com/watch?v=RSC0ft-hdRk (consulté le 14 juin 2019).

[94] Le Programme PRISM également appelé US-984XN est un programme américain de surveillance électronique par la collecte de renseignement à partir d'internet et d'autres fournisseurs de service électronique. Voir l'article de synthèse proposé par le Guardian, principal médiateur d'Edward SNOWDEN lors de ses révélations par l'intermédiaire du journaliste Glenn Greenwad : « NSA Files Decoded. What revelations mean for you », The Guardian, 1er novembre 2013. Pour plus d'éclaircissements sur le programme PRISM, voir E. MEILLAN, F. LEVIEUX, Survivre à la guerre numérique, Paris, 2017, pp.157-159 ; voir aussi A. CATTARUZZA, D. DANET, La cyberdéfense: quel territoire, quel droit? *Op. Cit*. p. 64 ; L. BLOCH, « Surveillance américaine sur l'Internet, antécédents et conséquences », 2014, disponible en ligne sur https://www.diploweb.com/Surveillance-americaine-sur-l.html (consulté le 14 juin 2019)

[95] Voir Le dessous des cartes « les câbles sous marins », disponible en ligne sur https://www.youtube.com/watch?v=RSC0ft-hdRk (consulté le 14 juin 2019) ; L. BLOCH, « Surveillance américaine sur l'Internet, antécédents et conséquences », *Op. Cit.*

international de la sécurité informatique est l'émergence de la délocalisation des Datacenters créant ainsi la question de la territorialité dans le Cloud Computing[96].

Para 2 : L'émergence croissante de la conflictualité et des principes de territorialité dans le cyber

Les règles de territorialité ont envahi le monde du cyber à travers les conséquences agéographique d'internet. En effet, avec l'avènement d'internet, certains Etats gagnent des territoires alors que d'autres en perdent. Il s'agit non seulement des territoires numériques mais aussi des territoires physiques qui sont conquis par les Etats ou leurs entreprises par le biais de l'application extra territoriale des lois relatifs à la protection des données personnelles (A). De ce fait, une cyberconflictualité nait entre les Etats d'autant plus que la sécurité des données est devenue un instrument d'influence géopolitique et économique (B).

A-L'émergence croissante des règles de territorialité dans le cyber

Compte tenu de son caractère agéographique, le monde du cyber ne cesse de générer de nouveaux territoires numériques et physiques pour les Etats. En effet certains Etats gagnent du terrain là où d'autres en perdent. Le phénomène de déterritorialisation se manifeste par le stockage à distance des données internet et l'application extraterritoriale des lois nationales de sécurité des données. Il convient de rappeler que les Etats Unis sont le premier pays au monde qi a le plus de connaissance en matière numérique d'autant plus que internet est née aux Etats Unis[97]. De part sa position stratégique dans la création et le développement

[96] Le Cloud Computing est le générique anglais qui désigne le stockage distant des données informatiques par l'intermédiaire d'un réseau généralement Internet.

[97] S. LAURENT, « Il y a 40 ans naissait presque internet », 2009, disponible en ligne sur http://www.lefigaro.fr/web/2009/09/02/01022-20090902ARTFIG00263-il-y-a-40-ans-naissait-presque-internet-.php (consulté le 17 juin 2019) ; voir aussi « Brève histoire d'internet », disponible en ligne sur https://www.tuteurs.ens.fr/internet/histoire.html (consulté en ligne sur 18 juin 2019).

d'internet, les Etats-Unis constituent le principal pole d'hébergement des sites internet des entreprises et un pole de transit du flux de données des Datacenters et des câbles sous marins. De ce fait, une bonne partie des données des utilisateurs d'internet se retrouvent aux Etats-Unis. Cette situation ne rassure pas les utilisateurs étrangers du web, ce qui amène de nombreuses entreprises américaines des télécommunications[98] à décentraliser leurs Datacenters dans les pays d'origine des utilisateurs pour rassurer ceux ci quant à la sécurité de leur donnée. Ce mécanisme de délocalisation des Datacenters n'est pas sans conséquence sur la soumission de l'entreprise au droit de l'Etat d'accueil notamment l'obligation de se conformer aux règles de sécurisation des données des utilisateurs. Aussi, depuis l'adoption du Règlement Général sur la Protection des Données (RGPD) par l'UE, toute entreprise étrangère qui traite les données personnelles des citoyens européens est soumise à l'obligation de protection des données que consacre cet instrument juridique européen[99]. De ce fait, les règles de sécurité informatique que consacre le RGPD s'appliquent aux entreprises étrangères qui traiteraient des données personnelles des citoyens européens quelques soit le pays d'établissement de l'entreprise. Se sentant menacé par l'entrée en vigueur du RGPD, les Etats-Unis adoptent précipitamment le *Cloud Act* qui octroie au gouvernement américain l'accès à l'ensemble des données personnelles de n'importe quel citoyen, peu importe sa nationalité, du moment où les données sont stockées chez des hébergeurs américains et peu importe la position géographique du data center, et ce sans avoir à saisir un tribunal et, bien évidemment, sans avoir à le notifier aux personnes concernées. Cette loi américaine permet donc aux Etats-Unis de contraindre les firmes américaines à fournir des données stockées sur leurs

[98] Il s'agit des entreprises telles que Google qui a délocalisé ses Datacenters dans le monde entier notamment en France, Facebook qui dispose d'un grand Datacenters en Suède (voir Y. EUDES, « Le Datacenter de Facebook aux abords du cercle polaire », disponible en ligne sur https://www.lemonde.fr/grands-formats/visuel/2016/06/29/dans-le-data-center-de-facebook-aux-abords-du-cercle-polaire_4960471_4497053.html consulté le 17 juin 2019).

[99] Cf. Article 3 du RGPD : « Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:
a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non;ou
b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

serveurs (Google, Facebook, Twitter, Amazon, WhatsApp, etc[100]. Cet antagonisme croissant entre Etats à propos de l'influence d'internet et de ses sous produits est source de conflictualités.

B-Naissance d'une cyber conflictualité aux enjeux géopolitico-économiques

Les enjeux du cyberespace sont sources de profondes conflictualités entre les Etats[101]. Nous sommes dans un état de guerre froide numérique et certains Etats ne publient pas la fréquence des cyberattaques qu'ils subissent au risque de passer pour des Etats en perte de puissance. Certains chercheurs prédisent même que la troisième guerre mondiale a déjà commencé et se passe dans le cyber[102]. C'est une guerre qui se fait en silence. Les positions des Etats sont tranchées et chacun légitime sa position à travers des théories juridiques ubuesques. Si la plupart des cyberattaques restent anonyme il est devenu courant de voir des cyberattaques ouvertement assumées par leurs auteurs ou réunissant tous les indices d'être attribué à un Etat donné[103]. Certaines cyberattaques ont purement un but politico-militaire notamment la paralysie de l'Etat attaquée mais de plus en plus de cyberattaque ont des motifs économiques. Ces dernières sont souvent le fait des personnes physiques. Mais il n'est pas exclu qu'un Etat organise une vague de cyberattaque à des fins économiques. Ce fut le cas de la vague de cyberattaque de 2017 dénommée *WannaCry*[104] dont la responsabilité a été attribuée à la Corée du

[100] J.L CHAMBON, « Le Cloud Act, la riposte américaine du RGPD européen », 2018, disponible en ligne sur https://www.lesechos.fr/idees-debats/cercle/le-cloud-act-la-riposte-americaine-au-rgpd-europeen-139429 (consulté en ligne le 17 juin 2019).

[101] Voir J .NOCETTI, « Géopolitique de la cyber-conflictualité », politique étrangère, 2018, p. 15, disponible en ligne sur https://www.ifri.org/sites/default/files/atoms/files/geopolitique_de_la_cyber-conflictualite.pdf (consulté le 18 juin 2019).

[102] D. J. RAHMIL, « Nous sommes déjà dans la troisième guerre mondiale et elle est cyber », 2019 ; voir aussi M. BLAINE, E. ROCHE, « Convention internationale sur l'utilisation pacifique du cyberespace », *Op. Cit*.

[103] C'est le cas de la vague de cyberrattaques subie par l'Estonie en 2007 alors qu'elle était en situation de guerre avec la Russie. L'on peut aussi évoquer la grande cyberrattaque qu'a subi la Corée du nord en 2014. Tout portait à croire que les Etats-Unis étaient derrière cette cyberattaque. Cette cyberattaque est intervenue quelques jours seulement après la promesse du Président américain Barack Obama d'une «réponse proportionnée» à la cyberattaque imputée par le FBI à Pyongyang la même année ; voir http://www.leparisien.fr/international/piratage-la-coree-du-nord-privee-d-internet-pendant-plus-de-9-heures-23-12-2014-4395653.php (consulté le 21 juin 2019).

[104] Aussi connu sous le nom *Wannacrypt* ou *ransomware WannaCry*

Nord. Selon Ben WALLACE, Ministre britannique de la sécurité à l'époque de l'attaque *WannaCry*, cette cyberattaque était une stratégie de la Corée du Nord-isolée sur la scène internationale-d'accéder à des devises étrangères[105].

Face aux différentes vagues de cyberattaques répétitives et leurs graves conséquences dans la vie des utilisateurs du web-que les théoriciens de l'effondrement qualifient de « collapsologie numérique[106] »-, les Etats ne parlent pas d'une même voix pour instaurer une gouvernance internationale de la cybersécurité. Toute fois la situation n'est pas non plus au point mort. En effet l'on constate l'existence d'éléments épars d'une gouvernance internationale de la cybersécurité.

---

[105] Voir http://www.leparisien.fr/international/piratage-la-coree-du-nord-privee-d-internet-pendant-plus-de-9-heures-23-12-2014-4395653.php (consulté le 21 juin 2019).

[106] Voir, D. DANET, « Collapsologie numérique », *Op. Cit.* pp.1-3.

CHAPITRE 2

L'EXISTENCE D'ELEMENTS EPARS D'UNE GOUVERNANCE INTERNATIONALE DE LA CYBERSECURITE

L'état de la gouvernance internationale de la cybersécurité n'est pas au point mort. Bien que les principaux acteurs n'aient pas encore développé des mécanismes et normes sûrs en vue de répondre aux cyberattaques au plan international, l'on peut affirmer avec certitude qu'il existe des éléments épars d'une gouvernance de la cybersécurité au plan international. Ainsi l'on peut relever l'existence d'une dichotomie entre l'OTAN et l'ONU en matière de cybersécurité (**Section 1**). Cette dichotomie se manifeste dans l'appréhension de la cybersécurité par ces deux grandes organisations internationales. Aussi, convient-il de souligner le dynamisme de gouvernance de la cybersécurité au plan régional (**Section 2**). La gouvernance de la cybersécurité ne se résume pas à la prééminence des acteurs étatiques dans la sphère de décision du cyber. Elle voit émerger des institutions internationales privés notamment l'Internet Corporation for Assigned Names and Numbers (ICANN) dont les compétences sont remarquables dans la gouvernance d'internet et la lutte pour la sécurité informatique (**Section 3**).

SECTION 1 : L'ECART DE DYNAMIQUE ENTRE L'OTAN ET L'ONU SUR LA CYBERSECURITE

En matière de cybersécurité l'OTAN se révèle être l'une des plus grandes organisations internationales qui a compris très tôt les nombreux enjeux du cyber et l'intérêt de développer une vision claire en vue de répondre aux cybermenaces dans le cadre d'une union politico-militaire (paragraphe 1). Contrairement à l'OTAN, les Nations Unies semblent timide face à la fulgurante émergence des cybermenaces dans le monde. Elles n'offrent pas un cadre juridique clair pour lutter contre les cyberattaques au plan international (paragraphe 2).

Para 1 : La prise en compte de la cybersécurité dans le concept stratégique de l'OTAN

L'émergence des cyberattaques dans le monde et leurs conséquences sur la sécurité nationales des Etats a amené l'OTAN à étendre sa politique militaire dans le cyber afin de répondre à ses principales tâches que sont la défense collective, la gestion de crise et la sécurité coopérative[107]. De ce fait, l'OTAN adapte ses objectifs aux enjeux de l'heure afin d'être efficace sur le terrain. C'est ainsi qu'après d'âpres improvisations elle consacre la cyberdéfense dans son concept stratégique[108] afin de répondre aux cybermenaces de grandes envergures susceptibles d'affecter la sécurité nationale de ses membres[109] (A). Mais la construction otanienne reste muette sur les cyberattaques provenant des personnes privées qui peuvent s'avérer aussi néfastes que les cyberattaques entre Etats (B).

A- La consécration du régime de cyberguerre entre Etats

L'adoption par l'OTAN d'un nouveau concept stratégique le 19 et 20 novembre 2010[110] titré « Engagement actif, défense moderne » marque l'adaptation officielle de l'OTAN à gérer la menace cybernétique. En effet, l'OTAN manifeste son intérêt pour la cyberdéfense depuis le début des années 2000. Mais cet engagement est resté improvisée car l'OTAN n'avait pas jusque là une base d'action claire en cyberdéfense. Ainsi le 14 mai 2008, l'OTAN créa un

[107] Cf. article 5 du Traité de Washington du 04 avril 1949 disponible en ligne sur le site de l'OTAN à l'adresse https://www.nato.int/cps/fr/natohq/official_texts_17120.htm (consulté le 25 juin 2019).

[108] Dans la politique militaire de l'OTAN, les concepts stratégiques dotent l'Alliance des moyens de répondre aux défis de sécurité, et guident son évolution politique et militaire future. Ils rappellent la nature et l'objectif immuables de l'OTAN ainsi que ses tâches de sécurité fondamentales. Ils sont revus de manière à tenir compte de l'évolution de l'environnement de sécurité mondial, afin que l'Alliance soit dûment préparée à exécuter ses tâches fondamentales. La transformation au sens large du terme est donc une caractéristique permanente de l'Organisation. Voir plus d'explications sur « Les concepts stratégiques de l'Otan » sur le site de l'organisation à l'adresse https://www.nato.int/cps/fr/natohq/topics_56626.htm (consulté le 25 juin 2019).

[109] L'OTAN compte actuellement 29 pays membres. A sa création elle comptait 12 membres fondateurs dont La Belgique, Le Canada, Le Danemark, Les États-Unis, La France, L'Islande, L'Italie, Le Luxembourg, La Norvège, Les Pays-Bas, Le Portugal et Le Royaume-Uni.

[110] Le nouveau concept stratégique de l'OTAN de 2010 est disponible sur le site de l'OTAN à l'adresse https://www.nato.int/strategic-concept/pdf/Strat_Concept_web_fr.pdf (consulté le 25 juin 2019).

Centre d'excellence de cyberdéfense coopérative basé à Tallin la capitale de l'Estonie[111] dont la mission est d'améliorer les capacités, la coopération et le partage d'information entre les pays membres et partenaires de l'OTAN dans le domaine de la cyberdéfense entre autres par des actions de formation et de recherche et développement[112]. Ce Centre d'excellence reste une structure d'appui au commandement militaire de l'OTAN qui est responsable de la cyberdéfense de l'Alliance. Le concept stratégique de 2010 vient donc à point nommé car dans son identification des menaces auxquelles l'Alliance fait face, les cyberattaques sont désormais considérées comme une préoccupation prioritaire, après le terrorisme et la prolifération des armes de destruction massive[113]. Ainsi l'article 12 du concept stratégique de 2010 décrit l'ampleur de la menace cybernétique en ces termes : « Les cyberattaques augmentent en fréquence, sont mieux organisées et causent des dommages plus coûteux aux administrations, aux entreprises, aux économies, voire aux réseaux de transport et d'approvisionnement ou autres infrastructures critiques; elles risquent d'atteindre un seuil pouvant menacer la prospérité, la sécurité et la stabilité des États et de la zone euro-atlantique. Des forces armées et services de renseignement étrangers, la criminalité organisée, des groupes terroristes et/ou extrémistes sont autant de sources d'attaque possibles[114] ». Pour répondre aux menaces cybernétiques énoncées dans le concept stratégique de 2010, l'OTAN élabore le Manuel de Tallinn[115] afin de caractériser les cyberattaques de grandes ampleurs et proposer des réponses collectives pour parer la menace

[111] Le choix de l'Estonie n'est pas fortuit. L'Estonie s'affirme comme une « démocratie numérique » et son économie dépend de l'internet. Après son passé douloureux en cyberattaques en 2007, l'Estonie a revendiqué fortement la création d'un centre de cette nature. Grâce à ses quatre "licornes" (Skype, Taxify, Playtech, Transferwise) et l'accès à tous les services publics en ligne depuis son ordinateur, le pays balte est devenu, en une vingtaine d'années, une référence en matière d'e-gouvernance et de transformation numérique ; voir https://www.france24.com/fr/20181221-afrique-estonie-diplomatie-numerique-nouveaux-amis-benin-kersti-kaljulaid-e-gouvernance (consulté le 26 juin 2019).

[112] Voir https://www.nato.int/cps/fr/natolive/news_7266.htm (consulté le 26 juin).

[113] N. LACHMANN, « Les défis du nouveau concept stratégique de l'OTAN », *Points de mire*, vo. 11, no. 8, 3 août 2010, disponible en ligne sur http://www.ieim.uqam.ca/spip.php?article5776 (consulté le 25 juin 2019) ; voir aussi les articles 11-15 du concept stratégique de l'OTAN de 2010 disponible en ligne sur https://www.nato.int/strategic-concept/pdf/Strat_Concept_web_fr.pdf (consulté le 25 juin 2019).

[114] Cf. Article 12 du concept stratégique de l'OTAN de 2010.

[115] Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press : http://wdn.ipublishcentral.net/cambridge_university_press2956/viewinside/455511150748134 .

cybernétique[116]. Tel que présenté plus haut, le Manuel de Tallinn est le résultat d'un groupe d'expert formé d'une vingtaine d'experts de différentes nationalités pour produire un document de référence permettant l'analyse légale des cyberattaques majeures**,** c'est-à-dire pouvant être considérées comme des violations des lois sur le recours à la force et autorisant ainsi les États à exercer leur droit à l'autodéfense. Il s'agissait donc, dans un premier temps, de transposer les aspects les plus cruciaux du droit international[117] aux activités dans le cyberespace afin de proposer un ouvrage de référence qui permettrait d'analyser les cyberattaques soit entre États souverains, soit entre États et acteurs non-étatiques, et qui pourraient justifier le déclenchement d'hostilités[118]. Cette transposition vise à établir le fondement de la légitime défense en droit international[119] au cyberespace. De ce fait, le Manuel de Tallin ne s'applique pas aux cyber-opérations de faible intensité que le Manuel de Tallinn qualifie de cybercriminalité[120]. Assurément, aux termes de la 11ème règle du Manuel : « Une cyber opération constitue un recours à la force lorsque son ampleur et ses effets sont comparables à des opérations autres que la cybercriminalité allant jusqu'au

---

[116] Il convient de souligner qu'il ya deux manuels de Tallin : le premier, titré « *Tallinn Manual 1.0 : International Law Applicable to Cyber Warfare* » parait en 2013 et le second « *Tallin Manual 2.0 : International Law Applicable to Cyber Operations* » -qui est une mise à jour du premier parait en 2017.

[117] Il s'agit du corpus de règle de droit international à savoir : --

-les conventions et traités internationaux sur le droit de la mer, de l'air, des télécommunications et de l'espace extra-atmosphérique.

- les conventions et traités internationaux relatifs au droit de la guerre (les conventions de Genève, les protocoles additionnels, les conventions de La Haye et la convention sur l'interdiction ou la restriction de l'emploi de certaines armes.

- les conventions et traités relatifs aux statuts des Tribunaux pénaux internationaux et la Cour internationale de justice

- les conventions et traités relatifs aux droits de l'enfant, à la protection des biens culturels, ainsi qu'à l'environnement

- la jurisprudence comme source interprétative du droit

[118] Voir http://ultimaratio-blog.org/archives/8434 (consulté le 23 mai 2019).

[119] Conformément à l'article 51 de la Charte des Nations qui dispose que : « Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. Les mesures prises par des Membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité et n'affectent en rien le pouvoir et le devoir qu'a le Conseil, en vertu de la présente Charte, d'agir à tout moment de la manière qu'il juge nécessaire pour maintenir ou rétablir la paix et la sécurité internationales.

[120] Voir la 11ème règle du Manuel de Tallinn disponible en ligne sur https://hackademics.fr/forum/news/g%C3%A9n%C3%A9rales/68137-les-95-r%C3%A8gles-de-la-guerre-cybern%C3%A9tique-manuel-de-tallinn (consulté le 26 juin 2019).

niveau du recours à la force[121]. Le cas échéant l'Alliance pourrait répondre à l'attaque conformément à l'article 5 de la convention de Washington[122]. Le Manuel de Tallinn s'avère être une œuvre monumentale en raison de son originalité et de la qualité de ses propositions[123]. Mais un doute plane sur le choix des experts qui l'ont rédigé d'autant plus que la vingtaine d'experts vient des pays membres de l'OTAN[124]. Ce qui fragilise sa large acceptation par les acteurs du cyberespace. Des questions se posent aussi sur la valeur juridique du Manuel de Tallinn. Il n'ya aucun doute sur le caractère non contraignant du manuel en soi[125]. L'OTAN n'a jamais voulu créé un instrument juridique contraignant en élaborant ce précieux manuel. Toutefois, le contenu du Manuel de Tallin est basé sur la logique argumentative du droit positif conventionnel, la coutume et même la jurisprudence internationale[126]. De ce fait, son contenu pourrait constituer *un soft-law* en cyberdéfense ou la pépinière d'un futur instrument juridique international sur la cyberdéfense. La réalisation du Manuel de Tallin est un bon début de gouvernance internationale de la cybersécurité dans la mesure où les experts qui l'ont rédigé étaient des universitaires et non des politiques[127]. Le Manuel de Tallinn a cependant des faiblesses notamment l'inadaptation du manuel pour les cyberattaques provenant des personnes privées pour lesquelles la preuve s'avère difficile.

B- Le vide juridique sur les attaques provenant des personnes privées et la preuve d'une cyberattaque

[121] *Ibidem*.
[122] Voir H. H. DINNISS, *Cyber Warfare and the Laws of War*, *Op. Cit*. p. 57.

[123] O. BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? » *Op. Cit*. p. 204 ;

[124] C'est notamment le point de vue du Professeur Huang Zhixiong de l'université de Wuhan.
[125] Il s'agit bien d'un manuel et non un code encore moins un instrument juridique international. De ce fait le Manuel de Tallin est un Guide sur la cyberdéfense au service des Etats et des décideurs politiques. Voir O. BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? » *Op. Cit*. p. 205.

[126] Voir note de bas de page n° 114.
[127] Voir G. CORNET, « Le Manuel de Tallin 2.0 ou comment le droit veut rattraper la technologie », 2017, disponible en ligne sur http://ultimaratio-blog.org/archives/8434 (consulté le 26 juin 2019).

Malgré sa richesse, le Manuel de Tallinn est inapplicable aux cybers opérations de faible intensité provenant des personnes privées. En effet, l'on conviendra volontiers qu'un Etat puisse ordonner à une personne physique d'attaquer un Etat pour son compte. Or, le plus souvent il est difficile d'établir le lien entre l'auteur d'une attaque et l'Etat donneur d'ordre. Ce qui semble logique car la principale caractéristique d'une bonne cyberattaque c'est l'anonymat de l'origine de l'attaque et de l'attaquant. De ce fait, le Manuel de Tallinn serait source d'incompréhension entre Etats quand l'Etat victime d'une cyber-opération chercherait à mettre en œuvre la légitime défense que consacre l'article 51 de la charte des Nations Unies. Une bonne cyberdéfense ne saurait donc se passer de la preuve qui reste un élément essentiel de la politique de cybersécurité[128]. De ce fait, le Manuel de Tallinn n'apporte pas toute la lumière nécessaire à une bonne appréhension des cyber-opérations. Contrairement à l'OTAN qui fait la promotion de la sécurité coopérative entre ses membres, les Nations Unies-berceau de la sécurité collective, semblent timide en matière de gouvernance de la cybersécurité.

Para 2 : L'absence de la cybersécurité dans les mécanismes de sécurité collective des Nations Unies

L'Organisation des Nations Unies consacre dans sa charte[129] le maintien et la consolidation de la paix et la sécurité dans le monde[130]. De ce fait, les Nations Unies se présentent comme l'organisation internationale par excellence chargé de

[128] Voir la définition de la cybersécurité de l'UIT précitée, qui mentionne l'exigence de la preuve dans une fiable politique de cybersécurité.

[129] La charte des Nations-Unies est disponible en ligne sur https://www.un.org/fr/sections/un-charter/chapter-i/ (consulté le 27juin 2019).

[130] Cf. article 1 de la Charte des Nations Unies.

la sécurité collective dans le monde et promoteur du droit international[131]. Cette sécurité collective passe aujourd'hui par le cyber et la cyberpaix est désormais un objectif des Nations Unies. Malheureusement, la vitesse de croissance des cyberattaques d'envergures internationales dépasse celle de la gouvernance du phénomène par les Nations Unies. Ce fait est lié à l'absence de convergence des points de vue des Etats sur la cybersécurité au sein des grandes instances onusiennes (A). Cependant à défaut de briller en cybersécurité à travers ses organes[132], les Nations Unies marquent des pas sûrs dans la gouvernance internationale de la cybersécurité à travers son organisme chargé de télécommunication (B).

A- Absence de convergence de points de vue des Etats sur la cybersécurité

Depuis que la Fédération de Russie a soumis à l'AG-NU une proposition de résolution sur la cybersécurité-intitulé « *les progrès de la téléinformatique dans le contexte de la sécurité internationale* » -en 1998[133], l'ONU s'est engagée à rassembler les points de vue des Etats autour d'un idéal sécuritaire en matière cyber[134]. Cet engagement s'est concrétisé par une commission d'information dont le rapport a été validé par l'AG-NU et suivi de différents rapports annuel qui sont présentés par le Secrétaire général de l'ONU. L'on n'oubliera pas les groupes de travail qui sont mis en place par le SG-NU pour avoir les positions des Etats et l'orientation que doit prendre la position officielle de l'ONU en matière de

[131] Voir F. MESTRE-LAFAY, « La contribution de l'ONU à l'évolution du droit international », L'Organisation des Nations-Unies, 2013, pp.51-52.

[132] Assemblée générale des Nations unies, Conseil de sécurité des Nations unies, Conseil économique et social des Nations unies (ECOSOC), Conseil de tutelle des Nations unies, Cour internationale de justice (CIJ), Secrétariat des Nations unies.

[133] Cette initiative peut être surprenante quand on prend en compte les soupçons médiatiques qui planent sur la Russie pour son implication dans les grandes cyberattaques qui ont secoué le monde ces dernières années.

[134] Voir https://www.un.org/disarmament/fr/informatique-et-telematique/ (consulté le 24 mai 2019).

cybersécurité[135]. Les Nations Unies restent donc dans un *brainstorming* alors que les cyberattaques sont devenu une menace collective de la communauté internationale. Ce manque d'élan des Nations Unies ne dépend pas de la mauvaise foi de ses organes mais des divergences de position des Etats sur l'encadrement juridique des cyberattaques par les Nations Unies[136]. En effet, certains Etats estiment que l'ONU ne doit pas se mêler de la cybersécurité qui relève de la sécurité nationale des Etats membres. D'autres encore pensent que chaque Etat doit développer sa propre architecture de cyberdéfense avant de penser à une cyberdéfense collective sous les auspices des Nations-Unies[137]. En l'absence d'une construction normative contraignante en cybersécurité, les Nations Unies sont plus actives dans la gouvernance internationale de la cybersécurité à travers l'UIT.

B-Un engagement embryonnaire des Nations Unies en cybersécurité à travers l'UIT

Comme son nom l'indique l'UIT est l'Agence du système des Nations Unies qui est chargé des télécommunications dans le monde. Il dispose d'un programme sur la cybersécurité dont l'utilité et l'efficacité n'est plus à démontrer. L'UIT est un grand réseau de fédération des acteurs de la télécommunication dans le monde. Elle compte 193 états membres et 700 membres et associés du secteur[138]. Fondée sur le principe de la coopération entre les Etats membres et le secteur privé, l'UIT dispose d'un programme sur la cybersécurité[139] qui offre des outils précieux, des informations essentielles, des éléments d'évaluation et une assistance technique en vue d'aider les membres de l'UIT, en particulier les pays en développement, à accroître leurs capacités en matière de cybersécurité et à instaurer la confiance

[135] Voir les différents rapports de ces groupes de travail dans les résolutions de l'AG-NU : A/RES/65/201 du 30 juillet 2010 ; A/RES/66/24 du 13 décembre 2011 et A/RES/68/98 du 24 juin 2013.

[136] *Ibidem*.

[137] Voir https://www.un.org/press/fr/2018/agdsi3613.doc.htm (consulté le 26 mai 2019).

[138] Voir le site internet de l'UIT à l'adresse https://www.itu.int/fr/about/pages/membership.aspx (consulté le 28 juin 2019).

[139] Ce programme a été lancé en 2007 par le Secrétaire général de l'UIT, Hamadoun I. Touré.

dans l'utilisation des Technologies de l'Information et de la Communication(TIC)[140]. Ce programme vient en appui aux programmes qui sont exécutés par les Etats sur le plan national et régional. De ce fait, l'UIT offre quantité d'outils et activités pour concrétiser le but de son programme cybersécurité. Il publie périodiquement l'Indice global de la cybersécurité dont la fiabilité est mondialement reconnue, effectue des cyberexercices pour préparer les Etats et les organisations à faire face aux cyberattaques. La sensibilisation sur la nécessité d'une législation harmonisée est un exercice permanent de l'UIT sans oublier la promotion d'un partenariat mondial entre les acteurs du cyber pour le partage d'information[141]. Se faisant l'UIT contribue efficacement à la gouvernance internationale d'Internet et ses risques. La Conférence mondiale des télécommunications (CMTI) qu'elle a organisé en décembre 2012 à Dubai[142] a ouvert une large fenêtre d'opportunités pour les revendications des pays en développement. L'UIT n'était pas à son premier sommet d'un rayonnement mondial sur les TIC. En effet, depuis le premier Sommet Mondial de la Société de l'Information (SMSI) qui a eu lieu à Genève du 10 au 12 décembre 2003 et la seconde qui s'est tenu à Tunis en 2005, l'UIT s'est engagé à harmonisé la gouvernance international des télécommunications en général et de l'internet en particulier[143]. Le SMSI de 2005 a été marqué par la création du Forum International de la Gouvernance de l'Internet[144] dont la treizième édition qui s'est tenu à Paris en novembre 2018 a été couronnée par l'Appel de Paris pour la

[140] Programme sur la cybersécurité de l'UIT disponible à l'adresse https://www.itu.int/fr/ITU-D/Cybersecurity/Pages/default.aspx (consulté le 28 juin 2019).
[141] Voir https://www.itu.int/fr/ITU-D/Cybersecurity/Pages/default.aspx (consulté le 28 juin 2019).
[142] L'objet de cette conférence fut la renégociation du Règlement des Télécommunication Internationale (RTI), traité qui régule les télécoms dans le monde, resté inchangé depuis 1988 et l'arrivée d'Internet dans le domaine public. Il convient de préciser que 55 pays dont la France ont refusé de signer le nouveau traité ; voir A. CATTARUZZA, D. DANET, S. TAILLAT, *La Cyberdéfense, Politique de l'espace numérique*, *Op. Cit*. p. 132.
[143] Voir https://www.itu.int/net/wsis/basic/about-fr.html (consulté le 28 juin 2019) ; A. SAMASSEKOU, « Le Sommet mondial sur la société de l'information », Hermès, La revue 2004/3 (n°40), p. 238-240, disponible aussi en ligne sur https://www.cairn.info/revue-hermes-la-revue-2004-3-page-238.htm (consulté le 28 juin 2019).

[144] Ce forum se veut une plateforme mondiale et multipartite de débat sur l'ensemble des questions de politique publique relatives à l'Internet.

confiance et la sécurité dans le cyberespace[145]. Ce texte n'a pas de valeur juridique contraignante mais reste un engagement de 66 Etats, 347 acteurs du secteur privé, 139 organisations, à travailler ensemble pour la sécurité et la confiance dans le cyberespace[146]. La gouvernance internationale de la cybersécurité ne se limite pas aux grandes instances internationales qui réunissent les Etats. Elle trouve aussi un écho favorable sur le plan régional.

SECTION 2 : UNE GOUVERNANCE DE LA CYBERSECURITE PLUS ELOQUENTE SUR LE PLAN REGIONAL

Face aux faiblesses de la mondialisation, certains Etats trouvent plus confiance dans la régionalisation[147]. Dans certains cas la mondialisation accouche de la régionalisation[148]. Cette dernière peut être efficace dans bien des domaines compte tenu de la facilité des discussions et de la communion des cultures entre Etats voisins. De ce fait l'on voit émergé une construction européenne en matière de gouvernance de la cybersécurité (paragraphe 1). De même d'autres régions telles que l'Afrique, l'Amérique ou la région des pays arabes s'organisent pour être à la page en matière de cybersécurité (paragraphe 2).

Para 1 : La fulgurante émergence de la cybersécurité dans la politique de sécurité de l'UE

[145] Voir le texte de l'Appel de Paris à l'adresse https://www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf (consulté le 28 juin 2019).

[146] Voir la liste des soutiens à l'Appel de Paris-actualisée le 15 mai 2019-sur https://www.diplomatie.gouv.fr/IMG/pdf/soutiens_appel_de_paris_15052019_cle0c6126.pdf (consulté le 28 juin 2019).

[147] La régionalisation est définie comme le fait par lequel un groupe de pays voisins transfère une partie de leurs pouvoirs administratifs, économiques et politiques à une entité supranationale fondée sur l'idée d'une région, entendue dans le sens continental donc fondée sur la proximité géographique. Voir T. KERNALEGENN, « Le régionaliste. Quelques pistes théoriques pour une approche cognitive », Civitas Europa 2017/1, pp. 59-62, disponible en ligne à l'adresse https://www.cairn.info/revue-civitas-europa-2017-1-page-59.htm (consulté le 30 juin 2019) ; F. NICOLAS, « Mondialisations et régionalisation dans les pays en développement-les deux faces de Janus », Politique étrangère 1997, pp. 293-296, disponible en ligne à l'adresse https://www.persee.fr/doc/polit_0032-342x_1997_num_62_2_4641 (consulté le 30 juin 2019).

[148] *Ibidem*.

L'Union européenne est un exemple parlant d'une véritable intégration régionale. Elle est une association politico-économique de 28 Etats européen[149]. Conformément à la Politique Etrangère et de Sécurité Commune[150] (PESC) devenu Politique de Défense et de Sécurité Commune[151] (PSDC). Ainsi face aux défis sécuritaires dans le cyber, l'UE n'a pas hésité à intervenir sur cette question en adoptant des mesures législatives et réglementaires (A). Dans la même dynamique une structure a été créée par l'UE pour coordonner la cybersécurité de l'institution européenne et celle des pays membres (B).

A-Un exemple réussi d'encadrement juridique de la cybersécurité sur le plan régional

L'UE n'a pas eu d'approche avant-gardiste en matière de cybersécurité. A l'instar de l'OTAN, c'est au début des années 2000 que l'UE a pris conscience de la nécessité de définir et de mettre en place une politique de cybersécurité pour protéger les systèmes d'information et les réseaux de ses institutions[152]. Ainsi dès qu'elle a perçu la dangerosité des cyberattaques elle s'est engagée dans l'encadrement du phénomène à travers ses propres mécanismes de gouvernance des risques qui menacent l'UE. Ainsi après de nombreuses improvisations, l'UE a lancé des réflexions sur la cybersécurité. La Direction « Sécurité, sûreté et systèmes d'information et de communication » du Conseil de l'Europe incarnait l'engagement de l'UE en matière de cybersécurité au cours de ses premières années de gouvernance de la cybersécurité[153]. Mais cet engagement était focalisé

[149] Le Royaume-Uni ne fera plus parti des 28 pays dans quelques mois après le referendum de sortie de l'Union européen qui a eu lieu le 23 juin 2016.
[150] La PESC était le deuxième des trois piliers de la construction européenne instauré en 1992 par le traité de Maastricht.
[151] La PSDC a remplacé la PESC à la suite des Traités d'Amsterdam et de Nice.
[152] V. JOUBERT, J-L SAMAAN, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », Hérodote, 2014, disponible en ligne à l'adresse https://www.cairn.info/revue-herodote-2014-1-page-261.htm?try_download=1 (consulté le 01 juillet 2019).
[153] Il convient de faire la distinction entre le Conseil de l'Europe et l'UE pour éviter toute confusion. Il s'agit de deux organisations distinctes Le premier est une organisation intergouvernementale créée en 1949 réunissant 47 Etats membres alors que l'UE est une association politico-économique suis generis qui regroupe 28 Etats européens qui sont tous membres du Conseil de l'Europe. Les deux organisations entretiennent d'étroites relations au point où près de 180 programmes ont été mis en œuvre entre les deux organisations européennes dans des domaines tels que les droits de l'homme, la culture de la démocratie et de l'Etat de droit. L'UE a tenté d'adhérer au Conseil de l'Europe sans succès mais la plupart des arrêts de la Cour de Justice de l'Union Européenne sont conformes aux instruments juridiques du Conseil de l'Europe notamment la Convention européenne des droits de l'homme.

sur la protection des infrastructures des institutions européennes[154]. Ce n'est qu'à partir de 2012 que l'UE s'est vraiment impliquée activement à la gouvernance de la cybersécurité des Etats membres. La compétence de l'UE se dégage de l'article 15 du Traité de Lisbonne, attribuant compétence partagée entre l'Union européenne et les Etats pour les réseaux transeuropéens[155]. Ainsi, pour ratisser large en matière de cybersécurité, l'UE lance des consultations nationales pour avoir les avis des Etats membres sur l'orientation de la Stratégie européenne de cybersécurité[156]. Cette dernière est adoptée par l'UE le 07 février 2013[157] et se décline en cinq grandes priorités que sont[158] :

- Parvenir à la cyber-résilience ;

-Faire reculer considérablement la cybercriminalité ;

-Développer une politique et des moyens de cyberdéfense liée à la PSDC ;

-Développer les ressources industrielles et technologiques en matière de cybersécurité ;

-Instaurer une politique internationale de l'UE cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'UE.

Pour mettre en œuvre la Stratégie européenne de cybersécurité l'UE adopta la directive relative la sécurité des réseaux et des systèmes d'informations (directive SRI)[159] en 2016[160]. L'adoption de cette directive marque un grand tournant dans la politique de cybersécurité de l'UE. En effet, la directive SRI fixe quatre grands axes à l'attention des 28 Etats européens. La directive prévoit d'abord le renforcement des capacités nationales de cybersécurité ; ensuite elle préconise

[154] V. JOUBERT, J-L SAMAAN, « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'OTAN et de l'UE », *Op. Cit*., (consulté le 1er juillet 2019).
[155] J.C. VIDELIN, « L'armée française et la cyberguerre », *in Annuaire du droit de la sécurité et de la défense 2018*, *Op. Cit*. p. 152-153.
[156] Voir O. KEMPF, « La cyberstratégie de l'Union européenne », Sécurité globale, 2013, disponible en ligne sur https://www.cairn.info/revue-securite-globale-2013-2-page-25.htm (consulté le 1er juillet 2019)
[157] La Stratégie européenne de cybersécurité est disponible en ligne sur http://register.consilium.europa.eu/pdf/fr/13/st06/st06225.fr13.pdf (consulté le 1er juillet 2019).
[158] *Ibid*. p. 5 ; voir aussi O. KEMPF, « La cyberstratégie de l'Union européenne », *Op. Cit*.
[159] La directive SRI est aussi appelée directive Network and Information Security ou « directive NIS ».
[160] Elle a été adoptée par le Conseil de l'UE en mai 2016 puis adopté par le parlement européen en juillet. Toutefois la date butoir de sa transposition au niveau national était en mai 2018.

l'établissement d'un cadre de coopération volontaire entre Etats membres ; en outres elle propose le renforcement par chaque Etat de la cybersécurité d' « opérateurs de service essentiels » au fonctionnement de la société et de l'économie ; enfin elle prévoit l'établissement de règles européennes communes en matière de cybersécurité des prestataires de services numériques dans les domaines du *cloud*, des moteurs de recherche et place de marché en ligne[161]. Si les Etats de l'UE restent obliger à l'égard des directives par rapport aux objectifs de celle ci, ils restent libres quant au choix des mesures d'application[162] de la directive[163]. Il en est autrement des règlements européens qui lient les Etats à la lettre. Ces derniers ont marqué la cybersécurité des Etats de l'UE ces derniers mois. L'UE a connu deux importants règlements sur la sécurité des données personnelles en l'espace de douze mois. Le premier est le RGPD et le second est le Règlement européen sur la cybersécurité. L'adoption du RGPD a été un coup de tonnerre dans le monde numérique dans la mesure où son l'article 3.2 consacre un champ d'application territorial « quasi-universel[164] ». Il convient d'émettre des doutes sur l'effectivité

---

[161] Voir https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/ (consulté le 01 juillet 2019) ; voir aussi M. QUEMENER, « La directive NIS, un texte majeur en matière de cybersécurité », Sécurité et stratégie, 2016, disponible en ligne sur https://www.cairn.info/revue-securite-et-strategie-2016-3-page-50.htm (consulté le 1er juillet 2019).

[162] Les mesures d'application sont encore appelé les mesures de transposition. Elles peuvent se faire de différentes manières soit par adoption de nouvelles mesures législatives ou règlementaires, soit en abrogeant les dispositions nationales qui sont contraires à la directive soit en les modifiant.

[163] Voir la valeur juridique de la directive européenne sur https://europa.eu/european-union/eu-law/legal-acts_fr (consulté le 06 juillet 2019). Voir aussi l'arrêt Van Duyn de la Cour de Justice de l'Union Européenne du 4 décembre 1974, l'arrêt du Conseil d'État français du 30 octobre 2009 (Mme Perreux) à propos de l'invocabilité de la directive européenne par les particuliers des Etats membres de l'UE si l'Etat membre n'a pas pris de mesures efficace pour transposition de la directive dans un délai raisonnable.

[164] Cf. article 3 du RGPD :

1. *Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.*

2. Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:

a)à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou

b)au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

de la mise en œuvre du RGPD au-delà des frontières de l'UE. D'ailleurs c'est par crainte de subir l'extraterritorialité du RGPD que les Etats-Unis adoptent dans une précipitation législative le *Cloud Act*. Un an après l'entrée en vigueur du RGPD, l'UE doit se familiariser avec un nouveau règlement sur la cybersécurité. En effet, le 12 mars 2019, le Parlement européen a adopté le *Cybersecurity Act*[165]. Ce règlement vise deux objectifs : la définition d'un cadre européen de certification de cybersécurité, essentiel pour renforcer la sécurité du marché unique numérique européen et l'adoption du mandat permanent de l'ENISA[166], l'Agence de l'Union européenne pour la sécurité des réseaux et de l'information.

B-Le rôle de l'ENISA en matière de cybersécurité: une gouvernance verticale de la cybersécurité

Créée le 13 mars 2004[167] et pleinement opérationnelle depuis le 1er septembre 2005, l'ENISA est l'Agence européenne de la cybersécurité. Elle aide l'UE, les Etats membres et leur démembrement à être mieux équipé et préparé pour prévenir et détecter les problèmes de sécurité de l'information et y répondre. L'ENISA incarne donc la gouvernance de la cybersécurité par l'UE. Son mandat a évolué au fil du temps. A sa création, l'Agence européenne de la cybersécurité était investit d'une mission limitée dans le temps. Son mandat a été renouvelé plus d'une fois notamment en 2008[168], 2011[169] en 2013[170] et récemment en 2019 avec l'adoption du règlement européen de la cybersécurité qui donne à l'ENISA un

---

3. Le présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.

[165] Cf. Règlement UE 2019/881 du Parlement européen et du Conseil du 17 avril 2019.
[166] European Union Agency for Network and Information Security.
[167] Voir Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'ENISA disponible en ligne sur https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:FR:HTML (consulté le 01 juillet 2019).
[168] Cf. Règlement CE1007/ 2008 du Parlement européen et du Conseil du 24 septembre.
[169] Cf. Règlement (UE) no 580/2011 du Parlement européen et du Conseil.
[170] Cf . Règlement (UE) no 526/2013 qui a prorogé le mandat de l'ENISA jusqu'au 19 juin 2020.

mandat permanent[171]. En dehors de ses activités de conseil, l'ENISA disposait jusqu'ici d'une compétence opérationnelle précaire. Elle édifiait les capacités des bénéficiaires[172] de ses actions en organisant régulièrement des formations et des exercices de cyber-résistance[173]. Le règlement sur la cybersécurité vient renforcer les compétences de l'ENISA en lui dotant des moyens financiers et techniques conséquents pour faire face aux cybermenaces de l'UE[174]. Ce règlement prévoit aussi une consultation accrue du secteur privé dans la gouvernance de la cybersécurité européen. La gouvernance actuelle semble se faire dans un seul sens et de façon verticale entre l'ENISA et les Etats membres.

En dehors de l'Union européenne, d'autres régions du globe s'engagent aussi activement dans la gouvernance de la cybersécurité.

Para 2 : La tendance générale vers une régionalisation de la cybersécurité

En attendant de trouver des solutions mondiales en matière de cybersécurité, les Etats s'activent dans leurs regroupements régionaux. Ainsi, différents cas de régionalisation de la gouvernance de la cybersécurité méritent d'être étudiés (A). Cette tendance à la régionalisation est fondée sur la recherche d'une confiance numérique et la stratégie culturelle des Etats (B).

A- La récurrente régionalisation de la gouvernance de la cybersécurité

[171] Voir le texte du règlement UE 2019/881 du Parlement européen et du Conseil du 17 avril 2019 disponible en ligne sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.FRA&toc=OJ:L:2019:151:TOC (consulté le 02 juillet 2019). Voir aussi l'Avis de l'ANSSI à propos de l'adoption du règlement UE 2019/ 881 à l'adresse https://www.ssi.gouv.fr/actualite/adoption-definitive-du-cybersecurity-act-un-succes-pour-lautonomie-strategique-europeenne/ (consulté le 02 juillet 2019).
[172] Institutions européennes, Etats, entreprises, …
[173] Il s'agit des exercices de « Hacking étique» c'est-à-dire un piratage à des fins probatoires et de test.
[174] Voir l'article 19 du règlement UE 2019/881 du Parlement européen et du Conseil du 17 avril 2019.

A l'instar de l'Union européenne, l'Union africaine (UA) a compris les enjeux de la cybersécurité et la nécessité pour chaque Etat membre et l'Union dans son ensemble de développer des politiques et mécanismes efficaces pour luter contre les cyberattaques et leurs conséquences sur la vie des acteurs et les usagers de l'internet. Ainsi, le 27juin 2014, l'UA adopte sa Convention sur la cybersécurité et la protection des données à caractère personnels[175]. Cette dernière se propose de résoudre les défis sécuritaires que les pays africains rencontrent sur internet à savoir les cyberattaques *stricto sensu*[176], le crime organisé[177] et la cyberescroquerie. Cette dernière a pris une dimension inquiétante en Afrique de l'ouest notamment au Nigéria et en Côte d'Ivoire comme les deux grands pôles de délinquance informatique[178]. Il convient de relever que la cybersécurité est encore à l'étape embryonnaire dans les pays africains qui sont plus préoccupés par la connectivité de leurs Etats[179]. Une prise de conscience des enjeux de sécurisation des infrastructures numérique à l'étape de construction des réseaux africains serait un bon début pour ses pays car cela éviterait de se retrouver dans la situation des pays européens qui ont développé le réseau internet avant de prendre conscience de la nécessité de les sécuriser.

En dehors de l'UA, les Etats américains s'unissent autour de différents accords de gouvernance du cyberespace. Les Etats-Unis s'affirment là aussi comme la locomotive du cyber. En Asie, les Etats arabes ont posé les bases de leur engagement en cybersécurité le 21 février 2008 pour lutter contre les cyberattaques et éradiquer la criminalité[180]. La tendance des Etats à régionaliser la cybersécurité

---

[175] Disponible en ligne sur https://www.afapdp.org/wp-content/uploads/2018/06/CONV-UA-CYBER-PDP-2014.pdf (consulté le 11 juillet 2019).

[176] Atteinte à l'intégrité physique et ou fonctionnel d'un système informatique.

[177] Cf. préambule de la Convention de l'UA sur la cybersécurité disponible en ligne sur https://www.afapdp.org/wp-content/uploads/2018/06/CONV-UA-CYBER-PDP-2014.pdf (consulté le 11 juillet 2019).

[178] Le phénomène est généralement connu sous le nom de « broutage » ou « l'arnaque à la nigériane ».

[179] Voir l'indice global de cybersécurité de l'UIT sur le site de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (consulté le 11 juillet 2019); voir aussi O. ZAKARIA, « Palmarès africain de la cybersécurité », in *La Tribune Afrique*, janvier-février 2019, p. 50-51.

[180] Voir https://news.un.org/fr/story/2008/02/126402-nouvelles-technologies-les-pays-arabes-adoptent-la-declaration-de-doha-sur-la (consulté le 12 juillet 2019) ; voir aussi L. Le BARREAU, E. LONGEON, « Les enjeux de cybersécurité en Arabie saoudite », Etudes internationales, septembre 2016, p. 161.

est justifiée par la recherche d'une confiance numérique et l'identité stratégique culturelle[181]

B- Une tendance justifiée par la recherche d'une confiance numérique et l'efficacité du bon voisinage

La gouvernance internationale de la cybersécurité pose la question de la confiance numérique. Cette confiance est recherchée à la fois au plan interne entre les acteurs de la cybersécurité et au plan international entre les Etats, les organisations et les grandes entités privés du monde numérique. Le recours des Etats à la régionalisation de la cybersécurité prouve l'existence d'une confiance entre les Etats au plan régional en raison de l'identité stratégique culturelle des Etats en matière sécuritaire[182]. La culture stratégique est un outil de compréhension des postures étatiques ; il repose sur la compréhension des particularités nationales stratégique historiquement fondées[183]. Le Professeur Colin GRAY l'envisage comme étant : « *basé sur l'auto-appréciation d'une expérience historique et du caractère national. [...] Telle qu'il l'envisage, la culture stratégique est un mélange d'histoire, de géographie, de philosophie politique, de culture civique. En fait, Gray présuppose l'existence de cultures stratégiques distinctes. Il les considère comme un environnement qui influence la prise de décision*[184] ». La régionalisation de la cybersécurité est donc le fruit d'un passé commun et d'une culture commune unissant les Etats et les peuples issues d'une même zone géographique. Cette régionalisation résulte souvent de la volonté politique des Etats. Or, la gouvernance de la cybersécurité-à la différence des opérations militaires des siècles précédents –n'est pas l'apanage des gouvernements ni des armées régulières. Ceux-ci ne sont qu'un acteur parmi tant d'autre : du simple

[181] L. Le BARREAU, E. LONGEON, « Les enjeux de cybersécurité en Arabie saoudite », *Op. Cit*. p. 161-162.
[182] *Ibidem.*
[183] *Ibidem*, p. 161 ; voir aussi C. WASINSKI, *La culture stratégique: Evaluation d'un concept et de ses ramifications en relations internationales*, les cahiers du RMES, 2006, p.118.
[184] *Ibid*. pp. 123-124.

particulier aux organisations de dimensions mondiales[185]. Au rang de ces organisations l'ICANN occupe une place de choix et mérite d'être connu[186].

SECTION 3 : DE LA CREATION DE L'ICANN A L'EMERGENCE D'UN SOFT LAW EN CYBERSECURITE

En matière de gouvernance de l'internet, l'ICANN est une organisation cosmopolite aux missions pertinentes (Paragraphe 1). Ses actions aboutissent à l'émergence d'un *soft-law* dans la gouvernance de l'internet (Paragraphe 2).

Para 1 : l'ICANN, une organisation cosmopolite aux missions pertinentes

La contribution de l'ICANN à la gouvernance de l'internet fait appel à différentes structures parallèles. En effet, les acteurs qui concourent au bon fonctionnement de l'ICANN sont diversifiés (B) et les missions de l'organisation sont fondamentalement techniques mais aussi sécuritaires (A). Toutefois l'ICANN est une organisation internationale privée inféodées à l'administration américaine (C). Ce qui soulève de plus en plus la contestation de son fonctionnement[187].

A- Les missions techniques et sécuritaires de l'ICANN

L'ICANN est une organisation à but non lucratif de droit californien (Etats-Unis) et reconnue d'utilité publique rassemblant des participants du monde entier qui œuvrent à la préservation de la sécurité, la stabilité et l'interopérabilité de

[185] N. ARPAGIAN, *La cybersécurité*, *Op. Cit*. p. 74.
[186] P. JACOB, « La gouvernance de l'internet du point de vue du droit international public », *in Annuaire Français de droit international LVI*, Paris, CNRS Editions, 2010, p.551.

[187] A. CATTARUZA, D. DANET, *La Cyberdéfense : quel territoire, quel droit, Op. Cit*. p.85.

l'Internet[188]. Elle est au centre de la gouvernance des aspects techniques de l'internet d'autant plus qu'elle régule le fonctionnement même de l'internet. Par exemple pour contacter une personne sur internet, il faut saisir un identifiant sur son ordinateur qui à son tour dispose d'une adresse appelée « adresse IP[189] » et l'ICANN veille à ce que ces identifications soient uniques pour éviter les doublons et le plantage[190]. Cette supervision du réseau internet gigantesque et complexe d'identifications uniques qui permettent aux ordinateurs de se reconnaitre s'appelle la « résolvabilité universelle »[191]. L'identification des sites internet pose la problématique des noms de domaines[192] (NDD) dont la gestion est assurée par l'ICANN[193]. L'ICANN est donc au cœur de l'informatique. Eu égard à ces grandes missions techniques que mènent l'ICANN il y va de soit qu'elle s'engage fortement dans la cybersécurité pour protéger ses propres infrastructures numériques et protéger le système dans sa globalité car s'attaquer à l'ICANN c'est s'attaquer à la racine même de l'internet. Le fonctionnement de l'ICANN est parsemé d'un ensemble d'acteurs de qualité différente qui tourne autour de l'institution californienne[194].

B- L'ICANN, une organisation aux acteurs diversifiés

L'ICANN est constituée de plusieurs groupes distincts représentants chacun un intérêt différent sur Internet et participant aux décisions prises par l'ICANN[195]. Cette gouvernance participative répond aux caractéristiques d'Internet qui est un

---

[188] Voir la description de l'ICANN sur le site web de l'organisation sur https://www.icann.org/fr (consulté le 03 juillet 2019) ; Voir aussi N. ARPAGIAN, *La cybersécurité, Op.Cit.* p.87.

[189] IP ou « Internet Protocol » est un numéro d'identification unique qui permet d'identifié chaque périphérique relié à un réseau informatique.

[190] Voir https://www.icann.org/resources/pages/what-2012-02-25-fr (consulté le 04 juillet 2019). Voir aussi J. GRIMMELMANN, *Internet Law : cases ans problems, Op. Cit*. pp. 388-390.

[191] *Ibidem.*

[192]Un domaine est un ensemble d'ordinateurs reliés à Internet et composant une caractéristique commune. Par exemple : «.fr », « .org », « .net » sont des noms de domaines reliés à des Etats ou des entités privés. Les noms de domaines forment le système de noms de domaine (DNS).

[193] Voir https://www.icann.org/resources/pages/what-2012-02-25-fr (consulté le 04 juillet 2019).

[194] O. ITEANU, « L'ICANN un exemple de gouvernance originale ou un cas de law intelligence ? Les cahiers du numérique », 2002 vol.3, disponible en ligne sur https://www.cairn.info/revue-les-cahiers-du-numerique-2002-2-page-145.htm (consulté le 08 juillet 2019).

[195] *Ibidem*.

bien commun[196] et bénéficiant du régime de la coproduction du bien public[197]. Cette coproduction du bien publique s'affirme de plus en plus dans de nombreux domaine dans la vie des Etats. Il en est ainsi de la sécurité intérieure où on parle de plus en plus de l'émergence de la police de proximité[198]. Ainsi, l'hétérogénéité structurelle de l'ICANN se présente sous la forme d'un chœur à deux voix: d'abord les organisations de soutien à l'ICANN ensuite les organisations consultatives. Les organisations de soutien à l'ICANN sont au nombre de trois regroupant les organisations qui gèrent les adresses IP, les organisations qui gèrent les noms de domaine[199], les responsables des domaines nationaux de premier niveau[200]. Ensuite il y'a quatre organisations consultatives qui fournissent conseils et recommandations à l'ICANN. Ces organisations consultatives représentent les gouvernements et les organisations de traités internationales telles que l'UIT, les opérateurs de serveurs racines, toutes les organisations qui œuvrent pour la sécurité sur internet, et enfin la communauté « dans son ensemble » c'est-à-dire les utilisateurs d'Internet standard. Il convient de relever aussi le groupe de liaison technique qui travaille avec les organisations chargées de concevoir les protocoles de bases pour les technologies Internet[201]. Cette description de « l'univers ICANN » ou « système ICANN » qui parait complexe[202] démontre que l'institution californienne qui est de droit privé, fédère autour d'elle des acteurs étatiques et non étatiques. Le rôle des acteurs étatiques est ici différent de leur rôle sur la scène

[196] Voir C. MABI et F. MASSIT-FOLLEA, « La gouvernance des biens communs: du climat à Internet, premières leçons d'une comparaison », 2013, disponible en ligne sur https://journals.openedition.org/communication/4403 (consulté le 04 juillet 2019) ; voir aussi O. ITEANU, « L'ICANN un exemple de gouvernance originale ou un cas de law intelligence ? Les cahiers du numérique », *Op. Cit*.

[197] La coproduction du bien public est un concept de la gouvernance qui est axé sur l'implication de tous les acteurs de la société à la construction du bien public. Voir S. BELLINA, C. LAUNAY-GAMA, Michel SAUQUET, M. VIELAJUS, *Les chroniques de la gouvernance 2009 -2010*, Editions Charles-Léopard MAYER, pp .108-112 ;

[198] Y. EMERY et Julien NIKLAUS, « La coproduction dans les prestations relevant de puissance publique. L'exemple de la police de proximité en Suisse », Management et Avenir, 2015, disponible en ligne à l'adresse https://cairn.info/revue-management-et-avenir-2015-2-page-37.htm (consulté le 05 juillet 2019).

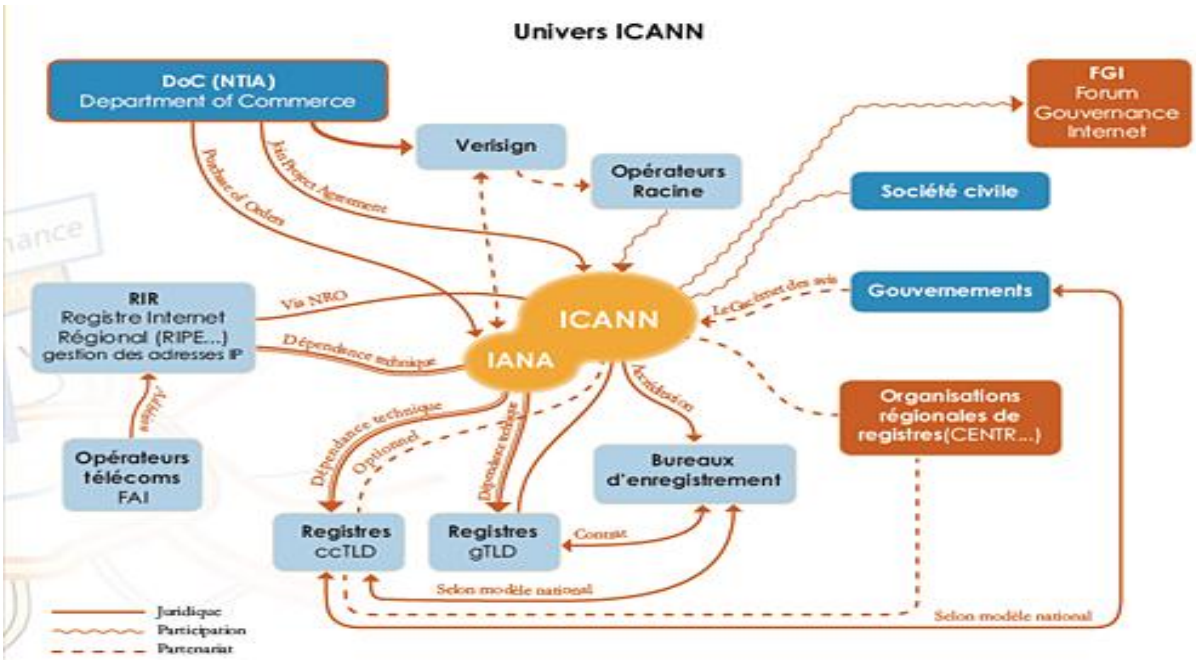
[199] Il s'agit principalement de l'Internet Assigned Numbers Authority (IANA) un département technique de l'ICANN.

[200] Les noms de domaines de premier niveau sont par exemple [.com], [.fr], [.org], [.tg].

[201] Cf. la description de l'ICANN à l'adresse https://www.icann.org/resources/pages/what-2012-02-25-fr (consulté le 05 juillet) ; voir aussi https://www.amenschool.fr/quest-ce-que-licann/ (consulté le 05 juillet 2019).

[202] Pour plus d'éclaircissement sur le système ICANN et ses organismes partenaires voir N. ADAM, L'ICANN et la gouvernance d'internet : une histoire organisationnelle, Cahier de recherche, 2007, pp. 7-12, disponible en ligne sur http://www.ieim.uqam.ca/IMG/pdf/AdamN_ICANN-FINAL-2007.pdf (consulté le 08 juillet 2019).

internationale où tout tourne autour des intérêts des Etats dans une dynamique westphalienne[203]. L'ICANN marque donc une exception car en matière de gouvernance technique d'Internet elle est en position de leader et non de suiveur. Cette influence de l'ICANN est comparable au rôle de la Fédération internationale de football association (FIFA) dans la *lex sportiva* par rapport aux mesures de dopage[204]où les mesures prises par la FIFA-organisation de droit privé- s'appliquent aux Etats.



Source : http://www.afnic.fr/medias/documents/afnic-dossier-gouvernance-internet-06-2008.pdf

C- Une institution inféodée à l'administration américaine

[203] Les traités de Westphalie signés le 24 octobre 1648 érige l'Etat-nation comme socle du droit international ; Voir B. QUENAULT, « Dilemme westphalien et gouvernance des biens publics mondiaux : le cas de la protection du climat », Mondes en développement, 2013, disponible en ligne sur https://cairn.info/revue-mondes-en-developpement-2013-2-page-11.htm (consulté le 05 juillet 2019) ; voir aussi O. ITEANU, « L'Icann un exemple de gouvernance originale ou un cas de law intelligence ? Les cahiers du numérique », *Op. Cit.*

[204] Voir F. LATTY, « La gestion internationale du football, un service public international », in *Droit(s) du football*, M. TOUZEIL-DIVINA, MAISONNEUE, Editions L'épitoge –Lextenso, pp. 22-26.

Tel qu'énoncé plus haut, l'ICANN est une organisation privé de droit californien. De ce fait l'institution de réglementation d'Internet reste soumise à l'administration et aux lois américaines[205]. La plupart des organismes et associations affiliées à l'ICANN sont localisées sur le territoire américain. Ce qui est une aberration venant d'une organisation à vocation mondiale[206]. Rappelons que pendant longtemps l'ICANN est restée sous la tutelle directe du ministère américain du commerce. De ce fait, les contestataires de l'influence américaine sur l'ICANN demandent que l'ICANN soit mise sous la tutelle des Nations-Unies pour qu'elle devienne une organisation internationale onusienne. Le gouvernement américain s'y est farouchement opposé mais l'ICANN semble s'affranchir de cette tutelle depuis le 1er octobre 2016 où un nouveau modèle de gouvernance voit le jour[207]. Ce nouveau modèle de gouvernance est axé sur un modèle multipartite de gouvernance dans lequel une assemblée générale[208] voit le jour aux cotés du conseil d'administration de l'ICANN qui a longtemps gouverné seul. Cette assemblée générale peut, si elle a le consensus de ses membres, opposer son véto aux décisions du conseil d'administration de l'ICANN[209]. Cette révolution de l'ICANN est le fruit d'une longue contestation des autres Etats[210] et organisations qui voient la main mise de l'Etat américain comme une violation de leur souveraineté. Cette prétention est justifiée par les nombreux enjeux géopolitiques de l'internet. Cependant, l'indépendance réelle de l'ICANN réside dans la mise en œuvre de ses nouveaux mécanismes de gouvernance.

---

[205] P. JACOB, « La gouvernance de l'internet du point de vue du droit international public », *in Annuaire Français de droit international LVI*, Paris, CNRS Editions, 2010, p.552-553.

[206] A. CATTARUZZA, D. DANET, *La cyberdéfense : quel territoire, quel droit, Op. Cit*. p. 86 ; voir aussi

[207] Voir http://ipzen.com/fr/licann-est-enfin-independante/ (consulté le 08 juillet 2019) ; voir aussi http://www.iredic.fr/2016/11/21/licann-et-le-gouvernement-americain-cest-fini/ (consulté le 08 juillet 2019).

[208] La nouvelle Assemblée générale de l'ICANN est constituée de quatre collèges : le secteur privé qui réunit des acteurs comme les GAFAM et les grandes entreprises, la communauté technique, les gouvernements composé de 160 membres, la société civile réunissant les associations de consommateurs et de défense des libertés ; voir N. DREYFUS, « L'ICANN enfin émancipée du gouvernement américain ! », 2017, disponible en ligne sur https://www.village-justice.com/articles/ICANN-enfin-emancipee-gouvernement-americain,24164.html (consulté le 08 juillet 2019).

[209] *Ibidem*.

[210] La Chine, la Russie et la France sont les principales contestataires de l'influence américaine sur l'ICANN.

Para2 : L'émergence des mécanismes de soft law en cybersécurité : Appels, Code de bonnes pratiques, guides …

La gestion d'Internet et ses risques dans le cadre de la cybersécurité, est confrontée par leurs impossibilités d'être gouverné par une seule entité. De ce fait, là où la loi[211] manque de force ou est en pratique inexistante, l'on voit émergé des mécanismes alternatifs d'encadrement de l'action des acteurs de la cybersécurité pour une convergence de la lutte contre les cyber-menaces. Ces mécanismes alternatifs que d'aucuns qualifient de *soft law*[212] se présente sous la forme d'appels, code de bonne conduite, engagement au sens du droit international ou gentlemen's agreement[213] et émanent de toutes les parties prenantes de la cybersécurité sur le plan international individuellement ou collectivement. Il en est ainsi de l'Appel de Paris pour la confiance et la sécurité numérique du 12 novembre 2018[214]. Un tel appel est dépourvu de tout effet juridique mais il engage moralement ses signataires qui sont amenés à faire une prestation pour avoir mis en jeu leur honneur. Le texte de l'Appel a été rédigé par l'Etat français et soumis à la signature des autres Etats. De ce fait, la France se présente comme le promoteur de l'Appel de Paris et à ce titre il doit donner le bon exemple aux autres Etats en les

[211] Entendu comme l'ensemble des règles juridiques dont la violation implique une sanction juridique.

[212] Le dictionnaire du droit international publié sous la direction de Jean Salmon nous livre les éléments suivants de définition : le *soft law* serait l'expression par laquelle nous désignerions « des règles dont la valeur normative serait limitée soit parce que les instruments qui les contiennent ne seraient pas juridiquement obligatoires, soit parce que les dispositions en cause, bien que figurant dans un instrument contraignant, ne créeraient pas d'obligation de droit positif, ou ne créeraient que des obligations peu contraignantes » ; voir J. CAZALA, « Le Soft Law international entre inspiration et aspiration », Revue interdisciplinaire d'études juridiques, 2011/1 vol.66, disponible en ligne sur https://www.cairn.info/revue-interdisciplinaire-d-etudes-juridiques-2011-1-page-41.htm (consulté le 09 juillet 2019).

[213] Il s'agit d'Accords ou engagements international engageant moralement leurs signataires-des personnes publiques ou privées-et dépourvu de force juridique ; de nombreux chercheurs ont écrit sur la notion de gentlemen's agreement et sa valeur dans l'ordre juridique des Etats ; voir R. COTE, « Les gentlemen's agreement à l'ère technologique », Mc GILL Law journal, disponible en ligne sur http://lawjournal.mcgill.ca/userfiles/other/7573843-Cote.pdf (consulté le 11 juillet 2019) ; D. CARREAU, F. MARRELLA, « Les engagements non contraignants entre Etats, le droit international *flexible* et *soft law » in Droit international*, 11ème édition disponible en ligne sur http://pedone.info/di/Carreau-Marrella_Chap6.pdf (consulté le 11 juillet 2019) ; P. DMOCHOWSKY, « *soft law* internationale » validité et autorité de l'*instumentum* », 2009, Tome 2, pp. 221-225, disponible en ligne sur http://www.softlawinternationale.net/download/tom_2.pdf (consulté le 11 juillet 2019).

[214] Voir https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la (consulté le 11 juillet 2019).

incitants à s'engager dans la dynamique de l'Appel lancé et signé par eux. Partant de ce constat, le *soft law* a donc une fonction d'orientation des choix politiques de ses destinataires[215]. Aussi dans le fonctionnement des entités privées de promotion de la sécurité informatique telle que l'ICANN et ses structures affiliées[216] l'on voit naitre un *soft law* qui prend forme sur le plan international. Ces mesures peuvent être sous la forme de résolutions de l'ICANN ou les bonnes pratiques de cybersécurité que l'institution californienne vulgarise à travers ses formations et sensibilisations dans le monde entier[217].

[215] Voir A. FLÜCKIGER, « Pourquoi respectons-nous la *soft law* ? », 2009, disponible sur https://journals.openedition.org/ress/68 (consulté le 11 juillet 2019).
[216] Voir l'ICANN et ses structures affiliées sur le tableau indexé plus haut « Univers ICANN ».
[217] Voir https://www.icann.org/news/blog/diffusion-des-connaissances-en-2014-formation-technique-avec-le-nsrc (consulté le 11 juillet 2019).

PARTIE II

DU CARACTERE POURTANT CONSOLIDABLE DE LA GOUVERNANCE INTERNATIONALE DE LA CYBERSECURITE

La recrudescence des cybermenaces ne laissent aucun acteur du cyberespace indifférent et tous s'accorde à l'idée de réglementer les activités humaines dans le cyberespace. Cette réglementation mérite de se faire à différent niveau notamment sur le plan juridique, organisationnel, technique militaire…. Il est donc nécessaire de renforcer la gouvernance internationale de la cybersécurité (**chapitre 1**). A ce propos de nombreuses actions sont menées à différents niveaux et laissent penser que l'ont s'achemine vers une réelle gouvernance de la cybersécurité (**chapitre 2**).

CHAPITRE 1

LA NECESSITE D'UNE GOUVERNANCE INTERNATIONALE RENFORCEE DE LA CYBERSECURITE

La globalité des risques informatiques impose à la communauté des utilisateurs d'Internet de repenser ou plutôt de renforcer la gouvernance de la cybersécurité sur le plan international. Ce renforcement de la gouvernance de la cybersécurité s'impose d'autant plus qu'une cybersécurité efficace ne peut être instauré dans un repli sur soi. Même les cyberpuissances font l'objet de cyberattaques d'origine étrangère ce qui conforte l'institutionnalisation de mécanismes internationaux de prévention et d'action contre les cyberattaques. Cette nécessité d'une gouvernance renforcée est le pendant de la souveraineté numérique. Elle permettra de pallier les failles de sécurité informatique en fédérant le génie de chaque acteur du cyber sur le plan international. Pour ce faire, il est nécessaire d'instaurer une gouvernance internationale centralisée de la cybersécurité (section 2). Mais il serait judicieux de consolider d'abord les acquis actuels de la gouvernance de la cybersécurité (section 1).

SECTION 1: LES RAISONS D'UN RENFORCEMENT DE LA GOUVERNANCE INTERNATIONALE DE LA CYBERSECURITE

Face à la recrudescence des cyberattaques dans le monde, il est devenu impérieux pour les acteurs du cyberespace de renforcer les piliers d'une lutte globalisée. Pour se faire la coopération entre les principaux acteurs de la cybersécurité sur le plan international mérite d'être renforcée (paragraphe 1). Il urge aussi de reconsidérer le rôle des acteurs privés dans la mise en place d'une cyberrélisience efficace (paragraphe 2).

Para 1 : Le renforcement de la coopération entre acteurs de la cybersécurité

La base d'une cybersécurité collective sur plan international réside dans l'uniformisation de la définition de la cybersécurité sur le plan international (A).

En effet, tous les acteurs de la cybersécurité doivent s'entendre sur un idéal commun avant de penser à sa réalisation. Partant de cet idéal commun, une coopération autour de la cybersécurité peut être mise en place entre les acteurs du cyberespace (B).

A. L'uniformisation de la définition de la cybersécurité sur le plan international

Dans de nombreux ouvrages sur la cybersécurité, le concept de cybersécurité n'est pas défini. Les chercheurs se contentent de l'expliquer littéralement. Mais sur le plan international l'UIT reste et demeure à ce jour l'organisation fédérative qui a proposé une définition sur la cybersécurité. Cette définition ne jouit pas d'une acceptation universelle en raison de nombreux facteurs. D'abord elle procède en une définition en plusieurs temps-ce qui nécessite une interprétation de cette définition-, en plus la définition de la cybersécurité de l'UIT est citée dans une recommandation de ladite institution[218]. Ce qui ne facilite pas l'obligatoriété de la définition en raison du caractère non contraignant d'une recommandation en général et celle d'une organisation internationale en particulier[219]. De ce fait, l'on assiste à une définition subjective de la cybersécurité par chaque acteur de la cybersécurité en commençant par les Etats. Partant de ce constat, il importe d'uniformiser la définition de la cybersécurité sur le plan international ou renforcer la définition qui existe déjà par les soins de l'UIT. Cette uniformisation de la définition de la cybersécurité est plus qu'une nécessité d'autant plus que c'est la base d'une lutte commune pour l'instauration d'une cybersécurité efficace dans le monde. A titre d'exemple, la Russie a une vision plus politique de la cybersécurité que la France ou les Etats Unis. La politique russe de cybersécurité touche parfois

[218] Cf. recommandation UIT-T X.1205 portant présentation générale de la cybersécurité de l'UIT.

[219] La valeur juridique des recommandations des organisations internationales a fait l'objet de nombreuses recherches. Pour plus de précisions voir M. VIRALLY, « La valeur juridique des recommandations des organisations internationales », Annuaire français de droit international, 1956/2, pp. 66-71 ; D. CARREAU, F. MARRELLA, « Les actes unilatéraux des organisations internationales », in *Droit international*, 11ème édition, Pedone, 2012, pp. 265-267.

la sécurité de l'information et a pour finalité de lutter contre l'activisme politique hostile au régime sur les réseaux sociaux. Une telle vision n'est pas forcement partagée par les autres Etats[220]qui redoutent une violation de la liberté d'expression. Cet écart de vision sur la cybersécurité est la manifestation des enjeux géopolitiques des Etats autour du cyber[221]. C'est donc à partir d'une vision commune sur la cybersécurité que les acteurs du cyberespace pourront construire une cybersécurité efficace (B).

B. La mise en place de mécanismes internationaux de construction d'une cybersécurité

Rappelons d'emblée qu'il n'existe pas un instrument juridique universel réunissant les acteurs du cyberespace dans le monde. Les quelques instruments qui existent sont d'ordre régional et ceux qui ont une finalité mondiale n'ont aucune portée juridique dans la mesure où il s'agit le plus souvent des recommandations, des appels ….. Il est donc nécessaire de rassembler les acteurs de la cybersécurité autour d'un cadre juridique international. Partant de l'idée selon laquelle la cybersécurité procède de la réunion de différents mécanismes-à savoir la construction d'une sécurité des systèmes d'information[222], la mise en place d'une cyberdéfense, et la lutte contre la cybercriminalité[223]-, un instrument juridique international mettant en lumière les trois aspects de la cybersécurité méritent d'être adopté par la communauté des utilisateurs du web. Concernant la lutte contre la criminalité, l'on pourrait s'inspirer du modèle que prévoit déjà la Convention du

[220] C'est le cas de la France qui a pendant longtemps exclu la « sécurité de l'information » de sa cybersécurité ; voir https://www.diplomatie.gouv.fr/IMG/pdf/190513_-_reponse_de_la_france_aux_resolutions_73-27_et_73-266_fr_cle893713.pdf (consulté le 03 aout 2019). Toutefois l'adoption de la loi « *fakenews* » par le parlement français en 2018 laisse une porte ouverte pour que la sécurité de l'information s'invite dans les mécanismes de cybersécurité français.

[221] R. N. GOMEZ, « Cybergéopolitique : de l'utilité des cybermenaces », in *Cyberespace enjeux géopolitiques*, Hérodote, 2014, 98-104.

[222] La sécurité des systèmes d'information est le volet préventif de la cybersécurité et relève de l'action quotidienne de la cyber-résilience.

[223] Voir Marc WATTIN ANGOUARD, « Cybermenaces et sécurité nationale », in *Le droit de la sécurité et de la défense en 2013*, *Op. Cit*. p. 300-301.

Conseil d'Europe sur la cybercriminalité de 2001. Cette convention qui a certes connu des ratifications en dehors de l'Europe n'est pas une convention à portée universelle ; elle reste une convention européenne, ce qui ne facilite pas sa large ratification. Cette construction peut aussi procéder de l'adoption de trois instruments juridiques distincts. Dans tous les cas, la nécessité d'adapter le droit aux exigences de la cybersécurité s'impose. Un ordre public sur le cyberespace mérite d'être érigé sur le plan international à l'instar de la consécration de l'ordre public des mers et océans par la Convention des Nations Unies sur le droit de la mer de Montego Bay de 1982[224]. Cet ordre public permettra d'autoriser, d'obliger, d'interdire, d'encadrer, et de réguler les activités de l'Homme dans le cyberespace[225].

Le renforcement de la cybersécurité sur le plan international passera aussi par la reconsidération du rôle des acteurs privés en commençant par la sensibilisation de l'internaute *lambda* aux règles de sécurité informatique.

Para 2 : De la reconsidération à l'institutionnalisation du rôle des acteurs privés dans la cyber-résilience

L'Etat ne peut plus garantir seul, sur la toile, la tranquillité publique, la sécurité des personnes et des biens. S'il doit pour rester souverain, en assurer la stratégie et la gouvernance, il partage néanmoins leur mise en œuvre avec des partenaires privés responsables (B) et surtout les citoyens qui restent et demeurent le maillon essentiel d'une cybersécurité globale[226] (A).

---

[224] *Ibid*. p. 307.
[225] *Ibidem* ; Cf Appel de Paris pour la Confiance et la sécurité dans le cyberespace disponible en ligne sur https://www.diplomatie.gouv.fr/IMG/pdf/texte_appel_de_paris_-_fr_cle0d3c69.pdf (consulté le 26 juillet 2019).
[226] M. QUEMENER, A. SOUVIRA, « Cybersécurité et entreprises : se protéger juridiquement et se former », Sécurité et stratégie, 2012/4, (11), pp. 87-89, disponible en ligne sur https://www.cairn.info/revue-securite-et-strategie-2012-4-page-86.htm (consulté le 26 juillet 2019).

A- De l'importance du facteur humain dans la cybersécurité

D'après le Digital report 2019, réalisé par *We Are Social et Hootsuite*, le monde compte 4, 39 milliards d'internautes[227]. Cette communauté d'utilisateurs d'Internet n'est pas suffisamment informée des impératifs de cybersécurité dans l'utilisation de l'outil informatique. Or, une cybersécurité fiable passe par la mise en place d'une cyberrésilience. Cette dernière est une approche visant à impliquer davantage les individus dans la protection de leurs systèmes d'information et ceux de leurs entreprises. La cyberrésilience est donc définie comme une méthode de gestion active de la sécurité basée sur une implication croisée des individus, des processus et de la technologie[228]. Elle procède de la sensibilisation à la formation du citoyen aux mesures et comportements de la cybersécurité. Par exemple, les internautes peuvent être sensibilisés à l'intérêt d'avoir un mot de passe fiable ou aux risques de piratage de webcam encore appelé *Webcam hacking*. Le but d'un *web hacking* est varié : il peut s'agir du voyeurisme, d'un cyberchantage ou d'un détournement bancaire. Face à ce type de faille de sécurité, les internautes doivent disposer de mesures matérielles et fonctionnelles pour parer la menace à titre préventif et en cas d'atteinte réel ils doivent pouvoir saisir les structures compétentes afin de mettre fin à la menace et si possible repérer l'auteur de l'acte malveillant à travers les mécanismes de preuve de la cybersécurité[229]. Dans cette dynamique, le dispositif *Signal Spam* a été mis en place par les autorités françaises pour lutter contre le spam. Il s'agit d'un mécanisme novateur qui réunit tous les acteurs privés, les associations industrielles et les pouvoirs publics préoccupés par les menaces véhiculées par le spam, les attaques informatiques et la fraude[230]. Ce

---

[227] https://www.journaldunet.com/ebusiness/le-net/1071539-nombre-d-internautes-dans-le-monde/ (consulté le 26 juillet 2019) ; voir aussi https://www.clubic.com/internet/actualite-846879-monde-compte-4-2-internautes-2018-3-4-reseaux-sociaux.html (consulté le 26 juillet 2019).

[228] Cf. définition de la cyber-résilience dans le Lexique de la cybersécurité réalisé par Hub One, Lexique disponible en ligne sur https://www.hubone.fr/ressources/lexique-cyber/ (consulté le 26 juillet 2019).

[229] Cf. définition de la cybersécurité selon l'UIT ou l'ANSSI qui prévoient toutes la preuve dans les méthodes et techniques de définition de la cybersécurité.

[230] M. QUEMENER, J-P. PINTE, *Cybersécurité des acteurs économiques: risques, réponses stratégiques et juridiques, Paris, Lavoisier*, 2013, p. 82.

dispositif donne la possibilité aux internautes de signaler tout ce qu'ils considèrent être un spam dans leur messagerie afin de l'assigner ensuite à l'autorité publique ou au professionnel qui saura le mieux prendre l'action qui s'impose pour lutter contre le spam signalé et poursuivre le spammeur en cas de spam de nature cybercriminelle[231]. Ce dispositif semble mobiliser les internautes d'autant plus que le deuxième trimestre de l'année 2019 a connu 6.803.292 signalements[232]. Il convient donc de diffuser une véritable culture de la sécurité informatique auprès de tous les échelons des utilisateurs d'Internet[233]. Eu égard à ce qui précède, il est clair que les citoyens doivent être considérés dans la mise en place d'une cybersécurité efficace. Pareillement, le rôle des acteurs institutionnels privés mérite d'être officialisé car ces acteurs semblent détenir le cœur même d'Internet qui est l'environnement de la cybersécurité.

B- De l'importance de la reconsidération du rôle des entreprises et organisations privées

La cybersécurité est une sécurité spécifique compte tenu de la nature insaisissable d'Internet. Comme souligné *supra*, les acteurs de la cybersécurité sont nombreux et les acteurs privés se révèlent dans bien des cas détenir la racine d'Internet mettant ainsi les acteurs étatiques dans le fait accompli. Nous sommes sur un terrain où les Etats exercent une souveraineté très relative. Ils sont donc obligés de constater leurs limites et édifier une cybersécurité mondiale avec les autres forces du cyberespace. L'histoire semble donner raison en partie à John PERRY BARLOW sur son idée de d'indépendance du cyberespace. Les acteurs

[231] Cf. description des missions du dispositif Signal Spam sur le site de l'institution à l'adresse https://www.signal-spam.fr/ (consulté le 30 juillet 2019).
[232] Voir https://www.signal-spam.fr/ (consulté le 30 juillet 2019).
[233] N. ARPAGIAN, La cybersécurité, Op. Cit. p.86; M. QUEMENER, J-P. PINTE, *Cybersécurité des acteurs économiques: risques, réponses stratégiques et juridiques, Op. Cit*. p. 83.

privés d'Internet se sont peu à peu configurés en deux camps : d'une part les acteurs techniques d'Internet[234] et d'autres part les acteurs commerciaux et ou industriels[235]. La reconsidération de leur rôle par les acteurs étatiques reviendrait à prendre conscience du rôle de ces acteurs privés et initier des partenariats avec eux pour qu'ils mettent leur force au service du projet de cybersécurité mondiale. Par exemple en ce qui concerne les acteurs techniques, l'ouverture de l'ICANN doit être encouragée afin de démocratiser la gouvernance de l'institution américaine. Concernant les acteurs commerciaux et industriels, un regard croissant des Etats sur le fonctionnement de ces entreprises mérite d'être souligné d'autant plus que ces géants du net mettent parfois leurs intérêts en avant au détriment de la sécurité des données des internautes. En témoigne la récente sanction contre Facebook dans l'affaire *Cambridge Analytica* à hauteur de 5 milliards de dollars par l'Etat américain-qui veut reprendre la main sur les géants du web-pour manquement à la protection des données personnelles de ses utilisateurs.

L'instauration d'une gouvernance internationale renforcée de la cybersécurité passe par la mise en place des mécanismes internationaux centralisés sur la cybersécurité.

SECTION 2 : LA NECESSITE D'UNE GOUVERNANCE INTERNATIONALE CENTRALISEE DE LA CYBERSECURITE : LA RECHERCHE D'UNE CYBERSECURITE COLLECTIVE

L'administration d'un bien commun ou d'une cause commune à l'humanité passe par la mise en place d'un mécanisme de gouvernance centralisé afin de fédérer les forces des différentes parties prenantes. En matière de gouvernance de

[234] Il s'agit des organisations et associations telles que l'**ICANN**, le World Wide Web Consortium (**W3C**)², l'Internet Engineering Task Force (**IETF**), l'Internet Architecture Board (IAB), l'Internet Society (**ISOC**), ou encore l'Internet Engineering Steering Group (**IESG**). Pour plus d'éclaircissement sur le role des quatre dernières organisations voir N. ARPAGIAN, La cybersécurité, *Op. Cit*. pp. 87-94.
[235] Il s'agit entre autre des **GAFAM**.

la cybersécurité, une gouvernance centralisée garantirait le développement de la confiance numérique entre acteurs du cyber (paragraphe 1) et la répression efficace des attaques informatiques sur le plan international (paragraphe 2).

Para 1 : Le développement de la confiance numérique, gage d'une cybersécurité collective dans le monde

Dans un discours au Bundestag le 29 janvier 2014, la chancelière allemande Angela MERKEL déclarait « *La confiance est la base de la paix et de l'amitié entre les peuples*[236]». En effet, la confiance entre les peuples et les organisations est aussi nécessaire dans la gouvernance internationale de la cybersécurité. Cette confiance numérique doit être déclinée en deux branches : d'une part la confiance institutionnelle ou la confiance entre les utilisateurs et les entreprises et d'autre part la confiance interorganisationnelle ou la confiance entre entreprises. Les deux dimensions de la confiance numérique procèdent de la confiance dans les personnes, la confiance dans les processus et la confiance dans les technologies numériques. De ce fait, les différents acteurs de la chaine de cybersécurité doivent assurer la sécurité de leurs systèmes d'information pour avoir du crédit aux yeux de leurs partenaires. Ainsi, sur le plan international, l'érection d'une confiance numérique se manifestera-t-elle par l'assistance entre acteurs de la cybersécurité à la survenance d'un risque informatique (B). Mais la consécration d'une Autorité de coordination de la cybersécurité serait le point d'encrage (A) d'une véritable gouvernance internationale de la cybersécurité.

A- La nécessaire consécration d'une Autorité de coordination de la cybersécurité sur le plan international

[236] Voir N. ARPAGIAN, *La cybersécurité*, *Op. Cit*. p. 3.

La mise en place d'une cybersécurité efficace sur le plan international, passe par l'instauration d'une Autorité internationale de la cybersécurité[237]. Cette Autorité doit avoir des pouvoirs de direction et d'action en matière de cybersécurité. La consécration d'une Autorité internationale de la cybersécurité est justifiée par la nécessité d'une planification des mesures de prévention et d'action en cas d'atteinte à l'intégrité des systèmes d'information d'un pays par le fait d'une attaque extérieure. En cas d'une attaque provenant d'un acteur étatique étranger les services de l'Autorité seront d'un secours inestimable pour l'établissement de la preuve devant les instances compétentes. En l'état actuel l'UIT est de fait l'instance internationale compétente sur les problématiques de cybersécurité. Au demeurant, son action en matière de cybersécurité semble timorée car l'UIT brille à travers des conférences et sessions de formation. Ses capacités techniques notamment en matière de sécurité sont encore inefficaces. De ce fait, la communauté internationale dispose de deux solutions possibles. En premier lieu, elle peut créer une structure de type ENISA ou ANSSI pour faire face aux cybermenaces touchant la communauté internationale. Le cas échéant cette structure sera rattachée à l'UIT. En second lieu, l'UIT mérite d'être renforcée durablement au-delà de son fonctionnement actuel. C'est ce que semble viser le programme sur la cybersécurité qui est lancé depuis 2007[238]. Aussi, convient-il de rappeler que dans un groupe la solidarité est le lien social qui permet au groupe de ne pas rester indifférent face à la souffrance d'un ou plusieurs membres.

B- La nécessité d'une assistance entre acteurs en cas de risques informatiques

[237] Voir E. M. ROCHE, et M. J. BLAINE, « Convention internationale sur l'utilisation pacifique du cyberespace », *Op. Cit.*

[238] Voir https://www.itu.int/itunews/manager/display.asp?lang=fr&year=2008&issue=09&ipage=18&ext=html (consulté le 05 août 2019).

Les acteurs du cyberespace dans le monde gagneraient à cultiver l'assistance numérique dans leur relation mutuelle. Cette assistance mutuelle dépendrait du degré de coopération numérique entre les acteurs du cyberespace. Elle est essentielle dans la construction d'un écosystème numérique sécurisé d'autant plus qu'elle permet de lutter contre la fracture numérique entre les acteurs du cyberespace. De façon pratique, l'assistance numérique s'avère indispensable dans la gestion des crises de grande ampleur. Par exemple, pendant la vague de cyberattaque qu'à subi l'Estonie en 2007, les Etats qui s'en sortent mieux en matière de cybersécurité pouvaient aider l'Estonie à faire face à cet incident de grande ampleur en limitant la paralysie de l'économie estonienne. Cette assistance passera forcement par le partage de technologie entre les acteurs de la cybersécurité et l'Autorité de centralisation de la gouvernance internationale de la cybersécurité serait la courroie de transmission de l'assistance numérique. Ce qui n'exclut pas l'assistance que pourrait bénéficier un Etat dans le cadre d'une coopération bilatérale avec un autre acteur. Une gouvernance centralisée de la cybersécurité serait aussi une aubaine pour une répression efficace de la cybercriminalité sur le plan international.

Para 2 : Le renforcement de la répression des cybercriminels sur le plan international

La répression de la cybercriminalité est un facteur de la construction d'une cybersécurité durable. En effet, tel que mentionné *supra*, la cybersécurité fait appel à des techniques de sécurités des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense[239]. Partant de ce constat, il convient de souligner que la mise en œuvre d'une politique de

[239] M. WATTIN-ANGOUARD, « Cybermenaces et sécurité nationale », in *Le droit de la sécurité et de la défense en 2013*, *Op. Cit.* p. 300-301 ; voir aussi A. CATTARUZZA, D. DANET, *La cyberdéfense : quel territoire, quel droit*, *Op. Cit.* p. 167.

répression de la cybercriminalité dans le monde passe par la mise en place de structures d'enquêtes et de contrôle sur la criminalité (A) et le renforcement de la juridictionnalisation des infractions à caractère numérique (B).

A- Le renforcement des pouvoirs des structures d'enquêtes et de contrôle de la cybercriminalité

Il importe de rappeler qu'il n'existe pas de définition communément admise de la cybercriminalité bien qu'environ 470 types infractions sont liés aux systèmes d'information. Ces infractions peuvent être regroupées en deux catégories: les unes sont tentées ou commises contre les systèmes de traitement automatisé de données (STAD), tandis que les autres le sont grâce à ces systèmes. Les premières concernent notamment l'accès non autorisé à ces systèmes, les atteintes à l'intégrité des données et des systèmes informatiques, ou les atteintes à leur confidentialité ; les secondes regroupent les infractions de droit commun commises au moyen d'un STAD[240]. Ainsi, face à l'inflation de la cybercriminalité dans le monde, une approche coopérative et innovante sur les questions de sécurité mondiale s'impose-t-elle[241]. L'Organisation internationale de police criminelle (INTERPOL) est en pleine métamorphose pour répondre à ce défi. Créée le 07 septembre 1923 sous la devise « relier les polices pour un monde plus sûr », INTERPOL a pour mission de prévenir et combattre la criminalité grâce à une coopération policière internationale. Son action dans la lutte contre la cybercriminalité est remarquable mais mérite d'être renforcé au regard de la fréquence des cyberattaques dans le monde. Il s'agira notamment d'habiliter INTERPOL pour qu'elle soit proactive dans la veille opérationnelle de traque des cybercriminels. De façon pratique, la capacité pour INTERPOL de détecter une

[240] B. PEREIRA, « La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité », Revue internationale de droit économique, 2016/3, pp. 387-388, disponible en ligne sous la référence https://www.cairn.info/revue-internationale-de-droit-economique-2016-3-page-387.htm# (consulté le 06 aout 2019).
[241] M. QUEMENER, J-P. PINTE, *Cybersécurité des acteurs économiques: risques, réponses stratégiques et juridiques, Op. Cit.* p. 193.

action malveillante et de pister l'auteur de l'action afin de faciliter la mission que les Etats membres lui ont confié serait un plus vers une cybersécurité mondiale. Une telle capacité répondrait à l'une des conditions d'une bonne cybersécurité qu'est la preuve de l'attaque qui sous-entend la capacité de remonter à l'auteur de l'attaque pour des poursuites judiciaires. Elle doit aussi s'inspirer des actions de certaines organisations régionales telles que l'EUROPOL une des plus grandes consultations internationales en matière de cybercriminalité[242]. EUROPOL est une agence européenne de police criminelle qui facilite l'échange de renseignement entre polices nationales en matière de stupéfiants, de terrorisme, de criminalité internationale et de pédophilie au sein de l'Union européenne[243]. En matière de lutte contre la cybercriminalité EUROPOL se révèle être une grande innovation. Sa réussite serait liée à la vision commune des Etats membres d'EUROPOL qui sont tous partie prenante à la Convention de Budapest sur la cybercriminalité. Le bon sens voudrait qu'après une harmonisation des mécanismes d'investigation et de contrôle de la cybercriminalité, l'on s'achemine vers la juridictionnalisation des infractions du numérique sur le plan international.

B- Le renforcement de la juridictionnalisation des infractions du numérique sur le plan international

Le contentieux de la cybercriminalité est un contentieux à la fois national et international en raison de l'existence éventuelle d'éléments d'extranéité dans ce contentieux d'une part et de la qualité des auteurs des attaques qui peuvent être des acteurs de droit privés ou des acteurs étatiques. En cas d'attaque évidente entre deux ou plusieurs Etats, la compétence de la Cour Internationale de Justice sera engagée alors que l'atteinte des systèmes d'informations d'un Etat, téléguidée par

[242] *Ibid.* p. 194.
[243] M. QUEMENER, J-P. PINTE, *Cybersécurité des acteurs économiques: risques, réponses stratégiques et juridiques, Op. Cit.* pp. 194-195.

une personne privée pourrait poser une question notamment l'existence ou non d'une puissance étatique derrière l'acte malveillant. La recherche de la preuve pourrait être confiée à un comité d'experts indépendants sous la coordination de l'Autorité internationale de la cybersécurité. Dans le cas où l'atteinte d'un système informatique serait planifiée et exécuter par une personne privée pour son propre compte, un régime de compétence universelle pourrait être institué pour que chaque Etat soit compétent pour juger le cybercriminel. Il se pose donc la question de la compétence territoriale en raison du caractère universel de l'environnement numérique. Encore faut-il que la cyberattaque soit incriminée. Etant donné qu'il n'existe pas encore d'instrument mondial juridiquement contraignant sur la cybercriminalité, l'on peut se retrouver dans une situation où un acte soit délictueux dans un pays alors que le même acte est dépourvu de tout caractère délictueux dans un autre pays. Ce qui peut constituer un frein à la mise en œuvre de certains mandats d'arrêt internationaux pour cybercriminalité. Cette situation encouragerait certains cybercriminels à commanditer leurs cyberattaques à partir des pays qui sont considérés comme des paradis de la cybercriminalité. Il urge donc d'harmoniser la juridictionnalisation de la cybercriminalité sur le plan international pour que les systèmes judiciaires des Etats puissent parler le même langage en matière de répression de la cybercriminalité et même pour aller loin mettre en place une juridiction pénale internationale pour réprimer les actes de cybercriminalité les plus graves. Dans cette optique, il serait plus facile d'habiliter les juridictions pénales internationales qui existent déjà-telle que la Cour pénale internationale- à connaitre de la répression de la cybercriminalité de grande ampleur. Pour ce qui concerne les attaques cybernétiques entre Etats, la compétence de la CIJ serait qualifiée à partir du moment où l'attaque cybernétique serait qualifiée de recours à la force entre Etats conformément à la Charte des Nations-Unies. Comme souligné *supra,* le Manuel de Tallinn retient pour une telle qualification qu'un seuil de dommage soit atteint[244]. Si dans l'instant présent la

[244] Voir la 11ème règle du Manuel de Tallinn.

gouvernance internationale de la cyberscurité reste lacunaire, il serait bien d'espérer à une amélioration de l'état du droit et des institutions dans un proche avenir car des projets de régulations sont en cours et l'on s'achemine vers une réelle gouvernance de la cybersécurité sur le plan international.

CHAPITRE 2

VERS UNE REELLE GOUVERNANCE INTERNATIONALE DE LA CYBERSECURITE

L'étude de la gouvernance internationale de la cybersécurité peut susciter des craintes chez tout bon observateur des enjeux du cyberespace. Mais ces craintes méritent d'être vite dissipées d'autant plus qu'un optimisme semble naitre dans la gouvernance mondiale de la cybersécurité. En effet, il est permis de penser que l'on tend vers une réelle gouvernance internationale de la cybersécurité. De nombreux travaux sont entrepris notamment dans le cadre onusien sur la sécurité du cyberespace depuis une dizaine d'années[245] et ces travaux semblent répondre à l'idée d'une gouvernance à travers la multilatéralité des différents groupes de discussions et la diversité des acteurs qui sont associés aux différents Groupes de travail sur le progrès de l'informatique et des télécommunications dans un contexte de sécurité internationale. Ainsi ces Groupes contribuent à l'édification d'une architecture de gouvernance de la cybersécurité sur le plan international (section 1). D'autres initiatives de soutien à ces travaux onusiens sur la cybersécurité méritent d'être présentées dans la présente étude (section 2).

SECTION 1 : L'APPORT SIGNIFICATIF DES GROUPES DE TRAVAIL DES NATIONS UNIES SUR LA SECURITE DU CYBERESPACE

La cybersécurité ne laisse aucune institution à vocation sécuritaire indifférente. En dehors des stratégies que chaque Etat mène individuellement en interne pour rester à jour dans la défense d'éventuels attaques contre ses systèmes d'informations, d'autres initiatives voient le jour aux Nations Unies -véritable cadre de la multilatéralité- pour gouverner le risque cyber dans toutes ses dimensions en instituant le respect des règles internationales et un code de conduite

[245] A.A. STRELTSOV, « La sécurité de l'information au niveau international : description et aspects juridiques », p. 5, disponible en ligne sur http://unidir.org/files/publications/pdfs/les-technologies-de-l-information-et-la-securite-internationale-fr-332.pdf (consulté le 12 août 2019).

en matière de cybersécurité[246]. Il importe de visiter l'architecture générale des Groupes de discussions des Nations Unies sur la sécurité du cyberespace (paragraphe 1). Ces Groupes de discussions bien qu'étant en cours ont déjà des retombées dans la conception et l'utilisation des technologies informatiques et des moyens de télécommunication de pointe (paragraphe 2).

Paragraphe1 : L'architecture générale des Groupes de travail des Nations Unies sur la sécurité du cyberespace

De façon générale, les Groupes d'experts gouvernementaux chargés d'examiner les progrès de l'informatique et des télécommunications dans un contexte de la sécurité internationale se sont succédé depuis l'année 2004 (A). A ce jour les travaux des différents Groupes d'experts gouvernementaux ont permis de connaitre la position des Etats sur l'idée de gouverner le cyberespace notamment à des fins sécuritaires (B).

A. Une succession répétitive des groupes de discussions

En 2004, le premier Groupe d'Experts Gouvernementaux (GEG) ou (GGE[247]) sur le progrès de l'informatique et des télécommunications dans un contexte de la sécurité internationale a été mis en place par l'Assemblée générale des Nations Unies à l'initiative de la Russie[248]. L'objectif des GGE est de produire un rapport consensuel répondant aux enjeux du progrès de l'informatique et des télécommunications dans le domaine de la sécurité internationale[249]. Après le GGE de 2004, quatre autres GGE ont été mis en place autour du même objet et le

[246] Cf. Résolution de l'AG-NU A/RES/*58/32 ;* voir aussi O. BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? », *Op. Cit*. p. 203.
[247] GGE est l'abréviation anglaise du Groupe d'experts gouvernementaux qui est mentionné dans les documents officiels des Nations Unies.
[248] Voir https://omc.ceis.eu/lechec-du-group-of-governmental-experts-gge-sur-la-cybersecurite-consequences-et-perspectives/ (consulté le 14 août 2019).
[249] *Ibidem*.

dernier a fini ses activités en 2017 aboutissant à l'adoption de trois grands rapports notamment en 2010, 2013 et en 2015. Les rapports de 2013 et de 2015 se révèlent assez riches en enseignements. Face à l'échec d'adoption d'un rapport en 2017, faute de consensus entre les parties, deux Groupes de travail ont été mis en place par l'AG-NU en fin 2018 pour continuer les discussions sur la gouvernance internationale de la cybersécurité. Il s'agit cette fois-ci de deux groupes de nature différentes. Le premier est un GGE à l'image des précédents cadres de discussions. Ses discussions débuteront en décembre 2019 pour une durée d'un an[250]. Le deuxième est un Groupe de travail à composition non limité (OEWG) qui est ouvert aux représentations étatiques et non étatiques[251]. Ce Groupe de travail débutera ses activités en septembre 2019 pour une durée de deux ans[252]. Il convient de relever que parallèlement aux résolutions des GGE, les Nations Unies ont adopté d'autres résolutions sur la sécurité du cyberespace. De tous ces groupes de discussions, il se dégage une idée générale de la position des Etats sur l'encadrement du cyberespace. Comme l'on pouvait s'attendre, cette position n'est pas souvent la même d'un Etat à l'autre ou d'un groupe d'Etats à un autre.

B. De la cristallisation des positions des Etats sur la cybersécurité

Les discussions onusiennes dans les différents Groupes de discussions qui se sont succédé de 2004 à 2017 mettent les parties prenantes face à leurs visions sur la régulation du cyberespace. Tous reconnaissent l'intérêt de gouverner le cyberespace à des fins sécuritaires afin d'assurer la protection des systèmes d'informations de leurs pays[253]. Toutefois, l'on assiste à la formation de deux blocs d'Etats autour de la cyberdiplomatie aux Nations Unies. D'un coté, l'on a les Etats qui sont pour une transposition pure et simple des règles et institutions du

[250] Voir https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/lutter-contre-la-criminalite-organisee/la-france-et-la-cybersecurite/ (consulté le 13 août 2019).
[251] Voir https://www.un.org/press/fr/2018/agdsi3619.doc.htm (consulté le 13 août 2019).
[252] *Ibidem*.
[253] O. BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? », *Op. Cit*. p. 203.

droit international positif à la régulation du cyberespace. Dans ce groupe d'Etats on retrouve les Etats membres du G7 et certains Etats de l'Union européenne. De l'autre côté, la Chine et la Russie s'imposent comme chefs de fil d'un courant de pensée. Ce dernier tout en tirant chapeau au droit international et aux institutions actuelles, estime qu'il est nécessaire de créer un nouveau cadre de gouvernance du cyberespace et de la cybersécurité en raison de la spécificité du cyberespace et des problèmes qu'il pose. Quel qu'en soit la position où l'on se situe, la cyberconflictualité actuelle impose que s'érige un *droit international en 3D* pour reprendre les propos de David Martinon[254]. A ce jour, les GGE ont réussi à poser les bases d'un début de gouvernance internationale de la cybersécurité.

Paragraphe 2 : Les acquis des travaux des Groupes d'experts gouvernementaux

Après d'âpres discussions, les GGE ont réussi à adopter des principes intangibles sur la bonne conduite des Etats dans le cyberespace (A). De même, sans être unanime, les parties prenantes reconnaissent à leur majorité l'applicabilité du droit international au cyberespace quoi qu'elles restent diviser sur les modalités de son application (B).

A.L'adoption de principes intangibles sur l'attitude responsable des Etats dans le cyberespace

Des trois rapports adoptés par les GGE en 2010[255], 2013[256], et 2015[257], les deux derniers ont un apport didactique qui mérite notre attention[258]. En effet, si le

[254] David MARTINON est l'Ambassadeur français pour la cyberdiplomatie.
[255] *Assemblée générale des Nations unies*, Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, *document des Nations Unies A/65/201, 2010.*

rapport du GGE de 2013 rappelle aux acteurs du cyberespace l'importance d'une coopération internationale dans le domaine de la cybersécurité, le rapport du GGE de 2015 adopté par consensus propose plusieurs normes de comportement responsable et des mesures de confiance. Ces normes facultatives et non contraignantes ont pour objectif « d'aboutir à une vision commune afin de renforcer la stabilité et la sécurité de l'environnement informatique mondial[259] ». *Grosso modo,* elles prescrivent les mesures suivantes :

-l'interdiction d'attaquer les infrastructures informatiques d'un Etat en temps de paix[260],

-l'obligation de porter assistance à un Etat victime d'une cyberattaque[261]

-la culture des mesures de confiance entre Etats afin de développer un climat de paix dans le cyberespace tout en érigeant une cyberdéfense optimale[262].

Pour le GGE de 2015, ces mesures peuvent être essentielles pour promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique[263]. Pour ce faire, l'applicabilité du droit international est plus qu'une nécessité.

B. La majoritaire reconnaissance de l'applicabilité du droit international au cyberespace

---

[256] Assemblée générale des Nations unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, document des Nations Unies A/68/98, 2013.
[257] Assemblée générale des Nations unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, document des Nations Unies A/70/174, 2015.
[258] A. GERY, « Droit international et prolifération des cyberarmes », Politique étrangère, 2018/2, p. 51,
[259] *Ibidem*. Voir aussi Rapport GGE 2015, *Op. Cit*., para. 14, p. 9.
[260] *Ibid*. para. 13, p. 8.
[261] *Ibid*., para. 20, p. 12.
[262] *Ibid*. para. 13, p. 8-9.
[263] Cf. Rapport GGE, *Op. Cit*., para. 14, p.10.

Dans son rapport de 2013, le GGE affirmait laconiquement que le droit international, en particulier la Charte des Nations Unies, est applicable et essentiel pour maintenir la paix et la stabilité, ainsi que pour promouvoir un environnement informatique ouvert, sûr, stable, accessible et pacifique[264]. Le rapport de 2015 corrobore dans ce sens en apportant plus d'éclaircissements à l'applicabilité du droit international au cyberespace[265]. En effet, le GGE estime que les engagements des Etats à respecter les principes suivants de la Charte des Nations Unies et d'autres principes de droit international étaient d'une importance centrale: l'égalité souveraine, le règlement des différends internationaux par des moyens pacifiques, de telle manière que la paix et la sécurité internationale ainsi que la justice ne soient pas mises en danger, le fait de s'abstenir, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies[266]. De même, les normes et principes internationaux qui procèdent de la souveraineté étatique s'appliquent à l'utilisation de l'outil informatique par les États ainsi qu'à leur compétence territoriale en matière d'infrastructure informatique[267]. Cette reconnaissance de l'applicabilité des règles du droit international est une grande avancée vers la régulation de la cybersécurité sur le plan international bien que la plus part des rapports de ces GGE n'ont pas de force obligatoire. Ces rapports constituent donc un *soft law* de plus dans la gouvernance de la cybersécurité au point où la doctrine et même les Etats n'hésitent plus à mentionner l'applicabilité du droit international à l'espace numérique dans leurs cyberstratégies nationales[268]. En soutien aux travaux des GGE, d'autres initiatives s'invitent dans la gouvernance de la cybersécurité.

[264] Cf. Rapport GGE de 2013 *Op. Cit.,* voir aussi F. DELERUE, A. GERY, « Le droit international et la cyberdéfense » *in La cyberdéfense, politique de l'espace numérique, Op. Cit.* p. 61 -62.
[265] Cf. Rapport du GGE de 2015, para. 25, p. 14.
[266] *Ibid*. para. 26, p. 14.
[267] *Ibid*., para 27. p. 14.
[268] F. DELERUE, A. GERY, « Le droit international et la cyberdéfense », *Op. Cit*. p. 62.

SECTION 2 : LES INITIATIVES DE SOUTIEN AU GROUPE DE TRAVAIL DES NATIONS UNIES SUR LA SECURITE DU CYBERESPACE

Quelques initiatives parallèles se font et d'autres encore pourraient se faire pour accompagner les travaux qui sont entrepris aux Nations Unies pour la sécurité du cyberespace. Ainsi après l'échec du GGE de 2016 à adopter un rapport en 2017, les acteurs du cyberespace ont entrepris d'autres initiatives en dehors du système des Nations Unies (paragraphe 1). L'interprétation du droit international étant la pomme de discorde, il serait judicieux d'impliquer la commission du droit international pour une interprétation objective des règles du droit international qui seront appliquées au cyberespace (paragraphe 2).

Paragraphe 1 : L'apport volontariste des initiatives officieuses après l'échec du GGE de 2016

Après l'échec du GGE de 2015, plusieurs Etats ont fait des suggestions sur l'avenir des GGE (A). Des initiatives privées se sont fait sentir dans le monde, réunissant les géants de l'Internet autour de l'avenir de la sécurité informatique[269] (B).

A. Les initiatives étatiques au secours de l'avenir des GGE

[269] Voir https://omc.ceis.eu/lechec-du-group-of-governmental-experts-gge-sur-la-cybersecurite-consequences-et-perspectives/ (consulté le 16 aout 2019).

L'échec du GGE de 2016 à adopter un rapport en 2017 a vu émerger des propositions unilatérales de certains Etats sur l'avenir du cyberespace. Les délégations cubaines, russes et chinoises ont proposé la création d'un Groupe de travail ouvert à tous les Etats volontaires[270]. C'est sans doute cette proposition qui a inspiré à l'AG-NU à mettre en place un Groupe de travail dont les activités vont débuter en septembre 2019. Dans la foulée, deux conceptions émergent : d'un côté, celle de la Russie et du Brésil qui privilégient une coopération régionale, et de l'autre côté, celle qui promeut une coopération bilatérale soutenue par l'Inde et la Suisse. Dans le premier bloc, la Russie clame l'adoption d'un Traité global sur la cybercriminalité pour remplacer la Convention de Budapest, dont elle conteste l'article 32 qui permet à un Etat étranger d'accéder ou de recevoir des données stockées sur le territoire d'autres Etats s'il obtient le consentement du propriétaire de ses données. Dans le même temps, le Brésil évoque un nouveau cadre juridique qui interdirait en priorité l'usage offensif des capacités cyber, notamment par l'introduction délibérée de vulnérabilités dans différents types de supports dans l'objectif de compromettre la sécurité des informations d'autres États. Cette position privilégie une utilisation défensive des capacités cyber et appelle à la mise en place d'une réglementation contraignante pour lutter principalement contre la cybercriminalité par une coopération internationale renforcée[271]. Dans le second bloc d'Etats, l'Inde et la Suisse proposent la création d'un « *Cyber Committee of the General Assembly* » sur le modèle du « *Committee on the Peaceful Uses of Outer Space »* créé en 1959. Il était alors composé de 84 membres et de différents sous-comités spécialisés notamment dans des domaines juridique et scientifique. Face à ce positionnement étatique, les acteurs privés ne sont pas restés silencieux parce que la participation interétatique ne peut apporter à elle seule des solutions efficaces et durables à ces défis sécuritaires[272].

[270] *Ibidem.*
[271] *Ibidem.*
[272] J. NOCETTI, « Géopolitique de la cyber-conflictualité », *Op. Cit*. p.27.

B. L'apport des initiatives privées au secours des GGE

En février 2017, Brad Smith, Président de Microsoft Corporation, annonce la création d'une « *Convention de Genève Digital* » n'ayant pour le moment remporté qu'un succès mitigé auprès des États. Dans le but de rassembler alors le secteur privé, 40 entreprises leaders du numérique tels que Dell, Facebook, Oracle ou Trend Micro signent le *Cybersecurity Tech Accord*, proposé par Microsoft. Le principe retenu est celui du « *Strong defense, No offense*[273] » : l'accord n'autorise que des opérations défensives. En cas de menaces, les entreprises s'engagent à répondre collectivement pour protéger les utilisateurs[274]. Cette Convention de Genève digital s'inspirerait des Conventions de Genève sur les conflits armés[275]qui régissent la conduite des hostilités en temps de guerre. Une autre initiative s'est fait entendre sous les hospices de deux *think tank* hollandais et américain. Ceux-ci créèrent la « *Global Commission on the stability of cyberspace*[276] ». Cette commission est composée de 26 commissaires de professions diverses-universitaires, organisations non gouvernementales, entreprises-et a pour objectif de promouvoir une compréhension commune des enjeux du cyberespace permettant de renforcer la stabilité et la sécurité. Elle vise à encadrer aussi bien les actions étatiques que celles issues d'acteurs non-étatiques[277].

---

[273] Littéralement cette devise veut dire « défense forte, aucune offense ». Elle consacre donc une meilleure architecture de défense au détriment de la volonté offensive des acteurs du cyberespace.

[274] Voir https://omc.ceis.eu/lechec-du-group-of-governmental-experts-gge-sur-la-cybersecurite-consequences-et-perspectives/ (consulté le 19 août 2019) ; voir aussi https://dig.watch/actors/global-commission-stability-cyberspace (consulté le 19 août 2019).

[275] Convention de Genève (I) sur les blessés et malades des forces armés sur terre du 12 aout 1949 ; Convention de Genève (II) sur les blessés, malades et naufragés des forces armés sur terre du12 aout 1949 ; Convention de Genève (III) sur les prisonniers de guerre du 12 aout 1949. Convention de Genève (IV) sur les personnes civiles du 12 aout 1949. Ces quatre conventions sont complétées par deux protocoles additionnels adoptés le 08 juin 1977. Le premier porte sur la protection des victimes lors des conflits internationaux, mais également lors des « conflits armés dans lesquels les peuples luttent contre la discrimination coloniale et l'occupation étrangère et contre les régimes racistes dans l'exercice du droit des peuples à disposer d'eux-mêmes (article 2 dudit protocole). Le deuxième porte sur la protection des conflits armés non-internationaux ou guerres civiles.

[276] Voir https://dig.watch/actors/global-commission-stability-cyberspace (consulté le 19 août 2019).

[277] Voir https://omc.ceis.eu/lechec-du-group-of-governmental-experts-gge-sur-la-cybersecurite-consequences-et-perspectives/ (consulté le 19 août 2019).

Face à la difficulté des acteurs du GGE de définir les modalités d'application du droit international au cyberespace et à la cybersécurité, il serait judicieux de saisir la commission du droit international qui reste et demeure une institution de référence en matière de développement du droit international.

Paragraphe 2: La nécessaire implication de la commission du droit international sur les questions d'ordre juridique liées à l'interprétation du droit international

Rappelons d'emblée que la gouvernance internationale de la cybersécurité pose de nombreuses problématiques notamment d'ordre politique et juridique. Le dernier GGE a échoué à adopter un rapport face à une question d'ordre juridique spécialement les modalités d'application du droit international. En effet, si tous les Etats s'accordent à l'idée que le droit international régisse le cyberespace très peu ont réussi à s'entendre sur comment le droit international s'appliquerait aux cybermenaces et les réactions des Etats en vue de faire face à ce phénomène qui prend de l'ampleur. L'implication de la Commission du Droit International[278] (CDI) faciliterait la tâche au processus de réglementation du cyberespace. Etant chargé de développer progressivement le droit international, la CDI est amené conformément à l'article 15 de son statut à « *rédiger des conventions sur des sujets qui ne sont pas encore réglés par le droit international ou relativement auxquels le droit n'est pas encore suffisamment développé dans la pratique des Etats*[279] ». De ce fait, elle pourrait contribuer à l'émergence d'un droit international du cyberespace en interprétant les aspects du droit international qui semble flou aux

[278] La Commission du Droit International est un organe des Nations Unies chargé de la codification et du développement progressif du droit international. Elle a été mise en place par l'Assemblée générale des Nations Unies en 1947 et est composé d'experts juristes représentant chacun un Etat. L'on compte 34 experts à ce jour.

[279] Cf. article 15 du statut de la CDI disponible en ligne sur http://legal.un.org/ilc/texts/instruments/french/statute/statute.pdf (consulté le 19 août 2019).

yeux des Etats et des géants d'Internet. Par exemple, s'agissant de l'applicabilité des Conventions de Genève aux cyber-opérations de grande intensité, certaines notions telles que le statut de *combattant du cyberespace* sera expliqué de même que celle de la conduite des hostilités numériques. De même, les notions de légitime défense et celle d'agression seront interprétées au regard de la spécificité des cyber-opérations. La CDI aura donc pour mission de faire le précieux travail d'adaptation que les rédacteurs du Manuel de Tallin ont effectué dans le cadre de l'OTAN.

CONCLUSION

Somme toute, la question de la gouvernance internationale de la cybersécurité est une importante question d'actualité multidimensionnelle d'autant plus qu'elle engage différentes disciplines et différents acteurs de la vie nationale et internationale. Son intérêt se justifie par les nombreux enjeux notamment sécuritaires qui tournent autour de la sécurité des systèmes d'informations. Cette dernière engage le simple citoyen jusqu'à l'administration la plus numérisée de l'Etat en passant par les entreprises. Une telle exposition des nombreux utilisateurs du web à la cybermenace est liée à la dépendance des sociétés modernes à l'outil informatique. La prise de conscience de la réalité de la menace n'est plus à démontrer. Toutefois, les moyens de lutte ne sont pas encore à la hauteur de la recrudescence de la menace. Au niveau militaire, le ministre français de la défense, alors Jean-Yves LEDRIAN, affirmait en 2015 que « *le premier enjeu, pour nos forces armées, est désormais d'intégrer le combat numérique y compris de manière offensive ce qui constitue leur principale faiblesse, ce nouveau milieu est devenu un domaine militaire à part entière, dans lequel il faut positionner ses forces, défendre sa puissance et y exploiter toutes les occasions pour vaincre l'adversaire*[280] ». Le combat numérique étant par essence un combat asymétrique, toute stratégie défensive et offensive doit tenir compte de l'implication de tous les acteurs du cyberespace pour une réussite globale. Les initiatives étatiques visant à développer une armée numérique ne doivent pas ignorer l'impact négatif des cyberattaques civiles de type *ransomeware* qui peuvent affecter les OIV d'un pays en laissant des conséquences assez lourdes comme ce fut le cas en 2017. La fédération des forces et des volontés des acteurs du cyberespace[281] sur le plan international pourrait assurer au cyberespace-cet espace insaisissable et sans frontière-une sécurité fiable. Une bonne cybersécurité passera donc par la prévention. Et cette dernière commence par la connaissance des phénomènes cyber

[280] Nathalie Guibert, « La France revendique sa place dans la cyberguerre offensive », Le monde, 25 septembre 2015, cité par J.C. VIDELIN, « L'armée française et la cyberguerre », *in Annuaire du droit de la sécurité et de la défense 2018, Op. Cit.* p. 146.

[281] Etats, organisations internationales, entreprises multinationales du web, les entreprises à l'échelle nationale, les internautes….

et la sensibilisation des utilisateurs. Toute initiative visant à écarter un élément de la chaine de cybersécurité crée sa propre faille et donne ainsi aux cybercriminels une vulnérabilité pour réaliser leurs actions malveillantes. D'où gouverner serait le bon verbe pour mieux prévoir et agir contre les cybermenaces afin de construire une cybersécurité efficace et durable.

BIBLIOGRAPHIE

I- OUVRAGES

1- OUVRAGES GENERAUX

BAUDE Florent, WARUSFEL Bertrand, *Annuaire 2018 du Droit de la sécurité et de la défense*, Mare et Martin, 2018, 433 p.

CATTOIR-JONVILLE Vincent et SAISON Johanne, *Les différentes facettes du concept juridique de sécurité*, Mélanges en l'honneur de Pierre-André LECOCQ, Lille, Imprimerie Centrale du Nord, 2011, 480 p.

DAILLIER Patrick, FORTEAU Mathias et PELLET Alain, *Droit international public*, Paris, L.G.D.J., 8ème éd., 2009, 1709 p.

ROUSSEAU, Charles, *Droit international public*, Tome IV, Paris, Sirey, 1980, 672 p.

LATOUR Xavier, VALLAR Christian, *Le droit de la sécurité et de la défense en 2013*, Aix-en-Provence, Presses Universitaires d'Aix-Marseille, 2014, 334 p.

2- OUVRAGES SPECIAUX

ARPAGIAN Nicolas, *La cybersécurité*, Paris, NIL, 2018, 128 p.

ACHILEAS Phillipe, MIKALEF Willy, TIC*: Innovation et droit international*, Paris, Pédone, 2017, 294 p.

BLANDIN-OBERNESSER ANNIE, *Droits et souveraineté numérique en Europe*, Bruylant, 2016, 216 p.

CATTARUZA Amael, DANET Didier, *La cyberdéfense : quel territoire, quel droit ?*, Lonrai, Economica, 2014, 286 p.

CATTARUZA Amaël, DANET Didier, TAILLAT Stéphane, *La cyberdéfense, politique de l'espace numérique*, Malakoff, Armand Colin, 2018, 255 p.

DINNISS Heather Harrison, *Cyber warfare and the Law of war*, Cambridge, British Library, 2012, 331 p.

FERRY Joël, QUEMENER Myriam, *Cybercriminalité : défi mondial*, Lonrai, Economica, 2009, 308 p.

GROSJEAN Alain, *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, 465 p.

GRIMMELMANN James, *Internet Law: cases and problems*, Poland, Seventh Edition, 2017, 682 p.

ITEANU Olivier, *Quand le digital défie l'Etat de Droit*, Paris, Eyrolles, 2016,188 p.

JABER Abbas, *Les infractions commises sur internet*, Paris, L'Harmattan, 2009, 315 p.

MEILLAN Eric, LEVIEUX François, Survivre à la guerre numérique, Paris, Jean Picollec, 2017,187 p.

OANTA Gabriela Alexandra, RIOS RODRIGUEZ Jacobo, *Le droit public à l'épreuve de la gouvernance*, Perpignan, Collections Etudes, 2012, 479 p.

PINTE Jean-Paul, QUEMENER Myriam, *Cybersécurité des acteurs économiques: risques, réponses stratégiques et juridiques*, Paris, Lavoisier, 2013, 239 p.

REYMOND Michel, *La compétence internationale en cas d'atteinte à la personnalité par internet*, Romandes, 2015, 364 p.

RODRIGUE Léa, *Les aspects juridiques de la régulation européenne des réseaux*, Bruxelles, Bruylant, 2012, 499 p.

II- ARTICLES

BAKIS Henri, « fragilité du géocyberespace à l'heure des conflits cybernétiques », 27-¾-2013, disponible sur le site https://journals.openedition.org/netcom/1438 , consulté le 10 Mai 2019.

BLAINE Micheal, ROCHE Edward, « convention internationale sur l'utilisation pacifique du cyberespace », disponible sur le site https://journals.openedition.org/netcom/1449 , consulté le 07 Mai 2019.

DE LA CHAPELLE Bertrand, « Gouvernance de l'internet et gouvernance sur l'internet », disponible sur https://www.lajauneetlarouge.com/gouvernance-de-linternet-et-gouvernance-sur-linternet/ , consulté le 12 avril 2019.

GOMEZ Rodriguo Nieto, « Cybergéopolitique : de l'utilité des cybermenaces », in *Cyberespace enjeux géopolitiques*, Hérodote, 2014, 98-104.

JACOB Patrick, « La gouvernance de l'internet du point de vue du droit international public », *in Annuaire Français de droit international LVI*, Paris, CNRS Editions, 2010, p. 543-563.

QUENAULT, Béatrice « Dilemme westphalien et gouvernance des biens publics mondiaux : le cas de la protection du climat », Mondes en développement, 2013, disponible en ligne sur https://cairn.info/revue-mondes-en-developpement-2013-2-page-11.htm (consulté le 05 juillet 2019)

TALIHÄRM Anna-Maria, « En quête de la cyberpaix: gérer la cyberguerre par la coopération internationale », septembre 2013, disponible sur https://unchronicle.un.org/fr/article/en-qu-te-de-la-cyberpaix-g-rer-la-cyberguerre-par-la-coop-ration-internationale , consulté le 04 Mai 2019.

TROUCHAUD Philippe, « La gouvernance de la cybersécurité : savoir anticiper les risques », disponible en ligne sur https://www.pwc.fr/fr/publications/cybersecurite/gouvernance-de-la-cybersecurite-savoir-anticiper-les-risques.html (consulté le 12 juin 2019).

III- DOCUMENTS CONVENTIONNELS

Charte des Nations Unies signée le 26 juin 1945 à San Francisco et entrée en vigueur le 24 octobre 1945.

Convention de Budapest sur la cybercriminalité de 2001.

Convention de l'Union Africaine sur la cybersécurité et la protection des données du 27 juin 2014.

Convention de l'Union Internationale des Télécommunications adoptée le 22 décembre 1992.

Objectifs de Développement Durable.

Règlement européen sur la cybersécurité du 12 mars 2019.

IV- RAPPORTS ET RESOLUTIONS DES NATIONS UNIES

Rapport du SG A/68/98, 2013

Rapport du SG A/70/174, 2015

Résolution A/RES/58/32, 2003

Résolution A/RES/66/24, 2011

V- AUTRES DOCUMENTS

KAMINSKY Jean, Guide de la Cybersécurité, Bruxelles, Corelio, 2018, 172.

SAIDI Aziz, Péril digital, un front lucratif, Casablanca, La Tribune Afrique, 2019, 94 p.

Global Security Index, Publication de l'UIT (2018,2017, 2016).

DURAND Phillipe, Revue de la gendarmerie nationale, Limoges, SDG, décembre 2018, N°263, 168 p.

Actes du FIC 2014, 2015.

TABLES DES MATIERES