International Journal of Social Sciences and Scientific Studies (2022)

Listes de contenus disponibles sur: Scholar

LE DROIT INTERNATIONAL À L'ÈRE DE L'INTERNET ET DE L'INTELLIGENCE ARTIFICIELLE.

Journal homepage: ijssass.com/index.php/ijssass

LE DROIT INTERNATIONAL À L'ÈRE DE L'INTERNET ET DE L'INTELLIGENCE ARTIFICIELLE☆

SANGWA LUMBU Pathy [a *]

a. Université de Lubumbashi, Département de Droit Privé et Judiciaire. Kinshasa, Commune de Ngaliema, Quartier GB, 1Rue, 6 Villa, Camp Américain.

Received 25 September 2022; Accepted 24 October 2022
Available online 25 October 2022

A R T I C L E I N F O

Keywords:

Internet

Droit international

Cyberspace

Cybercriminalité et Cyberattaque

A B S T R A C T

La présente réflexion tient compte des réalités de l'heure liées à l'implication de l'internet dans la vie internationale et ses conséquences juridiques. L'espace virtuel, dit « cyberespace » apparait comme un lieu favorable pour les délinquants de contourner les mécanismes juridiques mis en place par la communauté internationale afin d'atteindre leurs objectifs criminels.

Depuis la fin des années 1990, le développement d'Internet à haut débit, et plus généralement du cyberespace, a bouleversé notre société du fait que, notre quotidien, nos droits fondamentaux, notre vie sociale et notre économie dépendent désormais des technologies de l'information et des communications. Cependant, la complexification des crimes informatiques aux retombées militaires à grande échelle rend difficile la gestion du cyberespace par les Etats seuls.

La vie sociale est en effet de plus en plus digitalisée sur base de l'internet de sorte que l'opérationnalité des activités des particuliers, des Entreprises publiques ou privées, des forces armées et même des Etats, se trouvent facilitées.

Les bouleversements suscités par le numérique dans le domaine économique, technologique et social, remet en cause l'avenir de la société humaine à cause du développement des machines connectées et « intelligentes ». Cette nouvelle donne constitue tout aussi un terrain favorable pour les délinquants étatiques et non étatiques au vu de son caractère vulnérable nécessitant l'intervention du Droit international à l'instar des certaines législations nationales.

Nous pensons que le nouveau défi ne se résume pas seulement au non respects des normes existantes du Droit international humanitaire par les forces en présence pendant les conflits armés, mais aussi, est-il nécessaire pour le Droit international de prendre en compte la nouvelle physionomie des conflits armés, telle que l'incursion de la nouvelle technologie militaire dans le règlement des différends.

Cette étude analytique plaide pour la prise en charge des nouvelles technologies de l'informatique par le Droit international afin d'éviter à ce que l'espace cyber ne puisse se transformer en un far West des criminels étatiques.

Introduction

Depuis la fin des années 1990, le développement d'Internet à haut débit, et plus généralement du cyberespace, a bouleversé notre société. Car, notre quotidien, nos droits fondamentaux, notre vie sociale et notre économie dépendent désormais des technologies de l'information et des communications. Cependant, la complexification des crimes informatiques aux retombées militaires à grande échelle rend difficile la gestion du cyberespace par les Etats seuls.

L'internet est en train de transformer la société toute entière avec comme conséquence, le transfert de la criminalité du réel vers l'immatériel. Il s'avère que les délinquants s'accommodent vite et très facilement au point d'être en avance par rapport aux services ordinaires. Cette réalité pousse à dire que le criminologue doit prendre comme repère les évolutions de la société pour analyser les comportements déviants. Faisant un aperçu superficiel de l'évolution du comportement criminel dans la société, l'on se rend compte qu'à l'origine de l'agriculture comme secteur primaire de la vie, les prédateurs s'en prenaient aux personnes : Caïn tua Abel ! Meurtres, assassinats, agressions, viols enlèvements, esclavage, constituaient l'essentiel des transgressions. Avec l'apparition de la production des biens manufacturés grâce à l'artisanat puis à l'industrialisation comme secteur secondaire, il eut un glissement de la criminalité des personnes vers les atteintes aux biens.

Enfin le secteur tertiaire suivi du quaternaire dont le précèdent est lié aux services, ouvre le champ de la délinquance intelligente en « col blanc », dominé par les infractions complexes difficiles à comprendre avec la justice ordinaires, tel est le cas de l'escroquerie, le blanchiment, fraudes, faux, etc. et le second émerge avec la transformation numérique, offrant une extraordinaire opportunité pour la criminalité et la délinquance qui permettent de s'en prendre aux personnes, aux biens, aux services et aux systèmes de traitement automatisé de données. En ayant un périmètre plus large que tous les autres espaces en ce qu'il recouvre plusieurs domaines de la vie humaine, notamment, les télécommunications (téléphone, radio, télévision, ordinateur) et Internet, le numérique a presque modifié notre mode traditionnel de vie en changeant pratiquement notre façon de comprendre la vie, de l'affronter et de penser, bref la vie humaine se trouve être numérisée. C'est donc tout l'univers qui se trouve transformé par cette réalité de sorte que toutes les activités humaines sont au quotidien presqu'informatisées. Tel est le cas de l'Estonie[1] où l'internet est un outil indispensable pour leur quotidien.

I. L'Internet, un nouveau défi du Droit international

L'article 19 de la Déclaration Universelle des Droits de l'Homme (DUDH), donne à tout individu le droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit2. Ce principe juridique, universellement reconnu par tous les Etats, est à la base de la nouvelle technologie de l'information « internet » dont l'objectif est la liberté d'expression, c'est à dire de recevoir ou de communiquer les informations ou des idées.

La liberté d'expression, droit reconnu à l'individu de faire connaître le produit de sa propre activité intellectuelle jusqu'aux confins de la terre, procède de la faculté de communiquer entre humains, longtemps considérée

[1] CHAMPETIER DE RIBES V., L'Estonie, un Etat numérique performant, in Revue civique http://revuecivique.eu, consulté le 13 mars 2022.
[2] Déclaration Universelle des Droits de l'Hommes du 10 Décembre 1948.

comme un simple phénomène naturel conditionnant la vie sociale, avant d'être solennellement érigée en liberté individuelle, juridiquement garantie. Cette libération de la parole a conduit le monde dans l'ère de l'internet.

L'internet est conforme au principe relatif à la libre circulation de l'information qui remonte en 1792 lors de l'émergence du télégraphe[3]. Depuis, ce principe a émergé graduellement de la rencontre progressive puis de la symbiose entre libre-circulation internationale des services et la liberté d'expression[4]. Cependant, il s'avère qu'avec l'apparition de l'internet, la technologie s'est développée plus vite que le cerveau provoquant au même moment une série d'infractions informatiques à tel point que la cybercriminalité est devenue une réalité inhérente à la société que le Droit ne peut plus ignorer. Depuis lors, la cybercriminalité couvre toute activité criminelle réalisée par le biais de l'informatique. Ce qui suppose que le comportement, bien que commis au moyen de l'internet et des nouvelles technologies, demeure criminel relevant du droit pénal national et international.

La vie sociale est en effet de plus en plus digitalisée sur base de l'internet de sorte que l'opérationnalité des activités des particuliers, des Entreprises publiques ou privées, des forces armées et même des Etats, se trouvent facilitées. Cette nouvelle donne constitue tout aussi un terrain favorable pour les délinquants étatiques et non étatiques au vu de son caractère vulnérable.

Ainsi, l'internet est considéré comme le réseau informatique mondial accessible au public dont les utilisateurs sont appelés « internautes ». Le terme « internet » est d'origine américaine, qui est le dérivé du vocable « internetting », qui veut dire interconnecter des réseaux. Cette nouvelle technologie a d'une part, augmenté les échanges entre personnes en offrant d'immenses potentialités pour participer au débat public, d'autre part, elle a transformé l'économie, réduit les frontières, accéléré la communication et surtout elle a offert à toutes et à toute la possibilité de traiter l'information, qui n'est plus l'exclusivité des professionnels.

Cette croissance de la vie numérique dans le monde est à la fois une réalité incontournable et remet en cause des conceptions anthropologiques traditionnelles. Car, tous les jours, à chaque instant et dans tous les secteurs, les services de l'internet sont sollicités.

Les bouleversements suscités par le numérique dans le domaine économique, technologique et social, remet en cause l'avenir de la société humaine à cause du développement des machines connectées et « intelligentes ». L'intelligence artificielle influe directement sur les vies privées et professionnelles, nul ne sait rester loin de son smartphone, que ça soit pendant la journée ou la nuit. Avec l'avènement du numérique, l'Etat n'a plus le monopole de l'action dans le cyberespace de sorte qu'aucun pays n'est épargné par les actions criminelles des délinquants « hackers » dans le cyberespace.

Les technologies numériques apparaissent non seulement comme des outils essentiels, ayant facilité l'accès à la parole pour les personnes dont les droits sont bafoués ou qui sont exposées à différentes formes de censure, mais aussi elles sont devenues un terrain favorable pour la criminalité. D'où la notion de cybercriminalité, une activité criminelle qui s'est développé dans un environnement constitué par l'ensemble des équipements et logiciels informatiques, dit « cyberespace »5.

[3] Le télégraphe optique a été conçu par l'Ingénieur français Claude Shappe et ses quatre frères en 1794. En 1832, l'idée d'un télégraphe électrique fut de Samuel Morse. Celui-ci inventa en parallèle un alphabet propre à son utilisation : le code Morse, testé pour la première fois en 1837.

[4] OCHOA N., « Principe de libre circulation de l'information-recherche sur les fondements juridiques d'internet », in *HALSHS*, 2016, sur https://halshs.archives-ouvertes.fr, consulté le 23 février 2021 à 12 h 34.

[5] GHERNAOUTI S., *La cybercriminalité, les nouvelles armes du pouvoir*, 2ème

1. Le cyberspace

L'internet est non seulement à la base des nouvelles technologies mais aussi apporte un nouveau langage puisque depuis son apparition, il existe des vocables tels que, le cyber guerre, cyberculture, cyber-patrimoine, cybercrime, cyberdéfense, … cyberespace, termes auxquels tout internaute doit se familiariser. Parmi toutes ces terminologies issues de la nouvelle technologie, ce qui nous importe pour l'instant, c'est le cyberespace.

Le substantif « espace »

Pour mieux cerner le sens du préfix « cyber », l'on se propose d'analyser à l'avant plan le substantif « espace » que, Alain RENAUD considère comme étant à la fois une notion ambigüe, imprécise et un mot chargé des sous-entendus, des présupposés et d'acceptions multiples. Tout en étant un élément fondamental pour la discipline géographique, l'espace n'est plus qu'un élément parmi tant d'autres n'ayant rien de déterminant[6]. Il indique que dans le domaine de la géographie, l'importance de l'espace se fait sentir dans la rédaction des cartes pour la localisation des points remarquables de la surface de la terre afin de préciser les limites et la forme des continents. Kan précise à ce propos que, l'espace étant une représentation nécessaire a priori qui sert de fondement à toutes les perceptions extérieures[7], n'a pas d'existence réelle.

Le sens du préfix « cyber »

Le préfix « Cyber » du grec "kubernao" qui signifie piloter, d'abord inventé par le mathématicien, physicien, chimiste et philosophe Français[8], André-Marie Ampère dans l'étude des moyens de gouvernement en 1834, puis repris en 1948 après la deuxième guerre mondiale par l'américain Norbert Wiener dont la mission consistait à mettre au point des missiles capables d'atteindre les V1[9] et le V2[10], est une coupure du mot « cybernétique ».

L'usage du « cyber » est consécutif au développement exponentiel de l'informatique et de la robotique, plus généralement à l'avènement du réseau internet et de la « révolution numérique », qui en est la synthèse. Le terme **cyber** recouvre donc l'ensemble d'activités liées à l'utilisation offensive du cyberespace : une géographie imaginaire.

Si du point de vue classique, le territoire doit être compris comme une étendue sur laquelle vit un groupe humain qui le considère comme sa propriété, l'internet vient remettre en cause cette façon de voir les choses par ses nouvelles notions, tel que celle relative à l'espace cyber, conventionnellement appelé « cyberespace », entant qu'un monde virtuel souvent identifié comme constitutif d'une nouvelle forme d'espace hors de l'espace géographique classique[11]. Il est également considéré par Solange comme étant un espace où l'on peut avoir accès au réseau Internet et ainsi à un « univers » de réalité virtuelle[12].

Contrairement à la géographie classique, l'internet a son espace, appelé : « cyberespace », qui n'est ni moins ni plus, un nouvel espace « numérique » de souveraineté à conquérir par les Etats, outre les espaces traditionnels : territorial, maritime et aérien. En effet, il est considéré comme *l'espace de communication constitué par*

édition entement actualisées, PPUR Lausanne 2017.

[6] RAYNAUD A., « Notion d'espace en géographie », in *Travaux de l'Institut de Géographie de Reims,* /année 1971/5/pp. 3-14 en ligne sur https://www.persee.fr/doc/tigr_0048-7163_1971_num_5_1_926, consulté le 14 mars 2021

[7] KANT, critique de la raison pure, cité par Raynaud A., Idem, p4

[8] THEVENET BERANGERE, L'ère Cyber et ses nouveaux enjeux, publié le 8 octobre 2018 - dernière mise à jour : 16 juillet 2020, tiré sur https://www.e-xpertsolutions.com, le 15 mars 2014

[9] V_1 : est une vitesse de décision au décollage en-dessous de laquelle, le pilote peut encore interrompre le décollage. Mais, au-delà, même en cas de panne moteur ou système, le décollage doit être poursuivi sinon la sortie de piste est assurée.

[10] V_2 : est une vitesse de décollage qui *doit être atteinte au plus tard à 35 pieds d'altitude (10 m) et maintenue au moins jusqu'à 400 pieds « 120 mètres »*.

[11] DOUZET F., DESFORGES A., LIMONIER K., « Géopolitique du cyberespace : "territoire", frontières et conflits. CIST2014 - Fronts et frontières des sciences du territoire », in *Collège international des sciences du territoire (CIST)*, Mar 2014, Paris, France. pp.173-178 en ligne sur https://hal.archives-ouvertes.fr, mise en ligne le 11 aout 2016, consulté le 20 février 2021.

[12] GHERNAOUTI-HELIE S., *La Cybercriminalité, le visible et l'invisible*, Presses polytechniques et universitaires romandes, première édition 2009, p. 15.

l'interconnexion mondiale d'équipements de traitement automatisé de données numérisées[13]. Il est en réalité un espace où l'on peut avoir accès au réseau Internet et ainsi un « univers » de réalité virtuelle[14].

En d'autres termes, puisque l'internet a fait du « cyberespace » une réalité indépassable, bien que ce dernier reste encore un espace ayant un champ d'action non encore délimité au plan horizontal et vertical, le rendant ainsi un endroit déterritorialisé et dématérialisé ; le territoire subit automatiquement une modification de sa physionomie traditionnelle pour devenir un espace multidimensionnel qui intègre à la fois des facteurs statiques et des caractéristiques plus dynamiques.

Il s'avère que depuis les origines de l'humanité, l'homme s'est toujours livré à la découverte des espaces : aérien, maritime, territorial. Mais, cette fois si, il s'est lancé à la découverte du cyberespace, considéré comme le nouvel Eldorado des criminels et des délinquants[15], une nouvelle réalité non seulement pour des disciplines traditionnelles telles que la géographie et la criminologie, mais aussi pour le droit.

Au regard de l'évolution de la technologie à l'échelle universelle, et sans qu'il se détache de l'espace, le cyberespace pris dans son sens intrinsèque apparait non seulement comme un endroit où se gèrent les différentes données informatiques et la transmission d'informations pour les Etats ou les Organisations internationales. Son objectif principal est la sécurisation des informations contre toute forme de cyberattaque, mais également comme un milieu propice pour une offensive asymétrique à moindre frais ; un espace universel non restreint par des frontières étatiques. Dans cet, espace les agresseurs peuvent être des personnes morales ou physiques : les Etat, les Organisations internationales, nationales, les Entreprises, les organisations criminelles ou terroristes ou même des individus. Tel est le cas des Etats-Unis qui restent gouvernés par l'idée selon laquelle : toute cyberattaque fera l'objet d'une réponse offensive incluant si nécessaire des moyens conventionnels et non conventionnels.

2. La Cybercriminalité en droit interne

La « cybercriminalité », une notion floue et abstraite ayant vu le jour vers la fin des années 1990, traduit les comportements malveillants qui s'affichent dans un environnement cybernétique par des internautes. Elle désigne toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique.

Il existe une multitude d'infractions dans le domaine d'internet, plus de 470[16] tel que le cas de cyber escroquerie, le blanchiment d'argent, la fraude financière, le crime économique, l'atteinte au droit d'auteur, le hacking ou piratage, le spoofing, le carding et le skimming, le scamming, le spamming, la cryptologie, le google bombing, le cracking, la fraude aux sites aux enchères, la cyber sexualité, la pédopornographie, le cyber proxénétisme, le téléchargement illégal, le vol d'ordinateur et de fichiers, ou le piratage de logiciel, ou des nouveaux délits rendus possibles grâces à la nouvelle technologie de l'information, comme l'accès indu à un système, etc. Il ne faut toutefois pas perdre de vue que la palette des crimes informatiques est multiforme et le nombre est croissant.

L'internet apparait ainsi non seulement comme un moyen de rechercher et de se renseigner, mais aussi comme celui qui facilite la commission d'un panorama des actes de

[13] HUYGHE F.-B.– KEMPF O., MAZZUCHI N., *Gagner les Cyber conflits – Au-delà du technique*, Economica, 2015, cité par GASANÇON C., « Le cyberespace, nouvel espace de souveraineté à conquérir », in *CHEM. Mis en ligne le 22 mai 2018 sur* www.geostrategia.fr, consulté le 01 février 2021.
[14] GHERNAOUTI-HELIE S., *Op. cit*., p. 15.
[15] XAVIER L., *Guide de cyber sécurité, Droits, méthodes et bonnes pratiques, "piratage en cours"*, l'Harmattan, Paris, 2015, p. 19.
[16] PEREIRA B., La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité, in *Revue internationale de droit économique*, 2016/3 (t. XXX), pp. 387 à 409

malveillances, faisant de lui vecteur de multiplication des infractions réalisées au moyen de la technologie[17]. Dans le cadre de lutte contre la délinquance technologique, la nouvelle réalité de l'Internet a fait que le code pénal français de 1994 intègre les dispositions relatives à la cybercriminalité.

3. La Cybercriminalité en Droit international

Outre les législations nationales de certains Etats, quelques instruments internationaux sont mis en place dans le cadre de la règlementation de la vie dans le nouvel espace dit « cyberespace », lieu où il se passe toute forme d'activité, même criminelle violant les règles internationales traditionnelles. Dans cette perspective, mention peut être faite à la Convention du Conseil de l'Europe sur la cybercriminalité du Conseil de l'Europe, mise en place dans l'unique but de combattre le cyber crime, notamment le crime contre l'humanité[18]. Il en de même en ce qui concerne la convention de l'Union africaine[19] ainsi que les deux résolutions de l'AG relatives au cyberespace, prise dans le contexte de la sécurité internationale. Il s'agit de la résolution 73/266 et la résolution 73/27.

Cependant, la responsabilité qui en découle est à la foi pénale et civile dont les auteurs peuvent être des personnes physiques ou morales. Bref, le cyber crime englobe tous les délits réalisables via l'informatique et les techniques de l'internet dont les auteurs sont des personnes ayant des niveaux requis de compétence en informatique. Toutefois, force est de reconnaitre que les cyber-délinquants sont différents des autres délinquants ordinaires du point de vue connaissance scientifique. Les premiers doivent préalablement être des lettrés (criminels en col blanc), ce qui ne pas forcément le cas pour les seconds. Aussi, ceux-ci ont-ils besoin d'un contact physique avec la cible ou la victime, alors que ceux-là, un simple contact virtuel, derrière un écran suffit.

Selon l'Organisation de coopération et de développement économiques (OCDE), la cybercriminalité renvoie à la notion d'infraction informatique comme étant tout comportement illégal, immoral ou non autorisé qui implique la transmission ou le traitement automatique de données[20]. En effet, la cybercriminalité, est un vocable qui renvoie à une nouvelle forme de délinquance qui se commet dans un espace virtuel communément appelé le **cyberespace** ; assimilable à tout comportement illégal ayant trait au traitement automatique de données et, ou de leur transmission.

Cette nouvelle forme de délinquance virtuelle, s'étend à tout ce qui peut se faire par le moyen de l'informatique, les télécommunications, y compris la téléphonie fixe ou mobile, à tous les équipements qui intègrent un traitement électronique et informatique de données[21], elle n'épargne aucun secteur de la vie sociale, puisqu'elle arrive à opposer même les Etats entre eux.

4. Les attaques dans l'espace Cyber

Pour Olivier Kempf, le cyberespace est un « espace constitué de systèmes informatiques de toute sorte connectée en réseaux et permettant la communication technique et sociale d'informations par des utilisateurs individuels ou collectifs[22]. L'avènement de cet espace virtuel permet aux individus de s'attaquer aux Etats ou aux Entreprises. De la même manière, les Etats peuvent

[17] FERAR-SCHUHL C., *Cyber droit, le droit à l'épreuve de l'internet*, 6ème édition Dalloz 2010
[18] Convention du Conseil de l'Europe sur la Cybercriminalité, Budapest, 23/11/2001.
[19] Convention de l'Union Africaine sur la cyber sécurité et la protection des données à caractère personnel, adoptée par la 23ème session à Malabo, le 27 juin 2014.

[20] PEREIRA B., Op cit., p. 388.

[21] GHERNAOUTI S., *Cybercriminalité, les nouvelles armes de pouvoir*, 2ème Ed., PPUR, 2017, p. 12.
[22] KEMPF O., *Introduction à la cyber stratégie*, Paris, 2012, p. 14.

stimuler ce type de comportement dans le but d'accompagner leurs intérêts stratégiques.

Si les 14.000 guerres répertoriées depuis le début de l'histoire étaient basées sur des causes multiples, notamment, les rivalités coloniales entre grandes puissances, ambitions territoriales, logique agressive des alliances, course aux armements, fièvre nationaliste, esprit de revanche etc. ; à l'ère du numérique, la guerre moderne sera virtuelle, mieux « cyberguerre » aux conséquences pires qu'un tsunami qu'on ne peut comparer aux formes des guerres traditionnelles,[23] au vu de l'intensité de formes de violences exercées et des armes qui y sont employées.

Aujourd'hui la technologie avance à une vitesse de croisière, une guerre ne doit plus être définie au regard des armes classiques utilisées, puisque celles-ci ne font presque plus l'affaire. En effet, la maitrise des technologies de l'information et des communications remplace peu à peu les causes de guerres traditionnelles. Cette nouvelle perspective mondiale conduit à affirmer que dans l'espace cyber, la guerre l'information présente le visage de la guerre moderne[24] où les conflits sont désormais axés sur l'acquisition du savoir et sa maitrise.

A cette allure, la société actuelle représente un double défi : à savoir utiliser la connaissance comme levier du développement et maitriser son usage dans les rapports de force globaux et locaux. Ainsi, nous sommes presque dans un monde où l'influence des outils de communication numériques fait jeu égal avec le pouvoir des armes dites traditionnelles.

Prenant ce fléau à-bras-le-corps, le Président américain a signé un Décret incitant les entreprises privées à partager leurs informations sur les risques d'attaques. Une décision qui encourage la création « d'organisations de partage et d'analyse d'informations », lesquelles peuvent être formées en tant qu'entités à but lucratif ou non, et ce afin d'améliorer la collaboration sur le cyber sécurité. La Maison Blanche a aussi souligné que ce décret vient s'ajouter à la proposition législative formulée par le gouvernement conçu pour améliorer la sécurité informatique des services publics, du secteur public et des particuliers. La volonté de contraindre les entreprises à coopérer avec le gouvernement sur des intrusions informatiques montre l'ampleur du fléau des cyberattaques et la volonté du gouvernement américain de contrer ce phénomène.

Cette cybercriminalité révèle l'importance de sécuriser les systèmes d'information afin d'éviter au mieux les risques d'intrusion dans les systèmes informatiques dont les conséquences peuvent être importantes. Malgré la coopération avec le Gouvernement, les Entreprises, les petites comme les plus grandes, doivent mettre en œuvre tous les moyens nécessaires pour lutter contre ces instructions informatiques en maitrisant les risques liés à la mise en place d'une solution permettant de les protéger contre les attaques informatiques.

Le cyber offensif, la cyberdéfense, le cyber espionnage sont ainsi des domaines d'activités ayant pris une ampleur croissante pour les services étatiques comme tous les acteurs non étatiques (entreprises, particuliers). Les premiers enseignements de ce nouvel espace de rivalités révèlent, contrairement à une idée acquise, qu'Internet ne crée pas une révolution fondamentale des procédés d'opposition. Il est tout simplement le prolongement de luttes de pouvoir existantes, dans une autre dimension. L'utilisation du télégraphe au 19ème siècle donnait une avance technologique à la puissance britannique, mais n'a pas révolutionné les conditions de rivalités entre États. Elle a favorisé des procédés de luttes et de concurrence qui étaient déjà mis en œuvre. Le cyberespace présente

[23] XAVIER L., *Op. cit*, p. 90.
[24] Ibidem, p. 91.

une dynamique similaire. Il est interdépendant des espaces physiques (le câble sous-marin en fibre optique peut être coupé par exemple), suit la même logique de course à l'armement et connaît une militarisation accrue comme d'autres secteurs caractérisant la puissance…

En réalité, une Cyberattaque est une attaque informatique menée, tant par des personnes physiques, morales que des Etats, uniquement dans et par le Cyberespace avec comme objectif d'exploiter les failles pouvant émerger ou résulter de l'accès d'un usage au cyberespace[25]. Le but poursuivi doit être celui de perturber, neutraliser, détruire ou contrôler de façon malveillante l'infrastructure informatique de la cible ou d'en détruire l'intégralité des données ou voler les informations protégées[26]. L'attaque cybernétique devient étatique toutes les fois qu'il y a l'implication de celui-ci par parrainage, ou lorsqu'elle est lancée directement par un Etat ou pour son compte, à son instigation ou en raison de sa passivité délibérée, à partir du territoire dudit Etat, contre un environnement informatique ou une infrastructure située sur un territoire d'un autre Etat[27].

Par ailleurs, si lors de la Conférence de Bruxelles de 1874, les idées recommandées étaient d'une part, d'adopter des dispositions ayant pour objet de définir et de régler les usages de la guerre sur terre, dont la rédaction était inspirée par le désir de diminuer les maux de la guerre, autant que les nécessités militaires le permettent, d'autre part, de stipuler que les belligérants n'avaient pas un droit illimité quant au choix des moyens de nuire à l'ennemi[28], d'attaquer ou de bombarder, par quelque moyen que ce soit, des villes, villages, habitations ou bâtiments qui ne sont pas défendus[29], attaquer les établissements fixes, les formations sanitaires mobiles du Service de santé[30], attaquer les aéronefs sanitaires[31] etc. Il devient aussi nécessaire pour le Droit international de déterminer les limites à ne pas franchir dans le cadre des cyberattaques étatiques ou de cyberguerre.

Même si la détermination juridique d'une cyberattaque comme une agression armée n'est ni chose aisée et ne fait ni l'unanimité au motif que, jusque-là les conséquences des cyberattaques étatiques n'ont pas encore atteint le seuil d'une guerre réelle au regard de leur basse intensité, il en demeure pas moins vrai que les infrastructures vitales d'un Etat méritent une protection internationale juridique en cas d'attaque cybernétique, afin d'éviter la récidive d'Estonie et Géorgie, où c'est toute une vie sociale qui s'était arrêtée pendant quelques longues heures. Plusieurs heures sans connexion dans un pays où plus de 80% de la population vit au dépend de l'internet, les conséquences sont arithmétiquement pires par rapport à celles d'une guerre classique. Mais, dans le cas de la Géorgie, les cyberattaques lancées de manière concordante avec le rythme des manœuvres militaires russes[32] clouent au sol l'aviation militaire géorgienne, soit une flotte de dix-huit appareils.

Dans tous les cas, que ça soit une attaque classique dite « agression armée » ou l'attaque moderne, appelée « cyberattaque », c'est l'homme qui en est toujours victime, directement ou pas, étant donné que c'est lui qui est au centre de tout intérêt.

C'est pour cela que Katie Hafner et Matthew Lyon soutiennent que l'Internet aurait été inventé « ...pour défendre la sécurité nationale américaine face à une

[25] AKOTO E., Les cyberattaques étatiques constituent-elles des actes d'agression en vertu du droit international public ? Revue de Droit d'Ottawa, 2014-2015, Vol 46 n°1, pp23.
[26] Idem
[27] Ibidem, p10
[28] Art 22, Règlement de la Haye concernant les lois et coutumes de la guerre sur terre
[29] Art 25, Idem.
[30] Art 19 Convention de Genève pour l'amélioration du sort des blessés et des malades dans les Forces armées en campagnes du 12 aout 1949.
[31] Art 36 Idem.
[32] JOUBERT V. et SAMAAN J.-L., « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE », in *Hérodote*, n° 152-153, 2014/1, p. 265.

attaque nucléaire [33]», c'est-à-dire, conçu non pas pour un intérêt imaginaire mais bien réel et palpable.

A. Attaque contre l'OTAN

Tout au long du XXème siècle le Kosovo a été un foyer de tensions et de violence entre la population de souche albanaise de ce territoire et les Serbes. Les atrocités dans la crise suscitèrent l'intervention des forces armées de l'OTAN, le 24 mars 1999[34].

A cause de l'immense frappe aérienne de l'OTAN pendant cette guerre, les activités serbes, opposées aux activités de l'alliance s'attaquent au site de l'alliance par l'effacement de la page Web SHAPE et par « déni de service »[35].

B. Attaque contre l'Estonie

En 2007 l'Estonie[36] a connu une série de cyberattaques qui visaient les sites web d'organisations estoniennes, tels que le parlement estonien, les banques, les ministères, les journaux et les diffuseurs à la suite des désaccords de ce pays avec la Russie en ce qui concerne le déplacement du Soldat de bronze, une statue d'un soldat en uniforme soviétique située dans un cimetière militaire à Tallinn[23].

En effet, le 27 avril 2007 l'Estonie décide de déboulonner un monument à la gloire de l'armée rouge, acte qui fut perçu en Russie comme un outrage, au pire une provocation et les réactions ne se sont pas fait attendre. Plusieurs attaques informatiques dirigées contre des banques, des journaux, de nombreux sites gouvernementaux ou partis politiques estoniens furent signalées. En représailles, plusieurs sites russes en furent visés.

Un affrontement qui mit en mal les relations diplomatiques de deux Etats malgré qu'au terme de cette tension diplomatique, c'est une personne seulement, un Estonien d'origine russe, qui fut accusée et condamnée pour avoir « provoqué une cyberguerre » contre l'Estonie[5]. Vu comme un sujet sans précèdent, cet assaut fit l'objet d'études intensives par certains observateurs et planificateurs militaires, puisque considéré comme la plus grande cyberguerre depuis Titan Rain[37].

Cet événement a conduit à la création le 14 mai 2008 du Centre d'excellence de cyberdéfense coopérative de l'OTAN, établi à Tallinn avec comme le statut d'organisation militaire internationale dont la mission consiste à renforcer les capacités, la coopération et le partage d'informations entre l'OTAN, ses pays membres et ses partenaires dans le domaine de la cyberdéfense grâce à l'éducation, à la recherche, au développement et aux enseignements tirés et à la consultation.

La situation estonienne est atypique du fait qu'elle démontre que l'informatique a été utilisée pour qu'une nation s'attaque à une autre. A cet égard, le recours à l'intelligence artificielle, soit pour soutenir une guerre réelle, soit pour faire la guerre cybernétique devient vraisemblable.

Dans tous les deux cas, les dégâts, sont non moins différents même, si l'affrontement se déroule sur un terrain nouveau « virtuel » encore moins, les conséquences ne sont pas forcément immatérielles que l'EU et l'OTAN considèrent comme un nouveau domaine

[33] HAFNER K. et LYON M., *Where Wizards Stay Up Late : the Origins of the Internet* (New York, 1996), p. 10.
[34] DJAMCHID MOMTAZ, l'intervention d'humanité » de l'OTAN au Kosovo et la règle du non-recours à la force, 31-03-2000, Article, Revue internationale de la Croix-Rouge, 837, consulté le 21/3/2021 sur www.icrc.org.
[35] BALLARIN S., L'OTAN dans la cyberguerre : stratégie globale et capacités opérationnelles, *Diploweb.com : la revue géopolitique, 12 avril 2017 sur*
[36] Estonie : Pays pionnier de l'Union européenne (UE) en matière d'utilisation de l'Internet, soit 46% de foyers connectés dont 99 % des transactions bancaires sont faites via Internet ; le budget de l'Etat est accessible en ligne, et les députés du Parlement ont été élus, via la Toile.
[37] TITAN RAIN est le nom qui a été donné à une série d'attaques informatiques coordonnées visant des systèmes d'information américains. Ces attaques ont débuté en 2003 et auraient duré 3 ans (*Bradley Graham, « Hackers Attack Via Chinese Web Sites » [archive], Washington Post, 25 août 2005).* L'action principale des attaques semble avoir été la récupération massive d'informations auprès d'organismes variés, y compris militaires (*Nathan Thornburgh, « Inside the Chinese Hack Attack » [archive], Time, 25 août 2005*) ou via des contractants tels que Lockheed Martin, Sandia National Laboratories, Redstone Arsenal ou la NASA (« *What are Titan Rain Attacks?* » [archive], wegilant.com, 10 octobre 2013).

opérationnel[38].

Cette crise avec toutes ses ramifications, fait en sorte qu'elle soit, à tort ou à raison, qualifiée de « cyberguerre ». Raison pour laquelle, il devient nécessaire pour la communauté internationale d'en tirer de leçon.

Pour faire face aux cyberattaques dans un contexte de crise, l'UE et l'OTAN ont mis en place une stratégie euro-atlantique en matière de défense par la mise en commun d'un certain nombre d'informations liées à la cyberdéfense. Une démarche qui ne cesse de se heurter aux Etats en tant cyber puissance dans la protection d'informations.

Puisque dans cette offensive, l'Estonie voyait la main du Kremlin à partir des ordinateurs officiels russes, il y avait lieu de craindre le premier conflit international électronique dont la solution ne peut découler que d'un Droit international mis à jour qui tient compte de la nouvelle technologie dans le règlement des différends.

C. Attaque contre la Belgique

En 2014 le système informatique des affaires étrangères de la Belgique fut attaqué par un logiciel espion baptisé « Snake », lequel, une fois téléchargé sur un ordinateur de l'Ambassade de Belgique en Ukraine, la totalité du réseau diplomatique belge fut infecté conduisant à la suspension du réseau concerné pendant dix jours[39].

D. Attaque de l'Israël

L'attaque des sites Web israéliens en 2014 au mois de juillet avait comme objectif d'infiltrer les systèmes informatiques qui contrôlent les infrastructures en vue de perturber le transport des trains, de l'eau, de l'électricité ou de tout autre système vital, sachant qu'en Israël comme dans certains d'autres pays, les grands réseaux d'infrastructures sont pilotés par ordinateur.

E. Attaque des USA

Ces dernières années les cyberattaques sont de plus en plus nombreuses et sont désormais révélées au grand public. En 2013, l'affaire SNOWDEN-PRISM avait déjà suscité la polémique en révélant l'accès aux données des plus grands acteurs du web et des Etats par la NSA et le FBI.

Dans une large interview accordée à Wired, Edward évoque le programme de la NSA « Monstermind » : un outil de cyberguerre capable de réagir sans intervention humaine, mais avec un risque d'erreur de cibles[40]. Ce programme serait automatiquement activé en cas de tentatives d'attaques contre les Etats-Unis. Selon lui, cet outil a été construit en partie pour analyser le trafic Internet et détecter des cyberattaques et les bloquer. Mais il dispose aussi « d'un côté offensif automatique sans intervention humaine ».

En 2014, les Etats-Unis avaient accusé la Chine d'espionnage et de vol de secrets économiques.

Plus récemment en 2016, il a été fait état d'une cyberattaque russe qui a déstabilisé les élections présidentielles américaines en publiant des e-mails des dirigeants du parti démocrate en faveur d'Hillary Clinton au détriment des autres candidats.

Alors que ces attaques informatiques étaient hier de simples piratages isolés, elles apparaissent désormais

[38] Le Centre d'excellence coopératif de cyberdéfénse de Tallinn définit le « cyberdomaine » comme un « espace de mise en relation de données numériques qui utilise le spectre électronique ou électromagnétique pour stocker, classer, traiter et transférer des données et des informations au travers de réseaux de télécommunications » (cité par G. Lasconjarias, « L'Otan et le domaine opérationnel cyber », dans TAILLAT S., CATTARUZZA A. et DANET D., *La Cyberdéfense. Politique de l'espace numérique*, Paris, 2018, p. 151) : voir HOORICKX E. L'implication de la Belgique dans le cyber stratégie euro-atlantique : état des lieux et défis à relever de l'Institut Royal supérieur de Défense : sécurité et stratégie n°139, Fév. 2012, p. 6 ; sur le site internet : www.irsd.be. Consulté le 21 mars 2021.

[39] XAVIER L.., *Op cit*, p. 94.

[40] CHEMINAT J., 13 août 2014, 18 :22, « Cyberguerre : Edward Snowden dévoile l'outil Monstermind de la NSA », https://www.silicon.fr/cyberguerre-edward-snowden-devoile-loutil-monstermind-nsa, consulté le 16/3/2021, 4 :59.

comme des attaques quotidiennes au point de se demander si nous ne sommes pas à l'aune d'une vraie « cyberguerre » qui doit intéresser le Droit international.

F. Attaque de la Géorgie

Le 28 octobre 2019, une cyberattaque à grande échelle a été menée contre les sites web, les serveurs et les systèmes d'exploitation de l'administration du président de la Géorgie, des tribunaux, de plusieurs Assemblées municipales, des organismes publics et privés ainsi que des organes de presse. Dans cette crise où près de 1500 sites (publics et privés) étaient visés, la Géorgie et ses alliés ont pointé du doigt le renseignement militaire russe (GRU).

Ces illustrations démontrent que l'espace cybernétique est un champ de bataille hors pair pour des attaques plus organisées. Ces nouvelles pratiques s'apparentent à l'arme de destruction massive (ADM) du 21ème siècle dont la différence réside au niveau de l'utilisation d'ADM traditionnelles et les cyberattaques d'infrastructures. En effet, les premières relèvent des Etats, qui sont les seuls à détenir la capacité de mettre en œuvre une arme nucléaire, bactériologique ou chimique, alors que les dernières, même de groupuscules disposent des compétences techniques leur permettant de lancer une cyberattaque d'infrastructures dont les précédents n'en sont pas moins éloignés.

Au regard des bouleversements dus à la mondialisation, la protection des frontières matérielles d'un Etat ne suffit plus, à l'instar de la France qui a introduit dans sa politique et stratégie de défense nationales, la sécurisation permanente des espaces, réels et virtuels[41].

La réalité actuelle fait qu'on ne peut pas parler des nouveaux défis du droit international sans faire allusion à l'internet, fil conducteur des progrès technologiques à la base des bouleversements des valeurs sociales traditionnelles. Ces exemples non limitatifs démontrent que le cyberespace est l'un des nouveaux domaines de confrontation dans le cadre de la stratégie indirecte qui se situe en dehors du champ de guerre réelle.

En effet, les cyberattaques lancées quotidiennement contre les intérêts étatiques ou des Entreprises par des unités spécialisées ou des groupes de hackers non étatiques constituent des preuves suffisantes que, le cyberespace est un nouvel espace de bataille, avec ses procédés et ses tactiques propres, parallèlement aux autres espaces physiques (terre, mer, air). Ceci montre que, pour renverser les régimes adverses, les belligérants, étatiques ou non-étatiques recourent aux moyens détournés se trouvant en dehors du champ de la guerre réelle[42], notamment, la cyber délinquance, la cybercriminalité[43], mieux la cyberguerre. A ce titre, Xavier affirme que, le cyberespace constitue un théâtre d'opération pour les affrontements modernes[44], un nouvel enjeu géopolitique pour les États depuis les années 200045, de fois en violation des Conventions de Vienne de 1961 et 1963.

En ce début du 21ème siècle, le rythme des progrès technologiques s'accroît toujours au point d'être exploités à des fins belliqueuses, ce qui constitue des nouveaux risques majeurs pour les nations. De plus, l'avènement de la communication de masse et notamment l'extraordinaire puissance de l'outil Internet, offre aux acteurs de toute nature un accès aux informations et aux savoirs les plus divers, conférant ainsi à la technologie un certain pouvoir égalisateur. Cette évolution met les

[41] Livre blanc, Défense et sécurité nationales, France 2013, p. 47.

[42] TENEN BAUM E., Le piège de la guerre hybride, octobre Paris 2015, ifri, Laboratoire de Recherche sur la défense ; focus stratégique n°63. Tiré sur www.ifri.org, consulté le 25 avril 2021.

[43] COULLUME-LABARTHE J., Nouvelles conflictualité et defense modern : l'approche globale, 2008/4 n°32/pages 95 à 107. Article en ligne : https : www.cairn.info/Revue-raisons-politiques-2008-4-page-95.htm, consulté le 25 avril 2021

[44] Idem, p. 89.

[45] BOULANGER P., *Dans Géopolitique des médias* (2014), pages 263 à 294, Mis en ligne sur Cairn.info le 09/03/2016, consulté le 16/3/2021, 5 :30

nations en prise avec des acteurs d'une grande diversité recourant à des formes de conflictualité nouvelles. Les confrontations symétriques ainsi que la guerre entre États ne sont pas à exclure mais le plus souvent il faudra faire face à de nouveaux acteurs aux objectifs irréconciliables avec les valeurs qui fondent nos sociétés occidentales.

Selon Nicola Arpagian, les évènements dont sont victimes ces Etats illustrent « la première génération de cette forme annoncée de cyberguerre, lorsque les technologies de l'information et de la communication sont mises à contribution pour appuyer un jeu diplomatique et géopolitique bien réel »[46]. En effet, toutes ces attaques informatiques contre les intérêts étatiques vitaux, fait croire que l'Internet peut être utilisé pour agresser virtuellement un autre Etat et être une source de conflit entre deux pays. Cependant, la question est celle de savoir si les Cyberattaques étatiques ci-dessus sont au sens du Droit international, les actes internationalement répréhensibles pour lesquels l'Etat victime peut recourir à la force armée dans le cadre de la légitime défense. La précision à apporter est que, même si les attaques Cybernétiques n'impliquent pas l'emploi direct de la force armée, il en demeure qu'elles ne sont pas moins contraires à l'esprit et la lettre de l'article 2 (4) de la Charte des Nations-Unies. Même si les conséquences des Cyberattaques étatiques ne sont pas toujours matérielles, leurs actes demeurent en violation des normes internationales, puisque semblables aux violences dirigées contre un État.

Eveline AKOTO[47], assimile aux actes de subversion commis à des fins agressives constitutifs d'agression indirecte, le fait pour un Etat de s'attaquer par des procédés informatiques à un autre. Tel est le cas en l'occurrence, où à cause des cyberattaques les Etats victimes (Estonie et Géorgie) étaient empêchés d'exercer leur autorité sur le cyberespace relevant de leur juridiction.

Au sujet du recours à la force, « conquérir ou être conquis » était une loi de jungle qui régissait les rapports entre entités politiques anciennes, par nature méfiantes et hostiles vis-à-vis de leur entourage ; une attitude défavorable aux petits Etats ayant une triste destinée[48]. Pour mettre fin à ce mode de vie egocentrique et permettre à l'Organisation d'atteindre les objectifs qu'elle s'est assignés depuis le Pacte de la Société des Nations[49], l'article 2 de la Charte fut mis sur pied[50]. Cette disposition de la Charte dispose en son paragraphe 4 que : « les Membres de l'Organisation s'abstiennent, 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. ». Bien avant 1945, lors de la première conférence en 1907 il fut adopté une Convention pour le règlement pacifique des conflits internationaux dont l'objectif était « de prévenir autant que possible le recours à la force dans les rapports entre les Etats »[51].

Au cours de cette même conférence, il fut adopté la Convention Drago-Porter qui interdit également aux Etats de recourir à la force pour recouvrer des dettes si l'Etat débiteur ne rejette pas l'offre de règlement arbitral et s'engage à respecter la décision[52]. Bien que modeste dans ses ambitions, cette Convention n'en demeure pas moins marquante dans la mesure où elle est venue limiter aussi

[46] ARPAGIAN N., *la cyber sécurité*, Que sais-je ?, Paris, 2010, p. 25.
[47] AKOTO E., Op. cit, p23

[48] KEBA M., *Charte des Nations-Unies, commentaires articles par articles*, Economica-Bruylant, Paris Bruxelles, 2014, p. 96.
[49] Ces objectifs consistaient à fonder une Société internationale chargée du maintien de la paix et de la sécurité internationales, du développement des relations amicales entre les nations et de la réalisation de la coopération internationale tout en constituant un forum où s'harmonisent les efforts des Etats.
[50] KEBA M., *Op. cit.,* p. 83.
[51] Article 1er Convention pour le règlement pacifique des conflits internationaux. Conclue à La Haye le 18 octobre 1907.
[52] Article 1er de la convention (II) concernant la limitation de l'emploi de la force pour le recouvrement de dettes contractuelles adoptée le 18 octobre 1907 à La Haye.

le recours à la force dans le règlement des différends. Après la première guerre mondiale, cette question va logiquement connaître un regain d'intérêt. Si le Pacte de la Société des Nations impose à ses membres dans son préambule « certaines obligations de ne pas recourir à la guerre », il n'en interdit pas pour autant l'usage[53]. La doctrine renseigne que, le Pacte de la Société des Nations n'interdisait pas la guerre, mais la subordonnait à un préalable : l'arbitrage, le règlement judiciaire ou la délibération du Conseil. Mais, c'est le pacte Briand-Kellogg du 27 août 1928 qui s'en chargea en mettant la guerre hors-la-loi, par la prohibition solennelle du recours à la guerre comme moyen de politique nationale[54]. En effet, les Hautes parties contractantes ont condamné solennellement le recours à la guerre pour le règlement des différends internationaux et y ont renoncé en tant qu'instrument de politique nationale dans leurs relations mutuelles.

Pour contourner toutes ces règlementations du Droit international traditionnel, les acteurs étatiques et non-étatiques recourent aux cyberattaques ou autres moyens technologiques pour obtenir le même résultat.

En effet, c'est en raison de leur caractère très subreptice que les cyberattaques remettent en question les notions traditionnelles du droit international, notamment celles de frontières[55], étant par ailleurs coutumièrement inviolables. Alors que, bien que menées dans le cyberespace, les cyberattaques peuvent produire des effets aussi bien cinétiques que non électroniques à l'extérieur du cyberespace, ceci pouvant être le but exact recherché par l'attaquant[56]. Les Cyberattaques et les nouvelles technologies dites « l'intelligence artificielle » remettent également en cause les notions classiques de la guerre.

Eveline Akoto estime que, même s'il est difficile d'estimer les conséquences de telles attaques sur l'économie, la santé ou la sécurité publique d'un État, il ne fait aucun doute qu'une interruption simultanée des réseaux de distribution d'eau et d'électricité, couplée à une perturbation des services bancaires et financiers, sur toute l'étendue du territoire d'un pays pendant quelques heures, pourrait suffire à provoquer un vent de panique au sein de la population[57]. Selon l'auteur, étant donné que la plupart des cyberattaques ont résulté en des dommages peu apparents, elles ont une basse intensité qui explique la réticence des États à les qualifier de « faits de guerre ». Avec leur faible coût de mise en œuvre, les cyberattaques étatiques viennent toutefois bouleverser les modes traditionnels de conflits et remettre en question l'actuel cadre normatif du jus ad bellum.

Cette conception nous pousse à dire que, puisque les cyberattaques, désormais considérées comme un nouveau champ de bataille offrant aux Etats une autre façon de s'affronter sans en avoir l'air, elles demeurent, au-delà de leur basse intensité un défi auquel le Droit international fait face.

Le retard du Droit international à s'adapter aux réalités de l'heure a conduit les Etats-Unis à considérer que, un État victime a le droit d'entreprendre des actions militaires au titre de la légitime défense ou des représailles, en réponse à des cyberattaques prétendument commanditées par d'autres pays[58]. Pour le Général français Dominique Delawarde, il s'agit là des formes modernes de la guerre, celles qui évitent de faire appel aux moyens militaires et

[53] *Le Pacte interdit les guerres d'agression (article 10), le conflit ouvert pour contester une décision judiciaire ou arbitrale internationale (article 12 § 1) et la guerre décidée malgré une recommandation adoptée à l'unanimité du Conseil de la S.d.N. (article 15 § 4). Par ailleurs, avant de recourir à la guerre, les Etats devaient d'abord soumettre leur différend à l'arbitrage ou au Conseil de la S.d.N. puis respecter un délai de trois mois à compter de la décision arbitrale ou judiciaire ou du rapport du Conseil (article 12).*

[54] Art 1er du Pact Briand-Kellogg du 27 aout 1928 à Paris.

[55] AKOTO E., Op. cit, p4.

[56] Idem, p 5.

[57] Idem.,

[58] Ibidem.

permettent de l'emporter contre son adversaire sans risquer la vie des soldats[59].

A l'instar des guerres de l'information et économique, la guerre électronique peut aussi s'avérer extrêmement efficace et provoquer des dommages très importants chez l'adversaire. Pour preuve, en ce qui concerne le guerre économique, l'embargo sur les médicaments dont a été l'objet l'Irak, a causé la mort de plusieurs millions de femmes, d'enfants et de vieillards, mieux de personnes vulnérables qui ne pouvaient pas être soignées. Une situation qui a été qualifiée de guerre non déclarée[60].

II. Le Droit international face aux cyberattaques

La Charte des Nations Unies, rédigée pour faire face aux dangers qu'impliquent les conflits de forte intensité, semble ne pas pouvoir répondre aux défis juridiques que présentent l'avènement et le développement fulgurant des nouvelles technologies[61].

En matière de cyberattaque, l'identification de l'auteur, personne physique ou morale, est techniquement complexe. Néanmoins, certains pays avancés dans le domaine du numérique sont d'avis que la victime étatique a le droit de recourir à la force en termes de légitime défense. Une telle réaction de la part d'un Etat, appel également l'intervention d'un Droit international public moderne capable de réguler le règlement des conflits armés opposant deux Etats souverains, résultant du cyberespace. Car, en cas de cyberattaque étatique, aux conséquences déshumanisantes, le Droit international public devra être à mesure de sanctionner les Etats délinquants.

Ce raisonnement est dû au fait qu'aux premières heures du Droit international public, les Etats n'avaient aucune idée des avancées que la technologie pouvait réaliser au sein de la communauté internationale. En effet, dans la mise en place des mécanismes juridiques qui régissent les relations étatiques, les nations souveraines et indépendantes qui composent la Communauté internationale avaient élaboré les textes qui les gouvernent en tenant compte uniquement des réalités d'avant internet. Cependant, avec le développement de l'informatique et son incursion vertigineuses dans tous les secteurs de la vie humaine, le problème peut se poser dans la manipulation des ordinateurs et être source de conflits entre Etats, mieux, un conflit cybernétique peut être à la base d'une guerre réelle entre deux Etats.

Dès lors que d'aucuns n'ignorent que la vie internationale ne peut continuer à être règlementée sur base des principes traditionnels sans avoir égard aux réalités actuelles qu'apporte l'internet, notamment la cybercriminalité à l'échelle internationale, touchant aux intérêts des Etats ou des Organisations internationales, la réforme du Droit international, mieux de son texte constitutionnel s'avère opportun. Aussi, si au plan du droit pénal interne, tel qu'en France, une législation adéquate est mise en place pour s'adapter aux évolutions de la criminalité[62], le Droit international traditionnel quant à lui n'est-il pas à mesure de sanctionner les personnes morales auteurs de la cyberdélinquance.

Au vu du fait qu'il est possible que les réseaux informatiques et l'information électronique puissent être utilisés pour commettre des infractions pénales et que leurs preuves soient stockées et transmises par le biais de ces réseaux, le Conseil de l'Europe a estimé qu'il était nécessaire de mener en priorité, une politique pénale

[59] GOYA M., Conflits et violences : vers de nouvelles formes de guerre ? Dans Revue internationale et stratégique 2020/2 (N° 118), pages 109 à 116 en ligne sur https://www.cairn.info, consulté le 30/3/2021.
[60] ROUSTEL D., « En Irak, des sanctions qui tuent », le Monde diplomatique, février 1999 sur https://www.humanite.fr, consulté le 31 mars 2021
[61] AKOTO E., Op Cir., p.199.
[62] Loi n°2004-204 de mars 2004 portant adaptation de la justice aux évolutions de la criminalité ; Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

commune destinée à protéger la société de la criminalité dans le cyberespace[63].

La résolution 73/266[64] de l'assemblée Générale de l'ONU relève en ce qui la concerne la nécessité de renforcer la coordination et la coopération entre Etats afin d'éviter à ce que l'informatique ne puisse être utilisée à des fins criminelles au risque de porter atteinte à l'infrastructure des Etats, nuisant ainsi à leur sécurité dans les domaines tant civil que militaire. Il en résulte que, les technologies numériques sont des technologies à double usage en ce qu'elles peuvent être utilisées à des fins aussi bien légitimes que malveillantes. Tel est également le sens de la Résolution 73/27 de l'Assemblée Générale relative au Progrès de l'informatique et des télécommunications et sécurité internationale, qui accueille favorablement les normes, règles et principes internationaux de comportement responsable des États.

Ces textes ont le mérite de démontrer que les nouvelles technologies de l'information et de la communication constituent le nouveau défi auquel fait face le Droit international, de sorte qu'il est plus que temps de s'y penche afin de prévenir les conflits à venir entre Etats. La doctrine considère que, le cyberespace étant un nouveau terrain de conflictualité en dehors de la terre, la mer, l'air et l'espace extra-atmosphérique, il est alors nécessaire d'étendre la notion de guerre et de conflit en droit international public[65].

A ce titre la question qui mérite d'être posée est celle de savoir si, l'Etat qui recours aux méthodes cybernétiques comme mode de règlement des conflits internationaux, viole-t-il l'article 2 § 4 de la Charte des Nations-Unies ?

L'évidence est que, les NTIC sont devenues prédominantes dans la vie des Etats, des Entreprises et des citoyens. En ce qui concerne les Etats, l'espace issu des NTIC appelé cyberespace, est devenu comme un espace où chaque Etat organise de manière souveraine son système de défense nationale. Alors que, le même système peut devenir vulnérable et faire l'objet d'attaque cybernétique de la part des autres Etats.

La difficulté de répondre à une telle préoccupation résulte du fait que la Charte des Nations-Unies est antérieure aux NTIC ainsi qu'à tous les évènements qui en résulte. Notamment, les cyberattaques, le cyberguerre et la cybersécurité. Ce qui est paradoxal, est que, le même texte en son article 2 § 4, interdit le recours à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout Etat, soit de toute autre manière incompatible avec les buts des Nations Unies.

Réforme de l'article 2 § 4 de la Charte

Guillaume le Floch[66], renseigne que, la règle de non recours à la force telle que considérée par la Cour Internationale de Justice comme une pierre angulaire de la Charte des Nations-Unies[67], a déjà fait l'objet d'un certain nombre de violations. Par ailleurs, toutes les interdictions et considérations qu'elle contient n'ont pas pu empêcher les différentes guerres que le monde a connu jusqu'à ce jour. Il s'agit notamment, de la deuxième guerre mondiale avec son cortège d'atrocités, celles d'Afghanistan en 2001[68], en Irak[69] et enfin celle qui est en cours en Ukraine[70].

[63] Convention sur la Cybercriminalité, Budapest, 23.XI.2001.
[64] A/RES/73/266, AG, 65ème séance plénière, point 96 de l'ordre du jour, du 22 décembre 2018
[65] BORAT-GENIES O., Existe-t-il un Droit international du cyberespace ? Hérode 2014/1, n°152-153, pages 201 à 220.
[66] FLOCH G., Le principe de l'interdiction du recours à la force a-t-il encore valeur positive ? *Revue internationale interdisciplinaire, Droit et Cultures, 57/2009-1, Interdit (s), Interdiction (s), p.49-76*.
[67] C.I.J., *Activités armées sur le territoire du Congo (République démocratique du Congo c. Ouganda),* arrêt du 19 décembre 2005, § 148.
[68] A la suite des attentats du 11 septembre, les Etats-Unis ont déclenché l'opération « liberté immuable » contre l'Afghanistan à partir du 6 octobre 2001.
[69] Le 20 mars 2003, une coalition de 49 Etats, menée par les Etats-Unis et le Royaume-Uni, est intervenue militairement en Irak sous prétexte de l'autorisation implicite du Conseil de sécurité.
[70] C.I.J., Allégations de génocide au titre au titre de la Convention pour la prévention et la répression du crime de génocide, Ukraine c. Fédération de Russie, Ordonnance du 16 mars 2022.

Ces violations nombreuses et fréquentes de l'article 2 § 4 en vedette conduisent certains auteurs à affirmer que la règle de l'interdiction du recours à la force a évolué voire n'existe plus. C'est le cas de Glennon, qui considère que, la règle de l'interdiction du recours à la force est tombée en désuétude et passée par conséquent de vie à trépas[71], une thèse que Guillaume ne partage pas[72]. Car, il considère que ces différentes transgressions à ce principe ne sauraient remettre en cause son contenu et sa valeur, puisque cette règle demeure un principe de droit positif nonobstant les différentes violations déplorées. Au vu de cette réalité indéniable, il propose la fortification du principe de l'interdiction du recours à la force, laquelle devra passer nécessairement par un approfondissement du système de sécurité collective. Proposition que nous soutenons en ajoutant, sur base de la dernière incise de l'article 2 § 4 de la Charte, la prise en compte des réalités des nouvelles technologies de l'information et de la communication. Ceci est d'autant plus vrai, puisque nous pensons que la règle interdisant le recours à la force armée, non seulement ne reflète plus le droit positif, mais aussi elle est en inadéquation parfaite avec les nouveaux défis auxquels fait face le droit international. Tel est le cas des cyber-évènements résultant des NTIC auxquels le droit international doit très vite s'adapter, puisque les gouvernements des pays membres des Nations-Unies, réunis le 26 juin 1945 à San Francisco n'y en avaient pas pensé.

L'analytique sémantique de l'incise de l'article 2 § 4 de la Charte démontre la nécessité de la fortification et l'adaptation tant souhaitées du principe de non recours à la force, du fait des nouvelles réalités actuelles liées aux NTIC et de l'amendement qui ne vient toujours pas.

En effet, si l'interdiction de recourir à la menace ou à l'emploi de la force, de l'article 2 § 4 de la Charte implique aussi les cyber opération dans la mesure où elles atteignent un seuil élevé d'agression armée en termes de degré, de niveau d'intensité et d'effets engendrés. A titre d'exemple : lorsque l'emploi de la force entraîne des pertes en vies humaines, des blessures aux personnes ou des dommages aux biens (protégés par le droit international humanitaire) au même titre que les dommages résultant d'une guerre classique ; il s'en déduit l'importance de l'application du droit des conflits armés internationaux dans les cyber opérations. Tel peut être le cas des cyber attaques étatiques.

Sur ce point, *le manuel de Talinn*, précise qu'une cyber opération peut constituer un recours à la menace ou à l'emploi de la force ou une agression armée ouvrant le droit pour l'Etat victime d'invoquer la légitime défense (conformément à l'article 51 alinéa 1 de la Charte), toutes les fois que son ampleur et ses effets sont comparables à ceux de l'emploi de la force non numérique[73] ;.

Ainsi, bien que le Manuel de Tallinn soit un document hautement scientifique et incontournable, mais puisqu'il n'a ni vocation pour devenir une doctrine juridique officielle de l'OTAN et est dépourvu d'un caractère contraignant, même à l'endroit des membres partenaires de cette Organisation ; à l'inverse un travail purement académique ayant vocation d'analyser et discuter le droit international applicable sur les cyber opérations, il est impérieux d'envisager la réforme du droit international en général, plus particulièrement la Charte ou l'amendement de son article 2 § 4 en vue d'éviter toute interpretation analogique abuse de la regle de non recours à la menace ou à l'emploi de la force.

[71] GLENNON M.., « How International Rules Die ? », *The Georgetown L.J.*, 2005, vol. 93/3, pp. 939-991.

[72] Selon Guillaume, La thèse de la « désuétude » du principe de l'interdiction du recours à la force doit cependant d'être écartée. Les différentes transgressions à ce principe ne sauraient remettre en cause son contenu et sa valeur. Le principe de l'interdiction du recours à la force demeure un principe de droit positif.

[73] Idem.

La numérisation de tous les domaines de la vie humaine indique que, au tant l'internet est devenu un instrument de guerre d'influence entre Etats ou Entreprises, au tant il peut l'être pour la transgression des règles de droit international. Le raisonnement le plus adapté est celui qui est fait par Xavier[74], lorsqu'il rappelle que la chute du mur de Berlin et la fin du bloc soviétique ont pu laisser croire à une évolution des rapports de puissance, laissant présager une fin de l'Histoire des conflits, alors qu'en réalité, seules les modalités de la guerre ont évolué, les costumes traditionnels du soldat se trouvent être transformés. Les principaux conflits géostratégiques existent toujours, ils se traduisent simplement par d'autres formes de représentation. Bien plus, l'auteur souligne, qu'avec 2.7 milliards d'internautes dans le monde, il n'est plus possible pour les Etats d'ignorer les conséquences d'actions conduites dans les cyberespaces. Notamment, l'attaque, l'espionnage, défense, l'espace virtuel dans lequel un ou plusieurs individus peuvent défier des entreprises, des organisations internationales ou des Etats.

La multiplication des conflits entre Etats à cause de la cybercriminalité, démontre que la régulation du cyberespace constitue un effort international où se croisent intérêts publics, privés et souverains[75]. L'analyse de l'évolution des menaces cybernétiques et des doctrines étatiques y répondant, ainsi que le cas particulier de la régulation des contre-mesures justifient cette nouvelle façon de voir les choses. La raison est simple, puisque face à l'avancée vertigineuse de la technologie, de l'intelligence artificielle ; les doctrines militaires doivent être revues, ou encore sont en train d'être revue, notamment par la course aux armements capables de faire face à la cybercriminalité avec ses corollaires : la cyberguerre, cyberdéfense, cyberattaque, etc.

Dans le cadre de cybercriminalité, il existe le programme tel que : le « Stuxnet »[76] un mystérieux ver informatique autrement appelé Advanced persistent threat (APT) conçu pour s'attaquer aux systèmes informatiques des industries nucléaires de certains pays. De telles cyber-attaques reproduisent le comportement d'une attaque complexe, intelligente, avec des capacités de raisonnement et de déclenchement de commandes autonomes ou pilotées à distance. En juin 2010, un code malicieux, capable d'établir une communication externe pour déclencher une instruction visant à paralyser et saboter l'installation nucléaire ciblée, fut introduit dans le logiciel d'un composant hardware de la firme allemande « Siemens » destiné à intégrer le système de contrôle et d'acquisition de données (SCADA) d'un site d'enrichissement d'uranium à Natanz, en Iran. Ses caractéristiques sont la programmation comportementale autonome ayant pour objectif de compromettre un système en y résidant de manière anonyme, ou en trompant la vigilance des systèmes de détection en augmentant leurs privilèges.

1. Le cyberespace au service des Etats

L'OTAN considère le cyberespace comme un champ de conflictualité dont le risque de connaître le cas de cyberattaque étatique devient de plus en plus accru pour les pays développés beaucoup plus présents sur les réseaux de leurs adversaires. Au départ, les Etats dits développés se connectent par souci de se mettre à la hauteur de la nouvelle technologie de l'information et de communication qui ne laisse personne indifférente. Mais, par souci de répondre aux défis sécuritaires actuels que représentent l'avènement et le développement fulgurant

[74] LEONETTI X., Op cit, p87

[75] BAUMARD P., la cybercriminalité comportementale : historique et régulation, France Octobre 2014, pp38-75, en ligne sur https://www.researchgate.net/publication/298417731, consulté le 02 mars 2021.

[76] Stuxnet est un ver informatique découvert en 2010 qui aurait été conçu par la NSA en collaboration avec l'unité israélienne 8200 pour s'attaquer aux centrifugeuses iraniennes d'enrichissement d'uranium. Le programme a été initié sous l'administration Bush et a continué sous l'administration Obama. Il fait partie de l'opération Olympic Games, et ses caractéristiques le classent parmi les APT sur https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, consulté le 02 mars 2021.

des nouvelles technologies, les intentions changent au fur et à mesure au point où chacun cherche à s'entourer des infrastructures technologiques nécessaires. Or, le fait de tout numériser augmente aussi le risque d'être exposé à une espèce d'attaque informatique. Plus on est connecté plus on est vulnérable, dit-on.

A cette allure, l'escalade d'une troisième guerre mondiale se profile être une cyberguerre à laquelle les Etats puissants se préparent déjà par l'acquisition des armements de la nouvelle technologie. A ce sujet, Eveline Akoto affirme que, les infrastructures informatiques sont devenues les points névralgiques de nos sociétés modernes puisque tout est maintenant numérisé : les entreprises privées, les administrations publiques, la gestion des trafics aériens, routiers et ferroviaires, les centrales électriques et de distribution d'eau et les nouvelles armes de guerre telles que les drones, fonctionnent toutes à l'aide d'ordinateurs connectés à des réseaux au maillage si diffus qu'ils exposent les États à une nouvelle menace polymorphe et particulièrement furtive capable de conduire à ce qu'elle qualifie de « cyberattaque étatique »[77].

En effet, dans son raisonnement l'auteur considère que, puisque les cyberattaques étatiques pourraient être sommairement décrites comme des offensives attribuables à un État et menées contre les réseaux informatiques d'un autre pays afin d'occasionner des perturbations dans le fonctionnement des activités et services publics ou privés de l'État cible ; ce qui provoque des désagréments pour le quotidien des ressortissants dudit pays. Elles présentent « deux types de préoccupations » : d'une part, les risques liés à l'attaque des « services essentiels au fonctionnement [d'un] pays ou à sa défense », et d'autre part, les enjeux et défis posés par « la protection des informations sensibles du point de vue politique, militaire ou économique, face à des techniques d'intrusion informatique de plus en plus sophistiquées ». Selon cet auteur, si la subversion et les conflits de basse intensité étaient les méthodes privilégiées des grandes puissances pendant la Guerre froide, l'acquisition progressive de l'arme nucléaire par de plus en plus de pays, a fait des cyberattaques étatiques l'outil parfait pour atteindre les mêmes objectifs d'hégémonie.

Pour preuve les États-Unis ont déclaré qu'ils pourraient entreprendre des actions militaires au titre de la légitime défense ou des représailles en réponse à des cyberattaques prétendument commanditées par d'autres pays. Une telle prise de position constitue à la fois la problématique de qualification d'une cyberattaque étatique en droit international et une nécessité pour que les normes juridiques internationales adaptées soient mises en place, d'autant plus que le cyberespace ne doit pas être le far West du Net échappant au droit international existant.

Une avancée dans le domaine international qui vaut la peine d'être signalée est le fait que le droit des conflits armés et les droits de l'homme s'y appliquent déjà au niveau européen. L'Union européenne a adopté en février 2013 la stratégie de cybersécurité et un projet de directive. Elle ne traite pas de la cyber-guerre mais se focalise sur la dimension privée de la cybersécurité. De même, L'ENISA (L'Agence européenne chargée de la sécurité des réseaux et de l'information) créée en 2004 dont la mission consiste à *assurer un niveau élevé de sécurité des réseaux et de l'information,* veille également sur la cybersécurité.

Dans la même perspective, en analysant la question du Droit international applicable aux cyber-opérations, François Delerue, indique qu'il est vrai que la vaste majorité des cyber opérations demeurent sous le seuil du

[77] OKOTO E., Op Cit., p. 3.

recours à la force et n'ont pas lieu dans le cadre d'un conflit armé et que, par voie de conséquence, ni *le jus contra bellum* ni le *jus in bello* ne leur sont applicables[78]. Néanmoins, aux vues du fait que chaque sphère de la société devient de plus en plus connectée, au point où le Droit international enregistre une hausse spectaculaire des opérations cybernétiques.

2. De la cyber-guerre

Face à l'incursion de l'internet dans les conflits armés, Marie-Loraine considère que, la *cyber-guerre n'est pas fondamentalement différente de la guerre matérielle* conventionnelle : *«* Une *cyber-guerre totale provoque des dégâts matériels et fait des victimes, soit par suite d'attaques lancées délibérément pour semer la destruction, soit à cause d'une dégradation (…) dans des domaines tels que le contrôle de la circulation aérienne, de la gestion des services d'urgence, de la gestion de l'approvisionnement en eau et de l'alimentation en énergie électrique ».* Le danger survient aussi car la cyber-guerre «*ne connaît pas de limites ni de distinction entre les cibles militaires et civiles* ». En conclusion « *La planification de la défense doit prendre en compte le monde virtuel si l'on veut avoir une chance de limiter les dégâts matériels dans le monde réel.* »[79].

Matthieu Mondoloni, le journaliste de France info dans ses analyses, indique que, en cas d'attaque contre la Syrie, la guerre ne se jouerait pas que sur le terrain du réel. Elle se jouerait aussi virtuellement, sur Internet. La menace de cyberattaques syriennes, appuyées par l'Iran ou la Russie, inquiète les Etats-Unis et ses alliés[80]. Ceci indique le rapport étroit qui peut exister entre le réel et le virtuel.

Conclusion

Les nouvelles technologies de l'information et de la communication sont à la base de la transformation de la vie en société et remettent en question le cadre normatif de *Jus ad bellum*[81]. Cette mutation sociale crée un espace nouveau, appelé « cyberespace » et donne naissance à la cybercriminalité dont les auteurs peuvent être des personnes physiques ou morales agissant derrière un ordinateur. Cependant, devenu partie intégrante de la société moderne, l'espace cyber est également devenu un nouveau terrain d'affrontement des Etats pour régler leurs différends en contournant les règles juridiques qui régissent leurs relations internationales.

Une situation qui fait du cyberespace un far-West puisque la Charte des Nations Unies, rédigée pour règlementer les relations internationales des Etats et faire face aux dangers qu'impliquent les conflits de forte intensité, ne semble plus, pouvoir répondre aux défis juridiques que présentent l'avènement et le développement fulgurant des nouvelles technologies, alors que la maxime « Ubi societas Ibi Jus » veut qu'il y ait le droit là où il y a la société.

Cet article plaide pour une élaboration des normes internationales qui tiennent compte de la spécificité des nouvelles technologies de l'information et de la communication. Car, le Droit international en vigueur est inadapté aux exigences numériques de la société actuelles du 21ème siècle. Il mérite donc d'être doté d'une Charte reformée, conformément à ses articles 108 et 109, en regroupant l'ensemble des dispositions qui incluent les réalités actuelles impliquant le recours aux cyber opérations dans le règlement des différends internationaux.

[78] DELERUE F., Analyse du Manuel du Tallin 2.0 sur le Droit international applicable aux cyber-opérations, études prospective et stratégique, novembre 2017, pp. 18-74…

[79] ATAMANIUK M.-L., Syrie, la cyberguerre, mis en ligne le 23 mai 2015, consulté le 15 mars 2021 sur https://obsweb.net/blog/2015/05/23/syrie-cyberguerre.

[80] MONDOLOLONI M., Syrie : la menace d'une cyberguerre, Publié le 29/08/2013 15h : 21. Mis à jour le 07/05/2014 16h : 22, https://www.francetvinfo.fr/monde/syrie-la-menace-d-une-cyberguerre, consulté le 16 mars 2021 à 4 :01.

[81] OKOTO E., Op Cit., p23.

Bref, il faut un Droit international inspiré des nouvelles technologies pour l'intérêt supérieur de l'humanité et des Etats.

References Bibliographiques

I. Instruments juridiques légaux

1. Convention (II) concernant la limitation de l'emploi de la force pour le recouvrement de dettes contractuelles adoptée le 18 octobre 1907 à La Haye.
2. Convention de Genève pour l'amélioration du sort des blessés et des malades dans les Forces armées en campagnes du 12 aout 1949.
3. Convention pour le règlement pacifique des conflits internationaux. Conclue à La Haye le 18 octobre 1907.
4. Convention sur la Cybercriminalité, Budapest, 23.XI.2001.
5. Convention de l'Union Africaine sur la cybercriminalité et la protection des données à caractère personnel, adoptée par 23ème session à Malabo, le 27 juin 2014.
6. Déclaration Universelle des Droits de l'Hommes du 10 Décembre 1948, Paris.
7. Pact Briand-Kellogg du 27 aout 1928 à Paris.
8. Règlement de la Haye concernant les lois et coutumes de la guerre sur terre.
9. Résolution 73/266, A.G., 65ème séance plénière, point 96 de l'ordre du jour du 22 décembre 2018.
10. Loi n°2004-204 de mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
11. Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

II. Ouvrages

1. ARPAGIAN N., la cyber sécurité, Que sais-je ?, Paris, 2010.
2. BAUMARD P., la cybercriminalité comportementale : historique et régulation, France Octobre 2014.
3. DELERUE F., Analyse du Manuel du Tallin 2.0 sur le Droit international applicable aux cyber-opérations, études prospectives et stratégique, novembre 2017.
4. FERAR-SCHUHL C., Cyber droit, le droit à l'épreuve de l'internet, 6ème édition Dalloz 2010.
5. GHERNAOUTI-HELIE S., La Cybercriminalité, le visible et l'invisible, Presses polytechniques et universitaires romandes, première édition 2009.
6. GHERNAOUTI-HELIE S., La cybercriminalité, les nouvelles armes du pouvoir, 2ème édition entement actualisées, PPUR Lausanne 2017.
7. HAFNER K. et LYON M., Where Wizards Stay Up Late: the Origins of the Internet (New York, 1996).
8. JOUBERT V. et SAMAAN J.-L., « L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE », in Hérodote, n° 152-153, 2014/1.
9. KEBA MBAYE, Charte des Nations-Unies, commentaires articles par articles, Economica-Bruylant, Paris Bruxelles, 2014.
10. KEMPF O., Introduction à la cyber stratégie, Paris, 2012.
11. OCHOA N., « principe de libre circulation de l'information-recherche sur les fondements juridiques d'internet », in HALSHS, 2016.
12. XAVIER L., Guide de cyber sécurité, Droits, méthodes et bonnes pratiques, "piratage en cours", l'Harmattan, Paris, 2015.

III. Articles et Revues

1. AKOTO E.**,** « Les cyberattaques étatiques

constituent-elles des actes d'agression en vertu du droit international public ? » in Revue de Droit d'Ottawa, 2014-2015, Vol 46 n°1.

2. BALLARIN S., « L'OTAN dans la cyberguerre : stratégie globale et capacités opérationnelles », Diploweb.com : la revue géopolitique, 12 avril 2017.
3. BAUMARD P., la cybercriminalité comportementale : historique et régulation, France Octobre 2014, pp38-75, en ligne sur https://www.researchgate.net/publication/298417731, consulté le 02 mars 2021.
4. BORAT-GENIES O., Existe-t-il un droit international du cyberespace ? Hérode 2014/1, n°152-153.
5. BOULANGER P., Dans Géopolitique des médias (2014), pages 263 à 294, Mis en ligne sur Cairn.info le 09/03/2016.
6. CHEMINAT J., « Cyberguerre : Edward Snowden dévoile l'outil Monstermind de la NSA », 13 août 2014.
7. CHAMPETIER DE RIBES V., l'Estonie un Etat numérique performant, in Revue civique : http://revuecivique.eu
8. COULLUME-LABARTHE J., Nouvelles conflictualité et défense moderne : l'approche globale, 2008/4 n°32.
9. DJAMCHID MOMTAZ, « l'intervention d'humanité » de l'OTAN au Kosovo et la règle du non-recours à la force, 31-03-2000, in Revue internationale de la Croix-Rouge, 837.
10. DOUZET F., DESFORGES A., LIMONIER K., « Géopolitique du cyberespace : "territoire", frontières et conflits. CIST2014 - Fronts et frontières des sciences du territoire », in Collège international des sciences du territoire (CIST), Mar 2014, Paris, France.
11. GOYA M., Conflits et violences : vers de nouvelles formes de guerre ? Dans Revue internationale et stratégique 2020/2 (N° 118).
12. GRENNON M., « How international Rule die?», The Georgetown L.J., 2005, vol 93/3.
13. PEREIRA B., La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité, in Revue internationale de droit économique, 2016/3 (t. XXX).
14. ROUSTEL D., « En Irak, des sanctions qui tuent », le Monde diplomatique, février 1999.
15. RAYNAUD A., « Notion d'espace en géographie », in Travaux de l'Institut de Géographie de Reims, /année 1971/5.
16. TENEN BAUM E., Le piège de la guerre hybride, octobre Paris 2015, ifri, Laboratoire de Recherche sur la défense ; focus stratégique n°63.
17. THEVENET BERANGERE, L'ère Cyber et ses nouveaux enjeux, publié le 8 octobre 2018.
18. ATAMANIUK M.-L., Syrie, la cyberguerre, 23 mai 2015.
19. DELERUE F., Analyse du Manuel de Tallinn 2.0 sur le Droit international applicable aux cyber-opérations, études prospective et stratégique, novembre 2017.

IV. Documents divers

1. Livre blanc, Défense et sécurité nationales, France 2013
2. Revue internationale de la Croix-Rouge, 837.

* Université de Lubumbashi, Département de Droit Privé et Judiciaire. Kinshasa, Commune de Ngaliema, Quartier GB, 1Rue, 6 Villa, Camp Américain. gilbrethpaterne@yahoo.fr

Received 25 September 2022; Accepted 24 October 2022
Available online 25 October 2022