Remarques sur les Manuels de Tallinn (1.0 et 2.0) et le droit international applicable aux cyber-opérations

Ilène Choukri

Remarques sur les Manuels de Tallinn (1.0 et 2.0) et le droit international applicable aux cyber – opérations

Ilène Choukri

Docteur en Droit, Avocat aux Barreaux de Nice et de Paris

Désormais les moyens numériques ne sont plus seulement des éléments d'appoint aux menaces. Ils sont de plus en plus employés comme des moyens directs d'attaques pouvant entraîner des destructions matérielles. Comment faire face ? La genèse des Manuels de Tallinn permet de mettre en évidence la pertinence de la méthode adoptée - celle de la « soft law » -, pour répondre à des besoins de plus en plus mouvants, hétérogènes et complexes. En privilégiant la règle du consensus, les travaux de Tallinn contribuent à l'émergence de plusieurs axes permettant l'affirmation de l'applicabilité pleine et entière du droit international au cyberespace.

From now on, digital means are no longer only complementary elements to threats. They are increasingly used as direct means of attack that can lead to material destruction. How to deal with it? The genesis of the Tallinn Manuals makes it possible to highlight the relevance of the method adopted - that of "soft law" - to meet increasingly changing, heterogeneous and complex needs. By favoring the consensus rule, the Tallinn work contributes to the emergence of several axes allowing the affirmation of the full applicability of international law to cyberspace.

I. Introduction

La sécurité collective, telle qu'organisée par la Charte de Nations-Unies autour de la primauté des Etats et du multilatéralisme, est une réalité dynamique faite d'équilibres imparfaits entre stratégies, puissances et interdépendances. A ces rapports dialectiques et parfois conflictuels, le cyberespace a ajouté une nouvelle dimension, se révélant comme le siège privilégié de nouvelles formes de menaces à la sécurité. Ainsi, le « *Darkweb* » et le « *Deep Web* », véritables faces cachées du cyberespace, sont-ils devenus les creusets d'agissements illicites en tout genre, facilités par l'immatérialité, la déterritorialisation et l'anonymisation[1].

Désormais les moyens numériques ne sont plus seulement des éléments d'appoint aux menaces. Ils sont de plus en plus employés comme des moyens directs d'attaques pouvant entraîner des destructions matérielles. Une attaque en déni de service (« attaque *DDos* » : « *Distributed Denial of Service attack*")[2] peut ainsi, par la mise hors service des serveurs ciblés, avoir des conséquences graves sur certaines

[1] Yves Charpenel, *Le Darkweb, un objet juridique parfaitement identifié*, Dalloz IP/IT février 2017, p.71.

[2] https://www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DDoS.pdf - ANSSI

infrastructures critiques (tels que les Opérateurs d'Importance Vitale, OIV : hôpitaux, banques, ministères, médias, secteur de l'énergie, etc.)[3].

La cyber attaque est donc passée du statut d'instrument de nuisance à celui d'outil de combat à part entière. La liste des Etats qui ont dû faire face à ces opérations hostiles ne cesse de s'allonger. Force est de constater que le cyberespace systématise l'asymétrie des conflits. Avec peu de moyens, un groupe d'individus, bien informé et doté d'une agilité technologique efficace, éventuellement mandaté par un Etat, peut déstabiliser le fonctionnement d'une infrastructure sensible, d'un territoire donné ou même d'un pays tout entier. Les enjeux en termes de sécurité nationale sont donc particulièrement importants.

A cet égard, l'une des attaques les plus marquantes reste celle subie par l'Estonie en mai 2007, à la suite du cyber-assaut en déni de service (dite attaque *DDos*) contre les infrastructures vitales du pays, lequel a été partiellement paralysé. Certains analystes ont attribué cette action à la Russie sur la base d'éléments techniques et de contexte[4]. De même, l'utilisation du malware *Stuxnet* par les services de renseignement israélien et américain en 2007 a permis à ces derniers de perturber notablement le programme nucléaire iranien, en ciblant les centrifugeuses de la centrale de Natanz, au point de causer la destruction de plusieurs d'entre elles.

A l'échelle nationale, la cybermenace et les cyber conflits sont appréhendés de manière spécifique d'un Etat à l'autre, chacun se dotant d'un arsenal technologique et juridique qui lui est propre. En France, dans le sillage du Livre Blanc sur la défense et la sécurité nationale de 2013[5], la loi de programmation militaire (LPM)[6] a remis à niveau le code de la défense en prenant en considération la sécurité des systèmes d'information. La sanctuarisation des OIV et des systèmes d'information d'importance vitale (SIIV) se fait désormais sous l'autorité du Premier ministre[7]. Sur

---

[3] Voir l'attaque d'EDF en 2011 : https://www.usine-digitale.fr/article/attaque-ddos-le-cas-d-edf-et-ses-consequences-juridiques.N490969. Il existe d'autres déclinaisons d'attaques telles que la pratique du Ransomware qui consiste à utiliser un logiciel malveillant pour prendre en otage des données en les chiffrant ou bien en bloquant l'accès à un serveur par exemple. Les éléments "otages" ne seront "libérées" qu'au versement d'une rançon. Le retentissement des affaires "WannaCrypt" et "Not Petya" en mai 2017 permet de mesurer la proximité du risque de frappes numériques et la portée du danger inhérent (outre des institutions financières, certains hôpitaux britanniques ont été touchés). Voir Eve Tourny : Cybersécurité et attaques informatiques : les leçons à tirer de Wanna Cry et Not Petya, PSEI, n°7, 22 juillet 2017.

[4] Selon l'article 5 du Traité, « *les parties conviennent qu'une attaque armée contre l'une ou plusieurs d'entre elles survenant en Europe ou en Amérique du Nord sera considérée comme une attaque dirigée contre toutes les parties, et en conséquence elles conviennent que, si une telle attaque se produit, chacune d'elles, dans l'exercice du droit de légitime défense, individuelle ou collective, reconnu par l'article 51 de la Charte des Nations Unies, assistera la partie ou les parties ainsi attaquées en prenant aussitôt, individuellement et d'accord avec les autres parties, telle action qu'elle jugera nécessaire, y compris l'emploi de la force armée, pour rétablir et assurer la sécurité dans la région de l'Atlantique Nord.(…)*»

[5] Document disponible sur http://www.livreblancdefensetsecurite.gouv.fr.

[6] Article 22 de la loi 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 portant diverses dispositions concernant la défense et la sécurité nationale. Texte disponible sur https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id. ; voir également, Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense, JORF n°0075 du 29 mars 2015 page 5676.

[7] Eve Tourny : Cybersécurité et attaques informatiques : les leçons à tirer de Wanna Cry et Not Petya, PSEI, n° , 22 juillet 2017.

le plan européen, l'adoption de la Directive « NIS »[8] du 19 juillet 2016 accompagne les mouvements nationaux, structurant les stratégies de cybersécurité. Les Etats-Unis, pour leur part, n'ont pas hésité à placer leur politique dans une perspective historiquement orientée en agitant le spectre d'un « *Cyber Pearl Harbor* »[9]. Si les premières attaques sont finalement passées par perte et profit, compte tenu de la difficulté de désigner clairement leur auteur, l'affaire du piratage, de la divulgation et de la destruction de données confidentielles appartenant à la *Société Sony Pictures Entertainment* en décembre 2014, a marqué une étape nouvelle. La Maison Blanche a considéré que ces agissements constituaient une *« grave affaire de sécurité nationale »*, et a orienté explicitement ses accusations vers la Corée du Nord, marquant ainsi un tournant dans l'appréhension de la menace numérique. L'affaire de la captation et de la divulgation des données du *Democratic National Committee* (DNC)[10]

d'enjeu stratégique majeur.

L'algorithme n'est pas qu'un code immatériel : il peut causer des destructions majeures dans le monde matériel, sans avoir de limites frontalières, temporelles ou spatiales. Dès lors, toute réponse exclusivement nationale serait certainement vaine.

La formule « Code is law » pose la question de l'interdépendance entre la réalité physique et la réalité immatérielle et en particulier les règles pouvant régir cette interdépendance[11]. La question se pose avec une acuité particulière lorsqu'il s'agit du droit des conflits armés, aussi bien le *jus ad bellum* que le *jus in bello.* Le cyberespace risque de devenir une voie de contournement des règles du droit international et il apparait ainsi comme un facteur d'extension du domaine de la menace à la sécurité, y compris collective. Les règles qui encadrent l'emploi de la force dans les relations internationales, ne sont-elles pas remises en cause par la cybernétique ?

L'objectif poursuivi par les Manuels de Tallinn vise, précisément, à proposer des réponses possibles à cette gageure, en examinant dans quelle mesure les règles de droit international actuellement applicables à l'utilisation des armes conventionnelles en période de conflits peuvent être transposées aux menaces et aux armes cybernétiques. Cette analyse est d'autant plus complexe que l'emploi de la force digitale présente souvent un caractère hybride et que des critères aussi subjectifs que l'intentionnalité ou les seuils de gravité ont une importance décisive.

La genèse des Manuels de Tallinn permet de mettre en évidence la pertinence de la méthode adoptée : celle de la « soft law » pour répondre à des besoins de plus en plus mouvants, hétérogènes et complexes (II). En privilégiant la règle du consensus, les travaux de Tallinn contribuent à l'émergence de plusieurs axes permettant l'affirmation de l'applicabilité pleine et entière du droit international au cyberespace (III).

[8] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

[9] Propos repris par M. Leon Panetta, en 2012, en tant que Secrétaire à la Défense américaine.

[10] Assessing Russian Activities and Intentions in Recent US Elections, U.S. SENATE SELECT COMM.ON INTELLIGENCE2(Jan.6,2017),https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

[11] Voir Lawrence Lessig, « Code is law », Janvier 2000, Harvard Magazine, https://harvardmagazine.com/2000/01/code-is-law-html.

II. La genèse de la « méthode Tallinn » : le nécessaire recours à la « soft law ».

Les travaux du Manuel de Tallinn ont été lancés sous l'égide du Centre d'excellence de coopération de l'OTAN sur l'organisation de la Cyber-défense (Cooperative Cyber Defense Center of Excellence - CCDCOE)[12], réunissant un panel d'une vingtaine d'experts[13], issus de plusieurs Etats membres de l'OTAN et ayant conduit une réflexion avancée sur l'applicabilité du droit international aux cyber-conflits. La question se posait, en effet, pour l'OTAN de déterminer si une cyberattaque pouvait entrer dans le champ des « solidarités » du Pacte de l'Atlantique du Nord, et, le cas échéant, de quelle manière, eu égard aux difficultés particulières résultant de l'immatérialité et/ou de l'asymétrie de telles attaques. L'opération lancée contre l'Estonie en 2007 n'avait pas manqué d'interpeller l'Organisation et de faire de la cybermenace un enjeu de défense collective, nécessitant de clarifier les modalités de mise en œuvre de l'article 5 du Traité de l'Atlantique Nord[14].

Paru en 2013, après 4 années de travaux, la première version du Manuel de Tallinn[15] a attiré l'attention des observateurs du fait de l'ampleur et du détail des réflexions présentées. Les 95 règles dégagées par l'ouvrage passent en revue l'état du droit positif international pour le confronter aux défis des cyber-attaques susceptibles de constituer un usage prohibé de la force au sens de l'article 2 §4 de la Charte des Nations-Unies, voire une agression justifiant la mise en œuvre de la légitime défense au titre de l'article 51.

Les experts de Tallinn s'inscrivent dans la tradition de la méthode de la « soft law »[16], en recensant les points pour lesquels des règles de droit doivent être définies, avançant dans les débats par la voie du consensus, tout en relevant les avis dissidents ou les contradictions et en soulignant les zones grises. S'ils n'ont aucune portée juridique obligatoire et s'ils ne constituent pas les seules propositions sur la scène internationale[17], ces travaux représentent une offre notable de cadrage juridique utile à des problématiques en pleine expansion. Ils sont surtout, de nature à fournir une base pour l'adoption de futurs accords bilatéraux ou multilatéraux contraignants. Nul

---

[12] Ce panel réunit des experts mandatés par l'OTAN sous la direction juridique de Michaël Schmitt (USA) de l'Université britannique d'Exeter, Président et professeur au département juridique de l'United States Naval War College. Le centre a été créé en 2008 peu après l'attaque subie par l'Estonie.

La mission du centre est d': « *améliorer les capacités, la coopération et le partage d'informations au sein de l'OTAN, membres de l'Alliance et de ses partenaires dans le domaine de la cyberdéfense grâce à la recherche et le développement, la concertation.* »

[13] Le Comité International de la Croix Rouge fait partie des quelques organisations ayant pu suivre, en tant qu'observateur, certains travaux, à l'instar également de l'US Cyber Command.

[14] **Déclaration du sommet du Pays de Galles publiée par les chefs d'État et de gouvernement participant à la réunion du Conseil de l'Atlantique Nord tenue au pays de Galles les 4 et 5 septembre 2014 : « Les cyberattaques peuvent atteindre un seuil susceptible de menacer la prospérité, la sécurité et la stabilité des États et de la zone euro-atlantique. Leur impact sur les sociétés modernes pourrait être tout aussi néfaste que celui d'une attaque conventionnelle. »https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=fr**

[15] **Tallinn Manual on the International Law Applicable to Cyber Warfare, sous la direction de Michael N. Schmidtt, 7 mars 2013, Ed. Cambridge University Press**

https://ccdcoe.org/tallinn-manual.html -

[16] René-Jean Dupuy, *Droit déclaratoire et droit programmatoire : de la coutume sauvage à la « soft law »*, Dialectiques du droit international, Ed. Pedone, 1999, pp.107 et s.

doute que le cadre retenu traduit la volonté de l'OTAN de disposer d'une proposition juridique crédible le moment venu.

Le point focal des travaux du manuel de Tallinn réside dans la reconnaissance du caractère transposable du droit international au cyberespace. Il n'est donc pas question de faire émerger un droit « *sui generis* », à quelques spécificités près et une certaine continuité du *jus ad bellum* et du *jus in bello* reste préservée, semble-t-il[18]. Ainsi, dans le sillage de la Charte des Nations-Unies en ses articles 2 §4 et 51, la Règle n°13 du Manuel de Tallinn v.1.0 indiquait qu' : « *un État qui est la cible d'une cyberopération qui atteint le niveau d'une agression armée peut exercer son droit naturel à la légitime défense. Une cyberopération constitue une attaque armée selon sa dimension et ses effets* ». Cette reprise de l'acquis doit, néanmoins, se faire sans naïveté : la prise en compte de la dimension et des effets de l'attaque constitue un élément soumis à interprétation et nécessitera un éclairage par la pratique. En attendant, cette persistance d'importantes zones grises, a justifié la poursuite des travaux et des réflexions.

C'est ainsi, qu'en février 2017, une deuxième version a été publiée mettant à jour et approfondissant les précédents travaux[19].

Le prolongement des travaux de Tallinn vers une deuxième version met en évidence une consolidation de la démarche collégiale, corroborée par l'élargissement du panel d'experts à des Etats majeurs dans le cyberespace, qui avaient pu exprimer des réserves à la première mouture du Manuel. L'intégration d'un expert chinois en est certainement la manifestation la plus notable[20].

Malgré l'absence de caractère juridique obligatoire du Manuel de Tallinn, l'élargissement du champ de ses contributeurs est un élément qualitatif substantiel pour la portée de ces travaux qui se présentent comme une réflexion préparatoire à un éventuel texte juridique ou para-juridique (Résolution, Traité, Charte, Code de Bonne Conduite, etc.) multilatéral, pouvant faire référence au sein de la Communauté Internationale.

Si la continuité des réflexions de Tallinn vers une deuxième version confirme la difficulté de fixer des règles fermes (problématique du « hack back »[21], d'une cyber-légitime défense préventive, etc.), force est de constater également la flexibilité des règles internationales face à des enjeux qui n'auraient pas pu être anticipées à l'époque de leur élaboration. Engagés dans un travail préparatoire digne d'une

[17] Il convient également de relever les travaux de GGE - groupes d'experts gouvernementaux (GGE) de l'ONU sur la cybersécurité, composé de représentants d'une quinzaine d'Etats, dont les Etats-Unis, la Russie et la Chine, mandatés par le Secrétaire Général des Nations-Unies pour définir des recommandations. Dans le même sens que le Manuel de Tallinn, les travaux de ce groupe d'expert ont réaffirmé l'applicabilité du droit international tel que construit autour de la Chartes des Nations-Unies, dans le cyber-espace. Ainsi, le principe de souveraineté des Etats, les principes et les règles corollaires à ce dernier principe ainsi doivent-ils trouver leur plein effet dans le cadre des cyber-activités. Concomitamment, le GGE a également affirmé la pleine application du droit humanitaire international. Voir le rapport du 22 juillet 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[18] L'un des objectifs annoncés dans le cadre du manuel de Tallinn 1.0 est d'apporter « *un certain niveau de clarté aux difficultés juridiques complexes entourant les cyberopérations, avec une attention particulière à celles relatives au* jus ad bellum *et au* jus in bello », p.18.

19 **Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0, sous la direction de Michael N. Schmidtt, 2 février 2017, Ed. Cambridge University Press.**

https://ccdcoe.org/tallinn-manual.html -

[20] Le Manuel de Tallinn v.1.0 était considéré par une partie de la Communauté internationale comme étant le fruit d'une réflexion orientée par les anglo-saxons. Il convient de souligner la bataille diplomatique qui règne autour de l'établissement d'un texte de référence en matière de cyber-conflits. Ainsi, en septembre 2011, la Chine, la Russie, le Tadjikistan et l'Ouzbékistan avaient soumis aux Nations-Unies une proposition conjointe sur la bonne conduite sur Internet : https://web.archive.org/web/20120113233019/http://blog.internetgovernance.org/pdf/UN-infosec-code.pdf

[21] Ce terme renvoie à l'idée d'une riposte ou de représailles numériques.

codification du droit international du cyberespace, les experts du Groupe n'ont pas manqué d'établir une table des concordances entre les 95 règles initiales et les 135 nouvelles règles définies par la version de 2017. La publication de cette deuxième mouture met en évidence la persistance de la volonté d'une partie importante de la Communauté Internationale d'inscrire cet effort normatif sur le long terme, dans une démarche *de lege ferenda*, pour favoriser les bonnes pratiques, voire même l'émergence d'usages coutumiers.

Dans un ordre juridique verrouillé par la logique des puissances, cette approche souple, consensuelle pourrait être plus que louable et réellement salvatrice, eu égard à son potentiel d'intégration et de propagation rapides dans le champ effectif du droit.

III. Le Manuel de Tallinn 2.0 : l'affirmation de l'applicabilité du droit international au cyberespace.

Les règles et les opinions dégagées dans le cadre des travaux des manuels de Tallinn sont aussi riches que diverses. Il semble néanmoins possible de dégager trois axes principaux.

D'une part, le caractère incontournable de la souveraineté de l'Etat malgré les difficultés flagrantes posées par l'asymétrie de ces nouveaux conflits, est affirmée (III.1). D'autre part, le rôle de l'Etat apparaît également indispensable, face aux incertitudes induites par l'immatérialité et la déterritorialisation des cyber- menaces : ce rôle est particulièrement déterminant pour la mise en place d'un régime de responsabilité garantissant une sécurité juridique suffisante (III.2.). Enfin, dans le même mouvement de reprise de l'acquis du droit international (et notamment des principes dégagés par la jurisprudence de la Cour Internationale de Justice), le traitement de la problématique de la légitime défense face à la cyber- menace digitale constitue une des thématiques principales des réflexions de Tallinn : pour autant, de profondes incertitudes persistent. (III.3.).

III.1. La persistance du rôle de la souveraineté dans le cyberespace.

Dès sa première version, le Manuel de Tallinn consacrait le principe de souveraineté, s'inscrivant ainsi dans la continuité des décisions de la Cour Internationale de Justice. En effet, selon les experts, le cyberespace, tout immatériel et tout déterritorialisé qu'il soit, constitue une zone d'expression des souverainetés des Etats autour desquelles se structurent un certain nombre de règles. C'est donc la même pierre angulaire qui unirait le droit international classique et celui applicable au cyberespace. Il est vrai que le contournement du principe de souveraineté aurait hypothéqué substantiellement l'affirmation de l'applicabilité du droit international. On relèvera, d'ailleurs que les experts n'ont pas eu recours au concept de « souveraineté numérique » : c'est bien l'acception classique du concept de souveraineté, - telle qu'explicitée notamment dans le cadre de la sentence Iles de Palme et l'arrêt Detroit de Corfou[22] - qui est consacrée et qui a vocation à s'appliquer dans le cyberespace.

[22] *Voir la* Sentence arbitrale rendue le 4 avril 1928, par M. Max Huber, entre les Etats-Unis et les Pays-Bas, dans le litige relatif à la souveraineté sur l'île de Palmas (ou Miangas),

« La souveraineté, dans les relations entre Etats, signifie l'indépendance. L'indépendance, relativement à une partie du globe, est le droit d'y exercer à l'exclusion de tout autre Etat, les fonctions étatiques. » http://www.haguejusticeportal.net/index.php?id=10035.

Arrêt du « Détroit de Corfou » de la CIJ du 19 novembre 1949 : « Entre Etats indépendants, le respect de la souveraineté territoriale est l''une des bases essentielles des rapports internationaux », Recueil CIJ, 1949, pp.237 et s.

Cependant, les débats qui ont émaillé les travaux de la deuxième version du Manuel de Tallinn ont mis en évidence des résistances face à la réaffirmation de la primauté du principe de souveraineté. Ainsi, certains anciens membres du Département de la Défense américain, s'exprimant en leurs noms propres, ont défendu la position selon laquelle, dans le cyberespace, il n'existe pas d'interdiction absolue de violer la souveraineté d'un autre Etat[23], reléguant ce dernier principe au rang de simple corollaire des règles de non-ingérence et d'interdiction du recours à la force. Cette position ne constitue cependant pas la position officielle américaine. Les autorités américaines n'avaient d'ailleurs pas manqué de considérer que les attaques de la Corée du Nord à l'encontre de *Sony Pictures* ainsi que l'implication russe dans l'affaire DNC constituaient une atteinte à la sécurité nationale et une violation de la souveraineté américaine[24]. L'idée d'un déclassement du principe de souveraineté, dans le cadre du droit international applicable au cyberespace apparait dès lors difficilement envisageable [25].

Le respect de la souveraineté des Etats soulève néanmoins des problèmes particuliers. Les débats autour de la Règle n°4 du Manuel de Tallinn 2.0 portant sur la violation de la souveraineté ont mis en relief la difficulté posée par l'immatérialité des cyber-activités et, *a fortiori*, des cyber-attaques et par leur capacité à ignorer la notion même de territoire[26]. Dès lors, se pose la question de savoir à partir de quel moment, une cyber-attaque peut être considérée comme violant la souveraineté nationale.

La problématique s'exprime avec une particulière acuité en ce qui concerne les opérations de renseignement, d'observation ou d'espionnage, beaucoup facilitées par les outils numériques. Il est possible de considérer que leur constance et leur réitération est susceptible de porter atteinte à la souveraineté. Or, il existe un consensus selon lequel l'acte d'espionnage, en lui-même, ne constitue pas une violation du droit international et ne peut à ce titre relever que du droit national[27]. Dans le même sens, les experts de Tallinn 2.0 considèrent donc que les activités de cyber-espionnage ne constituent pas nécessairement une atteinte à la souveraineté nationale relevant du régime du droit international[28].

Pourtant, dans le cadre de son arrêt « Nicaragua contre Etats-Unis d'Amérique, à propos des activités militaires et paramilitaires du Nicaragua et contre celui-ci » en [29], la CIJ a également eu l'occasion de mettre en évidence le critère de la contrainte exercée sur les libertés pour caractériser une ingérence illicite au regard du droit international : « *l'intervention interdite doit donc porter sur des matières à propos desquelles le principe de souveraineté des Etats permet à chacun d'entre eux de se décider librement. Il en est ainsi du choix du système politique, économique, social et culturel et de la formulation des relations extérieures. L'intervention est illicite lorsque à propos de ces choix, qui doivent demeurer libres, elle utilise des moyens de contrainte* »[30].

La difficulté est donc apparue lorsqu'il s'est agi de déterminer à partir de quel seuil une cyber-intervention (espionnage ou influence) atteint le niveau de contrainte prohibé par le droit international. L'affaire du piratage des serveurs du Congrès du

[23] Gary P. Corn, Jennifer M. O'Connor & Robert Taylor, *Sovereignty in the Age of Cyber*, AJIL UNBOUND.

[24] Voir note n°12, *supra*.

[25] - Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 Texas Law Review

[26] Manuel de Tallinn 2.0., Règle n°4, commentaire 7 et 8.

[27] Manuel de Tallinn 2.0, Règle n°32.

[28] Voir les débats autour de la Règle n°4 du Manuel de Tallinn 2.0.

[29] Arrêt de la CIJ du 27 juin 1986, « Activités militaires et paramilitaires au Nicaragua et contre celui-ci » dit « Nicaragua », Recueil CIJ, 1986, §202 p. 106.

[30] Arrêt « Nicaragua », Recueil CIJ, 1986, §205, p. 108.

Parti Démocrate américain pourrait ainsi tout à fait relever d'une ingérence prohibée au sens de la CIJ dans la mesure où d'une part, l'affaire va au-delà de l'espionnage « classique »[31] et que, d'autre part, c'est bien l'indépendance politique de l'Etat qui pourrait être visée par cette attaque.

Le fait est que, par nature, toutes les activités dans le cyberespace sont marquées par leur ubiquité. Elles ignorent les territoires. La mise en œuvre des règles impliquées par la souveraineté, telle que la non-ingérence a constitué un défi pour les experts de la deuxième version du Manuel. En effet, la CIJ avait eu l'occasion d'expliciter que « *le principe de non intervention met en jeu le droit de tout Etat souverain de conduire ses affaires sans ingérence extérieure ; bien que les exemples d'atteinte au principe ne soient pas rares, la Cour estime qu'il fait partie intégrante du droit international coutumier* » (arrêt Nicaragua). Cette approche pragmatique convient a *priori* tout à fait au cyberespace dans le cadre duquel une démarche *in concreto*, au cas par cas, s'imposera. D'ailleurs, les experts du Manuel de 2017 ont réitéré l'importance et l'applicabilité de ce principe dans la Règle n°66.

En réalité, tout dépendra de la manière suivant laquelle les cyber-attaques sont conduites et des finalités qu'elles poursuivent[32]. Ainsi, lorsqu'une cyber-opération cause des dommages matériels et/ou humains, la violation des principes d'intégrité et d'inviolabilité du territoire serait aisément caractérisée[33].

Les travaux de Tallinn 2.0 donne une importance considérable aux seuils sans pour autant être parvenu à les fixer : certains experts ont considéré que la neutralisation ou la perturbation du fonctionnement d'un système d'information ou d'une infrastructure n'est pas en elle-même une atteinte suffisante pour constituer une violation de la souveraineté de l'Etat ciblé, compte tenu du fait que les dommages restent immatériels, en particulier s'ils sont temporaires[34]. Sur ce point, le consensus n'a pas été atteint et une zone grise persiste concernant les attaques ne causant pas de préjudices matériels.

III.2. L'Etat, acteur incontournable d'un régime de responsabilité internationale effectif dans le cyber- espace.

Plaquer la cartographie des territoires sur le cyberespace est donc illusoire. Pour autant, les travaux de Tallinn mettent en évidence le fait que l'ancrage à l'Etat reste un socle utile, nécessaire à la mise en place d'un ordre juridique structurant. L'exemple le plus significatif de cette réalité concerne la mise en œuvre d'un régime de responsabilité internationale permettant de régir le domaine de la réparation des dommages en cas de menaces et de dommages causés à la sécurité collective.

C'est ainsi, que les règles 15 à 18 du Manuel de Tallinn de 2017 proposent d'adopter les dispositions classiques en matière d'engagement de la responsabilité internationale, mettant l'Etat au centre du dispositif[35], pour surmonter les difficultés de l'imputabilité d'une cyber-attaque. Il est vrai que l'article 8 du projet d'articles sur

[31] L'espionnage n'est pas en soi prohibé selon la Règle 32 du Manuel de Tallinn.

[32] Manuel de Tallinn 2.0, Règle n°32.

[33] Il convient cependant de relever que certains Experts ont pu considérer que les préjudices physiques constituent un critère de l'atteinte à la Souveraineté mais pas forcément le critère déterminant. En ce sens, voir la Règle n°4, commentaire 12

[34] Règle n°4, commentaire 13

[35] L'article 4 du projet d'articles sur la responsabilité de l'Etat pour fait internationalement illicite dispose que : « *Le comportement de tout organe de l'Etat est considéré comme un fait de l'Etat d'après le droit international, que cet organe exerce des fonctions législative, exécutive, judiciaire ou autres, quelle que soit la position qu'il occupe dans l'organisation de l'Etat, et quelle que soit sa nature en tant qu'organe du gouvernement central ou d'une collectivité territoriale de l'Etat.* »

la responsabilité de l'Etat pour fait internationalement illicite permet de faire face à l'asymétrie de certaines attaques en disposant que : « *Le comportement d'une personne ou d'un groupe de personnes est considéré comme un fait de l'Etat d'après le droit international si cette personne ou ce groupe de personnes, en adoptant ce comportement, agit en fait sur les instructions ou les directives ou sous le contrôle de cet Etat.* ». L'ensemble des arrêts de la CIJ en matière de mise en œuvre de la responsabilité des Etats constitue également un vivier intéressant et utile dans le cadre des cyber-agressions.

Pour autant, la nature spécifique de ces attaques complique beaucoup la mise en œuvre des règles classiques du droit international. Si des agissements sur instructions de l'Etat sont aisés à déterminer, les notions de « *direction* » et de « *contrôle* » laissent une marge d'incertitude que les réflexions de Tallinn n'ont pas permis surmonter. Il est, en effet, particulièrement difficile de déterminer qu'une cyberattaque lancée par un groupe privé l'a été sous la « direction » ou le « contrôle » d'un Etat déterminé, alors que la spécificité de telles attaques est de rester immatérielles et souvent anonymes. Le critère du « contrôle effectif » rappelé par la CIJ ne simplifie pas forcément l'analyse, quand bien même la démonstration d'une « totale dépendance » à un Etat déterminé ne serait plus nécessaire[36]. Pour rappel, l'arrêt de la CIJ dans le cadre de l'affaire relative à l'application de la convention pour la prévention et la répression du crime de génocide (BOSNIE-HERZEGOVINE c. SERBIE-ET-MONTENEGRO) du 26 février 2007 assouplit quelques peu les critères de l'imputabilité mais sans pour autant se distancier de la notion de « contrôle effectif » : « *(…) il n'est plus nécessaire ici de démontrer que les personnes ayant accompli les actes prétendument contraires au droit international étaient en général placées sous la «totale dépendance» de l'Etat défendeur; il convient de prouver que ces personnes ont agi selon les instructions ou sous le « contrôle effectif » de ce dernier. Mais, d'autre part, il est nécessaire de démontrer que ce « contrôle effectif» s'exerçait, ou que ces instructions ont été données, à l'occasion de chacune des opérations au cours desquelles les violations alléguées se seraient produites, et non pas en général, à l'égard de l'ensemble des actions menées par les personnes ou groupes de personnes ayant commis lesdites violations* »[37]. Dans le cadre des cyberattaques, de telles exigences conditionnant l'imputabilité des actes aux Etats, s'avéreront particulièrement difficile à respecter.

La difficulté augmente lorsqu'est abordée l'obligation de « *due diligence* » de l'Etat - rappelée à la règle n°6 du Manuel de 2017 - lorsque son territoire sert d'hôte ou de voie de transit à des cyber-opérations hostiles à un autre Etat[38]. Il convient de souligner que, suite aux travaux conduits en 2013, le nouveau panel a, par souci de réalisme et de légitimité, fait appel à l'éclairage d'un groupe d'experts techniques pour comprendre dans quelle mesure un Etat est susceptible d'intervenir et de faire cesser une cyber-attaque transitant par son territoire et portant préjudice à un autre Etat. Les situations étant variables et protéiformes, il fut difficile de dégager une règle générale, acceptée de tout le panel.

En définitive, le Manuel de 2017 se borne à reprendre la position de la CIJ dans l'affaire du « Détroit de Corfou » qui rappelle l'obligation « *pour tout Etat, de ne pas laisser utiliser son territoire aux fins d'actes contraires aux droits d'autres Etats* »[39].

Cependant, les commentaires et observations portant sur la Règle n°6 mettent en évidence les fortes divergences au sein du panel. Les Experts se sont ainsi opposés sur l'équilibre à trouver entre le droit de l'Etat de contrôler son territoire de manière

[36] Arrêt de la CIJ « Nicaragua » : Recueil CIJ, §115 p. 64-65.

[37] Recueil CIJ- §400, p. 208.

[38] Cela renvoie notamment à la problématique des réseaux botnet malveillants (ou réseaux de machines « zombies »), servant de voies de passages à des cyber-attaques en tout genre, et difficilement traçables.

[39] Affaire du « Détroit de Corfou », Recueil CIJ, 1949, p.22,

indépendante et le devoir de préserver les autres Etats des préjudices causés par des opérations fomentées à partir de celui-ci[40]. Certains ont posé comme critères de mise en œuvre de cette obligation, la notion de « *conséquences négatives sérieuses* » alors que d'autres lui ont préféré le terme de « *significatif* ». Au-delà de la bataille sémantique sur les seuils de gravité, se pose la difficulté de mettre à la charge de l'Etat, une responsabilité pour les cyber-opérations organisées à partir ou à travers son territoire alors même qu'il n'aurait pas la capacité opérationnelle de faire cesser le trouble et les dommages qui s'en suivraient. A l'instar des conclusions du rapport du GGE en 2013[41], les experts ont donc opté en 2017 pour une approche graduelle et incitative, en convenant de l'existence d'une obligation pour les Etats de mettre en œuvre les moyens nécessaires pour faire cesser une cyber-attaque en cours ou imminente pouvant avoir des conséquences « *sérieuses* » et dans la mesure où ils disposent des moyens pour le faire[42].

Il convient de relever qu'une proposition au sein du panel reposait sur la mise en œuvre d'un principe de précaution, impliquant une obligation pour l'Etat de veiller à ce que ses infrastructures et ses réseaux ne servent pas à des cyberattaques. Cette proposition a été mise en minorité compte tenu de la portée intrusive d'une telle règle, nonobstant le fait que sa faisabilité technique n'est pas garantie pour l'ensemble des Etats[43].

III.3. Les incertitudes liées à l'exercice de la légitime défense dans le cyber espace.

Malgré le caractère asymétrique d'une partie substantielle des cyber-conflits, l'Etat conserve le monopole de la violence légitime. Celle-ci est particulièrement délicate à manier dans le cadre de la mise en œuvre de la légitime défense. Sur ce point, le Manuel de Tallinn de 2017 reprend, en sa règle n°68, le consensus qui s'est cristallisé, dès 2013, autour de l'applicabilité de l'article 2 §4 de la Charte des Nations-Unies[44] la Charte : « *un État qui est la cible d'une cyber opération qui atteint le niveau d'une agression armée peut exercer son droit naturel de légitime défense. Une cyber opération constitue une attaque armée selon sa dimension et ses effets* »[45].

L'incertitude réapparaît, cependant, dès lors qu'il s'agit de déterminer les seuils et les critères qui permettent de retenir qu'une cyber-attaque constitue une agression

[40] Selon la Règle n° 6, commentaire 70 du Manuel de Tallinn 2.0: "*the other approach would create an imbalance between the right to control territory and the duty to ensure it is not used to harm other States*."

[41] Les conclusions du rapport GGE indique que les Etats « *devraient* » (et non « *doivent* ») déployer leurs meilleurs efforts : "*States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.*", Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - A/68/98 - 24 June 2013, p. 8. §23.

[42] La Règle n°6, Commentaire 13 indique : "*as a strict matter of law, the 'transit State' shoulders the due diligence obligation and must act pursuant to Rule 7 when it (1) possesses knowledge (on actual and constructive knowledge) of an offending operation that reaches the requisite threshold of harm and (2) can take feasible measures to effectively terminate it*."

[43] Voir la Règle 6, Commentaire 42.

[44] L'article 2 § 4 de la Charte des Nations-Unies dispose 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 Etat, soit de toute autre manière incompatible avec les buts des Nations Unies.* ».

[45] Règle n°13 du Manuel de Tallinn v.1.0.

armée, justifiant la mise en œuvre de l'article 51 de la Charte des Nations-Unies[46]. La question est d'autant plus cruciale dans le domaine de la cyber- menace que la cyber-riposte (« Hack-back ») peut être déclenchée sans contrôle effectif et préalable de la Communauté internationale, de manière invisible, fulgurante, et donc aisément disproportionnée à l'attaque initiale.

Suivant un raisonnement par analogie, les experts de Tallinn 1.0 avaient, de manière consensuelle, retenu que la fourniture de logiciels malveillants ou des moyens humains pouvant être utilisés à l'encontre d'un autre Etat constituent un usage illicite de la force[47]. Cette analyse va dans le sens de la jurisprudence de la CIJ qui a eu l'occasion d'affirmer le principe de neutralité technologique et l'indifférence de la nature de l'arme pour caractériser l'emploi de la force[48]. Il convient de rappeler que dans son arrêt Nicaragua, la CIJ a pu considérer que l'emploi illicite de la force pouvait concerner le soutien logistique (entrainement et armements par exemple)[49].

Les acquis du Manuel de Tallinn 1.0 sont évidemment repris par le Manuel de Tallin 2.0, rien dans la pratique depuis 2013 ne justifiant une remise en question du principe.

Le Manuel de Tallinn 2.0 considère également qu'il ne sera pas nécessaire que des dommages matériels aient été causés par une cyber-attaque pour retenir l'usage de la force[50]. De même, la Règle 71 du Manuel de 2017[51]
attaque menée par un groupe non étatique. Les travaux de Tallinn 2.0 ont donc mis l'accent sur l'identification des critères permettant de qualifier telles ou telles attaques ou actions comme étant un usage de la force. Parmi ces critères, il est possible de recenser la gravité, la prise en considération du contexte politique, le profil de la cyberattaque et ses liens avec une possible et future utilisation militaire

[46] L'article 51 de la Charte des Nations-Unies 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* ».

[47] Voir la Règle n° 69, Commentaire 4 du Manuel de Tallinn v. 2.0 : "*On the premise that in the absence of a conclusive definitional threshold, States contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition of the use of force.*"; voir également la Règle n°69, Commentaire n°8 du Manuel de Tallinn 2.0.

[48] « *La Cour estime que, comme dans le cas des principes du droit humanitaire applicable dans les conflits armés, le droit international ne laisse aucun doute quant au fait que le principe de neutralité - quel qu'en soit le contenu -, qui a un caractère fondamental analogue à celui des principes et règles humanitaires, s'applique (sous réserve des dispositions pertinentes de la Charte des Nations Unies) à tous les conflits armés internationaux, quel que soit le type d'arme utilisé.* », , avis consultatif de la CIJ du 8 JUILLET 1996 sur la licéité de la menace ou de l'emploi d'armes nucléaires, Recueil CIJ, p. 39.

[49] Dans le cadre de son arrêt « Nicaragua », « *La Cour constate que, sous réserve de la question de savoir si leurs actes se justifient par l'exercice du droit de légitime défense, les Etats-Unis, par leur assistance aux contras au Nicaragua, ont commis primafacie une violation de ce principe en ((organisant ou encourageant l'organisation de forces irrégulières ou de bandes armées ... en vue d'incursions sur le territoire d'un autre Etat et en participant à des actes de guerre civile ... sur le territoire d'un autre Etat* ***D,*** *selon les termes de la Résolution 2625 (XXV) de I'Assemblée générale* ». Recueil CIJ §228, p. 108-109.

[50] Voir la Règle 11, Commentaire 4 et 8.

[51] Commentaire 18.

de la force, la nature de la cible, etc.[52]. Cependant, cette liste n'est pas exhaustive et elle n'a pas fait l'objet d'un consensus au sein du groupe d'experts.

Il est vrai que la question est d'autant plus complexe que la notion d'armes – et *a fortiori* de cyber-armes - n'est pas définie en droit international, nourrissant ainsi les nombreuses zones grises qui continuent d'émailler les réflexions des experts. Ainsi, ces derniers ont-ils laissé sans réponse l'hypothèse d'une attaque informatique

ou encore le cas d'une implication combinée de [53].

IV. Conclusion

L'apparition du cyberespace n'a évidemment pas spontanément conduit à l'émergence d'un droit *sui generis*, ni même à une organisation institutionnelle devançant les difficultés que la création de cette nouvelle zone de relations immatérielles entre les hommes, les Etats et les machines allait provoquer.

L'injonction qui est systématiquement faite au droit d'apporter des réponses sur-mesure, anticipant des problématiques aussi complexes et imprévisibles que celles du cyberespace est aussi vaine qu'abusive.

Le Manuel de Tallinn paru en 2017, s'inscrit dans la logique d'une offre juridique de l'ordre de la *soft law*, dont les capacités de consolidation par transposition ne sont plus à démontrer[54]**.** Il s'inscrit également en réponse à des besoins que les affrontements de puissances rendent souvent inaudibles.

L'annonce d'un accord de non-agression dans le cyberespace entre la Russie et la Chine en mai 2015[55], les déclarations mutuelles des Etats-Unis et de la Chine concernant la nécessité d'un travail commun autour d'un code de conduite concernant les cyber-activités depuis 2015, l'annonce d'un accord entre le Canada et la Chine concernant le piratage informatique en 2017 sont autant de signes de l'utilité prospective des travaux de Tallinn, qui ne devraient pas en rester là.

[52] Selon la Règle n°69, Commentaire 10 : "*the prevailing political environment, whether the cyber operation portends the future use of military force, the identity of the examiner, any record of cyber operations by the attacker, and the nature of the target.*"

[53] Voir la Règle n°71, Commentaire 11.

[54] René-Jean Dupuy, *Droit déclaratoire et droit programmatoire : de la coutume sauvage à la « soft law »* , Dialectiques du droit international, Ed. Pedone, 1999, p.120.

[55] https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html?_r=0