Les cyber-attaques face au jus ad bellum Etude et commentaires sur le manuel de Tallinn

Cyber-attacks against the jus ad bellum A Study and Comments on the Tallinn Manual

Dt./ / Elacheache Ishak[1,2]
[1] Université d'Alger 1, (Algérie)
[2] Auteur Correspondant: elacheache.ishak@gmail.com

Date de soumission : 30/08/2018 Date d'acceptation : 14/02/2019 Date de publication : 28/12/2019

****

(Révision de l'article: Langue Française: D./ BASSI Mohamed ElHadi (Uni.d' El Oued)
Langue Anglaise: D./ Mohamed Akram Arabet (Uni. Constantine 1)

Résumé:

Le siècle actuel assiste à une révolution unique dans le monde de la technique numérique au point que certains experts et spécialistes le considèrent comme une cinquième dimension de guerre après terre, mer, air et espace extra-atmosphérique. Dans les guerres conventionnelles où l'ennemi est connu et prédictif de son comportement, les choses sont déférentes dans le cadre des cyber-attaques, l'ennemi ne provient pas forcément un État voisin, mais suffit juste d'être une entité Étatique connectée à un réseau numérique, qui menace l'infrastructure critique des États avec une série de cybers-attaques, dont les effets aboutissent à une échelle de destructions massives. Ce qui soulève la question de savoir si la réglementation actuelle du droit de recourir à la force en droit international s'applique à de telles attaques. Ce problème a été traité par un manuel jurisprudentiel unique comprenant un ensemble de règles et d'observations, connu par « le Manuel de Tallinn » sur le droit international applicable à la cyberguerre. Dans ce contexte, la présente étude décrit et commente le chapitre II de ce guide pour l'année 2013 et le chapitre XIV de sa version révisée de l'année 2016, dans le but d'analyser ces règles et de déterminer le caractère vague de l'applicabilité des règles de droit international à la réalité des faits de la cyberguerre.

***Mots-Clés**: Manuel de Tallinn; Cyber guerre; Recourir à la force; Cyber-Attaques.*

***Abstract**:*

This century has witnessed a unique revolution in digital technology to the point that some experts and specialists regard it as a fifth area for war after land, sea, air and space. The behavior of the enemy in conventional wars is known and predictive; however, this is different in regards to the area of cyber attacks. The enemy is not

necessarily a geographically neighboring state, but it may be a state connected to a digital tool through which it threatens the critical infrastructure of other states with a series of cyber attacks whose effects reach the pinnacle of destruction. This raises the question of whether the current regulation of the current law of recourse to war in international law applies to such attacks. The latter was processed through a unique legal Manual that includes a set of rules and commentary, named "Tallinn's Manual" to International Law Applicable to Cyber War. In this context, this study focuses its commentary and description to the second chapter of the Manual (2013) and the fourteenth chapter of its revised version (2016) for the purpose of analyzing these rules and determining the vagueness of the applicability of the rules of international law to the realities of cyber warfare.

***Key Words**: Tallinn Manual; Cyber Warfare; Use of Force; Cyber Attacks.*

Introduction:

Le *jus ad bellum* est un droit ancien qui se fonde sur la théorie de la guerre juste qui fut développée, notamment par les catholiques Saint Augustin et Thomas d'AQUIN au 13ème siècle. Ce dernier exigeait que soient respectées trois conditions:

- Auctoritas principis: la guerre ne peut relever que de la puissance publique qui à l'époque était le roi. Seul le monarque pouvait déclarer la guerre.
- Causa justa: la cause doit être juste. C'est-à-dire que le souverain ne doit déclarer la guerre que si les raisons sont justes.
- Intention recta: l'intention ne doit pas être entachée de causes cachées mais uniquement dans le but de faire triompher le bien commun.

Au cours du temps, la situation a changé. Aujourd'hui, nous ne nous cantonnons plus à ces conditions modifiées par les corrections apportées au principe de la guerre juste qui est devenue jus ad bellum.

Le *jus ad bellum* encadre la période pré-conflit, c'est-à-dire tout ce qui concerne les éléments déclencheurs au conflit. C'est le droit du recours à la force. En effet, en droit international, il est interdit en vertu de l'article 2(4) de la Charte des Nations Unies de recourir à la menace ou à l'emploi de la force dans ses relations internationales, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies. De ce fait, les cyber-attaques ne peuvent être envisagées, au même titre que les attaques conventionnelles comme un moyen de règlement des différends en vertu du présent article, **(PREMIERE PARTIE)** il est interdit de menacer ou d'employer des attaques cybernétiques ou conventionnelles contre un État. Même si cela est réglementé, il n'empêche qu'au vu des différents conflits ayant éclaté ces dernières années, cet article ne soit pas forcément respecté.

Dans pareille situation, l'article 51 de la CNU va jouer un rôle essentiel, à une condition bien spécifique. Pour que ce dernier puisse s'appliquer, il doit y avoir attaque armée. Or pour appliquer cette notion aux cyber-attaques, il faut que certains principes soient respectés **(DEUXIÉME PARTIE)** : la nécessité, la

proportionnalité et l'immédiateté. C'est à partir de cet instant que la légitime défense, individuelle ou collective pourra être envisagée en attendant que le Conseil de sécurité des Nations Unies trouve un moyen pour que le conflit cesse et n'atteigne pas le stade de la menace à la paix et à la sécurité internationales.

L'importance de cette étude est de conduire à répondre à certaines questions relatives à l'utilisation de la force dans le droit international et en particulier le droit international humanitaire, donc Nous essayerons dans cette recherche de savoir **si les règles existantes de ce droit sont suffisantes pour traiter les problèmes juridiques découlant dans le cas d'utilisation d'outils Cybernétiques au recours à la force ?** Méme s'il est important de savoir que la réponse à cette problèmatique découle des hypothèses de la réalité internationale qui concernent tout d'abord que chaque cyber-attaque est considérée comme telle que conventionnelle, En d'autres termes, chaque cyber-attaque doit etre qualifiée comme une attaque armée. Ce qui nécessite de recourir aux exigences de la légitime défense.

Enfin, **l'objectif** de l'étude réside dans l'encadrement du statut juridique applicable aux cyber-attaques et la connaissance de la jurisprudence à cet égard à partir de l'analyse et commentaires qui mettent l'accent sur le Guide Tallinn qui traite (le droit international humanitaire applicable sur la Cyberguerre), version 1.0 de l'année (2013) (chapitre 2) et la version 2.0 (chapitre 14) pour l'année 2016, en définissant sa base juridique et aborder les implications pratiques dans le contexte cybernétique et de la juridiction internationale et à énoncer des positions divergentes quant à la portée ou à l'interprétation. Ce manuel qui n'est pas un traité international ou coutumier, conformément à l'article 38 du Statut de la Cour internationale de Justice, mais comme un point positif, reste comme une deuxième source du droit international selon le même article, qui pourra aider à développer des futurs traités ou bien d'être une pratique pour les armées des pays selon le degré d'influence.

LE PREMIER PARTIE

Les Cyber-attaques comme « attaque armée » et l'interdiction de recourir à la force en droit international.

D'abord, il faut attirer l'attention à un rapport basic (A/68/98) 2013) publié par le Groupe d'experts gouvernementaux sur les développements en matière d'information et des télécommunications dans le contexte de la sécurité internationale de l'Assemblée générale des Nations Unies. Ce qui en a fait un tournant décisif en ce qui concerne le sujet (Cyber guerre), car il a conclu que le droit international et en particulier la Charte des Nations Unies (CNU) s'applique à l'utilisation des technologies de l'information et de la communication par les États. Un composant doit être préservé afin de maintenir la paix et la stabilité et la création d'un environnement technologique saint et confidant.

Cet avis est venu comme un résumé des appels de nombreux pays, mais la communauté internationale et les organisations internationales ne faisaient pas des

progrès sérieux dans ce domaine, et ceci en raison de sa complexité et de son interférence ainsi que l'émergence de ses nouveaux concepts technique et juridique.

Le Principe du recours à la force est énoncé à l'article 2(4) de la Charte des Nations Unies. Il y est exposé que:

« Les membres des Nations Unies 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. »

Nous étudierons donc dans un premier temps, les cyber-attaques en tant que « recours à la force » et menaces à la stabilité des relations internationales **(Chapitre 1)** et, dans un second temps, les cyber-attaques et la notion d'« attaque armée » **(Chapitre 2)**.

CHAPITRE 1: Les cyber-attaques comme « recours à la force » et menaces à la stabilité des relations internationales.

Le maintien de la paix et de la sécurité internationales était la raison première ayant poussé à la création des Nations Unies. **(1)** Le maintien de la paix et de la sécurité internationale passe par un encadrement juridique concret que l'on retrouve dans l'article 2(4) de la CNU interdisant la menace ou le recours à la force. L'arrêt de la Cour Internationale de Justice de 1986 des activités militaires et paramilitaires au Nicaragua vient renforcer cela en confirmant que l'interdiction du recours à la force est un principe à valeur coutumière. L'article 38 du statut de la Cour Internationale de justice « defines customary law as general practice accepted as law ». En matière de conflit armé usant exclusivement de moyens conventionnels, il ne peut pas y avoir de doute en la matière. Cependant, on se place dans un conflit usant de moyens cybernétiques, il est plus compliqué de faire appel à la coutume puisque les États ne sont pas encore en accord sur leur utilisation. **(2)**

Par suite le manuel de Tallinn est d'accord avec cet avis, c'est la règle 10 (2013) ou bien 68 (2016) qui a indiqué : « Une cyber-opération qui constitue une menace ou un usage de la force contre l'intégrité territoriale …, est illégale ».

Même si les États éprouvent des difficultés à se mettre d'accord sur la définition du recours à la force, il convient tout de même de comprendre que ce dernier concerne exclusivement les forces armées. Il faut cependant faire attention car sont non seulement visées les attaques conventionnelles mais également les attaques lancées à travers des armes dites par destination. Celles-ci se définissent comme des objets dont la fonction première n'est pas d'être une arme mais qui sont utilisés ou destinés à être utilisés comme tels dans certaines situations. Elles s'opposent aux armes dites par nature. On peut prendre pour exemples : **(3)** Le fait de détruire un barrage pour le territoire d'un État voisin, ou bien Le fait d'utiliser la nature comme tel lors de la guerre du Vietnam, ou Le fait de lancer une cyberattaque ou autres.

Ainsi les cyber-attaques peuvent faire partie des moyens utilisés pour recourir à la force conventionnelle qui est également une arme dont l'utilisation doit être réglementée. Vient appuyer ces dires l'avis rendu par la Cour Internationale de justice du 8 juillet 1996 intitulé Licéité de la menace ou de l'emploi des armes nucléaires. Cette dernière y énonce dans son paragraphe 39 que l'interdiction générale de l'emploi de la force édictée par la Charte des Nations Unies ne préjugeait pas de l'usage d'armes particulières et s'appliquait à n'importe quel emploi de la force, indépendamment des armes employées. Ainsi, on peut estimer que des attaques informatiques peuvent relever de l'usage de la force au sens de l'article 2(4) de la CNU, à condition toutefois que les effets de ces attaques soient comparables, en termes de létalité et de destruction à ceux d'attaques conventionnelles ou nucléaires, biologiques ou chimiques. Le Manuel de Tallinn [(4)] énonce dans la règle 11 (2013) ou 69 (2016) « qu'une cyber opération constitue un recours à la force lorsque son ampleur et ses effets comparables à des opérations non cybernétiques devenant un recours à la force ». L'analyse porte donc sur des facteurs quantitatifs et qualitatifs. [(5)] Les faisceaux d'indices permettant de qualifier une opération cyber en emploi de la force sont d'ailleurs les points que Michaël N. SCHMITT développe dans son article « Cyber operations and the jus ad bellum revisited ». [(6)]

La définition de la « force » est d'une importance cruciale, mais c'est l'une des questions éternelles qui affectent la portée de la règle interdisant la menace ou l'emploi de la force. Le Manuel (2013 et 2016) rejette une approche instrumentale de la force et adopte une approche fondée sur les effets. [(7)] L'absence générale des critères exposés ci-dessus est la raison pour laquelle la cyber-attaque menée contre l'Estonie en 2007 aurait difficilement pu, même si elle avait conduit à l'incrimination d'un État étranger, déboucher sur des représailles armées car la perte d'aucune vie humaine n'a heureusement été déplorée. On peut citer d'autres exemples d'utilisation des cyber-attaques en tant que recours à la force en reprenant ceux énoncés dans le rapport de l'UNIDIR de 2011 celui de Stuxnet. [(8)] La question qui se pose immédiatement est de savoir si les cyber opérations contre des infrastructures d'État critiques qui ne causent pas de dommages physiques mais qui perturbent gravement le fonctionnement de l'État peuvent être assimilées à un recours à la force au sens de l'article 2(4). Le manuel donne l'impression que de telles opérations cybernétiques échappent à l'article 2(4), en excluant la contrainte économique ou politique de la définition de la force. Elle s'appuie sur les travaux préparatoires et sur la déclaration des relations amicales de l'Assemblée générale. Cependant, la possibilité de qualifier les opérations cybernétiques qui affectent sérieusement l'infrastructures d'Etat critique en tant qu'usages de la force ne devrait pas être écartée facilement. Par exemple, Ces infrastructures comprennent, entre autres, pour la production, la transmission et la distribution d'énergie, le transport aérien et maritime, les services bancaires et les services financiers, l'E- commerce, l'approvisionnement en eau, la distribution alimentaire et la santé publique ; et

aussi les infrastructures critiques de l'information qui sont de plus en plus interconnectées et dépendantes les unes des autres ce qui affectent leur fonctionnement. Qui peuvent ne pas entraîner la mort ou la destruction immédiates, mais peut être grave compte tenu de la dépendance des États modernes à l'information. La technologie. Cela peut avoir le même effet que celui qui peut être produit par la destruction physique des institutions économiques d'un Etat. Pourquoi la destruction physique des principales institutions économiques d'un État devrait-elle être un recours à la force et non à leur paralysie fonctionnelle ? (9)

Dans le cadre d'un conflit, certes peuvent être touchées des personnes physiques, militaires ou civiles, ces dernières peuvent donc être blessées, mais également et malheureusement, tuées. Par ailleurs, en temps de guerre, des habitations, des bâtiments publics, des locaux militaires, etc. peuvent être détruits. Certaines infrastructures qualifiées de « critiques » peuvent, si elles font l'objet d'une attaque conventionnelle ou cybernétique, permettre de prendre l'avantage sur l'ennemi, ce que les États ont bien compris. Dans sa résolution 59-199 du 30 janvier 2004, l'Assemblée générale des Nations Unies a énoncé que chaque pays devra déterminer quelles sont ses infrastructures critiques afin de mettre en place les défenses nécessaires pour les protéger. (10) Celle-ci explique ce que peuvent être les infrastructures critiques.

Par ailleurs, le manuel de Tallinn (2013) indique dans la règle 7 qu'une cyber-opération ait été lancée ou qu'elle provienne d'une infrastructure informatique gouvernementale ne constitue pas une preuve suffisante pour attribuer l'opération à cet État, mais indique que l'État en question est associé à l'opération.

Enfin, l'article 2(4) de la CNU prohibe également la menace du recours à la force. Celle-ci est illicite là où l'emploi de la force serait lui-même illicite Ainsi, un État ne peut pas s'avancer en énonçant, comme par exemple la Chine l'a fait dans le cas de la dissuasion nucléaire, qu'il n'hésitera pas à répondre par des moyens conventionnels si jamais il faisait l'objet d'une attaque. (11)

De l'autre côté, dans l'article 2(4) de la Charte des Nations Unies, il est énoncé que les États s'abstiennent dans leurs relations internationales (12) de recourir à la menace ou à l'emploi de la force. Néanmoins L'État reste l'acteur principal en matière de relations Internationales notamment en ce qui concerne le recours à la force, Le problème est qu'il est plus compliqué, dans le cadre de cyber-attaques, pour un État, de savoir comment les envisager. Est-ce une attaque contre Mon pays personnellement? Est-ce une attaque que j'ai reçue pour donner suite à une autre attaque lancée sur un pays et qui, malheureusement a produit un effet domino ! (13) Est- ce que l'attaque qui m'a été lancée n'est pas due à un effet boomerang, c'est-à-dire n'aurais-je pas envoyé une cyber-attaque contre une structure d'un autre État qui aurait pu me toucher ?

Donc, il est très difficile par la complexité des cyber-attaques, de pouvoir trouver et/ou prouver qui l'a lancé. Certains États ne se cachent pas pour accuser,

dans tous les cas les cyber-attaques, jouisses le rôle principal dans la déstabilisation du relations internationales dans différents domaines. (14)

CHAPITRE 2: Qualification juridique du cyberattaque comme «attaque armée»

Les experts du Manuel de Tallinn, ont choisi pour les cyber-attaques le terme «d'attaque armée» mais à certaines conditions. La question est de savoir si celles-ci sont employées en tant que forces au sens de l'article 2(4) de la CNU ou si elles correspondent plus aux critères de l'attaque armée que l'on retrouve à l'article 51 de ce même texte. En effet, ce dernier explique la possibilité de recourir au droit de légitime défense lorsqu'un État fait l'objet d'une agression armée.

Comme nous l'avons déjà vu Le Manuel de Tallinn est très clair concernant le recours à la force. Un État ne doit en aucun cas autoriser l'utilisation des infrastructures cybers pour commettre des actes malveillants. Il y aura violation de souveraineté lorsqu'une attaque perpétrée par un État sur les infrastructures cybers d'un autre État en traine des effets néfastes et notamment des dommages. L'État victime pourra alors utiliser des contre-mesures et intervenir en légitime défense dans le cadre de l'article 51 de la Charte.

À partir du moment où on envisage d'user de la menace voire de l'emploi de la force, il est logique de penser que l'attaque armée sera utilisée. L'article 1er de la résolution 3314 (14 décembre 1974) de l'Assemblée générale des Nations Unies énonce que l'agression est l'emploi de la force armée par un État contre la souveraineté, l'intégrité territoriale ou l'indépendance politique d'un autre État, ou de toute manière incompatible avec la Charte des Nations Unies. Cette définition fut adoptée par consensus.

Ainsi, même si le droit international n'a pas fourni de liste claire de ce qui peut être qualifié d'agression armée, cette résolution de l'Assemblée générale des Nations Unies nous éclaire sur certains points dans son article 3, et même l'article 4, quant à lui, nous déclare que l'énumération des actes ci-dessus n'est pas limitative et le Conseil de sécurité peut qualifier d'autres actes d'actes d'agression conformément aux dispositions de la Charte. Ainsi, la cyber-attaque peut également faire partie des actes qualifiés d'agression armée. Le Conseil de sécurité sera certainement amené, dans l'avenir, à faire évoluer cette liste en les y intégrant. Cependant, actuellement, les experts du Manuel de Tallinn estiment qu'aucun incident cybernétique international n'a atteint à ce jour le seuil de qualification d'une agression armée. Même l'attaque cybernétique en Iran (Natanz) de 2010, souvent appelée conflit cybernétique ou cyberguerre n'a été publiquement qualifiée par la Communauté internationale « d'agression armée ». L'acte d'agression armée permet donc à un État d'envisager de recourir à la légitime défense, ce qui n'est pas forcément le cas lorsqu'on fait l'objet d'une menace de l'emploi de la force. (15)

À partir du moment où on fait le choix de qualifier les cyber- attaques en tant qu'attaques armées, on se doit de vérifier que ces dernières respectent des caractéristiques bien précises. Si ces conditions ne sont pas respectées, les armes

cybernétiques ne peuvent pas relever de cette notion. Certes, comme cela a été exposé dans la première section de cette partie, Michael N. Schmitt a posé les bases avec les experts ayant rédigé le Manuel de Tallinn en énonçant le respect de certains critères comme: la persistance de l'attaque, la sophistication des moyens employés, l'implication de forces constituées, etc. Tous ces éléments caractérisent l'attaque. Cependant, pour qu'une cyber-attaque devienne un acte de guerre/attaque armée, susceptible d'entrainer une riposte.

En effet, la cyber-attaque se doit de produire des effets équivalents à ceux produits par une attaque lancée par des moyens conventionnels **(Section 1)**, produisant ainsi le dysfonctionnement des infrastructures critiques de l'État permettant ainsi d'avoir l'avantage sur le conflit comme nous avons déjà éclairci précédemment. Il convient également d'étudier qu'elle a été l'intention de l'adversaire au moment où la cyber-attaque a été lancée **(Section 2).**

SECTION 1: La nécessité de produire des effets équivalents à une attaque armée conventionnelle

Dans un premier temps, il convient de comprendre qu'à partir de l'instant où on décide de parler « d'attaque armée », on envisage l'utilisation d'une arme. Les cyber-attaques sont une arme, notamment lorsqu'elles sont utilisées dans le cadre d'un conflit armé. Il en existe plusieurs modèles comme l'explique Paul Rosenzweig : [(16)]

- **DoS Attack** : assaut sur un réseau qui se voit inondé d'un nombre incalculable de demandes provoquant ainsi un ralentissement voire une interruption complète du trafic régulier.
- **Malicious programs:** attaque perturbant les fonctions normales de l'ordinateur ou ouvrant une "porte dérobée" permettant à l'attaquant de s'immiscer dans l'ordinateur afin d'en prendre le contrôle.
- **Logic** Bomb**:** il s'agit d'un code malveillant conçu pour s'exécuter à un événement bien précis ou à un temps déterminé.
- **IP Spoofing:** il s'agit d'une technique de détournement dans laquelle les pirates se font passer pour un hôte de confiance en dissimulant leur identité, en parodiant un site Web, en détournant les navigateurs, pour avoir accès à un réseau.
- **Digital Manipulation:** il s'agit de la modification d'une image réalisée à travers des outils de programmation et des logiciels informatiques afin de produire une image artificielle qui, généralement, reflétera une signification toute autre que l'initiale.

Les cyber-attaques doivent être placées au même niveau que les attaques conventionnelles. Le Manuel de Tallinn est d'accord sur ce point et s'appuie sur l'affaire Activités militaires et paramilitaires au Nicaragua qui met en avant deux critères : scale and effects (*échelle et effet*). Ceux-ci permettent de distinguer les

agressions armées des autres formes d'emploi de la force en les qualifiant de la forme la plus grave d'emploi de la force. Rien de plus n'est précisé. Lorsque l'emploi de la force entraîne des pertes en vie humaines, des blessures aux personnes ou des dommages aux biens, le seuil nécessaire à la qualification « d'agression armée » sera atteint. Les experts n'ont cependant pas quantifié ce seuil. Les cyber-incidents n'atteignant pas, pour l'instant, individuellement le degré d'intensité nécessaire à la qualification d'agression armée, peuvent, grâce à la théorie de l'accumulation des effets en atteindre le seuil. Il s'agit bien d'une situation qui ne durera pas dans le temps, car au fur et à mesure de l'évolution des techniques et des moyens cybernétiques, les cyber-attaques arriveront au final à produire des effets équivalents aux attaques conventionnelles. C'est-à-dire qu'il ne sera plus nécessaire d'envisager des attaques en déni de service pour arriver à atteindre son objectif et le paralyser. Une seule cyber- attaque sera à même de détruire des infrastructures, de blesser ou tuer des personnes physiques.

SECTION 2: L'obligation de se poser la question de l'intention :

La question de l'intention, dans un premier temps, peut être envisagée de cette manière, à savoir les raisons ayant poussé un État à attaquer en premier. Aujourd'hui, il est rare qu'une déclaration de guerre soit prononcée avant que n'éclate un conflit. Ainsi, on analysera les raisons ayant poussé à lancer en premier une attaque conventionnelle ou cybernétique. Beaucoup d'États n'osent pas se lancer dans une guerre, à proprement parler, conventionnelle et préfèrent se lancer des piques via des attaques cybernétiques. Cela est moins couteux et leur permet également de rester anonymes. Tous ces éléments relèvent du caractère « psychologique » de la guerre : savoir pourquoi on fait ça ? Pourquoi décide-t-on d'employer des moyens cybernétiques plutôt que des moyens conventionnels ? Pourquoi décide-t-on de lancer une attaque contre telle ou telle infrastructure ? Qu'est-ce qui nous pousse à répondre à une cyber- attaque dont on a été la victime?

En temps de guerre l'intention des parties est de vaincre l'ennemi. Or pour se faire, il convient d'en avoir les moyens. Les armes quelles qu'elles soient sont utilisées dans ce but : avoir l'ascendant sur l'adversaire. Karl Zemanek l'a compris:

« Ce n'est ni la désignation d'un objet, ni son usage normal qui en font une arme mais l'intention avec laquelle il est utilisé et l'effet qu'il produit. L'utilisation de tout dispositif, quelque en soit le nombre, entrainant une perte considérable en vies humaines et/ou des destructions de biens, doit donc être considérée comme remplissant les conditions d'une attaque armée ». [(17)]

Ainsi, l'intention crée l'arme car tout peut en devenir une à partir du moment où on choisit quelle en sera sa destination : la mort, les blessures, la destruction, toucher des infrastructures critiques, mettre un État à genou, etc. Les cyber-attaques sont une arme à partir du moment où on décide de les utiliser comme telle. Seulement, il y a « arme employée de façon légale » et « arme employée de manière illégale. »

Une arme est légale à partir du moment où elle est utilisée dans le cadre d'un conflit armé en respectant le droit international humanitaire. C'est-à-dire que la cyber-attaque doit être lancée pour atteindre un objectif qui stratégiquement apportera un avantage certain aux forces armées. Dans ce cas, tout doit être analysé : la géographie du lieu, la destination de l'infrastructure visée (militaire, communication…), s'il y a des personnes civiles ou des combattants irréguliers dans la zone, etc. Une cyber-attaque, comme pour toutes les attaques conventionnelles, doit avoir été réfléchie avant d'être lancée.

Une arme, par contre, devient illégale à partir du moment où on ne prend pas en compte le fait de devoir viser exclusivement des objectifs qui apporteraient un avantage militaire certain. C'est-à-dire que sont illégales les attaques lancées à l'encontre d'un hôpital, d'une école, des organisations humanitaires en place (CICR et ONG diverses), etc.

La question de l'intention est vraiment importante, et ce d'autant plus lorsque malencontreusement des civils sont touchés. La répression pénale étudiera tous les éléments qui ont fait que cet acte malheureux a abouti à ce désastre et l'intention est un des premiers éléments à analyser en pareille situation. Personne n'est à l'abri : que ce soit l'État ou le militaire seul. Tous seront passés au crible pour savoir ce qu'il s'est passé lorsque des dommages collatéraux qui auraient, éventuellement voire certainement, pu être évités sont constatés.

Quoi qu'il en soit, à partir du moment où un État fait l'objet d'une attaque, celui-ci a le droit de se défendre. Le 28 mai 2011, une attaque cybernétique a été lancée contre les États-Unis à l'encontre du géant américain de la défense Lockheed Martin. Les responsables américains ont annoncé que de tels actes, dans la mesure où ils provoqueraient la paralysie ou la destruction partielle du fonctionnement de l'État, de l'économie nationale ou des systèmes civils collectifs, seraient désormais considérés comme des « actes de guerre » ouvrant la voie à une riposte militaire de même nature que celle que s'attirerait une attaque armée. À partir de cet instant, la légitime défense a été déclarée par certains États comme possible en réponse à une attaque cybernétique en vertu de l'article 51 de la CNU.

LE DEUXIEME PARTIE
L'utilisation de la légitime défense dans le cyberespace comme exception au recours à la force.

La légitime défense est l'exception au recours à la menace ou à l'emploi de la force. Celle-ci est réglementée à l'article 51 de la CNU.

Selon la règle 13 (2013) et 71 (2016) du manuel de Tallinn, « un État qui fait l'objet d'une cyber-opération qui arrive au niveau d'une attaque armée peut exercer son droit naturel de légitime défense. Le fait qu'une cyber-opération constitue une attaque armée dépend de son ampleur et de ses effets ».

Le Manuel suit une catégorisation d'utilisations de la force par la CIJ en catégories graves et moins graves, [(18)] la légitime défense n'étant autorisée qu'en

réponse à une cyber-opération équivalente à une attaque armée. Un cyber utilisation de la force est une « attaque armée » si son ampleur et ses effets sont graves. (19) Cependant, comme le note le Manuel, la CIJ n'a fourni aucune explication sur la façon dont la gravité de l'attaque peut être mesurée. (20) Outre Manuel fournir d'autres précisions. En conséquence, toute détermination est vouée à être contestée. Par exemple, certains membres du Groupe international d'experts considéraient l'attaque de Stuxnet contre le programme nucléaire iranien comme une attaque armée alors que, implicitement, d'autres ne la considéraient pas comme une attaque armée et, plus important encore, l'Iran ne prétendait pas qu'elle était même un usage de la force. La détermination de ce qui constitue une cyberattaque à des fins d'autodéfense devient encore plus compliquée du fait que le Manuel introduit un seuil de minimis même pour les utilisations de la cyber force par l'Article 2(4). S'il n'existe aucun critère permettant de distinguer entre les utilisations graves et moins graves de la force, et si toutes les conséquences raisonnablement prévisibles (21) doivent être prises en compte pour déterminer les effets de l'attaque, le risque est que toute force cybernétique d'une certaine importance puisse être étiquetée une attaque armée et une force défensive étant donné qu'n Etat ne peut pas utiliser la force en réponse à un recours à la force en deçà du seuil d'une attaque armée, selon le Manuel. La question est de savoir si une telle disparité peut être corrigée en alignant l'usage de la force à l'article 2(4), sur l'attaque armée de l'article 51. C'est la position des États-Unis (22) mais il existe encore une résistance doctrinale à un tel Approche selon les experts de Tallinn.

Un certain nombre d'autres questions concernant la légitime défense sont laissées en suspens dans le Manuel. Une de ces questions est de savoir si une attaque qui ne produit pas de conséquences physiques ou une attaque contre une infrastructure d'état critique peut être qualifiée d'attaque armée à des fins d'autodéfense. Le Groupe international d'experts était divisé sur le point de savoir si de telles attaques constitueraient des attaques armées, (23) mais comme cela a été dit précédemment dans le contexte de l'usage de la force, il ne sera pas déraisonnable de traiter une attaque débilitante ou extrêmement perturbatrice comme une attaque armée à des fins d'autodéfense. Mais ils reste encore des points a remarqué telle de l'attribution de la responsabilité et les moyens d'envisager à une cyberattaque **(Chapitre 1)**, finalement les principes que la réponse a certains attaques doit les respecter **(Chapitre 2)**.

CHAPITRE 1: Faire face aux Cyber-attaques et Responsabilité

SECTION 1: L'attribution de la responsabilité

Avant de recourir au droit de légitime défense il faut attribuer la responsabilité au Etat qui mène l'attaque cybernétique. Cette dernière (l'attribution) est une composante essentielle du régime de recours à la force, car elle détermine qui sera la cible de la contre-force. Le Manuel traite des critères d'attribution applicables dans la section sur la responsabilité de l'État. Selon le manuel, toutes les utilisations de la force commises par ses organes (24) peuvent être

attribuées à un État, par des personnes ou des organes habilités à exercer une autorité gouvernementale [25] ou par des personnes ou des groupes placés sous l'instruction, la direction ou le contrôle de l'État. [26] À cette dernière norme, il existe un désaccord sur le point de savoir si le seuil requis est celui de « contrôle effectif » - comme la CIJ l'a jugé dans les affaires de génocide de la Bosnie [27] - ou si le seuil requis est « contrôle effectif » a des groupes non organisés et « contrôle global » dans le cas des groupes organisés. [28]

Le Manuel n'énonce pas sa position sur la question. [29] C'est regrettable car, comme on l'a dit, l'attribution est essentielle au recours à la force. En outre, il n'est pas établi que les critères d'attribution applicables ne sont que ceux contenus dans la loi de responsabilité de l'Etat. IL convient de rappeler que la CIJ a accepté que différents critères d'attribution puissent s'appliquer à différentes situations. [30] Alors, Après les attentats du 11 septembre 2001 et en particulier les attaques terroristes, les critères d'attribution de la « tolérance » et de La « réticence » a été mentionnée et la CIJ les a bien accueillis dans l'affaire Congo Vs Ouganda. [31] Par conséquent, si un État tolère des groupes qui lancent des cyberattaques contre un autre État ou ne sont pas disposés à réprimer leurs activités, la, les attaques seront attribuées à cet État qui deviendra alors la cible d'une action d'autodéfense.

Le Manuel ne traite pas de la question de savoir si des critères d'attribution supplémentaires existent, mais examine plutôt la question de savoir si un État peut agir directement contre des groupes situés dans un autre État ou contre des groupes qui utilisent des biens situés dans un autre État.

Pour la majorité des membres du groupe international d'experts, l'État victime peut prendre des mesures d'autodéfense contre des acteurs non-étatiques lorsque l'État ne veut pas ou ne peut pas réprimer ses activités à condition que certaines exigences procédurales soient satisfaites. Une minorité du groupe était d'avis qu'il était inadmissible de le faire. [32]Lorsqu'un État est incapable de contrôler des acteurs non étatiques, il va de soi que les acteurs non étatiques deviennent la cible directe de l'autodéfense mais État n'est pas disposé à les contrôler. Comme on l'a dit la règle 7 du Manuel (2013) indique que: *« le simple fait qu'une cyber-opération ... n'est pas une preuve suffisante pour attribuer l'opération à cet État, mais indique que l'État en question est associé avec l'opération »* dans ce cas les preuves techniques sont importantes pour attribuer la responsabilité.

Pratiquement aussi, Il a également été soutenu que depuis les attentats du 11 septembre 2001 sur le sol américain, les États ont un droit de légitime défense contre les attaques terroristes s'ils sont autorisés par les résolutions du Conseil de sécurité de l'ONU, telles que les résolutions 1368 et 1373 du Conseil de sécurité 2001, adoptée après les attentats du 11 septembre.

Ce qui était le cas, les résolutions adoptées par le Conseil de sécurité des Nations Unies ont autorisé l'exercice du droit de légitime de défense contre l'Afghanistan, L'État a habité et soutenu Al-Qaïda à ce moment-là, [33] compliquant

ainsi, ou aidant et encourageant, les attentats terroristes d'Al-Qaïda du 11 septembre.

SECTION 2: Riposter à une cyber-attaque :

Il est plus pertinent d'analyser le sujet des contremesures **(1)** avant de parler des moyens de riposter à une cyber-attaque soit individuelle ou collective et soit avec les même moyens Cybernétiques ou avec d'autres moyens conventionnels **(2)**, même si ces mesures refaites une partie de ces moyens, mais la question du temps fait la distinction entre les sujets.

1. Les contremesures à une Cyber-attaque :

La CIJ dans le projet Gabčíkovo-Magymaros (Hongrie / Slovaquie) a élaboré trois conditions pour une contre-mesure justifiable:

1. *L'État doit être prise en réponse à un fait international illicite antérieur d'un autre État et doit être dirigée contre cet État;*
2. *L'État lésé doit avoir demandé à l'État qui a commis l'acte illicite de mettre fin à son comportement illicite ou d'en réparer le dommage;*
3. *Les effets d'une contre-mesure doivent être proportionnés au préjudice subi, compte tenu des droits en question.* [(34)]

Selon le manuel de Tallinn, les contre-mesures dans le contexte cybernétique peuvent ne pas être assimilables à une « attaque armée ». [(35)] Comme le coordinateur du Manuel de Tallinn Michaël N. SCHMITT l'a souligné ailleurs, *« le seul but des contre-mesures est d'une situation à la licéité » ou à « un retour à des relations licites entre les États » ou à « encourager la reprise d'interactions licites»*. [(36)]

Il ne serait donc pas logique d'aggraver la situation internationale en recourant à une attaque armée en réponse à un fait internationalement illicite antérieur d'un autre État qui ne donne pas naissance au droit de légitime défense de l'État victime en premier lieu.

Enfin, la Légitime défense préventive et légitime défense préemptive dans le cyberespace est clair selon L'article 51 de la CNU, reconnait le droit à la légitime défense lorsque l'agression armée est avérée, c'est-à-dire lorsque les effets ont été causés ou sont en train de causer des dommages. Au vu des situations actuelles, un État peut se défendre lorsque l'agression armée est imminente. On se place ainsi dans le cadre de la légitime défense préemptive. Le Manuel de Tallinn a été d'un grand secours pour les juristes lorsqu'il s'agit d'envisager la légitime défense dans le cas des cyber-attaques. La règle 15 (2013) énonce que:

« Le droit d'user de la légitime défense se pose à partir de l'instant où on fait face à une cyber-attaque armée venant de se produire ou qui est imminente. Ce droit reste, en outre, soumis à l'exigence de l'immédiateté ».

2. Moyens et mesures légitimes pour L'envisager.

Pour riposter à une cyber-attaque, l'article 51 de la Charte des Nations unis est très clair: On peut soit envisager de répondre à une agression armée de façon individuelle, soit de façon collective. C'est en fonction de l'État et de l'impact qu'a

eu l'attaque vis-à-vis de la Communauté internationale et plus précisément des États Membres; et surtout cela dépend de l'État ayant subi l'attaque **(a).**

Par ailleurs, outre le fait de savoir qui participera à la légitime défense, IL convient de se demander également quels seront les moyens de réponses envisagés: cybernétiques ou conventionnels **(b).**

a. L'utilisation de la légitime défense d'une façon individuelle ou collective:

L'article 51 de la Charte est clair:

« 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... »

La légitime défense collective permet de justifier le recours à la force en réaction à une cyber-attaque. Aux termes de la CNU, il est clair qu'une série d'attaques informatiques constituerait un recours à la force, et que de façon comparable une série de contre-mesures relèverait de la légitime defense. [(37)]

Outre, l'Organisation des Nations Unies qui a développé ce principe de légitime défense dans sa Charte, on retrouve aussi cette notion dans le Traité de Lisbonne et dans le Traité de l'Atlantique Nord.

Le Traité de Lisbonne du 13 décembre 2007 est un texte de l'Union européenne qui a renforcé la solidarité des États membres face aux menaces extérieures en introduisant une clause de défense mutuelle que l'on retrouve à l'article 42(7) (T.UE). Au cas où un État membre serait l'objet d'une agression armée sur son territoire, les autres États membres lui doivent aide et assistance par tous leurs moyens, conformément à l'article 51 de la CNU relatif à la légitime défense. Cette disposition a une portée novatrice puisqu'elle affirme pour la première fois une solidarité militaire spécifique aux États membres de l'Union et distincte du lien transatlantique. Cette disposition est complétée par la clause de solidarité figurant à l'article 222 (T.UE), pour ce qui concerne les autres menaces (terrorisme, catastrophes d'origine humaine ou naturelle).

Le Traité de l'Atlantique Nord du 4 avril 1949 vient également appuyer et compléter la Charte puisque dans son article 4, il est convenu que les parties se consulteront chaque fois que, de l'avis de l'une d'elles, l'intégrité territoriale, l'indépendance politique ou la sécurité de l'une des parties sera menacée. C'est-à-dire qu'à partir de l'instant où un État partie fait l'objet d'une attaque, les autres États membres étudieront la situation mais devront tout de même attendre d'avoir l'aval de l'État victime pour agir. C'est ce qu'énonce également le Manuel de Tallinn dans sa règle 16 (2013):

« Le droit de légitime défense peut être exercé collectivement. Le recours à la légitime défense collective employée en réponse à une cyber-opération s'élevant au rang d'attaque armée ne peut s'effectuer qu'à la demande de l'État victime et seulement dans le cadre de cette demande ».

Ainsi, tous les textes reconnaissent la légitime défense, qu'elle soit individuelle ou collective, comme étant possible en cas d'agression armée. La légitime défense collective est autorisée lorsque l'État victime demande assistance. Elle doit être menée dans le cadre d'un accords de défense ou par l'intermédiaire d'un accord au sein de l'OTAN, par exemple. Quant à la légitime défense préemptive, « celle-ci fait encore débat ». Les critères de menaces imminentes, ripostes immédiates doivent être étudiés tout en respectant le Principe de nécessité (l'utilisation d'autres réponses comme la diplomatie, les sanctions économiques etc.) et de riposte proportionnelle à l'attaque cyber (pas d'attaques cyber ou non cyber plus violentes).

b. Les moyens de réponses envisagés: conventionnels ou cybernétiques?

À partir de l'instant où on considère que l'arme cybernétique peut être qualifiée d'attaque armée, cela sous-entend forcément qu'elle sera placée au même niveau que l'attaque conventionnelle. De ce fait, les moyens de réponses envisagés peuvent être soit conventionnels, soit cybernétiques, voire même, peuvent être combinés. Chaque État à sa propre position sur le sujet, mais la plupart n'excluent aucune option.

1) **Les États-Unis** considérant, depuis la cyber-attaque qu'ils ont subie le 28 mai 2011, les armes cybernétiques comme relevant de « l'acte de guerre », ont annoncé qu'ils attendraient d'avoir utilisés tous les moyens dont ils disposent en matière cyber avant d'envisager l'usage de la force conventionnelle.
2) **La Corée du Sud, comme Taïwan**, se prépare également à faire face à des cyber-attaques chinoises en développant leur stratégie offensive et défensive. Ces États ont développé leurs forces cyber se préparant, au vu des tensions géopolitiques en Asie, à s'affronter d'une manière ou d'une autre dans le cyberespace.
3) **Le Japon** a également annoncé le renforcement à venir de ses capacités de cyberdéfense. Celui-ci souhaitait depuis plusieurs années développer une véritable unité de cyberdéfense mais s'était heurté au refus du Ministère des Finances de se voir attribuer les fonds nécessaires. C'est à présent chose faite puisque le rapport définit le cyberespace comme l'infrastructure essentielle aux décisions politiques ainsi qu'aux opérations des unités des SDF (forces d'auto-défense), et le considère comme le cinquième terrain d'opérations militaires. Pour prévenir des attaques contre le « cyberespace japonais », l'unité créée devra, développer ses capacités de préparation, ses connaissances techniques d'attaques et s'en trainera par des exercices de simulation. Point le plus important, le rapport stipule que si les cyber-attaques font parties d'une attaque militaire plus large, le Japon considérera qu'elles justifient son droit à engager des mesures d'auto-défense. Autrement dit, Tokyo se réserve le droit de répondre à des cyber-attaques par tous les moyens d'auto-défense à disposition.[(38)]

4) **L'Algérie** a connait un retard certain dans la production de solutions nationales de Cybersécurité et surtout dans la mise en place de son cadre juridique et organisationnel, et peu de mesures techniques sont abordés aux scènes de la technologie technique (finalité et moyens en même temps), tels les outils et techniques pour détecter les attaques et d'y répondre, à savoir, la surveillance, d'alerte et de réponse, Ces actions peut être mesurée par le nombre d'institutions de Cybersécurité, tels que CERT, CIRT et CSIRT, [(39)] aussi aucun critères sont respectés comme les normes établies par des organismes internationaux tels que l'Organisation internationale de normalisation ISO (Ex ; Norme ISO/IEC 27001), l'Union internationale des télécommunications ITU, [(40)] et l'équipe de l'Internet Engineering Task Force IETF, Et d'autres institutions internationalement accréditées. Ainsi que les certificats ou les licences Mondialement reconnus qui sont pris en charge ou approuvés par les gouvernements tels que le certificat de sécurité dans le nuage (Cloud), certificat Détective de la cybersécurité légale ..

Dans ce contexte, l'Algérie n'a adopté aucune mesure d'urgence ou de sécurité informatique à l'exception de l'organe affilié du centre CERSIT Ce qu'il nommé Dz-Cert et le portail algérien de sécurité de l'information Wikayanet (sont pas encore opérationnels) ou d'autre structure Militaire Comme le service de surveillance de la cyberdéfense et de la sécurité affilié du service de l'emploi et de la motivation (Récemment crée fin 2016) Pour donner suite à des Cyber-attaques contre L'Algérie début d'année 2015. [(41)] Et les algériens ont été rendues publiques. Alors que des opérations de Cyber espionnage de « Equation Group » et « Desert Falcons » utilisent le virus de Cyber espionnage le plus dangereux jamais découvert, et une série de maliciels, Babar, Bunny, Casper, Dino, Nbot et Tafacalou, n'ont été découvertes que récemment alors qu'elles ont débuté depuis des années. [(42)] Et ses victimes tombent généralement dans les catégories suivantes: Gouvernement, Défense, Energie, et Finances. [(43)]

Donc nous remarquons que L'Etat Algérien a fait peu d'efforts dans ce contexte par apport d'autres Etats, L'Algérie doit donc travailler plus dur à cet égard, d'ailleurs Il est clair que ce modèle (CERT, CIRT, CSIRT) n'est plus en phase avec le modèle avancé pour de nombreuses raisons, notamment parce que ce dernier type dépend du nombre de personnes compétentes pour développer une stratégie offensive et une cyberdéfense dans le cadre de leur potentiel militaire de confrontation pour envisager a n'importe cyber-guerre possible et en complément de la guerre technologique et même de faire la distinction des attaques militaires et autres attaques criminelles régulières et les infiltrations ou un acte d'hacktivisme.[(44)]

Ainsi les cyber-attaques sont bel et bien envisagées en tant que moyens de riposte. Cependant, il y a certains critères qu'elles se doivent de respecter et Marco Roscini les énonce très clairement dans son livre intitulé « Cyber Operations and the Use of Force In international Law » : [(45)] *« La réaction en auto-*

défense contre les cyber-opérations s'élevant à des attaques, comme toute réaction d'autodéfense contre des États ou des acteurs non étatiques, doit répondre aux exigences de nécessité, de proportionnalité et d'immédiateté ». [(46)]

CHAPITRE 2: L'obligation de respecter avant tout certains principes

Comme pour les attaques conventionnelles lancées dans le cadre de la légitime défense, les cyber-attaques se doivent de respecter trois principes essentiels en ce domaine : la Nécessité et proportionnalité **(Section 1)**, Imminence et Immédiateté **(Section 2)**, ainsi les processus d'informer le CS.

SECTION : Nécessité et proportionnalité

Selon la règle 14 (2013), *« un usage de la force impliquant des opérations cybernétiques entreprises par un État dans l'exercice de son droit de légitime défense doit être nécessaire et proportionné»*. Les principes de nécessité et de proportionnalité font partie du droit coutumier de légitime défense. [(47)]

En ce qui concerne la nécessité, elle répond à la question de savoir si l'usage de la force par l'autodéfense est le seul moyen de repousser efficacement l'attaque. Dans quelle mesure le critère de nécessité a-t-il une signification pratique? La légitime défense est-elle une réaction à une attaque en cours, où l'exigence de nécessité est peut-être Ipso Facto satisfaite, ou bien une réaction à une attaque immédiate ou prospective? où la nécessité de la légitime défense peut être évaluée par rapport à d'autres moyens de prévention de l'attaque. Il convient toutefois de noter que le principe de nécessité n'exige pas l'épuisement de tous les moyens pacifiques disponibles, mais que la nécessité de la légitime défense est déterminée par le but de l'action de légitime défense que les autres mesures ne peuvent pas respecter. [(48)]

Et même, Article 25 (nécessité) de la CDI projet sur la responsabilité des Etats se dit comme suit:

*« **1.** La nécessité ne peut être invoquée par un État pour faire obstacle à l'illicéité d'un fait qui n'est pas conforme à une obligation internationale de cet État, sauf si l'acte : **a)** est le seul moyen pour l'Etat de sauvegarder un intérêt essentiel contre un péril grave et imminent ; et. **b)** ne porte pas gravement atteinte à un intérêt de l'État ou des États envers lesquels l'obligation existe ou de la communauté internationale dans son ensemble.*

***2.** En tout état de cause, la nécessité ne peut être invoquée par un État pour empêcher l'illicéité si : a) l'obligation internationale en question exclut la possibilité d'invoquer la nécessité ; ou b) l'État a contribué à la situation de nécessité. »* [(49)]

La proportionnalité est liée à l'intensité, l'ampleur, la portée et la durée de l'action d'autodéfense mesurée par rapport à son objectif. La proportionnalité peut être assez élastique selon que l'objectif de l'action de légitime défense est de repousser l'attaque, d'empêcher de futures attaques ou d'éliminer la source de la menace.

De façon simple, le principe de proportionnalité se fonde sur le fait qu'une attaque cybernétique qui causerait accidentellement des pertes civiles, des blessures aux personnes ou des dommages aux biens civils, ou une combinaison de ces facteurs et qui serait excessive au regard de l'avantage militaire recherché est interdite. L'opération est donc proscrite lorsque les dommages collatéraux sont excessifs au regard de ce que la cyber-attaque aurait dû causer accidentellement et les résultats de l'avantage militaire attendu pour cette attaque. Seuls les dommages excessifs au regard des conséquences concrètes et directes d'un avantage militaire recherché sont prohibés. Le terme « excessif » n'a pas été quantifié dans le Manuel par les experts internationaux. Malgré le commentaire contradictoire du CICR, ces derniers ont considéré que les dommages collatéraux sont autorisés seulement si l'anticipation concrète et directe de l'avantage militaire est suffisante au regard de toute l'attaque.

Il ressort de ce qui précède que la nécessité et la proportionnalité ne sont pas des « critères stricts et objectifs », comme l'a dit la CIJ, **(50)** mais plutôt des critères flexibles et contextuels ; et comme le dit le Manuel, ils sont jugés du point de vue de la victime-Etat. **(51)**

Ceci conduit à la question suivante, à savoir si la nécessité de l'autodéfense est éclipsée une fois que le Conseil de Sécurité des Nations Unies intervient. Il convient de rappeler que, conformément à l'article 51 de la CNU, la légitime défense est un droit provisoire jusqu'à ce que le Conseil de sécurité prenne les mesures nécessaires pour maintenir la paix et la sécurité internationales. Le Manuel reconnaît l'autorité du CS de se dessaisir expressément de son droit de légitime défense et de prendre des mesures parallèlement à la légitime défense, mais ne dit pas, en l'absence d'une décision claire du CS, quelles mesures peuvent être cédées? Le droit à l'autodéfense est un état qui détermine que le droit est devenu superflu. **(52)** Le raisonnement qui sous-tend l'article 51 et le système de sécurité collective des Nations Unies va dans le même sens que la nécessité de la légitime défense ne s'applique que lorsque le comité de surveillance prend des mesures efficaces qui se substitueront au droit de légitime défense.

En ce qui concerne la question de savoir qui détermine que les mesures sont nécessaires, le CS et l'État victime peuvent le faire: parce que le CS a ce pouvoir en vertu de la Charte et de l'État et le droit à la légitime défense est un droit individuel. Cela signifie que les évaluations peuvent différer mais, à moins qu'il y ait une détermination claire du CS, l'évaluation de l'État devrait prévaloir. Souvent, le CS, lorsqu'il agit en vertu du chapitre VII, reconnaît également le droit à la légitime defense. **(53)**

SECTION 2: Imminence et Immédiat

La Règle 15 du manuel prévoit que: *« Le droit de recourir à la force en cas de légitime défense survient si une cyberattaque est commise ou est imminente. Il est en outre soumis à une exigence d'immédiateté»*.

La question critique est de savoir comment l'imminence est interprétée. La majorité du groupe international d'experts a rejeté le critère temporel dans l'interprétation de l'imminence et a adopté la norme de la « dernière fenêtre d'opportunité », selon laquelle un État peut recourir à la légitime défense dès qu'il juge que l'absence d'action entravera sa capacité à se défendre efficacement lorsque l'attaque est finalement lancée. **(54)** La prise en considération de critères factuels et temporels est raisonnable et inévitable, en raison de la nature des cyber-armes. Il apparaît cependant que les mesures d'autodéfense peuvent être prises longtemps. Avant que l'attaque ne soit sur le point de se produire, la ligne entre l'autodéfense anticipée et préventive (c'est-à-dire l'action défensive contre une attaque potentielle) s'effondre. Par exemple, quand est la « dernière fenêtre d'opportunité » si les capacités technologiques ou autres de l'état affecté sont également prises en compte?

Le Manuel introduit une forme de sauvegarde quand il dit que l'attaque prospective ne doit pas être spéculative, mais que la décision d'attaquer doit avoir mûri**(55)**. Que la décision ait mûri peut-être déduite d'actes, de comportements, de déclarations et, de façon cruciale, à partir des informations de renseignement, bien qu'il soit toujours difficile de tirer des conclusions définitives de ces preuves. Par exemple, si l'attaque Stuxnet est placée dans le contexte de déclarations belliqueuses contre l'Iran, pourrait-on conclure que la décision d'utiliser la force a mûri? Cela indique que la disponibilité et la probité de l'information sont essentielles pour évaluer l'imminence et la distinction entre auto-défense préventive et préventive, mais que les informations sur les capacités ou les intentions d'un autre État peuvent être difficiles à recueillir ou à vérifier. L'information sera secrète. Par conséquent, les décisions sur la question de savoir si le seuil d'imminence a été atteint seront politiques et, comme le dit le Manuel, dépendent du « caractère raisonnable de l'évaluation de la situation par l'État victime ». **(56)**

En ce qui concerne le critère de l'immédiateté, il faut que l'action de légitime défense soit très proche de l'attaque initiale. Une fois de plus, cette exigence est contextuelle. Il faut tenir compte des préparatifs précédant l'action d'autodéfense, des processus politiques ou autres pour trouver une solution, ou des enquêtes pour identifier l'auteur de l'attaque. Ainsi, les limites de l'immédiateté peuvent être étendues.

Ces quatre critères sont donc essentiels pour que puisse être envisagée une riposte pour donner suite à une agression armée et ce, dans le cadre de la légitime défense exposée à l'article 51 de la CNU. Cependant, une condition très claire revient perpétuellement celle de tenir informée le Conseil de sécurité de la situation en cours afin que ce dernier puisse trouver une solution au conflit en cours pour éviter que cela ne devienne une menace à la paix et à la sécurité internationales.

En matière de légitime défense, le Manuel de Tallinn a été clair concernant le rôle à jouer du Conseil de sécurité. La règle 18 déclare:

« Si le Conseil de Sécurité des Nations Unies détermine qu'un acte constitue une menace pour la paix, une rupture de la paix ou un acte d'agression, il peut autoriser des mesures non-agressives, y compris Les opérations informatiques. Si le Conseil de sécurité estime que ces mesures sont insuffisantes, il peut prendre des mesures énergiques, y compris des mesures de cybersécurité ». Cette règle se fonde sur le Chapitre 7 de la Charte des Nations Unies;

« Action en cas de menace contre la paix, de rupture de la paix et d'acte d'agression ». Le Conseil de sécurité a pour rôle de constater l'existence d'une menace à la paix et à la sécurité internationale, d'une rupture de la paix ou d'un acte d'agression. Celui-ci prendra des mesures en vertu des articles 41 et 42 de la présente Charte pour maintenir ou rétablir la paix et la sécurité internationals. **(57)**

La liste exposée dans cet article (41) est non exhaustive. C'est ce que souligne le Manuel de Tallinn. La référence faite à l'interruption complète des communications postales, télégraphiques, radioélectriques et des autres moyens de communication sont très importantes lorsqu'on se place dans le contexte cyber. Cela signifie - dans le cadre de cet article - que le Conseil de sécurité peut décider de l'interruption partielle ou totale des communications cybers avec un État ou un acteur non étatique.

Ainsi, tandis que l'article 42 indique que les mesures d'application peuvent être prises par air, mer, terre par les forces des États membres des Nations Unies, le Groupe international d'experts a convenu que toute action entreprise sur la base de cette règle peut être mise en œuvre pour, ou contre, les capacités du cyberespace.

Conclusion:

Au terme de cette étude, nous retiendrons que la jurisprudence des spécialistes et experts (les Manuels internationals) joue toujours un rôle central dans la compréhension et la clarification des faits, notamment en l'absence de droit conventionnel qui énonce les règles du recours à la force dans le cyberespace, qui repose principalement sur l'interprétation du contenu de la Charte des Nations Unies.

Les principales conclusions normatives peuvent être résumées dans:

Premiérement, Les cyberattaques qui cause des dommages matériels, des pertes de vie, des blessures à des personnes ou bien une perturbation grave du fonctionnement des infrastructures critiques de l'Etat sont qualifies en t'ant des attaques armées, sont interdites par l'article 2(4) de la CNU et son équivalent coutumier selon les experts. Dan's tous les cas meme ses attaques ne causant pas ses effets Ils restent des interventions illégales dans les affaires intérieures d'autres États.

Deuxiément, L'autodéfense cybernétique ou cinétique en vertu de l'article 51 de la Charte et le droit international coutumier peuvent être exercés contre une cyberattaque d'un État ou d'un acteur non étatique uniquement dans la mesure où

elle constitue une « attaque armée », lorsque la cybersécurité assimilable à un recours à la force répond à la norme « échelle et effets » identifiée par la CIJ.

Troisièmement, la norme de preuve pour les allégations de légitime défense contre des cyber-opérations équivalant à une attaque armée ne diffère pas de celle applicable à la légitime défense contre des attaques cinétiques armées et nécessiterait normalement des « preuves claires et convaincantes ».

Et Enfin, Le chercheur recommande Ce qui suit:

La communauté internationale doit aller de l'avant pour examiner l'impact des nouvelles technologies pendant la guerre et pour élaborer des règles juridiques contraignantes permettant aux États de se conformer strictement à la Charte des Nations Unie, Dans ce contexte, il est recommandé de suivre les travaux, notamment en ce qui concerne le rapport basic **(A/68/98) 2013)** publié par le Groupe d'experts gouvernementaux sur les développements en matière d'information et des télécommunications dans le contexte de la sécurité international.

Il est également recommandé que l'Etat algérien doit donc travailler plus dur à cet égard, Notamment sur la gouvernance de l'Internet et de rester loin de la logique de protection de la sécurité publique au détriment des libertés et des droits des individus, Ce dernier s'illustre à travers l'article (02) l'alinéa (a) de la loi 09-04 qui n'a pas limité le nombre de crimes liés à la cybercriminalité, il est clair que cette régle est contraire au principe de légalité, qui conduit à la persistance de la peine et de la criminalisation. Enfin, Grâce à cette initiative, la gouvernance de l'Internet pousse l'État algérien à progresser pour atteindre les rangs des pays développés en matiére de cyber sécurité, pour ensuite bien négocier à l'échelle mondiale afin de préserver les intérêts nationaux de l'Algérie et les Etats en voie de développement.

RÉFÉRENCES:

(1) Major SCHAPP Arie J, Cyber Warfare operations: development and use under international law, Air Force Law Review, Cyberlaw edition, 2009, P 33.

(2) Le Commandant de l'US Cyber Command a fait l'observation suivante : «*il n'existe aucun consensus* international concernant une définition précise de ce qui relèverait de l'emploi de la force, que ce soit dans ou en dehors du cyberespace. Par conséquent, chaque nation a établi sa propre définition et applique ses propres critères (seuils) de ce qui serait susceptible d'être caractérisé comme relevant de l'emploi de la force. » Idem, Major SCHAPP, P 34.

(3) Laura Baudin, Les cyber-attaques dans les conflits armés : qualification juridique, imputabilité et moyens de réponse envisagés en droit international humanitaire, L'harmattan édition, Paris, 2014, P 112.

(4) En 2009, un petit groupe d'experts juridiques et techniques internationaux s'est réuni au Centre d'excellence de la cyberdéfense de l'OTAN à Tallinn, en Estonie, à l'invitation de ce centre pour discuter de la nécessité de rédiger un manuel traitant de la cyber-guerre. Ce qui, à l'époque et même au moment de la rédaction, était considéré comme étant à ses débuts. La décision a été prise de procéder à un projet de rédaction d'un tel manuel et, en 2013, le manuel de Tallinn 1,0 a été publié.et en 2016 la version manuel Tallinn 2,0 a été publié.

(5) Ces critères quantitatifs et qualitatifs sont :

- La sévérité des dommages Gravité (Severity) : L'attaque doit provoquer des dommages physiques.
- L'immédiateté (Immediacy) : Les conséquences de l'acte doivent survenir immédiatement.
- La cause à effet Le caractère indirect (Directness) Les conséquences de l'acte doivent résulter directement de l'intention.
- Le degré d'invasion-pénétration dans le système Le caractère invasif (Invasiveness) Ce critère se définit par rapport à l'intrusion opérée sur l'État ciblé, plus à même d'entrainer une instabilité internationale.
- L'évaluation des effets Mesurabilité (Measurability) Ce critère ne s'attarde pas sur la dimension économique mais sur les dommages et le degré de souffrance causés.
- Le caractère militaire Légitimité présumée (Presumptive legitimacy) Celle-ci présuppose que les formes de coercition plus « douces » sont plus légitimes que celles employant la violence.
- L'implication de l'État et encore la présomption de légalité Responsabilité (Responsability) Un État engage sa responsabilité lorsque ce dernier est l'instigateur du lancement de cyber- opérations.

(6) Michaël N. SCHMITT, Cyber operations and the jus ad bellum revisited, Villanova Law review, volume 56, 2011, p 569.

(7) Règle 11 (2013), paragraphes 1 et 8.

(8) Institut des Nations Unies pour la recherche sur le désarmement (UNDIR) Forum du désarmement N° 4 intitulés « Faire Face aux Cyber conflits », 2011, P 21.

(9) Adel AbdeSadek, Les armes Cybernétiques à la lumière du droit international humanitaire, série Awrak, N° 23, Unité des études futures, Bibliothéque Alexandrina, 2016, P 89.

(10) Certains États et Organisations internationales ont défini ce qui pour eux représente une infrastructure critique :

États-Unis : *Les infrastructures critiques correspondent non seulement aux infrastructures physiques mais également aux cybers et incluent (mais ne se limitent pas qu'à cela) les télécommunications, l'énergie, les finances et les banques, le transport, l'approvisionnement en eau et la santé publique, que tout cela relève du secteur public ou privé. Le terme « infrastructure critique » désigne des systèmes physiques ou virtuels, considérés comme vitaux pour les États-Unis. Leur incapacité ou leur destruction aurait un impact sur la sécurité nationale ainsi que sur la sécurité économique et sur la santé publique de l'État ou une combinaison de tout cela.*

The White House, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", 2003, p. 35.

Voir aussi: The White House, International Strategy for Cyberspace, 2011, p. 3.

(11) Mouna Al Achkar Djebor, Cyber, obsède du siècle, Centre arabe de recherche juridique et judiciaire, Ligue des Etats Arabes,2014, P 88.

(12) De façon plus large, les relations Internationales peuvent être étudiées en termes de rapports transfrontaliers. Ces derniers sont entretenus par différents acteurs : les États, les Organisations Internationales, les Organisations non- gouvernementales…

Voir ; Kazim hachem Niimaa, la théorie des relations Internationales, institut des études supérieurs et les recherches économiques, tripoli, Libye, 1999, P 15.

(13) Exemple ; l'Affaire Stuxnet qui a touché, outre les ordinateurs de la centrale nucléaire de Natanz, ceux de plus d'une centaine de pays à Travers le monde dont des Etats qui auraient eux-mêmes lancés la cyber-attaque (Etats-Unis et L'entité sioniste (Israël)).

(14) J.P. Farwell et R. Rohozinski, Stuxnet and the Future of Cyber War, Survival, vol. 53, N° 1, 2011, P. 23-40.

(15) Laura Baudin, Les cyber-attaques dans les conflits armés, Op.cit. P 110.

(16) Paul Rosenzweig, Cyber warfare; How conflicts in Cyberspace are challenging America and changing the World, The Changing Face of War, James Jay Carafano, Series Editor, PREAGER Edition, Oxford, England, 2012, P 17-29.

(17) ZEMANEK Karl, Armed attack in Rüdiger Wolfrum, Max Planck Encyclopedia of Public International Law, 2010, P 21.

(18) Affaire relative aux actions militaires et paramilitaires de (Nicaragua Vs États-Unis d'Amérique), CIJ Rep. 1986, p. 14, par. 34, 48, 187-201.

(19) Svetlana Zasova, "La légitime défense des Etats et la guerre cybernétique," Revue de Société Française pour le Droit International, Colloque de Rouen : Internet et le droit international, Editions A. Pedone Paris, 2014, P, 265–275.
(20) Affaire aux actions militaires et paramilitaires au Nicaragua contre USA, Ibid. p. 16.
(21) Kriangsak Kittichaisaree, Public International Law of Cyberspace, Law, Governance and Technology Series, Volume 32, Springer International Publishing Switzerland, 2017, P 166.
(Kriangsak Kittichaisaree est un membre aux premières commissions de désarmement de l'ONU, aussi un expert participant aux préparations de manuel de Tallinn)
(22) *Règle 11, para 7 (2013)*. Voir aussi. Harold Hongju Koh, Droit international dans le cyberespace, Conférence juridique inter institutions USCYBERCOM (18 septembre 2012), disponible sur:
http://www.state.gov/s/l/releases/remarques/197924.htm Accédé le 23/07/2018.
Règle 13, para *9 (2013)* et le même cas pour *la règle 71 para 13 (2016).*
(24) *Règle 6, para 6-7 (2013.*
(25) Ibid., para 8.
(26) Ibid., para 9.
(27) Affaire concernant l'application de la Convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine Vs Serbie-et-Monténégro) Arrêt du 26 février 2007, CIJ, par. 402-406.
(28) L'affaire de Tadic, 15 July 1999, para 131. Le Tribunal pénal international pour l'ex-Yougoslavie.
(29) Règle 6 (2013), para 10.
(30) Le Tribunal pénal international pour l'ex-Yougoslavie, Ibid. para 404-405
(31) Kriangsak Kittichaisaree, Op.cit. P 168.
(32) Knut Dörmann, « Computer Network Attack and International Humanitarian Law », ICRC, Extract from The Cambridge Review of International Affairs "Internet and State Security Forum", 19 May, Trinity College, Cambridge, UK. 2001.
https://www.icrc.org/eng/resources/documents/article/other/5p2alj.htm Accédé le 27/07/2018.
(33) Lindsay Moir, Reappraising the Resort to Force: International Law, Jud ad Bellum and the War on Terror, Oxford: Hart Publishing, 2010, P 32.
(34) Kriangsak Kittichaisaree, Op.cit. P 191.
(35) Règle 9 (2013), para 5.
(36) Michael N. Schmitt, Katharina Ziolkowski, "Cyber Activities and the Law of Countermeasures," in Peacetime Regime for State Activities in Cyberspace, (Tallinn: NATO CCD COE, 2013), 659.
(37) Laura Baudin, Op.cit. P 125.
(38) Site internet Géopolitique et enjeux stratégiques du cyberespace, Japon : la cyberdéfense va devenir un élément majeur des Self-Defense Forces. Crée le 11/09/2014. Accédé le 28/007/2018.
(39) CERT : (computer Emergency Response Team) Équipes d'intervention d'urgence informatique ;
CIRT : (computer incident Response team) Équipes d'intervention en cas d'accident informatique ;
CSIRT : (Computer Security Incident Response Team) Equipes de réponse aux incidents de sécurité informatique. Aujourd'hui ont trouvons plusieurs CERT's dans différents domaines dans un seule Etat.
(40) Report World Index for cybersecurity and cyber safety features 2017, ABI Research and ITU, P 32.
(41) ELACHEACHE Ishak, Cyberterrorisme et défis des Etats, Un document de recherche présenté dans la journée d'étude surnommé « le Model algérien de lutte contre le terrorisme » organisée par l'Ecole Nationale des Sciences Politiques ENSSP, le 13 Mars 2018, P 15.
(42) Abdelaziz Derdouri, Une loi sur la Cybersécurité pour L'Algérie ? Journal Le Soir D'Algérie, Mardi le 28 avril 2015, P 6.
(43) Meriem Ali Marina. Centre de prévention et de lutte contre la criminalité informatique et la cybercriminalité « Les gendarmes du Net », El Djazair magazine, le 28 juin 2015. P 23.
(44) ELACHEACHE Ishak. Op. Cit, P 16.
(45) Marco Roscini, Cyber Operations and the Use of Force In international Law, The Leverhulme Trust, Oxford University Press, First Edition, 2014, P 88.
(46) Règle 14 et 15 de Tallinn Manuel (2013), pp 61, 63.

(47) Affaire relative de (Nicaragua Vs USA), CIJ Rep. 1986, par. 176, 194, 237.
(48) Le Guide de Tallinn (2013) Règle 14, Paras 2.
Voir aussi Guide de Tallinn (2016) Règle 72, Para 2.
(49) L'exemple classique de cet abus est peut-être l'occupation du Luxembourg et de la Belgique par l'Allemagne en 1914, une occupation que l'Allemagne a essayé de justifier par nécessité
(50) Affaire concernant les plates-formes pétrolières (République islamique d'Iran Vs États-Unis d'Amérique), arrêt du 6 novembre 2003, (2003), CIJ Rep. 161, par 73.
(51) Règle 14 (2013), para 4.
(52) Règle 17 (2013), para 2–3.
(53) L'affaire de L'Irak Vs le Kuwait 1990 (Invasion et Occupation), Rés 661 le 6 Aout 1990.
(54) Règle 15 (2013), para 4.
(55) Op.cit., para 7.
(56) Op.cit., para 6.
(57) Article 39 CNU.