UNIVERSITÉ DE LILLE

FACULTÉ DES SCIENCES JURIDIQUES, POLITIQUES ET SOCIALES

L'APPLICATION DU DROIT INTERNATIONAL HUMANITAIRE AUX MOYENS ET MÉTHODES DE COMBAT CYBERNÉTIQUES

Mémoire en vue de l'obtention du Master II Justice pénale internationale, présenté et soutenu par

Mathieu CALLOCH

Sous la direction du professeur Muriel UBÉDA-SAILLARD

Année universitaire 2018/2019

REMERCIEMENTS

En premier lieu, je tiens à remercier Madame Muriel Ubéda-Saillard, professeur en droit public et directrice du Master II Justice pénale internationale au sein de l'Université de Lille. En tant que directrice de mémoire, elle m'a guidé dans mon travail et je la remercie pour la justesse des conseils prodigués durant l'année écoulée.

Je remercie également la promotion 2018/2019 du Master II Justice pénale internationale qui m'a permis de m'épanouir dans un cadre de travail particulièrement enrichissant. Après six années dans le monde universitaire, j'ai le plaisir de dire que la plus belle de toutes s'est déroulée à Lille.

Je tiens à remercier spécialement ma compagne, qui m'a soutenu tout au long de la rédaction de ce mémoire. Sa patience, ses encouragements, sa confiance en moi, sa sollicitude et son engouement pour mon travail ont été de véritables moteurs dans la dernière ligne droite.

Je tiens à remercier ma famille, qui m'a toujours soutenu dans le cadre de mes études et de mes projets et n'a eu de cesse de m'encourager dans le cadre de la rédaction de mémoire.

SOMMAIRE

• Introduction

Le 5 mai 2019, par le biais d'un tweet, les Forces de Défense Israéliennes annonçaient avoir contrecarré une cyberattaque du Hamas. L'opération défensive se serait déroulée à la fois dans le cyberespace et dans l'espace tangible : dans le cyberespace, où les militaires spécialisés israéliens auraient mis en échec l'offensive du groupe armé ; dans l'espace tangible, lorsqu'une frappe aérienne a visé l'immeuble depuis lequel les cyber-combattants ennemis étaient soupçonnés d'opérer[1]. Cette riposte hybride à une attaque cybernétique constituerait *a priori* une première, notamment dans la relation attaque cybernétique-riposte cinétique[2]. Alors que les experts des mondes militaires et juridiques s'évertuent depuis maintenant plusieurs années à déterminer dans quelle mesure s'applique le droit international humanitaire aux opérations militaires cybernétiques, cet évènement sonne comme le rappel que toutes les problématiques liées au phénomène de cybernétisation de la force n'ont pas trouvé leur solution. Avant d'aborder ledit phénomène et ses implications sur l'application du droit international humanitaire, il est nécessaire de délivrer des explications sur le vocabulaire qui sera employé.

Il est d'abord important de traiter les notions de cybernétique et de cyberespace pour expliquer ce qu'évoque l'expression de cybernétisation de la force et des conflits armés.

---

[1] Compte Twitter des Forces de Défense Israéliennes, « *We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work* », 5 mai 2019, consulté en ligne le 27 juillet 2019. Disponible en ligne : « https://twitter.com/IDF/status/1125066395010699264 ».V. également : M. UNTERSINGER, « Israël dit avoir déjoué une cyberattaque du Hamas à Gaza, avant de frapper le site d'origine », *Le Monde*, 6 mai 2019, consulté en ligne le 27 juillet 2019. Disponible en ligne : « https://www.lemonde.fr/pixels/article/2019/05/06/israel-dit-avoir-replique-a-une-attaque-informatique-par-une-frappe-aerienne-une-premiere_5459063_4408996.html?xtor=RSS-3208 »

[2] La frappe effectuée par les États-Unis contre Junaid Hussain, un cyber-combattant de l'État Islamique, en août 2015, ne peut pas être appréhendée de la même manière que la frappe évoquée ici. En effet, cette opération n'a pas été effectuée en réponse immédiate à une cyber-attaque, elle s'inscrit davantage dans la stratégie de frappes « chirurgicales » menée par les États-Unis contre les cibles jugées d'intérêt.

Le préfixe *cyber* doit être rattaché à la cybernétique. La cybernétique est imaginée par Norbert Wiener, appuyé par un collège de chercheurs, comme une science centrée autour de la notion de rétroaction, visant à englober notamment les disciplines de l'automatique et de l'électronique. Il la qualifie de « *théorie entière de la commande et de la communication, aussi bien chez l'animal que dans la machine* »[3]. Le dictionnaire de la langue anglaise de Cambridge évoque « *the scientific study of how information is communicated in machines and electronic devices, comparing this with how information is communicated in the brain and nervous system* »[4]. Celui de l'Académie française parle de la « [s]*cience des systèmes dans lesquels l'effet obtenu agit à son tour, par rétroaction, sur le mécanisme provoquant cet effet, afin d'obtenir un résultat constamment adapté au but désiré* »[5]. Sémantiquement, un moyen ou une méthode de combat cybernétique s'entendrait de tout moyen ou méthode pouvant être rattaché à la cybernétique : les moyens et méthodes informatiques, comme les virus ou les attaques par déni de service, mais également certains moyens et méthodes qui suivent les lois de l'automatique, comme les systèmes d'armes létales autonomes. Cependant, et bien que l'on puisse dès lors considérer son emploi comme abusif[6], le terme cybernétique fait très majoritairement référence, dans la doctrine militaire comme juridique, à ce qui touche au cyberespace[7]. La démarche de la présente étude n'étant pas de

---

[3] N. WIENER, *Cybernetics or Control and Communication in the Animal and the Machine*, 2ème édition, Cambridge, The M.I.T. Press, 1948.

[4] Cambridge University Press, *Cambridge English Dictionary*, 2011, consulté en ligne le 29 juillet 2019. Disponible en ligne : « https://dictionary.cambridge.org/fr/dictionnaire/anglais/cybernetics ».

[5] Académie Française, *Dictionnaire de l'Académie française*, 9ème édition, tome 2, 1992, consulté en ligne le 29 juillet 2019. Disponible en ligne : « https://www.dictionnaire-academie.fr/article/A9C5393 »

[6] A. SUDRES, « Cyberespace et dimension stratégique de la force informatique », dans *Stratégie*, n°117, Institut de Stratégie Comparée, 2017, p. 66.

[7] V. pour exemple : K. BANNELIER et T. CHRISTAKIS, « Cyberdéfense active par des entreprises privées ? Le hack-back entre l'hostilité de la Revue stratégique de cyberdéfense de la France et le projet de loi ACDC aux États-Unis », dans *Stratégie*, n°117, Institut de Stratégie Comparée, 2017, p. 104 ; Ministère de la Défense, *Revue stratégique de défense et de sécurité nationale*, 2017, §4.2, point 88, p. 35 ; Ministère de la Défense, *Livre blanc Défense et Sécurité nationales*, 2013, p. 30.

proposer un changement de vocabulaire[8], l'emploi du terme cybernétique désignera les moyens et méthodes de combat ayant trait au cyberespace.

Le cyberespace ne jouit d'aucune définition faisant l'unanimité. Deux visions sont dominantes d'un point de vue théorique : celle de William Gibson et celle de John Barlow. Pour Gibson, le cyberespace est une « *représentation graphique de données extraites des mémoires de tous les ordinateurs du système humain.* […] *des amas et des constellations de données* ». Pour Barlow, le cyberespace est un espace « *construit par l'Homme, structuré autour de technologies informatiques qui ont infiltré la quasi-totalité des activités humaines* »[9]. Ces deux visions cohabitent et se retrouvent dans différentes définitions. MM. Richard A. Clarke et Robert K. Knacke évoquent un « *ensemble des réseaux informatiques mondiaux et tout ce qu'ils connectent* »[10], se rapprochant de la vision barlovienne, tandis que le Département de la défense américain l'analyse de façon gibsonnienne comme un « *domaine global au sein de l'environnement informationnel, généré par les réseaux d'information* »[11]. L'Agence nationale de la sécurité des systèmes d'information, si elle adopte une position plus barlovienne que le Département de la défense américain, nuance sa définition en mettant à l'équilibre les deux visions, caractérisant le cyberespace d'espace de « *communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques* »[12].

---

[8] Si l'emploi du terme cybernétique semble abusif, un changement de vocabulaire n'est pas à exclure. L'emploi du terme « informatique » pour désigner ces moyens et méthodes semble se répandre. V. en ce sens : Secrétariat général de la Défense et de la Sécurité nationales, *Revue stratégique de cyberdefense*, 12 février 2018, absence du terme « cybernétique » ; Ministère des armées, *Eléments publics de doctrine militaire de lutte informatique offensive*, DiCoD, 2019.

[9] A. SUDRES, « Cyberespace et dimension stratégique de la force informatique », *Stratégie*, n°117, Institut de Stratégie Comparée, 2017, p. 67.

[10] R.A. CLARKE et R.K.KNACKE, *Cyber war*, New York, HarperCollins, 2010, p. 38.

[11] Department of Defense, *Dictionary of Military and Associated Terms*, Joint Publication 1-02, 2010, amendé en 2016, p. 58.

[12] Agence nationale de la sécurité des systèmes d'information, *Glossaire*, « cyberespace », consulté en ligne le 29 juillet 2019. Disponible en ligne : « https://www.ssi.gouv.fr/entreprise/glossaire/c/ ».

Si aucun consensus n'existe actuellement autour de la notion de cyberespace, il en existe un autour de ce qui le compose. Le raisonnement par couches pensé par Edsger Wybe Dijkstra[13] permet de visualiser la composition du cyberespace. Un consensus a été trouvé autour de l'existence de trois « *grandes couches* »[14]. D'abord, il y a la couche physique : elle est composée de l'ensemble des équipements tangibles qui permettent l'existence du cyberespace, tels que les câbles, les routeurs, et tout ce que l'on peut qualifier de *hardware*[15]. Ensuite, il y a la couche logique, composée des *software*[16], qui est immatérielle mais peut avoir un impact sur le monde physique. Enfin, il y a la couche sémantique ou cognitive, espace de la perception des informations traitées. Suivant la vision barlovienne du cyberespace et le consensus existant autour de ces couches, le cyberespace ne constitue pas un environnement purement immatériel et intangible, même s'il l'est principalement : il s'agirait du conglomérat de différentes couches, dont les trois principales ont été citées, existant à la fois de manière physique et immatérielle ; universel et opaque, il viendrait se superposer à l'espace tangible[17]. Un autre élément doit être mis en lumière : il n'existe pas de frontière réelle entre cyberespace civil et cyberespace militaire. Par exemple, l'internet[18] est un vecteur important d'interconnectivité et est arpenté aussi bien par les civils que les militaires.

---

[13] E.W. Dijkstra, « The Structure of the "THE" Multiprogramming System », *Communications of the ACM*, Volume 11, n°5, Université de technologie, Eindhoven, Pays-Bas, mai 1968.

[14] A. SUDRES, « Cyberespace et dimension stratégique de la force informatique », *Stratégie*, n°117, Institut de Stratégie Comparée, 2017, p. 69.

[15] Le terme *hardware* s'est largement démocratisé dans le milieux informatique pour qualifier ce que l'on désigne habituellement de matériel informatique nécessaire au fonctionnement de l'ordinateur : processeur, mémoire vive, carte mère etc.

[16] Les *software* sont, au même titre que le *hardware*, nécessaires au fonctionnement de l'appareil. Ils permettent à l'utilisateur de prendre contrôle de l'unité et de s'en servir, notamment en proposant à l'Homme des informations qu'il peut comprendre. On peut parler plus classiquement de logiciel.

[17] Le cyberespace ne jouissant d'aucune définition faisant consensus, ses caractéristiques sont variables d'un auteur à l'autre. On peut toutefois en citer certaines qui semblent admises : opacité, universalité, publicité, mutabilité, viralité, ubiquité, imprévisibilité, dangerosité. V. : O. KEMPF, *Introduction à la cyberstratégie*, Paris, Economica, 2015, p. 19-25 et Y. HARREL, *Cyberstratégies économiques et financières*, Paris, Nuvis, 2014, p. 22.

[18] Le cyberespace ne peut pas être réduit à l'internet, qui en est un composant.

Encore, l'armée utilise des infrastructures du cyberespace à des fins militaires, comme certains satellites.

Il n'existe pas de définition claire des moyens et méthodes de combat cybernétiques. Les moyens peuvent être envisagés comme les armes cybernétiques et leur vecteur. Elles sont caractérisées par différents potentiels de destruction et de perturbation[19]. Elles peuvent avoir des effets directs mais aussi être développées de sorte à rester en sommeil et à se réactiver sur commande ou sur action propice ; on parle alors de bombe logique[20]. Elles peuvent cibler un élément précis, ou non. Elles sont sujettes à propagation en raison du milieu dans lequel elles sont déployées. Milieu qui, du fait de son opacité, rend ces armes difficiles à détecter avant que leurs effets ne se produisent, *a fortiori* en cas de propagation sur des éléments civils. Propagation ou diffusion[21] qui peut s'effectuer par internet, par un réseau local ou encore par des éléments externes[22]. Les méthodes cybernétiques sont les tactiques, techniques et procédures cybernétiques par lesquelles les hostilités sont conduites[23]. À titre d'exemple, on peut imaginer l'emploi d'un

---

[19] A. GÉRY, « La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense », *Les champs de Mars*, Presses de Sciences Po, n° 30, p. 307.

[20] Agence nationale de la sécurité des systèmes d'information, *Glossaire*, « Bombe logique », disponible en ligne : « https://www.ssi.gouv.fr/entreprise/glossaire/b/ ». Consulté le 26/07/2019.

[21] Ici, on peut établir une distinction entre propagation et diffusion. La diffusion de l'arme se fait dans le cadre maitrisé de l'opération. La propagation est incontrôlée est peut dépasser le cadre de l'opération. On peut imaginer une opération visant une entreprise et qui emploi un ver et une diffusion en réseau local : si un des employés connecte son unité personnelle - en opposition avec son unité professionnelle - audit réseau, le ver pourra se propager sur cette unité, et à d'autres unités lorsque l'employé se connectera à un autre réseau local.

[22] Il existe différents modes de diffusion de l'arme cyber. Via internet, en prenant l'exemple d'une attaque par déni de service. En réseau local, en parasitant les unités connectées à ce réseau. Par le biais d'un élément externe, comme dans le cas de Stuxnet, avec l'emploi vraisemblable d'une clé U.S.B.

[23] M.N.SCHMITT (Dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 103. Les auteurs proposent de délimiter l'emploi du terme d'arme cybernétique au potentiel destructeur du moyen employé ; ainsi, seul un moyen permettant de qualifier l'opération d'attaque au sens du droit international pourrait être considéré comme arme cybernétique. Cette position semble restrictive, aussi ne sera retenue pour l'instant que la distinction basique entre moyens et méthodes, sans considération pour les critères de qualification de l'arme cybernétique.

réseau de machines zombies[24] pour mener une opération de déni de service[25] : ici, le « *botnet* » constitue le moyen cybernétique, et l'opération par déni de service la méthode.

Partant, il sera question d'étudier l'application du droit international humanitaire aux moyens et méthodes de combats cybernétiques dans le cadre des notions définies *supra*.

D'après le Comité international de la Croix-Rouge, le droit international humanitaire est un ensemble de règles coutumières et conventionnelles qui ont vocation à limiter les moyens et les effets de la guerre dans une optique d'humanité. Le Comité considère que cette branche du droit international public ne s'applique qu'en situation de conflit armé et ne concerne pas la question de savoir si un « *[é]tat a ou non le droit de recourir à la force* »[26]. Cette définition se base sur la distinction classique entre *jus in bello* et *jus ad bellum,* le droit international humanitaire s'entendant alors strictement comme *jus in bello*. Cette séparation repose notamment sur la nécessité d'éviter que l'application du *jus in bello* ne soit conditionnée par le respect initial du *jus ad bellum*. Bien qu'elle émane directement du Comité, cette distinction stricte n'est pas absolue. En effet, l'on tend à considérer que si *jus ad bellum* et *jus in bello* sont distincts, ils n'en restent pas moins perméables. À ce titre, le *jus in bello* serait sujet à trois formes de perméabilité au *jus ad bellum* : l'occupation, qu'elle soit consentie ou autorisée par le Conseil de Sécurité, l'exclusion de l'application du droit international humanitaire par le même Conseil et la survie de l'État. Le *jus ad bellum* serait lui aussi perméable à son voisin : le recours au mécanisme de sécurité collective pour

---

[24] Un réseaux de machines zombies, ou *botnet*, est un « *réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise* ». Agence nationale de la sécurité des systèmes d'information, *Glossaire*, « Réseaux de machines zombies », consulté en ligne le 18/08/2019. Disponible en ligne : « https://www.ssi.gouv.fr/particulier/glossaire/r/ ».

[25] Le déni de service est une méthode de multiplication des requêtes adressées à un serveur cible ayant pour objectif de saturer ce dernier pour perturber ou empêcher son fonctionnement.

[26] Comité international de la Croix-Rouge, « *Qu'est-ce que le droit international humanitaire ?* », Services consultatifs en droit international humanitaire, août 2004.

faire cesser des violations du *jus in bello*, les interventions humanitaires unilatérales ainsi que le principe de la responsabilité de protéger seraient autant d'indices de la porosité entre les deux corpus[27]. Partant, l'on pourrait considérer que les tensions et les perméabilités entre ces deux branches valident l'idée d'un droit international humanitaire représentant *lato sensu* un ensemble composé du *jus ad bellum* et du *jus in bello*[28]. Ainsi, il sera question d'appréhender l'application aux moyens et méthodes de combat cybernétiques du droit international humanitaire entendu de manière large, englobant *jus ad bellum* et *jus in bello*.

Le droit international humanitaire et le cyberespace délimités, il est obligatoire de déterminer si le premier s'applique au second. Barlow considère dans sa *Déclaration d'indépendance du cyberespace*[29] que les concepts légaux classiques ne s'appliquent pas à cet espace. Il envisage le cyberespace comme un domaine qui ne saurait être contraint par des règles initialement prévues pour s'appliquer au monde physique. Ce raisonnement se baserait sur deux postulats[30]. Premièrement, celui que le cyberespace est totalement différent du plan physique : il n'est pas un territoire, n'est pas délimité par des frontières et est omniprésent[31]. Secondement, que le cyberespace, par sa nature initiale, devrait rester un environnement ouvert et libre des régulations légales[32]. Pourtant, il semble désormais admis que le droit et *a fortiori* le droit international s'appliquent au cyberespace. En ce sens, on peut mentionner les travaux du Groupe d'experts

---

[27] J. D'ASPRERMONT et J. DE HEMPTINNE, *Droit international humanitaire*, Éditions A.Pedone, Paris, octobre 2012, p. 369.

[28] T.DOMINIQUE, « ONU, CICR, et droit international humanitaire », *Revue Québécoise de droit international*, volume 8-1, 1993. pp. 78-87

[29] J. BARLOW, *A Declaration of The Independence of Cyberspace*, Davos, Suisse, 8 février 1996.

[30] N. TSAGOURIAS, « The legal status of cyberspace », dans *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 26 juin 2015, p. 13.

[31] D.R.JOHNSON et D.G.POST, « Law and borders: The rise of law in cyberspace », *Stanford Law Review*, vol.48, n°5, 1996.

[32] J.GOLDSMITH et T.WU, *Who controls the internet ? Illusions of a borderless world*, Oxford University Press, 2006, p.23.

gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale qui permettent de considérer que le *jus ad bellum* s'applique au cyberespace[33]. Concernant le *jus in bello*, de nombreux États occidentaux ont déclaré qu'il s'appliquait au cyberespace - on peut citer, notamment, les positions des États-Unis[34], du Royaume-Uni[35] et de la France[36]. Il est utile de souligner la position de deux autres États : la Russie et la Chine. La Russie et la Chine comptaient des représentants dans le Groupe d'experts gouvernementaux qui a affirmé l'application du droit international au cyberespace, mais ces derniers ont refusé que le droit international humanitaire[37] ne soit mentionné expressément[38]. La position de la Chine a été largement débattue[39] mais reste ambiguë : dans son discours de septembre 2011, l'ambassadeur de Chine à fait différentes propositions visant à garantir la sécurité du cyberespace sans pour autant citer le *jus in bello*[40]. Ces propositions sont doublées d'une nouvelle déclaration de l'ambassadeur en 2016, selon laquelle la Chine reconnait l'application de certains

---

[33] Assemblée Générale des Nations Unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, 24 juin 2013, Document A/68/98, §19-20.

[34] H.H.KOH, « International law in cyberspace », discours prononcé dans le cadre de l'*U.S. Cyber command inter-agency legal conference*, 18 septembre 2012.

[35] Nations Unies, Assemblée Générale, *Developments in the field of information and telecommunications in the context of international security*, 20 juillet 2010, Document A/65/154, p. 14 et 15.

[36] Ministère de l'Europe et des affaires étrangères, *Réponse de la France à la résolution 73/27 relative aux « Progrès de l'informatique et des télécommunications et sécurité internationale » et à la résolution 73/266 relative à « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale »*, p. 9 et 10. Ce document reprend les différents documents officiels dans lesquels la France à pu affirmer sa position sur cette question et peut être considéré comme une confirmation de ladite position.

[37] Ici, le droit international humanitaire est entendu *stricto sensu*.

[38] M.N.SCHMITT, « The law of cyber warfare : *quo vadis* ? », dans *Stanford Policy and Law Review*, 2014, p. 270 et 271.

[39] Bien que la première position soit dominante, il a été affirmé alternativement que la Chine refusait l'application du *jus in bello* et, au contraire, qu'elle considère qu'il s'appliquait. V. en ces sens : A. SEGAL, « China, international law and cyber space », dans *Council on Foreign Relations*, 2 octobre 2012 et L. ZHANG, « A chinese perspective on cyber war » dans la *Revue internationale de la Croix-Rouge*, version anglaise, volume 94, 2012.

[40] W. QUN, *Discours devant l'Assemblée Générale des Nations Unies*, 66ème session de l'Assemblée générale, 2011.

principes de droit international public au cyberespace, notamment ceux de souveraineté et de paix[41], mais toujours sans évoquer le droit international humanitaire. La position russe est plus difficile à déterminer : dans sa doctrine militaire la plus récente, la Fédération ne mentionne pas une seule fois le cyberespace. Elle mentionne en revanche l'utilisation contraire au droit international des technologies de l'information et de la communication à des fins militaires comme une des menaces les plus importantes qui la visent[42]. Dans les deux cas, le droit international humanitaire entendu *stricto sensu* n'est pas évoqué, seul le droit international l'est. Par extrapolation, le droit international humanitaire faisant partie *lato sensu* du droit international, on pourrait considérer que la Chine et la Russie admettent son application au cyberespace.

In fine, appréhender l'application du droit international humanitaire[43] aux moyens et méthodes de combat cybernétiques nécessite trois postulats. D'abord, que la cybernétique est entendue de manière restrictive comme relevant du cyberespace. Ensuite, que le cyberespace n'est pas simplement un environnement immatériel étranger à certains principes de droit international comme la souveraineté. Enfin, que le droit international humanitaire entendu de manière large peut s'appliquer à cet espace car rien dans sa nature intrinsèque ne semble indiquer le contraire.

Pour autant, appliquer le droit international humanitaire aux moyens et méthodes cybernétiques par analogie reviendrait à nier leur particularité et celle de l'environnement dans lequel ils sont déployés. Le cyberespace est bien plus mouvant que l'espace tangible, il évolue plus vite. Les armes qu'il est possible d'y déployer possèdent la même caractéristique : elles évoluent inlassablement. Cette grande mutabilité à la fois de l'espace ainsi que des moyens et méthodes ne

---

[41] W. QUN, *Discours devant l'Assemblée Générale des Nations Unies*, 71ème session de l'Assemblée générale, 2016

[42] Fédération de Russie, *Military doctrine of the Russian Federation approved by the President*, 2014, 12-k.

[43] Entendu *lato sensu*.

permet pas d'appliquer strictement à la force cybernétique ce que l'on peut employer pour la force cinétique. Pourtant, la doctrine tend à considérer que le *jus ad bellum* peut - et doit - s'appliquer de manière analogue ; alors même que l'application du *jus ad bellum* repose sur la caractérisation de la force classique, il apparait difficile d'imaginer qu'il puisse s'appliquer par simple analogie à un autre type de force. Au même titre, les spécificités des éléments étudiés font que l'application du *jus in bello* ne peut pas se limiter à la simple analogie de principe entre moyens et méthodes cinétiques et moyens et méthodes cybernétiques. La nature militaro-civile du cyberespace et par extension la haute potentialité de dommages collatéraux civils dans le cadre de l'emploi de moyens et méthodes cybernétiques semble appeler à des règles particulières. C'est donc l'appréhension spécifique de la force cybernétique qui va conditionner l'application du droit international humanitaire aux moyens et méthodes de combat cybernétique.

Afin d'analyser cette application, il sera procédé à un raisonnement en deux temps. Dans un premier temps, il sera question d'aborder en détail la notion de force cybernétique et l'application du *jus ad bellum* à cette nouvelle déclinaison de la force. Dans un second temps, l'application du *jus in bello* sera étudiée en biais avec les spécificités du déploiement de la force cybernétique dans les conflits armés traditionnellement cinétiques pour mettre en relief les difficultés qu'elle peut poser.

- **Partie I - *Jus ad bellum* et emploi de la force cybernétique**

La première partie de cette étude se concentrera sur les relations entre la force cybernétique et l'application du *jus ad bellum.* Cette analyse nécessite d'abord de déterminer ce qu'on entend par force cybernétique afin d'en délimiter les spécificités et d'imposer un cadre qui permettra de s'interroger ensuite sur la façon dont le *jus ad bellum* va s'appliquer.

- **Chapitre I - L'application du *jus ad bellum* à un emploi de la force cybernétique**

Le développement toujours plus rapide de moyens et méthodes de combat cybernétiques représente l'un des plus grands défi du *jus ad bellum* à notre époque. Pour aborder ce défi, il est nécessaire de déterminer ce que constitue la force cybernétique dans le cadre de la Charte des Nations Unies (I). Alors, il sera possible d'envisager les modalités d'application du *jus ad bellum* à cette nouvelle déclinaison de la force (II).

I. La force cybernétique dans le cadre de la Charte des Nations Unies

Selon le dictionnaire de l'Académie française, la *force* peut s'entendre de la puissance d'un groupe ou d'un État[44]. Cette puissance est multifacette : économique, idéologique, politique, géographique. Souvent, la notion de force ramenée à l'État renvoie à la puissance militaire. La force désigne alors les moyens militaires dont dispose un État pour se défendre ou pour se projeter. En deux temps, nous évoquerons ce qui doit être entendu par « emploi de la force cybernétique » (A) et présenterons une classification des comportements cybernétiques (B).

A. L'emploi de la force cybernétique

Pour établir ce qui doit être entendu par « emploi de la force cybernétique », il est d'abord nécessaire de définir la force cybernétique (A). Ensuite, il sera possible de déterminer ce qui constitue un emploi de cette force (B).

1. La définition de la force cybernétique

La force cybernétique devrait être abordée de manière spécifique par le droit international. Mais, avant de voir pourquoi, il est important de démontrer qu'elle reste une déclinaison de la force au même titre que la force cinétique. Seront étudiées successivement la notion générale de force présente dans la Charte des Nations Unies et l'application de cette notion au domaine cybernétique.

[44] Académie Française, *Dictionnaire de l'Académie française*, 9ème édition, tome 2, 1992, consulté en ligne le 29 juillet 2019. Disponible en ligne : « https://www.dictionnaire-academie.fr/article/A9F1230 »

a. La notion générale de force dans le cadre de la Charte des Nations Unies

Dans le cadre de la Charte des Nations Unies, la force renvoie à la dimension militaire de la puissance. L'article 41 semble établir une distinction entre ce que la charte considère comme la force et d'autres mesures qui, si on prend la notion de force largement, pourraient en d'autres cadres êtres considérées comme telle[45]. Par exemple, l'article considère comme mesure ne relevant pas de l'emploi de la force les mesures économiques, alors que l'on pourrait considérer que certaines d'entre-elles constituent des projections de la force. Dans la Charte, la force est donc comprise comme puissance militaire[46]. La force se décline en différents volets : force terrestre, maritime, aérienne, spatiale et cybernétique. Ces subdivisions ne sont pas inscrites dans la Charte et n'ont pas d'impact sur son application. Peu importe lequel de ces vecteurs est employé, la Charte les assimile à la force armée[47]. Ainsi, la force armée terrestre est constituée des moyens de projections militaires terrestres, comme la cavalerie blindée ou l'infanterie. La force armée aérienne est constituée des moyens militaires aéroportés d'un État, comme les avions ou les hélicoptères. La force maritime renvoie aux unités militaires maritimes : navires de surface et sous-marins notamment. La force spatiale est composée d'unités qui opèrent à la fois dans le domaine aérien et spatial ou seulement dans ce dernier[48], comme certains satellites. La force cybernétique ne semble pas échapper à ce cadre.

---

[45] Article 41, Charte des Nations Unies, San Francisco, 26 juin 1945.

[46] M.N.SCHMITT, « Cyber operations and the jus ad bellum revisited », *Villanova aw review*, Vol. 56, n°3, 2011, p. 573.

[47] Cour Internationale de Justice, Avis consultatif, *Licéité de la menace ou de l'emploi d'armes nucléaires*, Recueil des arrêts, avis consultatifs et ordonnances, 8 juillet 1996, para. 39. La Cour considère que la Charte n'opère aucune différence entre les différentes armes qui peuvent être employées pour employer la force.

[48] L'organisation des branches spatiales de la force armée peut différer d'un État à l'autre. Le triptyque classique terre-mer-air est par exemple maintenu en France qui incorpore le volet spatial à l'Armée de l'air en tant qu'organisme interarmées. Aux États-Unis, le Président actuel à annoncé vouloir créer une branche indépendante, l'*United States Space Force*, qui sera opérationnelle en 2020.

b. L' application de la notion de « force » au domaine cybernétique

Si la force armée constitue le tout qui est désigné comme *force* dans la Charte des Nations Unies, la force cybernétique n'en est qu'une des composantes[49]. Force armée terrestre, maritime, aérienne, spatiale et cybernétique constitueraient donc un ensemble indissociable dans l'esprit de la Charte.

En soit, cette vision monolithique n'est pas injustifiée. Si la force est réduite à sa dimension militaire, peu importe, *a priori*, le type de force armée est employé. Pourtant, il apparait clairement que la force cybernétique peut se distinguer des autres types de force armée. Le point commun entre les forces armées terrestres, maritimes, aériennes et spatiales est qu'elles sont toutes cinétiques. Elles se présentent sur le plan physique et leur emploi est facilement perceptible, au même titre que les conséquences de cet emploi. La force cybernétique, par définition, se présente dans le plan immatériel du cyberespace. Les conséquences qui peuvent en résulter sont essentiellement immatérielles, bien qu'elles puissent se poursuivre dans le domaine physique, et sont plus difficiles à évaluer. L'éloignement géographique est également une caractéristique particulière, bien qu'elle ne soit plus propre au seul pan cybernétique de la force[50]. À elles seules, les spécificités du cyberespace font que l'emploi de la force cybernétique est par nature différent de l'emploi de la force cinétique.

---

[49] La doctrine semble unanime sur la place de la force cybernétique dans le cadre de la Charte. V. : M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, p. 328, la notion de force ne fait l'objet d'aucune tentative de subdivision entre forces cybernétique et cinétique.

[50] L'emploi de plus en plus fréquent de drones de combat indique que la « désincarnation » du conflit armé n'a pas seulement lieu d'un point de vue cyber.

Ainsi la force cybernétique peut être vue de deux façons : de manière générale comme faisant partie de la force armée au même titre et sans distinction de la force cinétique, de manière spéciale comme une force armée distincte de la force cinétique. Pour l'instant, il est utile de déterminer ce qui caractérise un emploi de la force cybernétique.

2. La caractérisation de l'emploi de la force cybernétique

L'emploi de la force cybernétique se caractérise par différents éléments. Dans un premier temps, il est nécessaire d'établir l'origine de l'emploi de la force alors que dans un second temps, il est important de préciser les caractéristiques de cet emploi pour déterminer s'il est cybernétique.

a. L'origine de l'emploi de la force cybernétique

Dans le cadre de la Charte, il est largement admis que l'usage de la force est du ressort des États. Par extension, il apparait que l'emploi de la force cybernétique a forcément une origine étatique. L'État peut avoir employé la force directement, peut avoir commandité cet usage ou encore avoir armé et entrainé un groupe pour qu'il puisse opérer[51]. Les actes d'un groupe ou d'un individu agissant de leur propre chef ne peuvent pas constituer des usages de la force, bien qu'ils puissent être contraires au droit international ou au droit national d'un État[52].

[51] *Ibid*, para. 228.

[52] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 68, para. 5, règle 17.

b. Les caractéristiques de l'emploi de la force cybernétique

La caractéristique essentielle de l'emploi de la force cybernétique est l'usage d'un composant cybernétique au travers du cyberespace, comme un virus. Il existe toujours un enracinement tangible à l'emploi de la force cybernétique, à partir de la couche physique.

D'autres caractéristiques sont proposées par Michael N. Schmitt[53] et reprises par le groupe d'experts chargé de rédiger le Manuel de Tallinn. Cette liste expose différents facteurs qui pourraient pousser les États à considérer une opération cybernétique comme un emploi de la force. Il apparait intéressant de s'appuyer sur cette liste pour déterminer les caractéristiques d'un emploi de la force cybernétique.

i. La sévérité

L'emploi de la force cybernétique se caractériserait par sa sévérité. Ici, ce sont les conséquences de l'opération cybernétique qui sont visées. Deux extrêmes sont identifiés : d'une part, les dégâts physiques infligés à des individus ou des biens constituent un usage de la force. D'autre part, la simple « irritation » ne représente jamais un usage de la force. C'est la question des opérations qui se situent entre ces deux extrêmes qui pose le plus de problème. Les auteurs du Manuel de Tallinn 2.0 proposent que des critères *infra* puissent permettre de qualifier la sévérité de l'opération : l'ampleur de l'opération, la durée et l'intensité des conséquences[54].

ii. L'immédiateté

---

[53] M.N.SCHMITT, « Computer network attack and use of force in international law : thoughts on a normative framework », *Columbia Journal of Transnational* Law, 1999, p. 914-916.

[54] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 69, para.9-a.

Le caractère d'immédiateté[55] mentionné dans le Manuel semble d'abord se référer aux conséquences et non à l'opération en elle-même. Dans ce cadre, on peut imaginer qu'une opération longue dans le temps - par sa discrétion ou son sommeil - mais dont les effets poursuivis sont immédiats une fois l'objectif atteint, remplirait le critère d'immédiateté. Pourtant, les experts considèrent ensuite que les États seraient plus prompts à caractériser d'usage de la force une « opération cybernétique qui produit des effets immédiats qu'une opération qui aurait besoin de plusieurs mois pour produire ses effets »[56]. Ainsi, un État qui subit une opération cybernétique fulgurante détruisant l'une de ses centrales nucléaires serait plus à même de qualifier l'opération d'usage de la force qu'un État subissant une opération lente résultant également en la destruction d'une centrale. Ce critère doit être resserré à la nature des conséquences : une opération, fulgurante ou lente, qui détruirait ou blesserait un grand nombre de personnes une fois son objectif atteint remplit le critère d'immédiateté, là où une opération qui génère des conséquences lentes, comme un effondrement de l'économie, serait moins grave.

iii. L'aspect direct

Le caractère direct, proche de celui d'immédiateté, est relatif à la chaine de causalité entre l'acte initial et ses conséquences. Plus le lien est direct, plus l'opération cybernétique s'apparente à un usage de la force[57].

---

[55] *Ibid*, para. 9-b.

[56] Traduction, Original : « [States] *are more likely to characterise a cyber operation that produces immediate results as a use of force than one that takes weeks or monts to achieve its intended effects* ».

[57] *Ibid*, para. 9-c.

iv. L'invasivité

L'invasivité de l'opération est également un critère qui permet d'établir si une opération atteint le seuil d'usage de la force[58]. L'invasivité se mesure à l'aune du degré d'intrusion dans l'architecture cybernétique d'un État. L'invasivité est proportionnellement corrélée au degré de protection du système visé : ainsi, moins un système est protégé, moins l'opération est invasive, et inversement[59]. L'invasivité peut aussi se mesurer en fonction de la délimitation de ses effets. Lorsque une opération vise un État en particulier, l'invasivité est élevée. À ce titre, on peut évaluer la spécificité de l'invasivité en s'appuyant sur les noms de domaines qui sont visés. Ainsi, si l'opération ne vise que des noms de domaine en .fr, l'opération est hautement invasive. L'invasivité est un critère particulier puisqu'il n'est pas limité à l'action cybernétique militaire ; il ne doit pas être le facteur déterminant lorsque l'action ne relève pas clairement du domaine de l'opération militaire.

v. Le caractère militaire

Le caractère militaire de l'opération est un facteur évident permettant de déterminer si une action cybernétique constitue un usage de la force[60]. Ce postulat repose en grande partie sur la propension de la Charte à considérer que l'usage de la force est lié à sa dimension militaire.

Cette sélection de critères permet de déterminer si l'opération cybernétique est sévère et immédiate dans ses conséquences, directe, invasive et de caractère militaire. D'autres paramètres

---

[58] *Ibid*, para. 9-d.

[59] On peut imagine une opération qui vise un système purement civil, comme celui d'un hôpital. L'opération est peu invasive. *A contrario*, une opération qui viserait le système cyber d'une infrastructure militaire critique serait hautement invasive.

[60] *Ibid*, para. 9-f.

peuvent être pris en compte, comme la quantification des conséquences ou la présomption de légalité de l'acte entrepris[61]. Ces critères permettent de déterminer ce qui relève de l'opération cybernétique et ce qui relève d'autres types d'actions cybernétiques.

B. L'opération cybernétique et l'action cybernétique

La notion d'opération cybernétique doit être rattachée à celle d'opération militaire (1). Ce type d'acte cybernétique se distingue d'autres actions qui ne relèvent pas de la qualification d'opération et qui, *a priori*, ne relèvent pas non plus du *jus ad bellum* (2).

1. La définition de l'opération cybernétique

La notion d'opération a une portée spécifique dans le domaine militaire. Lorsque le recours à la force armée est exercé par le médium cybernétique, la notion d'opération trouve à s'appliquer.

L'Académie française considère l'opération dans le cadre militaire comme l'« [e]*nsemble des mouvements stratégiques ou tactiques exécutés par les forces engagées dans une action militaire* »[62]. Elle expose différents types d'opérations militaires : offensive, défensive, aéroportée, commando. L'action militaire est le fruit d'une planification détaillée : heure, lieu, objectifs, moyens, effectifs, risques. Cette action planifiée se traduit sur le terrain par la conduite de l'opération. Elle est donc la concrétisation opérationnelle de la volonté militaire d'un acteur - généralement un État. Les notions de mouvements stratégiques et tactiques sont en soit difficile à

[61] *Ibid*, para. 9-e et 9-h.

[62] Académie Française, *Dictionnaire de l'Académie française*, 9ème édition, tome 2, 1992, consulté en ligne le 29 juillet 2019. Disponible en ligne : « https://www.dictionnaire-academie.fr/article/A9O0515 ».

distinguer en raison de la confusion fréquente entre les deux concepts. Selon différentes vision, la tactique est inféodée à la stratégie, ou indépendante[63].

L'opération cybernétique est de caractère militaire. Elle peut être défensive ou offensive. Elle s'intercale dans l'action militaire au même titre qu'une opération cinétique. Elle peut être effectuée en soutien à une opération cinétique ou de manière totalement indépendante. L'opération cybernétique varie de l'opération classique en raison de l'environnement dans lequel elle a lieu, puisqu'elle se déroule dans le cyberespace. D'un point de vue opérationnel, les différences classiques sont l'immatérialité de l'opération, l'éloignement physique des forces en opposition[64], les difficultés d'attribution, les délais de réalisation[65]. On peut considérer qu'elle fait appel à la fois à des mesures stratégiques et des mesures tactiques, selon les mêmes nécessités qu'une opération cinétique. L'opération cybernétique est soumise au droit international.

L'opération cybernétique doit toutefois être distinguée de certains autres comportements cybernétiques.

2. La distinction entre l'opération cybernétique et certaines autres actions cybernétiques

[63] Il est possible de mentionner les positions de l'amiral français Raoul Castex, qui considérait que la tactique n'était pas une notion totalement distincte de la stratégie, mais qu'elle s'appliquait simplement à un niveau inférieur, la bataille, quand la stratégie s'applique à un niveau supérieur. Cette vision n'est pas absolu. Clausewitz note une première limite : il établi une différence entre les buts de la guerre - la stratégie - et les buts dans la guerre - la tactique. Les seconds, dans la réalité de la guerre, prennent parfois le dessus, dépassant le cadre prédéfini par la stratégie.

[64] En raison de la nature de la conflictualité cybernétique, les cybercombattants sont souvent amenés à opérer depuis les « bases arrières », loin du terrain.

[65] L'opération cybernétique, en raison du milieu dans lequel elle est menée, est souvent plus rapide que l'opération cinétique. Ce constat doit toutefois être nuancé, notamment eu égard à certains types d'opérations longues.

L'opération cybernétique relève du domaine militaire et de l'application du droit international. En outre, elle doit pouvoir être attribuée à un État. Elle ne doit pas être confondue avec certains actes qui ne sont pas attribuables à un État et avec d'autres qui, s'ils sont attribuables, ne relèvent pas du domaine militaire ni de l'application du droit international.

a. Les actes non attribuables à un État

On distingue deux grands types d'actes cybernétiques qui ne sont pas attribuables à un État : les actes de cybercriminalité et les actes commis par une entité non étatique contre un État.

i. La cybercriminalité

L'opération cybernétique doit être distinguée des actes cybernétiques illicites *per se.* Les comportements « cybercriminels » se sont multipliés au cours des dernières années[66]. Ces comportements sont très variables. Ils peuvent aller de la simple intrusion illégale dans un système cible jusqu'à ce que certains appellent « cyberterrorisme ».

Les faits les plus courants relèvent de la criminalité classique. Les pirates vont mener des actions d'intrusion, d'acquisition ou encore de falsification pour obtenir certaines données ou informations d'un particulier ou d'une entreprise. Ces actes ne peuvent pas être assimilés à des cyberopérations telles qu'on les entend ici et sont donc étrangers à l'application du droit international humanitaire.

---

[66] V. Statistiques d'analyse Symantec, notamment : augmentation signification du *formjacking*, prolifération des *ransomware*, vols de fichiers etc. Disponible en ligne : « https://resource.elq.symantec.com/LP=6863?inid=symc_threat-report_istr_to_leadgen_form_LP-6863_ISTR-2019-report-main&cid=70138000001QvLeAAK »

La question du « cyberterrorisme » est plus complexe. Il n'existe pas de définition unanime de ce phénomène. Du point de vue anglo-saxon, il peut être entendu de manière restrictive ou large. Restrictivement, le cyberterrorisme est une attaque qui vise à dérégler les systèmes d'information d'une cible afin de susciter la panique. Largement, Kevin G. Coleman considère que le cyberterrorisme constitue « *l'utilisation préméditée des capacités de perturbation ou la menace de cette utilisation contre des ordinateurs ou des réseaux, avec l'intention de causer un dommage, de faire avancer un objectif social, idéologique, religieux ou politique, ou encore d'intimider qui que ce soit dans la poursuite de ces objectifs* ». Pour Olivier Kempf, le cyberterrorisme peut renvoyer soit à l'utilisateur, soit à l'acte[67]. À l'utilisateur lorsqu'on considère que le cyberterrorisme résulte de l'utilisation du cyberespace par des terroristes. À l'acte lors de la commission d'un acte terroriste dans ou par le cyberespace. Lorsqu'on se réfère à l'auteur des faits - le potentiel cyberterroriste - Kempf considère que la nature opaque du cyberespace empêche intellectuellement d'appréhender la notion de cyberterrorisme. Il considère en effet que le « cyberterroriste », en raison de son grand anonymat, est davantage une conception de l'ennemi. Il considère cette approche comme subjective. *A contrario*, il considère qu'appréhender le cyberterrorisme sous l'angle de l'acte commis est plus objectif. Il est alors question d'analyser la nature de l'acte commis et ses conséquences pour déterminer s'il relève du cyberterrorisme. S'il évacue rapidement les effets physiques, il souligne l'importance des effets psychologiques, de la disproportion et de l'indiscrimination que l'on considérerait alors comme des caractéristiques du cyberterrorisme. Il conclue toutefois que le cyberterrorisme n'est pas vraiment réel par analogie au terrorisme tel qu'on le décrit habituellement, mais qu'il s'agit plus d'une position américaine prenant racines dans leur discours sur la *terreur*.

[67] O. KEMPF, « Le cyberterrorisme : un discours plus qu'une réalité », *Hérodote*, n°152-153, 2014, p. 83.

ii. Les actes cybernétiques effectués par des groupes non étatiques

Les actes cybernétiques commis par des entités non étatiques et indépendantes ne sont régis par le droit international que dans des cas particuliers. C'est le cas notamment des droits et obligations qui résultent de certaines branches du droit international, comme le droit international des droits de l'Homme ou encore le droit des conflits armés[68]. En dehors du cas spécial d'un acte cybernétique commis par un groupe non étatique dans le cadre d'un conflit armé, les actes cybernétiques effectués par des groupes non étatiques ne représentent pas des opérations cybernétiques tel qu'on l'entend ici.

b. Les actes attribuables à un État

Parmi les actes attribuables à un État, on soulignera particulièrement les actes de cyberespionnage.

L'opération cybernétique est militaire par nature. Elle doit être distinguée des actes de cyberespionnage conduits en dehors d'un conflit armé. Dans le cadre d'un conflit armé, les règles du *jus in bello* prévalent.

Les rédacteurs du Manuel de Tallinn définissent le cyberespionnage comme les actes « *entrepris clandestinement ou sous de fausses raisons usant de capacités cybernétiques pour réunir ou tenter de réunir des informations* »[69]. Le cyberespionnage constitue l'emploi des capacités

---

[68] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 33, para. 1.

[69] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 32, para.2 .

cybernétiques pour surveiller, maitriser et extraire des communications, des données ou d'autres informations transmises ou stockées électroniquement. Le cyberespionnage doit pouvoir être attribué à un État. Il se distingue de l'espionnage traditionnel pour les mêmes raisons que les opérations militaires : la spécificité du milieu et des moyens employés.

L'espionnage n'étant pas illicite en soi, le cyberespionnage ne l'est pas non plus. Toutefois, les méthodes employées pour conduire ce cyberespionnage peuvent être contraires au droit international[70], notamment eu égard au principe de souveraineté. Cette question reste toutefois délicate dans la mesure où certains des actes d'espionnage classique peuvent aussi être considérés par l'État victime comme une violation de leur souveraineté.

L'acte de cyberespionnage, s'il n'est pas illicite *per se*, peut faire partie d'un tout qui représente un acte illicite. On peut imaginer une opération cybernétique qui viserait à faire exploser une centrale nucléaire et dont la première phase serait celle d'un acte de cyberespionnage. Il reste alors à déterminer si les actes de cyberespionnage et ceux ayant mené à la destruction de la station sont dissociables ou non.

Après avoir déterminé ce qui relevait et ce qui ne relevait pas de l'emploi de la force cybernétique, nous étudierons l'application du *jus ad bellum* à ce type de force.

II. L' application du *jus ad bellum* à l'emploi de la force cybernétique

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*

[70] *Ibid*, para. 6.

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 »[71]. Il est admis que cette prohibition générale du recours à la force est de valeur coutumière[72]. Comme le prévoit l'article 51, cette prohibition n'est pas de nature à porter atteinte au droit de légitime défense des États[73]. Nous étudierons successivement le principe d'interdiction du recours à la force cybernétique (A) et le droit de légitime défense dans le cadre d'opérations cybernétiques (B).

A. Le principe d'interdiction du recours à la force cybernétique

Il a été établi que si la force cybernétique se distinguait sur certains points de la force cinétique, elle restait une composante de la force telle qu'elle est entendue dans la Charte. À ce titre, la force cybernétique n'échappe pas à la prohibition de la menace de l'emploi de la force (A) ni à celle de l'emploi de la force (B).

1. Menace de l'emploi de la force et vecteur cybernétique

Il n'existe pas de définition précise de la menace de l'emploi de la force[74]. Certaines clés d'interprétation permettent toutefois de distinguer ce qui représente une menace licite et une menace illicite au titre de la Charte.

---

[71] Article 2(4), Charte des Nations Unies, San Francisco, 26 juin 1945.

[72] Cour Internationale de Justice, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci*, Recueil des arrêts, avis consultatifs et ordonnances, p.103, para. 193.

[73] Article 51, Charte des Nations Unies, San Francisco, 26 juin 1945.

[74] O. BARAT-GINIES, « Existe-t-il un droit international du cyberespace ? », *Hérodote*, n°152-153, p. 208.

Selon la Cour de Justice Internationale, une menace est licite lorsque l'action envisagée est elle-même licite[75]. Par exemple, un État qui en menace un autre de sanctions économiques ne viole pas le droit international et *a fortiori* la Charte tant que ces sanctions sont légales. Si ces menaces sont communiquées de manière cybernétique, la licéité de la menace est toujours liée à celle des actes envisagés.

La menace de l'emploi de la force, dans le cadre cybernétique, peut cibler deux types de situations. Dans un premier temps, on peut utiliser le vecteur cybernétique pour menacer de l'emploi de la force - cinétique ou cyber. Dans un second temps, on peut menacer par tout moyen de communication d'employer la force cybernétique.

Les experts chargés de la rédaction du Manuel de Tallinn 2.0 se sont penchés sur la question des capacités et des intentions des États qui auraient recours à la menace.

Dans un premier temps, ils se sont demandés si les menaces d'un État qui ne possède manifestement pas les capacités cybernétiques opérationnelles nécessaires à réaliser lesdites menaces étaient illicites[76]. Les rédacteurs ne sont pas arrivés à un consensus. Pourtant, il semble difficile de considérer que le critère de l'apparente incapacité puisse être admis dans le cas de la force cybernétique. En raison des caractéristiques du cyberespace et des moyens et méthodes cybernétiques déjà exposés, il apparait évident que la force cybernétique est difficilement évaluable. Il serait même logique de considérer que la force cybernétique est désormais très fortement liée à la notion de conflit asymétrique. Un État « faible » de manière cinétique ne l'est pas forcément d'un

---

[75] Cour Internationale de Justice, Avis consultatif, *Licéité de la menace ou de l'emploi d'armes nucléaires*, Recueil des arrêts, avis consultatifs et ordonnances, 8 juillet 1996, para. 47.

[76] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 70, para. 5.

point de vue cybernétique. Au surplus, quand bien même un État laisserait paraitre qu'il ne possède pas une force cybernétique développée, cette apparence est forcément tempérée par les spécificités de cette force. Il apparait donc que l'illicéité de telles menaces ne devrait pas être analysée sous le prisme de l'apparente capacité ou incapacité d'un État.

Dans un second temps, les experts se sont demandés si de telles menaces étaient illicites lorsque leur auteur n'avait en réalité aucune intention de les mettre à exécution - par exemple pour des raisons de politique nationale[77]. À nouveau, aucun consensus n'a été atteint. Pourtant, même si l'auteur de la menace n'a pas l'intention de mener à bien ladite menace, il est difficile de voir comment elle pourrait être compatible avec les objectifs poursuivis par la Charte et plus précisément par l'interdiction de la menace de l'emploi de la force. En effet, on peut considérer que la menace en soit est contraire aux objectifs de l'organisation, sans considération de la potentialité qu'elle soit menée à bien. De plus, évaluer l'intention de l'auteur de la menace de manière totalement objective nécessiterait des critères spécifiques et, même si l'on peut conclure que l'auteur n'a aucune intention de commettre ces actes, ces conclusions ne peuvent pas être fiables de manière absolue.

Ces menaces sont donc illicites, à deux exceptions près : la menace de l'exercice de la légitime défense et la menace de l'emploi de la force cyber/via le vecteur cybernétique dans le cadre d'une résolution sous chapitre VII du Conseil de Sécurité des Nations Unies, qui seront évoquées ultérieurement.

[77] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 70, para. 6.

La menace illicite du recours à la force se traduit parfois de manière effective par un recours illicite à la force.

2. Le recours illicite à la force cybernétique

Supra, nous avons défini ce qui pouvait être entendu par *force* dans le cadre de la Charte et déterminé par extension ce que l'on pouvait entendre par force cybernétique en établissant une liste non exhaustive de caractères.

Concernant le recours à la force, la Charte n'offre aucune définition précise de la notion. Pour déterminer à partir de quel seuil certains actes peuvent constituer des usages de la force, on peut adopter l'approche de l'ampleur et des effets des actions entreprises[78]. De manière analogue, on pourrait mesurer l'ampleur et les effets d'un acte cybernétique pour déterminer s'il s'agit d'un recours à la force cybernétique.

La nature spéciale de la force cybernétique et du cyberespace doit demeurer un critère d'analyse de ce que l'on pourrait considérer ou non comme un emploi de la force cybernétique. Lorsqu'un État lance une opération cinétique de grande envergure aux effets multiples et sévères contre un autre État, il est facile de le caractériser d'emploi de la force. Lorsqu'un État lance une opération cybernétique, il est plus difficile de déterminer ce que l'on entend par *envergure*. Il est également plus dur d'évaluer les effets de l'attaque lorsque ceux-ci sont cantonnés au cyberespace. On peut dire que la Charte a été rédigée dans un cadre « conventionnel », et qu'elle appréhende donc les effets cinétiques. Mais la destruction de plusieurs milliers de téraoctets de données est-elle

[78] Cour Internationale de Justice, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci*, Recueil des arrêts, avis consultatifs et ordonnances, p.103, para. 195.

vraiment moins grave, dans ses effets, que la destruction d'un ou plusieurs immeubles dans le cadre d'une opération cinétique ?[79]. Partant, doit-on seulement considérer les dégâts cinétiques d'une opération cybernétique pour apprécier sa gravité ? Cette approche semble nier la spécificité du cyberespace et de la conflictualité cybernétique en s'accrochant à la conception tangible des dommages - les immeubles détruits, les unités détruites, les vies perdues.

Quoiqu'il en soit, ce recours à la force cybernétique est illicite *de facto* lorsqu'il a lieu en dehors des exceptions à l'interdiction du recours à la force prévues par la charte.

B. Les recours licites à la force cybernétique

L'article 51 de la Charte des Nations Unies dispose qu' « [a]*ucune 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* »[80]. Le droit à la légitime défense a vocation à s'exercer en cas d'attaque cybernétique.

1. La cyberdéfense et l'exercice de la légitime défense

La notion de cyberdéfense renvoie aux mécanismes mis en place pour protéger, contrecarrer et contrattaquer un assaillant en cas de cyberopération. Elle est traditionnellement de deux types : passive et active. Il est intéressant de se demander si les notions de cyberdéfense et de légitime

[79] Dans cette hypothèse, aucune victime civile ou militaire n'est envisagée.

[80] Article 51, Charte des Nations Unies, San Francisco, 26 juin 1945.

défense sont indissociables ou, au contraire, si elles répondent chacune à une problématique différente.

a. La cyberdéfense passive et la cyberdéfense active

La cyberdéfense s'organise classiquement autour de deux actes : la cyberdéfense passive et la cyberdéfense active.

i. La cyberdéfense passive

La cyberdéfense passive peut être considérée comme « *un simple recours aux systèmes automatiques de protection des réseaux* […]*, placés à la frontière entre ceux-ci et l'extérieur* »[81]. Les mesures de cyberdéfense passive sont essentiellement préventives. On peut citer notamment la mise à jour des logiciels - notamment des systèmes d'exploitation, la détection et la correction des vulnérabilités, la mise en place de pare-feu et d'anti-virus. Au fond, il est questions de « *politiques d'hygiène et de sécurité informatiques* »[82].

Certaines méthodes de cyberdéfense sont difficiles à classer dans l'une ou l'autre des catégories. Karinne Bannelier et Théodore Christakis mentionnent à titre d'exemple le cas du « *honeypot* ». Le *honeypot* ou « pot de miel » peut être défini comme « *un ensemble de pièges permettant de détecter ou de guider des tentatives d'utilisation non autorisées d'un système*

---

[81] Sénat français, *Cyberdéfense : un nouvel enjeu de sécurité nationale*, Rapport d'information n°499, 8 juillet 2008.

[82] K. BANNELIER et T. CHRISTAKIS, « Cyberdéfense active par des entreprises privées ? Le hack-back entre l'hostilité de la revue stratégique de cyberdéfense de la France et le projet de loi ACDC aux États-Unis », *Stratégique*, Institut de Stratégie Comparée, n°177, p. 102.

d'information »[83]. Lance Spitzner qualifie quant à lui le *honeypot* de « *ressource système dont la seule utilité est de se faire attaquer ou compromettre* »[84]. Le « pot de miel » est une tactique cybernétique passive, mais elle peut également être utilisée de manière plus agressive pour introduire dans le système cible des « *capacités cyber-offensives susceptibles de voler ou détruire des données* »[85]. Dans le cadre de ces méthodes, il est sûrement plus avisé de s'attarder sur la manière dont elles sont employées et les buts qu'elles poursuivent pour déterminer s'il s'agit de cyberdéfense passive ou active. Dans le cas où le « pot de miel » ne sert qu'a leurrer l'adversaire dans son opération, il semble s'agir de cyberdéfense passive. Dans le cas où il est employé afin de faciliter la mise en oeuvre d'une contre-offensive, il tient plus de la cyberdéfense active.

ii. La cyberdéfense active

La cyberdéfense active est une notion ambiguë. Comme nous l'avons évoqué *supra*, la cyberdéfense active peut se caractériser par des actes offensifs de destruction ou de perturbation en réponse à une activité hostile. Selon Karinne Bannelier et Théodore Christakis, elle semble renvoyer implicitement à la notion de légitime défense. Dans leur article, les auteurs décident de ne pas employer ce terme pour désigner les techniques « *les plus offensives de riposte à une cyberattaque* »[86]. Ils préfèrent employer le terme de « *hack-back* » ou de « contre-piratage ». Dans ce cadre, le *hack-back* est la riposte à une cyberattaque. Mais, dès lors, il est envisageable de considérer que la cyberdéfense active constitue un mode de riposte à certaines opérations cybernétiques, indépendamment du droit à la légitime défense où intervient le *hack-back*.

---

[83] A. BOULAICHE, *Technologies Honeypots*, Université Abderrahmene Mira de Béjaia, 2006, p. 10.

[84] L. SPITZNER, *Honeypots : tracking hackers*, Addison Wesley, 13 septembre 2002.

[85] K. BANNELIER et T. CHRISTAKIS, « Cyberdéfense active par des entreprises privées ? Le hack-back entre l'hostilité de la revue stratégique de cyberdéfense de la France et le projet de loi ACDC aux États-Unis », *Stratégique*, Institut de Stratégie Comparée, n°177, p. 102.

[86] *Ibid*, p. 103-104.

b. L'articulation entre cyberdéfense et légitime défense

Si l'on tend à considérer qu'il existe des modes de riposte différents en fonction du type de cyberopération dont un État est victime, il apparait que les cyberopérations peuvent être classées en deux catégories : les cyberopérations constituant une cyberattaque et celles n'atteignant pas ce seuil. On se demandera alors quelle est la place de la légitime défense cybernétique dans ce paradigme.

i. Cyberopération offensive et cyberattaque

La cyberopération a été décrite précédemment comme une action cybernétique entreprise par un État dans le cadre d'une action militaire. Elle peut s'effectuer en soutien d'une opération cinétique ou de manière autonome. Elle est soumise au droit international. Elle se déroule dans le cyberespace et se différencie d'une opération cinétique par l'immatérialité de son déroulement, l'éloignement physique des forces en oppositions, les difficultés d'attribution et les délais de réalisation.

La cyberattaque renverrait à la notion d'attaque armée prévue par l'article 51 de la Charte. La Cour de Justice a été amenée à se positionner sur les notions d'emploi de la force et d'attaque armée, toutes deux présentes dans la Charte. Ainsi, elle considère que si toutes les attaques armées constituent un emploi de la force, tous les emplois de la force ne constituent pas une attaque armée. L'emploi de la force doit, pour parvenir au seuil d'attaque armée, atteindre une certaine gravité[87]. La cyberattaque constitue donc le stade le plus violent d'une cyberopération offensive. La Cour de

[87] Cour Internationale de Justice, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci*, Recueil des arrêts, avis consultatifs et ordonnances, p.103, para. 195.

Justice ne définissant pas expressément ce qui représente une attaque armée et ce qui représente un simple usage de la force, il peut être utile d'illustrer par l'exemple ce qu'il en est pour le médium cybernétique. Concernant un simple usage de la force cybernétique, on peut imaginer une cyberopération intrusive et perturbatrice qui bloquerait brièvement ou périodiquement des infrastructures cyber non vitales. Pour une cyberopération qui s'élèverait au rang de cyberattaque, on peut imaginer une opération ayant pour effet de causer la mort de plusieurs personnes ou de causer des dommages significatifs à certaines infrastructures[88].

La cyberattaque doit avoir un élément transfrontalier et émaner d'un État ou d'un groupe non étatique mandaté ou supporté par un État. Elle ne peut pas être le fait d'un groupe non étatique[89].

Pour répondre à ces deux types d'actes cybernétiques hostiles, il est possible d'envisager des modes de riposte distincts.

ii. Les modes de riposte aux cyberopérations offensives et aux cyberattaques

Chacun des deux types d'acte hostile défini ici nécessite un mode de riposte adapté. On répondra à une cyberopération offensive par des contremesures ou par une cyberopération de défense active et à une cyberattaque par l'exercice du droit de légitime défense. Il convient de préciser que la mise en place de contremesures, le recours à la cyberdéfense active ou à la légitime défense font tous trois appel à une attribution préalable du fait illicite.

---

[88] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations,* Cambridge University Press, 2 février 2017, règle 71, para. 8.

[89] Dans le cas où une action cybernétique entreprise par un groupe armé remplirait les critères définis ici, l'acte pourrait être assimilé à du cyberterrorisme.

- Cyberopération offensive, contremesure et cyberdéfense active

La cyberopération offensive est un usage de la force qui, en raison de son intensité et de ses effets, n'atteint pas le seuil d'attaque armée. Pour répondre à ce type d'acte hostile, l'État victime est fondé à employer des « contremesures ». La question est de savoir si la cyberdéfense active tombe dans le giron de ces contremesures ou si il s'agit d'un mode de riposte à part entière.

La contremesure peut uniquement être prise par un État victime pour amener ou contraindre l'État hostile à cesser son comportement illicite[90]. Elles sont donc réactives et doivent être prises en réponse à l'acte illicite[91]. La contremesure n'est envisageable que pour autant que l'acte illicite perdure. Dans le cadre cybernétique, l'opération hostile doit être prise dans son ensemble : lors d'une attaque par déni de service massive mais intermittente, la contremesure reste une option envisageable. Idéalement, les contremesures ont des effets temporaires. Toutefois, ce critère de réversibilité n'est pas absolu et s'avère particulièrement difficile à mettre en oeuvre dans le cadre cybernétique. La contremesure doit être annoncée, mais ce critère n'est pas non plus absolu[92]. Les contremesures doivent être proportionnelles au préjudice subi[93]. Elles sont notamment limitées par les obligations relatives aux droits fondamentaux de l'Homme, aux obligations de caractère humanitaire excluant les représailles et aux obligations découlant de normes impératives de droit

---

[90] Article 49(1), *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite*, Résolution AGNU 56/83, annexe, 12 décembre 2001.

[91] Cour Internationale de Justice, *Affaire relative au projet Gabčíkovo-Nagymaros (Hongrie/Slovaquie)*, Recueil des arrêts, avis consultatifs et ordonnances, 25 septembre 1997, para. 83.

[92] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 21, para. 1-12.

[93] *Ibid*, article 51.

international général[94]. Théoriquement, elles ne doivent pas non plus enfreindre l'interdiction du recours à la force. La difficulté réside ici dans l'appréciation du seuil à partir duquel une contremesure cybernétique devient un recours à la force. La solution à cette difficulté pourrait être d'envisager un troisième stade de riposte intermédiaire : la cyberdéfense active.

La contremesure empêche l'État lésé d'entreprendre une action qui violerait la prohibition du recours à la force, alors même que dans le cas d'une cyberopération offensive qu'il subirait, il est victime d'un usage de la force. Cet usage de la force est particulier et demande une riposte particulière. La cyberdéfense active est la réponse à ce type d'opération. Si la cyberdéfense active est un usage de la force, elle ne répond pas ici à une attaque armée et ne dépend donc pas du régime de légitime défense. Elle est toutefois nécessaire et utile, d'un point de vue pragmatique, pour faire cesser la cyberopération offensive hostile. Elle pourrait être limitée par les mêmes paramètres que la contremesure, mais constituerait un emploi de la force admissible. Le principe de nécessité prévu par l'article 25 des articles sur la responsabilité des États pour fait internationalement illicite servirait alors de mire pour définir les contours de l'action de cyberdéfense active.

- Cyberattaque et exercice de la légitime défense

La cyberattaque est une cyberopération offensive qui atteint le seuil de l'attaque armée. Le franchissement de ce seuil dépend des effets et de l'ampleur de l'attaque. Elle déclenche naturellement le droit pour un État d'exercer sa légitime défense, au même titre qu'une attaque

[94] Article 50(1), *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite*, Résolution AGNU 56/83, annexe, 12 décembre 2001.

armée cinétique, le choix de l'arme ou de la méthode étant négligeable en pareil cas[95]. La légitime défense cybernétique peut être exercée individuellement ou collectivement.

La cyberattaque est menée par un État ou pour un État par un groupe non étatique. Les rédacteurs du Manuel de Tallinn 2.0 considèrent qu'une cyberattaque visant un État peut émaner d'un groupe non étatique depuis le territoire d'un autre État mais sans soutien de ce dernier. Ils considèrent que la pratique des États montre qu'en pareil cas, les États victimes sont fondés à agir au nom de la légitime défense[96]. Dans le cadre de la notion de cyberattaque et de recours à la force cybernétique qui a été déployé dans cette étude, ce genre de comportement émanant d'acteurs non étatiques relèvera du domaine de l'acte de cyberterrorisme et non de la cyberattaque.

La légitime défense, dans le cadre cybernétique, doit répondre à quatre exigences : la nécessité, la proportionnalité, l'imminence et la concomitance.

Les critères de nécessité et de proportionnalité ont été reconnus par la Cour international de Justice dans l'affaire *Nicaragua* et dans l'affaire des *Plate-formes pétrolières*[97]. La nécessité signifie qu'un recours à la force est nécessaire pour repousser une cyberattaque imminente ou pour

---

[95] Cour Internationale de Justice, Avis consultatif, *Licéité de la menace ou de l'emploi d'armes nucléaires*, Recueil des arrêts, avis consultatifs et ordonnances, 8 juillet 1996, para. 39.

[96] Il est essentiellement fait référence aux résolutions du Conseil de sécurité qui ont été adoptées dans le cadre des attentats ayant frappé les États-Unis en 2001. [96] V. en ce sens : S/RES/1373, 2001, prise sous l'égide du chapitre VII de la charte des Nations Unies. Cette position reste toutefois sujette à controverse. Si elle a semblé être renforcée par l'intervention israélienne au Liban contre le Hezbollah, la Cour de Justice a adopté des positions divergentes dans deux décisions notables. V. en ces sens : M.N.SCHMITT, « Change Direction 2006 : Israeli opérations in Lebanon and the International Law of self-defense », *Michigan Journal of International Law,* 2008, L.127 ; Cour internationale de Justice, Avis consultatif, *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, 9 juillet 2004 et *Affaire Congo c/Ouganda dite des activités militaires sur le territoire du Congo*, 19 décembre 2005.

[97] Cour Internationale de Justice, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci*, Recueil des arrêts, avis consultatifs et ordonnances, p.103, paras. 176 et 194 ; Cour Internationale de Justice, *Affaire des plates-formes pétrolières*, Recueil des arrêts, avis consultatifs et ordonnances, 12 décembre 1996, paras. 43, 73-74 et 76.

contrecarrer une cyberattaque en cours. La nécessité ramenée au vecteur cybernétique justifie la légitime défense dans les situations où les contremesures et la cyberdéfense active ne sont pas suffisantes pour repousser l'assaillant. Le critère de proportionnalité vise à délimiter l'ampleur de la riposte qui peut être envisagée, par comparaison avec les effets de l'attaque initiale. La proportionnalité se mesure à l'aune de ce qui est nécessaire d'être mis en place pour mettre un terme à une attaque en cours[98]. En cas de riposte cinétique, le critère de proportionnalité n'implique pas de question supplémentaire, les dégâts collatéraux étant plus facilement évaluables. La proportionnalité dans le choix du moyen ou de la méthode employé doit être particulièrement mesurée dans le cadre d'une riposte cybernétique. Il est plus difficile d'évaluer le potentiel destructeur collatéral d'une arme cyber, en raison de la versatilité du milieu dans lequel elle peut être amenée à évoluer. Si l'attaque s'articule autour d'un *ver*, dans un circuit informatique fermé, par exemple contre une seule unité centrale mise hors réseaux, il est facile de cantonner les effets de la riposte. En revanche, en cas d'emploi d'une arme à potentiel de propagation élevée en réseaux, cette évaluation est plus délicate, avec elle l'appréciation du respect de l'exigence de proportionnalité.

On retrouve la notion de concomitance dans la neuvième Convention de La Haye de 1907[99]. Il est exigé des États que leur réaction soit spontanée et directe. Le choix du mode de riposte relativement à l'exigence de concomitance et dans le cadre d'une cyberattaque revêt un certain intérêt. Les cyberattaques peuvent se caractériser par une attaque rapide ou par une attaque dont les effets se mettront en place de manière progressive. La concomitance doit alors être analysée relativement aux effets de l'attaque. Si la cyberattaque est menée rapidement, la concomitance est simple à évaluer. Dans le cadre d'une attaque échelonnée, la concomitance devrait être évaluée à

[98] M. N. SCHMITT, *Cyber Operations and the Jud Ad Bellum Revisited*, 56 Vill. L. Rev. 569, 2011, p. 593.

[99] Article 2§3, Convention IX de La Haye, La Haye, 1907.

partir du seuil de caractérisation de l'attaque armée : si un élément offensif cybernétique est mis en sommeil dans le système visé et qu'il produit les effets nécessaires à la qualification d'une attaque armée, c'est à cet instant là que la concomitance doit être évaluée. Dès lors qu'on a déterminé le moment à partir duquel la concomitance doit être appréciée, il est nécessaire de déterminer quels moyens et méthodes de ripostes respectent ladite exigence. Un *hack-back* automatique semble remplir le critère de concomitance face à une cyber-attaque spontanée et immédiate ou lorsque le seuil de gravité visé *supra* est atteint par une attaque échelonnée. En revanche, on peut se demander si une riposte *via* une cyberattaque échelonnée remplit le critère de concomitance. Une riposte conventionnelle, si elle est effectuée dans des délais jugés concomitants à la cyberattaque, devra être jugée comme légale à cet égard. Mais il est toujours possible de se demander si la notion de concomitance s'applique de manière analogue pour la riposte cybernétique et pour la réponse conventionnelle : au fond, une riposte conventionnelle peut-elle être concomitante à une cyberattaque, eu égard à son potentiel de célérité ?

Les experts en charge de la rédaction du Manuel de Tallinn 2.0 dégagent un quatrième critère nécessaire à l'exercice de la légitime défense : l'imminence[100]. Ils considèrent qu'un État n'a « *pas à rester immobile alors que l'ennemi se prépare à attaquer* ». Ce critère renvoie à la notion de légitime défense préemptive, introduite dans le cadre du droit international contemporain[101] par G.W Bush lors des attaques terroristes subies par les États-Unis en 2001. Cette logique se base donc sur l'imminence absolue d'une cyberattaque corroborée par des informations concordantes comme fondement à une attaque préemptive. Dans le cadre cybernétique, il apparait difficile de légitimer ce type d'action. Les experts mentionnent l'hypothèse d'une situation où des informations indéniables

[100] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 73, paras 2-11.

[101] La notion d'opération de légitime défense préemptive pourrait aussi trouver son origine dans l'affaire *Caroline.* V. : M.C. WAXMAN, *The Caroline affair in the evolving international law f self-defense*, Irwin Law, 2018.

montrent l'imminence d'une attaque : étant donnée la nature hautement opaque du cyberespace, et les risques de manipulations qui en découlent, cette simple base ne suffit pas. Au surplus, il apparait difficile de déterminer comment un État pourrait établir qu'une cyberattaque est imminente avant que celle-ci ne se déroule. À ce titre, les experts effectuent toutefois une distinction entre les « *actes préparatoires* » de l'attaque et l'attaque elle même : mais, dans le cyberespace, la distinction entre les deux est difficile, et il apparait improbable qu'un État puisse réagir de manière préemptive entre le stade préparatoire et l'attaque elle même[102].

Il existe un autre cas où un État peut être amené à exercer légitimement la force cybernétique : les autorisations du Conseil de sécurité délivrées au titre du chapitre VII de la Charte.

2. Les autorisations au recours à la force du Conseil de Sécurité des Nations Unies

En dehors du cas classique de légitime défense, un État peut user légitimement de la force lorsqu'il a été habilité à le faire par le Conseil de Sécurité des Nations Unies au titre du chapitre VII de la Charte.

En vertu de l'article 39 de la Charte, le Conseil de sécurité « *constate l'existence d'une menace contre la paix, d'une rupture de la paix ou d'un acte d'agression et fait des recommandations ou décide quelles mesures seront prises conformément aux articles 41 et 42 pour maintenir ou rétablir la paix et la sécurité internationales* »[103]. À ce titre, le Conseil est amené à prendre des mesures qui ne relèvent pas de l'emploi de la force et qui sont nécessaires à la poursuite

[102] À l'exclusion éventuelle de certaines opérations échelonnées.

[103] Article 39, Charte des Nations Unies, San Francisco, 26 juin 1945.

de ces objectifs[104], mais également à prendre des mesures relevant du recours à la force si les premières échouent ou sont inadaptées[105].

À l'heure actuelle, aucune cyberopération n'a poussé le Conseil à juger qu'il existait une menace ou une rupture de la paix. Cependant, rien n'indique que cela ne puisse arriver.

En revanche, on peut très bien imaginer une situation représentant une rupture de la paix nécessitant des mesures relevant de l'article 42. Dans ce cas, un État - ou une organisation régionale - serait fondée à employer la force, force cybernétique comprise. Dans le cadre d'une opération de maintien ou de rétablissement de la paix, le constat est le même : l'État est autorisé à employer ses capacités cybernétiques en adéquation avec le mandat.

Après avoir envisagé les interactions pratiques entre le *jus ad bellum* et l'emploi de moyens et méthodes de combat cybernétiques, il est question de déterminer sur l'emploi de tels moyens et méthodes est compatible avec les buts poursuivis par cet ensemble de règles.

[104] Article 41, Charte des Nations Unies, San Francisco, 26 juin 1945.

[105] Article 42, Charte des Nations Unies, San Francisco, 26 juin 1945.

- **<u>Chapitre II - L'intérêt du *jus ad bellum* à l'épreuve de l'emploi de la force cybernétique</u>**

L'article 1 paragraphe 1 de la Charte des Nations Unies dispose que l'un des but de l'organisation est de « *maintenir la paix et la sécurité internationales et à cette fin* [de] *prendre des mesures collectives efficaces en vue de prévenir et d'écarter les menaces à la paix et de réprimer tout acte d'agression ou autre rupture de la paix, et réaliser, par des moyens pacifiques, conformément aux principes de la justice et du droit international, l'ajustement ou le règlement de différends ou de situations, de caractère international, susceptibles de mener à une rupture de la paix* »[106]. L'article poursuit ensuite en exposant d'autres buts de l'organisation relatifs à l'égalité entre les peuples et à leur droit à disposer d'eux-mêmes ainsi qu'a la coopération internationale nécessaire au développement de certaines branches du droit, comme les droits de l'Homme.

L'un des objectifs essentiels de la Charte est donc de maintenir ou de rétablir la paix et la sécurité internationales. Nous verrons d'abord l'articulation entre cet objectif et l'emploi de moyens et méthodes de combat cybernétiques avant d'envisager certaines solutions aux difficultés rencontrées par cette articulation.

[106] Article 1, Charte des Nations Unies, San Francisco, 26 juin 1945.

I. L'articulation difficile entre l'objectif de maintien et de rétablissement de la paix et de la sécurité internationales et l'emploi de moyens et méthodes de combat cybernétiques

Le *jus ad bellum* règlemente l'accès à l'emploi de la force dans le cadre de la Charte pour poursuivre l'objectif de maintien et de rétablissement de la paix et de la sécurité internationales. Les moyens et méthodes de combat cybernétiques, en raison de leur particularité et de celle de l'environnement dans lequel ils sont déployés, peuvent apparaitre comme intrinsèquement incompatibles avec l'objectif de maintien de la paix (A). Ces mêmes particularités rendent le rétablissement de la paix délicat (B).

A. Les moyens et méthodes de combat cybernétiques naturellement incompatibles avec l'objectif de paix et de sécurité internationales

Les moyens et méthodes de combat cybernétiques sont incompatibles à deux égards avec l'objectif de maintien de la paix : leur propension à proliférer et à se propager.

1. Le potentiel de prolifération des armes cybernétiques

En biologie, la prolifération s'entend de la « *multiplication rapide, normale ou pathologique, d'éléments biologiques, en particulier de cellules* »[107]. Cette notion peut être appliquée au domaine militaire. La prolifération s'entend alors de la production et de la diffusion sévère voire incontrôlée de certaines armes. Ce sont généralement les armes de destruction massive

[107] Académie Française, *Dictionnaire de l'Académie française*, 9ème édition, tome 2, 1992, consulté en ligne le 29 juillet 2019. Disponible en ligne : « https://www.dictionnaire-academie.fr/article/A9P4541 »

qui sont visées. On parle alors de prolifération nucléaire, chimique ou biologique. Il ressort du préambule au Traité sur la Non-prolifération des Armes Nucléaires que la prolifération de certaines armes constitue une menace contre la paix[108]. Cette position est confirmée par le Conseil de Sécurité[109] et se retrouve dans la position de la diplomatie française[110].

Les statistiques actuelles en matière de cybersécurité montrent une multiplication des actes cybernétiques malveillants. Cette multiplication est le fruit d'une prolifération rapide des moyens de combat cybernétiques, lesquels échappent souvent au contrôle de leur créateur, qu'il soit étatique ou non. L'épisode *Wannacry* illustre parfaitement ce type de prolifération. *Wannacry* est un « *ransomware* » ou « rançongiciel »[111] qui a été utilisé en mai 2017 pour bloquer l'accès aux fichiers de plus de 200 000 personnes à travers le monde. Ce rançongiciel utilisait un *exploit* dénommé *EternalBlue*, développé par la *National Security Agency* (N.S.A) américaine et qui lui avait été dérobé par un groupe de hackers. Depuis, l'étude du code de *Wannacry* montre que l'*exploit* développé par la N.S.A aurait été employé dans plusieurs campagne de rançonnage, comme *Petya*[112] et *BadRabitt*[113].

---

[108] Traité sur la non-prolifération des armes nucléaires, Nations Unies, *Recueil des traités*, vol. 729, n °I-10485.

[109] V. : Conseil de sécurité des Nations Unies, Résolution 1887, S/RES/1887, Préambule.

[110] Ministère de l'Europe et des affaires étrangères, *Désarmement et non-prolifération*, disponible en ligne : « https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/desarmement-et-non-proliferation/ », consulté le 3 août 2019.

[111] Le *ransomware* ou rançongiciel est une « *forme d'extorsion imposée par un code malveillant sur un utilisateur système. Pour y parvenir, le rançongiciel va empêcher l'utilisateur d'accéder à ses données, par exemple en les chiffrant, puis lui indiquer instructions utiles au paiement de la rançon* », Agence nationale de la sécurité des systèmes d'information, *Glossaire*, « rançongiciel », consulté en ligne le 29 juillet 2019. Disponible en ligne : « https://www.ssi.gouv.fr/entreprise/glossaire/r/ ».

[112] Symantec Security Response Team, *Petya ransomware outbreak : here's what you need to know*, 24 octobre 2017. Disponible en ligne : « https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper », consulté le 7 août 2019.

[113] Symantec, *About the BadRabitt ransomware*, alerte2452, 25 octobre 2017. Disponible en ligne : « https://support.symantec.com/us/en/article.alert2452.html », consulté le 7 aout 2019.

Selon Aude Géry, cette prolifération des armes cybernétiques serait le fruit de quatre facteurs[114].

Le premier facteur serait purement technologique. Certains progrès technologiques constitueraient de nouvelles portes pour mener à bien des actes cybernétiques malveillants. L'auteure cite notamment le cas des objets connectés : en 2016, le gestionnaire de noms de domaine *Dyn* subissait une campagne de déni de service propagée par des caméras de surveillance connectées infectées par le *malware Mirai*[115].

Le deuxième acte a trait à la disponibilité des armes cyber. On peut citer à nouveau l'*exploit EternalBlue* qui a été développé par la N.S.A avant de lui être dérobé et d'être mis à disposition par le groupe *Shadow Brokers*. Le célèbre *Stuxnet* est aujourd'hui en *open source*[116]. L'opacité du cyberespace rend aisés le stockage et la distribution d'armes cyber. Là où accéder à certaines armes conventionnelles ou de destruction massive s'avère relativement complexe, quasiment tout État, tout groupe non étatique et tout individu peut s'armer sur le cyberespace.

Le troisième est relatif à certaines pratiques des acteurs du cyberespace. D'un côté, on peut observer que les armes cyber font aujourd'hui l'objet d'un véritable commerce. Au surplus, certaines méthodes de cybersécurité peuvent également concourir à la prolifération des armes cybernétiques : on pense notamment à certaines mesures de cyberdéfense active.

---

[114] A. GÉRY, « La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense », dans *Les champs de Mars*, Presses de Sciences Po, n°30, p. 311-313.

[115] Z.MA, « Undesrtanding the Mirai botnet », dans *Proceedings of the 26th USENIX Security Symposium*, Vancouver, Canada, 16-18 aout 2017.

[116] On parle le logiciel *open source* lorsque son code est gratuitement et librement accessible pour l'utilisation ou la duplication.

Le dernier facteur tient du manque de progrès et de cadre au niveau du droit international. Étant donné que la question de l'application du droit international aux armes cyber ne rencontre pas encore un consensus satisfaisant, aucun véritable cadre légal international n'a été mis en place pour freiner cette prolifération, du moins au plan universel. Nous verrons ultérieurement ce qu'il en est de certaines tentatives régionales.

La prolifération rapide et persistante des armes cyber est doublée d'un énorme potentiel de propagation des armes cyber.

2. Le potentiel de propagation des armes cybernétiques

Supra, nous avions proposé une distinction entre la diffusion et la propagation de l'arme cyber[117]. La propagation renvoie à une contamination incontrôlée qui peut dépasser le cadre de l'opération entreprise. Elle est particulièrement envisageable dans l'emploi de certaines armes cyber qui opèrent sur un mode de diffusion automatique.

La propagation représente par nature un danger au maintien de la paix et de la sécurité internationales dans la mesure où l'arme qui se propage a échappé à l'instigateur de l'opération entendue *lato sensu*. Elle peut dès lors dépasser le cadre de l'emploi licite de la force et se propager à d'autres cibles illégitimes. L'analogie peut être faite avec l'arme biologique qui peut se propager de manière incontrôlée dans l'espace tangible, à l'instar de l'arme cyber qui peut se propager dans le cyberespace en raison de son origine cybernétique. La sévérité du risque est proportionnelle au potentiel destructeur de l'arme cyber considérée.

[117] V. *Supra* : p.5, note 20.

Ces deux facteurs, manifestement contraires aux objectifs de la Charte, sont doublés des grandes difficultés d'attribution des actes cybernétiques malveillants.

B. Les difficultés d'attribution inhérentes à l'emploi de la force cybernétique et leur impact sur l'action du Conseil de sécurité

La Charte prévoit de défendre la paix et la sécurité internationales en interdisant le recours à la force. Ce procédé repose sur la conviction qu'un usage de la force illicite soit attribuable. Or, dans le cyberespace, l'attribution peut s'avérer extrêmement difficile. Cette difficulté a un impact direct sur l'action du Conseil de sécurité en cas de violation de l'article 2 paragraphe 4.

1. Les difficultés d'attribution inhérentes à l'emploi de la force cybernétique

L'attribution représente l'un des principaux écueils de l'application du droit international aux actes cybernétiques[118]. Selon Guillaume Poupard, directeur générale de l'Agence nationale de la sécurité des systèmes d'information, « *l'attribution des attaques est le grand problème du cyber* ».

Ces difficultés d'attribution sont expliquées par différents facteurs propres à l'emploi de moyens et méthodes de combat cybernétiques[119]. D'abord, comme cela a déjà été expliqué, le cyberespace est un environnement opaque au sein duquel il est difficile voire impossible d'identifier

[118] S.G. HANDLER, « The new cyber face of battle : developing a legal approach to accommodate emerging trends in warfare », *Stanford Journal of International Law*, 2012, p. 213.

[119] Assemblée nationale, *Rapport d'information déposé en conclusion des travaux d'une mission d'information sur la cyberdéfense*, 4 juillet 2018, B.3.b.

clairement l'adversaire. La chaine d'anonymisation peut être extrêmement dense et il est parfois impossible de la remonter entièrement. Ensuite, les cyberattaques et cyberopérations offensives sont rarement revendiquées par les États. Encore, les cyberattaques et cyberopérations offensives sont rarement « directes » dans le sens où elles transitent généralement par plusieurs systèmes pour brouiller les pistes. Au surplus, l'État qui agit ainsi peut mettre en place les dispositions nécessaires pour effacer progressivement les traces de son passage, rendant encore plus délicate l'attribution[120]. Le risque de propagation de l'arme cyber est aussi un facteur entravant l'attribution : en effet, une attaque se propageant de manière incontrôlée à d'autres victimes va empêcher d'identifier la cible initiale et donc obscurcir un des indices d'attribution. Pire encore, l'arme cyber pourrait être employée de manière à se diffuser de façon contrôlée à des victimes collatérales pour brouiller sciemment les pistes. Enfin, l'attribution peut être limitée par certaines cyberopérations ou cyberattaques dont le déclenchement se déroule bien après l'intrusion initiale.

Cette difficulté à attribuer les actes cybernétiques hostiles va phagocyter le droit d'employer des contremesures, le droit de faire appel à la cyberdéfense active ou encore d'exercer la légitime défense, ces trois modes de riposte nécessitant une attribution préalable du fait illicite. Elle constitue donc un obstacle manifeste à l'application du *jus ad bellum* et, par extension, constitue un risque pour la paix et la sécurité internationales, notamment dans la mesure où elle rend quasiment inopérable un exercice de la légitime défense respectueux du droit international.

Pour palier cette difficulté, il est considéré que l'attribution relève en dernier ressort d'une appréciation politique corroborée par un faisceau d'indices. L'affaire *Stuxnet* illustre ce « *glissement*

[120] D.E. BAMBAUER, « Conundrum », *Minnesota Law Review*, 2011-2012, p. 589.

probatoire au profit des suppositions »[121]. Ce mode d'attribution n'est absolument pas satisfaisant eu égard au but poursuivi par la Charte dans sa prohibition de l'usage de la force.

Cette difficulté d'attribution va avoir un impact direct sur l'action du Conseil de sécurité face à un État pour une violation du *jus ad bellum*.

2. L'action du Conseil de sécurité et l'écueil de l'attribution

Les articles 39, 41 et 42 de la Charte déterminent l'action du Conseil face à une situation d'emploi illicite de la force. Le Conseil constate la menace ou la rupture de la paix, prend les mesures n'impliquant pas l'emploi de la force qu'il estime utiles pour leur rétablissement puis, si elles ne suffisent pas, décide ou non de délivrer une autorisation à employer la force. Ces dispositions s'appliquent *de facto* au cas de l'emploi de la force cybernétique[122]

Or, si l'on considère qu'il est extrêmement difficile voire impossible d'attribuer de manière satisfaisante d'un point de vue probatoire, on imagine mal comment le Conseil de sécurité pourrait agir. Cette hypothèse s'inscrit surtout dans le cas de cyberopérations ou de cyberattaques autonomes qui ne sont pas effectuées en support d'opérations cinétiques. Mais dans les cas où une cyberopération ou une cyberattaque autonome constituerait une violation du *jus ad bellum*, quelle solution reste-t-il au Conseil ? À part la constatation de la situation prévue par l'article 39, le

---

[121] L. CHANG-TUNG, *Le droit international à l'épreuve de la cyberguerre - le cas de Stuxnet*, Université de Grenoble, janvier 2018, p.7. Le faisceau d'indice renvoyant l'attribution du ver aux États-Unis et Israël était composé de plusieurs éléments. Sa complexité et la manière dont il a été codé ont notamment été citées. V. : J.HALLIDAY, « Stuxnet Worm is the work of a national government agency », *The Guardian*, 24 septembre 2010 ; J.F.MURPHY « Cyber War and international law : does the international legal process constitue a threat to U.S vital interests ? », dans *International Law Studies U.S. Naval War College*, 2013, p. 314-315.

[122] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 2 février 2017, règle 76.

Conseil semble paralysé par l'absence d'attribution satisfaisante. Le Conseil pourrait alors, comme au niveau national, procéder à une analyse politique basée sur un faisceaux d'indices ; toutefois, il est difficile d'envisager que les membres du Conseil puissent se mettre d'accord sur une telle analyse.

Les moyens et méthodes de combat cybernétiques, associés à l'environnement dans lequel ils sont déployés, semblent donc incompatibles avec les objectifs de la Charte et le *jus ad bellum*. Il est toutefois possible d'imaginer certaines solutions à ce problème.

II. Les solutions envisageables à l'incompatibilité entre moyens et méthodes de combat cybernétiques et les objectifs du *jus ad bellum*

Deux solutions semblent envisageables pour articuler de manière satisfaisante l'emploi de moyens et méthodes de combat cybernétique et le *jus ad bellum* : le développement d'une règlementation internationale et le renforcement du principe de *due diligence*.

A. La mise en place d'une réglementation stricte de l'emploi des moyens et méthodes de combat cybernétique

La première solution pour encadrer l'emploi des moyens et méthodes de combat cybernétiques du point de vue du *jus ad bellum* aurait été de faire appel au Conseil de sécurité. Cependant, comme il a été exposé *supra*, les difficultés d'attribution empêchent ce dernier d'intervenir. La doctrine a alors envisagé la rédaction d'un traité international[123]. Cette proposition

[123] V. pour exemple : B. RABOIN, « Corresponding évolution : International law and the emergency of Cyber Warfare », *Journal of National Association of Administrative Law Judiciary*, 2011, p. 661.

n'a pas rencontré le consensus espéré : bien qu'elle ait été soutenue par la Russie[124], il a été considéré que les dispositions de la Charte étaient suffisantes pour encadrer l'usage de la force cybernétique[125]. En soit, les dispositions de la Charte sont effectivement suffisantes pour régir ces actes. Cependant, d'un point de vue pratique, les difficultés d'attribution les rendent inopérantes.

Une autre solution, du point de vue de la prolifération des armes cybernétiques, serait de s'inspirer de l'article 6 de la Convention sur la cybercriminalité[126] qui impose aux États signataires d'« *ériger en infraction pénale* […] *la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition* » d'éléments cyber servant à commettre des actes cybernétiques malveillants. En somme, il serait question d'établir un traité de non-prolifération des armes cybernétiques.

Cependant, l'attrait actuel pour les moyens et méthodes de combat cybernétiques qui réside essentiellement dans leur anonymat est tel qu'il semble inenvisageable que les États puissent se mettre d'accord sur la question. Pour les États « dominants », le vecteur cybernétique est un moyen d'asseoir leur contrôle. Pour les États « dominés », le vecteur cybernétique représente un moyen de compensation.

Si l'instauration d'un cadre conventionnel plus strict et plus précis semble impossible aujourd'hui, il faut envisager une solution « détournée » : le principe de *due diligence*.

---

[124] *Ibid*, p. 664.

[125] W.MCGAVRAN, « Intended consequences : regulating cyber attacks », *Tulane Journal of Technology and Intellectual Property*, 2009, pP. 272-273.

[126] Article 6, Convention sur la Cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001.

B. Le renforcement du principe de *due diligence*

Le principe de *due diligence* repose sur la responsabilité des États de s'assurer que leur territoire ne sert pas à la conduite d'activités contraires aux droits d'autres États[127].

Dans le cadre cybernétique[128], il ne serait alors plus question de déterminer l'auteur de l'acte illicite, mais d'identifier les États dont le territoire a permis l'acheminement de l'opération. Cependant, en l'état, cette solution ne semble pas des plus satisfaisantes. D'abord parce que dans le cadre de ce principe, il est obligatoire de démontrer que l'État dont le territoire était utilisé avait connaissance de cette utilisation[129]. Dès lors, l'État victime devrait prouver que l'État avait connaissance de l'utilisation qui était faite de son territoire, ce qui peut s'avérer très difficile dans le cadre cybernétique. Bien que le critère probatoire ait été adoucit[130], l'établissement du faisceau d'indices reste délicat. Ensuite, et surtout, parce que appliquer le principe de *due diligence* n'invite pas à chercher et éventuellement sanctionner l'État auteur de l'acte cybernétique, mais seulement les États dont le territoire à permis le transit de la cyberattaque ou de la cyberopération offensive.

Il serait alors nécessaire de renforcer le principe de *due diligence* pour le rendre proactif dans le cadre cybernétique. On peut imaginer, par exemple, instaurer une obligation pour chaque État développant des armes cybernétiques d'incorporer dans le code de l'arme une balise d'identification pour instaurer une sorte de balistique cybernétique. Cependant, l'adoption de ce

---

[127] Cour internationale de justice, *Détroit de Corfou*, Recueil, 1949, p. 22.

[128] K.BANNELIER, « Cyber Diligence : A low-intensity due diligence principle for low-intensity Cyber-Operations ? », *Baltic Yearbook of International Law*, vol. 14, 2014, pp. 23-29.

[129] Cour Internationale de Justice, *Personnel diplomatique et consulaire des États-Unis à Téhéran*, Recueil, 24 mai 1980, para. 68.

[130] L. CHANG-TUNG, *Le droit international à l'épreuve de la cyberguerre - le cas de Stuxnet*, Université de Grenoble, janvier 2018, p. 25.

genre de dispositions ne peut pas se faire *ex nihilo* : elle doit certainement être rendue possible par la ratification d'accords spécifiques ou d'un traité international. Alors, nous retombons dans les difficultés déjà exposées sur la détermination d'un cadre plus stricte à l'emploi d'armes cybernétiques.

Finalement, nous avons démontré que l'usage de moyens et de méthodes cybernétiques constituait un véritable défi pour l'application du *jus ad bellum*. La spécificité à la fois du milieu cybernétique et des vecteurs cybernétiques est de nature à entraver l'application du *jus ad bellum*. L'opacité du cyberespace pose des difficultés considérables pour l'attribution des cyberopérations offensives et cyberattaques illicites, entravant toutes les formes de recours licites à la force prévues par la Charte. La mutabilité du cyberespace et l'incapacité patente de certains États à maitriser leur stock d'armes cybernétiques est un véritable facteur d'instabilité pour la paix et la sécurité internationales. Ces différents éléments semblent tendre vers le constat que le développement d'une règlementation internationale est nécessaire pour préserver le *jus ad bellum* et les objectifs qu'il poursuit. Pourtant, les avantages que présentent les moyens et méthodes de combat cybernétiques rendent inenvisageable la mise en place d'un nouveau système de régulation de leur production et de leur emploi.

Dès lors, en l'absence de cadre plus strict, il est certain que les moyens et méthodes de combat cybernétiques vont continuer de se développer rapidement. Parallèlement, leur emploi dans le cadre de conflit armés va augmenter de manière exponentielle. Il est alors nécessaire de déterminer comment le *jus in bello* s'applique à l'utilisation de moyens et méthodes de combat cybernétiques.

• Partie II - *Jus in bello* et emploi de la force cybernétique

Le *jus in bello* constitue l'ensemble des règles conventionnelles et coutumières qui règlementent la conduite des hostilités dans le cadre d'un conflit armé. Ces règles ont vocation à limiter les moyens et les effets de la guerre dans une optique d'humanité. Cet ensemble est notamment composé du droit de La Haye[131], du droit de Genève[132] et d'autres traités de limitation ou d'interdiction spécifiques[133]. Le développement des moyens et méthodes de combat cybernétiques pose la question des relations entre cette nouvelle déclinaison de la force armée et les règles du *jus in bello*. Dans un premier temps, ces interrogations nous conduiront à déterminer la place des armes cybernétiques dans l'arsenal visé par les règles du *jus in bello*. Dans un second temps, c'est l'application de ce dernier à l'utilisation de moyens et méthodes de combat cybernétiques dans le cadre de conflits armés qui sera abordée.

[131] On peut citer les différentes conventions conclues en 1907, et notamment la quatrième convention relative aux lois et coutumes de la guerre sur terre.

[132] Les quatre conventions de Genève (1949) et leur deux protocoles additionnels (1977).

[133] V. notamment : Convention sur l'interdiction des armes biologiques, Londres, Moscou et Washington, 10 avril 1972. Convention sur certaines armes classiques, Genève, 10 octobre 1980. Convention sur l'interdiction des armes chimiques, Genève, 3 septembre 1992, Convention d'Ottawa sur l'interdiction des mines antipersonnel, Ottawa, 18 septembre 1997. Convention sur les armes à sous-munitions, Dublin, 30 mai 2008. Traité sur le commerce des armes, New York, 2 avril 2013.

- **Chapitre I - La place des moyens et méthodes de combat cybernétiques dans le *jus in bello***

Du point de vue du *jus in bello* et de la pratique militaire, les armes peuvent être classifiées selon différentes catégories (I). Le *jus in bello* impose également certaines normes dans la mise au point de nouvelles armes, ce qui touche particulièrement le cas des armes cybernétiques (II).

I. L'arme cybernétique et les classifications traditionnelles

Les classifications les plus courantes répartissent les armes selon deux grandes dichotomies. D'une part, on retrouve la distinction entre les armes conventionnelles ou classiques et les armes de destruction massive (A). D'autre part, on trouve une distinction entre les armes stratégiques et les armes tactiques (B).

A. L'arme cybernétique : arme conventionnelle ou de destruction massive.

La question est de déterminer si les armes cybernétiques peuvent être classées dans la catégorie des armes conventionnelles, ou si, en raison de leur nature, elles pourraient être assimilées à des armes de destruction massive.

1. Une arme conventionnelle

Les armes conventionnelles ou classiques se définissent comme des armes qui ne sont pas contraires aux règles conventionnelles internationales de régulation des moyens de guerre. Il

n'existe pas de véritable définition des armes conventionnelles et elles sont généralement définies négativement : les armes conventionnelles sont les armes qui ne sont pas non-conventionnelles

Les armes non-conventionnelles font généralement l'objet d'un traité qui limite ou interdit leur utilisation. La Convention sur certaines armes classiques[134] interdit ou limite l'emploi, le stockage, la production et le transfert de différents moyens de guerre : les éclats non localisables[135], les mines, pièges et autres dispositifs[136], les armes incendiaires[137], les armes à laser aveuglantes[138]. On peut également citer la Convention sur les armes à sous-munitions qui prévoit l'interdiction absolue du recours, de la mise au point, de la production, de l'acquisition, du stockage, de la conservation ou du transfert d'armes à sous-munitions[139].

À l'heure actuelle, aucun traité ne vise les armes cybernétiques. À défaut de convention contraire, l'arme cybernétique pourrait donc être considérée comme une arme conventionnelle. Pourtant, plusieurs éléments laissent planer un doute sur cette position. D'abord parce que l'arme cybernétique, bien que ses effets puissent atteindre l'espace tangible, opère dans le cyberespace, ce qui n'a rien de « classique ». Ensuite parce que le potentiel destructeur d'une arme cybernétique est par nature flou. L'arme cybernétique peut aussi bien avoir les effets d'une bombe conventionnelle que ceux d'une bombe nucléaire. La réalité est que, en raison de l'opacité du cyberespace, les

---

[134] Convention sur certaines armes classiques, Genève, 10 octobre 1980.

[135] Protocole I relatif aux éclats non localisables, Convention sur certaines armes classiques, Genève, 10 octobre 1980.

[136] Protocole II sur l'interdiction ou la limitation de l'emploi des mines, pièges et autres dispositifs, Convention sur certaines armes classiques, Genève, 10 octobre 1980.

[137] Protocole III sur l'interdiction ou la limitation de l'emploi des armes incendiaires, Convention sur certaines armes classiques, Genève, 10 octobre 1980.

[138] Protocole IV relatif aux armes à laser aveuglantes, Convention sur certaines armes classiques, Genève, 13 octobre 1995.

[139] Article 1, Convention sur les armes à sous-munitions, Dublin, 30 mai 2008.

moyens et méthodes cybernétiques possèdent des potentiels destructeurs si variables qu'il est difficile de déterminer s'ils constituent forcément des armes conventionnelles du fait d'une absence de réglementation.

Si les armes cybernétiques ne sont pas des armes conventionnelles, peut-on considérer qu'il s'agisse d'armes de destruction massive ?

2. Une arme de destruction massive

Une arme de destruction massive se caractérise par une capacité destructrice immense, incontrôlable ou totalement inhumaine. Les armes de destruction massive réunissent les armes nucléaires, les armes biologiques, les armes radiologiques et les armes chimiques.

Al Mauroni propose trois conditions pour déterminer si un moyen de combat donné correspond à une arme de destruction massive[140]. Conditions qu'il est possible de rapporter au modèle cybernétique.

D'abord, l'architecture initiale du système envisagé doit avoir été pensée pour qu'il serve d'arme. Par exemple, on peut imaginer un *malware* dont le code a été spécifiquement élaboré pour causer des dommages physiques[141]. Ensuite, l'arme cybernétique doit avoir la capacité de causer un nombre massif de victimes à un instant donné. Comme l'indique W. Seth Carus, il n'existe pas de

---

[140] A. MAURONI, *Countering Weapons of Mass Destruction: Assessing the U.S. Government's Policy*, Rowman & Littlefield, 2016, pp. 36-42.

[141] Par exemple, *Stuxnet*.

définition de la notion de « perte de vies massive »[142]. Aucun seuil officiel n'existe quantitativement. En ce sens, la proposition de Mauroni de restreindre la notion à un élément temporel et spatial semble intéressante. Elle doit toutefois être étendue aux effets résiduels de l'arme employée. Évidemment, le critère doit également être recentré autour du lien causal. L'arme A employée une seule fois doit causer un nombre X de victimes à un instant T+Y, Y représentant alors les effets résiduels de son emploi, notamment lors d'une attaque biologique ou nucléaire. De l'avis général, il existe plusieurs cas de figure où une arme cyber pourrait avoir de telles conséquences. Les plus emblématiques sont l'activation de la fusion d'un réacteur nucléaire, la désactivation des systèmes et services de contrôle du trafic aérien résultant en *crash*, et l'ouverture d'un barrage en amont d'une zone peuplée. Enfin, le dernier critère proposé par Mauroni est que l'arme considérée soit définie par une convention internationale comme une catégorie particulière d'arme.

Si l'on suit ce schéma de pensées, l'arme cybernétique remplit les deux premières conditions envisagées par Mauroni : l'arme cybernétique à été développée dans l'intention de servir d'arme, et elle peut posséder le potentiel destructeur exprimé par l'auteur. En revanche, aucune convention internationale ne désigne les armes cybernétiques comme une catégorie d'arme spéciale. Pour certains, les efforts de la communauté internationale, ainsi que ceux de certaines organisations régionales et plus largement de la doctrine pourraient signifier que le troisième critère est rempli[143]. À nos yeux, ce procédé viendrait fragiliser le schéma proposé par Mauroni.

---

[142] W.S.CARUS, Defining « Weapons of Mass Destruction », *Occasional Paper,* n°8*,* Center for the Study of Weapons of Mass Destruction, National Defense University, janvier 2012, pp. 39-42.

[143] B.B.HATCH, « Defning a Class of Cyber Weapons as WMD: An Examination of the Merits », dans *Journal of Strategic Security*, vol. 11, n°1, 2018, pp. 46-47.

Une troisième option est alors envisageable : celle d'une voie alternative, où l'arme cybernétique ne serait ni une arme conventionnelle, ni une arme de destruction massive.

3. Une arme cybernétique

La solution alternative à la classification traditionnelle entre les armes conventionnelles et les armes non-conventionnelles ou de destruction massive serait d'envisager l'arme cybernétique pour ce qu'elle est : une arme cybernétique.

Nous l'avons vu, l'arme cybernétique montre des particularités assez marquées par rapport aux armes « classiques » et ce notamment en raison de l'environnement si particulier qu'est le cyberespace. Ces armes ont le potentiel de perturber grandement l'adversaire mais sans causer de véritable destruction physique. Elles ont également le potentiel de causer des victimes et des destructions physiques d'une ampleur analogue à celle d'armes conventionnelles, non-conventionnelles ou encore de destruction massive. En réalité, l'arme cybernétique est appréhendée comme un tout : soit comme une arme conventionnelle, au même titre qu'un missile, soit comme une arme de destruction massive, au même titre qu'une bombe nucléaire. C'est ce postulat de base qui est erroné : l'arme cybernétique est un ensemble d'armes diverses et variées propre à un environnement précis. Dès lors, il serait bien plus judicieux de proposer une classification des différentes armes cybernétiques en fonction de leur potentiel destructeur et de leur rapport aux spécificités du cyberespace. La catégorie des armes cybernétiques ainsi autonome, il serait plus simple de les encadrer.

Toutefois, la réelle difficulté concernant l'encadrement et la classification des armes cybernétiques réside dans le manque de volonté des États qui peuvent user de certaines de ces caractéristiques pour contourner leurs obligations internationales[144].

Sur le plan militaire, il est intéressant de déterminer si l'arme cybernétique est par nature plutôt tactique ou stratégique.

B. L'arme cybernétique, arme tactique ou stratégique.

La distinction entre arme tactique et arme stratégique n'est pas la plus satisfaisante puisqu'elle créé un paradigme où stratégie et tactique seraient déterminés par un paramètre de distance ou de portée, ce qui n'est pas l'essence de leur nature[145]. Pour autant, faute d'une classification plus adéquate, la question sera de déterminer si les armes cybernétiques doivent plutôt être considérées comme des armes tactiques ou comme des armes stratégiques. Généralement ces deux types d'armes sont de nature nucléaire.

1. L'arme stratégique

L'arme stratégique est une arme de longue portée dont la puissance est maximale et dont l'objectif peut être l'anéantissement de l'adversaire. L'arme stratégique joue essentiellement un rôle dissuasif : tel est le cas, par exemple, de nos sous-marins nucléaires lanceurs d'engins. Ces armes

---

[144] Notamment, en raison de l'opacité et des difficultés d'attribution, les armes cybernétiques permettent certaines entorses au droit international, *jus in bello* compris, lesquelles entorses sont difficilement répréhensibles.

[145] C.AILLERET, « Armes tactiques et stratégiques », dans *Correspondance*, n°043, décembre 1947. V. également : CIVIS, « À propos d'une classification des armements », dans *Politique étrangère*, n°3, 1962, p. 223.

ont vocation à dissuader l'adversaire d'envisager toute opération militaire hostile à l'égard de leur possesseur. La nature dissuasive de ces armes est toutefois sujette à certaines controverses : la dissuasion suppose qu'un État soit prêt à employer une telle arme dans une situation qui le nécessite. Mais employer ces armes aurait des conséquences si dramatiques qu'un doute subsiste en tous temps sur l'intention réelle de l'État de l'employer[146].

L'arme cybernétique est très largement envisageable et envisagée comme une arme de longue portée. Au surplus, il a été démontré que certaines déclinaisons de l'arme cybernétique étaient susceptibles de produire des effets similaires à ceux d'une arme stratégique. Cependant, le propre de l'arme cybernétique est d'opérer dans l'ombre : le concept de cyberdissuasion, s'il existe, reste sujet à un obstacle majeur, celui de la poursuite de l'anonymat des cyberattaques[147]. Pour dissuader, il faut exposer ses capacités ; or, exposer ses capacités nie l'intérêt essentiel du cyberespace. Dès lors, peut-on raisonnablement considérer que l'arme cybernétique puisse être une arme stratégique ? On le peut, mais son efficacité en ce domaine reste limitée.

On peut alors se demander si l'arme cybernétique tient plus de l'arme tactique que de l'arme stratégique.

2. L'arme tactique

L'arme tactique est une arme de courte portée ou moyenne portée. La puissance de l'arme est limitée et son objectif aussi - on peut même considérer qu'il est défensif[148]. Généralement, on

---

[146] *Ibid*, p. 225.

[147] J.BURTON, « Cyber Deterrence: A Comprehensive Approach? », C.C.D.C.O.E, avril 2018.

[148] Le Monde Diplomatique, *Qualifier les armes*, disponible en ligne : « https://www.monde-diplomatique.fr/2018/03/A/58476 ». Consulté le 14/08/2019.

songe à des canons de courte portée ou encore à des mines nucléaires. Ces armes sont également de nature dissuasive, mais ce n'est pas là leur premier objectif, qui reste la défense. Dès lors, l'emploi de ces armes est beaucoup plus probable en cas d'attaque[149], ce qui pourrait en réalité avoir un effet mélioratif sur leur potentiel de dissuasion. En effet, là où on imagine mal un État employer l'arme stratégique, arme suprême, on l'imagine mieux employer l'arme tactique, moins dévastatrice, mais tout de même hautement destructrice.

L'arme cybernétique que l'on envisage essentiellement comme de longue portée ne l'est pas nécessairement. Dans le cas de *Stuxnet*, l'arme cybernétique avait été déployée via un vecteur physique, une clé U.S.B. Dès lors, il est envisageable d'imaginer que les armes cybernétiques peuvent aussi se décliner en armes tactiques.

Au final, l'on peut conclure que les armes cybernétiques peuvent être tactiques ou stratégiques, en gardant à l'esprit, toutefois, que leur potentiel stratégique est limité par l'intérêt essentiel que représente l'anonymat de l'armement cybernétique.

Maintenant qu'il a été établi que l'arme cybernétique n'est ni totalement conventionnelle, ni totalement non-conventionnelle, qu'elle peut être stratégique comme tactique, il est nécessaire de déterminer comment le *jus in bello* entend réglementer l'accès à ces armes et leur développement.

[149] CIVIS, « À propos d'une classification des armements », dans *Politique étrangère*, n°3, 1962, p. 226.

II. L'acquisition et la mise au points des moyens et méthodes de combat cybernétiques

Le *jus in bello* impose certaines règles dans le cadre de l'évolution des moyens et méthodes de combat. Ces obligations émanent essentiellement des conventions de Genève et de leur premier protocole additionnel. Il sera question de déterminer si ces règles s'appliquent au cas du moyen ou de la méthode de combat cybernétiques.

A. L'acquisition de nouveaux moyens ou méthodes de combat cybernétiques

L'obligation pour les États de s'assurer qu'une nouvelle arme acquise respecte les obligations du *jus in bello* provient de l'article 1 commun aux quatre conventions de Genève[150] et de l'article 1 de la Convention de La Haye de 1907[151]. Ces articles instaurent un devoir général de respect du *jus in bello*[152]. Ce devoir à valeur coutumière[153].

Les experts chargés de la rédaction de la nouvelle mouture du Manuel de Tallinn ont développé une position intéressante sur le rapport entre cette obligation et le cas des armes cybernétiques[154]. Ils se sont demandés comment devait se manifester le contrôle exercer par l'État sur la licéité de l'arme et ont conclu majoritairement que cette obligation était satisfaite pour autant

---

[150] Article 1 commun, Conventions de Genève, Genève, 12 aout 1949.

[151] Article 1, Convention de La Haye concernant les lois et coutumes de la guerre sur terre, La Haye, 18 octobre 1907.

[152] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 110, para. 2.

[153] *Ibid*.

[154] M.N. SCHITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, règle 110-a.

que l'État ait pris des mesures positives pour s'assurer de la licéité de l'arme cybernétique considérée[155]. Ils se sont ensuite posés la question de savoir si cette obligation s'étendait également aux méthodes de combat cybernétiques, sans atteindre de consensus[156]. Dans le cyberespace, méthode et moyen de combat semblent intimement connectés, ce qui pourrait pousser à adopter la position d'une partie des experts qui considère que ce contrôle doit s'étendre aux méthodes.

D'autres obligations, plus larges, sont envisagées pour les États partie au Protocole Additionnel I.

B. La mise au point et le développement de nouveaux moyens ou méthodes de combat cybernétiques

Cette obligation provient de l'article 36 du Protocole additionnel I aux conventions de Genève. Il dispose que « [d]*ans l'étude, la mise au point, l'acquisition ou l'adoption d'une nouvelle arme, de nouveaux moyens ou d'une nouvelle méthode de guerre, une Haute Partie contractante à l'obligation de déterminer si l'emploi en serait interdit, dans certaines circonstances ou en toutes circonstances, par les dispositions du présent Protocole ou par toute autre règle du droit international applicable à cette Haute Partie contractante* »[157].

Les experts chargés de la rédaction de la seconde version du Manuel de Tallinn se sont d'abord penchés sur la question de la portée coutumière de cette règle. Ils ont considéré qu'elle

[155] *Ibid*, para. 4.

[156] *Ibid*, para. 5.

[157] Article 36, Protocole additionnel aux Convention de Genève relatif à la protection des victimes des conflits armés internationaux, Genève, 8 juin 1977.

n'avait pas valeur coutumière[158]. Le Protocole Additionnel I comporte 174 États parties. Ce grand nombre de ratifications pourrait permettre de préjuger du caractère coutumier des règles qu'il contient. Pourtant, le Comité international de la Croix-Rouge ne semble pas considérer que la règle 36 dudit Protocole ait une portée coutumière[159]. Nous partirons donc du même postulat que le groupe d'experts.

Ainsi, les États parties au Protocole Additionnel I sont tenus d'effectuer une analyse des moyens et méthodes cybernétiques qu'ils acquièrent. Ils doivent également s'assurer aux phases d'étude, de mise au point et de développement de ces moyens et méthodes que ceux-ci respectent les dispositions du *jus in bello* et même du droit international pris *lato sensu*.

C. La conduite de l'examen de licéité des moyens et méthodes de combat cybernétiques

La conduite de l'examen de licéité des moyens et méthodes de combat cybernétiques comporte des similitudes entre les deux groupes d'obligations.

Dans les deux cas, l'État acquéreur n'est pas dégagé de son obligation de contrôle pour seule raison que l'État vendeur aurait déjà effectué un contrôle[160]. L'État acquéreur peut prendre en compte l'examen déjà effectué par l'État vendeur, mais il ne peut pas se passer d'effectuer lui même un contrôle.

---

[158] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 110, para. 2.

[159] Comité International de la Croix-Rouge, *Étude sur le droit international coutumier*, vol. 1, annexe « Liste des règles coutumières du droit international humanitaire », 2005.

[160] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017, règle 110, para. 8.

Selon les experts, la détermination de la légalité du moyen ou de la méthode de combat cybernétique doit être effectuée par référence à l'effet normal attendu dans le cadre de son emploi[161]. Tout changement significatif dans la nature du moyen ou de la méthode - par exemple, un changement majeur dans le code d'un *malware* qui serait susceptible de le rendre plus instable bien que plus efficace - doit entrainer un nouvel examen[162]. De manière plus précise, l'examen d'un nouveau moyen ou d'une nouvelle méthode de combat cybernétiques devrait s'attarder sur plusieurs questions. Notamment, ce nouveau système, dans son usage normal, est-il de nature à causer des maux et des souffrances superflus ? Respecte-t-il le principe de distinction ?

Les experts sont de l'avis que la conduite de cet examen pourrait s'avérer délicate, par exemple en raison de la difficulté de reproduire à l'identique le système cible pour prévoir par des essais les conséquences de l'emploi d'une nouvelle arme cyber. Cependant, ces difficultés ne dégagent pas les États de leurs obligations[163]

Maintenant que la place des moyens et méthodes de cybernétiques dans le cadre du *jus in bello* a été établie et que les obligations qui en découlent concernant l'acquisition et le développement de nouvelles armes ont été exposées, il est temps de s'attarder sur l'application concrète du *jus in bello* à l'emploi de ces mêmes moyens et méthodes de combat.

---

[161] *Ibid,* para. 9.

[162] *Ibid.*

[163] *Ibid,* para. 13.

- **Chapitre II - L'application du *jus in bello* à l'emploi de moyens et méthodes de combat cybernétiques**

La place des moyens et méthodes de combat cybernétiques dans les conflits armés est grandissante et pose de nombreuses questions quant à l'application *in concreto* du *jus in bello*. D'abord, il est important de déterminer en quoi les opérations de qualifications classiques sont influencées par ce nouveau type de moyens et méthodes (I). Ensuite, il sera question d'aborder l'articulation entre les règles essentielles de conduite des hostilités et l'emploi de moyens et méthodes de combat cybernétiques (II).

I. Les opérations de qualifications

Les opérations de qualifications sont nombreuses et centrales dans l'application du *jus in bello*. La primo-qualification est celle de conflit armé (A). Ensuite viennent des qualifications opérationnelles (B).

A. La qualification du conflit

Le *jus in bello* a pour vocation de ne s'appliquer qu'en cas de conflit armé, situation qui doit être distinguée de celles des troubles et tensions intérieurs. Cette exigence s'impose naturellement à l'emploi de moyens et méthodes de combat cybernétiques. Nous verrons successivement l'influence de l'emploi de ces nouveaux systèmes sur la caractérisation d'un conflit armé international puis sur celle d'un conflit armé non international.

1. Un conflit armé international

Les conflits armés internationaux sont notamment régis par les quatre Conventions de Genève et leur premier protocole additionnel. L'article 2 commun aux conventions dispose qu'elles s'appliquent « *en cas de guerre déclarée ou de tout autre conflit armé surgissant entre deux ou plusieurs des Hautes Parties contractantes, même si l'état de guerre n'est pas reconnu par l'une d'elles* »[164]. Le conflit armé international s'entend donc d'abord d'un confit armé qui oppose au moins deux entités étatiques. L'affrontement se fait par le biais de leurs armées ou bien par celui de plusieurs groupements armés sur lesquels les États exercent un contrôle global[165]. Enfin, certains conflits armés non internationaux peuvent s'internationaliser par l'effet de l'intervention directe ou indirecte d'un État tiers ou d'une organisation internationale[166]. Lorsqu'un conflit armé international est caractérisé au vu de l'emploi de moyens et méthodes de combat cinétiques, l'application subséquente du *jus in bello* aux opérations cybernétiques qui seraient entreprises dans le cadre de ce conflit s'opère *de facto*. La question réside plutôt sur la situation où aucune opération cinétique n'est entreprise. En d'autres termes, un conflit armé international peut-il être caractérisé lorsque seule la force cybernétique est employée ?

D'après Cordula Droege, cette possibilité dépend de deux éléments. D'une part, l'attaque doit pouvoir être attribuée à un État, d'autre part, elle doit constituer un recours à la force armée[167].

---

[164] Article 2 commun, Conventions de Genève, Genève, 12 octobre 1949. Le Protocole Additionnel renvoie à cet article, v. : Article 1 paragraphe 3, Protocole Additionnel I, Genève, 8 juin 1977.

[165] Tribunal pénal international pour l'ex-Yougoslavie, *Affaire Tadic*, arrêt du 15 juillet 1999, para. 137.

[166] J.D'ASPREMONT et J. DE HEMPTINNE, *Droit international humanitaire*, Pedone, octobre 2012 p. 77.

[167] C. DROEGE, « Sortez de mon « Cloud »: la cyberguerre, le droit international humanitaire et la protection des civils », dans *Revue internationale de la Croix-Rouge*, vol. 94, n°886, 2012, p. 412.

Cette position est reprise dans le Manuel de Tallinn[168]. Ces deux conditions sont délicates à mettre en oeuvre dans le cyberespace.

Concernant le critère d'attribution à un État, l'opacité du cyberespace vient une nouvelle fois entraver le processus d'attribution et donc de qualification de la situation en conflit armé international. Au surplus, dans l'hypothèse où l'État fait appel à un groupe non étatique pour opérer, la preuve du contrôle global de l'État sur ledit groupe est encore plus délicate à amener dans le cadre de l'emploi de moyens et méthodes de combat cybernétiques. L'une des solution serait de faire appel à la présomption juridique[169] que nous avions déjà évoquée dans le cadre de l'application du *jus ad bellum*. Pour les mêmes raisons qu'exposées précédemment, ce mode de fonctionnement semble totalement incompatible avec les spécificités du cyberespace et de la force cybernétiques.

Concernant la notion de recours à la force armée, il est d'abord nécessaire de différencier le concept d'agression armée déjà étudiée dans le cadre de la partie relative au *jus ad bellum*, et le recours à la force armée tel qu'on l'entend dans le *jus in bello*. Dans le cadre du *jus ad bellum*, la qualification en agression armée s'effectue essentiellement pour déterminer s'il est légitime de recourir à la force face à une cyberopération donnée[170] . Pour le *jus in bello*, il s'agit de déterminer le cadre dans lequel les hostilités devront être menées. Toutefois, il n'existe aucune définition conventionnelle de la force armée. Pour déterminer si l'opération cybernétique concerné constitue un recours à la force armée, plusieurs approches sont possibles. Le critère le plus évident est celui

---

[168] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber operations* », Cambridge University Press, 2 février 2017, règle 82, paras. 1-10 et 11-17.

[169] C. DROEGE, « Sortez de mon « Cloud »: la cyberguerre, le droit international humanitaire et la protection des civils », dans *Revue internationale de la Croix-Rouge*, vol. 94, n°886, 2012, p. 413.

[170] H.S.LIN, « Offensive Cyber Operations and the Use of Force », dans *Journal of National Security Law and Policy*, vol. 4, 2010, p. 63.

des effets analogues à une opération cinétique qui constituerait elle-même un recours à la force armée[171]. Cette approche se limite toutefois aux cyberopérations les plus agressives, l'essentiel de ces dernières ayant surtout des répercussions directement dans le cyberespace. Dans ce cas, une approche plus générale des effets peut être envisagée, dépassant le seul cadre des effets analogues à l'opération cinétique. Une autre approche serait de considérer « *toute cyberopération hostile portant atteinte au fonctionnement de biens comme un recours à la force armée* »[172]. Enfin, une dernière approche serait de considérer non seulement les effets de l'opération, mais l'ensemble des facteurs caractéristiques de l'opération qui inciteraient à la qualifier de recours à la force armée : la sévérité des conséquences, les moyens employés, le caractère militaire, la nature de la cible[173]. Les experts en charge de la rédaction du Manuel de Tallinn reprennent ces critères[174].

Partant, il est admis qu'un conflit armé international puisse être qualifié lorsqu'une cyberopération atteint le seuil de recours à la force armée et qu'elle est attribuable à un État. Le critère du recours à la force armée ne pose pas vraiment problème. La troisième approche proposée par Cordula Droege semble permettre de manière satisfaisante d'appliquer ce critère au cas cybernétique. Le problème essentiel est de nouveau posé par la nécessité d'attribuer l'opération à un État et, à l'heure actuelle, il est difficile d'envisager une solution pleinement satisfaisante.

---

[171] H.H.DINNISS, *Cyber warfare and the laws of war*, Cambridge University Press, 2012, p. 131.

[172] C. DROEGE, « Sortez de mon « Cloud »: la cyberguerre, le droit international humanitaire et la protection des civils », dans *Revue internationale de la Croix-Rouge*, vol. 94, n°886, 2012, p. 417.

[173] *Ibid*, p. 418.

[174] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber operations* », Cambridge University Press, 2 février 2017, règle 82, paras. 14-17.

Toutefois, dans le cas où les deux critères sont remplis, rien ne s'oppose à la qualification d'un conflit armé international[175].

Nous allons maintenant voir si certaines cyberopérations offensives peuvent amener à qualifier une situation de conflit armé non international.

2. Un conflit armé non international

Dans le cadre de l'étude de l'application du *jus ad bellum* aux moyens et méthodes de combat cybernétiques, nous avons évoqué le fait que la force cybernétique et les cyberattaques sont le monopole des États[176]. Cette position n'est pas incompatible avec le fait que, dans le cadre d'un conflit armé non international, un groupe armé puisse recourir à la force cybernétique : elles poursuivent des objectifs différents.

Les conflits armés non internationaux sont traités par l'article 3 commun aux Convention de Genève[177]. Cet article constitue une base conventionnelle minimale à l'encadrement des conflits armés non internationaux. Cette base est complétée par le deuxième protocole additionnel aux conventions de Genève qui a pour but de développer et de compléter l'article 3[178]. Les conflits armés non internationaux peuvent opposer un État à un groupe armé ou des groupes armés entre eux

---

[175] À titre d'exemple, on peut évoquer le cas de *Stuxnet*. *Stuxnet* est une cyberopération autonome qui a été déployée contre l'Iran sans opération cinétique concomitante. Elle avait pour objectif d'empêcher le fonctionnement de certaines centrales iraniennes en causant des dommages physiques aux installations. Cet objectif a été rempli et cette opération s'élève donc au rang de recours à la force armée. S'il avait été possible d'attribuer l'opération à un État de manière certaine, on aurait pu considérer que l'opération *Stuxnet* constituait le commencement d'un conflit armé international.

[176] Qu'ils agissent par eux même ou par le biais d'un groupe non étatique.

[177] Article 3 commun, Conventions de Genève, Genève, 12 aout 1949.

[178] Protocole additionnel aux conventions de Genève (Protocole II), Genève, 8 juin 1977.

sur le territoire d'un État. Il existe deux catégories de conflits armés non internationaux : ceux de basse intensité et ceux de haute intensité. Les conflits armés de basse intensité sont concernés uniquement par l'article 3 commun aux convention de Genève là où les conflits armés de haute intensité mettent en jeu l'application de l'article 3 et du protocole. Encore une fois, on peut aisément envisager un confit armé non international traditionnel au cours duquel le groupe armé fait usage de la force cybernétique. La question est davantage de savoir si les actions purement et uniquement cybernétiques d'un groupe non étatique peuvent amener à une qualification de conflit armé non international.

Pour être qualifiée de conflit armé non international, une situation doit montrer un affrontement armé d'une certaine intensité et un degrés d'organisation minimum pour les parties au conflit[179].

Le Tribunal pénal international pour l'ex-Yougoslavie a été amené à se poser la question des indices attestant du degrés d'organisation d'un groupe armé. Il a notamment été fait référence à l'existence d'une véritable chaine de commandement et à la capacité de planifier et de mener des opérations d'une certaine envergure et la capacité à les mener de concert[180]. Le degrés d'organisation du groupe doit être suffisant pour qu'il ait la « *capacité de faire respecter les obligations fondamentales découlant du droit international humanitaire* »[181]. Les groupes visés traditionnellement par le *jus in bello* et par la justice pénale internationale sont des groupes

[179] Tribunal pénal international pour l'ex-Yougoslavie, *Le procureur contre Dusko Tadić,* Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, 2 octobre 1995, para. 70.

[180] Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur contre Boskoski*, 10 juillet 2008, paras. 199-203. V. aussi : Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur contre Limaj*, 30 novembre 2005, paras. 90-134 ; Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur contre Haradinaj*, 3 avril 2008, para. 60.

[181] C. DROEGE, « Sortez de mon « Cloud »: la cyberguerre, le droit international humanitaire et la protection des civils », dans *Revue internationale de la Croix-Rouge*, vol. 94, n°886, 2012, p. 421.

« physiques », qui ont un rattachement évident à l'espace tangible : des bases, des troupes armées traditionnelles et des activités militaires cinétiques. La question est alors de savoir si un groupe non étatique totalement « immatériel » peut constituer un groupe armé organisé au sens de la jurisprudence citée et du *jus bello*. D'un point de vue opérationnel, on peut très bien imaginer un groupe dont l'organisation virtuelle satisfait à certains critères dégagés par la pratique : on peut imaginer un groupe structuré et organisé autour d'une hiérarchie formelle - bien que virtuelle - avec une division des tâches et un haut degré de coordination dans les actions qu'il entreprendrait[182]. Dans ce cadre, le fait que les individus ne soient pas réunis physiquement, voire même le fait qu'ils ne se soient jamais rencontrés et ne connaissent par leur identité respective n'est pas un frein à la qualification de conflit armé non international[183]. En revanche, la nécessité de pouvoir imposer les règles du *jus in bello* aux membres du groupe semble être le critère d'achoppement pour permettre une telle qualification en pareille situation[184]. On semble en effet considérer que la mise en place d'un cadre disciplinaire qui permettrait d'imposer le respect de ces règles n'est pas réaliste dans le cadre d'un groupe purement virtuel. En effet, la capacité d'une chaine de commandement virtuelle à sanctionner de manière efficace un membre qui se serait rendu coupable d'une violation du *jus in bello* semble relativement limitée par le choix des possibilités. On peut imaginer différents types de sanctions, comme la mise hors de service de l'unité informatique du membre du groupe, mais ces mesures sembles insuffisantes. À ce niveau, la nécessité de pouvoir contraindre physiquement semble toujours importante.

---

[182] Par exemple, on peut imaginer un groupe de *hackers* qui serait structuré en différents groupes opérationnels tous soumis aux ordres d'une chaine de commandement supérieure et qui aurait la capacité d'opérer de concert contre un État.

[183] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber operations* », Cambridge University Press, 2 février 2017, règle 83, para. 13.

[184] *Ibid*, para. 14. V. aussi C. DROEGE, « Sortez de mon « Cloud »: la cyberguerre, le droit international humanitaire et la protection des civils », dans *Revue internationale de la Croix-Rouge*, vol. 94, n°886, 2012, p. 421.

Concernant le critère d'intensité, on peut de nouveau citer la jurisprudence du Tribunal pénal international pour l'ex-Yougoslavie. Différents indices ont été dégagés : le recours à la force militaire plutôt qu'a la force de police, la gravité et la multiplicité des affrontements, le nombre de victimes, les moyens mis en oeuvre dans la conduite des opérations, l'ampleur des destructions sont notamment des critères significatifs permettant d'établir si l'intensité du conflit à atteint le seuil requis pour une qualification de conflit armé non international[185]. Cordula Droege considère que la nature des cyberopérations exclut l'appréciation de certains de ces critères, comme ceux d'affrontements armés, de déploiement de la force militaire ou de l'utilisation d'armes lourdes[186]. Partant, elle considère que ce sont les « *conséquences des cyberopérations à elles seules qui seraient assez graves pour atteindre le degré d'intensité requis* »[187]. Cette position n'empêche pas de considérer que l'intensité requise pour une qualification de conflit armé non international soit atteinte, mais elle demeure réductrice. L'affrontement armé entre cybercombattants existe, même s'il est immatériel. Le déploiement de la force militaire cybernétique ne s'effectue certes pas dans le plan physique, mais il existe bien dans l'environnement cybernétique. Enfin, il est bel et bien envisageable de considérer certaines armes cybernétiques comme des armes lourdes, en contraste avec d'autres armes cybernétiques au potentiel destructeur moins marqué.

In fine, les deux critères retenus pour attester de l'existence d'un conflit armé non international sur le fondement des seules cyberopérations semblent pouvoir être remplis en certaines situations. Le critère de l'organisation semble poser plus de difficultés que celui de l'intensité mais, le cas échéant, un groupe non étatique suffisamment organisé pour remplir ce critère et qui opère

---

[185] Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur contre Boskoski*, 10 juillet 2008, paras. 177-178. V. aussi : Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur contre Limaj*, 30 novembre 2005, paras. 135-170 ; Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur contre Haradinaj*, 3 avril 2008, para. 49.

[186] C. DROEGE, « Sortez de mon « Cloud »: la cyberguerre, le droit international humanitaire et la protection des civils », dans *Revue internationale de la Croix-Rouge*, vol. 94, n°886, 2012, p. 422.

[187] *Ibid*.

d'une manière suffisamment régulière et violente pour remplir celui de l'intensité pourrait amener à une qualification de conflit armé non international.

Bien que la pratique ne montre actuellement aucun exemple validant ces deux hypothèses, l'application des critères de qualification classiques aux seules cyberopérations ne semble pas exclure la possibilité de qualifier une situation de conflit armé - international ou non international. Toutefois, la même difficulté récurrente semble venir assombrir cette possibilité : les difficultés d'attribution rendent très improbable de valider l'hypothèse d'un conflit armé qualifié sur la simple base de cyberopérations.

Après avoir déterminé qu'il était possible mais hautement hypothétique de pouvoir qualifier une situation de conflit armé sur la base de simples cyberopérations, nous allons nous intéresser à d'autres opérations de qualifications.

B. Les qualifications opérationnelles

Une fois que l'existence d'un conflit armé est admise, le *jus in bello* impose différentes qualifications opérationnelles nécessaire à la poursuite de ses objectifs. Il sera essentiellement question de déterminer comment s'organisent l'emploi des moyens et méthodes de combat cybernétiques et les qualifications d'attaque et de participation directe aux hostilités.

1. L'attaque

Il sera question de déterminer ici en quoi les cyberopérations peuvent s'apparenter à des attaques telles qu'elles sont entendues dans le *jus in bello*.

La notion d'attaque est centrale dans les conventions régissant le *jus in bello* et plus précisément la conduite des hostilités. On retrouve cette notion pour de nombreuses règles contenues dans ces conventions : interdiction des attaques visant des civils[188] ou des biens de nature civile[189], l'interdiction des attaques indiscriminées[190], l'interdiction d'attaquer certaines personnes et biens comme les unités sanitaires[191] ou les personnes hors de combat[192]. L'article 49 du Protocole I donne des premiers éléments de définition de l'attaque : « [l]'*expression «* attaques » *s'entend des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs* ». La notion de violence, dans l'esprit des conventions, renvoie d'abord à la violence physique. Dès lors, on peut se demander à partir de quel stade une cyberopération peut être qualifiée d'attaque.

D'abord, on peut noter qu'il est admis que la violence, si elle a d'abord été pensée d'un point de vue cinétique, ne se restreint pas à ce seul aspect. En effet, des opérations faisant usage

[188] Article 51, para. 2, Protocole additionnel aux Conventions de Genève (Protocole I), Genève, 1977.

[189] *Ibid*, art. 52, para. 1.

[190] *Ibid*, art. 51, para. 4.

[191] *Ibid*, art. 12, para. 1.

[192] *Ibid*, art. 41, para. 1.

d'arme chimique, biologique ou radiologique s'élèveraient toutes au rang d'attaque[193]. Rien ne s'oppose donc à ce qu'une opération cybernétique soit qualifiée d'attaque.

Ensuite, c'est l'étude des effets de la cyberopération qui va permettre de déterminer si elle constitue une attaque au sens du *jus in bello*. On distingue deux positions contraires sur cette question. La première est celle de Michael Schmitt qui considère « *qu'une cyberopération, comme toute autre opération, est une attaque lorsqu'elle provoque la mort ou blesse des individus, que ceux-ci soient des civils ou des combattants, ou lorsque elle endommage ou détruit des biens, qu'ils soient militaires ou civils* »[194]. Dans ce cadre, les dommages sont entendus d'un point de vue physique : la mort, les blessures, les dommages et la destruction renvoient tous, *a priori*, à une dimension physique. Pour Knut Dörmann, une opération cybernétique pourrait atteindre le seuil d'attaque dans le sens du *jus in bello* lorsqu'elle a des conséquences physiques « violentes » mais également dans le cadre de la simple neutralisation d'un objectif militaire, sans forcément que des dommages physiques soient constatés[195]. Il base ce raisonnement sur l'article 52 du Protocole I qui dispose que : « [l]*es attaques doivent être strictement limitées aux objectifs militaires*. *En ce qui concerne les biens, les objectifs militaires sont limités aux biens qui, par leur nature, leur emplacement, leur destination ou leur utilisation apportent une contribution effective à l'action militaire et dont la destruction totale ou partielle, la capture ou la neutralisation offre en l'occurrence un avantage militaire précis* »[196]. On peut extraire de cet article que l'*attaque* peut

---

[193] N.MELZER, « Les cyber-opérations et le *jus in bello* », dans *Forum du désarmement : faire face aux cyberconflits*, Rapport UNIDIR, 2011, p. 7. V. aussi : Y.DINSTEIN, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, 2004, p. 84 ; M.N.SCHMITT, « Cyber Operations and the *Jus in bello:* Key issues », dans *Naval War College International Law Studies*, vol. 87, 2011, p. 5 ; M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2 février 2017, règle 92, para. 3.

[194] M.N.Schmitt, « Cyber Operations and the *Jus in bello:* Key issues », dans *Naval War College International Law Studies*, vol. 87, 2011, p. 6, traduction.

[195] K.DÖRMANN, « Applicability of the Additional Protocols to Computer Network Attacks », CICR, 2004, p. 4.

[196] Article 52 paragraphe 2, Protocole I, Genève, 1977.

constituer une opération qui *neutralise* ou *capture* l'objectif militaire. Partant, on pourrait très bien considérer qu'une cyberopération qui neutralise un bien, sans pour autant le détruire ni le dégrader physiquement, constitue une attaque au sens du *jus in bello*. Le Manuel de Tallinn retient naturellement la première position mais la nuance. Dans la règle 92 relative à une définition de la cyberattaque, certains experts ont pu considérer que des dommages immatériels entrainant l'obligation de réinstaller le système ou des données particulières pour refaire fonctionner l'infrastructure cyber étaient suffisants pour caractériser une attaque[197]. En ce sens, les positions du Comité international de la Croix-Rouge et celles du groupe d'experts mandaté par l'Organisation du traité de l'atlantique nord semblent se rapprocher.

Il semble donc tout à fait crédible d'envisager que certaines cyberopérations atteignent le seuil de cyberattaque au sens du *jus in bello*. Cela s'explique d'abord par le fait que rien ne semble empêcher en soit qu'une telle qualification soit faite. Ensuite, que l'on adopte l'une ou l'autre des positions exposées *supra*, il semble que certaines cyberopérations aient le potentiel d'être assimilées à des attaques. L'une comme l'autre de ces approches présente des avantages et des inconvénients, et, en ce sens, un compromis entre elles s'avérerait être la meilleure solution.

Une fois la qualification d'attaque analysée, il sera question d'appréhender la notion de participation directe aux hostilités ramenée au contexte cybernétique.

[197] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2 février 2017, règle 92, para. 11.

2. La participation directe aux hostilités

La notion de participation directe aux hostilités n'est pas définie dans les conventions régissant le *jus in bello*. Cette notion apparait pourtant dans l'article 3 paragraphe 1 commun aux Conventions de Genève, à l'article 51 paragraphe 3 du Protocole additionnel I et à l'article 4 paragraphe 1 du Protocole additionnel II. Le Comité international de la Croix-Rouge, conscient de cette carence, propose un *Guide interprétatif sur la notion de participation directe aux hostilités*[198] qui servira de base aux réflexions suivantes.

Pour Melzer, la notion d' « hostilités » fait référence à des situations de conflit armé international ou non international[199]. Les hostilités telles qu'on les entend ici ne peuvent avoir lieu que dans le cadre d'un conflit armé. Les hostilités n'englobent pas nécessairement tous les comportements d'une partie à un conflit[200]. Elles désignent donc « *l'ensemble des actes hostiles réalisés par des personnes directement impliquées dans ces actes* »[201]. La « participation » renvoie quant à elle à « *l'implication individuelle d'une personne dans ces hostilités* »[202]. Cette participation directe aux hostilités peut être du fait d'une personne civile comme d'un militaire : elle s'attache au comportement et non pas à la qualité du participant. Melzer dégage trois critères cumulatifs permettant de conclure qu'un acte spécifique relève de la participation directe aux hostilités. L'acte

---

[198] N.MELZER, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, Comité international de la Croix-Rouge, 2009.

[199] V. par exemple : Voir titre et article 1 Convention III de La Haye; titre de la section II H IV R; article 3 [1] CG I-IV; article 17 CG I; article 33 CG II; titre de la section II et articles 21 [3], 67, 118, 119 CG III; articles 49 [2], 130, 133, 134, 135 CG IV; articles 33, 34, 40, 43 [2], 45, 47,51 [3], 59, 60 PA I et titre du Titre IV, Section I PA I; articles 4 et 13 [3] PA II; articles 3 [1] – [3] et 4 Protocole relatif aux restes explosifs de guerre.

[200] N.MELZER, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, Comité international de la Croix-Rouge, 2009, p. 43.

[201] N.MELZER, « Les cyber-opérations et le *jus in bello* », dans *Forum du désarmement : faire face aux cyberconflits*, Rapport UNIDIR, 2011, p. 8.

[202] N.MELZER, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, Comité international de la Croix-Rouge, 2009, p. 45.

envisagé doit atteindre un certain seuil de nuisance[203], il doit y avoir un lien direct entre l'acte commis et les nuisances envisagées[204] et ces actes nuisibles doivent avoir été commis à l'avantage d'une partie et au détriment d'une autre[205]. Il est important de noter que les civils participants directement aux hostilités perdent le bénéfice de leur protection pour autant que dure leur participation. La durée de cette participation s'étend aux mesures préparatoires, au déploiement vers le lieu d'exécution, à la durée de l'exécution et au retour de ce lieu[206].

Dans le cadre de l'emploi de moyens et méthodes de combat cybernétiques, la question de la participation directe aux hostilités soulève certaines interrogations. Dans un premier temps, il convient de préciser que les trois critères dégagés par Melzer s'appliquent de fait aux opérations cybernétiques. Ensuite, il convient de déterminer en quels cas une opération cybernétique peut atteindre le seuil de nuisance invoqué. Selon Melzer toujours, les hostilités englobent ici non seulement les cyberopérations de nature à causer destruction et pertes de vies civiles, mais également les cyberopérations hautement perturbatrices qui empêcheraient une autre partie au conflit de mener les hostilités[207]. À l'inverse, les cyberopérations qui ne causent pas de tels dommages et n'ont pas pour effet de perturber la capacité d'une partie de conduire les hostilités, ne relèvent pas de la participation directe aux hostilités[208]. Les personnes qui peuvent participer

---

[203] *Ibid*, pp. 49-53, « *Pour atteindre le seuil de nuisance requis, un acte spécifique doit être susceptible de nuire aux opérations militaires ou à la capacité militaire d'une partie à un conflit armé, ou alors l'acte doit être de nature à causer des pertes en vies humaines, des blessures et des destructions à des personnes ou à des biens protégés contre les attaques directes* ».

[204] *Ibid*, pp. 53-60, « *Pour que l'exigence de causation directe soit satisfaite, il doit exister une relation directe de causalité entre un spécifique et les effets nuisibles susceptibles de résulter soit de cet acte, soit d'une opération militaire coordonnée dont cet acte fait partie intégrante* ».

[205] *Ibid*, pp. 60-67, « *Afin de satisfaire à l'exigence du lien de belligérance, un acte doit être spécifiquement destiné à causer directement des effets nuisibles atteignant le seuil requis, à l'avantage d'une partie au conflit et au détriment d'une autre* ».

[206] *Ibid*, p. 68.

[207] N.MELZER, « Les cyber-opérations et le *jus in bello* », dans *Forum du désarmement : faire face aux cyberconflits*, Rapport UNIDIR, 2011, pp. 8-9.

[208] *Ibid*.

directement aux hostilités dans le cadre d'une cyberopération sont les mêmes que pour une opération classique : les combattants[209], les membres de levées en masses[210], les mercenaires[211] et les civils[212]. Les combattants et les membres d'une levée en masse bénéficient des statuts de combattant et de prisonnier de guerre - le cas échéant. Les mercenaires ne bénéficient pas de ces statuts. Les civils, lorsqu'ils participent directement à une cyberopération constitutive d'« hostilités », perdent leur protection spéciale pour autant que cette participation dure.

Les opérations de qualifications les plus importantes ayant été traitées, nous nous pencherons désormais sur l'articulation entre l'emploi de moyens et méthodes de combat cybernétiques et certains principes de la conduite des hostilités.

---

[209] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2 février 2017, règle 87.

[210] *Ibid*, règle 88.

[211] *Ibid*, règle 90.

[212] *Ibid*, règle 91.

II. La conduite des hostilités

Dans la conduite des hostilités, le *jus in bello* s'articule autour de différents principes. Le principe de distinction (A), le principe de proportionnalité (B) et le principe de précaution (C) nous intéressent particulièrement. L'application de chacun de ces principes à l'emploi de moyens et méthodes de combat cybernétiques soulève certaines questions.

A. Le principe de distinction

Le principe de distinction impose aux parties à un confit armé de faire « *en tout temps* […] *la distinction entre la population civile et les combattants ainsi qu'entre les biens de caractère civil et les objectifs militaires et, par conséquent, ne diriger leurs opérations que contre des objectifs militaires* »[213]. Il sera donc question d'étudier l'articulation de ce principe à l'usage de moyens et méthodes de combat cybernétiques et d'évoquer de manière subséquente l'élargissement de ce principe à certains biens et personnes.

1. La distinction entre objectif militaire et personnes et biens civils

Le principe de distinction présuppose de pouvoir effectuer un distinguo entre les objectifs militaires et les personnes et biens civils[214]. Ce postulat prévaut également dans le cadre de l'emploi de moyens et méthodes de combat cybernétiques, mais il se heurte à l'écueil du double usage particulièrement présent en matière cybernétique.

---

[213] Article 48, Protocole I, Genève, 1977.

[214] Cette obligation est largement reprise dans le Manuel de Tallinn 2.0. V. : M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2 février 2017, règles 94, 99, 111 et 112.

a. L'obligation de cibler des objectifs militaires

Dans le cadre d'un conflit armé, les parties au conflit sont obligées de cibler des objectifs militaires. Ramenée au cadre cybernétique, nous tenterons de définir ce qui représente un objectif militaire.

Le *jus in bello* coutumier considère que les objectifs militaires sont des bien qui « *par leur nature, leur emplacement, leur destination ou leur utilisation apportent une contribution effective à l'action militaire et dont la destruction totale ou partielle, la capture ou la neutralisation offre en l'occurrence un avantage militaire précis* »[215]. Une cyberopération offensive peut être conduite contre tout bien qui remplit ces conditions. Déterminer ce qui représenterait un objectif militaire cybernétique ne soulève pas beaucoup plus de questions : tout bien cybernétique, peu importe dans quelle couche du cyberespace il se trouve, représente un objectif militaire valable pour autant qu'il remplisse les conditions posées par la règle citée.

Toutefois, une controverse semble persister sur la question du degré de violence qui doit être atteint pour violer ce principe. Selon Michael Schmitt, l'interdiction vise les « attaques » contre les personnes ou biens civils. Dès lors, il considère que les cyberopérations qui n'atteignent pas le seuil d'attaque au sens du *jus in bello* et qui ciblent des personnes ou des biens civils ne violent pas le principe de distinction[216]. Pour d'autres, le principe de distinction ne s'applique pas seulement aux cyberopérations atteignant le seuil d'attaque, mais à toutes les cyberopérations qui atteignent celui

---

[215] Comité International de la Croix-Rouge, *Étude sur le droit international coutumier*, vol. 1, annexe « Liste des règles coutumières du droit international humanitaire », 2005, règle 8.

[216] M.N.SCHMITT, « Wired warfare : Computer network attack and *jus in bello* », dans *Revue internationale de la Croix-Rouge*, no°846, 2002, p. 376.

des « hostilités »[217]. Cette seconde position semble être la plus à même de « *préserver la raison d'être du principe* »[218]

Après avoir déterminé comment s'appliquait l'interdiction de mener des cyberopérations hostiles contre des civils ou des biens civils, nous évoquerons la question des « attaques indiscriminées » et de l'emploi de moyens et méthodes de combat cybernétiques.

b. L'interdiction des attaques indiscriminées et l'emploi de moyens et méthodes de combat cybernétiques

L'interdiction des attaques indiscriminées se heurte à une difficulté particulière dans le cadre de l'usage de moyens et méthodes de combat cybernétiques : celle du double usage. Une attaque indiscriminée est une attaque qui ne peut pas être dirigée contre un objectif militaire identifié ou une attaque dont les effets ne peuvent être limités[219]. Une cyberopération indiscriminée s'entend donc d'une cyberopération qui ne peut pas cibler précisément un objectif - notamment en raison du choix de l'arme ou de la méthode - ou d'une cyberopération dont les effets ne peuvent être limités.

Cette interdiction des attaques indiscriminées rapportée à la considération de l'emploi de moyens et méthodes de combat cybernétiques soulève un problème de premier ordre : celui de l'aspect dual militaro-civil du cyberespace. L'on sait que les objets civils sont les objets qui ne sont pas des objectifs militaires, et que tout objet s'il est civil à l'origine peut devenir un objectif militaire valable en fonction des conditions. Les biens à *double-usage* sont des biens qui sont à la

---

[217] N. MELZER, Cyberwarfare and International Law, UNIDIR, 2011, p. 27.

[218] K.BANNELIER-CHRISTAKIS, « Is the Principle of Distinction Still Relevent in Cyberwarfare? », dans *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 26 juin 2015, p. 14.

[219] J.D'ASPREMONT et J. DE HEMPTINNE, *Droit international humanitaire*, Pedone, octobre 2012 p. 301.

fois de nature civile et de nature militaire. En tant que tels, ils représentent des objectifs militaires valables[220]. Mais là où une usine chimique est un bien matériel tangible, identifiable et « indépendant », le cyberespace est un ensemble qui est presque entièrement *dual*. En effet, la frontière entre cyberespace civil et militaire demeure extrêmement fine, voire inexistante. Par exemple, les dorsales transnationales de fibre optique sont entièrement duales. *Internet* en tant que tel est également dual. Dès lors, on peut craindre que dans le cyberespace, les conséquences de ce principe de double usage soient telles que rien de civil ne subsisterait[221]. En l'état actuel des choses, le principe de distinction semble donc inopérant dans le domaine cybernétique en raison de la nature quasi intégralement duale du cyberespace.

En dehors du principe cardinal de distinction, certaines personnes, activités et biens disposent d'une protection particulière contre les attaques.

2. Les régimes de protection de certaines personnes, activités et biens

Le principe de distinction opère *ab initio* une différenciation entre ce qui est militaire et ce qui est civil. Cependant, certaines catégories de personnes et de biens bénéficient d'un statut particulier et, par extension, il est possible de considérer que ces catégories bénéficient d'une déclinaison spéciale du principe de distinction. Dès lors, il sera question d'analyser l'articulation entre ces régimes spéciaux de protection et l'emploi de moyens et méthodes de combat cybernétiques.

---

[220] K.BANNELIER-CHRISTAKIS, « Is the Principle of Distinction Still Relevent in Cyberwarfare? », dans *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 26 juin 2015, p. 18.

[221] C. DROEGE, « Sortez de mon « Cloud »: la cyberguerre, le droit international humanitaire et la protection des civils », dans *Revue internationale de la Croix-Rouge*, vol. 94, n°886, 2012, p. 438.

a. La protection de certaines personnes et biens en raison de leur activité

Certaines catégories de personnes et de biens bénéficient d'une protection particulière en raison de l'activité à laquelle ils sont affectés. C'est notamment le cas du personnel sanitaire des armées. Nous verrons en quoi cette protection influence la conduite des hostilités d'un point de vue cybernétique.

Certaines catégories de personnes et de biens sont donc spécialement protégés par le *jus in bello* en raison de leur activité. Ce régime de protection peut être vu comme une dérivation spéciale du principe de distinction. Ainsi, on peut notamment souligner le cas du personnel, des unités et des biens sanitaires[222]. Ceux-ci ne doivent pas faire l'objet d'attaque pour autant qu'ils exercent leur rôle ou qu'ils sont effectivement affectés à cette activité. Cette protection, dans le cadre cybernétique, s'étend aux ordinateurs, aux réseaux et aux données affectées à l'activité concernée[223]. Le problème essentiel qui va se poser ici est celui de la haute interconnectivité des systèmes cybernétiques, notamment militaires. On peut imaginer une cyberopération qui viserait à dérégler le système de géolocalisation par satellite[224]. Une unité de véhicules blindés légers se déplace en se localisant via ce système : ils représentent un objectifs militaire valable. Dans le même temps, une unité sanitaire militaire qui utilise ce même système se rend en mission de récupérations des blessés. La cyberopération risque et va très certainement dérégler le système pour les deux unités. Ce faisant, la cyberopération va empêcher l'unité sanitaire de mener sa mission à bien, contrevenant ainsi au régime de protection.

---

[222] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2 février 2017, règle 131.

[223] *Ibid*, règle 131.

[224] *Global Positioning System* ou G.P.S.

En dehors de ces régimes de protections attachés à l'exercice de certaines activités, d'autres biens particuliers jouissent d'une spécifique particulière au titre de leur nature particulière.

b. La protection de certains biens en raison de leur nature

Certains biens sont considérés d'une manière particulière par le *jus in bello,* qui leur accorde un régime de protection particulier. C'est particulièrement le cas des biens contenant des forces dangereuses. Nous verrons en quoi cette protection influence la conduite des hostilités d'un point de vue cybernétique.

Les biens contenant des forces dangereuses sont définis comme « *les ouvrages d'art ou installations contenant des forces dangereuses, à savoir les barrages, les digues et les centrales nucléaires de production d'énergie électrique* »[225]. Ces biens ne peuvent pas être attaqués, quand bien même ils abriteraient un objectif militaire, pour autant que leur destruction peut provoquer la libération de forces dangereuses susceptibles de causer de grandes pertes civiles. Ce régime de protection cesse de s'appliquer lorsque ces biens confèrent à une partie un appui militaire important et direct à des opérations militaires. L'avantage du vecteur cybernétique vis-à-vis de ces structures et qu'il pourrait être employé pour les neutraliser, sans les détruire, limitant donc les risques de libération d'une force dangereuse - bien loin du fantasme pas si irréel d'un virus qui détruirait une centrale nucléaire. Le fait est que ces biens sont souvent à double usage. Les cibler a donc quasi systématiquement des conséquences pour les personnes civiles. Au surplus, peut-on envisager l'existence dans le cyberespace de bien contenant des forces dangereuses ? Peut-on imaginer un *cloud* interne de la N.S.A. qui contiendrait un arsenal d'armes cybernétiques à haut potentiel

[225] Article 56, Protocole I, Genève, 1977.

destructeur, et que ce *cloud* soit qualifié de bien renfermant des forces dangereuses ? *A priori*, rien ne semble indiquer que cela soit impossible.

Le phénomène des biens à double usage est en nette expansion, ce qui à pour conséquences d'affaiblir considérablement le principe de distinction et certains régimes de protections spéciaux. Le déploiement de plus en plus fréquent de la force dans le cyberespace n'est qu'un facteur d'accélération du phénomène. À ce jour, aucune solution viable ne semble être entreprise par les États pour y remédier. Une des solutions serait d'imposer une délimitation stricte des biens militaires et civils, en tous cas de certaines infrastructures, et d'étendre cette obligation au cyberespace. Cette solution serait toutefois si coûteuse qu'il est plus envisageable que les États s'en remettent au principe de proportionnalité.

B. Le principe de proportionnalité

Le principe de proportionnalité impose aux parties à un conflit armé de s'abstenir de lancer des attaques dont « *on peut attendre qu'elles causent incidemment des pertes en vies humaines dans la population civile, des blessures aux personnes civiles, des dommages aux biens de caractère civil, ou une combinaison de ces pertes et dommages, qui seraient excessifs par rapport à l'avantage militaire concret et direct attendu* »[226]. En raison de la nature hautement duale du cyberespace, l'importance du principe de proportionnalité dans la conduite d'hostilités dans le cyberespace est assez significative. Nous verrons comment ce principe s'applique à l'emploi de moyens et méthodes de combat cybernétiques et incidemment s'il peut s'appliquer efficacement.

[226] J.D'ASPREMONT et J. DE HEMPTINNE, *Droit international humanitaire*, Pedone, octobre 2012 p. 299.

1. Le principe de proportionnalité entre le moyen ou la méthode employé et l'objectif poursuivi

La cyberopération, comme toute opération entreprise dans le cadre d'un conflit armé, doit se soumettre à l'application du principe de proportionnalité.

Partant, toute cyberopération, dans le choix de l'objectif et du moyen ou de la méthode de combat envisagés, doit permettre d'éviter des dégâts ou des pertes civiles qui seraient manifestement superflues eu égard à l'avantage militaire dégagé. Ce principe n'interdit pas *per se* les dommages collatéraux. Ils doivent par contre êtres pris en considération, aussi bien à court terme qu'a long terme[227].

Le principe de proportionnalité est particulièrement important dans le cadre du cyberespace en raison de la nature hautement duale de ce dernier. Là où le principe de distinction semble s'effacer, le principe de proportionnalité est censé pallier ce problème en intimant aux parties à un conflit armé de s'assurer que leur opération n'est pas disproportionnée. Cependant, d'autres aspects techniques du cyberespace risquent de déséquilibrer l'application du principe.

2. Les spécificités des moyens et méthodes de combat cybernétiques, obstacle au principe de proportionnalité.

Ici, il va être question de se demander si la nature hautement duale du cyberespace représente ou non un frein à l'application du principe de proportionnalité.

[227] *Ibid.*

En soi, c'est plutôt le principe de proportionnalité qui représente un palliatif à la nature profondément duale du cyberespace. Dans la pratique, cette idée se heurte à certaines spécificités du cyberespace et des moyens et méthodes de combat cybernétiques.

D'abord, le cyberespace est par nature très interconnecté. Sans considération de sa nature duale militaro-civile, les systèmes cybernétiques sont de manière générale hautement connectés entre eux, même si l'on se place dans le cadre du réseau local. Ensuite, un certain nombre d'armes cybernétiques sont de nature à se propager. Ce cocktail pourrait remettre en question assez souvent l'application du principe de proportionnalité - on peut en effet considérer qu'étant donné la nature connue et établie du cyberespace, le risque de propagation de l'arme fait partie des risques attendus et évaluables. Cependant, deux solutions existent pour palier cette difficulté. La première, à nouveau, est de séparer le cyberespace civil du cyberespace militaire. Pourtant, en raison des coûts que représenterait une telle opération, cette solution n'est pas envisageable à l'heure actuelle. Dès lors, une autre solution serait que les armes cybernétiques soient toutes dotées d'une commande d'autodestruction, permettant de freiner et de stopper une éventuelle propagation qui violerait le principe de proportionnalité. *A priori*, une telle obligation ne peut émaner que d'une convention spéciale. Il serait peut-être envisageable de considérer que cette obligation puisse découler de l'association du principe de proportionnalité et de l'obligation de s'assurer que les armes cybernétiques développées respectent le *jus in bello.* Cette proposition semble tout à fait crédible d'un point de vue théorique.

Après avoir analysé l'application du principe de proportionnalité à l'usage de moyens et méthodes de combat cybernétiques, c'est celle du principe de précaution qui sera développée.

C. Le principe de précaution

Face aux spécificités du cyberespace, le principe de précaution représente peut être un des principes les plus important du *jus in bello*. Le principe de précaution se distingue en deux catégories d'obligations : celles de précaution dite active et celles de précaution dite passive[228].

1. Les précautions actives

Les précautions actives, ou précautions dans l'attaque, se réfèrent à un ensemble de mesures devant être prises dans l'aspect pratique d'une opération. On se demandera comment vont s'opérer ces précautions dans le cadre d'une cyberopération.

a. Le choix de la cible et le choix de l'arme ou de la méthode

Les premières obligations de précautions se situent au stade de la mise au point du plan d'attaque. Ainsi, le choix de la cible et le choix du moyen ou de la méthode employé représentent les premières étapes de précaution dans le cadre de toute opération.

Les experts chargés de la rédaction du Manuel de Tallinn établissent que « *ceux qui planifient ou décident d'une cyberattaque doivent faire tout ce qui est nécessaire pour vérifier que les objectifs qui doivent être attaqués ne soient ni des personnes civiles, ni des objets civils, ni des*

[228] J.D'ASPREMONT et J. DE HEMPTINNE, *Droit international humanitaire*, Pedone, octobre 2012 p. 300.

des éléments sujets à une protection particulière »[229]. Ils se basent à nouveau sur une distinction entre attaque et hostilités, distinction que nous avons jugée inadaptée au cas cybernétique. Il est toutefois possible d'assimiler les règles qu'ils dessinent et de les appliquer plus largement aux hostilités. Le moyen le plus sûr de respecter cette précaution est la collecte d'informations sur le réseau visé[230] afin de déterminer comment l'arme va réagir sur ledit réseau[231]. Par exemple, l'arme cybernétique ne réagira pas de manière identique dans un réseau local restreint et dans un réseau ouvert. Les personnes chargées d'assumer ce rôle de précaution sont celles qui organisent l'opération et ceux qui prennent les décisions opérationnelles en temps réel[232]. Cependant, étant donné la structure du cyberespace - hautement interconnectée et duale - on se demande si le respect de ce principe de précaution est raisonnablement envisageable.

Le choix de l'arme ou de la méthode est également restreint par le principe de précaution. La règle 116 du Manuel dispose que « *ceux qui planifient ou décident d'une cyberattaque doivent prendre toutes les précautions envisageables dans le choix du moyen ou de la méthode de combat en vue d'éviter ou de minimiser les dommages collatéraux* »[233]. Cette règle est l'extension de l'article 57 du Protocole I à l'emploi de moyens et méthodes cybernétiques[234]. Elle représente aussi un renfort du principe de proportionnalité en opérant en amont au stade de la détermination d'un moyen qui, s'il ne peut éviter des dommages collatéraux, va au moins permettre de les limiter. Dans ce genre de situation, cette règle impose d'ailleurs de rechercher une alternative qui épargnerait les

---

[229] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2 février 2017, règle 115.

[230] *Mapping*.

[231] *Ibid*, règle 115, para. 4. V. aussi : E.T.JENSEN, « Unexpected Consequences from Knock-On Effects », dans *American University International Law Review*, vol. 18, n°5, 2003, p.1185.

[232] *Ibid,* règle 115, para. 2.

[233] *Ibid*, règle 116.

[234] Article 57, paragraphe 2-a-ii, Protocole additionnel I, Genève, 1977.

civils[235]. Le choix de l'arme est central dans le cadre cybernétique en raison de la nature du cyberespace. Le moyen ou la méthode employé devra donc prendre en considération à la fois l'interconnectivité du milieu et sa nature duale pour limiter un effet de propagation de l'arme.

D'autres précautions actives doivent être prises dans le cadre du déroulement de la cyberopération.

b. L'avertissement de l'attaque et l'annulation de l'attaque

L'avertissement et l'annulation de l'attaque sont des précaution de second degré : il n'est plus question de prendre des précautions dans l'élaboration du plan d'attaque, mais d'en prendre parce que l'attaque est imminente.

La règle 119 du Manuel de Tallinn propose que « *ceux qui planifient, approuvent et mettent à exécution une cyberattaque doivent annuler ou suspendre l'attaque s'il apparait que l'objectif n'est pas militaire ou qu'il est sujet à une protection spéciale, ou si elle serait de nature à causer des dommages superflus par rapport à l'avantage militaire anticipé* »[236]. Cette disposition sert essentiellement à s'assurer que le principe de précaution s'étende au-delà de la seule planification de l'opération pour palier à d'éventuels changements de situation. Le paragraphe b) en particulier renforce le principe de proportionnalité en instaurant l'existence d'une évaluation de la proportionnalité face à l'imminence de l'exécution de l'opération en tant qu'obligation de précaution.

---

[235] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2 février 2017, règle 116, para. 2.

[236] *Ibid*, règle 119.

La difficulté réside ici dans la faisabilité de la suspension de l'attaque. Certaines cyberopérations sont fulgurantes et les effets de l'arme cybernétique peuvent être quasi immédiats. En pareil cas, on imagine mal comment l'opération pourrait être suspendue, rendant impraticable l'application du principe de précaution à cet égard. En revanche, d'autres armes et méthodes cybernétiques peuvent permettre une suspension ou une annulation de l'attaque. On peut par exemple imaginer une bombe logique dotée d'une *kill command* : une fois activée, cette commande permettrait en quelque sorte d'effacer la bombe logique sans qu'elle ne produise ses effets destructeurs, permettant ainsi l'annulation de l'attaque.

Concernant l'avertissement, le Manuel de Tallin dispose qu'« *un avertissement préalable doit être donné si une cyberattaque est de nature à affecter la population civile, sauf si les circonstances ne le permettent pas* »[237]. Les experts limitent ce principe à leur notion d'attaque, qui n'englobe pas l'intégralité des hostilités tel que nous l'entendons. En considération de cette règle et de l'intérêt de l'emploi de la force cybernétique, ce postulat ne nous semble pas ici immodéré. Ainsi, le principe d'avertissement toucherait aux cyberopérations les plus dangereuses. L'avertissement doit être donné aux autorités compétentes ; en revanche, s'il existe des raisons de croire que l'adversaire n'avertira pas ou ne peut pas avertir lui même la population, il reviendra à l'attaquant d'avertir lui même la population[238]. Cet avertissement n'est pas obligatoire « *lorsque les circonstances ne le permettent pas* ». Ce postulat renvoie à l'idée que l'avertissement pourrait priver l'attaque de son intérêt. Ainsi, « *quand la cyberattaque nécessite l'effet de surprise, un avertissement n'a pas à être donné* »[239]. Souvent, le propre des cyberattaques réside dans l'effet de surprise. Cette dernière observation pourrait vider de son sens la disposition entière. Dès lors, on

[237] *Ibid*, règle 120.

[238] *Ibid*, règle 120, para. 6.

[239] *Ibid*, règle 120, para. 8.

peut envisager que les autres éléments de la règle prévalent sur celui-ci. Ainsi, une cyberattaque nécessitant la surprise mais qui serait de nature à atteindre massivement les civils devra faire l'objet d'un avertissement.

Les précautions actives sont doublées de précautions passives.

2. Les précautions passives

Les précautions passives, ou précautions contre les effets d'une attaque, sont un ensemble de précautions qui doivent être prises en dehors de la considération d'une attaque précise et imminente : elles visent simplement à éviter des pertes matérielles et humaines en prenant certaines dispositions en amont d'une éventuelle opération hostile.

a. La protection de la population civile soumise à l'autorité d'une partie au conflit

La première de ces mesures de précaution passive repose sur l'obligation pour toute partie à un conflit de prendre les mesures nécessaires pour assurer la protection de la population civile soumise à son autorité[240]. Ces précautions relèvent plus du défenseur que de l'attaquant.

Le Manuel de Tallinn souligne une possibilité intéressante de précaution passive : la séparation des infrastructures cybernétiques civiles et militaires, que nous avions déjà envisagée

[240] Article 58, para. c, Protocole Additionnel I, Genève, 1977.

comme solution aux problèmes d'application des principes précédents[241]. D'autres propositions toutes aussi intéressantes sont faites, et notamment celle de séparer les systèmes informatiques dont dépendent des infrastructures vitales à la population civile de l'Internet. Ces deux solutions permettraient de résoudre nombre des difficultés posées par l'emploi de moyens et méthodes de combat cybernétiques quant à l'application des principes « cardinaux » du *jus in bello*. En revanche, les experts sont majoritairement de l'avis que cette disposition s'applique seulement aux attaques, limitant la portée de l'obligation. Au surplus, ces précautions renvoient à la notion du « maximum faisable », ce qui limite encore une fois sa portée. Des obligations positives de séparer les réseaux militaires et civils seraient plus efficaces.

La deuxième obligation repose sur le fait d'éloigner les civils des objectifs militaires et, inversement, de ne pas installer d'objectifs militaires dans des zones peuplées.

b. L'obligation d'éloigner les civils du voisinage des objectifs militaires

La seconde de ces mesures de précaution passive est relative à la situation géographique des objectifs militaires[242].

Concernant la proximité de l'objectif avec les civils, deux situations peuvent apparaitre. D'abord, la destruction via le vecteur cybernétique d'un objectif donné pourrait avoir des conséquences sur les populations civiles avoisinantes. En pareil cas, la solution réside en leur évacuation. Ensuite, une cyberopération hostile pourrait avoir des effets indirects sur les ordinateurs

---

[241] M.N.SCHMITT (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2 février 2017, règle 121, para. 3.

[242] *Ibid*, paras. 9-12.

de civils ou sur certaines infrastructures cybernétiques civiles, par leur proximité « cybernétique » avec l'objectif visé. La solution proposée par les experts est, à nouveau, de compartimenter les réseaux civils et militaires[243].

Concernant le fait de ne pas installer d'objectif militaire dans des zones densément peuplées. Deux interprétations de cette règle peuvent être admises. D'une part, c'est seulement la localisation physique de l'objectif qui est concernée par la règle. D'autre part, ce sont les localisations physiques et cybernétiques de l'objectif qui sont concernées. Dans le premier cas, il suffit de ne pas installer d'objectif militaire dans une zone peuplée. Mais cela peut s'avérer plus délicat : encore, la nature à double usage de certains biens cybernétiques risque d'entraver le fonctionnement de cette règle. Par exemple, comment empêcher l'installation d'une dorsale optique dans les zones peuplées alors que c'est précisément le genre de zone qui sont recherchées pour les installer ? Dans le second cas, la situation est encore plus complexe : où se situe un objectif cybernétique dans le cyberespace ? Dans la couche physique, avec le *hardware*, dans la couche logique, qui peut être cantonnée à l'unité physique, et aussi dans la couche cognitive. Mais l'emplacement de l'objectif cybernétique n'est pas fixe : il se connecte à différents réseaux, il est à différents endroits à la fois. Notamment, on peut considérer qu'il est « au travers » de l'Internet. Dès lors, comment appliquer cette précaution ? Dans les deux cas, la solution reste la compartimentation.

[243] *Ibid*, para. 10

- **Conclusion**

Très souvent, les progrès technologiques de la société civile finissent par s'étendre au domaine militaire. En 2007, lorsque l'Estonie était la proie d'une attaque cybernétique de grande ampleur, la première en son genre, il a été permis pour tout un chacun de constater que la conflictualité était en train d'évoluer sur un plan jusque là jamais envisagé. L'exercice de la force s'effectuait jusqu'ici en dernier recours sur le champ de bataille, un espace tangible et bien connu, réglementé par un large ensemble de dispositions. Alors, quand un nouvel espace de conflictualité intangible s'est développé, il apparaissait logique de penser que des instruments juridiques allaient voir le jour pour réglementer ce nouveau théâtre d'opération. Pourtant, à l'heure actuelle, aucun nouveau traité international n'a été adopté à ce sujet. Pire encore, les groupes d'experts mandatés par les Nations Unies pour oeuvrer en ce sens finissent généralement dans des impasses, souvent d'ordre politique. À défaut de nouveau texte, la meilleure stratégie à adopter restait encore de tenter d'appliquer les règles déjà existantes au cas du cyberespace. C'est ainsi qu'il a été décrété que le droit international s'appliquait *lato sensu* au cyberespace, ce qui s'avère être une première étape importante et nécessaire. Par extension, on considère aujourd'hui que le droit international humanitaire *lato sensu* s'applique au cyberespace et donc à la nouvelle conflictualité cybernétique. D'une part, le *jus ad bellum* s'applique à l'emploi de la force cybernétique, et, d'autre part, le *jus in bello* s'applique à l'emploi de moyens et méthodes de combat cybernétiques dans le cadre de conflits armés - internationaux et non internationaux. Cette position établie, la doctrine s'est empressée de chercher à déterminer *comment* s'appliquait ces corpus au phénomène cybernétique. C'est ainsi que, notamment, le Manuel de Tallinn a été rédigé sous l'égide de l'Organisation du

traité de l'atlantique nord. Parallèlement, le Comité international de la Croix-Rouge s'est également mobilisé autour de cette question.

Ici, en partant du postulat que le droit international humanitaire s'appliquait aux moyens et méthodes de combat cybernétiques, il était question de tenter d'analyser les modalités de cette application. Cette analyse proposait de tenir compte à tout instant des spécificités de l'environnement cybernétique et des moyens et méthodes cybernétiques, et de les mettre en opposition avec les règles classiques du droit international humanitaire. Nous avons cherché à démontrer que si les règles du *jus ad bellum* et du *jus in bello* pouvaient bien s'appliquer aux moyens et méthodes de combat cybernétiques, les caractéristiques spécifiques de ceux-ci entravaient de manière non négligeable ladite application. Ainsi, nous avons pu constater dans le cadre du *jus ad bellum* comme dans celui du *jus in bello* que les difficultés profondes d'attribution des actes illicites, inhérentes à la nature du cyberespace et de ces nouveaux moyens et méthodes, atteignaient sensiblement certaines règles classiques de droit international humanitaire, comme la légitime défense ou la qualification d'un conflit armé. L'instabilité de l'environnement cybernétique et son corollaire, l'imprévisibilité, font qu'un certain nombre de dispositions ne sont pas opérantes, notamment quant à la précaution ou la proportionnalité. Dans une certaine mesure, on considèrera même que la prolifération actuelle des moyens et méthodes de combat cybernétiques pourrait s'apparenter à une menace contre la paix et la sécurité internationales. Au surplus, certaines notions controversées du droit international humanitaire, comme celles d'agression armée ou d'attaque, trouvent un écho nouveau dans le cadre cybernétique - mais aucune autorité n'est légitime, à l'heure actuelle, pour trancher ces questions, limitant *de facto* l'application du droit international humanitaire aux moyens et méthodes de combat cybernétiques.

Plusieurs solutions sont envisageables pour palier ces problèmes. Si, d'un point de vue théorique, il semble difficile de parvenir à un accord sur la nature de certaines notions dans le domaine cybernétiques alors qu'elles ne font pas forcément consensus sur le plan conventionnel, des mesures pratiques peuvent être prises pour limiter par avance les effets toujours plus néfastes de la prolifération des armes cybernétiques et des cyberopérations. La plus simple et la plus radicale serait d'exclure le cyberespace des domaines d'opérations envisageables, mais elle n'est pas réaliste. D'un point de vue plus pragmatique, on s'aperçoit que certaines armes, du fait de leur spécificités, font l'objet de conventions spéciales. Dès lors, on pourrait envisager une convention spéciale réglementant la question des moyens et méthodes de combat cybernétiques. Une autre solution serait d'établir un traité de séparation du cyberespace, entre le cyberespace militaire et le cyberespace civil. Le fait est qu'a l'heure actuelle, l'appétence des acteurs étatiques pour le cyberespace et les moyens et méthodes de combat cybernétiques réside principalement dans le fait que le cyberespace permet de mener des opérations dans un grand anonymat. Ainsi, les solutions exposées ne seront surement pas accueillies par les États les plus concernés par la lutte informatique. Puisque la volonté étatique est nécessaire à tout processus conventionnel, il apparait qu'une convention portant trop sensiblement atteinte aux avantages que les États tirent des spécifiés du cyberespace ne semble pas prête à voir le jour. On peut toutefois souligner, à titre régional, l'existence de certains instruments qui pourraient un jour constituer des bases pour de nouvelles conventions et qui montre que même si le phénomène est lent, une réglementation du cyberespace et des instruments cybernétiques est bien à l'oeuvre.

Quoiqu'il en soit, il apparait que si l'applicabilité du droit international humanitaire aux moyens et méthodes de combat cybernétique est maintenant largement admise, l'application concrète de ces règles demeure compliquée à bien des égards, et que la situation appelle à une mobilisation plus grande de la communauté internationale pour parfaire ce cadre.

BIBLIOGRAPHIE

OUVRAGES

BANNELIER (Karine), « Is the Principle of Distinction Still Relevent in Cyberwarfare? », dans *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 26 juin 2015

CLARKE (Richard) et KNACKE (Robert), *Cyber war*, New York, HarperCollins, 2010

D'ASPREMONT (Jean) et DE HEMPTINNE (Jérôme), *Droit international humanitaire*, Éditions A.Pedone, Paris, octobre 2012.

DINNISS (H.H), *Cyber warfare and the laws of war*, Cambridge University Press, 2012.

DINSTEIN (Y.), *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, 2004.

GOLDSMITH (Jack) et WU (Tim) *Who controls the internet ? Illusions of a borderless world,* Oxford University Press, 2006.

HARREL (Yannick) *Cyberstratégies économiques et financières*, Paris, Nuvis, 2014.

KEMPF (Olivier), *Introduction à la cyberstratégie*, Paris, Economica, 2015.

MELZER (N.), *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, Comité international de la Croix-Rouge, 2009

SCHMITT (Michael), T*allinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2 février 2017.

SPITZNER (Lance), *Honeypots : tracking hackers*, Addison Wesley, 13 septembre 2002.

TSAGOURIAS (Nicholas), « The legal status of cyberspace », dans *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, 26 juin 2015, p. 13

WAXMAN, *The Caroline affair in the evolving international law f self-defense*, Irwin Law, 2018

WIENER (Norbert), *Cybernetics or Control and Communication in the Animal and the Machine*, 2ème édition, Cambridge, The M.I.T. Press, 1948.

REVUES

AILLERET (C.), Armes tactiques et stratégiques », dans *Correspondance*, n°043, décembre 1947

BAMBAUER (D.E), « Conundrum », Minnesota Law Review, 2011-2012.

BANNELIER (Karine) et CHRISTAKIS (Theodore), « Cyberdéfense active par des entreprises privées ? Le hack-back entre l'hostilité de la Revue stratégique de cyberdéfense de la France et le projet de loi ACDC aux États-Unis », *Stratégie*, n°117, Institut de Stratégie Comparée, 2017

BANNELIER (Karine), « Cyber Diligence : A low-intensity due diligence principle for low-intensity Cyber-Operations ? », Baltic Yearbook of International Law, vol. 14, 2014.

BARAT-GINIES (Orane), « Existe-t-il un droit international du cyberespace ? », *Hérodote*, n°152-153, 2014.

BURTON (J.), « Cyber Deterrence: A Comprehensive Approach? », C.C.D.C.O.E, avril 2018.

CARUS (W.S), Defining « Weapons of Mass Destruction », *Occasional Paper,* n°8, Center for the Study of Weapons of Mass Destruction, National Defense University, janvier 2012.

CIVIS, À propos d'une classification des armements », dans *Politique étrangère*, n°3, 1962.

DIJKSTRA (Edsger), « The Structure of the "THE" Multiprogramming System », *Communications of the ACM*, Volume 11, n°5, Université de technologie, Eindhoven, Pays-Bas, mai 1968

DORMANN (K.), « Applicability of the Additional Protocols to Computer Network Attacks », CICR, 2004.

DROEGE (Cordula), « Sortez de mon « Cloud »: la cyberguerre, le droit international humanitaire et la protection des civils », dans *Revue internationale de la Croix-Rouge*, vol. 94, n°886, 2012.

GÉRY (Aude), « La lutte contre la prolifération des armes cyber : un défi pour la stratégie française de cyberdéfense », *Les champs de Mars*, Presses de Sciences Po, n° 30.

HALLIDAY (J.), Stuxnet Worm is the work of a national government agency », *The Guardian*, 24 septembre 2010.

HANDLER (S.G), « The new cyber face of battle : developing a legal approach to accommodate emerging trends in warfare », *Stanford Journal of International Law*, 2012.

HATCH (B.B), « Defning a Class of Cyber Weapons as WMD: An Examination of the Merits », dans *Journal of Strategic Security*, vol. 11, n°1, 2018.

JENSEN (E.T.), « Unexpected Consequences from Knock-On Effects », dans American University International Law Review, vol. 18, n°5, 2003.

JOHNSON (David) et POST (David), « Law and borders: The rise of law in cyberspace », *Stanford Law Review*, vol.48, n°5, 1996

KEMPF (Olivier), « Le cyberterrorisme : un discours plus qu'une réalité », *Hérodote*, n°152-153, 2014.

LIN (H.S.), « Offensive Cyber Operations and the Use of Force », dans *Journal of National Security Law and Policy*, vol. 4, 2010.

MA (Z.) « Undesrtanding the Mirai botnet », dans Proceedings of the 26th USENIX Security Symposium, Vancouver, Canada, 16-18 aout 2017.

MAURONI (Al), Countering Weapons of Mass Destruction: Assessing the U.S. Government's Policy, Rowman & Littlefield, 2016.

MCGAVRAN (W.), « Intended consequences : regulating cyber attacks », *Tulane Journal of Technology and* Intellectual Property, 2009.

MELZER (N.), « Les cyber-opérations et le jus in bello », dans Forum du désarmement : faire face aux cyberconflits, Rapport UNIDIR, 2011.

MURPHY (J.F), « Cyber War and international law : does the international legal process constitue a threat to U.S vital interests ? », dans *International Law Studies U.S. Naval War College*, 2013.

RABOIN (B.), « Corresponding évolution : International law and the emergency of Cyber Warfare », *Journal of National Association of Administrative Law Judiciary*, 2011.

SCHMITT (Michael), « The law of cyber warfare : quo vadis ? », dans *Stanford Policy and Law Review* 2014.

SCHMITT (Michael), « Cyber operations and the jus ad bellum revisited », *Villanova aw review*, Vol. 56, n °3, 2011.

SCHMITT (Michael), « Computer network attack and use of force in international law : thoughts on a normative framework », Columbia Journal of Transnational Law, 1999.

SCHMITT (Michael) « Change Direction 2006 : Israeli opérations in Lebanon and the International Law of self-defense », Michigan Journal of International Law, 2008.

SCHMITT (Michael), « Cyber Operations and the Jus in bello: Key issues », dans Naval War College International Law Studies, vol. 87, 2011.

SCHMITT (Michael), « Wired warfare : Computer network attack and jus in bello », dans Revue internationale de la Croix-Rouge, no°846, 2002.

SEGAL (Adam), « China, international law and cyber space », dans *Council on Foreign Relations*, 2 octobre 2012.

SUDRES (Arnaud), « Cyberespace et dimension stratégique de la force informatique », dans *Stratégie*, n °117, Institut de Stratégie Comparée, 2017.

TURPIN (Dominique), ONU, CICR, et droit international humanitaire », *Revue Québécoise de droit international*, volume 8-1, 1993.

ZHANG (Li), « A chinese perspective on cyber war » dans la *Revue internationale de la Croix-Rouge*, version anglaise, volume 94, 2012.

MEMOIRES ET ARTICLES

BOULAICHE (Ammar), Technologies Honeypots, Université Abderrahmene Mira de Béjaia, 2006

CHANG-TUNG, , Le droit international à l'épreuve de la cyberguerre - le cas de Stuxnet, Université de Grenoble, janvier 2018

TEXTES INTERNATIONAUX

Charte des Nations Unies, San Francisco, 26 juin 1945

Convention de La Haye concernant les lois et coutumes de la guerre sur terre, La Haye, 18 octobre 1907 .

Convention IX de La Haye, La Haye, 1907

Conventions de Genève du 12 aout 1949

Convention sur certaines armes classiques, Genève, 10 octobre 1980

Convention sur l'interdiction des armes chimiques, Genève, 3 septembre 1992

Convention sur l'interdiction des armes biologiques, Londres, Moscou et Washington, 10 avril 1972

Convention d'Ottawa sur l'interdiction des mines antipersonnel, Ottawa, 18 septembre 1997

Convention sur les armes à sous-munitions, Dublin, 30 mai 2008

Convention sur la Cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001

Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, Résolution AGNU 56/83, annexe, 12 décembre 2001

Protocoles additionnels I et II aux Conventions de Genève, 1977.

Traité sur la non-prolifération des armes nucléaires, Nations Unies, *Recueil des traités*, vol. 729, n °I-10485.

Traité sur le commerce des armes, New York, 2 avril 2013.

DÉCISIONS

Cour internationale de justice, *Détroit de Corfou*, Recueil, 1949

Cour Internationale de Justice, *Personnel diplomatique et consulaire des États-Unis à Téhéran*, Recueil, 24 mai 1980

Cour Internationale de Justice, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci*, Recueil des arrêts, avis consultatifs et ordonnances, 1984.

Cour Internationale de Justice, *Avis consultatif, Licéité de la menace ou de l'emploi d'armes nucléaires*, Recueil des arrêts, avis consultatifs et ordonnances, 8 juillet 1996

Cour Internationale de Justice, *Affaire relative au projet Gabčíkovo-Nagymaros (Hongrie/Slovaquie)*, Recueil des arrêts, avis consultatifs et ordonnances, 25 septembre 1997.

Cour internationale de Justice, Avis consultatif, *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, 9 juillet 2004

Cour internationale de Justice, *Affaire Congo c/Ouganda dite des activités militaires sur le territoire du Congo*, 19 décembre 2005

Tribunal pénal international pour l'ex-Yougoslavie, *Le procureur contre Dusko Tadić*, Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, 2 octobre 1995

Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur contre Limaj*, 30 novembre 2005

Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur contre Haradinaj*, 3 avril 2008

Tribunal pénal international pour l'ex-Yougoslavie, *Le Procureur contre Boskoski*, 10 juillet 2008

DOCUMENTS OFFICIELS

Assemblée Générale des Nations Unies, Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale, 24 juin 2013, Document A/68/98

Assemblée nationale, Rapport d'information déposé en conclusion des travaux d'une mission d'information sur la cyberdéfense, 4 juillet 2018

Comité international de la Croix-Rouge, « *Qu'est-ce que le droit international humanitaire ?* », Services consultatifs en droit international humanitaire, août 2004.

Comité International de la Croix-Rouge, *Étude sur le droit international coutumier*, vol. 1, annexe « Liste des règles coutumières du droit international humanitaire », 2005

Department of Defense, Dictionary of Military and Associated Terms, Joint Publication 1-02, 2010, amendé en 2016

Fédération de Russie, Military doctrine of the Russian Federation approved by the President, 2014.

Ministère de la Défense, *Revue stratégique de défense et de sécurité nationale*, 2017.

Ministère de la Défense, Livre blanc Défense et Sécurité nationales, 2013

Ministère de l'Europe et des affaires étrangères, Réponse de la France à la résolution 73/27 relative aux « Progrès de l'informatique et des télécommunications et sécurité internationale » et à la résolution 73/266 relative à « Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale »

Nations Unies, Assemblée Générale, Developments in the field of information and telecommunications in the context of international security, 20 juillet 2010, Document A/65/154.

Secrétariat général de la Défense et de la Sécurité nationales, *Revue stratégique de cyberdefense*, 12 février 2018

Sénat français, Cyberdéfense : un nouvel enjeu de sécurité nationale, Rapport d'information n°499, 8 juillet 2008.

DISCOURS

BARLOW (John), A Declaration of The Independence of Cyberspace, Davos, Suisse, 8 février 1996.

KOH (Harold), « International law in cyberspace », U.S. Cyber command inter-agency legal conference, 18 septembre 2012.

QUN (Wang), Discours devant l'Assemblée Générale des Nations Unies, 66ème session de l'Assemblée générale, 2011.

QUN (Wang), Discours devant l'Assemblée Générale des Nations Unies, 71ème session de l'Assemblée générale, 2016.

RESSOURCES INFORMATIQUES

Académie Française, Dictionnaire de l'Académie française, 9ème édition, tome 2, 1992. Disponible en ligne : « https://www.dictionnaire-academie.fr/article/A9C5393 »

Agence nationale de la sécurité des systèmes d'information, *Glossaire*, « cyberespace ». Disponible en ligne : « https://www.ssi.gouv.fr/entreprise/glossaire »

Cambridge English Dictionary, Cambridge University Press, 2011. Disponible en ligne « https://dictionary.cambridge.org/fr/dictionnaire/anglais/cybernetics ».

Compte Twitter des Forces de Défense Israéliennes, « We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work », 5 mai 2019, consulté en ligne le 27 juillet 2019. Disponible en ligne : « https://twitter.com/IDF/status/1125066395010699264 »

SYMANTEC, Petya ransomware outbreak : here's what you need to know, 24 octobre 2017.

SYMANTEC, *About the BadRabitt ransomware*, alerte2452, 25 octobre 2017.

UNTERSINGER (Martin), « Israël dit avoir déjoué une cyberattaque du Hamas à Gaza, avant de frapper le site d'origine », *Le monde*, 6 mai 2019. Disponible en ligne : « https://www.lemonde.fr/pixels/article/2019/05/06/israel-dit-avoir-replique-a-une-attaque-informatique-par-une-frappe-aerienne-une-premiere_5459063_4408996.html?xtor=RSS-3208 »

TABLES DES MATIÈRES