Le Manuel de droit des opérations militaires français : remarques sur une vision extensive discutable du jus ad bellum

Eric Pomès

Le *Manuel de droit des opérations militaires* français : remarques sur une vision extensive discutable du *jus ad bellum*

Eric Pomès

Maître de Conférences de l'Institut Catholique d'Enseignement Supérieur de Vendée (ICES), HDR, Doyen de la Faculté de droit et d'économie

Résumé : Le Manuel de droit des opérations militaires français publié en 2022 et long de 375 pages constitue une innovation. Il offre en effet une présentation très complète des positions de la France sur le cadre juridique de l'intervention de la force armée sur ou en dehors du territoire national, de l'emploi de la force en situation de conflit armé, aussi bien sur mer et dans les airs que dans l'espace extra-atmosphérique et le cyberespace et enfin, du contrôle du respect du droit dans le cas d'emploi de la force. Le Manuel fournit ainsi aux militaires les connaissances juridiques indispensables en opération et, à tous les lecteurs, l'éclairage nécessaire sur l'usage de la force par la France. La présente contribution se propose de discuter certaines des analyses présentées par le Manuel sur la qualification des opérations exclues du champ d'application du *jus ad bellum*, sur les fondements du recours à la force armée dans le cadre des cyber-opérations et sur l'élargissement opéré de la légitime défense.

Mots-clés : agression armée, attentats terroristes, arrentas terroristes, chapitre VII, de la Charte des Nations Unies, Cour Internationale de Justice, conflit armé, cyber-attaque, cyber-opérations, droit international humanitaire, emploi de la force armée, évacuation des ressortissants, jus ad bellum, légitime défense, légitime défense préemptive, moyens cinétiques, moyens cybernétiques, pérations militaires, responsabilité de protéger

Abstract: The French Military Operations Law Manual published in 2022 and 375 pages long constitutes an innovation. It indeed offers a very complete presentation of France's positions on the legal framework for the intervention of armed force on or outside the national territory, the use of force in situations of armed conflict, both at sea and in the air as well as in outer space and cyberspace and finally, the control of respect for the law in the case of the use of force. The Manual thus provides soldiers with the legal knowledge essential in operations and, to all readers, the necessary insight into the use of force by France. This contribution aims to discuss some of the analyzes presented by the Manual on the qualification of operations excluded from context of cyber operations (III), and on the expansion of self-defense.

Keywords: armed aggression, terrorist attacks, terrorist arrentas, chapter VII, of the Charter of the United Nations, International Court of Justice, armed conflict, cyber-attack, cyber-operations, international humanitarian law, use of armed force, evacuation of nationals, jus ad bellum, self-defense, pre-emptive self-defense, kinetic means, cybernetic means, military operations, responsibility to protect

I. Introduction

Pour la première fois, le ministère français des armées édicte un guide en matière de droit opérationnel, le *Manuel de droit des opérations militaires* (ci-après le *Manuel*)[1], afin d'aider les militaires sur le terrain, là où il n'y avait jusqu'alors qu'un simple lexique, contrairement à de nombreuses armées étrangères. Cette publication doit être saluée en ce qu'elle explicite les positions juridiques françaises dans un contexte de diversification et de mutations des missions des forces armées. Le manuel fournit une analyse sans précédent de l'approche française des problèmes les plus pressants des conflits modernes notamment en matière d'armement, d'usage des forces armées sur le territoire national ou encore des cyber-opérations. Comptant 375 pages – loin des 1254 p. du *United States Department of Defense* (US DoD) (2015 mis à jour 2023) – il se compose ainsi de cinq parties qui ambitionnent d'embrasser l'ensemble des opérations aujourd'hui dévolues aux armées[2].

La présente contribution n'entend pas, naturellement, commenter l'ensemble de ce document, le *Manuel* s'avérant en effet très riche, notamment en accordant une place conséquente aux règles opérationnelles d'engagement. La partie relative au droit international humanitaire, pour sa part, ne présente pas d'apports majeurs. Il peut cependant être noté que la qualification de conflit armé international nécessite la présence de « l'intention belligérante »[3]. Cette exigence d'un critère subjectif et non objectif paraît conforme à la doctrine des incidents de frontières dans laquelle les États considèrent qu'il n'y a pas de conflit armé malgré des accrochages entre leurs forces[4]. Pourtant il ressort de la lecture de la jurisprudence[5], des commentaires du CICR[6] et d'une partie de la doctrine[7] que l'existence d'un conflit armé international est objective[8] : il existe dès lors qu' « il y a recours à la force armée entre États », quels qu'en soient les motifs ou l'intensité[9]. Sur le DIH toujours, deux réflexions supplémentaires peuvent également être formulées. D'abord, le *Manuel* précise à propos de l'article 50 par. 1 du Protocole I qu' « en cas de doute sur la qualité d'une personne, celle-ci sera considérée comme civile et sera donc protégée contre les attaques et les effets des attaques »[10]. Ce faisant, il ne tient pas compte du fait – est-ce une évolution de la position française ? – que, lors de sa ratification, la France a précisé que « le gouvernement de la

---

[1] *Manuel de droit des opérations militaires,* C. Faure, R. Stamminger (éd.), Direction des affaires juridiques État-major des armées, Paris, 2022.

[2] Partie 1 : Le cadre juridique d'intervention des forces armées sur le territoire national ; Partie 2 : Le cadre juridique d'intervention des forces armées en dehors du territoire national ; Partie 3 : L'emploi de la force en situation de conflit armé ; Partie 4 : Les règles spécifiques liées aux opérations dans différents milieux ; Partie 5 : Le contrôle du respect du droit en opération et la sanction des violations des règles liées à l'emploi de la force.

[3] *Manuel,* p. 83.

[4] *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique), fond*, p. 126, par. 195.

[5] CPI, *Situation en République de Corée : Rapport établi au titre de l'article 5*, juin 2014, par. 45-46.

[6] K. Dörmann *et al.* (éd.), *Commentary on the First Geneva Convention : Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, Cambridge, Cambridge University Press, 2016.

[7] É. David, *Principes de droit des conflits armés*, 6e édition, Bruxelles, Bruylant, 2019, p. 161-163.

[8] TPIR, *Akayesu*, jugement, 1998, par. 603 « [s]i l'application du droit international humanitaire dépendait de la seule appréciation subjective des parties aux conflits, celles-ci auraient dans la plupart des cas tendance à en minimiser l'intensité ».

[9] TPIY, *Tadić*, arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, 1995, par. 70.

[10] *Manuel,* p. 309.

République française considère que la règle édictée dans la seconde phrase du paragraphe 1 de l'article 50 ne peut être interprétée comme obligeant le commandement à prendre une décision qui, selon les circonstances et les informations à sa disposition, pourrait ne pas être compatible avec son devoir d'assurer la sécurité des troupes sous sa responsabilité ou de préserver sa situation militaire, conformément aux autres dispositions du Protocole »[11]. Le *Manuel* manque par ailleurs de clarté quant à la notion de participation directe aux hostilités puisqu'il semble n'y intégrer que les civils et non les membres de groupes armés non étatiques[12]. En effet, les rédacteurs ont décidé d'appliquer aux membres de ces groupes le terme de combattant tout en précisant que ce statut n'existe que dans le cadre des conflits armés internationaux et en reconnaissant que ce terme – qui est un statut dans le droit des conflits armés – est utilisé dans un sens large, c'est-à-dire non juridique[13]. Un tel choix créé une confusion entre le statut juridique de combattant, duquel dérive des protections et des obligations, et la qualification militaire de combattant qui est, elle, dénuée de portée juridique. Or, pour le *Guide interprétatif sur la Notion de Participation Directe aux Hostilités en Droit international humanitaire*, peuvent être considérés comme participant directement aux hostilités, d'une part, les membres des groupes armés non étatiques dès lors que ceux-ci exercent une fonction de combat continue, *ie*, préparent, exécutent ou commandent des actes ou des opérations constituant une participation directe aux hostilités[14] et, d'autre part les civils participant directement aux hostilités (employés de SMP notamment), c'est-à-dire, les civils commettant un acte hostile causant un dommage (la causalité doit être directe) à l'une des parties au conflit avec l'intention (*belligerent nexus*) de favoriser une des parties au détriment de l'autre.

Dans les deux cas présentés, le *Manuel* est insuffisamment précis et, quelle que soit l'interprétation retenue, cela constitue une source d'incompréhension tant de la position française que des règles devant être maîtrisées par les destinataires du *Manuel*.

En dépit de ces remarques qui mériteraient sans doute de plus amples développements, le *Manuel de droit des opérations militaires* constitue une ressource irremplaçable pour tout militaire qui souhaite comprendre l'environnement juridique des opérations modernes des forces armées (fonction instructive). L'ensemble du document fournit, de manière nécessairement synthétique, les connaissances juridiques indispensables aux militaires dans un environnement caractérisé par l'importance du droit et son utilisation possible contre les forces (*lawfare*). Le *Manuel de droit des opérations militaires* fournit également à tous les lecteurs avertis un document reflétant les positions juridiques françaises en matière d'utilisation des forces armées, leur permettant de comprendre et d'évaluer les déclarations juridiques et politiques prononcées (fonction d'information ou de transparence). C'est à la lumière de cette double exigence d'instruction des militaires et d'information et de transparence à destination d'un public plus large, formé essentiellement de civils, que le *Manuel* doit d'abord être abordé. Sur un plan plus strictement juridique, il devrait être aussi considéré comme ayant le statut que lui confère la présentation de la pratique étatique ou au moins de l'*opinio juris.* Dès l'introduction en effet, les rédacteurs précisent que le *Manuel* « expose à un plus large public la lecture que les autorités françaises font des règles de droit applicables aux forces armées françaises »[15] (fonction créative). Or, cette précision implique que la France

[11] *Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux* (Protocole I), 8 juin 1977, France 11/04/2001, par. 9.

[12] *Manuel,* p. 111-113.

[13] *Manuel,* p. 110 et note 270.

[14] *Guide interprétatif sur la Notion de Participation Directe aux Hostilités en Droit international humanitaire*, adopté par l'Assemblée du Comité International de la Croix-Rouge le 26 février 2009, p. 29, 36.

[15] *Manuel,* p. 18.

pourrait se trouver liée à des interprétations juridiques qui s'avérant gênantes ou dommageables à la lumière de circonstances futures imprévisibles. De même, ces interprétations juridiques, proposées en particulier sur la légitime défense ou les cyber-opérations, pourraient être utilisées par des adversaires soit pour justifier leurs propres positions soit pour délégitimer le comportement de la France.

Les rédacteurs précisent dans leur introduction que le droit international humanitaire (DIH) constitue le cœur du manuel[16]. Il constitue une branche du droit international qui désigne les règles relatives à la conduite des hostilités. Ses règles et principes visent à limiter les effets des conflits armés tout en prenant en compte les besoins militaires des belligérants. Il doit être distingué du droit relatif à l'usage de la force (*jus ad bellum*), qui est régi par la Charte des Nations unies. Dès lors, la précédente affirmation des rédacteurs du *Manuel* ne se comprend qu'à la condition d'avoir une acception large de cette expression afin d'y inclure tant le droit des conflits armés, le droit des armements que le droit international pénal[17]. Les parties 1 (utilisation des forces armées sur le territoire national hors conflit armé) et 2 (*jus ad bellum*) ne peuvent par contre en aucune manière relever du DIH. L'introduction aurait par ailleurs gagné en pertinence en insistant sur l'importance du droit pour les opérations militaires actuelles. On peut en effet lire que le « respect du droit international constitue la condition cardinale de la légitimité de nos actions nationalement et internationalement »[18]. Une telle idée – répétée un paragraphe plus loin – oblige à s'interroger sur le propos : soit l'opération respecte le droit, elle est alors licite, soit elle viole le droit, elle est alors illicite ; ce n'est donc pas une question de légitimité, mais bien de licéité de l'action. Il en va de même si on examine la mise en œuvre de l'opération. Cette phrase ne peut s'entendre que si l'on admet que les adversaires de la France ont identifié le respect du droit comme centre de gravité au sens de Clausewitz. Celui-ci correspond à « un élément, matériel ou immatériel, dont un État, ou un ensemble d'États, une collectivité, une force militaire, tire sa puissance, sa liberté d'action ou sa volonté de combattre[19] » ; il constitue le point central qu'un belligérant doit défendre à tout prix sinon il perd. Ainsi comprise, l'introduction aurait pu mettre en avant la notion de *Lawfare* qui s'attache désormais systématiquement aux engagements armés.

À partir de cette dimension d'utilisation stratégique du droit et de la volonté affichée par les rédacteurs d'exprimer l'interprétation française des règles relevant de l'usage de la force, cette contribution se propose d'apporter quelques commentaires critiques sur les passages consacrés au droit de faire la guerre. On peut estimer en effet que le *Manuel* retient une qualification discutable des opérations exclues du champ du *jus ad bellum* (II), demeure dans l'imprécision quant aux fondements du recours à la force armée dans le cadre des cyber-opérations (III), et opère un étirement critiquable de la légitime défense (IV).

II. Une qualification discutable des opérations exclues du champ du *jus ad bellum*

La partie 2 du *Manuel* traite du cadre juridique d'intervention des forces armées en dehors du territoire national. Le chapitre 1 aborde les interventions à l'étranger ne relevant pas du *jus ad bellum* (II.1.) puis la responsabilité de protéger (II.2.).

---

[16] *Ibid.*, p. 19. Cette branche du droit est également connu sous le nom de droit international des conflits armés, de droit des conflits armés (DCA), de droit de la guerre ou de *jus in bello*.

[17] R. Kolb, R. Hyde, *An introduction to the international law of armed conflicts*, Oxford, Hart Pub, 2008, p. 15 *sq*.

[18] *Manuel,* p. 22.

[19] PIA-5(B)_PNO(2014) N°152/DEF/CICDE/NP du 26 juin 2014, p. 32.

II.1. Des interrogations sur l'illicéité des opérations d'évacuation de ressortissants

Pour les rédacteurs, les opérations d'évacuation de ressortissants et la libération d'otages se définissant comme des « interventions unilatérales, qui se caractérisent par leur caractère momentané, urgent, conservatoire et militaire, conduites à des fins de protection de nationaux à l'étranger, sont illicites en droit international. Elles constituent une violation de l'indépendance, de la souveraineté et de l'intégrité territoriale d'un État. Le recours à la force durant de telles opérations est contraire à l'article 2 paragraphe 4 de la Charte ». Une ambiguïté doit cependant être notée dans ce paragraphe : évoque-t-il l'utilisation des armes dans de telles opérations ou bien signifie-t-il que celles-ci peuvent être qualifiées par elles-mêmes d'usage de la force contraire à l'article 2 par. 4 de la Charte ? Ni l'une ni l'autre de ces interprétations ne paraît satisfaisante.

L'hypothèse envisagée consiste en un usage ponctuel et éventuel de la force armée d'un État sur le territoire d'un autre État afin de secourir ses nationaux résidant sur le territoire de ce dernier. Est-il possible dans ce cas de recourir à des mesures armées pour protéger ses ressortissants et celles-ci violent-elles l'article 2 par. 4[20].

La définition militaire de ces opérations est la suivante : opérations de sécurité ayant pour objectif de protéger des ressortissants résidant à l'étranger en les évacuant d'une zone présentant une menace imminente et sérieuse risquant d'affecter leur sécurité, lorsque l'État dans lequel ils sont localisés n'est plus en mesure de la garantir[21]. L'action menée par la France au Shaba en est un exemple. Le 13 mai 1978, plusieurs centaines d'hommes en armes qui se réclament du Front de Libération nationale du Congo envahissent la ville de Kolwesi, occupent l'aérodrome et coupent toutes les communications. Face à l'inquiétude pour la vie des ressortissants étrangers, est déclenchée le 19 mai l' « opération Léopard » avec le largage sur la ville des hommes du 2e Régiment Étranger Parachutiste[22].

De telles opérations obligent à s'interroger sur leur fondement juridique. Selon le *Manuel* « seuls deux fondements juridiques alternatifs permettent la protection et l'évacuation de ressortissants : l'autorisation du Conseil de sécurité par une résolution fondée sur le chapitre VII, comme ce fut le cas de la résolution 1975 (2011) relative à la Côte d'Ivoire, qui a permis de protéger les ressortissants français, ou le consentement exprès de l'État hôte territorialement compétent ». Ces interventions n'auraient donc pas de fondement juridique propre[23]. Pourtant, certains auteurs et certains États estiment qu'il existe un droit coutumier permettant d'agir pour protéger ses propres nationaux reposant sur des considérations humanitaires : protéger des vies humaines en danger sur un territoire étranger[24]. Max Huber dans la sentence arbitrale du 1er mai 1925 dans l'affaire *Des biens britanniques au Maroc espagnol* écrivait que « ce droit a été revendiqué par tous les États et que seuls ses limites peuvent être discutées » et d'ajouter qu' « à un certain point, il apparait que l'intérêt de l'État de pouvoir protéger ses ressortissants et leurs biens prime le respect de la souveraineté

[20] K. Bannelier, T. Christakis, « Volenti non fit injuria ? Les effets du consentement à l'intervention militaire », *Afdi*, 2004, p. 102-137.

[21] *Les opérations d'évacuation de ressortissants (RESEVAC)*, DIA – 3.4.2, N°136/DEF/CICDE/NP du 02 juillet 2009, p. 6.

[22] A. Manin, « L'intervention française au Shaba (19 mai - 14 juin 1978) », *Afdi*, 1978, pp. 159-188.

[23] K. E. Eichensehr, « Defending Nationals Abroad : Assessing the Lawfulness of Forcible Hostage Rescues », *Virginia Journal of International Law*, 2008, vol. 48, no 2, pp. 451-484, O. Corten, *Le droit contre la guerre. L'interdiction du recours à la force en droit international contemporain*, *op. cit.*, p. 795.

[24] A. Manin, « L'intervention française au Shaba (19 mai - 14 juin 1978) », *op. cit.*, p. 160.

territoriale »[25]. L'antériorité de cette sentence par rapport à la Charte des Nations unies ne permet pas de conclure définitivement en faveur de la licéité de telles opérations. Qu'en est-il alors s'il s'agit de sauver des vie ?

Les prémisses du raisonnement reposent, d'une part, sur l'idée que ces opérations ne sont pas dirigées contre l'État et, d'autre part, sur le conflit existant entre les droits et obligations de l'État intervenant et les droits et obligations de l'État du for : interdiction du recours à la force, respect de la souveraineté, droit à la vie… Les droits du premier priment-ils ceux du second[26] ?

La possibilité de recourir à la force pour protéger des ressortissants a été envisagée par l'article 2 du projet d'article sur la protection diplomatique proposé par le *Premier rapport sur la protection diplomatique* du 7 mars 2000[27]. En substance, la licéité de ces opérations reposerait sur trois séries de conditions : une menace imminente contre la vie ou l'intégrité physique des ressortissants ; l'absence de protection ou l'incapacité par l'État hôte de garantir l'ordre et la sécurité publique sur son territoire ; des mesures strictement limitées par leur objet, la protection des ressortissants, et par leur temporalité[28]. La logique de l'opération est alors exclusivement défensive ce qui implique une action impartiale vis-à-vis des éventuelles parties au conflit. En outre, l'opération doit se dérouler dans un laps de temps suffisamment court pour que l'atteinte à la souveraineté soit le plus possible limitée. L'intervention israélienne à Entebbe (Ouganda), le 4 juillet 1976, pour libérer les otages d'un détournement d'avion est un bon exemple d'opération de protection des ressortissants pouvant nécessiter des actions de nature offensive (saisie de points clés, extraction d'autorités et de ressortissants isolés…). Pratique étatique confirmée par l'opération *Palliser* conduite par le Royaume-Uni en 2000 en Sierra Leone[29], elle montre que de telles opérations peuvent être licites ce qui n'est pas la position retenue par le *Manuel.* Pourtant, selon la CIJ, toutes les opérations militaires ne sont pas *ipso facto* qualifiées d'usage prohibé de la force armée[30].

Il convient en effet de distinguer les opérations de police et l'usage de la force armée des agressions armées et de se demander si ces opérations atteignent un seuil d'intensité suffisant violant l'article 2 par. 4. Au regard des conditions exposées, elles pourraient être exclues du champ d'application de l'article 2 (4) en raison de leur faible intensité et de l'absence d'intention de forcer l'État à faire ou ne pas faire quelque chose[31].

En conséquence, l'affirmation du caractère toujours illicite de ces opérations ne paraît pas opportune, en particulier dans une période de recrudescence des coups d'État militaires qui peuvent nécessiter des interventions rapides y compris au nom de la responsabilité de protéger.

---

[25] *Affaire des biens britanniques au Maroc espagnol (Espagne contre Royaume-Uni)*, sentence du 1er mai 1925, *RSA*, vol. II, pp. 615-742, p. 641.

[26] T. Schweisfurth, « Operations to rescue nationals in third States involving the use of force in relation to the protection of human rights », *German Yearbook of International Law*, 1980, vol. 23, pp. 159-180, L. A. Sicilianos, *Les réactions décentralisées à l'illicite. Des contre-mesures à la légitime défense*, Paris, Lgdj, 1990, pp. 458-475.

[27] A/CN.4/506, *Premier rapport sur la protection diplomatique*, John R. Dugard, 7 mars 2000. Cette proposition a disparu du projet final relatif à la Protection diplomatique (A/RES/62/67, 8 janvier 2008).

[28] R. Kolb, *Ius contra bellum. Le droit international relatif au maintien de la paix*, *op. cit.*, p. 219.

[29] Voir, A. Leboeuf, « L'intervention britannique en Sierra Leone (2000-2002) », *Les Lettres du RETEX* https://www.c-dec.terre.defense.gouv.fr/images/documents/retex/10_GB_Sierra_Leone.pdf.

[30] *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique), fond*, arrêt, *CIJ Recueil, 1986*, p. 14, par. 191.

[31] O. Corten, *Le droit contre la guerre. L'interdiction du recours à la force en droit international contemporain*, p. 803.

II.2. Une lecture ambiguë de la responsabilité de protéger

La deuxième hypothèse envisagée par le *Manuel* dans ce chapitre 1 porte sur la responsabilité de protéger issue du rapport de la *Commission Internationale de l'Intervention et de la Souveraineté des États* (CIISE)[32]. Son objectif était de proposer une alternative acceptable, à la fois pour les opposants à l'usage de la force et pour ceux qui l'acceptent au nom de la protection des populations en danger[33]. Cette alternative repose, pour la CIISE, sur la « responsabilité de protéger »[34], cadre de la protection des populations[35], qui apparaît comme une synthèse d'évolutions en cours[36]. Le concept de responsabilité de protéger doit être entendu comme la « protection contre les catastrophes qu'il est possible de prévenir – meurtres à grande échelle, viols systématiques, famine »[37]. Les réponses aux violations massives des droits de l'homme sont ici complètement repensées. Contrairement au droit d'ingérence, l'accent est mis sur la responsabilité première et primaire de l'État de protéger la population vivant sur son territoire, l'action de la Communauté internationale ne se déclenchant que si l'État est incapable ou ne veut pas protéger la population. Mais, se pose alors la question de la licéité de l'usage de la force dans les hypothèses où ni l'État responsable ni la Communauté Internationale ne peuvent ou ne veulent agir. Alors que l'article 2 par. 4 de la Charte interdit l'usage de la force armée sans autorisation du Conseil de sécurité, est-ce qu'un État tiers pourrait décider d'employer unilatéralement la force au seul motif de mettre un terme aux violences faites à une population qui lui est étrangère ? Le *Manuel*, qui se veut le reflet des positions françaises en matière de droit international, tranche la question : il n'y a pas de nouvelle exception à l'article 2 par. 4[38]. L'action ne peut donc être que multilatérale.

Depuis le sommet mondial de 2005, la responsabilité de protéger a ainsi été utilisée au Kenya en 2008, au Darfour et bien évidemment en Libye[39]. Par la résolution 1973 (2011) le Conseil de sécurité a autorisé, sur le fondement du chapitre VII de la Charte, les États membres « à prendre toutes les mesures nécessaires, (…) afin de protéger les civils et les zones peuplées de civils menacés par une attaque » (paragraphe 4), à l'exclusion de tout déploiement de forces d'occupation étrangère en territoire libyen. Le *Manuel* précise que « cette résolution a ainsi autorisé le recours à la force par une opération militaire contre les forces armées

---

[32] E. Pomès, « Recherche sur une conciliation du droit et de la force à des fins humanitaires », *Thèse de doctorat de droit*, sous la direction de Louis Balmond, Université de Nice Sophia Antipolis, 2009.

[33] G. Evans, « From Humanitarian Intervention to responsibility to protect », *Wisconsin International Law Journal*, Fall 2006, vol. 24, n° 3, p. 703-722.

[34] Commission Internationale de l'Intervention et de la Souveraineté des États, *La responsabilité de protéger*, Ottawa, Centre de recherches pour le développement international, décembre 2001, A. Peters, « Le droit d'ingérence et le devoir d'ingérence – vers une responsabilité de protéger », *Revue de droit international et de droit comparé*, 2002, p. 290-308, K. Naumann, « La responsabilité de protéger : l'intervention humanitaire et la force militaire », *Revue militaire canadienne*, Hiver 2004-2005, p. 21-30, J. S. T. Pitzul, K. Abbott, C. K. Penny, « Réflexions sur la responsabilité de protéger et le droit militaire », *Revue militaire canadienne*, Hiver 2004-2005, p. 31-38, E. Marclay, *La responsabilité de protéger, un nouveau paradigme ou une boîte à outils ?*, Etudes Raoul-Dandurand n° 10, 2005, http://www.dandurand.uqam.ca, L. Boisson de Chazournes, L. Condorelli, « De la responsabilité de protéger, ou d'une nouvelle parure pour une notion déjà bien établie », *R.G.D.I.P*, 2006, p. 11-18.

[35] CIISE, *La responsabilité de protéger*, *op. cit.*, p. IX.

[36] J.-M. Thouvenin, « Genèse de l'idée de responsabilité de protéger », p. 21-38 in *La responsabilité de protéger*, SFDI, Paris, Pedone, 2008.

[37] A. J. Bellamy, *Responsibility to protect*, Cambridge, Polity Press, 2009.

[38] « elle ne remet en cause ni le principe de la souveraineté étatique, ni les conditions de recours à la force, tels que définies par la Charte », *Manuel,* p. 68.

[39] « Kenya et responsabilité de protéger », *RGDIP*, 2008.

libyennes, emmenée par les États-Unis, la France et le Royaume Uni, à la tête d'une coalition placée sous le commandement de l'OTAN »[40].

Une telle déclaration ne fournit cependant qu'une partie de la réalité, de nombreux États et l'Union africaine soulignant que le mandat du Conseil de sécurité n'avait pas été respecté dans ce cas. Les opérations ont montré en effet que l'action des forces, notamment françaises et britanniques, pouvait être analysée comme ayant pour objectif un changement de régime[41], ce qui n'est pas celui, humanitaire, sur la base duquel les États membres du Conseil de sécurité avaient accordé le mandat. Comme on pouvait le craindre[42], son dépassement par la coalition en Libye a favorisé une remise en cause de la responsabilité de protéger, entrainant, pour le moins, la quasi disparition des opérations déléguées. De manière contradictoire d'ailleurs, comme pour l'hypothèse du consentement, le *Manuel* place les opérations déléguées par le Conseil de sécurité dans le chapitre traitant des opérations ne relevant pas du *jus ad bellum* avant d'y revenir plus loin dans le chapitre portant sur le fondement juridique du recours à la force dans les relations internationales.

III. L'imprécision des fondements retenus pour la licéité du recours à la force armée dans des cyber-opérations

Selon le *Manuel*, les hypothèses licites d'emploi de la force armée sont : « le consentement de l'État sur le territoire duquel l'intervention armée a lieu d'une part, l'adoption par le Conseil de sécurité des Nations unies d'une résolution placée sous le chapitre VII de la Charte autorisant une telle intervention d'autre part, enfin, le recours à la légitime défense (individuelle ou collective) pour faire face à une agression armée au sens de l'article 51 de la Charte et dans l'attente d'une action du Conseil de sécurité »[43].

Si ce passage semble n'être qu'un rappel, il convient de préciser l'expression utilisée : « le recours à la force armée par un État » exprime-t-il un recours matériel à la force armée, auquel cas il renvoie aux opérations militaires, ou retient-il une interprétation juridique de la formule utilisée par l'article 2 par. 4 ?

Dans la première acception, cette expression ne fait pas de difficulté. Dans la seconde, elle nécessite quelques commentaires. Sans présager de la volonté des rédacteurs, le fait que le paragraphe 2 de ce chapitre porte sur la substance de l'article 2 par. 4 milite pour la deuxième interprétation. Dès lors, le consentement au déploiement de forces armées d'un État sur le territoire d'un autre État à la demande de ce dernier dans le cadre d'une crise intérieure conduit à ce qu'une telle opération ne relève pas d'une exception à l'article 2 par. 4 puisque l'existence d'un consentement valide a pour effet de rendre inapplicable cet article[44]. Un tel consentement serait également nécessaire dans le cadre de la légitime défense collective. Dans son arrêt *Nicaragua,* la CIJ exige en effet que l'État « victime » se déclare objet d'une agression armée et demande une aide militaire pour y faire face[45]. Ces deux conditions sont

---

[40] *Manuel,* p. 68-69.

[41] S/PV.6595, pp. 4-5 (Afrique du Sud), S/PV.6620, p. 3 (Russie), p. 4-5 (Chine), S/PV.6731, p. 10 (Chine).

[42] Voir en ce sens, L. Balmond, « La pratique récente de l'emploi de la force par la France : entre légalité et légitimité », http://revel.unice.fr/psei/index.html?id-88.

[43] *Manuel*, p. 71.

[44] O. Corten, *Le droit contre la guerre. L'interdiction du recours à la force en droit international contemporain*, *op. cit.*, p. 390-395.

[45] *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique), fond*, C.I.J. Recueil 1986, p. 14, par. 165, 195 et 199. D. Kritsiotis, « Intervention and the Problematisation of Consent », dans D. Kritsiotis, O. Corten et G. H. Fox (éd.), *Armed intervention and consent*, Cambridge,

indispensables pour que l'État aidant puisse se prévaloir de l'exception de légitime défense pour justifier l'emploi de la force contre l'agresseur. Enfin, le même raisonnement devrait être appliqué aux résolutions du Conseil de sécurité déléguant l'emploi de la force car, dans ce cas, il ne s'agit pas d'une opération unilatérale – relevant de l'article 2 par. 4 – mais d'une opération multilatérale déléguée à un ou plusieurs États par le Conseil de sécurité dans le cadre de sa responsabilité principale du maintien de la paix et de la sécurité internationales et des compétences que lui octroie le Chapitre VII. L'exécution de mesures militaires est déléguée mais la décision et le périmètre du mandat restent de la seule compétence du Conseil.

Ces précisions quant à la licéité de l'emploi de la force n'apparaissent pas dans le *Manuel* lorsqu'il aborde la qualification des vecteurs utilisés dans le cadre des cyber-opérations (III.1.) ce qui entraîne la difficulté de les qualifier au sens du *jus ad bellum* (III.2.).

III.1. Une identification insuffisante des cyber-armes comme vecteurs constitutifs du recours à la force

La position française sur la qualification possible des cyber-opérations définie par le Manuel peut être synthétisée ainsi : les cyber-opérations peuvent constituer une violation de l'article 2 par. 4, car elles sont réalisées par des cyber-armes dont la définition est présentée dans la note de bas de page 1091, page 308 : « le terme « arme » est utilisé, ici, dans un sens générique. Une « cyber-arme » renvoie à l'ensemble des moyens numériques utilisés en contexte de conflit armé et en lien avec celui-ci, c'est-à-dire aux armes, moyens et méthodes de guerre au sens de l'art. 35 du PA I, mais également aux moyens numériques qui ne produisent pas de dommages (utilisés à des fins, par exemple, de renseignement) »[46]. Une telle définition paraît peu satisfaisante : en quoi un moyen de renseignement constitue-t-il une arme ?

Les cyberattaques obligent ainsi à s'interroger à nouveau sur ce qui relève de la force « armée »[47]. Plusieurs pistes se dessinent. De prime abord, la définition de la force armée dépend du vecteur utilisé pour délivrer la force. Il y aurait emploi de la force armée chaque fois qu'elle est mise en œuvre par l'entremise d'armes. Les États, comme la doctrine, utilisent ainsi le terme de cyberarme[48] sans qu'il y ait de véritable analyse approfondie de ce qu'il recouvre. De manière plus prudente, les Nations unies lui ont préféré divers termes pour aborder les moyens informatiques dits malveillants tels que « techniques et outils informatiques malveillants », « technologies de l'information et des communications », « pratiques informatiques jugées nocives » ou encore « activités informatiques contraires aux obligations »[49]. Ces termes génériques regroupent l'ensemble des procédés[50], pratiques et activités

Cambridge University Press, 2023, J. A. Green, « The 'additional' criteria for collective self-defence : request but not declaration », *Journal on the Use of Force and International Law*, vol. 4, n° 1, 2017.

[46] *Manuel,* p. 308 note 109.

[47] Pour une synthèse voir O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel, « Which Law Governs During Armed Conflict ? The Relationship Between International Humanitarian Law and Human Rights Law », *Minnesota Law Review*, 2012, vol. 96, p. 1883-1943.

[48] https://ccdcoe.org/cyber-definitions.html. Voir aussi *Cyber defence in the EU Preparing for cyber warfare ?*, Briefing d'octobre 2014 du Parlement européen.

[49] Rapport du *groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, A/70/174, 22 juillet 2015.

[50] Ceci renvoie ainsi, sans s'y limiter, aux virus, aux vers, aux chevaux de Troie, aux bombes logiques, aux trappes et aux attaques par déni de services. Le virus est un fragment de code qui s'attache à un programme et ne se met en œuvre que lorsque son programme d'accueil commence à fonctionner. Le ver est un programme indépendant cherchant à propager son code au plus grand nombre de cibles, puis à l'exécuter sur ces mêmes cibles. Les chevaux de Troie peuvent être définis comme des fragments de code qui masquent

informatiques permettant de porter atteinte aux systèmes (destruction ou endommagement d'infrastructures vitales) et données informatiques[51]. Leur utilisation présente ainsi l'intérêt de ne pas préciser la nature de la technique ou de l'outil malveillant. En quoi ces moyens cybernétiques pourraient-ils constituer des armes ? Peuvent-ils être traités de la même manière que les armes « classiques » ? La difficulté de cette question réside dans l'absence de définition du terme « arme » en droit positif. Or, la détermination de la nature des différents moyens cybernétiques est fondamentale afin de distinguer les cyberarmes des moyens cybercriminels.

L'utilisation du terme « arme » dans l'expression « cyberarme » montre d'abord que, dans l'imaginaire collectif, leur nature d'arme est présupposée en raison de leurs effets destructeurs potentiels. Ceci résulte-t-il d'une analyse approfondie de la nature de ces moyens cybernétiques ou de la volonté d'inventer un terme destiné à marquer les esprits ? On notera simplement que l'utilisation de certains moyens cybernétiques ne sera qualifiée d'arme que dès lors qu'un État en est la cible, non lorsqu'ils sont utilisés contre des particuliers. La qualification des moyens cybernétiques dépendrait donc moins de leur nature que de leur cible. Par ailleurs, recourir au terme « cyber » ne suffit pas pour déterminer une nouvelle catégorie d'arme, car tous les moyens cybernétiques ne sont pas des armes. Pour déterminer les capacités cybernétiques susceptibles d'appartenir à la catégorie de cyberarme, il faut les comparer à celles qui résultent des dispositifs répondant à la définition de l'arme. Les effets des moyens cybernétiques autoriseraient alors une telle qualification.

Si aucun traité ne donne une définition générale d'une arme, celle-ci peut être élaborée à partir de l'étude du Comité International de la Croix-Rouge intitulée *Guide de l'examen de la licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre* qui permet de connaître la vision de plusieurs États, mais aussi du *Manuel on International Law Applicable to Air and Missile Warfare* publié par l'*Humanitarian Policy and Conflict Research*[52] et de l'étude du Comité International de la Croix-Rouge sur le droit international humanitaire coutumier[53]. Une arme pourrait ainsi se définir comme tout dispositif conçu ou utilisé dans le cadre d'une attaque afin de porter atteinte (directement ou indirectement) à la vie ou à l'intégrité, physique ou mentale, d'un individu ou à l'intégrité, matérielle ou immatérielle, d'un bien. On le retrouve dans le *Manuel de Tallinn*, lequel, dans sa règle 41 définit une cyberarme comme « *'cyber means of warfare' that are by design, use, or intended use capable of causing either (i) injury to, or death of, persons ; or (ii) damage to, or destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack* »[54]. Mais, à la définition générique d'arme, les auteurs de ce manuel ont donc ajouté la nécessité de

---

des vers ou des virus et qui permettent aux pirates d'accéder aux systèmes. La bombe logique, type particulier de cheval de Troie, ne s'active que lorsqu'une condition particulière est remplie et peut rester en sommeil dans un système pendant de longues périodes avant l'activation. On trouve enfin les trappes, mécanismes qui permettent à un programmeur d'accéder à des logiciels à tout moment à l'insu du propriétaire, et l'attaque par déni de services dont le but est de chercher à empêcher les utilisateurs légitimes d'accéder à des informations ou des services en bombardant le système de demandes de renseignements, l'obligeant ainsi à fermer le système.

[51] Il s'agit en effet plus précisément d'un équipement, instrument, code, programme informatique ou de toute donnée conçus ou spécialement adaptés afin d'accéder, ou se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données, de l'entraver ou d'en fausser le fonctionnement, d'introduire des données ou de modifier frauduleusement les données qu'il contient.

[52] HPCR, *Manual on International Law Applicable to Air and Missile Warfare*, Cambridge, Cambridge University press, 2013, p. 49.

[53] J.-M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law*, Cambridge, Cambridge University Press, 2005, vol. I, Rule 6, p. 23.

[54] *Tallinn Manual on the International Law Applicable to Cyber*, Cambridge, Cambridge University Press, 2013, p. 141.

qualifier d'attaque, au sens du droit international humanitaire, l'action menée par des capacités cybernétiques. Impliquant l'existence d'un conflit armé, elle présente l'inconvénient de ne déterminer ce qu'est une cyberarme qu'*a posteriori*[55], Ainsi, les différents moyens cybernétiques ne peuvent-ils pas tous être qualifiés d'armes. Seuls les techniques et outils informatiques conçus ou utilisés à des fins anti-personnelles ou anti-matérielles dans l'intention de porter atteinte aux intérêts vitaux d'un État pourront l'être. Dès lors, si rien n'empêche de qualifier les moyens cybernétiques d'arme, cela ne permet pas d'en déduire automatiquement qu'une cyberattaque constitue un emploi de la force armée.

III.2. Des incertitudes sur la qualification du recours à la force dans le cadre des cyber-opérations

Outre l'absence d'une réelle définition d'une cyberarme, le Manuel néglige le fait que toutes les cyber-opérations ne pourront pas *ipso facto* être qualifiées d'usage prohibé de la force armée, en n'envisageant pas la question de leur niveau de gravité. Il permet en effet de les qualifier d'opérations de police, d'usage de la force armée où enfin d'agression armée, seule hypothèse dans laquelle l'État victime sera autorisé à répondre en légitime défense. Les cyberattaques apparaissant le plus souvent comme des opérations limitées, circonscrites quant à la cible, à l'espace et au temps, c'est bien l'appréciation du critère de gravité, tel qu'il a été dégagé par la Cour Internationale de Justice[56] qui permettra de les qualifier en vertu de l'article 2 par. 4. La jurisprudence n'en donne pas, toutefois, une définition précise.

Selon la Cour, les critères suivants doivent être réunis afin de caractériser l'agression armée[57] : un critère subjectif ou d'intention : forcer l'État à faire ou ne pas faire quelque chose ; un critère objectif, déjà évoqué, sa gravité qui repose, soit sur la généralité des moyens mis en œuvre, soit sur des dommages si substantiels que l'acte ne peut être qualifié que de violation de l'article 2 par. 4. Pour retenir la gravité d'un acte, il conviendra donc de considérer les circonstances, notamment le milieu, l'espace dans lesquels la force a été déployée ainsi que l'activité menée aussi bien par la cible que par l'État recourant à la force armée. Un examen de la nature de la cible et du contexte permettra également d'éclairer l'analyse de l'activité. La Cour ne définit donc pas directement l'agression armée, elle procède par comparaison : l'agression est une forme particulière d'usage de la force[58] qui revêt une certaine dimension et produit certains effets[59], mais elle ne précise pas ce que recouvre ces deux termes. Dès lors, le terme « gravité » apparaît comme faussement clair et susceptible de diverses compréhensions[60].

La gravité peut renvoyer dans un premier temps à une acception objective liée à l'intensité ou aux conséquences matérielles de l'acte. Dans ce cas, la gravité dérivera, soit d'un des éléments suivants, ou plus sûrement d'une combinaison de ceux-ci : (i) spatialement, les actes

---

[55] Un tel élément s'avèrerait gênant dans le cadre d'une régulation de ces armes, que ce soit pour une interdiction ou pour un contrôle à l'exportation. En effet, il n'existerait pas vraiment de cyberarme par nature ; des moyens cybernétiques le deviendraient lors de leur utilisation dans un conflit armé.

[56] *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique), fond*, arrêt, *CIJ Recueil, 1986*, p. 14, par. 191.

[57] O. Corten, *Le droit contre la guerre. L'interdiction du recours à la force en droit international contemporain*, Paris, Pédone, 2008, p. 65 *sq*.

[58] J. A. Green, *The International Court of Justice and self-defence in international law*, Oxford, Hart Publishing, 2009, p. 31-41.

[59] *Activités militaires et paramilitaires au Nicaragua et contre celui-ci*, par. 195.

[60] T. Ruys, *« Armed attack » and Article 51 of the UN Charter: customary law and practice*, Cambridge, Cambridge University Press, 2010, p. 158.

se déroulent sur des espaces terrestres, maritimes ou aériens – voire cybernétique – importants ; (ii) temporellement, les actes se déroulent sur une période relativement longue ; (iii) quantitativement, les actes impliquent des opérations militaires massives, l'usage d'une arme ayant une puissance de destruction élevée ou provoquant des dommages substantiels ; (iv) qualitativement, les actes doivent infliger de nombreuses pertes humaines et matérielles[61].

Dans une seconde acception plus subjective, la gravité dérive de la nature de l'acte ou de la cible[62] (peu importe l'ampleur matérielle des conséquences) ou des effets immatériels de l'opération. Elle dépendrait alors de l'*animus agressionis*[63]. Certains actes démontreraient en eux-mêmes, peu importe leurs conséquences, la volonté hostile d'un État, ce qui peut s'avérer précieux dans la qualification des cyberattaques, leurs conséquences matérielles étant le plus souvent relativement faibles.

Deux situations émergent dès lors si l'on applique le critère de gravité aux cyberattaques. Dans la première, leur emploi s'insère dans un usage plus large de la force armée : il n'est alors qu'une arme parmi d'autres, ce qui ne soulève pas de difficulté particulière de qualification. Dans la seconde où elles sont utilisées pour des opérations ciblées, il en va tout autrement. De la même manière que le recours à une seule arme nucléaire constitue une agression armée, une seule cyberattaque peut-elle être considérée comme franchissant le seuil de gravité nécessaire à une telle qualification ? La réponse dépend du type d'opérations et notamment de la nature de la cible[64]. L'analyse ne peut donc être menée *in abstracto*, mais au regard des circonstances de chaque espèce.

Selon la position adoptée par le *Manuel*, les cyberattaques seraient assimilables à la force armée en vertu de leurs effets, peu importe la qualification donnée aux vecteurs utilisés. Il précise qu'une simple intrusion ou une opération dénuée d'effets physiques pourrait également constituer une violation de l'article 2 par. 4. « notamment au regard de l'origine de l'opération, de la nature de l'instigateur, du degré d'intrusion, des effets recherchés ou encore de la nature de la cible visée. Ainsi, le fait de pénétrer des systèmes militaires en vue d'atteindre les capacités de défense françaises pourrait être qualifié de recours à la force »[65]. Pour autant, « il n'est pas exclu qu'une cyberattaque puisse constituer une agression armée au sens de l'article 51 de la Charte des Nations unies, dès lors que ses effets et son ampleur atteignent une certaine gravité et sont comparables à ceux d'un emploi de la force physique »[66].

Le *Manuel* semble ainsi hésiter entre les deux modèles fondés sur les effets proposés par la doctrine. Le premier est qualifié d' « approche instrumentale » ou d'équivalence des effets. Il retient l'existence de la force armée chaque fois que les dommages causés par une cyberattaque n'auraient pu être obtenus auparavant que par une attaque cinétique[67]. Ainsi, une

---

[61] Y. Dinstein, *War, aggression, and self-defense*, 5th éd, Cambridge, Cambridge University Press, 2011, p. 12.

[62] Ainsi, la CIJ dans son arrêt *Plates-formes pétrolières* rappelle d'une part qu'au nombre des critères à respecter dans l'analyse de nécessité et de proportionnalité « [f]igure notamment au nombre de ces critères la nature de la cible contre laquelle la force a été employée au nom de la légitime défense », et d'autre part « le d'un seul navire de guerre puisse suffire à justifier qu'il soit fait usage du "droit naturel de légitime défense" ». *Plates-formes pétrolières* (République islamique d'Iran c. États-Unis d'Amérique), arrêt, CIJ Recueil 2003, par. 72 et 74.

[63] J. Spiropoulos, « Second Report on a Draft Code of Offences Against the Peace and Security of Mankind », *Yearbook of the International Law Commission*, 1951, vol. II, p. 67-68.

[64] *Plates-formes pétrolières* (République islamique d'Iran c. États-Unis d'Amérique), arrêt, C.I.J. Recueil 2003, par. 72.

[65] *Manuel,* p. 302.

[66] *Ibid.*, p. 303.

[67] D. B. Silver, « Computer Network Attack as a Use of Force Under Article 2 (4) of the United Nations Charter », p. 73-97 in *Computer Network attack and international law* sous la direction de M. N. Schmitt, B. T. O'Donnell, 2002.

cyberattaque ciblant un réseau électrique constituerait un emploi de la force armée, car le même résultat ne pouvait par le passé être obtenu que par des bombardements. Le deuxième modèle s'appuie sur une « approche fondée sur les conséquences ». Il détermine l'existence de la force armée à partir de l'effet global de l'attaque sur l'État victime, sans tenir compte des moyens cinétiques ou cybernétiques utilisés. Ainsi, en comparant les conséquences des cyberattaques à celles des attaques non cybernétiques, il permettrait une évolution du terme « force » sans évolution du corpus juridique existant[68]. Même si une cybermanipulation de l'information bancaire et financière d'un État ne ressemblerait en rien à une attaque cinétique, le préjudice global que cette manipulation de l'information causerait à l'économie de l'État victime justifierait que cette action soit assimilée à un emploi de la force armée.

Si la nature du vecteur utilisé importe peu, les effets de l'attaque sont donc importants dans l'« approche instrumentale » ou d'équivalence des effets puisque seules les cyberattaques produisant des effets cinétiques seront considérées comme des emplois de la force. Fondamentalement, les cyberattaques conduisent à se demander quels effets doivent être pris en compte dans l'analyse. Ceux-ci doivent-ils se limiter aux destructions physiques ? Les effets virtuels doivent-ils être intégrés ? Doit-on s'en tenir aux effets directs sur la cible ou tenir compte d'effets plus lointains ?

Marco Roscini a parfaitement démontré que les effets des cyberattaques étaient complexes à cerner pour deux séries de raisons[69]. D'une part, ils peuvent être de trois ordres. Les cyberattaques peuvent tout d'abord occasionner des effets primaires ou immédiats qui consistent, comme en Estonie en 2007 ou en Géorgie en 2008, en des destructions, la corruption ou l'altération de données qui entraîneront une perturbation du fonctionnement du système. Elles peuvent ensuite causer des effets secondaires, destructions ou neutralisation de la machine ou des infrastructures, comme l'a montré *Stuxnet*. Elles peuvent enfin engendrer des effets tertiaires qui se manifesteront par des dommages aux personnes suite aux deux premiers types d'effets. D'autre part, leur durée pouvait être soit permanente (perte irrémédiable de données) soit temporaire (fonctionnement normal du système après la fin de l'attaque en déni de service).

Le *Manuel* (dans le chapitre traitant de la proportionnalité dans le cadre du DIH) énonce que « l'évaluation des effets d'une cyber-opération prend en compte l'ensemble des dommages prévisibles de la cyber-arme, que ces derniers soient de type direct (comme les dommages sur l'équipement informatique directement visé, ou l'interruption du système) ou indirect (comme les effets sur l'infrastructure contrôlée par le système attaqué, mais également sur les personnes affectées par le dysfonctionnement ou la destruction des systèmes ou des infrastructures visées, ou par l'altération et la corruption de données de contenu) »[70]. La France semble ainsi adopter une appréciation large des effets à prendre en considération. Toutefois, cet ensemble de questions et la position française relèvent davantage de l'appréciation de l'intensité que de la nature armée de l'opération. En outre, s'en tenir aux effets pour caractériser les cyberattaques conduirait à écarter la violation de l'article 2 par. 4

[68] Michaël N. Schmitt propose que les effets de la cyberattaque soient mesurés à la lumière de sept critères : la gravité du dommage ; l'immédiateté de la réalisation du dommage ; la causalité directe entre l'attaque et le dommage ; la condition de pénétration sur le territoire de l'État victime qui doit être appliqué avec prudence : toute intrusion dans un système ne constitue pas un recours à la force armée ; le degré de prévisibilité du dommage ; le fait que toute action cyber est présumée licite, la légitime défense consécutive à une cyberattaque ne doit être qu'une exception ; l'attribution de la cyberattaque à un État selon les règles de la responsabilité internationale. M. N. Schmitt, « Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework », *Columbia Journal of Transnational Law*, 1999, vol. 37, p. 885-937.

[69] M. Roscini, *Cyber Operations and the Use of Force in International Law*, *op. cit.*, p. 52-53.

[70] *Manuel,* p. 311.

de la Charte dès lors que l'attaque n'a pas produit d'effet. Or, l'article 2 par. 4 prohibe non seulement l'emploi, mais aussi la menace de l'emploi de la force.

En application de la thèse fondée sur les conséquences, proposée par Michaël N. Schmitt – qui semble être majoritaire –, deux questions relatives aux dommages se posent. La première résulte du fait que les auteurs adoptant cette position ne parviennent pas à s'entendre sur la détermination du seuil de dommage à partir duquel une cyberattaque peut être qualifiée d'agression armée, ce qui illustre le caractère vague du critère de gravité retenu par la CIJ. Les dommages doivent-ils être le résultat d'un certain niveau de violence, comme ceux résultant d'un bombardement aérien[71] ? Une réponse positive conduirait à retenir la qualification d'agression armée si, par exemple, un aéronef civil s'écrasait à la suite d'une cyberattaque du système informatique du contrôle aérien, et à repousser une telle qualification si les dommages occasionnés se limitaient à une atteinte au système économique provoquant une perte de liquidité. La seconde question conduit à se demander si les dommages, quelle que soit leur nature, doivent être importants. Une réponse affirmative permettrait ainsi de tenir compte de la dépendance actuelle de la société moderne aux systèmes d'information impliquant que des moyens non cinétiques puissent être aussi destructeurs que le recours à des armes classiques[72]. La difficulté est cependant de déterminer la signification d' « important ». Pour les États-Unis, par exemple, le déni de service, dont l'objectif est d'empêcher un système de fournir le service attendu ou, au moins, d'en limiter fortement la capacité en le saturant d'informations ou de communications, justifierait une action en légitime défense[73]. Une telle position ne semble toutefois pas correspondre à l'économie générale du régime de la légitime défense commandée par l'urgence. Afin de limiter les possibles excès du recours à cette thèse, la majorité des auteurs soutiennent l'approche fondée sur les conséquences, même si elle est perfectible, car elle ne tire pas tous les effets de l'introduction des « armes » cybernétiques et qu'elle ne prend pas en compte l'ensemble des effets de telles attaques.

L'autre modèle fondé sur les effets – équivalence des effets – permet de s'interroger par exemple sur la différence entre la destruction de la défense aérienne d'un État par moyens cinétiques qui serait constitutive d'une agression armée, et sa destruction par un virus qui ne constituerait pas toujours une agression armée. En vertu du modèle « d'équivalence des effets », une cyberattaque pourrait ainsi être qualifiée d'agression armée en utilisant le critère de l'identité des résultats opérationnels[74]. Il est cependant reproché à cette thèse d'être trop permissive, car, en qualifiant une action d'agression armée sans qu'il y ait dommage physique, elle s'éloignerait trop du régime prévu par la Charte. Cependant, le mérite de cette thèse, en tirant toutes les conséquences de la position de l'équivalence des effets, est d'englober l'ensemble des dommages issus des cyberattaques,

L'idée de qualifier les cyberattaques à partir de leurs seuls effets ne nous semble néanmoins pas pertinente. Une troisième voie est souvent envisagée : une qualification fondée sur le type de cible, les États déduisant de la cible de l'opération la nature de l'acte[75]. Cette idée se retrouve à partir de 2011 dans les déclarations des autorités américaines pour lesquelles une cyberattaque pourrait être qualifiée d'usage de la force armée, voire d'agression armée, dès lors qu'elle ciblerait des infrastructures vitales[76]. Elles recouvrent les secteurs étatiques

---

[71] M. C. Waxman, *op. cit.*, p. 435.

[72] *Ibid.*, p. 436.

[73] *Ibid.*, p. 423.

[74] S. Li, « When Does Internet Denial Trigger the Right of Armed Self-Defense ? », *The Yale Journal of International Law*, 2013, vol. 38, pp. 179-216.

[75] S. Gosnell Handler, « The New Cyber Face of Battle : Developing a Legal Approach to Accommodate Emerging Trends in Warfare », *Stanford Journal of International Law*, 2012, vol. 48, p. 209-237.

[76] *Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934*, 2011, p. 9.

(activités civiles, judiciaires, militaires, de recherche, de l'État), des secteurs liés à la protection de la population (santé, eau, alimentation) et des secteurs de la vie économique et sociale de la Nation (énergie, communication, transport, finance et industrie). En France, douze secteurs ont ainsi été identifiés comme étant d'importance vitale dont l'indisponibilité risquerait de diminuer de manière importante le potentiel militaire ou économique, la sécurité ou la capacité de survie de la Nation[77]. Le caractère large et automatique de cette approche présente toutefois l'inconvénient de faire potentiellement peser des risques sur la stabilité des relations internationales.

La dernière voie concevable est celle d'une définition à partir de l'objectif de l'opération, qui est toujours de contraindre un État. L'avantage est qu'un tel critère permettrait de distinguer les cyberattaques assimilables à un emploi de la force armée de celles qui relèvent, par exemple, de l'espionnage. Son inconvénient évident est qu'il signifierait le retour de l'*animus belli* qui est critiqué pour son caractère subjectif.

L'utilisation combinée des critères de l'objectif de l'opération et de l'équivalence des effets permettrait certainement une qualification objective d'une cyberattaque. Une lecture attentive du *Manuel* laisse penser que la position française adopte une telle approche plutôt que celle uniquement fondée sur les effets. Par exemple, l'emploi d'un virus informatique par un État dans le but de détruire l'ensemble du réseau électrique d'un autre État avec lequel il a de nombreux différends de frontières, pourra être considéré comme un usage de la force armée, car l'idée de contrainte par l'emploi d'un système d'arme ayant vocation à détruire, même si ce n'est pas physiquement, une infrastructure vitale, répond à la définition de la force armée.

Notre hypothèse, fondée sur la nécessité d'une vision pragmatique du droit international et la reconnaissance de son caractère politique, est que l'interprétation va dépendre des objectifs des acteurs (États, Organisations internationales, groupes armés). Si le principe de protection de la paix et de la sécurité internationale est mis en avant, l'interprétation devra être restrictive. Ces opérations pourraient ainsi être qualifiées d'atteinte à la souveraineté, de mesure de police ou encore de violation de l'article 2 par. 4, non d'agression armée, relevant ainsi leur illicéité tout en évitant une escalade de la violence qu'entrainerait éventuellement l'emploi de la force en légitime défense. À l'inverse, si le principe de protection de l'État devait être favorisé, alors le seuil d'intensité retenu pourrait être plus faible afin de permettre la qualification d'agression armée des cyberattaques,

Le *Manuel*, en s'abstenant d'expliciter clairement l'argumentation juridique française sur l'agression armée dans le cadre des cyber-opérations, manque donc l'occasion d'exprimer une position permettant d'assurer en même temps la sécurité des États et la sécurité internationale. Au contraire, ses positions relatives à la légitime défense constituent des atteintes potentielles à l'architecture du *jus contra bellum*.

IV. Une extension discutable de la légitime défense

Le *Manuel* reconnaît trois extensions possibles de la légitime défense : la légitime défense préemptive[78] (IV.1), la théorie de l'accumulation des événements (IV.2) et la légitime défense contre des groupes armées non étatiques (IV.3).

[77] Ces secteurs d'activités ont été définis dans un arrêté du 2 juin 2006 modifié par un arrêté du 3 juillet 2008. Ils sont désignés par arrêté du ministre coordonnateur pour chaque secteur d'importance vitale parmi les opérateurs publics ou privés (articles L. 1332-1 à L. 1332-7, L. 2151-1 à L.2151-5 et R. 1332-1 à R. 1332-42 du Code de la Défense).

[78] *Manuel,* p. 305.

IV.1. La confirmation de l'extension de la légitime défense préemptive

Si le *Manuel* rappelle que la légitime défense préventive, c'est-à-dire, avant tout projet d'action, est toujours illicite, il considère par contre, citant comme seule source un rapport du SGDN, que la légitime défense préemptive qui précède immédiatement l'attaque est licite.

Les cyberattaques rendent toutefois complexe la reconnaissance de leur licéité[79]. L'idée de la légitime défense anticipée est d'autoriser un État à agir, en cas d'attaque imminente, avant l'exécution de l'attaque. L'imminence[80] se déduirait de deux critères : une menace immédiate et clairement identifiable[81]. Malgré cette précision, cette notion souffre d'une incertitude[82]. Deux acceptions se dégagent en doctrine. La légitime défense anticipée ne serait autorisée que si la réponse intervient juste avant le moment où l'attaque est sur le point d'être lancée. Dans le contexte d'une cyberattaque, cette interprétation rend sans objet la légitime défense anticipée, car déterminer un tel moment est quasiment impossible. Le *Manuel de Tallinn*, sous l'impulsion de Michael N. Schmitt, a retenu dans sa règle 73 la théorie de la « dernière fenêtre d'opportunité » qui signifie qu' « a State may act in anticipatory self-defence against an armed attack, whether cyber or kinetic, when the attacker is clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively defend itself unless it acts »[83]. Le moment de l'action, juste avant l'attaque ou longtemps avant celle-ci, dépendra du fait de savoir, d'une part si la réalisation de l'attaque conduirait à des dommages permettant de la qualifier d'agression armée, et d'autre part de la possibilité pour l'État potentiellement victime de l'éviter efficacement.

Le problème de la première interprétation est que, dans le cadre des cyberattaques, il n'existe pas de manœuvres visibles justifiant l'action. Les États, le plus souvent, ne pourront pas savoir quand une cyberattaque sera déclenchée parce que le temps qui s'écoule entre le moment où elle est lancée et le moment où elle atteint sa cible sera minime[84]. Dès lors, le recours à la légitime défense anticipée serait peu pertinent. La seconde interprétation semble fusionner légitime défense anticipée et préventive. Si la légitime défense est autorisée à partir de la détection de l'intrusion ou de l'exécution du code, une réponse dès la planification paraît alors conduire à une extension dangereuse de l'emploi de la force pour la sécurité internationale. Quelle que soit l'hypothèse envisagée, reste toutefois le problème de la qualification d'agression armée : l'adoption de la théorie de l'équivalence des effets ne permettrait pas de la justifier car elle repose sur une analyse *a posteriori*.

De nouvelles interrogations relatives à la légitime défense se posent avec l'apparition du concept de cyberdéfense active[85] entendue comme l'ensemble des actions défensives directes adoptées pour détruire, annuler ou réduire l'efficacité des cybermenaces contre des forces et des moyens « amis » ; en d'autres termes, la défense active doit être comprise comme une

---

[79] R. Hayward, « Evaluating 'Imminence' of a Cyber Attack for Purposes of Anticipatory Defense », *Columbia Law Review*, 2017, vol. 117, p. 399-434.

[80] *Ibid.*, p. 407-434.

[81] N. Lubell, « The Problem of Imminence in an Uncertain World », p. 695 in *The Oxford Handbook of the Use of Force in International Law*, M. Weller (éd.), Oxford University Press, 2015.

[82] D. Bethlehem, « Self-Defense Against an Imminent or Actual Armed Attack by Non state Actors », *The American Journal of International Law*, 2012, vol. 106, n° 4, p. 769-777.

[83] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., M. N. Schmitt (éd.), Cambridge University Press, Cambridge, p. 350.

[84] A. L. Schuller, « Inimical Inceptions of Imminence : A New Approach to Anticipatory Self-Defense Under the Law of Armed Conflict », *UCLA Journal of International Law and Foreign Affairs*, 2014, vol. 18, n° 2, p. 161-206.

[85] « Le cadre juridique de la cyberdéfense active », *Défense et Sécurité Internationale*, Hors-série n° 52, 2017, p. 34-37.

action agressive contre la source de l'attaque[86]. Dans un sens étroit, la cyber-défense active peut s'entendre comme une réponse pour mettre un terme ou pour éviter une nouvelle perturbation du système, mais dans un sens plus large, elle pourrait conduire à lancer des cyberattaques pour prévenir une attaque future. Ce concept justifierait une riposte automatique à une cyberattaque, impliquant potentiellement des systèmes informatiques autonomes, sans intervention humaine[87]. Or, la légitime défense active pose de nombreuses questions juridiques, notamment si la réponse s'effectue durant l'attaque. Le concept semble mal s'assortir avec la théorie des conséquences, car le plus souvent les effets de la cyberattaque ne pourront pas être déterminés durant sa réalisation. La condition nécessaire au déclenchement de la légitime défense, à savoir l'existence d'une agression armée semble en outre faire défaut, sauf à imaginer que la cyberdéfense active puisse être assimilée à la légitime défense anticipée. Toutefois, même dans ce cas-là, elle paraît se heurter au problème de l'attribution de l'attaque, une réponse en légitime défense ne pouvant se contenter de présomptions plus ou moins biaisées.

IV.2. La reconnaissance contestable de la licéité de la théorie de l'accumulation d'évènements

Conformément à la position du *Tallinn Manual 2.0*[88], le *Manuel* fait sienne la théorie de l'accumulation d'événements[89]. Il précise en effet que « les cyberattaques qui, isolément, n'atteignent pas le seuil de l'agression armée pourraient être qualifiées comme telles si l'accumulation de leurs effets atteignait un seuil de gravité suffisant »[90].

Les cyberattaques posent en effet cette question de manière renouvelée : est-il possible de qualifier un ensemble d'actions conduites dans le cyberespace d'agression armée en appliquant la théorie de l'accumulation d'événements selon laquelle une agression armée est constituée par la réalisation d'un ensemble d'actes reliés par une même logique. Alors que des actions multiples, considérées individuellement, ne constitueraient pas une agression armée, elles pourraient cependant être qualifiées ainsi dès lors que serait pris en compte l'ensemble du plan d'agression qui relie chacune des actions. La théorie de la stratégie d'agression complexe ou doctrine de l'accumulation des événements[91] est particulièrement intéressante

---

[86] D. E. Denning, B. J. Strawser, « Active Cyber Defense : Applying Air Defense to the Cyber Domain », p. 64-75 in *Cyber Analogies*, J. Arquilla, E. O. Goldman (éd.), Technical Report sponsored by United States Cyber Command, Monterey, Department of Defense Information Operations Center for Research, Naval Postgraduate School, 2014.

[87] F. Grimal, J. Sundaram, « Cyber warfare and autonomous self-defence », *Journal on the Use of Force and International Law*, 2017, vol. 4, n° 2, p. 312-343.

[88] M.N. Schmitt (éd.), *Tallinn manual 2.0 on the international law applicable to cyber operations*, 2e éd., Cambridge, Cambridge University Press, 2017, p. 342.

[89] Opinion dissidente de M. le juge Stephen M. Schwebel, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique), fond*, arrêt, *CIJ Recueil, 1986*, p. 268-269 : « Au regard du droit international coutumier et du droit international conventionnel, ces actes de subversion nicaraguayens sont d'une ampleur telle qu'ils ne font pas que constituer une intervention illicite dans les affaires d'El Salvador ; ils équivalent en plus à une agression armée contre El Salvador ». Enzo Cannizzaro, « Contextualisation de la proportionnalité : jus ad bellum et jus in bello dans la guerre du Liban », (2006) RICR, 88:864, p. 275-290.

[90] *Manuel,* p. 303.

[91] Selon cette théorie, la répétition d'attaques provenant d'une même source à l'encontre d'un même État dans un certain laps de temps pourrait constituer une agression armée au sens de l'article 51. On trouve cette idée dans l'arrêt *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique)* de 1986 « Au regard du droit international coutumier et du droit international

dans le cadre des cyberattaques, car elles peuvent être nombreuses et de faible intensité, mais commises dans l'idée de porter atteinte à un État par leur répétition. Cette condition de la répétition souligne, en outre, que le seuil quantitatif est insuffisant pour conclure à une agression armée. Pour l'heure, en droit, cette théorie n'est ni acceptée ni rejetée par la Cour International de Justice[92]. La multiplication des actes hostiles au moyen des nouvelles technologies pourrait peut-être faire évoluer sa jurisprudence quoique l'on puisse en douter[93]. Cette théorie souffre, en effet, d'une limite : l'absence de gravité des attaques prises individuellement. Sans modification du droit positif, retenir cette théorie permettrait un accroissement du recours à la force en légitime défense, ce qui est contraire au but et à l'esprit du *jus contra bellum* depuis 1945.

IV.3. Une assimilation discutée des attentats terroristes à une agression armée

La puissance de certaines forces militaires non étatiques obligerait à une relecture du *jus ad bellum* en particulier de l'article 51 de la Charte des Nations Unies. Ainsi, en 2007, dans sa Résolution sur la légitime défense, l'Institut De Droit International (IDI) énonce qu'en « cas d'attaque armée d'un État par un acteur non étatique, l'article 51 de la Charte, tel que complété par le droit international coutumier, s'applique en principe »[94].

Deux situations peuvent être distinguées. D'une part, l'agression armée indirecte se définit comme l'agression commise par un État par l'intermédiaire d'un acteur non étatique. Cette hypothèse, qui soulève principalement des problèmes d'imputations, ne nous intéresse pas ici. Le *Manuel* s'intéresse à la deuxième hypothèse dans laquelle l'action de l'acteur non étatique constituerait la source autonome de l'agression armée[95]. Les rédacteurs du *Manuel* notent ainsi qu' « à la suite des attentats perpétrés à Paris le 13 novembre 2015, la France a également invoqué la légitime défense individuelle comme fondement de son intervention en Syrie »[96]. Ce faisant, elle a qualifié les attentats d'agression armée au sens de l'article 51 de la Charte alors qu'ils n'étaient pas le fait d'un État, par un étirement inédit de la conception française de la légitime défense, fondée sur un faisceau de trois critères. Ils résultent des caractéristiques exceptionnelles de Daech, « groupe armé dont la gravité des attaques a été qualifiée de menace à la paix et la sécurité internationale par la résolution 2170 (2014) adoptée par le Conseil de sécurité sur le fondement du chapitre VII, à ses capacités militaires, son degré d'organisation, l'ampleur inédite du territoire placé sous son contrôle […], aux termes de la résolution 2249 (2015) et enfin à la certitude selon laquelle ces attentats avaient été fomentés à Raqqa »[97].

---

conventionnel, ces actes de subversion nicaraguayens sont d'une ampleur telle qu'ils ne font pas que constituer une intervention illicite dans les affaires d'El Salvador ; ils équivalent en plus à une agression armée contre El Salvador ».

[92] Voir par exemple *Plates-formes pétrolières* (République islamique d'Iran c. États-Unis d'Amérique), arrêt, C.I.J. *Recueil 2003*, p. 191, par. 64. La Cour écrit que « A supposer que tous les incidents dénoncés par les États-Unis doivent être attribués à l'Iran, et laissant par conséquent de côté la question examinée plus haut de l'attribution à celui-ci de l'attaque menée contre le *Sea Isle City*, la question est de savoir si cette attaque, prise isolément ou dans le cadre de la "série d'attaques" invoquée par les États-Unis, peut être qualifiée d'"agression armée" contre les États-Unis, agression qui justifierait le recours à la légitime défense ».

[93] *Final Report on Aggression and the Use of Force*, International Law Association, Sydney, 2018, p. 7.

[94] 10A Résolution Institut De Droit International Session de Santiago – 2007, 27 octobre 2007, *Problèmes actuels du recours à la force en droit international : Légitime défense*.

[95] F. Latty, « Le brouillage des repères du *jus contra bellum*. À propos de l'usage de la force par la France contre Daech », *Revue générale de droit international public*, 2016/1, p. 11-39.

[96] *Manuel,* p. 74.

[97] *Manuel,* p. 74.

Afin de justifier ses actions, la France participe ainsi à l'entreprise d'étirement de l'article 51 de la Charte, fragilisant l'architecture du *jus contra bellum*. En effet, une réponse en légitime défense contre Daech n'était licite que si les actes de Daech étaient rattachables à la Syrie – ce qui est exclu – ou si Daech constituait un État – qualité qui lui était déniée par la Communauté internationale. Daech demeurait donc un groupe terroriste ne relevant pas de l'article 51[98] œuvrant sur le territoire syrien dont les frontières et le gouvernement – même contesté – obligeait la France à demander l'autorisation aux autorités syriennes avant toute opération militaire.

La qualification d'agression armée du fait des attentats du 13 novembre 2015 restant incertaine, le *Manuel*, dans sa note 1072, précise que « La France a invoqué exceptionnellement la légitime défense à l'encontre d'une agression armée menée par un acteur présentant les caractéristiques d'un quasi-État, lors de son intervention en Syrie face au groupe Daech. Ce cas exceptionnel ne saurait constituer l'expression définitive d'une reconnaissance de l'extension du droit à la légitime défense à l'encontre d'une agression non imputable à un État »[99]. Malgré l'argumentation adoptée, la position formulée et les actions qui l'ont suivie constituent un précédent qui pourrait être utilisé au profit de futures tentatives d'élargissement de la légitime défense.

Le *Manuel* rappelle également que l'intervention française en Syrie à compter de septembre 2015 reposait sur le fondement de la légitime défense collective de l'Irak, attaqué par Daech depuis le territoire syrien. La légitime défense collective se réfère principalement au droit bien établi des États, en vertu de la Charte des Nations unies, de défendre d'autres États. Comme il a été rappelé dans son arrêt *Nicaragua,* la CIJ exige le consentement de l'État victime aux actions militaires. Or, plusieurs lettres du gouvernement syrien au Conseil de sécurité démontre l'inexistence d'un tel consentement[100]. Les autorités françaises semblent

---

[98] Une telle interprétation peut trouver un soutien dans les déclarations interprétatives françaises au Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977, du 11/04/2001 dans laquelle le gouvernement énonce qu'il « considère que le terme 'conflits armés' évoqué au paragraphe 4 de l'article 1, de lui-même et dans son contexte, indique une situation d'un genre qui ne comprend pas la commission de crimes ordinaires, y compris les actes de terrorisme, qu'ils soient collectifs ou isolés » (par. 4).

[99] *Manuel,* p. 303.

[100] Lettres identiques datées du 17 septembre 2015, adressées au Secrétaire général et au Président du Conseil de sécurité par le Représentant permanent de la République arabe syrienne auprès de l'Organisation des Nations Unies, S/2015/719, 21 septembre 2015 :

La France, la Grande-Bretagne et l'Australie disent prendre ces mesures à la demande de la République d'Iraq en soutien à son droit de légitime défense. À cet égard, le Gouvernement syrien souhaite expliquer ce qui suit :

• La Syrie s'étonne que certains États, dont des membres permanents du Conseil de sécurité, violent le droit international et la Charte des Nations Unies et aient la témérité d'expliquer leurs actes en altérant sciemment le libellé de ce paragraphe charnière, au risque de provoquer la guerre et le chaos dans le monde entier. La Syrie n'a formulé aucune requête de ce type. Le Conseil a adopté dans le cadre de la lutte contre le terrorisme en Syrie de nombreuses résolutions, que les États Membres de l'Organisation sont tenus de respecter;

• Toute présence militaire sur le territoire syrien ou par voie aérienne, terrestre ou maritime sous prétexte de lutter contre le terrorisme et qui ne recueille pas l'aval du Gouvernement syrien sera considérée comme une violation de la souveraineté nationale. La lutte contre le terrorisme sur le sol syrien doit se faire en coopération et en coordination étroites avec le Gouvernement, conformément aux résolutions du Conseil de sécurité relatives à la lutte contre le terrorisme;

• La Syrie souligne que le Royaume-Uni, l'Australie et la France doivent respecter les résolutions du Conseil de sécurité, tout particulièrement ses résolutions 2170 (2014), 2178 (2014) et 2199 (2015), dans lesquelles il réaffirme la nécessité pour les États de respecter l'unité, la souveraineté et l'intégrité territoriale de la République arabe syrienne, et cesser d'interpréter délibérément à mauvais escient l'Article 51 de la Charte des Nations Unies.

justifier le recours à l'exception de légitime défense collective par le consentement de la Coalition nationale syrienne, représentant légitime de l'État syrien. Pourtant, la CIJ dans son arrêt *Nicaragua* a clairement énoncé que « le principe de non-intervention […] perdrait assurément toute signification réelle comme principe de droit si l'intervention pouvait être justifiée par une simple demande d'assistance formulée par un groupe d'opposants »[101]. En outre, cette argumentation ne peut être acceptée du fait de l'absence d'effectivité du pouvoir détenu par ce groupe. Dans les cas de concurrence de « gouvernement », il existerait une obligation de s'abstenir. Cette position, défendue par l'article 2 de la résolution de l'IDI de 1975, repose notamment sur le principe d'effectivité du gouvernement qui ferait défaut, empêchant l'expression d'un consentement valide à l'intervention d'un État tiers. Dès lors, l'abstention serait la seule solution permettant, en ne prenant partie pour aucun des deux camps, de respecter le principe de non intervention, qui protège tout l'État et pas seulement le gouvernement, ainsi que le droit des peuples à disposer d'eux-mêmes[102].

V. Conclusion

Si l'entreprise de rédaction du *Manuel* doit être saluée, elle doit être également bien comprise. Sa fonction première est d'expliciter et de faire connaître la position de la France sur le droit des conflits armés. Ses destinataires sont les militaires, dont on peut penser que la grande majorité en maîtrisent déjà les principes, et les citoyens civils qu'il est indispensable d'éclairer sur les conditions de l'usage de la force armée sur le territoire national comme sur les théâtres extérieurs. On peut en tirer deux conséquences. Bien qu'appuyé sur un appareil scientifique important, le *Manuel* n'est pas destiné à faire œuvre doctrinale en discutant tous les aspects juridiques du droit des conflits armés. Il est plutôt une illustration particulièrement éclairante, dans le domaine retenu, des principes et instruments de la « politique juridique extérieure » de la France[103]. C'est à ce titre qu'il doit susciter légitimement la discussion, non pas tant sur le droit international humanitaire et sur l'emploi des forces armées sur le territoire national, que sur le *jus ad bellum,* domaine dans lequel la « politique juridique » est beaucoup plus prégnante. Sur ce point, les conclusions reflétant la position française semblent s'orienter vers une interprétation plus souple des exigences du *jus ad bellum* traduisant une forme d'alignement sur les positions des États-Unis en la matière[104] et faisant craindre un retour à l'autoprotection[105]. Exprimant une position juridique officielle appuyée sur la pratique, elle pourrait fournir un prétexte à d'autres États pour délégitimer l'action de la France et ainsi menacer l'intégrité du *jus contra bellum* et par là même, la paix et la sécurité internationale.

---

[101] *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique), fond*, p. 126, par. 246.

[102] Résolution de 1975 relative au « principe de non-intervention dans les guerres civiles » : *Considérant*, en particulier, que la violation du principe de la non-intervention en faveur d'une partie à la guerre civile mène souvent, en pratique, à l'ingérence en faveur de la partie opposée.

[103] On renvoie ici à l'étude magistrale de G. de Lacharriere, « La politique juridique extérieure », Paris, Economica, 1983 et au commentaire de R. Kolb, « Réflexions sur les politiques juridiques extérieures », Paris, Pedone, 2015, 138 p.

[104] R. Kolb, « Quelques réflexions sur le droit relatif au maintien de la paix au début du XXIe siècle », *African yearbook of international law*, 2004, vol. 12, p. 193-215.

[105] N. Boyd, « Erich Kaufmann et la théorie hégélienne du droit international », É. Djordjevic (éd.), *Hegel et le droit*, Éditions Panthéon-Assas, 2023, p. 147-170.