Volume 101 Sélection française 2019/1

REVUE INTERNATIONALE de la Croix-Rouge

La guerre 3.0 par le biais des réseaux de communication : protéger la population civile pendant les cyberopérations

Michael N. Schmitt*

Michael N. Schmitt est membre du Comité éditorial de la *Revue*. Il est professeur de droit international public à l'Université d'Exeter et professeur émérite du Naval War College aux États-Unis. Il est également un éminent chercheur de l'Académie militaire des États-Unis (West Point) et directeur de publication du *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Manuel de Tallin 2.0 sur le droit international applicable aux cyber opérations)*.

Traduit de l'anglais

Résumé

D'une manière générale, le droit international humanitaire est à même de procurer le cadre juridique des cyberopérations pendant un conflit armé. Cependant, ce n'est qu'une fois que seront résolues deux questions qui sont encore pendantes, qu'il sera possible de déterminer avec précision le niveau de protection dont la population civile bénéficiera pendant les cyberopérations. La première a trait au sens du terme « attaque » dans les diverses règles relatives à la conduite des hostilités, tandis que la seconde porte sur le point de savoir si les données peuvent être considérées comme des biens, de façon à ce que les opérations qui les détruisent ou les altèrent soient soumises à l'interdiction d'attaquer des biens de caractère civil et si, ce faisant, leurs effets doivent être pris en considération lors de l'évaluation de la proportionnalité et des précautions à prendre dans l'attaque. Même si ces questions étaient tranchées,

* Les opinions exprimées dans cet article le sont à titre personnel. L'auteur est reconnaissant au Lieutenant Colonel Jeffrey Biller (Forces aériennes des États-Unis) de ses commentaires extrêmement précieux.

la population civile resterait exposée aux risques induits par les cyberopérations dont les capacités d'action sont inédites. Le présent article propose deux doctrines que les parties à un conflit devraient envisager d'adopter pour atténuer ces risques. Elles partent l'une comme l'autre du principe que les opérations militaires doivent être le fruit d'un équilibre entre les enjeux militaires et l'intérêt des États à dominer le conflit.

Mots clés : cyberopérations, attaques, données, biens de caractère civil, proportionnalité, précautions dans l'attaque, nécessité militaire.

Lors des travaux du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale (GGE-NU) en 2016–2017, le refus de la Russie, de la Chine et d'un certain nombre d'autres États de reconnaître expressément l'applicabilité du droit international humanitaire (DIH) aux cyberopérations, a profondément miné les efforts visant à préciser dans quelle mesure ces opérations sont encadrées par le droit international[1]. Ce refus était particulièrement étonnant compte tenu du fait que deux ans auparavant, le précédent GGE, dont la Russie et la Chine étaient membres, avait qualifié « les principes d'humanité, de nécessité, de proportionnalité et de discrimination » de « principes de droit international reconnus[2] », déclaration qui ne peut être interprétée autrement que comme une acceptation de ce que le DIH régit la conduite des cyberhostilités pendant les conflits armés.

D'un point de vue juridique, ce refus est déconcertant. Le fait que le DIH s'applique aux cyberopérations pendant un conflit armé fait l'objet d'un large consensus. C'est la position des principales cyberpuissances comme les États-Unis[3] ; d'organisations internationales comme l'OTAN et l'Union européenne[4] ; du Comité

1 Michael N. Schmitt et Liis Vihul, « International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms », *Just Security*, 30 juin 2017, disponible sur : www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

2 Groupe d'experts gouvernementaux des Nations Unies, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, document des Nations Unies A/70/174, 22 juillet 2015, par. 28 d).

3 Brian J. Egan, conseiller juridique, Département d'État des États-Unis, « Remarks on International Law and Stability in Cyberspace », 10 novembre 2016, disponible sur : https://perma.cc/B6TH-232L. Voir également « Applicability of International Law to Conflicts in Cyberspace », *Digest of United States Practice in International Law*, 2014, chap. 18, section A(3)(b), p. 737 ; Harold Koh, conseiller juridique, Département d'État des États-Unis, « International Law in Cyberspace », observations présentées lors d'une conférence juridique interinstitutionnelle sur le cybercommandement aux États-Unis, 18 septembre 2012. Au sujet de la déclaration de Koh, voir Michael N. Schmitt, « International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed », *Harvard Journal of International Law Online*, vol. 54, 2012.

4 Conseil de l'Atlantique Nord, *Déclaration du sommet du Pays de Galles*, 5 septembre 2014, par. 72, disponible sur : www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=fr. Voir également Commission européenne, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7 février 2013, p. 72.

international de la Croix Rouge (CICR)[5] ; et de la plupart des universitaires[6]. Le consensus repose en partie sur la pratique des États, lesquels reconnaissent depuis longtemps que les nouveaux moyens et méthodes de guerre sont soumis aux interdictions, limitations et obligations que l'on trouve dans les règles du DIH relatives à la conduite des hostilités et dans celles relatives aux armes[7]. Par exemple, dans son avis consultatif sur les *armes nucléaires*, la Cour internationale de Justice a confirmé l'applicabilité du DIH aux nouvelles armes[8]. En outre, l'article 36 du Protocole additionnel I aux Conventions de Genève de 1949 (PA I) impose aux parties « dans 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 ... 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[9] ». Même des États qui ne sont pas parties au PA I reconnaissent la nécessité de veiller à ce que les nouvelles armes, notamment les armes cybernétiques, soient conformes aux dispositions existantes du DIH[10]. Enfin, la simple logique veut que le DIH s'applique aux nouveaux modes de conduite des hostilités, étant donné que presque chaque conflit s'accompagne de nouvelles armes, tactiques et caractéristiques opérationnelles. Il serait absurde de considérer que seuls les moyens et méthodes de guerre antérieurs à l'adoption d'un traité ou à la cristallisation d'une norme de droit coutumier, sont soumis aux principes et aux règles qui y sont énoncés[11].

Dès lors, il ne s'agit pas tant de s'interroger sur le point de savoir si le DIH s'applique aux cyberopérations menées lors d'un conflit armé, mais de se demander comment il s'applique. Dans la plupart des cas, l'application est incontestable. Ce n'est vraiment pas une révélation jurisprudentielle que de conclure, par exemple, qu'une cyberopération visant des civils, causant des morts, des dommages et des

5 CICR, « Cyberwarfare and International Humanitarian Law: The ICRC's Position », juin 2013, p. 2, disponible sur : www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf. Voir aussi CICR, « Quelles limites le droit de la guerre impose-t-il aux cyberattaques ? Questions & réponses, 28 juin 2013, disponible sur : https://www.icrc.org/fr/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

6 Voir, par exemple, Michael N. Schmitt (dir.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013, règle 20 ; Michael N. Schmitt (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Manuel de Tallinn 2.0), règle 80.

7 William H. Boothby, *Weapons and the Law of Armed Conflict*, Oxford University Press, Oxford, 2009, pp. 340-341 ; CICR, *Guide de l'examen de la licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre*, janvier 2006, pp. 3-4.

8 Cour internationale de Justice (C.I.J.), *Licéité de la menace ou de l'emploi d'armes nucléaires*, Avis consultatif du 8 juillet 1996, *C.I.J. Recueil 1996*, par. 85-86.

9 Protocole additionnel I aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux, RTNU, vol. 1125, p. 3, 8 juin 1977 (PA I), art. 36.

10 Bureau du conseiller général, Département de la Défense des États-Unis, *Law of War Manual*, éd. révisée, décembre 2016 (Manuel du droit de la guerre des États-Unis), par. 16.6 ; Forces aériennes des États-Unis, *Legal Review of Weapons and Cyber Capabilities*, Instruction des Forces aériennes 51-402, 27 juillet 2011.

11 Pour une excellente étude exhaustive des questions de DIH découlant des cyberopérations, voir Cordula Droege, « Sortez de mon "Cloud": la cyberguerre, le droit international humanitaire et la protection des civils », *Revue internationale de la Croix-Rouge*, vol. 94, n° 886, *Sélection française* 2012/2.

destructions, non seulement viole le DIH[12], mais qu'en plus, elle constitue un crime de guerre, que ce soit dans un conflit armé international ou non international[13]. De même, les cyberattaques sont bien évidemment limitées par le principe de proportionnalité[14] et l'obligation de prendre des précautions dans l'attaque[15].

Il reste néanmoins un certain nombre de points qui ne sont pas réglés. Dans cette zone grise, deux questions dont la réponse aura d'importantes conséquences pour les populations civiles, restent pendantes. Les deux sont des questions de définition. La première concerne le champ du mot « attaque ». Il s'agit là d'un aspect capital s'agissant de cyberopérations, car diverses interdictions, limitations et obligations du DIH ne s'appliquent qu'aux opérations qui répondent à la définition d'une attaque[16]. La seconde question a trait au sens du mot « bien ». S'agissant des cyberopérations, il s'agit de savoir si une cyberopération qui détruit ou altère des données civiles sans causer aucun dommage matériel constitue une attaque interdite contre un bien de caractère civil[17].

J'ai abordé ces questions dans deux précédents articles publiés dans la *Revue*, intitulés « Wired Warfare » et « Rewired Warfare[18] ». Dans le présent article, je vais chercher au-delà du droit, des solutions permettant de sortir en partie de ces impasses. Cela nécessite de revenir brièvement sur les points de désaccord. En conséquence, dans la première partie de cet article, j'expose rapidement les différentes positions

12 PA I, art. 51, par. 2 ; Jean Marie Henckaerts et Louise Doswald Beck (dir.), *Droit international humanitaire coutumier*, vol. I : *Règles*, Bruylant, 2006 (CICR, Étude sur le DIH coutumier), Règle 1 ; Protocole additionnel II aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés non internationaux, RTNU, vol. 1125, p. 609, 8 juin 1977 (PA II), art. 4, par. 1. Voir également Manuel de Tallinn 2.0, *op. cit*. note 6, règle 94.

13 Voir, par exemple, Statut de Rome de la Cour pénale internationale, RTNU, vol. 2187, p. 90, 17 juillet 1998 (Statut de Rome), art. 8, par. 2, al. b, i), 8, par. 2, al. c, i).

14 PA I, art. 51, par. 5, al. b, 57, par. 2), al. a, iii), 5, par. 2, al. b ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 14 ; Manuel de Tallinn 2.0, *op. cit*. note 6, règle 113.

15 PA I, art. 57 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, chap. 5 ; Manuel de Tallinn 2.0, *op. cit*. note 6, règles 114-120. Voir également Eric Jensen, « Cyber Attacks: Proportionality and Precautions in Attack », *International Law Studies*, vol. 89, 2012.

16 Voir en général PA I, titre IV, section I. Certains universitaires étendraient l'application des règles au-delà des attaques malgré l'emploi du terme dans les règles elles-mêmes. Voir, par exemple, Nils Melzer, *Cyberwarfare and International Law*, UNIDIR, document d'information, 2011, p. 27, disponible sur : https://unidir.org/publication/cyberwarfare-and-international-law (qui soutient que l'applicabilité est subordonnée à la question de savoir si les cyberopérations constituent des « hostilités ») ; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, pp. 196-202 (qui se focalise sur la référence aux « opérations militaires » à l'article 48 du PA I).

17 PA I, art. 52, par. 1 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 7 ; Manuel de Tallinn 2.0, *op. cit*. note 6, règle 99.

18 Michael N. Schmitt, « Wired Warfare: Computer Network Attack and Jus in Bello », *Revue internationale de la Croix-Rouge*, vol. 84, n° 846, 2002 ; Michael N. Schmitt, « Rewired Warfare: Rethinking the Law of Cyber Attack », *Revue internationale de la Croix-Rouge*, vol. 96, n° 893, 2014. Voir également Knut Dörmann, « L'applicabilité des Protocoles additionnels aux attaques contre les réseaux informatiques », *in* Karin Bystrom (dir.), *Proceedings of the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19 November 2004*, collège suédois de la défense nationale, 2005, disponible sur : https://www.icrc.org/fr/doc/resources/documents/misc/68ukur.htm. Voir également Michael N. Schmitt, « "Attack" as a Term of Art in International Law: The Cyber Operations Context », dans Christian Czosseck, Rain Ottis et Katharina Ziolkowski (dir.), *Proceedings of the 4th International Conference on Cyber Conflict*, Centre d'excellence de l'OTAN pour la cyberdéfense en coopération, 2012.

sur le seuil à partir duquel une cyberopération peut être qualifiée d'« attaque », tandis que dans la deuxième partie, j'évoque les actuelles divergences quant à la question de savoir si une donnée est un bien. Je n'ai pas l'intention de revenir ici sur les arguments des uns et des autres ; les positions sur ces deux questions permettent seulement de montrer que le droit est imprécis en ce sens que soit il expose les civils à des risques, soit il fait l'impasse sur les cyberopérations qui, bien que licites aujourd'hui, pourraient néanmoins être extrêmement préjudiciables pour la population civile.

La situation ayant peu de chances d'être réglée en droit dans un avenir proche, je propose dans la troisième partie de cet article deux doctrines visant à combler les lacunes dans la protection des civils vis-à-vis de cyberopérations. Elles sont destinées à être appliquées par l'État qui mène une cyberopération lorsqu'il estime que l'opération soit ne peut pas être qualifiée d'attaque, soit n'est pas soumise à l'interdiction d'attaquer des biens de caractère civil parce qu'elle cible des données qui, de l'avis de l'État, ne sont pas des biens. Même si les propositions visent à renforcer la protection de la population civile, elles restent attentives à la nécessité pour les États de mener efficacement leurs opérations en temps de guerre. Ce faisant, ces propositions sont conçues de façon à reproduire l'équilibre entre nécessité militaire et considérations humanitaires, sur lequel reposent le DIH et d'autres normes de la guerre[19].

Il convient enfin de noter que je n'affirme pas que ces deux propositions expriment la *lex lata* ; à mon avis, ce n'est pas le cas, même si je dois admettre que d'autres peuvent ne pas être d'accord. Je propose, à la place, un filet de sécurité humanitaire, réaliste sur le plan militaire et s'inscrivant dans une démarche politique, que les États peuvent adopter dans les cas où ils estiment qu'une opération menée pendant un conflit armé n'est pas soumise aux limites imposées par le DIH. Avec le temps, les questions juridiques décrites ci dessous peuvent être résolues, renforçant ainsi la pertinence du DIH face à des cyberopérations. Mais en attendant, la communauté internationale a besoin d'une réponse concrète permettant de trouver une solution ces zones grises dans le droit applicable au cyberciblage.

Première question : le sens du terme « attaque »

Comme indiqué précédemment, les principales obligations, interdictions et limitations que l'on trouve dans le DIH conventionnel et/ou coutumier, sont établies par référence aux « attaques[20] ». Par exemple, il est interdit de diriger des attaques contre les personnes civiles ou les biens de caractère civil[21] ; de mener des attaques

19 Jean Pictet, *Développement et principes du droit international humanitaire*, Institut Henry Dunant, Genève et Éditions A. Pedone, Paris, 1983, pp. 61-63. Pour mon analyse de cet équilibre, voir Michael N. Schmitt, « Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance », *Virginia Journal of International Law*, vol. 50, n° 4, 2010.

20 Une attaque au sens du DIH ne doit pas être confondue avec l'expression « agression armée » au sens du *jus ad bellum* que l'on retrouve à l'article 51 de la Charte des Nations unies. L'analyse exposée dans cet article se limite seulement à la première.

21 PA I, art. 51, par. 2, 52, par. 1. Concernant leur statut coutumier, voir CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règles 1, 7.

sans discrimination[22] ou perfides[23] ; ou d'attaquer, moyennant diverses exceptions et sous réserve de certaines conditions, des personnes ou des biens bénéficiant d'une protection spéciale (comme les unités sanitaires[24] ; les biens indispensables à la survie de la population civile[25] ; l'environnement[26] ; les ouvrages et installations contenant des forces dangereuses, à savoir les barrages, les digues et les centrales nucléaires[27] ; les localités non défendues[28] ; et les combattants qui sont hors de combat[29]). Les attaques sont soumises au principe de la proportionnalité, qui interdit « les 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[30] ». En outre, une partie au conflit qui prépare une attaque doit prendre toutes les précautions pratiquement possibles pour réduire au minimum les dommages causés à la population civile[31].

L'interprétation et le statut coutumier de certaines de ces règles, en particulier au regard des cyberopérations, sont au cœur des désaccords. Toutefois, le fait de savoir si ces règles s'appliquent aux opérations cyber dépend du champ d'application du terme « attaque[32] ». Si une cyberopération ne peut pas être qualifiée d'attaque, les règles sont inapplicables, bien que d'autres règles du DIH puissent néanmoins interdire ou limiter les cyberopérations[33].

L'article 49, paragraphe 1 du PA I définit les attaques comme des « actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs ». Il est largement admis que des actes de violence dirigés contre des personnes civiles ou des biens de caractère civil constituent une attaque[34]. En s'appuyant sur cette définition, les experts qui ont élaboré le *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Manuel de Tallinn 2.0) ont estimé qu'une cyberattaque englobe toute « cyberopération, qu'elle soit offensive ou défensive, dont on peut raisonnablement s'attendre à ce qu'elle fasse des blessés ou des morts, ou qu'elle cause des dommages à des biens ou leur destruction [traduction CICR][35] ». Il en est ainsi

22 PA I, art. 51, par. 4 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 11.
23 PA I, art. 37, par. 1 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 65. Pour ce qui est de l'emploi du terme à propos de l'usage abusif de signes de nationalité, voir PA I, art. 39, par. 2 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 62.
24 PA I, *op. cit*. note 9, art. 12, par. 1 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 28. Pour ce qui est de l'emploi du terme à propos des attaques contre des aéronefs sanitaires, voir PA I, art. 27, par. 2, 31, par. 2.
25 PA I, art. 54, par. 2 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 54.
26 PA I, art. 55, par. 2. Le statut coutumier de cette règle n'est pas établi.
27 PA I, art. 56, par. 1. Le statut coutumier de cette règle n'est pas établi.
28 PA I, art. 59, par. 1 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 37.
29 PA I, art. 41, par. 1 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 47. Concernant l'interdiction d'attaquer des personnes sautant en parachute d'un aéronef en perdition, voir PA I, art. 42.
30 PA I, art. 51, par. 5, al. b, 57, par. 2, al. a, iii), 57, par. 2, al. b ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règles 14, 19.
31 PA I, art. 57 ; CICR, Étude sur le DIH coutumier, *op. cit*. note 12, règle 15.
32 Pour un excellent résumé concernant la question des cyberattaques, voir William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012.
33 Voir, par exemple, Manuel du droit de la guerre des États-Unis, *op. cit*. note 10, par. 16.5.2.
34 Nils Melzer, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, Genève, 2010 (Guide interprétatif du CICR), p. 51.
35 Manuel de Tallinn 2.0, *op. cit*. note 6, règle 92.

indépendamment du fait que les dommages soient causés à la cible de l'attaque ou qu'ils soient collatéraux[36]. Il semblerait qu'il n'y ait pas d'objection fondamentale à qualifier d'attaques les cyberopérations produisant de tels effets.

Ce que l'on oublie souvent, c'est que les experts n'ont pas limité le concept de « cyberattaque » aux cyberopérations provoquant des destructions et des dommages matériels. Dans l'ensemble, ils s'accordent pour dire que « les interférences dans la fonctionnalité constituent un dommage s'il est nécessaire, pour rétablir cette fonctionnalité, de remplacer des composants matériels [traduction CICR][37] ». Ainsi, une cyberopération qui entraîne une perte de fonctionnalité d'infrastructures cybernétiques constituerait une cyberattaque.

C'est sur ce point que le consensus entre les experts s'est effrité car ils ont divergé sur le sens à donner à la « perte de fonctionnalité ». Tandis que certains voulaient limiter la perte de fonctionnalité aux cas dans lesquels des composants matériels des infrastructures cybernétiques ciblées devaient être réparés ou remplacés, d'autres voulaient l'étendre aux situations dans lesquelles le rétablissement de la fonctionnalité nécessitait de réinstaller le système d'exploitation ou des données *ad hoc (bespoke data)* sans lesquelles le système ne pouvait pas remplir sa fonction première. Certains d'entre eux sont allés jusqu'à affirmer que la manière dont la perte de fonctionnalité survenait importait peu et que le simple fait que le système ne fonctionne plus comme prévu suffisait[38].

Une autre zone grise du droit concerne les cyberopérations qui ne causent ni blessures, ni dommages, mais qui ont néanmoins des conséquences néfastes pour la population civile, comme celles « perturbant toutes les communications électroniques dans tout le pays [traduction CICR][39] ». Tout en reconnaissant que de telles cyberopérations pouvaient perturber le quotidien des populations, la plupart des experts du Manuel de Tallinn ont estimé qu'il n'existait à ce jour aucun fondement juridique pour considérer ces opérations comme des attaques[40]. Tous les experts se sont accordés pour dire que les cyberopérations causant une simple nuisance ou un mécontentement n'atteignaient pas le niveau d'une cyberattaque[41].

Le CICR a abordé cette question dans ses rapports de 2011 et de 2015 sur *Le droit international humanitaire et les défis posés par les conflits armés contemporains* (rapports sur les défis[42]). Dans le rapport de 2015, l'organisation a relevé que « la manière dont les règles régissant la conduite des hostilités définissent la notion de

36 *Ibid*., p. 419.
37 *Ibid*., p. 417. Voir également C. Droege, *op. cit*. note 11, pp. 432-433.
38 Manuel de Tallinn 2.0, *op. cit*. note 6, pp. 417-418. Au sujet de la perte de fonctionnalité, voir W. Boothby, *op. cit*. note 32, pp. 386-387.
39 Manuel de Tallinn 2.0, *op. cit*. note 6, p. 418.
40 *Ibid*.
41 *Ibid*. Voir également CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, Genève, octobre 2015 (Rapport sur les défis de 2015), pp. 49-50, disponible sur : www.icrc.org/fr/document/le-droit-international-humanitaire-et-les-defis-poses-par-les-conflits-armes-contemporains.
42 CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, Genève, octobre 2011, p. 44, disponible sur : www.icrc.org/fr/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-fr.pdf ; Rapport sur les défis de 2015, *op. cit*. note 41, pp. 49-50.

cyber "attaque"… influencera considérablement la protection qu'offre le DIH aux infrastructures civiles essentielles[43] ». Elle s'est ensuite penchée sur la question essentielle du seuil à partir duquel la perte de fonctionnalité fait qu'une cyberopération peut constituer une attaque. Le CICR a notamment conclu qu'« une opération conçue pour mettre un bien hors d'usage – par exemple un ordinateur ou un réseau informatique – constitue une attaque au titre des règles relatives à la conduite des hostilités, que ce bien soit ou non mis hors d'usage par des moyens cinétiques ou cybernétiques[44] ». Le Rapport sur les défis de 2015 souligne, à juste titre, que

> une interprétation trop restrictive de la notion d'attaque serait difficile à concilier avec le but des règles relatives à la conduite des hostilités, qui est de garantir la protection de la population civile et des biens de caractère civil contre les effets des hostilités[45].

Le CICR s'est habilement servi du rapport pour souligner l'imprécision des éléments permettant de caractériser une attaque. Par exemple, s'agissant de l'exclusion des cyberopérations qui causent une simple nuisance, le CICR a souligné que « ce que l'on entend par "nuisance" n'est pas défini et cette terminologie n'est pas employée en DIH[46] ». Toutefois, à l'instar des experts du Manuel de Tallinn, le CICR reconnaît qu'à cet égard, pour qualifier une cyberopération d'attaque, c'est la nature des conséquences qui importe et pas nécessairement leur gravité. Le Rapport sur les défis de 2015 a notamment souligné que l'espionnage en tant que tel ne peut pas être considéré comme une attaque et a relevé que « le brouillage de communications radio ou d'émissions de télévision ... n'est pas traditionnellement considéré comme une attaque au sens du DIH[47] ».

Partant de cette approche conventionnelle, il est possible, sans aucun doute, de qualifier d'attaques des cyberopérations qui causent dommages et destructions et d'exclure celles dont les effets se situent tout en bas de l'échelle de gravité. Pourtant, la plupart des cyberopérations ne causeront probablement aucune destruction, ni aucun dommage matériel et nombre d'entre elles n'affecteront pas la fonctionnalité des infrastructures cybernétiques ciblées d'une manière qui dépasserait nettement le seuil retenu, quel qu'il soit, engendrant une perte de fonctionnalité.

Cela est troublant à deux égards. Premièrement, de nombreuses cyberopérations susceptibles d'être dirigées contre des infrastructures civiles ou d'avoir des conséquences graves et néfastes sur la population civile ne constitueraient peut être pas des cyberattaques et ne seraient donc pas couvertes par les règles du DIH relatives aux attaques. Deuxièmement, le flou entourant le seuil de la perte de fonctionnalité rend imprécise la qualification juridique de certaines cyberopérations dirigées contre la population civile ou lui portant atteinte. Une partie au conflit pourrait exploiter ce flou pour éviter que des cyberopérations dirigées contre des infrastructures cybernétiques civiles ou les perturbant de toute autre manière, soient unanimement

43 Rapport sur les défis de 2015, *op. cit*. note 41, p. 49.
44 *Ibid*., p. 50.
45 *Ibid*.
46 *Ibid*.
47 *Ibid*.

considérées comme illicites et condamnées. D'un point de vue humanitaire, cela n'est pas défendable.

Deuxième question : les données en tant que biens

Un second questionnement de particulière importance pour la population civile, concerne la question de savoir si la notion de « biens » s'étend aux données, de sorte que les données civiles seraient protégées par l'interdiction d'attaquer des biens de caractère civil[48]. Cette question est indépendante de la définition d'une attaque en ce sens que si les données constituent un bien, la suppression ou l'altération des données visées atteindraient clairement le niveau de dommage exigé pour qualifier la cyberopération d'attaque. Et si les données ne sont pas un bien, l'interdiction ne s'applique pas[49].

Sur ce point, deux positions dominent les discussions. Les experts du Manuel de Tallinn ont reconnu, en grande majorité, que le terme « bien » ne devrait pas être interprété comme englobant les données[50]. Leur conclusion est fondée sur le fait que les données ne tombent pas dans le « sens ordinaire[51] » du terme « bien » puisqu'elles sont intangibles, pas plus qu'elles ne « correspondent à l'explication qu'en donnent les Commentaires du CICR de 1987 des Protocoles additionnels [traduction CICR][52] ».

Les autres experts ont répondu qu'adopter cette approche

> signifierait que même la suppression d'ensemble de données civiles essentielles comme les données de sécurité sociale, les dossiers fiscaux et les comptes bancaires, échapperait potentiellement à la portée réglementaire du droit des conflits armés, ce qui serait contraire au principe selon lequel la population civile jouit d'une protection générale contre les effets des hostilités [traduction CICR].

48 Il convient de relever que ces discussions ne concernent pas les cyberopérations visant des données lorsque celles-ci ont eu des répercussions destructrices ou dommageables. Prenons le cas d'une cyberopération qui supprime ou manipule les données d'un système de contrôle du trafic aérien et qui risque ainsi de provoquer un accident d'avion. Il est largement admis qu'une telle opération constituerait une attaque. La question des données ne se pose que dans les cas où une cyberopération dirigée contre des données ne risque pas d'avoir des conséquences qui, dans d'autres circonstances, permettraient de la qualifier d'attaque.

49 Les opérations dirigées contre certaines données sont interdites par d'autres règles du DIH. Voir, par exemple, Manuel de Tallinn 2.0, *op. cit.* note 6, règle 132 et discussion p. 515 (données médicales), règle 142 et discussion pp. 535-536 (certains experts étendent la protection aux biens culturels sous forme de données).

50 *Ibid*., p. 437.

51 Convention de Vienne sur le droit des traités, RTNU, vol. 1155, p. 331, 23 mai 1969 (entrée en vigueur le 27 janvier 1980), art. 31, par. 1.

52 Yves Sandoz, Christophe Swinarski et Bruno Zimmerman (dir.), *Commentaire des Protocoles additionnels aux Conventions de Genève du 12 août 1949*, 1986 (Commentaire CICR des Protocoles additionnels), par. 2007-2008 : « Le mot "biens", en français, signifie "chose tangible, susceptible d'appropriation" ... En anglais, le mot utilisé est "objects", ce qui signifie "something placed before the eyes, or presented to the sight or other sense, an invididual thing seen, or perceived, or that may be seen or perceived; a material thing". ... On le voit, aussi bien en français qu'en anglais, il s'agit de quelque chose de visible, de tangible. » Il faut reconnaître que le contexte dans lequel cette explication a été donnée n'est pas directement applicable, mais les experts du Manuel de Tallinn l'ont néanmoins jugée utile lors de leurs discussions.

Ils ont examiné l'objet et le but de l'interdiction d'attaquer des biens de caractère civil avant de conclure que le principal critère était la « gravité des conséquences de l'opération et non la nature du dommage ». Pour ces experts, « les données civiles qui sont "essentielles" au bien être de la population civile sont comprises dans la notion de biens de caractère civil et protégées comme telles [traduction CICR][53] ».

Dans son Rapport sur les défis de 2015, le CICR a formulé une remarque analogue. Après avoir relevé que « la suppression ou l'altération de [certaines] données pourrait rapidement entraîner une immobilisation totale des services publics et des entreprises privées et pourrait nuire bien davantage aux civils que la destruction de biens de caractère civil[54] », l'organisation a estimé :

> La conclusion selon laquelle ce type d'opération ne serait pas interdit par le DIH dans le monde d'aujourd'hui, toujours plus cyberdépendant, soit parce que la suppression ou l'altération de ces données ne constituerait pas une attaque au sens du DIH, soit parce que ces données ne seraient pas considérées comme un bien qui mettrait en jeu l'interdiction des attaques contre les biens de caractère civil – semble difficile à concilier avec l'objet de ce corpus de règles[55].

Sur le principe, je suis d'accord avec cette appréciation.

D'autres approches de la question ont été proposées. L'une d'elles distingue les données dites opérationnelles des données de contenu[56]. Les premières visent les données dont dépend le fonctionnement des infrastructures cybernétiques, tandis que les secondes correspondent simplement aux informations sous forme de données, comme le traitement de texte utilisé pour élaborer le présent article. Ne portant que sur les données opérationnelles, cette approche rejette le critère de la tangibilité pour plutôt se focaliser sur la question de savoir si les données peuvent être qualifiées d'objectif militaire[57]. Ce faisant, elle adopte implicitement une vision absolutiste des données opérationnelles en tant que bien. Une approche un peu plus ouverte consiste simplement à traiter les données comme un bien. Pour l'illustrer, un des partisans de cette approche soutient qu'il est possible d'y parvenir « grâce à une interprétation textuelle, systématique et téléologique de la définition des objectifs militaires énoncés dans le droit conventionnel et coutumier [traduction CICR][58] ». Il conclut :

> La vie civile et les opérations militaires dépendent de plus en plus des informations et activités enfermées dans le cyberespace, avec peu ou pas de ramifications dans le monde physique. Pour rester d'actualité, le droit des conflits armés doit tenir compte de ce changement. C'est pourquoi on avance l'argument selon lequel

53 Manuel de Tallinn 2.0, *op. cit*. note 6, p. 437.
54 Rapport sur les défis de 2015, *op. cit*. note 41, p. 52.
55 *Ibid*.
56 Heather A. Harrison Dinniss, « The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives », *Israel Law Review*, vol. 48, n° 1, 2015.
57 *Ibid*., pp. 41-49.
58 Kubo Mačák, « Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law », *Israel Law Review*, vol. 58, n° 1, 2015, p. 55. J'ai répondu à ces deux approches dans « The Notion of "Objects" during Cyber Operations: A Riposte in Defence of Interpretive Precision », *Israel Law Review*, vol. 48, n° 1, 2015.

> ... les données informatiques sont des biens conformément au droit international humanitaire [traduction CICR][59].

Aucune des approches susmentionnées n'est pleinement satisfaisante. L'approche restrictive adoptée par la majorité des experts du Manuel de Tallinn a une portée limitée d'un point de vue pratique, car elle expose les données à d'éventuelles destructions ou altérations qui pourraient avoir des conséquences extrêmement graves pour la population civile, même si elles ne causent ni destructions ni dommages. Cela irait, comme l'affirment ses détracteurs, à l'encontre de l'objet et du but du DIH.

Au contraire, l'argument (quelle que soit la façon dont on y parvient) selon lequel les données en tant que telles peuvent être qualifiées de bien, est trop général. Les armées ont longtemps mené des opérations d'influence auprès de la population ennemie, par exemple pour ébranler le soutien qu'elle apporte au gouvernement ou à sa politique[60]. Agir de la sorte est particulièrement séduisant lors de contre-insurrections[61]. Avec l'avènement des cybercapacités, de telles opérations ont été menées grâce à des moyens cybernétiques[62]. Par exemple, la destruction ou l'altération de données, ou la perturbation des activités des médias civils peuvent faire partie de cyberopérations psychologiques.

L'approche fondée sur la gravité des effets défendue par une minorité d'experts lors du processus d'élaboration du Manuel de Tallinn, ainsi que par le CICR, est d'instinct la plus intéressante. Malheureusement, aucun argument juridique autre que l'argument plutôt général de la conformité à l'objet et au but n'a été avancé pour l'étayer. Pas plus que n'ont été établies des directives utiles et détaillées pour expliquer sa mise en œuvre. De plus, cette approche ignore le fait qu'il s'agit avant tout d'une question de définition. Se pose alors la question du raisonnement juridique qui permettrait de qualifier certaines données de biens eu égard à la gravité des conséquences, mais de ne pas en faire autant pour d'autres données lorsque les conséquences des dommages ou de l'altération sont moins graves. Il pourrait être cohérent de convenir d'une ligne juridique fondée sur les conséquences engendrées, comme pour la règle de la proportionnalité, mais le même raisonnement ne s'applique pas lorsqu'il s'agit uniquement de définir un terme.

Ces désaccords ne seront pas dissipés dans un avenir proche car l'adoption d'une approche selon laquelle les données sont ou ne sont pas des biens aboutit à des résultats qui ne sont ni satisfaisants, ni réalistes. Et même si le fait de tenir compte de la gravité des conséquences pour la population civile semble répondre aux objectifs

59 K. Mačák, *op. cit*. note 58, p. 80.

60 Voir en général, par exemple, les chefs d'état major interarmées des États-Unis, *Information Operations*, Publication conjointe 3-13, telle que modifiée le 20 novembre 2014.

61 Voir, par exemple, Armée des États-Unis, *Counterinsurgency*, Field Manual 3-24, décembre 2006, par. 5-19–5-34.

62 L'armée des États-Unis évalue soigneusement le recours à de telles capacités. Voir, par exemple, Liston Wells II, « Cognitive-Emotional Conflict: Adversary Will and Social Resilience », *Prism*, vol. 7, n° 2, 2017. *Prism* est publié par la National Defense University des États-Unis. L'accent mis sur ces opérations est attesté par la création d'une faculté de l'information et du cyberespace au sein de la National Defense University (site web disponible sur : https://www.ndu.edu).

fondamentaux du DIH, l'absence de fondement juridique clair pour étayer cette position fait qu'elle relève de la *lex ferenda* plutôt que la *lex lata*.

Que faire ?

Que faire face à cette situation préoccupante ? À mon avis, puisque la lettre ne suffit pas, c'est dans l'esprit du DIH que l'on peut trouver une réponse qui éclaire les choix politiques. C'est dans cet état d'esprit que je recommande donc deux doctrines, toutes deux axées sur la gravité des effets subis par la population civile, plutôt que sur le type (par exemple matériel) de dommages causés.

L'esprit du DIH réside dans l'équilibre délicat qu'il assure entre l'intérêt des États à mener efficacement leurs opérations militaires et les souffrances que ces opérations peuvent causer tant aux combattants qu'à la population civile. Cet équilibre a été maintes fois reconnu dans les principaux traités de DIH et dans les doctrines des États. Par exemple, le Code de Lieber de 1863, qui énonçait les instructions pour l'armée de l'Union pendant la guerre civile américaine, disposait :

> La nécessité militaire n'admet pas la cruauté, c'est-à-dire le fait d'infliger la souffrance pour elle même ou par vengeance, ni l'acte de blesser ou mutiler si ce n'est en combat, ni la torture pour obtenir des renseignements. Elle n'admet d'aucune manière l'usage du poison, ni la dévastation systématique d'une contrée. Elle admet la ruse, mais repousse les actes de perfidie ; et, en général, la nécessité militaire ne comprend aucun acte d'hostilité qui accroisse, sans nécessité, les difficultés du retour à la paix[63].

Cinq ans plus tard, la Déclaration de Saint-Pétersbourg a elle aussi insisté sur le besoin de « fix[er...] les limites techniques où les nécessités de la guerre doivent s'arrêter devant les exigences de l'humanité[64] ». La nécessité d'un équilibre fut également le fil rouge de la Conférence de la Paix de La Haye de 1907, tel qu'il ressort de la Convention (IV) qui a relevé que l'instrument, qui a depuis été reconnu comme ayant un caractère coutumier[65], a été « inspiré par le désir de diminuer les maux de la guerre, autant que les nécessités militaires le permettent[66] ». La Convention

63 Département de la guerre des États-Unis, *Instructions de 1863 pour les armées en campagne des États-Unis d'Amérique*, ordonnance générale n° 100, 24 avril 1863, (Code de Lieber), art. 16.

64 Déclaration à l'effet d'interdire l'usage de certains projectiles en temps de guerre, *Martens Nouveau Recueil*, Série 1, vol. 18, 11 décembre 1868, Préambule.

65 C.I.J., *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, Avis consultatif du 9 juillet 2004, *C.I.J. Recueil 2004*, p. 172 ; C.I.J., *Licéité de la menace ou de l'emploi d'armes nucléaires*, *op. cit.* note 8, p. 257 . Le Tribunal de Nuremberg a également conclu que les règles énoncées dans la Convention (IV) de La Haye appartenaient au droit coutumier ; voir *Trial of the Major War Criminals before the International Military Tribunal*, vol. 1, 1947, p. 254.

66 Convention (IV) concernant les lois et coutumes de la guerre sur terre, 36 Stat. 2277, 207 Consol. T.S. 277, 18 octobre 1907 (Convention (IV) de La Haye), Préambule. Voir également Convention (II) concernant les lois et coutumes de la guerre sur terre, 32 Stat. 1803, *Martens Nouveau Recueil*, série 2, vol. 26, 29 juillet 1899, Préambule. Les règlements de La Haye de 1899 et 1907, à l'article 22 de l'annexe des deux conventions, indiquent également : « Les belligérants n'ont pas un droit illimité quant au choix des moyens de nuire à l'ennemi ». Pour l'expression moderne de ce principe, voir PA I, art. 35, par. 1 (qui mentionne en outre les « méthodes » de guerre).

a également formulé la Clause de Martens, qui est réapparue 70 ans plus tard dans le PA I :

> En attendant qu'un Code plus complet des lois de la guerre puisse être édicté, les Hautes Parties contractantes jugent opportun de constater que, dans les cas non compris dans les dispositions réglementaires adoptées par Elles, les populations et les belligérants restent sous la sauvegarde et sous l'empire des principes du droit des gens, tels qu'ils résultent des usages établis entre nations civilisées, des lois de l'humanité et des exigences de la conscience publique[67].

Ces déclarations et dispositions illustrent l'observation faite par la Cour internationale de Justice (C.I.J.) dans l'*Affaire du Détroit de Corfou*, sa première affaire, selon laquelle « des considérations élémentaires d'humanité » inspirent le droit international[68].

Les cyberopérations changent la donne pour ce qui est d'atteindre l'équilibre recherché par le DIH. Le droit international humanitaire s'est construit au vu des moyens et des méthodes de guerre qui avaient pour effet d'endommager, de détruire, de blesser ou de tuer. Si la population civile a pu souffrir d'opérations militaires qui n'ont pas engendré de telles conséquences, la menace de dommages provenait essentiellement de ces effets. Ainsi, les règles du DIH sont fondées sur la nécessité de protéger les personnes civiles et les biens de caractère civil, du moins dans la mesure du possible, sans priver les États de leur capacité de mener des opérations militaires essentielles[69].

Toutefois, contrairement aux moyens et méthodes de guerre cinétiques, les cyberopérations peuvent gravement perturber la vie civile sans nécessairement enfreindre ces règles fondées sur la matérialité. Ainsi, comme la grande majorité de ces opérations ne cause ni dommages ni blessés, elles ne correspondent pas parfaitement à l'architecture normative en vigueur censée protéger la population civile. Il n'est pas possible de sortir de cette impasse en traitant simplement les données civiles comme des biens de caractère civil protégés car, au mieux et comme exposé plus haut, procéder ainsi serait non seulement juridiquement controversé, mais, de surcroît, s'avérerait très certainement inacceptable pour de nombreux États.

67 Convention (IV) de La Haye, Préambule ; PA I, art. 1, par. 2. La clause a été citée par la C.I.J., dans son avis sur les *armes nucléaires*, *op. cit.* note 8, p. 257.

68 C.I.J., *Affaire du Détroit de Corfou (Royaume-Uni c. Albanie)*, arrêt du 9 avril 1949, *C.I.J. Recueil 1949*, p. 22.

69 Ce paradigme cognitif de la matérialité ressort par exemple du principe général selon lequel la « population civile et les personnes civiles jouissent d'une protection générale contre les *dangers* résultant d'opérations militaires » (PA I, art. 51, par. 1 [nous soulignons]) ; de la référence à la violence dans la définition d'attaque (art. 49, par. 1) ; de la limitation dans l'application de la règle de proportionnalité et de certaines précautions dans l'attaque qui cause « incidemment des *pertes en vies humaines dans la population civile, des blessures aux personnes civiles, [et] des dommages* aux biens de caractère civil » (art. 51, par. 5, al. b), 57, par. 2, al. a, ii), 51, par. 2, al. a, iii) ; 51, par. 2, al. b [nous soulignons]) ; et de l'interdiction des « actes ou menaces de violence dont le but principal est de répandre la terreur parmi la population civile » (art. 51, par. 2 [nous soulignons]). En effet, pour expliquer le principe de distinction, qui impose aux parties à un conflit « en tout temps [de] faire la distinction entre la population civile et les combattants ainsi qu'entre les biens de caractère civil et les objectifs militaires et, par conséquent, [de] ne diriger leurs opérations que contre des objectifs militaires » (art. 48), le Commentaire CICR des Protocoles additionnels définissent les opérations militaires comme celles « au cours desquelles on recourt à la violence » (Commentaire CICR des Protocoles additionnels, *op. cit.* note 52, par. 1875 [nous soulignons]).

La première étape pour trouver une solution à cette impasse est de reconnaître, comme cela a été démontré, que la communauté internationale accepte généralement le principe selon lequel les souffrances infligées par la guerre à la population civile devraient être réduites au minimum dans la mesure du possible et en fonction des circonstances. Il n'y a aucune raison de limiter l'application de ce principe humanitaire au domaine du droit contraignant. Au contraire, la plupart des normes du DIH ont été soit adoptées sous la forme d'un traité, soit cristallisées dans le droit coutumier, mais une fois seulement que les actions auxquelles elles s'appliquent, aient été considérés en l'espèce comme inacceptables ou inappropriés par la communauté internationale. Les positions et les politiques humanitaires ont souvent fini, avec le temps, par aboutir à du droit.

C'est pourquoi je propose que les États adoptent deux doctrines humanitaires pour trouver des solutions aux lacunes et aux imprécisions évoquées ci-dessus. Certains États peuvent estimer que certains des éléments se trouvent déjà dans le DIH. Toutefois, puisqu'il n'y a pas de consensus, il est nécessaire de les formaliser dans des engagements politiques.

Doctrine n° 1 : fonctions civiles essentielles

La première proposition consiste à *accorder une protection spéciale à quelques « fonctions ou services civils essentiels » en s'engageant à ne pas mener de cyberopérations contre des infrastructures ou des données civiles qui empiètent sur leur fonctionnement* [traduction CICR]. J'ai avancé cette idée dans un article de 2014[70], dans lequel j'expliquais qu'avec le temps, les États pourraient « simplement commencer à considérer les opérations dirigées contre des services et des données civils essentiels comme des attaques en s'abstenant d'y recourir et en condamnant ceux qui les conduisent, établissant ainsi la pratique des États sur laquelle une évolution de la définition peut [en partie] être fondée [traduction CICR][71] ». Cette proposition était peu judicieuse en ce sens que je confondais l'ajustement de la définition d'un mot – « attaque » – avec ce qu'est réellement une protection spéciale. Aussi, je reformule maintenant l'idée sous la forme d'une protection spéciale fondée sur une doctrine que les États qui ne la considèrent pas déjà comme une obligation juridique, doivent adopter[72].

Il convient de souligner que la proposition vise à préserver des fonctions et services plutôt que des catégories précises d'infrastructures cybernétiques ou de

70 Michael N. Schmitt, « The Law of Cyber Warfare: Quo Vadis? », *Stanford Law and Policy Review*, vol. 25, n° 2, 2014.

71 *Ibid*., p. 296.

72 Pour une proposition faite précédemment dans ce sens, voir Adam Segal, « Cyber Space Governance: The Next Step », Council on Foreign Relations, Policy Innovation Memorandum No. 2, 14 novembre 2011, p. 3, disponible sur : https://www.cfr.org/report/cyberspace-governance-next-step. Un certain nombre d'auteurs se sont dits sceptiques quant aux possibilités qu'offrait cette proposition : voir C. Droege, *op. cit*. note 11, p. 453 ; Robin Geiss et Henning Lahmann, « Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space », *Israel Law Review*, vol. 45, n° 3, 2012, p. 394. Je suis moins pessimiste que ces auteurs pour ce qui est de la possibilité que des États fassent de telles déclarations ou élaborent de telles doctrines concernant lesdits « refuges numériques », mais je pense que la proposition, qui comprend aussi bien des questions de *jus ad bellum* que des questions de *jus in bello*, exige une plus grande finesse juridique.

données civiles (en d'autres termes celles qui ne peuvent pas être qualifiées d'objectifs militaires). Il s'agit d'éviter des désaccords sur la question de savoir si certaines infrastructures ou données tombent dans la catégorie protégée. En se concentrant sur des fonctions ou des services, la protection s'étend à toute infrastructure ou à toute donnée susceptible de les détériorer indépendamment de la nature ou de la catégorie des infrastructures ou des données en question. Une telle approche n'est pas sans précédent en DIH. Il est par exemple interdit d'utiliser des moyens cybernétiques pour interférer avec des fonctions sanitaires[73] ou, dans certaines circonstances, avec la fourniture d'une aide humanitaire[74]. Ma proposition suit le même raisonnement, mais selon une perspective politique.

Dans son Rapport sur les défis de 2015, le CICR a également souligné la nécessité de protéger les infrastructures et les données civiles essentielles, compte tenu notamment du manque de précision du droit[75]. Il a observé :

> S'agissant des données appartenant à certaines catégories de biens bénéficiant d'une protection particulière au titre du DIH, les règles de protection sont suffisamment générales. Par exemple, l'obligation de respecter et de protéger les structures sanitaires doit être entendue comme s'étendant aux données médicales appartenant à ces structures. Il serait néanmoins important de préciser la mesure dans laquelle les données civiles qui ne bénéficient pas de cette protection spécifique, comme les données de sécurité sociale, les dossiers fiscaux, les comptes bancaires, les fichiers clients des entreprises ou les listes ou registres électoraux, sont déjà protégées par les règles générales relatives à la conduite des hostilités[76].

Bien que je sois d'accord avec le CICR, des précisions pourraient aboutir à la conclusion que le DIH ne protège pas totalement des données essentielles ayant une incidence sur la population civile. La doctrine proposée réduirait ce risque car s'il ressortait des précisions apportées, que les données ne sont pas protégées par le DIH, les données bénéficieraient néanmoins d'une protection en vertu de cette doctrine. De plus, la doctrine pourrait s'appliquer jusqu'à ce que la question des données, ainsi que celle relative à la définition du seuil d'une attaque, soient réglées.

Le diable est dans les détails, en particulier pour définir les fonctions et les services qui sont essentiels. Il est certain que ce point génèrera des désaccords, comme

73 Manuel de Tallinn 2.0, *op. cit.* note 6, règle 131 (l'obligation de « respecter » est « violée par des actes qui empêchent le personnel et les services sanitaires et religieux, ou les transports sanitaires d'exercer leurs fonctions sanitaires ou religieuses [traduction CICR] » : *ibid.*, p. 514). Pour les obligations en général, voir Convention (I) de Genève pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne, 12 août 1949, RTNU, vol. 75, p. 31 (entrée en vigueur le 21 octobre 1950), art. 19, 24, 25, 35-36 ; Convention (II) de Genève pour l'amélioration du sort des blessés, des malades et des naufragés des forces armées sur mer, 12 août 1949, RTNU, vol. 75, p. 85 (entrée en vigueur le 21 octobre 1950), art. 22, 24, 25, 27, 36-39 ; Convention (III) de Genève relative au traitement des prisonniers de guerre, 12 août 1949, RTNU, vol. 75, p. 135 (entrée en vigueur le 21 octobre 1950), art. 33 ; Convention (IV) de Genève relative à la protection des personnes civiles en temps de guerre, 12 août 1949, RTNU, vol. 75, p. 287 (entrée en vigueur le 21 octobre 1950), art. 18-22 ; PA I, art. 12, 15, 21-24, 26 ; PA II, art. 9.

74 Manuel de Tallinn 2.0, *op. cit.* note 6, règle 145. Pour l'obligation en général, voir CG IV, art. 23, 59 ; PA I, art. 69-70.

75 Rapport sur les défis de 2015, *op. cit.* note 41, pp. 51-52.

76 *Ibid.*, p. 52.

ce fut déjà le cas des discussions interminables lorsqu'il s'est agi de désigner des systèmes d'« infrastructures critiques[77] ». Comme exemple d'un possible désaccord, voyez comment le CICR a mis l'accent sur les données liées à des comptes bancaires et à des registres électoraux dans l'extrait reproduit ci dessus. À mon avis, de nombreux États seraient peu disposés à ce que ces données leur échappent complétement. Par exemple, une cyberopération bloquant l'accès aux comptes bancaires des amis d'un dictateur ennemi ou des membres dirigeants de son parti politique pourrait bien être une idée séduisante pendant un conflit armé et, de la même manière, l'État ennemi pourrait être tenté de perturber sa réélection en manipulant les résultats des élections. Cette remarque n'a pas pour but d'exprimer un désaccord, mais plutôt de souligner qu'il sera difficile de dégager un vaste consensus sur les fonctions et services civils qui sont essentiels et qui méritent d'être protégés.

Pour autant, il est semble clair que certaines fonctions entrent dans le champ de cette catégorie. Ce serait par exemple le cas des dispositifs d'aide sociale à destination des personnes handicapées, des jeunes, des pauvres et des personnes âgées. Il en irait de même pour l'enseignement primaire et secondaire. Le fait que des interférences seraient susceptibles d'engendrer une grande anxiété au sein de la population civile pourrait être un indicateur permettant de déterminer si une fonction ou un service entre dans la catégorie. Par exemple, comme je l'ai déjà proposé, il conviendrait que « l'intégrité des données des institutions financières et la disponibilité des systèmes financiers indispensables » bénéficient, par principe, d'une protection spéciale[78].

Le fait qu'une cyberopération perturbant une fonction ou un service aurait des conséquences bien après la fin des hostilités, pourrait constituer un autre indicateur. Un parfait exemple consisterait à entraver le fonctionnement général du système universitaire d'un pays, alors que la protection ne s'étendrait pas aux infrastructures cybernétiques individuelles d'une université considérée comme un objectif militaire, comme dans le cas d'infrastructures utilisées pour mener des recherches sur des armes ou sur d'autres questions militaires.

Doctrine n° 2 : contrebalancer les effets négatifs sur les civils et les bénéfices liés au conflit

La seconde doctrine que je propose s'appliquerait aux situations qui ne sont pas couvertes par la première (ou jusqu'à ce qu'un accord soit obtenu concernant les fonctions et services désignés). Contrairement au premier engagement qui est absolu par nature, celui-ci est relatif en ce sens qu'il est fondé sur un équilibre entre des considérations humanitaires et l'intérêt d'un État à dominer le conflit armé. Par cette seconde doctrine, les États s'engageraient, politiquement, à *s'abstenir de mener des*

77 Voir, par exemple, John Moteff, Claudia Copeland et John Fischer, *Critical Infrastructures: What Makes an Infrastructure Critical?*, Rapport du Congressional Research Service, 29 janvier 2003.

78 Michael N. Schmitt et Tim Maurer, « Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms? », *Just Security*, 26 août 2017, disponible sur : www.justsecurity.org/44411/protecting-financial-data-cyberspace-precedent-progress-cyber-norms/. Cette proposition ne couvre pas les activités qui consistent à bloquer l'accès à des données pendant un laps de temps limité ou à pirater des données confidentielles.

cyberopérations auxquelles les règles du DIH régissant les attaques ne s'appliquent pas lorsque les effets négatifs concrets attendus sur des personnes civiles ou sur la population civile sont excessifs par rapport aux avantages concrets liés au conflit que l'opération devrait permettre d'obtenir [traduction CICR][79].

Compte tenu des désaccords exposés ci dessus, l'inapplicabilité du DIH pourrait venir soit du fait qu'un État estime que l'opération n'est pas une attaque au sens du DIH, soit de la position qu'il a adoptée selon laquelle les données ne sont pas des biens. Il est important de relever que l'appréciation de l'interprétation du droit applicable serait celle de l'État conduisant l'opération. En d'autres termes, selon cette proposition, un État accepterait d'appliquer la doctrine chaque fois qu'il estime qu'une opération n'est pas soumise aux règles du DIH relatives à la conduite des hostilités. Un autre État pourrait aboutir à une toute autre conclusion pour une opération analogue ; en pareil cas, il suivrait les indications énoncées dans ce droit.

Cet engagement mérite d'être analysé avec soin. Pour commencer, il couvre les opérations ciblant des infrastructures cybernétiques et des données qui sont soit des objectifs militaires soit des biens de caractère civil. À cet égard, une observation intéressante a été faite dans le Rapport du CICR sur les défis de 2015 concernant les biens dits « à double usage », à savoir ceux qui sont employés à des fins à la fois militaires et civiles. Selon la majorité des experts en DIH, tout usage militaire d'un bien de caractère civil, y compris d'infrastructures cybernétiques, fait du bien un objectif militaire, à l'exception des éléments du bien qui constituent clairement des composants distincts[80]. Le Rapport sur les défis exprime des inquiétudes quant à l'application de cette norme à des opérations cybernétiques :

> Une stricte application de cette conception pourrait amener à conclure que de nombreux biens qui font partie de l'infrastructure cyberspatiale constitueraient des objectifs militaires et ne seraient pas protégés des attaques, cybernétiques ou

79 L'accent mis par le DIH sur la matérialité pose des difficultés particulières en ce qui concerne les cyberopérations qui constituent *effectivement* une attaque. Plus particulièrement, les dommages collatéraux qui entrent en ligne de compte dans l'évaluation de la proportionnalité et dans l'obligation de prendre les précautions pratiquement possibles dans l'attaque se limitent littéralement aux blessures, aux décès ou aux dommages. Même si l'on peut raisonnablement estimer que les dommages comprennent la perte de fonctionnalité (quelle que soit la limite fixée), ils n'englobent pas d'autres formes de préjudice. Par exemple, en droit, l l'évaluation de la proportionnalité d'une attaque contre une infrastructure cybernétique à double usage ne devrait pas nécessairement tenir compte de la perturbation ou de l'interruption temporaire des services civils qui en dépendent, sauf si cette interruption expose des personnes civiles à un risque de dommage physique ou des biens de caractère civil à un risque de dommage. Alors qu'il en va de même pour les frappes cinétiques, comme l'attaque d'un magasin utilisé pour cacher des armes, la mise en place de réseaux et toute autre forme de connexion aggravent les effets en cascade ne causant ni destructions ni dommages, des cyberattaques. Le présent article ne se penche pas sur cette réalité, car il se limite aux cyberopérations qui échappent au champ du DIH, mais il s'agit d'un phénomène propre à la cybernétique qui mérite une attention particulière.

80 Manuel de Tallinn 2.0, *op. cit*. note 6, règle 101 ; programme de recherche de Harvard sur les politiques humanitaires et les conflits, *HPCR Manual on International Law Applicable to Air and Missile Warfare*, Cambridge University Press, Cambridge, 2013 (Manuel de Harvard), p. 119 ; Nils Melzer, *Droit international humanitaire : Introduction détaillée*, CICR, Genève, 2016, p. 108. Pour un débat sur la distinction entre les parties d'un bien ciblé, voir Michael N. Schmitt et John J. Merriam, « *The Tyranny of Context: Israeli Targeting Practices in Legal Perspective* », Journal of International Law de l'Université de Pennsylvanie, vol. 37, n° 1, 2015, pp. 119-123.

> cinétiques. Ce serait extrêmement préoccupant étant donné l'impact possible d'une telle perte de protection du point de vue des perturbations que pourrait subir l'usage concomitant du cyberespace par des applications civiles, un usage qui va croissant[81].

Je partage cette préoccupation. La question de savoir si les infrastructures cybernétiques devraient être considérées comme des objectifs militaires dépasse le cadre du présent article ; je fais mienne l'opinion la plus courante. Mais même si cette position devait évoluer au fil du temps et si certaines infrastructures cybernétiques à double usage commençaient à être qualifiées de civiles, les cyberopérations qui les visent, y compris les opérations ayant de graves conséquences pour la population civile, n'en resteraient pas moins licites tant qu'elles n'atteignent pas le niveau d'une attaque, en causant notamment des dommages et des destructions. La doctrine proposée trancherait partiellement cette impasse.

Certains termes contenus dans la doctrine ont été soigneusement choisis pour défendre une thèse précise et il est à espérer qu'ils serviront de fondement aux discussions à venir. L'expression « effets négatifs » se veut exhaustive. Elle couvre tous les effets sur la population civile qui ne permettent pas de qualifier une cyberopération d'attaque et donc de la soumettre aux règles applicables aux attaques. Bien qu'elle soit limitée aux effets sur les personnes et qu'elle ne concerne pas les biens, elle englobe les conséquences sur les civils résultant des effets d'une opération sur l'infrastructure visée. Pour prendre un exemple simple, une attaque menée par déni de service contre le système informatique d'une banque priverait les clients de la possibilité de retirer de l'argent ; les clients étant affectés, la doctrine s'applique.

Le fait de mettre l'accent sur les effets montre aussi que le type de cyberopération n'a aucune incidence sur l'applicabilité de la proposition. Par exemple, une attaque par déni de service ou une opération qui ralentit un système cybernétique ne serait pas moins régie par la doctrine qu'une attaque ou opération qui perturberait le fonctionnement du système. Au contraire, le facteur clé est que la population civile est en quelque sorte affectée d'une manière qui n'est pas visée par les règles du DIH, à tout le moins de l'avis de l'État qui mène l'opération.

Même si les experts du Manuel de Tallinn ont estimé que la nuisance n'est pas suffisamment grave pour constituer une attaque, il n'y a aucune raison de fixer des limites de cet ordre dans le cadre de la doctrine proposée. En effet, cela ne permettrait d'interdire une cyberopération qu'en cas d'effets négatifs sur les civils, excessifs par rapport aux bénéfices attendus liés au conflit. En principe, il est logique de ne pas considérer les nuisances ou les mécontentements comme des conséquences inacceptables si la partie conduisant la cyberopération ne peut pas avancer de raison suffisante pour les justifier. S'attendre à causer des nuisances ou des mécontentements qui seraient excessifs par rapport aux bénéfices attendus de la cyberopération, lesquels seraient *a priori* insignifiants, relèverait simplement de la malveillance. Le

81 Rapport sur les défis de 2015, *op. cit.* note 41, p. 51.

Département de la Défense des États-Unis a le mérite d'avoir fait de cette approche sa ligne de conduite[82].

S'agissant de l'équilibre entre les considérations humanitaires et les intérêts d'un État liés au conflit, la doctrine proposée retient le critère du caractère excessif de la règle de proportionnalité. Le *HPCR Manual on the International Law Applicable to Air and Missile Warfare* (Manuel de Harvard), élaboré par un groupe d'éminents praticiens et spécialistes du droit international, s'est rangé à une sage position selon laquelle le caractère excessif est avéré lorsqu'il « existe un important déséquilibre entre, d'une part, l'avantage militaire attendu et, d'autre part, les dommages collatéraux que les personnes civiles et biens de caractère civil devraient subir [traduction CICR][83] ». Cette norme est compatible avec le principe fondateur du DIH de la nécessité militaire. Après tout, il serait impossible d'appliquer le critère strict d'équilibre « 51-49 » à deux entrées – les dommages collatéraux et l'avantage militaire – qui sont si diamétralement opposées, en particulier lorsque les conséquences d'un léger déséquilibre qui serait perçu en faveur de la première empêchaient totalement de frapper un objectif militaire légitime. La difficulté de cet exercice ressort également de l'application du principe de proportionnalité par le Statut de Rome qui considère les dommages collatéraux uniquement lorsqu'ils sont « manifestement » excessifs par rapport à « l'ensemble » de l'avantage militaire attendu[84].

Étant donné que les cyberopérations couvertes par la doctrine comprennent celles qui sont dirigées contre des objectifs militaires, bien que dans certains cas elles n'atteignent pas le niveau d'une attaque, cela n'aurait aucun sens d'abaisser la barre du caractère excessif. S'il venait à être proposé d'abaisser le seuil, les États auraient les mêmes réserves que celles qui furent exprimées lors de l'adoption du critère du caractère excessif à propos de la proportionnalité. En effet, eu égard à la doctrine, l'argument en faveur d'un seuil élevé est en fait plus efficace car le préjudice, qui, généralement, n'entraîne ni destructions ni dommages, présente un caractère moins grave.

L'expression « avantage concret lié au conflit » employée dans la doctrine proposée doit être distinguée de l'expression « avantage militaire concret et direct » que l'on trouve dans le principe de proportionnalité. Tous les adjectifs se rapportent à la nécessité militaire qui fait partie de l'équilibre qui, selon moi, devrait orienter toutes les décisions militaires ayant une incidence sur la population civile. Toutefois, comme expliqué ci-après, la suppression du mot direct vise à élargir le champ d'application de la doctrine au delà de ce qui s'applique dans le cas de la proportionnalité.

Conformément au Commentaire des Protocoles additionnels élaborés par le CICR, « par les mots "concret et direct", on a voulu marquer qu'il s'agissait d'un intérêt substantiel et relativement proche, en éliminant les avantages qui ne seraient

82 Voir Manuel du droit de la guerre des États-Unis, *op. cit.* note 10, par. 16.5.2 : « Par exemple, même si une cyberopération n'est pas une "attaque" ou ne cause pas de blessures ou de dommages qu'il serait nécessaire d'examiner à la lumière du principe de proportionnalité dans la conduite d'attaques, il n'en reste pas moins que cette cyberopération ne doit pas être menée d'une manière qui causerait inutilement des nuisances aux personnes civiles ou à des personnes neutres [traduction CICR]. »

83 Manuel de Harvard, *op. cit.* note 80, p. 92 ; Nils Melzer, *Targeted Killings in International Law*, Oxford University Press, Oxford, 2008, pp. 344, 360.

84 Statut de Rome, *op. cit.* note 13, art. 8, par. 2, al. b, iv).

pas perceptibles ou qui ne se manifesteraient qu'à longue échéance[85] ». L'expression a également été expliquée dans la version non officielle, mais digne de foi (compte tenu de la participation des auteurs à la Conférence diplomatique ayant conduit à l'adoption des Protocoles additionnels) des commentaires des Protocoles publiés par Bothe, Partsch et Solf. Il y est indiqué que « concret » signifie « spécifique, non général ; perceptible par les sens » et le terme y est mis sur le même pied que « précis » dans la définition de l'objectif militaire, qui désigne un avantage qui n'est ni hypothétique ni spéculatif[86]. En revanche, selon les auteurs, le mot « direct » signifie « sans condition d'action intermédiaire [traduction CICR][87] ».

Rien ne permet raisonnablement de soutenir que les bénéfices à prendre en considération pour appliquer la doctrine proposée doivent être concrets. Laisser entendre que d'hypothétiques bénéfices liés au conflit suffiraient pour justifier qu'il est attendu des conséquences véritablement négatives pour la population civile, reviendrait en fait à ignorer totalement les considérations humanitaires. Toutefois, le même raisonnement ne s'applique pas au qualificatif « direct ». Les États s'opposeraient sans doute à imposer le critère du lien de causalité direct entre l'opération et le bénéfice, qui, dans le cadre de la proportionnalité, s'applique aux cyberattaques ou à d'autres formes d'attaques. Prenons le cas d'opérations conçues pour ébranler le soutien apporté par la population civile à la participation de leur pays à un conflit. Ces campagnes d'influence impliquent généralement une chaîne de causalité qui ne comprend pas qu'un seul maillon. L'opération d'information en question peut être conçue pour faire basculer l'opinion de la population à l'égard du gouvernement et, au fil du temps, à propos du conflit, par exemple en favorisant la mobilisation de la société civile et des médias. Tant qu'il existe un lien de causalité qui n'est pas si faible qu'il en deviendrait hypothétique, il conviendrait, selon la proposition, d'en tenir compte dans le processus de recherche d'équilibre.

C'est précisément la même logique, bien qu'inversée, qui permet de limiter les effets négatifs sur la population civile à ceux d'entre eux qui sont concrets. Laisser entendre qu'une partie au conflit devrait renoncer à une opération qui offrirait probablement de réels bénéfices liés au conflit et ce, sur la base de spéculations quant aux éventuels effets négatifs sur la population civile, reviendrait à fausser, de manière abusive, l'équilibre recherché.

L'autre différence considérable entre la doctrine proposée et le principe de proportionnalité est que l'expression « avantage militaire » a été remplacée par l'expression « avantage lié au conflit ». L'avantage militaire est un concept interprété de façon stricte en DIH. Par exemple, aux termes du Manuel Harvard :

> L'avantage militaire renvoie uniquement à un avantage qui est directement lié aux opérations militaires et non à d'autres formes d'avantages qui peuvent, dans une

85 Commentaire CICR des Protocoles additionnels, *op. cit.* note 52, par. 2209.

86 Michael Bothe, Karl Josef Partsch et Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, 2e éd., Martinus Nijhoff, Leiden et Boston, MA, 2013, p. 407. Voir également Ministère de la Défense du Royaume-Uni, *The Manual of the Law of Armed Conflict*, 2004 (Manuel du droit de la guerre du Royaume-Uni), par. 5.33.3.

87 M. Bothe, K. J. Partsch et W. A. Solf, *op. cit.* note 86, p. 407.

> certaine mesure, être liées au conflit de façon plus générale. L'avantage militaire ne renvoie pas à un avantage d'ordre exclusivement politique, psychologique, économique, financier, social ou moral. Ce faisant, contraindre l'ennemi à changer les termes de sa négociation en se contentant d'influer sur le moral de la population civile ne saurait être considéré comme un avantage militaire [traduction CICR][88].

La doctrine ne limiterait pas l'avantage obtenu grâce à des cyberopérations à un avantage qui est purement militaire. Si l'on reprend l'exemple cité plus haut, il serait acceptable d'envisager de mener des cyberopérations destinées à modifier les termes de négociation de l'ennemi, même en influant sur le moral de la population civile. Les États envisagent déjà des cyberopérations ne constituant pas une attaque, comme celles qui altèrent ou suppriment des données, dont les effets ne sont pas strictement militaires. Compte tenu de la probable résistance que ceux-ci opposeraient à l'adoption d'une règle qui imposerait la nécessité d'un avantage militaire, la proposition s'abstient d'employer le mot « militaire[89] ».

Il convient de souligner que le mot « avantage » renvoie généralement à l'avantage militaire que la partie attaquante obtient sur le plan tactique ou opérationnel de la guerre et non sur le plan stratégique, au sens politique du terme[90]. En d'autres termes, l'avantage doit avoir un impact sur le champ de bataille ou la campagne en question qui ne soit pas trop faible[91]. Par exemple, le fait d'amener les chefs militaires ennemis à reconsidérer leur participation au conflit, par exemple en s'attaquant à leurs biens ou à leurs avoirs personnels, constituerait un avantage, mais cela n'aurait pas pour effet de qualifier ces cibles d'objectifs militaires et ne justifierait pas les dommages collatéraux qu'elles pourraient subir comme c'est le cas lors de l'examen de la proportionnalité.

88 Manuel de Harvard, *op. cit.* note 80, p. 36.

89 Comme indiqué dans la déclaration du Royaume-Uni accompagnant la ratification du PA I, « l'avantage militaire escompté d'une attaque s'entend de l'avantage que l'on compte tirer de cette attaque considérée dans son ensemble, et non de celui qui découlerait d'éléments isolés ou déterminés de l'attaque ». Déclaration du Royaume-Uni sur la ratification du Protocole additionnel, par. i), disponible sur : https://ihl-databases.icrc.org/applic/ihl/dih.nsf/Notification.xsp?action=openDocument&documentId=BEFB567C3CA41A7BC12563FF0047E495.

90 « Tactical level of warfare — The level of warfare at which battles and engagements are planned an executed to achieve military objectives assigned to tactical units or task forces » : Département de la Défense des États-Unis, *Dictionary of Military and Associated Terms*, en vigueur en mars 2018, p. 226 ; « Operational level of warfare — The level of warfare at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas » : *ibid*., p. 173 ; « Strategic level of warfare — The level of warfare at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives » : *ibid*., p. 219.

91 Manuel du droit de la guerre du Royaume-Uni, *op. cit.* note 86, par. 5.33.5 ; Manuel de Harvard, *op. cit.* note 80, pp. 36-37 ; Manuel de Tallinn 2.0, *op. cit.* note 6, p. 442. Voir également Ian Henderson, *The Contemporary Law of Targeting*, Martinus Nijhoff, Boston, MA, 2009, pp. 199-202, qui propose une analyse plus approfondie de la question de savoir pourquoi l'avantage militaire peut être mesuré au niveau opérationnel contrairement au niveau tactique et pourquoi en principe il n'est pas approprié de mesurer l'avantage militaire au niveau stratégique.

Toutefois, les États cherchent à obtenir un avantage au niveau stratégique qui n'est pas lié aux opérations sur le champ de bataille et, dans cet objectif, ils peuvent, conformément au DIH, mener des opérations militaires qui, bien qu'elles s'en approchent, ne constituent pas une attaque. Ainsi, pour être acceptable pour les États, la doctrine proposée permet que des bénéfices concrets à tous les niveaux de la guerre soient pris en considération pour évaluer si une cyberopération peut être lancée. À titre d'exemple, le fait d'empêcher l'ennemi de diffuser de la propagande liée au conflit auprès de la population au moyen d'opérations de déni de service contre les médias, constituerait un avantage à mettre dans la balance.

Malgré cet élargissement du champ d'application du principe de proportionnalité, la doctrine limite les bénéfices à ceux pour lesquels le lien avec le conflit est clair. Bien que certains pourraient reprocher à la doctrine d'être trop restrictive, elle a pour but de renforcer la protection contre les perturbations que peut subir la population civile lors d'un conflit armé, une situation sans aucun doute, déjà épouvantable. Les cyberopérations malveillantes ou à titre de représailles dirigées contre des personnes civiles ou la population civile devraient être interdites.

Il ne faut pas confondre cette obligation avec l'application du principe de nécessité militaire. Selon certaines interprétations de ce principe, « seuls ce degré et ce type de force, que le droit des conflits armés n'interdit pas par ailleurs et qui sont nécessaires pour atteindre l'objectif légitime du conflit, à savoir la soumission complète ou partielle de l'ennemi le plus rapidement possible et en engageant le moins de dépenses possible [traduction CICR] », sont autorisés[92]. Appliquer ce principe ne suffirait pas pour résoudre les problèmes en question. Premièrement, comme indiqué, le principe de nécessité militaire ne s'applique qu'à l'usage de la force ; la doctrine proposée vise des cyberopérations que l'on peut difficilement décrire ainsi. Deuxièmement, si elle vise une nécessité fondée sur des considérations « militaires », l'expression « lié au conflit armé » employée dans la doctrine est plus générale. Troisièmement et surtout, considérer le principe de nécessité militaire comme une règle primaire du droit international qui s'applique indépendamment des autres règles primaires du droit international, se heurte à un refus. Cette question fut, en partie, à l'origine de désaccords sur le *Guide interprétatif sur la notion de participation directe aux hostilités* du CICR[93] et est considérée avec méfiance par certains spécialistes[94]. Je suis d'avis que la nécessité militaire est un principe fondateur du DIH,

92 Manuel du droit de la guerre du Royaume-Uni, *op. cit*. note 86, par. 2.2.

93 Un désaccord sur le chapitre IX du Guide interprétatif du CICR, *op. cit*. note 34, est apparu lorsque certains experts participant au projet se sont opposés à ce qu'ils considéraient comme une utilisation du principe en tant que règle de droit primaire. Voir, par exemple, W. Hays Parks, « Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect », *Journal of International Law and Politics de l'Université de New York*, vol. 42, n° 3, 2010, pp. 802-810. Mais voir la réponse de Nils Melzer, qui travaillait alors à la Division juridique du CICR et qui a dirigé le projet : Nils Melzer, « Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation to Hostilities », *Journal of International Law and Politics de l'Université de New York*, vol. 42, n° 3, 2010, pp. 892-912.

94 Pour un point de vue intéressant, voir Manuel du droit de la guerre des États-Unis, *op. cit*. note 10, par. 16.5.2. (les opérations qui ne peuvent pas être qualifiées d'attaque « ne doivent pas [pour autant] être dirigées contre des personnes civiles ou des biens de caractère civil ennemis, à moins que les opérations ne soient militairement nécessaires »). Cette position a été critiquée et à juste titre. Voir

mais pas une règle primaire[95]. Quelle que soit la bonne interprétation, le principe de nécessité militaire ne peut pas atteindre les buts recherchés par l'adoption de la doctrine proposée.

Enfin, comme pour le principe de proportionnalité, le critère proposé dans la doctrine s'applique *ex ante* et non *post factum* ; cela ressort de l'emploi des termes « attendu » et « dont on peut attendre [que] ». Ainsi, ceux qui appliquent la doctrine seront jugés par rapport aux faits tels qu'ils les auront raisonnablement appréciés au moment où la cyberopération a été planifiée, approuvée et exécutée.

Remarques conclusives

L'état actuel du DIH régissant les cyberopérations n'est pas entièrement satisfaisant. Dans le meilleur des cas, le manque de clarté quant à la question de savoir quelles cyberopérations peuvent être qualifiées d'attaques, expose les civils à des risques auxquels ils ne devraient par ailleurs, en aucune circonstance, aucunement être exposés et, au pire, laisse toute latitude aux États qui entendent profiter de ces imprécisions pour monter des cyberopérations qui engendrent de graves perturbations pour la population civile. De plus, certaines cyberopérations qui, clairement, ne pourraient pas être qualifiées d'attaque, pourraient néanmoins semer le chaos au sein de la population civile.

La question de savoir si les données sont des biens complique le problème. D'une part, si tel est le cas, de nombreuses cyberopérations actuellement menées par des États seraient interdites. Aussi louable que puisse être leur intention, les partisans de cette position ont la naïveté de croire que cette interprétation sera acceptable pour les États dotés de cybercapacités[96]. Mais, d'autre part, ne pas considérer certaines données civiles comme des biens de caractère civil qui bénéficient de la protection du DIH revient à sous-estimer les considérations humanitaires qui justifient l'interdiction d'attaquer des biens de caractère civil. Lorsqu'il s'agit de trouver un juste équilibre entre les considérations humanitaires et la nécessité militaire, aucun des deux arguments n'est à la hauteur.

Les doctrines proposées ont été conçues en tenant compte de ces réalités. Dans un premier temps, les États peuvent ne pas leur faire bon accueil. Une telle réaction est souvent observée lorsque des universitaires et des organisations non gouvernementales cherchent à limiter la marge de manœuvre des États sur le champ de bataille et, dans de nombreux cas, cette réaction est justifiée. Toutefois, dans de tels cas, les États devraient garder à l'esprit les considérations suivantes.

Premièrement, d'après mes discussions avec des cyberopérateurs, il semblerait que certains éléments des doctrines existent déjà sous la forme de règles

William H. Boothby et Wolff Heintschel von Heinegg, *The Law of War: A Detailed Assessment of the Deparment of Defense Law of War Manual*, Cambridge University Press, Cambridge, 2018.

95 M. N. Schmitt, *op. cit*. note 19.

96 À ce sujet, des travaux intéressants sont menés par le lieutenant-colonel Bart van den Bosch (armée néerlandaise) dans le cadre d'un doctorat à l'université d'Amsterdam (« Waging War Without Violence ») sous la direction du professeur Terry Gill et du brigadier général Paul Duchiene.

d'engagement, d'autres orientations ou simplement de pratiques acceptées. Fait plus important encore, l'article 57, paragraphe 1 du PA I impose aux parties à un conflit de tenir compte des éventuelles conséquences négatives pour la population civile ou les biens de caractère civil pendant les opérations militaires, notamment mais pas seulement en cas d'attaques. Je pense que cette obligation relève du DIH coutumier, tant des groupes d'experts que des manuels militaires confirmant que l'expression « en veillant constamment » vise à imposer une obligation positive, bien qu'elle soit générale et mal définie[97]. Les deux doctrines proposées ne font que fournir des orientations quant aux mesures à prendre pour respecter ce constat.

À cet égard, d'aucuns pourraient dire que l'objectif des doctrines est déjà atteint par l'application de la clause de Martens, car les situations abordées sont des situations qui devraient être soumises aux « lois de l'humanité » et aux « exigences de la conscience publique ». Pourtant, les États et les experts ne partagent pas le même avis sur les moyens de mettre en œuvre cette clause et sur la question de savoir si elle impose aux parties à un conflit des règles de droit spécifiques et contraignantes. Indépendamment de la position de chacun sur ces questions, la clause de Martens est connue pour son manque de précision et son peu d'application en pratique. Cela étant, les doctrines proposées offrent un degré de précision et d'orientation d'un point de vue pratique qui peuvent permettre de procurer une véritable protection à la population civile.

Deuxièmement, l'interdiction d'attaquer des infrastructures cybernétiques ou des données qui perturberaient des fonctions ou des services civils essentiels, est conforme au principe général selon lequel certaines activités, fonctions et certains biens méritent une protection spéciale contre les effets dommageables de la guerre. Les doctrines proposées admettent simplement que le système existant doit être étendu pour tenir compte des risques exceptionnels et parfois graves qui pèsent sur la population civile en cas de cyberopérations. De plus, elles laissent aux États le soin de déterminer quels fonctions et services peuvent être qualifiés d'essentiels et méritent, à ce titre, une protection spéciale, à tout le moins par principe.

Troisièmement, les lecteurs perspicaces auront remarqué que la seconde doctrine qui oblige à rechercher un équilibre est plus stricte en ce qui concerne les opérations qui ne peuvent pas être qualifiées d'attaques contre des objectifs militaires qu'en ce qui concerne celles qui constituent des attaques. Selon la règle de proportionnalité applicable aux cyberattaques, seuls les dommages (y compris, vraisemblablement, la perte de fonctionnalité), les blessures et les décès doivent être

97 Voir Manuel du droit de la guerre du Royaume-Uni, *op. cit*. note 86, par. 5.32.1 (« Ainsi, le commandant devra garder à l'esprit les effets que ce qu'il prévoit de faire pourrait avoir sur la population civile et prendre des mesures pour réduire ces effets le plus possible ») ; Manuel de Harvard, *op. cit*. note 80, p. 142 (« L'expression "en veillant constamment" signifie que l'obligation d'épargner la population civile, les personnes civiles et les biens de caractère civil n'admet aucune exception [traduction CICR] ») ; Manuel de Tallinn 2.0, *op. cit*. note 6, p. 477 (qui relève l'« importante obligation générale de "respecter" la population civile, c'est-à-dire de tenir compte des effets néfastes des opérations militaires sur les civils »). Par ailleurs, le Manuel de Tallinn 2.0 indique que « l'obligation d'agir en veillant constamment à épargner la population civile impose aux commandants et à tous les autres acteurs participant aux opérations de toujours prendre en compte les effets de leurs activités sur la population civile et les biens de caractère civil, et de chercher à éviter tout effet inutile [traduction CICR] » (p. 477).

pris en considération. En revanche, la doctrine proposée couvre tous les effets négatifs sur la population civile. Cela pourrait sembler contre-intuitif, mais le résultat est compensé par le fait que la doctrine est plus permissive s'agissant de ce dont la partie dirigeant la cyberopération peut tenir compte pour contrebalancer ces effets négatifs. Le principe de proportionnalité se limite à l'avantage militaire concret et direct. Au contraire, la doctrine proposée permet de tenir compte de bénéfices qui ne sont ni directs ni militaires par nature et ces bénéfices peuvent s'accroître sur le plan stratégique. Ainsi, la doctrine permet d'obtenir un juste équilibre entre les considérations humanitaires et les intérêts de l'État. Les États peuvent trouver davantage de réconfort dans le fait que la doctrine retienne le critère du caractère excessif, qui offre aux parties au conflit une importante marge d'appréciation lorsqu'ils appliquent la doctrine.

Ces propositions ne sont pas la panacée pour ce qui est des préjudices causés aux personnes civiles et à la population civile par des cyberopérations, qui ne sont ni des destructions ni des dommages. Une grande partie de ces préjudices reste sans réponse, comme pour l'application du principe de proportionnalité aux cyberattaques, car ce principe ne s'applique qu'en cas de dommages collatéraux, de blessures et de décès. Il n'en reste pas moins que les États et la communauté internationale doivent toujours répondre aux questions humanitaires avant qu'elles prennent une tournure tragique sur le champ de bataille. En l'occurrence, c'est maintenant qu'ils doivent y répondre.