# Sortez de mon « Cloud » : la cyberguerre, le droit international humanitaire et la protection des civils

**Cordula Droege***

Cordula Droege est cheffe de l'unité des conseillers juridiques aux opérations, division juridique, Comité international de la Croix-Rouge.

## Résumé

*La cyberguerre figure en bonne place parmi les préoccupations des responsables politiques et des commandements militaires de la planète. De nouvelles unités dédiées à la cybersécurité sont créées à différents niveaux de gouvernement, y compris dans les forces armées. Le recours à des cyberopérations dans des situations de conflit armé, cependant, risque d'avoir des conséquences très graves, surtout si leur effet ne se limite pas aux données du système informatique ou de l'ordinateur pris pour cible. De fait, les cyberopérations sont généralement censées avoir un impact dans le « monde réel ». En altérant le fonctionnement des systèmes informatiques sous-jacents, par exemple, on peut manipuler les systèmes de contrôle du trafic aérien, les oléoducs ou les centrales nucléaires d'un ennemi. Certaines cyberopérations peuvent avoir un impact humanitaire énorme pour la population civile. Il est donc important d'examiner les règles*

* Je tiens à remercier mes collègues du CICR, Knut Dörmann, Bruno Demeyere, Raymond Smith, Tristan Ferraro, Jelena Pejic et Gary Brown, pour leurs observations judicieuses sur les versions antérieures de cet article, ainsi que Nele Verlinden pour son aide en matière de références. Les opinions exprimées dans cet article sont celles de l'auteure et pas nécessairement celles du CICR. Sauf précision contraire, toutes les références sur Internet ont été consultées en octobre 2012.
La version originale en anglais est publiée sous le titre : « Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians », dans International Review of the Red Cross, Vol. 94, N° 886, été 2012, pp. 533-578.

*du droit international humanitaire (DIH) qui régissent ce type d'opérations, puisque l'un des principaux objectifs de ce corpus de droit est de protéger les civils des effets de la guerre. L'auteure de cet article se penche sur quelques-unes des questions qui se posent lorsque l'on applique le DIH à la cybertechnologie alors que cette branche du droit a été conçue pour réglementer la guerre classique, c'est-à-dire cinétique. La première est : quand la cyberguerre est-elle véritablement une guerre au sens de « conflit armé » ? Après avoir examiné cette question, l'article passe en revue trois règles qui figurent parmi les plus importantes du DIH régissant la conduite des hostilités – les principes de distinction, de proportionnalité et de précaution – ainsi que leur interprétation dans la cybersphère. La cybersphère suscite un certain nombre de questions concernant ces règles qui sont encore sans réponse. L'interconnexion propre au cyberespace, notamment, met en question le postulat essentiel sur lequel se fondent les règles relatives à la conduite des hostilités, à savoir que l'on peut et que l'on doit en tout temps faire la distinction entre biens civils et biens militaires. Il reste donc à voir si les normes traditionnelles du DIH protégeront suffisamment les civils des effets de la cyberguerre. Leur interprétation, quant à elle, devra sans nul doute tenir compte des caractéristiques spécifiques du cyberespace. Et, en l'absence d'une meilleure connaissance des effets potentiels de la cyberguerre, on ne saurait exclure que des règles plus strictes s'avèrent nécessaires.*

**Mots-clés :** cybersécurité ; cyberguerre ; cyberattaque ; droit international humanitaire ; cyberopération ; cyberarme ; conflit armé dans le cyberespace ; conduite des hostilités ; distinction ; proportionnalité ; attaque sans discrimination ; précaution.

: : : : : : :

## Introduction

La cyberguerre figure en bonne place parmi les préoccupations des décideurs et des commandements militaires de la planète. Une étude publiée récemment par l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) décrit les mesures prises par trente-trois États qui ont spécifiquement incorporé la cyberguerre dans leur planification et leur organisation militaires, et donne une vue d'ensemble de la stratégie de cybersécurité de trente-six autres États[1]. Si certains de ces États s'appuient sur une doctrine très avancée et des organisations militaires employant des centaines de milliers de personnes, d'autres ont des dispositifs moins élaborés qui intègrent cyberattaques et cyberguerre dans

1 Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare- Preliminary Assessment of National Doctrine and Organization*, UNIDIR Resources Paper, 2011, disponible sur : http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf. Voir aussi Eneken Tikk, *Frameworks for International Cyber Security*, Centre d'excellence de cyberdéfense de l'OTAN, CCD COE Publications, Tallinn, 2011.

leurs capacités existantes de guerre électronique. Plusieurs États créent des unités spécialisées au sein ou à l'extérieur de leurs forces armées pour effectuer les cyberopérations[2]. Il semblerait aussi que douze des quinze plus grandes forces militaires du monde mettent au point des programmes de cyberguerre[3].

### *La cybersécurité en général et la cyberguerre en particulier*

Si l'on parle souvent de la cybersécurité en général, le grand public en sait encore très peu sur la planification et les politiques militaires des États en matière de cyberguerre. Il semble que la plupart des stratégies gouvernementales combinent aspects défensifs et offensifs. D'une part, les États prennent de plus en plus de mesures visant à protéger des cyberattaques leurs propres infrastructures critiques. D'autre part, il semble qu'ils se dotent aussi des capacités technologiques nécessaires pour pouvoir lancer des cyberopérations contre la partie adverse en période de conflit armé[4].

Décideurs politiques et commentateurs débattent de la question de savoir s'il faudrait interdire purement et simplement la totalité ou certaines des nouvelles « cyberarmes », s'il vaudrait mieux envisager des mesures de confiance (comme dans le cas du désarmement nucléaire)[5], ou s'il faudrait établir un « code de la route » qui réglementerait le comportement dans le cyberespace[6]. Voilà maintenant plus de dix ans que l'on discute aussi de la nécessité d'un nouveau traité sur la cybersécurité. La Fédération de Russie plaide en faveur d'un tel traité depuis la fin des années 1990, tandis que les États-Unis et les autres pays occidentaux sont d'avis qu'un traité n'est pas nécessaire[7]. Dans une lettre adressée au Secrétaire général

2 Voir, par exemple, Ellen Nakashima, « Pentagon to boost cybersecurity force », dans *The Washington Post*, 27 janvier 2013 ; Gordon Corera, « Anti-cyber threat centre launched », dans *BBC News*, 2 mars 2013.

3 Scott Shane, « Cyberwarfare Emerges from Shadows of Public Discussion by U.S. Officials », dans *New York Times*, 26 septembre 2012, p. A10.

4 *Ibid*.

5 Ben Baseley-Walker, « Les mesures de transparence et de confiance dans le cyberespace : vers des normes de conduite », dans Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR), *Forum du désarmement,* « Faire face aux cyberconflits », N° 4, 2011, pp. 33-43, disponible sur : http://www.unidir.org/files/publications/pdfs/faire-face-aux-cyberconflits-fr-317.pdf ; James Andrew Lewis, *Confidence-building and international agreement in cybersecurity*, disponible sur : http://www.unidir.org/pdf/articles/pdf-art3168.pdf.

6 Voir William Hague, « Security and freedom in the cyber age – seeking the rules of the road », discours prononcé à la Conférence sur la sécurité de Munich, 4 février 2011, disponible sur : https://www.gov.uk/government/speeches/security-and-freedom-in-the-cyber-age-seeking-the-rules-of-the-road, et *Foreign Secretary opens the London Conference on Cyberspace*, 1er novembre 2011, disponible sur : https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace.

7 Voir le projet de résolution soumis par la Fédération de Russie à la Première Commission de l'Assemblée générale en 1998, lettre datée du 23 septembre 1998, adressée au Secrétaire général par le Représentant permanent de la Fédération de Russie auprès de l'Organisation des Nations Unies, Doc. ONU A/C.1/53/3, 30 septembre 1998 ; John Markoff et Andrew E. Kramer, « U.S. and Russia Differ on a Treaty for Cyberspace », dans *New York Times*, 28 juin 2009, p. A1 ; John Markoff et Andrew E. Kramer, « In Shift, U.S. Talks to Russia on Internet Security », dans *New York Times*, 13 décembre 2009, p. A1. Voir aussi Adrian Croft, « Russia says many states arming for cyber warfare », Reuters, 25 avril 2012, disponible sur : http://www.reuters.com/article/2012/04/25/

des Nations Unies en septembre 2011, la Chine, la Fédération de Russie, l'Ouzbékistan et le Tadjikistan proposaient un Code de conduite international concernant la sécurité de l'information, mais la portée de leur proposition dépassait largement les seules situations de conflit armé[8]. La Chine, la Fédération de Russie, le Kazakhstan, le Kirghizistan, l'Ouzbékistan et le Tadjikistan sont également parties à un accord adopté dans le cadre de l'Organisation de coopération de Shanghai en 2009[9]. L'Inde, la République islamique d'Iran, la Mongolie et le Pakistan participent en tant qu'observateurs. D'après une traduction anglaise non officielle de cet accord, il semble qu'il donne aux notions de « guerre » et d'« arme » un sens plus large que leur sens classique en droit international humanitaire[10].

Ce débat – dans lequel toutes les parties s'accusent les unes les autres, de façon plus ou moins voilée, d'espionnage et de prolifération d'armements[11] – reste très général du point de vue juridique. Aucune distinction n'est faite, en particulier, entre les situations de conflit armé et les autres, bien que ce soit important pour l'applicabilité du DIH. L'essentiel des préoccupations semble se concentrer sur l'espionnage, tant contre l'État que contre des intérêts économiques, mais il est

germany-cyber-idUSL6E8FP40M20120425 ; Keir Giles, « Russia's Public Stance on Cyberspace Issues », document publié à la quatrième Conférence internationale sur les cyberconflits tenue en 2012, Christian Czosseck, Rain Ottis et Katharina Ziolkowski (éds.), Centre d'excellence de cyberdéfense de l'OTAN, CCD COE Publications, Tallinn, 2012, disponible sur : http://www.conflictstudies.org.uk/files/Giles-Russia_Public_Stance.pdf.

8 Lettre datée du 12 septembre 2011, adressée au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, de l'Ouzbékistan et du Tadjikistan, Doc. ONU A/66/359 du 14 septembre 2011.

9 Accord entre les gouvernements des États membres de l'Organisation de coopération de Shanghai sur la coopération dans le domaine de la sécurité de l'information au niveau international.

10 Disponible sur : http://www.npr.org/templates/story/story.php?storyId=130052701 puis lien « Read the Shanghai Accord on 'Information Security' », http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf. L'annexe 1 définit la « guerre de l'information » comme une « confrontation entre deux ou plusieurs États dans l'espace de l'information, visant à endommager les systèmes d'information, ainsi que les procédés, ressources, infrastructures critiques et autres structures dans le domaine de l'information, à saper les systèmes politiques, économiques et sociaux, à exercer un conditionnement psychologique de masse pour déstabiliser la société et l'État, et forcer celui-ci à prendre des décisions qui soient dans l'intérêt d'une partie adverse ». L'annexe 2 précise que le danger de « développement et [d']utilisation d'armes de l'information, de préparation et de lancement d'une guerre de l'information » provient « de la création et du développement d'armes de l'information qui représentent un danger immédiat pour des structures essentielles des États, ce qui risque de mener à une nouvelle course aux armements et constitue une menace grave dans le domaine de la sécurité de l'information au niveau international. Ce danger a notamment les caractéristiques suivantes : utilisation d'armes de l'information pour préparer et mener une guerre de l'information et mettre à mal les transports, les systèmes de communication et de contrôle aérien, les systèmes de défense antimissile et autres, de telle façon que l'État perde ses capacités de défense face à l'agresseur et ne parvienne pas à exercer son droit légitime à l'autodéfense ; perturbation du fonctionnement des infrastructures d'information, ce qui entraîne l'effondrement des systèmes administratifs et décisionnels dans les États visés ; et impact destructeur sur des structures d'une importance critique ». [Traduction CICR]

11 Kenneth Lieberthal et Peter W. Singer, « Cybersecurity and U.S.-China Relations », dans *China US Focus,* 23 février 2012, disponible sur : http://www.chinausfocus.com/library/think-tank-resources/us-lib/peacesecurity-us-lib/brookings-cybersecurity-and-u-s-china-relations-february-23-2012/ ; Mandiant Intelligence Centre Report, *APT1: Exposing one of China's Cyber Espionage Units*, disponible sur : http://intelreport.mandiant.com/?gclid=CKD6-7Oo3LUCFalxOgod8y8AJg ; Ellen Nakashima, « US said to be target of massive cyber-espionnage campaign », dans *The Washington Post*, 11 février 2013 ; « North Korea says US 'behind hack attack' », dans *BBC News*, 15 mars 2013.

aussi question de cyberguerre et de la nécessité d'éviter la prolifération d'armes dans le cyberespace. Il n'est généralement pas établi de différenciation entre les situations de conflit armé et d'autres situations dans lesquelles des cyberopérations menacent la sécurité d'États, d'entreprises ou de ménages. La plupart des débats sur la cybersécurité ne mentionne même pas les situations de conflit armé, et l'on ne sait pas si ces situations sont implicitement incluses. De fait, à bien des égards – surtout en ce qui concerne la protection des infrastructures informatiques contre l'infiltration, la manipulation ou la détérioration – peu importe si une cyberattaque a lieu dans un contexte de conflit armé ou pas. Les moyens techniques de protection de l'infrastructure seront pour l'essentiel les mêmes. Cependant, s'il est probablement juste de dire que la plupart des menaces dans la cybersphère ne sont pas immédiatement liées à des situations de conflit armé mais relèvent plutôt de l'espionnage économique ou d'autres formes d'espionnage, ou encore de la cybercriminalité organisée, il est tout aussi évident que le recours aux cyberarmes et aux cyberopérations joue un rôle croissant dans les conflits armés et que les États se préparent activement à cette nouvelle donne.

En même temps, il règne une certaine confusion quant à l'applicabilité du DIH à la cyberguerre – confusion qui pourrait en fait provenir de conceptions différentes de ce qu'est la cyberguerre elle-même, allant des cyberopérations menées dans le contexte de conflits armés au sens du DIH à des cyberactivités criminelles de tous ordres. Certains États, comme les États-Unis[12], le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord[13] et l'Australie[14] ont déclaré que le DIH s'appliquait à la cyberguerre[15]. Cependant, ces prises de position publiques ne détaillent pas encore des questions telles que le seuil d'intensité à partir duquel il y a conflit armé, la définition des « attaques » en DIH, ou les implications de la cyberguerre en ce qui concerne les « biens à double usage ». Il a été dit que la Chine n'acceptait pas l'applicabilité du DIH à la cyberguerre[16]. On peut se demander, toutefois, si telle

12 Harold Koh, « International Law in Cyberspace », discours prononcé à la Conférence juridique interinstitutionnelle du cybercommandement des États-Unis (U.S. Cyber Command Inter-Agency Legal Conference), 18 septembre 2012, disponible sur : http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/ ; Rapport du Secrétaire général sur « Les progrès de l'informatique et de la télématique et la question de la sécurité internationale » (ci-après « Rapport du Secrétaire général »), 15 juillet 2011, Doc. ONU A/66/152, p. 17. Voir aussi, dans la stratégie des États-Unis pour le cyberespace : « Les normes internationales traditionnelles qui guident le comportement des États – en temps de paix comme de conflit – s'appliquent aussi dans le cyberespace. Néanmoins, du fait de certaines caractéristiques spécifiques de la technologie en réseau, il faut effectuer un travail supplémentaire pour préciser comment ces normes s'appliquent et quels accords additionnels pourraient être nécessaires pour les compléter » [traduction CICR], dans *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*, mai 2011, disponible sur : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

13 Rapport du Secrétaire général, 23 juin 2004, Doc. ONU A/59/116, p. 12 ; Rapport du Secrétaire général, 20 juillet 2010, Doc. ONU A/65/154, p. 16.

14 Rapport du Secrétaire général, *op. cit.*, note 12, p. 11.

15 Voir aussi la proposition de la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité, *Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé*, Bruxelles, 7.2.2013, JOIN (2013) 1 final.

16 Voir, par ex., Adam Segal, « China, International Law and Cyber Space », dans *Council on Foreign Relations*, 2 octobre 2012, disponible sur : http://blogs.cfr.org/asia/2012/10/02/china-international-law-and-cyberspace/.

serait réellement la position officielle de ce pays dans une situation de conflit armé au sens du DIH. Selon un autre point de vue :

> La position de la Chine est que les nations, partout dans le monde, devraient chérir les valeurs du cyberespace – le premier espace social créé par l'espèce humaine – et devraient fermement s'opposer à la militarisation de l'internet … Elle estime que la Charte des Nations Unies en vigueur et les lois existantes relatives aux conflits armés, ainsi que les principes essentiels du droit international humanitaire relatifs à la guerre et à l'emploi ou à la menace de la force s'appliquent encore tous au cyberespace – en particulier les impératifs de « non-recours à la force » et de « règlement pacifique des différends internationaux », ainsi que les principes de distinction et de proportionnalité en ce qui concerne les moyens et méthodes de guerre[17].

À notre connaissance, la Fédération de Russie n'a pas pris officiellement position sur l'applicabilité du DIH à la cyberguerre[18].

D'un point de vue juridique, il est important de faire la distinction entre la cyberguerre consistant en des cyberopérations menées dans le contexte de conflits armés au sens du DIH, et les cyberopérations menées en dehors de ce contexte. Ce n'est que dans le cadre de conflits armés que les règles du DIH s'appliquent, imposant des restrictions précises aux parties au conflit[19]. Ainsi, dans le présent article, le terme « cyberguerre » s'entendra uniquement de moyens et méthodes de combat consistant en des cyberopérations équivalant à un conflit armé ou menées dans le contexte d'un conflit armé au sens du DIH. Ces cyber-

17 Li Zhang, « A Chinese perspective on cyber war », dans cette publication. Dans son discours devant la Première Commission en septembre 2011, l'ambassadeur de la Chine a fait les propositions suivantes : « Les pays doivent s'engager à ne pas utiliser l'information et la technologie cybernétique pour mener des activités hostiles au détriment de la paix et de la sécurité internationales, à ne pas développer non plus des armes de l'information … », et « Les pays doivent veiller à ce que l'information et le cyberespace ne deviennent pas un nouveau champ de bataille ». Il n'est pas fait mention du DIH. Voir la déclaration sur la sécurité de l'information et du cyberespace faite par S.E. l'ambassadeur Wang Qun à la Première Commission pendant la 66e session de l'Assemblée générale, « Work to Build a Peaceful, Secure and Equitable Information and Cyber Space », New York, 20 octobre 2011, disponible sur : http://www.fmprc.gov.cn/eng/wjdt/zyjh/t869580.htm.

18 La doctrine militaire de la Fédération de Russie dont il est fait état ne mentionne pas le DIH en ce qui concerne la guerre de l'information. Voir « The Military Doctrine of the Russian Federation Approved by Russian Federation Presidential Edict on 5 February 2010 », disponible sur : http://www.sras.org/military_doctrine_russian_federation_2010. Il n'en est pas fait mention non plus par K. Giles, *op. cit.*, note 7. Roland Heikerö, « Emerging Threats and Russian Views on Information Warfare and Information Operations », FOI Swedish Defence Research Agency, mars 2010, p. 49, disponible sur : http://www.highseclabs.com/Corporate/foir2970.pdf, rapporte que la Fédération de Russie a proposé « l'application des règles de droit humanitaire interdisant les attaques contre les non-combattants, ainsi qu'une interdiction de la tromperie dans le cyberespace » [Traduction CICR].

19 Pour le Comité international de la Croix-Rouge (CICR), il est important d'attirer l'attention sur la situation spécifique des cyberopérations équivalant à des conflits armés ou conduites dans le contexte de conflits armés – c'est-à-dire de la « cyberguerre » au sens strict du terme. En effet, le CICR a, en vertu des Conventions de Genève de 1949, le mandat spécifique de fournir assistance et protection aux victimes de conflits armés. Il a également reçu de la communauté internationale mandat de travailler à la compréhension et à la diffusion du DIH. Voir, par ex., art. 126(5) de la CG III, art. 143(5) de la GC IV, et art. 5(2)(g) des Statuts du Mouvement international de la Croix-Rouge et du Croissant-Rouge.

opérations – souvent appelées également « attaques de réseaux informatiques » – sont dirigées contre ou lancées via un ordinateur ou un système informatique au moyen d'un flux de données[20]. Elles peuvent avoir divers objectifs, par exemple infiltrer un système informatique pour collecter, exporter, détruire, altérer ou crypter des données, ou pour déclencher, détourner ou manipuler de toute autre manière des processus contrôlés par le système infiltré. En d'autres termes, l'analyse qui suit porte sur des hostilités consistant à élaborer un code informatique et à l'envoyer d'un ou plusieurs ordinateurs aux ordinateurs ciblés.

### *La préoccupation humanitaire*

La préoccupation humanitaire que la cyberguerre suscite pour le CICR tient essentiellement à l'impact que ce type de guerre pourrait avoir sur la population civile – notamment parce que les cyberopérations pourraient gravement toucher les infrastructures civiles[21] en raison de plusieurs caractéristiques propres à la cybersphère.

Tout d'abord, du fait qu'elles dépendent de plus en plus de systèmes informatiques, les infrastructures civiles sont très vulnérables aux attaques de réseaux informatiques. Un certain nombre d'installations d'une importance cruciale telles que centrales électriques, centrales nucléaires, barrages, systèmes de traitement et de distribution de l'eau, chemins de fer et infrastructure de contrôle aérien, en particulier, dépendent de « systèmes d'acquisition et de contrôle des données » (ou systèmes SCADA) et de « systèmes de contrôle réparti » (systèmes DCS). Ces systèmes, qui constituent le lien entre les mondes numérique et physique, sont extrêmement vulnérables à l'intervention extérieure de pratiquement n'importe quel agresseur[22].

Ensuite, les infrastructures civiles sont menacées par l'interconnectivité propre à l'internet. La plupart des réseaux militaires reposent en effet sur une infrastructure informatique civile, essentiellement commerciale, par exemple les câbles sous-marins à fibre optique, les satellites, les routeurs ou les nœuds ; à l'inverse, il est de plus en plus fréquent que les véhicules civils et les infrastructures

20 US Department of Defense (département de la Défense des États-Unis), *Dictionary of Military and Associated Terms*, 8 novembre 2010 (tel que modifié au 31 janvier 2011), Washington, DC, 2010 : « Les attaques contre des réseaux informatiques sont des actions effectuées au moyen de réseaux informatiques dans le but de perturber, altérer ou détruire – ou refuser l'accès à – des informations résidentes dans des ordinateurs ou des réseaux d'ordinateurs, ou ces ordinateurs et réseaux eux-mêmes. » [Traduction CICR].

21 Dans le droit régissant la conduite des hostilités, « personnes civiles », « population civile » et « biens de caractère civils » sont des notions juridiques différentes auxquelles s'appliquent des règles différentes. Toutefois, lorsqu'il est fait mention, dans cet article, de l'impact de la cyberguerre sur la population civile, le concept englobe également les dommages aux infrastructures civiles, car c'est probablement surtout de cette façon que les cyberopérations toucheront la population civile.

22 Stefano Mele analyse des scénarios vraisemblables d'interférence avec différents types de systèmes militaires et civils, et déclare que la manipulation des systèmes de gestion de réseaux électriques représente probablement la plus grande menace à l'heure actuelle. Voir Stefano Mele, « Cyber Warfare and its Damaging Effects on Citizens », septembre 2010, disponible sur : http://www.stefanomele.it/public/documenti/185DOC-937.pdf.

de contrôle du trafic maritime et du trafic aérien soient équipés de systèmes de navigation dépendant de satellites GPS, qui sont également utilisés par l'armée. Ainsi, il est souvent impossible de différencier, parmi les infrastructures informatiques, celles qui sont purement civiles et celles qui sont purement militaires. Comme nous le verrons plus loin, cela représente un sérieux défi au respect de l'un des principes cardinaux du DIH, à savoir le principe de la distinction entre biens civils et militaires. De plus, même si les ordinateurs ou systèmes informatiques militaires et civils ne sont pas tout à fait les mêmes, l'interconnectivité signifie que les effets d'une attaque contre une cible militaire risquent de ne pas être limités à cette cible. Une cyberattaque peut en effet avoir des répercussions sur divers autres systèmes, y compris des systèmes et réseaux civils, par exemple en propageant des logiciels malveillants (ou «maliciels») tels que virus ou vers informatiques si ceux-ci sont incontrôlables. Cela signifie qu'une attaque contre un système informatique militaire risque bien d'endommager aussi des systèmes informatiques civils, ce qui risque à son tour d'être fatal pour certaines infrastructures civiles telles que les services d'approvisionnement en eau ou en électricité ou de transferts financiers.

Nous n'avons pas encore, à l'heure actuelle, d'exemples clairs de cyberattaques qui auraient eu lieu pendant un conflit armé, ni d'exemples dans lesquels la population civile aurait été gravement touchée par des attaques de réseaux informatiques pendant un conflit. Les spécialistes semblent toutefois convenir qu'il est techniquement réalisable, bien que difficile, d'interférer délibérément à partir du cyberespace avec les systèmes de contrôle aérien des aéroports, ou les systèmes de contrôle d'autres moyens de transport, de barrages ou de centrales nucléaires. On ne saurait, dès lors, exclure le risque de scénarios catastrophe comme les collisions entre avions, le dégagement de radiations de centrales nucléaires, le rejet de substances toxiques d'usines chimiques, ou l'arrêt du fonctionnement d'infrastructures et de services d'importance vitale tels que les réseaux d'approvisionnement en eau ou en électricité.

De tels scénarios ne seraient sans doute pas les plus vraisemblables. Il paraît beaucoup plus probable que des cyberopérations servent à manipuler des infrastructures civiles afin qu'elles subissent des dysfonctionnements ou des arrêts sans faire directement de morts ni de blessés. S'il est vrai que ce type de moyens et méthodes de guerre ne faisant pas « couler de sang » n'aurait pas d'effets aussi dramatiques pour les civils que les tirs d'artillerie ou les bombardements, il pourrait néanmoins avoir des conséquences graves – par exemple si l'approvisionnement en eau et en électricité est interrompu, ou si les réseaux de communication ou le système bancaire ne fonctionnent plus. Il convient dès lors d'avoir une vue plus précise de ces effets eux-mêmes et de clarifier comment les règles du DIH doivent en tenir compte.

Selon certains observateurs, le risque d'attaques informatiques contre les infrastructures civiles les plus importantes ne devrait pas être surestimé, notamment parce qu'il exigerait souvent que des cyberarmes offensives soient conçues spécifiquement pour porter atteinte à des systèmes informatiques cibles très

précis (comme dans le cas du virus Stuxnet[23], par exemple) et que ces armes ne pourraient pas facilement servir ensuite à atteindre d'autres cibles[24]. De plus, dans un contexte de système Internet interconnecté à l'échelle de la planète et d'économie mondialisée, les États pourraient hésiter à se nuire les uns aux autres, parce que les répercussions, par exemple sur leurs systèmes financiers, risqueraient de leur faire autant de tort qu'elles en feraient à leur adversaire[25]. Cela pourrait être le cas ou ne pas l'être. Le fait que les attaques de réseaux informatiques aient potentiellement la capacité de cibler des biens de caractère civil, puissent dans certains cas frapper ou être utilisées sans discrimination ou risquent d'avoir incidemment des conséquences dévastatrices pour les infrastructures civiles et la population civile elle-même justifie amplement que l'on clarifie les règles applicables à la conduite des hostilités que les parties à un conflit doivent respecter.

### *Le rôle du droit international humanitaire*

Dans ce contexte, comment le droit international humanitaire traite-t-il les conséquences potentielles de la cyberguerre sur la population civile ?

Les dispositions du DIH ne mentionnent pas précisément les cyberopérations. Pour cette raison, et parce que l'exploitation de la cybertechnologie est relativement nouvelle et semble parfois introduire un changement qualitatif radical dans les moyens et méthodes de guerre, il a parfois été allégué que le DIH est mal adapté à la cybersphère et ne peut s'appliquer à la cyberguerre[26]. Toutefois, l'absence de toute mention spécifique des cyberopérations dans le DIH ne signifie pas que ces opérations ne soient pas soumises aux règles du DIH. Toutes sortes de nouvelles technologies sont mises au point constamment, et le DIH est suffisamment large pour embrasser cette évolution. Il interdit ou limite l'emploi de certaines armes en particulier (par exemple, les armes chimiques ou biologiques, ou les mines antipersonnel), mais il réglemente aussi, par ses

23 Le « virus Stuxnet » a été lancé contre les installations iraniennes d'enrichissement de l'uranium de Natanz, ce qui aurait entraîné la destruction d'un millier de centrifugeuses. On a pu lire dans la presse que les États-Unis et/ou Israël auraient été à l'origine de ce virus, mais cela n'a pas été officiellement reconnu. David Albright, Paul Brannan et Christina Walrond, « Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment », ISIS Report (rapport de l'Institut pour la science et la sécurité internationale), 22 décembre 2010, disponible sur : http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ ; David E. Sanger, « Obama Order Sped Up Wave of Cyberattacks Against Iran », dans *New York Times*, 1er juin 2012, disponible sur : http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_moc.semityn.www.

24 Thomas Rid, « Think Again: Cyberwar », dans *Foreign Policy,* mars/avril 2012, pp. 5 et s., disponible sur : http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecomments=yes&page=full ; Thomas Rid et Peter McBurney, « Cyber-Weapons », dans *The RUSI Journal,* février-mars 2012, Vol. 157, N° 1, pp. 6-13. Voir aussi Maggie Shiels, « Cyber war threat exaggerated claims security expert », dans *BBC News*, 16 février 2011, disponible sur : http://www.bbc.co.uk/news/technology-12473809.

25 Stefano Mele (*op. cit.*, note 22) fait valoir que, pour cette raison, des attaques électroniques massives contre les systèmes financiers de pays étrangers sont peu probables.

26 Charles J. Dunlap Jr, « Perspectives for Cyber Strategists on Law for Cyberwar », dans *Strategic Studies Quarterly*, printemps 2011, p. 81.

dispositions générales, tous les moyens et méthodes de guerre, et notamment l'utilisation de toutes les armes. L'article 36 du Protocole additionnel I aux Conventions de Genève, en particulier, précise :

> 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, une Haute Partie contractante a l'obligation de déterminer si l'emploi en serait interdit, dans certaines circonstances ou en toutes circonstances, par les dispositions du présent Protocole ou par toute autre règle du droit international applicable à cette Haute Partie contractante.

Outre l'obligation spécifique qu'elle impose aux États parties au Protocole additionnel I, cette disposition montre que les règles du DIH s'appliquent aux nouvelles technologies.

Cela dit, la cyberguerre pose un défi au respect de quelques-uns des postulats essentiels du DIH. Premièrement, cette branche du droit est fondée sur l'hypothèse que les parties au conflit sont connues et identifiables, ce qui ne peut pas toujours être considéré comme acquis même dans les conflits armés classiques, en particulier dans les conflits armés non internationaux. Or, dans les cyberopérations qui se produisent au quotidien, l'anonymat est la règle plutôt que l'exception. Il paraît impossible, dans certains cas, de remonter jusqu'à leur auteur, et même lorsque cela s'avère possible, cela prend généralement beaucoup de temps. Comme tout système de droit est fondé sur l'attribution de responsabilité (en DIH, à une partie à un conflit ou à un individu), cela engendre des difficultés majeures. C'est ainsi, notamment, que si l'auteur d'une opération et, par conséquent, le lien entre cette opération et un conflit armé ne peut pas être identifié, il devient extrêmement difficile de déterminer si le DIH est ou non applicable à l'opération. Par exemple, si l'infrastructure d'un gouvernement est attaquée sans que l'on sache clairement qui est derrière l'attaque, il est difficile de définir qui sont les parties au conflit armé potentiel, et donc d'établir s'il y a ou non conflit armé. En outre, même si les parties au conflit étaient connues, il pourrait être difficile d'attribuer l'acte précisément à l'une ou l'autre. Deuxièmement, le DIH part du postulat que les moyens et méthodes de guerre auront des effets violents dans le monde physique. Or, souvent, les cyberopérations ont des effets perturbateurs mais on ne peut pas les considérer comme causant des destructions physiques immédiates. Troisièmement, toute la structure des règles régissant la conduite des hostilités – et en particulier le principe de distinction – est fondée sur le principe que l'on peut, le plus souvent, distinguer les biens militaires des biens civils. Dans le domaine de la cyberguerre, cette possibilité de distinction est plus généralement l'exception que la règle, car la plupart des infrastructures informatiques de la planète (câbles sous-marins, routeurs, serveurs, satellites) servent aussi bien à des communications civiles que militaires.

L'analyse qui suit vise par conséquent à examiner comment les règles du DIH peuvent être interprétées de façon à avoir du sens dans la cybersphère, et où se trouvent les failles et les limites des cybertechnologies. Comme nous le

constaterons, il est probablement trop tôt pour donner des réponses définitives à nombre des questions soulevées, parce que les exemples sont rares et les faits insuffisamment clairs, et parce que la pratique des États en matière d'interprétation et de mise en œuvre des normes applicables doit encore évoluer. Le Manuel de Tallinn sur le droit international applicable à la cyberguerre (*Tallinn Manual on the International Law Applicable to Cyber Warfare*, ci-après « Manuel de Tallinn ») représente le travail le plus poussé d'interprétation des règles de droit international (*jus ad bellum* et *jus in bello*) au regard de la cyberguerre qui ait été fait à ce jour[27]. Ce manuel a été élaboré par un groupe d'experts à l'invitation du Centre d'excellence de cyberdéfense de l'OTAN et constitue une compilation utile de règles assorties d'un commentaire, qui reflètent les différentes opinions sur certains des problèmes épineux que pose cette nouvelle technologie. Le CICR a pris part en tant qu'observateur aux délibérations du groupe d'experts, mais ne souscrit pas à tous les points de vue exprimés dans le manuel.

## Applicabilité du droit international humanitaire aux cyberopérations : qu'est-ce qu'un conflit armé dans le cyberespace ?

Le DIH ne s'applique que si les cyberopérations sont effectuées dans le contexte d'un conflit armé et en lien avec ce conflit. Ainsi, il devrait être assez incontestable que lorsque des cyberopérations sont conduites dans le cadre d'un conflit armé en cours, elles sont régies par les mêmes règles de DIH que ce conflit. On citera pour exemple le cas où, parallèlement ou en complément à un bombardement ou une attaque de missiles, une partie au conflit lance également une cyberattaque contre les systèmes informatiques de son adversaire.

Cependant, un certain nombre d'opérations que l'on qualifie de cyberguerre peuvent ne pas être effectuées du tout dans le contexte d'un conflit armé. Des termes comme « cyberattaque » et « cyberterrorisme » évoquent certes des méthodes de guerre, mais les opérations qu'ils désignent n'ont pas forcément pour cadre un conflit armé. Les cyberopérations peuvent servir – et servent effectivement – à commettre des délits dans des situations de tous les jours qui n'ont rien à voir avec la guerre.

D'autres cas, qui se situent entre les situations de conflit armé faisant appel à la fois à des moyens de combat classiques et à des cyberopérations, et des situations qui sont sans aucun rapport avec un conflit armé, sont plus difficiles à classifier. C'est ce qui se passe, en particulier, quand des attaques de réseaux informatiques sont les seules opérations hostiles qui soient effectuées, surtout s'il s'agit d'actes isolés. Ce scénario n'est pas totalement futuriste. L'attaque par le virus Stuxnet, qui aurait semble-t-il ciblé le site d'enrichissement d'uranium de Natanz, en Iran, est restée jusqu'à présent une attaque isolée (bien qu'étalée

27 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (ci-après « *Tallinn Manual* »), Cambridge University Press, Cambridge, (à paraître). Ce manuel est disponible sur : http://www.ccdcoe.org/249.html.

sur une certaine période), peut-être lancée par un ou plusieurs États contre la République islamique d'Iran. Si aucun État n'a qualifié cette attaque de conflit armé, le raisonnement de certains commentateurs laissait entendre que si elle avait été lancée par un État, elle aurait eu valeur de conflit armé international[28]. Un autre scénario envisageable serait celui de cyberopérations de grande envergure et prolongées qui seraient effectuées par un groupe armé organisé non étatique contre des infrastructures gouvernementales. De telles opérations pourraient-elles atteindre le niveau d'un conflit armé non international ?

Selon le droit international humanitaire en vigueur, il n'existe que deux types de conflits armés : les conflits armés internationaux et les conflits armés non internationaux. Nous n'examinerons pas ici tous les critères qui doivent être remplis pour qu'il y ait conflit armé, mais seulement certains aspects au sujet desquels semblent se poser des questions particulièrement difficiles concernant les cyberopérations.

## Les conflits armés internationaux

Aux termes de l'article 2 commun aux quatre Conventions de Genève de 1949, un conflit armé international est toute « guerre déclarée ou … tout autre conflit armé surgissant entre deux ou plusieurs des Hautes Parties contractantes, même si l'état de guerre n'est pas reconnu par l'une d'elles ». Il n'existe pas d'autre définition conventionnelle du conflit armé international, et il est maintenant accepté que, comme l'a déclaré le Tribunal pénal international pour l'ex-Yougoslavie (TPIY), un conflit armé international existe « chaque fois qu'il y a *recours à la force armée* entre États »[29]. L'application du DIH dépend des faits et non de la reconnaissance d'un état de conflit armé par les parties à ce conflit.

La question spécifique qui se pose s'agissant de la cyberguerre est : une attaque de réseau informatique peut-elle donner prise à la qualification de conflit armé international en l'absence de tout autre emploi de la force (cinétique) ? La réponse dépend de deux éléments : il convient de déterminer si l'attaque de réseau informatique 1) peut être attribuée à un État et 2) constitue un recours à la force armée – terme qui n'est pas défini dans le droit international humanitaire.

28 Michael N. Schmitt, « Classification of Cyber Conflict », dans *Journal of Conflict and Security Law*, Vol. 17, N° 2, été 2012, p. 252. Voir aussi Gary Brown, « Why Iran Didn't Admit Stuxnet was an Attack », dans *Joint Force Quarterly*, N° 63, 4e trimestre 2011, p. 71, disponible sur : http://www.ndu.edu/press/lib/images/jfq-63/JFQ63_70-73_Brown.pdf. G. Brown n'aborde pas la question de la classification des conflits, mais considère que Stuxnet constituait à l'évidence une attaque, et peut-être une violation de l'interdiction du recours à la force et une violation du droit de la guerre.

29 Tribunal pénal international pour l'ex-Yougoslavie (TPIY), *Le Procureur c/ Duško Tadić*, Affaire N° IT-94-1-A, Chambre d'appel, Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, 2 octobre 1995, para. 70 (nous soulignons). Les situations prévues à l'article 1(4) du Protocole additionnel I sont également considérées comme des conflits armés internationaux à l'égard des États parties au Protocole.

### *Attribution d'un comportement à un État*

La question de l'attribution d'une opération à un État pourrait s'avérer particulièrement problématique dans le cyberespace, où l'anonymat est la règle plutôt que l'exception. Pourtant, aussi longtemps que les parties ne peuvent pas être identifiées comme étant deux ou plusieurs États, il est impossible de qualifier la situation de conflit armé international. S'il s'agit là davantage d'un problème factuel que juridique, une façon de pallier l'incertitude quant aux faits serait la présomption juridique. Par exemple, si une attaque de réseau informatique provenait de l'infrastructure gouvernementale d'un certain État, on pourrait en tirer la présomption que l'opération est imputable à cet État – notamment au regard de la règle de droit international selon laquelle tout État a l'obligation de ne pas laisser sciemment utiliser son territoire aux fins d'actes contraires aux droits d'autres États[30]. Cette approche suscite néanmoins deux objections.

La première est qu'une telle présomption n'est étayée par aucune règle existante de droit international. Par exemple, les Articles sur la responsabilité de l'État pour fait internationalement illicite élaborés par la Commission du droit international ne contiennent pas de règles sur la présomption de responsabilité d'un État. En outre, la Cour internationale de Justice (CIJ) a fixé un seuil élevé pour l'attribution d'un fait à un État dans le contexte du droit de légitime défense. Dans l'*Affaire des plates-formes pétrolières,* elle a effectivement estimé que la charge de la preuve incombait à l'État invoquant le droit de légitime défense :

> La Cour doit en l'espèce simplement déterminer si les États-Unis ont démontré qu'ils avaient été victimes de la part de l'Iran d'une « agression armée » de nature à justifier l'emploi qu'ils ont fait de la force armée au titre de la légitime défense ; or, c'est à eux qu'il revient de prouver l'existence d'une telle agression[31].

Si cette déclaration a été faite dans le contexte du droit de légitime défense dans le *jus ad bellum*, elle pourrait s'appliquer plus généralement à toutes les questions factuelles d'attribution d'un comportement à un État. Puisqu'il s'agit de présumer des faits, il serait absurde de le faire dans un but et pas dans un autre.

La deuxième objection est qu'une telle présomption serait aussi trop lourde de conséquences dans le cas particulier de la cyberguerre. Étant donné la difficulté qu'il y a à protéger une infrastructure informatique de la manipulation, et la facilité avec laquelle on peut contrôler à distance un ordinateur et se présenter sous une identité différente dans le cyberespace, ce serait faire peser une très lourde charge sur les gouvernements que de les tenir pour responsables, sans autre preuve, de toutes les opérations provenant de leurs ordinateurs[32].

30 Cour internationale de Justice (CIJ), *Affaire du détroit de Corfou* (*Royaume-Uni c/ Albanie*), Arrêt du 9 avril 1949, CIJ Recueil 1949, p. 22. Voir aussi la règle 5 du Manuel de Tallin, *op. cit.*, note 27.

31 CIJ, *Affaire des plates-formes pétrolières (République islamique d'Iran c. États-Unis d'Amérique)*, Arrêt du 6 novembre 2003, CIJ Recueil 2003, para. 57.

32 Le Manuel de Tallin exprime un point de vue juridique semblable dans la règle 7 : « Le simple fait qu'une cyberopération ait été lancée depuis une cyberinfrastructure gouvernementale ou ait son

Une autre question, plus fréquemment examinée, est celle de l'attribution de cyberattaques lancées par des entités privées, par exemple des groupes de pirates informatiques (ou hackers), contre un État. À part les questions factuelles qui se posent en raison de l'anonymat des cyberopérations, les règles juridiques concernant l'attribution d'actes d'entités privées à un État sont énoncées dans les Articles sur la responsabilité de l'État pour fait internationalement illicite[33]. En particulier, un État est responsable du comportement d'une personne ou d'un groupe de personnes « si cette personne ou ce groupe de personnes, en adoptant ce comportement, agit en fait sur les instructions ou les directives ou sous le contrôle de cet État »[34]. Ce que signifie exactement en droit international « les instructions ou les directives » devra être précisé avec le temps. La CIJ considère que pour que la responsabilité d'un acte commis par une entité privée (qu'il s'agisse d'un individu ou des membres d'un groupe organisé) soit attribuée à l'État, il est nécessaire de démontrer que la direction ou le contrôle effectif de l'État s'exerçait à l'occasion de l'opération au cours de laquelle les violations alléguées se seraient produites, et non pas seulement en général, à l'égard de l'ensemble des actions menées par les personnes ou groupes de personnes ayant commis lesdites violations[35]. En l'absence d'un tel contrôle sur l'opération en cause, celle-ci ne peut être imputée à l'État même lorsqu'elle a été commise par un groupe extrêmement dépendant des autorités de l'État[36]. De même, le commentaire des Articles sur la responsabilité de l'État précise qu'un comportement ne peut être attribué à l'État que si ce dernier a dirigé ou contrôlé l'opération elle-même et que le comportement objet de la plainte faisait partie intégrante de cette opération[37]. Le TPIY est allé plus loin et a fait valoir que si un groupe – tel qu'un groupe d'opposition armée – est organisé et structuré hiérarchiquement, il suffit que l'État exerce un « contrôle global » sur ce groupe, sans nécessité d'un contrôle ou de directives spécifiques de sa part sur le comportement précis en cause[38]. Cependant, le TPIY a aussi reconnu que

origine, d'une façon ou d'une autre, dans cette infrastructure ne constitue pas une preuve suffisante pour que l'opération soit attribuée à cet État, mais permet de penser que l'État en question est associé à l'opération. » [Traduction CICR]

33 Commission du droit international, Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite, *Annuaire de la Commission du droit international,* 2001, Volume II (Deuxième partie). Texte repris de l'annexe de la résolution de l'Assemblée générale, Doc. ONU A/RES/56/83, 12 décembre 2001, corrigée par le Doc. ONU A/56/49(Vol. I)/Corr.4 (ci-après « Articles sur la responsabilité de l'État »).

34 Article 8 des Articles sur la responsabilité de l'État.

35 CIJ, *Activités militaires et paramilitaires au Nicaragua et contre celui-ci* (*Nicaragua* c. *États-Unis d'Amérique*), Arrêt du 27 juin 1986, CIJ Recueil 1986, paras 115-116 (ci-après « affaire du *Nicaragua* ») ; CIJ, *Affaire relative à l'application de la Convention pour la prévention et la répression du crime de génocide (Bosnie-Herzégovine c. Serbie-et-Monténégro)*, Arrêt du 26 février 2007, CIJ Recueil 2007, paras 400-406.

36 Affaire du *Nicaragua*, *ibid*., para. 115.

37 Rapport de la Commission du droit international sur les travaux de sa cinquante-troisième session (23 avril-1er juin et 2 juillet-10 août 2001), Doc. ONU A/56/10, commentaire de l'article 8 du Projet d'articles sur la responsabilité de l'État, para. 3.

38 TPIY, *Le Procureur c/ Duško Tadić*, Affaire N° IT-94-1, Chambre d'appel, Arrêt du 15 juillet 1999, para. 120. On entend parfois dire que la question sur laquelle le Tribunal devait se prononcer était une question de qualification du conflit en tant que non international ou international. Toutefois, l'argument selon lequel les deux questions sont totalement distinctes n'est pas convaincant, car il

lorsque l'État exerçant le contrôle n'est pas l'État territorial, « il faut davantage de preuves incontestables pour démontrer que l'État contrôle réellement les unités ou les groupes » – ce qui signifie que l'implication de l'État dans la planification d'opérations militaires ou son rôle de coordination pourraient être plus difficiles à démontrer[39]. La Commission du droit international déclare : « C'est au cas par cas qu'il faut déterminer si tel ou tel comportement précis se produisait ou non sous le contrôle d'un État et si la mesure dans laquelle ce comportement était contrôlé justifie que le comportement soit attribué audit État »[40]. Cette analyse, toutefois, n'est pas spécifique au domaine des cyberopérations. Une fois que les faits sont établis, les critères juridiques qui s'appliquent sont les mêmes que pour toute autre attribution du comportement d'entités privées à un État. Là encore, la difficulté résidera essentiellement dans l'évaluation des faits.

### *Recours à la force armée*

Le deuxième critère à remplir est celui du « recours à la force armée » entre États.

Avant de se pencher sur la problématique de la cyberguerre au regard de ce critère, il vaut la peine de préciser très brièvement que la question de la qualification d'un conflit en tant que conflit armé international se pose différemment selon le DIH (*jus in bello*) et le *jus ad bellum*. Les deux conceptions, toutefois, sont souvent combinées, y compris en ce qui concerne la cyberguerre.

Au regard du *jus ad bellum*, il s'agit de déterminer si, et quand, des cyberopérations constituent un « emploi de la force » au sens de l'article 2(4) de la Charte des Nations Unies et/ou une « agression armée » au sens de l'article 51 de la Charte, et dans quelles circonstances elles donnent droit à l'exercice de la légitime défense[41]. Quels que soient les points de vue sous l'angle du *jus ad bellum*, il convient de se rappeler que l'objet des règles du *jus ad bellum* est tout à fait différent de celui des règles du *jus in bello* : si le *jus ad bellum* réglemente spécifiquement les relations interétatiques et définit les conditions d'un emploi licite de la force entre États, le *jus in bello*, lui, réglemente le comportement des parties à un conflit et a pour objet de protéger les victimes militaires et civiles de la guerre. Ainsi, un acte pourrait constituer un recours à la force armée aux fins de qualification d'un conflit armé international, sans préjudice de la question de savoir s'il constitue aussi un recours à la force au sens de l'article 2(4) de la Charte

mènerait à la conclusion qu'un État pourrait être partie à un conflit du simple fait de son contrôle sur un groupe armé organisé, mais ne pas être responsable des actes commis pendant ce conflit.

39 *Ibid.*, paras 138-140.

40 Commentaire de l'article 8 du Projet d'articles sur la responsabilité de l'État, *op. cit.*, note 37, para. 5.

41 Voir Marco Roscini, « World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force », dans *Max Planck Yearbook of United Nations Law*, Vol. 14, 2010, p. 85 ; Michael N. Schmitt, « Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework », dans *Columbia Journal of Transnational Law*, Vol. 37, 1998-1999, p. 885 ; Herbert S. Lin, « Offensive Cyber Operations and the Use of Force », dans *Journal of National Security Law and Policy*, Vol. 4, 2010, p. 63 ; David P. Fidler, « Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law », dans *ASIL Insights*, 20 juin 2012, Vol. 16, N° 22 ; *Tallinn Manual*, *op. cit.*, note 27, règles 10-17.

des Nations Unies (bien que ce soit probable), *a fortiori* une agression armée au sens de l'article 51. Cette distinction s'applique aussi aux cyberopérations.

En ce qui concerne le *jus in bello*, il n'existe pas de définition conventionnelle de la « force armée » dans le DIH, car il s'agit d'un critère jurisprudentiel. Traditionnellement, l'objectif de la guerre est de l'emporter sur l'ennemi et, dans la guerre classique, un conflit suppose le déploiement de moyens militaires en vue d'un affrontement militaire. Ainsi, lorsqu'on utilise des moyens ou méthodes de guerre classiques – tels que bombardements, tirs d'artillerie ou déploiement de troupes – il est incontestable que ces actes constituent de la « force armée ». Cependant, les attaques de réseaux informatiques ne font pas intervenir l'emploi de telles armes.

En l'absence d'armes classiques et de force cinétique, qu'est-ce qui peut être considéré comme de la « force armée » dans la cybersphère ?

Dans un premier temps, il convient de considérer les effets des attaques de réseaux informatiques qui sont analogues à ceux de la force cinétique. Pour la plupart des commentateurs, si une attaque de réseau informatique est attribuable à un État et a les mêmes effets que le recours à la force cinétique, cela justifiera la qualification de conflit armé international[42]. De fait, si une cyberattaque provoque des collisions entre des avions ou des trains et fait des morts ou des blessés, ou cause des inondations massives qui ont de grandes conséquences, il y aurait peu de raisons de traiter la situation autrement que dans le cas d'attaques équivalentes faisant appel à des moyens ou méthodes de guerre cinétiques.

Ce parallèle est donc utile dans des situations où des attaques de réseaux informatiques font des morts ou des blessés, ou endommagent physiquement ou détruisent des infrastructures. Cependant, il pourrait s'avérer insuffisant pour appréhender tout l'éventail des effets possibles des cyberopérations et des dégâts qu'elles peuvent causer, qui ne ressembleront pas nécessairement aux effets physiques des armes classiques. Il sera souvent fait usage de cyberopérations pour ne pas détruire ni endommager physiquement des infrastructures militaires ou civiles mais plutôt porter atteinte à leur fonctionnement, par exemple en le manipulant, voire même en parvenant à le manipuler sans que cela soit détecté. Ainsi, un réseau électrique pourrait rester intact physiquement mais être néanmoins mis hors d'état de fonctionner par une cyberattaque ; de même, le système bancaire d'un pays pourrait être manipulé sans qu'aucun élément de son infrastructure ne soit endommagé physiquement et sans même que la manipulation du

42 M. N. Schmitt, « Classification of Cyber Conflict », *op. cit.*, note 28, p. 251 ; Knut Dörmann, « Applicability of the Additional Protocols to Computer Network Attacks » (L'applicabilité des Protocoles additionnels aux attaques contre les réseaux informatiques), CICR, 2004, p. 3, disponible sur : http://961.ch/fre/resources/documents/misc/68ukur.htm ; Heather Harrison Dinniss, *Cyber warfare and the laws of war*, Cambridge University Press, Cambridge, 2012, p. 131 ; Nils Melzer, *Cyberwarfare and International Law,* UNIDIR Resources Paper, 2011, p. 24, disponible sur : http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-L-en.pdf. Nils Melzer fait valoir que puisque l'existence d'un conflit armé international dépend principalement de la survenance d'hostilités armées entre des États, des cyberopérations donneraient prise à la qualification de conflit armé non seulement si elles faisaient des morts et des blessés ou causaient des destructions, mais aussi si elles portaient directement atteinte aux opérations militaires ou à la capacité militaire de l'État visé.

système sous-jacent soit même décelable pendant un certain temps. À première vue, même en l'absence de moyens militaires traditionnels ou d'une destruction physique immédiate, les effets potentiels de perturbations de ce type sur la population – qui pourraient être beaucoup plus étendus et graves que, disons, ceux de la destruction d'un bâtiment ou groupe de bâtiments particulier – justifieraient que ces perturbations soient considérées comme un « recours à la force armée ». Cependant, les États, même les États victimes, pourraient chercher à éviter une escalade d'affrontements internationaux ou avoir d'autres raisons d'éviter de traiter ce type d'attaques comme donnant lieu à la qualification de conflit armé. Il est difficile, à ce stade, de dégager une quelconque position juridique, les États semblant pour la plupart rester silencieux face aux cyberattaques[43]. En l'absence d'une pratique des États qui se manifeste clairement, il existe plusieurs façons possibles d'appréhender cette question.

Une approche possible consiste à considérer toute cyberopération hostile portant atteinte au fonctionnement de biens comme un recours à la « force armée ». L'objet et la finalité du DIH en général, et en particulier le fait qu'il ne définisse pas de seuil de violence à partir duquel il y aurait conflit armé international – omission délibérée afin d'éviter une lacune de protection, et en particulier de protection de la population civile face aux effets de la guerre – plaiderait en faveur de l'inclusion de telles cyberopérations dans la définition de la force armée aux fins de qualification en tant que conflit armé international. De plus, étant donné l'importance que les États attachent à la protection des infrastructures critiques dans leurs cyberstratégies, ils pourraient tout à fait considérer comme le début d'un conflit armé les attaques de réseaux informatiques lancées par un autre État pour mettre hors d'état de fonctionner ce type d'infrastructures[44]. Qui plus est, en l'absence d'un conflit armé, la situation ne donnerait pas lieu à la protection que confère le DIH. D'autres corpus de droit comme le *jus ad bellum*, le droit relatif à la cybercriminalité, le droit spatial ou le droit des télécommunications, pourraient bien sûr s'appliquer et fournir leur propre protection. L'analyse de leur effet dépasse le champ de cet article, mais tous ces corpus de droits donneraient lieu eux aussi à une série de questions. Par exemple, le droit international des droits de l'homme pourrait s'appliquer, mais une attaque de réseau informatique lancée depuis l'autre côté

43 Voir aussi G. Brown, *op. cit.*, note 28.

44 N. Melzer, *op. cit.*, note 42, p. 14. Melzer explique que l'on pourrait se référer au concept d'infrastructure critiquée pour examiner « l'ampleur et les effets » d'une attaque contre des réseaux informatiques afin d'identifier une agression armée au sens de l'article 51 de la Charte des Nations Unies. Pour la stratégie de la France en la matière, voir Agence nationale de la sécurité des Systèmes d'information, *Défense et sécurité des systèmes d'informations,* disponible sur : http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf. Pour la stratégie de l'Allemagne, voir Bundesamt für Sicherheit in der Informationstechnik, *Schutz Kritischer Infrastrukturen*, disponible sur : https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/Kritis/Kritis_node.html. Pour la stratégie du Canada, voir *Stratégie nationale sur les infrastructures essentielles*, disponible sur : http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-fra.aspx. Pour la stratégie du Royaume-Uni; voir *The UK Cyber Security Strategy*, disponible sur : http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy. Pour la stratégie de l'Australie, voir CERT Australia, *Australia's National Computer Emergency Response Team*, disponible sur : https://www.cert.gov.au/.

de la planète contre une infrastructure civile satisferait-elle au critère du contrôle effectif aux fins de l'applicabilité de ce droit ? De plus, dans quelle mesure le droit des droits de l'homme offrirait-il une protection suffisante contre une perturbation des infrastructures dont on ne pourrait pas forcément discerner tout de suite les effets sur la vie de populations civiles ?

Une autre approche consisterait à ne pas s'intéresser exclusivement aux effets analogues d'une cyberopération, mais de prendre en considération un ensemble de facteurs qui indiqueraient qu'il y a « force armée ». Ces facteurs seraient notamment une certaine gravité des conséquences de la cyberopération, les moyens employés, la participation de l'armée ou d'autres secteurs du gouvernement à l'opération hostile, la nature de la cible (militaire ou non) et la durée de l'opération. Pour prendre un exemple en dehors de la cybersphère, si le chef d'état-major des forces armées d'un État était tué lors d'une attaque aérienne lancée par un autre État, ce serait certainement considéré comme équivalant à un conflit armé international. En revanche, s'il était tué par l'envoi d'une lettre empoisonnée, cela serait-il également considéré en soi comme équivalant à un conflit armé international[45] ? Qu'en serait-il si la cible était un civil ? Les moyens utilisés pour détruire l'infrastructure entrent-ils en ligne de compte ? Par exemple, si des parties d'une installation nucléaire étaient sabotées par des agents étrangers infiltrés, cela constituerait-il aussi un « recours à la force armée » ? Cela fait-il une différence que la cible soit militaire ou civile ?

Dans la cybersphère, il est possible, par exemple, que les États traitent les attaques informatiques visant leur infrastructure militaire différemment de celles qui touchent des systèmes civils. Ceci n'est peut-être pas entièrement logique d'un point de vue technique, l'usage de la force étant l'usage de la force qu'il vise un bien civil ou militaire, mais le seuil de préjudice que les États sont prêts à tolérer pourrait être plus bas lorsqu'il s'agit d'opérations qui ciblent et endommagent leurs capacités militaires.

Selon cette approche, si l'attaque de réseau informatique n'est que ponctuelle et de courte durée, il se peut qu'elle ne soit considérée comme de la force armée que si ses conséquences sont particulièrement graves. L'exemple de l'attaque par le virus Stuxnet tel qu'il a été relaté dans la presse semble indiquer que des attaques de réseaux informatiques pourraient – du moins pendant un certain temps – demeurer des actes hostiles isolés commis par un État contre un autre État sans que soient menées aussi des opérations cinétiques, notamment si l'agresseur veut rester anonyme, souhaite que l'attaque reste non-détectée pendant un certain temps, ou souhaite (pour des raisons politiques ou autres) éviter une escalade de l'usage de la force, d'autres hostilités et un conflit armé. Si l'on se basait seulement sur la question de savoir si une attaque cinétique ayant les mêmes effets équivaut

45 Dans *Un droit dans la guerre ?,* Vol. I, seconde édition française, CICR, Genève, 2012, p. 141, les auteurs Marco Sassòli, Antoine Bouvier et Anne Quintin établissent une distinction entre recours à la force par l'armée ou par d'autres agents de l'État : « Lorsque les forces armées de deux États sont impliquées, le premier coup de feu tiré ou la première personne capturée (conformément à des instructions du gouvernement) suffit à rendre le DIH applicable, alors que dans d'autres cas (par exemple, une exécution sommaire par un agent secret envoyé à l'étranger par son gouvernement), il faut un degré de violence plus élevé pour déterminer l'applicabilité du DIH. »

à de la force armée, on pourrait être amené à conclure qu'un acte tel que l'attaque par Stuxnet constitue effectivement un emploi de la force armée, car le virus avait, semble-t-il, causé la destruction physique d'environ mille centrifugeuses IR-1 du site d'enrichissement d'uranium de Natanz, qui avaient dû être remplacées[46]. De fait, si les centrifugeuses d'une installation nucléaire sont détruites par un bombardement effectué par les forces aériennes d'un autre État, cette attaque sera considérée comme un recours à la force armée justifiant la qualification de conflit armé international. Dans le cas de Natanz, comme les moyens de l'attaque n'étaient pas cinétiques, qu'aucune autre attaque visant ces installations n'avait été signalée et qu'il n'y avait eu aucun autre dommage que les dégâts causés aux centrifugeuses, on peut faire valoir que cette attaque ne suffit pas à constituer un recours à la force armée et à donner lieu à la qualification de conflit armé international.

Pour résumer, il reste à savoir si les États traiteront les attaques de réseaux informatiques comme un recours à la force armée, et dans quelles conditions. Vouloir appliquer le concept de force armée à la seule manipulation d'un système bancaire ou autre manipulation d'une infrastructure critique, même si elle entraîne une grave perte économique, serait probablement exagéré par rapport à l'objet et à la finalité de ce concept : les effets ne sont pas équivalents à la destruction causée par des moyens physiques. En revanche, le fait d'interrompre le fonctionnement d'infrastructures vitales telles que les systèmes d'approvisionnement en électricité ou en eau – ce qui causerait inévitablement un grave préjudice à la population si cela durait un certain temps, même sans causer de morts et de blessés – devrait probablement être considéré comme un recours à la force armée. Bien que, en pareil cas, les effets de l'opération ne soient pas équivalents à des effets physiques, ils constituent précisément le type de conséquences graves dont le DIH s'efforce de protéger la population civile.

Il est vrai que les États ne peuvent pas se dérober à leurs obligations au regard du DIH en qualifiant eux-mêmes l'acte. L'application du droit des conflits armés internationaux a été dissociée de la nécessité d'une déclaration officielle il y a des décennies, afin d'éviter les cas où des États pourraient nier la protection conférée par ce corpus de règles. Ceci est établi clairement par l'article 2 commun aux Conventions de Genève, comme l'explique le Commentaire de ces instruments publié par le CICR :

> Un État peut toujours prétendre, lorsqu'il commet un acte d'hostilité armée contre un autre État, qu'il ne fait pas la guerre, qu'il procède à une simple opération de police, ou qu'il fait acte de légitime défense. Avec l'expression « conflit armé », une telle discussion est moins aisée[47].

46 C'est l'avis de M. N. Schmitt, *op. cit.*, note 28, p. 252. Sur les dommages causés, voir D. Albright, P. Brannan et C. Walrond, *op. cit.*, note 23 ; et D. E. Sanger, *op. cit.*, note 23.

47 Jean S. Pictet (éd.), *Commentaire des Conventions de Genève du 12 août 1949. Volume I. La Convention de Genève pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne,* CICR, Genève, 1952, p. 34. C'est là une question différente de celle de l'*animus belligerendi* : il arrive que des actes isolés ne soient pas considérés comme constituant un conflit armé, non pas parce qu'ils n'ont pas atteint un certain degré d'intensité, mais plutôt parce qu'il n'existe pas en l'espèce d'*animus belligerendi*, par exemple en cas d'incursions transfrontalières accidentelles. Voir *The*

Néanmoins, s'il est vrai que dans un incident précis, la classification du conflit ne dépend pas de la prise de position des États concernés, l'interprétation de la définition du « conflit armé international » en droit international est déterminée par la pratique des États et l'*opinio juris*. La classification des cyberconflits ne sera probablement déterminée de manière certaine qu'à travers la pratique future des États.

## Les conflits armés non internationaux

S'agissant des conflits armés non internationaux dans la cybersphère, la principale question est de savoir comment faire la différence entre comportement criminel et conflit armé. Il n'est pas rare d'entendre dire ou de lire que les actes de groupes de hackers ou d'autres groupes, dont Anonymous ou Wikileaks, sont une « guerre »[48]. Bien entendu, cette désignation ne fait pas forcément allusion à un conflit armé, ou plus précisément à un conflit armé non international, au sens juridique. Il vaut toutefois la peine de préciser les paramètres qui permettent de qualifier une situation de conflit armé non international.

Faute d'une définition conventionnelle, la pratique et la doctrine des États ont conduit à une définition des conflits armés non internationaux que le TPIY a résumée en ces termes : un conflit armé existe chaque fois qu'il y a recours prolongé à la violence armée entre les autorités gouvernementales et des groupes armés organisés ou entre de tels groupes au sein d'un État[49]. L'exigence d'un caractère « prolongé » de la violence a, avec le temps, été intégrée dans un critère selon lequel la violence doit atteindre une certaine intensité. Ainsi, deux critères déterminent l'existence d'un conflit armé non international : l'affrontement armé doit atteindre un niveau minimal d'intensité et les parties au conflit doivent faire preuve d'un minimum d'organisation[50].

### *Les groupes armés organisés*

Pour qu'un groupe soit qualifié de groupe armé organisé pouvant être partie à un conflit au sens du DIH, il faut qu'il ait un degré d'organisation qui lui permette

*Joint Service Manual of the Law of Armed Conflict*, Joint Service Publication 383, 2004, para. 3.3.1, disponible sur : http://www.mod.uk/NR/rdonlyres/82702E75-9A14-4EF5-B414-49B0D7A27816/0/JSP3832004Edition.pdf.

48 Voir, par ex., Mark Townsend *et al.*, « WikiLeaks backlash: The first global cyber war has begun, claim hackers », dans *The Observer*, 11 septembre 2010, disponible sur : http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-war ; Timothy Karr, « Anonymous Declares Cyberwar Against 'the System' », dans *The Huffington Post*, 3 juin 2011, disponible sur : http://www.huffingtonpost.com/timothy-karr/anonymous-declares-cyberw_b_870757.html.

49 TPIY, *Le Procureur c/ Duško Tadić*, *op. cit.*, note 29, para. 70.

50 Il existe deux types de conflits armés non internationaux. L'article 3 commun aux Conventions de Genève s'applique à tous ces conflits. En outre, les dispositions du Protocole additionnel II s'appliquent aux conflits armés non internationaux qui « se déroulent sur le territoire d'une Haute Partie contractante entre ses forces armées et des forces armées dissidentes ou des groupes armés organisés qui, sous la conduite d'un commandement responsable, exercent sur une partie de son territoire un contrôle tel qu'il leur permette de mener des opérations militaires continues et concertées et d'appliquer [ledit] Protocole ». (Art. 1(1) du PA I).

de mener des opérations militaires continues et d'appliquer le DIH. Au nombre des éléments indicatifs figurent l'existence d'un organigramme indiquant une structure de commandement, le pouvoir de lancer des opérations regroupant plusieurs unités, l'aptitude à recruter et à former de nouveaux membres ou l'existence d'un règlement interne[51]. S'il n'est pas nécessaire que le groupe ait le degré d'organisation des forces armées d'un État, il doit néanmoins posséder un niveau suffisant de hiérarchie et de discipline ainsi que la capacité de faire respecter les obligations fondamentales découlant du DIH[52].

En ce qui concerne les groupes de hackers ou autres groups similaires, la question qui se pose est de savoir si des groupes qui sont organisés entièrement en ligne peuvent constituer des groupes armés au sens du DIH. Comme le précise Michael Schmitt :

> Les membres d'organisations virtuelles peuvent ne jamais se rencontrer ni même connaître mutuellement leur véritable identité. Ils peuvent néanmoins mener une action coordonnée contre le gouvernement (ou un groupe armé organisé), recevoir leurs ordres d'un commandement virtuel et être extrêmement organisés. Par exemple, un élément du groupe pourrait être chargé de détecter les vulnérabilités des systèmes visés, un autre de concevoir des logiciels malveillants pour exploiter ces vulnérabilités, un troisième de conduire les opérations et un quatrième de tenir prêtes des cyberdéfenses en cas de contre-attaque[53].

Cependant, le critère selon lequel les groupes armés organisés doivent avoir un commandement responsable et la capacité d'appliquer le DIH semblerait empêcher les groupes organisés sur le plan virtuel de pouvoir être considérés comme des groupes armés organisés. Il serait difficile, par exemple, d'instaurer dans ce type de groupe un système de discipline efficace permettant d'assurer le respect du DIH[54]. En d'autres termes, il est peu probable que des groupes de hackers ou autres groupes liés par la seule communication virtuelle aient l'organisation ou la structure de commandement (et structure disciplinaire) requises pour pouvoir constituer une partie au conflit[55].

### *Intensité*

Les cyberopérations menées dans le contexte d'un conflit armé non international et en lien avec ce conflit sont régies par le DIH. La question qui se pose, bien

51 Pour un examen des facteurs indicatifs pris en compte par le TPIY dans sa jurisprudence, voir TPIY, *Le Procureur c/ Boškoski,* Affaire N° IT-04-82-T, Chambre de première instance II, Jugement, 10 juillet 2008, paras. 199-203. Voir aussi TPIY, *Le Procureur c/ Limaj*, Affaire N° IT-03-66-T, Chambre de première instance II, Jugement, 30 novembre 2005, paras. 90-134 ; TPIY, *Le Procureur c/ Haradinaj*, Affaire N° IT-04-84-T, Chambre de première instance I, Jugement, 3 avril 2008, para. 60.

52 TPIY, *Le Procureur c/ Boškoski*, *ibid.*, para. 202.

53 M. N. Schmitt, *op. cit.,* note 28, p. 256.

54 *Ibid.,* p. 257.

55 Voir, dans le Manuel de Tallinn, l'examen des différents types de groupes qui pourraient être pris en considération, *op. cit.*, note 27, commentaire de la règle 23, paras. 13-15.

qu'elle puisse sembler relever du futurisme à ce stade, est de savoir si le niveau d'intensité nécessaire pour qu'il y ait conflit armé non international pourrait être atteint si seuls des moyens virtuels sont utilisés (en supposant qu'il y a au minimum deux parties au conflit).

Contrairement à ce qui se passe pour la classification des conflits armés internationaux (au sens classique), on s'accorde à reconnaître qu'il n'y a conflit armé non international que si les hostilités atteignent un certain niveau d'intensité. Le Tribunal pénal international pour l'ex-Yougoslavie a relevé un certain nombre de facteurs indicatifs à considérer pour apprécier l'intensité d'un conflit, tels que le caractère collectif des hostilités, le recours à la force militaire contre les insurgés et non à de simples forces de police, la gravité des attaques et la multiplication des affrontements armés, la propagation des affrontements sur un territoire et une période donnés, l'intensification de l'armement des deux parties au conflit, le nombre de civils qui ont été forcés de fuir les zones de combat, le type d'armes utilisées, en particulier le recours à l'armement lourd et à d'autres équipements militaires, tels que les chars et autres véhicules lourds, l'ampleur des destructions et le nombre de victimes causées par les bombardements ou les combats[56]. Atteindrait-on le seuil d'intensité requis en menant seulement des cyberopérations ?

Il s'agit d'abord, là encore, de comparer l'intensité des effets respectifs de ces opérations et des opérations cinétiques. Il n'y a pas de raison que des cyberopérations ne puissent pas avoir les mêmes conséquences violentes que des opérations cinétiques, par exemple si on les utilise pour ouvrir les vannes d'un barrage ou pour provoquer des collisions entre des avions ou des trains. En pareilles circonstances, et si cette violence n'est pas seulement sporadique, elle peut atteindre le seuil requis pour qu'il y ait conflit armé non international.

Cela étant, des cyberopérations en elles-mêmes n'auraient pas plusieurs des effets mentionnés plus haut en tant qu'indicateurs de l'intensité de la violence (affrontements armés, déploiement de la force militaire, armes lourdes, etc.). Ce seraient vraisemblablement les conséquences des cyberopérations à elles seules qui seraient assez graves pour atteindre le degré d'intensité requis, comme par exemple une destruction de grande ampleur ou une répétition des attaques ayant des effets catastrophiques pour une grande partie de la population.

## Résumé

Il paraît incontestable que le DIH s'appliquera aux cyberopérations menées dans le cadre d'un conflit armé international ou non international en cours, parallèlement à des opérations cinétiques. En l'absence d'opérations cinétiques, une cyberguerre « pure » n'est pas exclue en théorie, mais il reste à voir si l'on en comptera de nombreux exemples dans la pratique ces prochaines années.

56 Voir, par ex., TPIY, *Le Procureur c/ Limaj*, *op. cit.,* note 51, paras. 135-170 ; TPIY, *Le Procureur c/ Haradinaj*, *op. cit.,* note 51, para. 49 ; TPIY, *Le Procureur c/ Boškoski*, *op. cit.,* note 51, paras. 177-178.

On ne sait pas vraiment, en particulier, dans quelle direction ira la pratique des États. Ceux-ci étant peu disposés à reconnaître une situation de conflit armé, notamment de conflit armé non international, la tendance pourrait être d'éviter de parler de conflit armé. La raison en est non seulement l'anonymat probable de nombreuses attaques de réseaux informatiques et les problèmes pratiques d'attribution de responsabilité, mais aussi le fait que la plupart des situations seraient sans doute non pas des cas extrêmes de destruction physique causée par des attaques contre des réseaux informatiques, mais plutôt des cas de faible intensité de manipulation d'infrastructure sans effusion de sang. Les États pourraient décider de traiter ces situations comme relevant du maintien de l'ordre et du droit pénal, et de ne pas les considérer comme régies par le cadre juridique applicable aux conflits armés.

## Application des règles relatives à la conduite des hostilités

Si des cyberopérations sont effectuées dans un contexte de conflit armé, elles sont régies par le droit international humanitaire, en particulier par les règles applicables à la conduite des hostilités. Le fait que les cyberarmes soient issues des nouvelles technologies ne suffit pas, en soi, à remettre en question l'applicabilité du DIH à ces armes.

Cela étant, la cyberguerre pose de sérieux défis aux prémisses mêmes sur lesquelles repose le DIH, en particulier le principe de distinction – et de possibilité effective de distinguer – entre biens militaires et biens de caractère civil. Ainsi, la question n'est pas tant de savoir si les règles régissant la conduite des hostilités s'appliquent à la cyberguerre, mais plutôt comment elles s'appliquent – comment elles doivent être interprétées pour être pertinentes dans ce nouveau domaine.

### À quels actes s'appliquent les règles de DIH régissant la conduite des hostilités ?

Avant d'aborder les règles relatives à la conduite des hostilités – notamment les principes de distinction, de proportionnalité et de précaution – il est important de se pencher sur une question qui fait débat depuis un certain temps, à savoir quel type de conduite, et en particulier quel type de cyberopération, donne prise à l'application des règles régissant la conduite des hostilités.

Cette question est fondamentale. En effet, ce n'est que si une cyberopération est soumise au principe de distinction qu'il est interdit à ses auteurs de prendre directement pour cible une infrastructure civile ; et, si une cyberopération est dirigée contre un objectif militaire, les effets qu'elle peut avoir incidemment sur des infrastructures civiles doivent être pris en considération si elle est soumise au principe de proportionnalité.

S'il y a débat, c'est parce que le cyberespace est différent des théâtres d'opérations classiques, en ce sens que les moyens et méthodes d'attaque ne font

pas intervenir la force cinétique habituelle, ou ce que l'on entend généralement par « violence ». Ainsi, nombre de cyberopérations peuvent avoir des effets graves sur le bien visé en perturbant son fonctionnement mais sans lui causer les dommages physiques qui se produiraient dans une guerre classique.

Il est donc d'une importance cruciale pour la population civile que cette question soit clarifiée. Selon que l'on considère de façon plus ou moins stricte ou large les types de cyberopérations auxquelles s'appliquent les règles relatives à la conduite des hostilités, les opérations suivantes pourraient être interdites ou licites dans le cadre d'un conflit armé :

- interrompre le fonctionnement du réseau électrique ou du système de traitement de l'eau civils (sans leur causer de dommages physiques) ;
- diriger contre un système bancaire en ligne une attaque du type « déni de service » ayant un impact important sur la capacité de quelques millions de clients d'accéder aux services bancaires[57] ;
- perturber le site web de la bourse d'un État adversaire, sans porter atteinte à ses fonctions commerciales[58] ;
- diriger une attaque du type « déni de service » sur le service de réservations en ligne d'une compagnie aérienne privée afin de causer des désagréments à la population civile ;
- bloquer les sites d'Al Jazeera ou de la BBC parce qu'ils contiennent des informations qui contribuent à l'image opérationnelle de l'ennemi ;
- bloquer l'accès à Facebook pour toute la population parce qu'il contient de la propagande favorable aux insurgés ;
- couper l'accès à Internet et au réseau de téléphonie mobile dans une région précise d'un pays pour juguler la propagande de la partie adverse[59].

Ceci amène deux questions : premièrement, les règles essentielles du DIH relatives à la conduite des hostilités – c'est-à-dire les principes de distinction, de proportionnalité et de précaution – s'appliquent-ils seulement aux opérations qui constituent des attaques au sens du DIH, ou s'appliquent-elles aux opérations militaires de façon plus générale ? Deuxièmement, quelles cyberopérations constituent des attaques au sens du DIH ?

57 Comme cela s'est produit en Estonie en mai 2007. Voir Larry Greenemeier, « Estonian attacks raise concern over cyber "nuclear winter" », dans *Information Week*, 24 mai 2007, disponible sur : http://www.informationweek.com/estonian-attacks-raise-concern-over-cybe/199701774.

58 Voir, par exemple, Yolande Knell, « New cyber attack hits Israeli stock exchange and airline », dans *BBC News*, 16 janvier 2012, disponible sur : http://www.bbc.co.uk/news/world-16577184.

59 En Égypte, le gouvernement a coupé l'accès à Internet et au réseau de téléphonie mobile pendant cinq jours pour endiguer les manifestations : « Internet Blackouts: Reaching for the Kill Switch », dans *The Economist,* 10 février 2011, disponible sur : http://www.economist.com/node/18112043. Des mesures semblables ont été prises par le gouvernement chinois en réaction aux troubles qui ont agité le Xinjiang et le Tibet : Tania Branigan, « China cracks down on text messaging in Xinjiang », dans *The Guardian*, 29 février 2010, disponible sur : http://www.guardian.co.uk/world/2010/jan/29/xinjiang-china; et Tania Branigan, « China cut off internet in area of Tibetan unrest », dans *The Guardian*, 3 février 2012, disponible sur : http://www.guardian.co.uk/world/2012/feb/03/china-internet-links-tibetan-unrest.

*Qu'est-ce qui détermine l'application des règles relatives à la conduite des hostilités : les « attaques », les « opérations militaires », les « hostilités » ?*

En ce qui concerne la première question, les divergences d'opinions proviennent de la règle générale relative à la conduite des hostilités qui est formulée aux articles 48 et suivants du Protocole additionnel I et qui est largement reconnue comme règle de droit coutumier. L'article 48 du Protocole additionnel I dispose en effet :

> En vue d'assurer le respect et la protection de la population civile et des biens de caractère civil, les Parties au conflit doivent en tout temps 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, ne *diriger leurs opérations* que contre des objectifs militaires. [Italique ajouté]

Les règles suivantes régissant la conduite des hostilités sont essentiellement formulées comme restreignant plus spécifiquement les attaques. Ainsi, l'article 51 du Protocole additionnel I, après avoir énoncé dans son premier paragraphe que « [l]a population civile et les personnes civiles jouissent d'une protection générale contre les dangers résultant d'opérations militaires », précise dans les paragraphes suivants « [n]i la population civile en tant que telle ni les personnes civiles ne doivent être l'objet d'attaques » et « les attaques sans discrimination sont interdites ». Les attaques enfreignant le principe de proportionnalité sont définies à l'article 51(5)(b) du Protocole additionnel I comme

> « 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 ».

L'article 51(6) interdit « les attaques dirigées à titre de représailles contre la population civile ou des personnes civiles ». L'article 52 dispose que « [l]es attaques doivent être strictement limitées aux objectifs militaires ». Et le principe de précaution énoncé à l'article 57 précise qu' « en ce qui concerne les attaques », un certain nombre de précautions doivent être prises. Le terme « attaque » est utilisé dans de nombreux autres articles restreignant les droits des belligérants[60].

Ainsi, il s'agit d'abord de savoir si les règles relatives à la conduite des hostilités ne concernent que les actes hostiles qui constituent des attaques (telles que définies à l'article 49 du Protocole additionnel I) ou si elles s'appliquent à un ensemble plus large d'opérations militaires. De manière générale, trois points de vue s'expriment sur ce sujet.

60 Voir, par ex., Arts. 12 et 54-56 du PA I.

La plupart des commentateurs estiment que la structure et le libellé du Protocole additionnel I montrent que, si l'article 48 énonce un principe général de protection de la population civile, les aspects « opérationnels » de ce principe sont précisés dans les articles suivants. Seules les cyberopérations qui constituent des attaques sont régies par les principes de distinction, de proportionnalité et de précaution[61]. Michael Schmitt a fait valoir à cet égard que certaines opérations militaires peuvent être intentionnellement dirigées contre des civils, par exemple des opérations psychologiques – ce qui, selon lui, montre que ce ne sont pas toutes les opérations militaires qui sont soumises au principe de distinction[62].

Nils Melzer considère que le débat relatif au concept d'attaque n'apporte pas de réponse satisfaisante à la question parce que les règles régissant la conduite des hostilités ne s'appliquent pas seulement aux attaques au sens strict, mais également à d'autres opérations. Pour lui,

> [b]ien comprise, l'applicabilité aux cyberopérations des restrictions à la conduite de la guerre imposées par le DIH dépend non du fait que les opérations en question puissent ou pas être qualifiées d'« attaques » (c'est-à-dire la forme la plus courante de conduite d'hostilités), mais du fait qu'elles fassent ou non partie d' « hostilités » au sens du DIH[63].

Il estime que les cyberopérations qui visent à porter préjudice à l'adversaire, soit en causant directement des morts, des blessures ou de la destruction, soit en portant directement atteinte à des opérations ou des capacités militaires, doivent être considérées comme des hostilités[64]. Par exemple, des cyberopérations visant à perturber ou mettre hors d'état de fonctionner les systèmes contrôlés par ordinateur d'un ennemi – qu'il s'agisse de systèmes de radar ou d'armement, ou de réseaux d'approvisionnement (logistique) ou de communication – pourront être qualifiées d'hostilités même si elles ne causent pas de dommages physiques. En revanche, des cyberopérations menées dans un but général de collecte de renseignements ne constitueraient pas des hostilités. S'agissant de la « neutralisation non destructrice » de biens civils, Melzer ne formule pas de conclusion précise mais évoque le dilemme qui se pose entre adopter une interprétation trop restrictive ou trop permissive du droit[65].

L'argumentation de Melzer est intéressante en ce sens qu'elle donne effet à l'objet même des règles relatives à la conduite des hostilités, qui est que « les civils inoffensifs doivent être tenus autant que possible en dehors des hostilités

61 M. N. Schmitt, « Cyber Operations and the *Jus in Bello*: Key issues », dans *Naval War College International Law Studies*, Vol. 87, 2011, p. 91 ; Robin Geiss et Henning Lahmann, « Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space », dans *Israeli Law Review*, Vol. 45, N° 3, novembre 2012, p. 2.
62 M. N. Schmitt, *ibid*., p. 91.
63 N. Melzer, *op. cit*., note 42.
64 *Ibid.,* p. 28.
65 *Ibid.*

et bénéficier d'une protection générale contre les dangers des hostilités »[66]. En revanche, elle laisse sans réponse la question la plus importante, à savoir si des opérations qui perturbent le fonctionnement d'infrastructures civiles sans les détruire entrent dans la catégorie des hostilités.

Heather Harrison Dinniss, pour sa part, estime que l'interdiction de prendre pour cible des personnes civiles ou des biens de caractère civil ne se limite pas aux attaques[67]. Elle s'appuie sur le libellé de l'article 48 du Protocole additionnel I et les premières phrases des articles 51 et 57 pour faire valoir que la population civile doit être protégée non seulement contre les attaques, mais aussi, de manière plus générale, contre les effets des opérations militaires. Ainsi, elle émet l'avis que les principes de distinction, de proportionnalité et de précaution s'appliquent aussi aux attaques de réseaux informatiques qui correspondent à la définition d'une opération militaire. Pour correspondre à cette définition, « l'attaque de réseau informatique doit être associée à l'emploi de la force physique, mais sans nécessairement avoir en elle-même des conséquences violentes »[68].

Malgré ces arguments en faveur d'un élargissement de la gamme d'opérations à laquelle doivent s'appliquer les règles relatives à la conduite des hostilités, il est évident que les États ont bien fait la distinction, dans le Protocole additionnel I, entre les principes généraux énoncés dans les paragraphes introductifs des règles concernant la distinction et les précautions et les règles spécifiques relatives aux attaques, et qu'ils ont jugé nécessaire de définir précisément les attaques à l'article 49 du Protocole. Il est difficile de faire abstraction de cette dichotomie entre opérations militaires et attaques.

Cela étant, l'argumentation de Heather Dinniss tient dûment compte du fait que les articles 48, 51 et 57 contiennent des dispositions générales qui imposent des limitations aux opérations militaires et pas seulement aux attaques, et dont la teneur, autrement, serait difficile à expliquer. Si l'on procède à une interprétation systématique de ces dispositions, les paragraphes introductifs ont un contenu important et ne sont pas superflus. De plus, l'argument de Michael Schmitt selon lequel certaines opérations, telles que des opérations psychologiques, peuvent être dirigées contre des civils – ce qui sous-entend que certaines opérations *militaires* pourraient être dirigées contre des civils – repose sur une compréhension erronée de la notion d'opérations militaires. De fait, s'il est vrai que certaines cyberopérations, telles que des opérations psychologiques, peuvent cibler la population civile, c'est parce qu'elles ne relèvent pas de la catégorie des opérations militaires ou des hostilités au sens prévu par les rédacteurs du Protocole. Selon le *Commentaire des Protocoles additionnels*, le terme « opérations » figurant à l'article 48 désigne des opérations militaires et signifie « tous les mouvements et actions en rapport avec les hostilités accomplis par les forces

66 Yves Sandoz, Christophe Swinarski et Bruno Zimmermann (éds.), *Commentaire des Protocoles additionnels du 8 juin 1977 aux Conventions de Genève du 12 août 1949*, CICR/Martinus Nijhoff Publishers, Genève, 1986, para. 1923 (ci-après *Commentaire des Protocoles additionnels*).
67 H. H. Dinniss, *op. cit.*, note 42, pp. 196-202.
68 *Ibid.*, p. 201.

armées »[69]. Le terme « opérations militaires » figurant à l'article 51 signifie également « tous les mouvements et actions en rapport avec les hostilités accomplis par les forces armées »[70]. À l'article 57, enfin, il est précisé : « par 'opérations militaires', il faut entendre les déplacements, manœuvres et actions de toute nature, effectués par les forces armées en vue des combats »[71]. Autrement dit, des opérations de propagande, d'espionnage ou des opérations psychologiques ne relèvent pas des concepts d'hostilités ou d'opérations militaires et ne sont donc pas régies par les principes de distinction, de proportionnalité et de précaution, même si elles sont effectuées par les forces armées.

Nous voyons donc que si certaines des dispositions plus spécifiques des articles 51 et 57 du Protocole additionnel I traitent précisément des attaques, on peut raisonnablement faire valoir que d'autres opérations militaires ne peuvent pas être entièrement exemptes des obligations de distinction, de proportionnalité et de précaution, car, s'il en était autrement, l'article 48 et les paragraphes introductifs des articles 51 et 57 seraient superflus. Cependant, cette question étant controversée, il est prudent d'examiner de plus près la définition du terme « attaque » et les types de cyberopérations qui en relèvent. De fait, la plupart des cyberopérations évoquées dans les exemples mentionnés plus haut relèvent du concept d'attaque et seraient interdites si elles visaient des infrastructures civiles. Nous montrerons donc que, dans la plupart de ces exemples, les opérations constituent des attaques, si bien qu'il devient sans objet de se demander si seules les « attaques », ou également les « hostilités » et les « opérations militaires », sont régies par les règles relatives à la conduite des hostilités.

### *Qu'est-ce qu'une attaque ?*

Comme nous l'avons vu plus haut, les opérations menées dans le cyberespace diffèrent de la guerre classique en ce que les moyens et méthodes d'attaque ne font pas intervenir de force cinétique, ou de « violence », pour utiliser le terme courant. Or, les attaques sont définies à l'article 49(1) du Protocole additionnel I comme « des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs ». Dans l'esprit des rédacteurs, cette formulation connotait de la violence physique.

Il convient de rappeler tout d'abord que, étant entendu qu'une attaque doit être un acte de violence, il est largement reconnu aujourd'hui que cette violence ne fait pas référence aux moyens de l'attaque – lesquels ne pourraient inclure que des moyens cinétiques[72]. Des opérations militaires ayant des conséquences violentes constituent également des attaques. Il est incontestable, par exemple, que l'emploi d'agents biologiques, chimiques ou radiologiques consti-

69 *Commentaire des Protocoles additionnels*, *op. cit.*, note 68, para. 1875.
70 *Ibid.*, para. 1936.
71 *Ibid.*, para. 2191.
72 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2004, p. 84 ; M. N. Schmitt, « Cyber Operations and the *Jus in Bello*: Key issues », *op. cit.*, note 61, p. 5.

tuerait une attaque bien qu'il ne s'agisse pas de recours à la force physique[73]. Il est donc admis depuis longtemps que ce qui définit une attaque n'est pas la violence des moyens, mais celle des conséquences[74]. Ainsi, même un flux de données (*data stream*) transmis par câble ou satellite pourrait relever de l'attaque.

La controverse porte sur les effets des cyberopérations. Elle concerne les opérations qui, contrairement aux opérations cinétiques, ne causent pas de pertes en vies humaines ni de blessures, et n'endommagent ni ne détruisent physiquement aucun bien, mais perturbent le fonctionnement de biens sans leur causer de dommages physiques – comme c'est le cas dans les exemples cités plus haut. Comme le montrent ces exemples, les cyberopérations n'ont pas nécessairement des conséquences violentes, en ce sens qu'elles ne causent ni dommages ni destruction physiques. Dans les exemples que nous avons cités, les effets dans le domaine physique seraient, au plus, indirects : si l'on provoque l'arrêt du réseau électrique, des services vitaux tels que les services hospitaliers peuvent se retrouver sans courant. Dans certains cas, les conséquences ne touchent que la capacité de communiquer ou de mener des activités commerciales, par exemple lorsqu'un système bancaire est perturbé. De telles opérations peuvent-elles être considérées comme des attaques au sens de l'article 49 du Protocole additionnel I ?

Deux positions se sont exprimées à cet égard. Selon Michael Schmitt,

> [u]ne cyberopération, comme toute autre opération, constitue une attaque lorsqu'elle tue ou blesse des personnes, qu'il s'agisse de civils ou de combattants, ou cause des dommages à des biens ou la destruction de ces biens, qu'il s'agisse d'objectifs militaires ou de biens civils[75].

Dans cette déclaration, le mot « dommages » désigne uniquement des dommages physiques. Les attaques de réseaux informatiques qui ne causent que des désagréments, ou ne font qu'interrompre temporairement le fonctionnement de biens, ne constituent pas des attaques – sauf si elles causent des souffrances humaines. Fondamentalement, le seul fait de perturber le fonctionnement d'un bien, s'il n'entraîne pas de souffrances humaines, n'endommage pas physiquement le bien pris pour cible ou ne le met pas complètement et définitivement hors d'état de fonctionner, ne constitue pas une attaque[76].

73 TPIY, *Le Procureur c/ Dusko Tadić*, Chambre d'appel, Arrêt relatif à l'appel de la défense concernant l'exception préjudicielle d'incompétence, 2 octobre 1995, paras. 120 et 124 (concernant les armes chimiques) ; *Tallinn Manual*, *op. cit.*, note 27, commentaire de la règle 30, para. 3 ; Emily Haslam, « Information warfare: technological changes and international law », dans *Journal of Conflict and Security Law*, Vol. 5, N° 2, 2000, p. 170.

74 Michael N. Schmitt, « Wired warfare: computer network attack and *jus in bello* » (La guerre par le biais des réseaux de communication : les attaques contre les réseaux informatiques et le *jus in bello*), dans *Revue internationale de la Croix-Rouge*, Vol. 84, N° 846, juin 2002, p. 377 ; *Tallinn Manual*, *op. cit.*, note 27, commentaire de la règle 30, para. 3.

75 M. N. Schmitt, « Cyber Operations and the *Jus in Bello*: Key issues », *op. cit.*, note 61, p. 6 [traduction CICR].

76 Michael Schmitt a maintenant un point de vue quelque peu différent et explique que : « La destruction comprend des opérations qui, tout en ne causant pas de dommages matériels à un bien, le détériorent

Selon Knut Dörmann, des cyberopérations peuvent aussi constituer des attaques même si elles ne causent pas la destruction du bien. Cette opinion se fonde sur la définition d'un objectif militaire figurant à l'article 52(2) du Protocole additionnel I, selon laquelle un objectif militaire est un bien « dont la destruction totale ou partielle, la capture ou la neutralisation offre en l'occurrence un avantage militaire précis ». Le mot « neutralisation » indique qu' « il est indifférent qu'un bien soit mis hors d'état de fonctionner par destruction ou de toute autre façon »[77]. Les critiques répondent à cela que la définition d'un objectif militaire n'est pas tout à fait adéquate, car elle présuppose une attaque sans pour autant définir l'attaque elle-même[78]. Cette critique ne tient pas compte du fait que le terme « neutralisation » était considéré comme signifiant « une attaque visant à empêcher un ennemi d'utiliser un bien sans nécessairement détruire ce bien »[79]. Ceci montre que les rédacteurs avaient à l'esprit non seulement les attaques visant à détruire ou à endommager des biens, mais aussi les attaques ayant pour but d'empêcher un ennemi d'utiliser un bien sans nécessairement détruire ce dernier. Par exemple, le système de défense aérienne d'un ennemi pourrait être neutralisé pendant un certain temps par une cyberopération consistant à agir sur son système informatique sans nécessairement endommager ou détruire son infrastructure physique[80].

Plus récemment, le Manuel de Tallinn définit une cyberattaque comme « une cyberopération, qu'elle soit offensive ou défensive, dont on peut raisonnablement attendre qu'elle blesse ou tue des personnes ou endommage ou détruise des biens »[81]. Toutefois, comme le montre le commentaire, les experts n'étaient pas tous du même avis sur ce qu'il fallait entendre exactement par « endommager » des biens, et sur la question de savoir si le fait d'altérer le fonctionnement d'un bien constituait un « dommage » ou quels types de perturbation entraient dans la catégorie des dommages[82].

La faiblesse de la première opinion tient au fait qu'elle est d'une portée trop limitée. Tout d'abord, il ne serait pas logique de considérer que si un bien

néanmoins en le rendant inutilisable, comme dans le cas d'une cyberopération qui ferait qu'un système dépendant d'ordinateurs ne pourrait plus fonctionner tant que les problèmes causés aux ordinateurs ne seraient pas réparés. » [traduction CICR] Voir « 'Attack' as a Term of Art in International Law: The Cyber Operations Context », dans *2012 4th International Conference on Cyber Conflict*, C. Czosseck, R. Ottis et K. Ziolkowski (directeurs de publication), 2012, OTAN, CCD COE Publications, Tallinn, p. 291. Voir aussi M. N. Schmitt, « Classification of Cyber Conflict », *op. cit.*, note 28, p. 252.

77 K. Dörmann, *op. cit.*, note 42, p. 4 [traduction CICR].

78 M. N. Schmitt, « Cyber Operations and the *Jus in Bello*: Key issues », *op. cit.*, note 61, p. 8.

79 Michael Bothe, Karl Josef Partsch et Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff Publishers, Dordrecht, 1982, p. 325 [traduction CICR].

80 C'est ce qui aurait été fait lors de l'attaque aérienne israélienne de septembre 2007 contre un bâtiment syrien présumé abriter un programme de mise au point d'armes nucléaires : il semble qu'Israël avait piraté les systèmes de défense aérienne syriens et les avait contrôlés pendant l'attaque. Voir « Arab & Israeli Cyber-War », dans *Day Press News*, 22 septembre 2009, disponible sur : http://www.dp-news.com/en/detail.aspx?articleid=55075

81 *Tallinn Manual*, *op. cit.*, note 27, règle 30 [traduction CICR].

82 *Ibid.*, commentaire de la règle 30, paras 10-12.

civil est mis hors d'état de fonctionner, quelle que soit la façon dont on procède, il n'est pas endommagé. Le fait que l'on empêche un réseau électrique de fonctionner en lui causant des dommages physiques ou en interférant avec le système électrique dont il dépend ne peut constituer un critère pertinent. L'opinion contraire permettrait de conclure que la destruction d'une maison par un bombardement serait une attaque, mais que le fait d'interrompre le fonctionnement d'un réseau électrique alimentant des milliers ou des millions de personnes n'en serait pas une. Ensuite, le principe de proportionnalité nous donne une indication des effets fortuits contre lesquels les règles régissant la conduite des hostilités doivent protéger les civils, à savoir « des pertes en vies humaines dans la population civile, des blessures aux personnes civiles, des dommages aux biens de caractère civil » causés incidemment. Le mot « dommage » n'a pas le même sens que « destruction ». Il signifie : détérioration portant atteinte à la valeur ou à l'utilité de quelque chose[83]. Ainsi, interrompre le fonctionnement de certains dispositifs en agissant sur les systèmes informatiques dont ils dépendent peut constituer un dommage dans la mesure où cela nuit à leur utilité. Troisièmement, l'idée qu'il doit y avoir une perte totale et définitive de la capacité de fonctionnement d'un bien, et cela sans qu'il y ait de dommage physique, n'a pas de sens dans les technologies de l'information. Comme les données peuvent toujours être récupérées ou changées, il n'y a pas de perte permanente et complète de cette capacité s'il n'y a pas de dommage physique. Par conséquent, la notion d'attaque doit toujours être comprise comme englobant les opérations qui interrompent le bon fonctionnement de biens sans qu'il y ait dommages physiques ni destruction, même si l'interruption est temporaire.

Cela étant, une interprétation trop large du terme « attaque » signifierait que toutes les interférences avec des systèmes informatiques civils constitueraient des attaques : l'interruption des communications par courrier électronique ou sur les réseaux sociaux, des systèmes de réservation ou d'achats en ligne, etc. Assimiler à des attaques ce type d'interruption de systèmes qui sont essentiellement des systèmes de communication dépasserait probablement la portée prévue des règles concernant la conduite des hostilités. Ces règles visent en principe à prévenir des dommages aux infrastructures civiles qui se manifesteraient dans le monde physique, et non des interventions visant à interrompre la propagande ou à perturber les communications ou la vie économique. Dans le monde d'aujourd'hui, le fait que la population civile dépende beaucoup des systèmes de communication efface ces lignes de démarcation, et il n'est pas facile de distinguer entre ce qui est « simple » communication et ce qui va plus loin.

Les normes de DIH existantes, leur objet et leur finalité donnent un certain nombre d'indications qui permettent de distinguer entre les opérations qui sont à considérer comme des attaques et celles qui ne le sont pas. Premièrement, comme nous l'avons vu plus haut, le concept d' « attaque » n'inclut pas la diffusion de propagande, les embargos ou d'autres moyens non physiques de guerre économique ou

83 D'après la définition du *Concise Oxford Dictionary*.

psychologique[84]. Les cyberopérations qui consistent en de l'espionnage, de la diffusion de propagande, des embargos ou d'autres moyens non physiques de guerre économique ou psychologique ne relèveront pas de la définition du terme « attaque ».

Deuxièmement, le DIH n'interdit pas les blocus ni les sanctions économiques qui visent délibérément non seulement l'armée mais aussi la population civile et l'économie. Ainsi, le terme « attaque » ne peut s'appliquer aux cyberopérations qui équivaudraient à des sanctions économiques. Cela ne veut pas dire que de telles opérations ne se verraient pas imposer de limites par le DIH (par exemple l'interdiction de détruire, d'enlever ou de mettre hors d'usage des biens indispensables à la survie de la population civile, ou des obligations en concernant le passage des secours humanitaires) mais, comme elles ne constituent pas des attaques, aucune disposition du DIH n'interdit de les diriger contre des civils.

Troisièmement, les règles relatives à la conduite des hostilités ne visent pas à interdire toutes les opérations qui interfèrent avec les systèmes de communication civils. Par exemple, les opérations par déni de service[85], comme le blocage d'une émission de télévision ou du site web d'une université, ne constitueraient pas toutes une attaque. Le simple fait d'interférer avec des actions de propagande, entre autres, ne constituerait sans doute pas non plus une attaque. L'équivalent de ce type d'opérations dans l'univers physique est probablement le brouillage de communications radio ou d'émissions de télévision – ce qui n'est pas considéré comme une attaque au sens du DIH.

Le critère du « désagrément » est parfois utilisé[86] pour faire la distinction entre les opérations qui sont des attaques et celles qui n'en sont pas. L'argument avancé est que des désagréments tels que le rationnement de nourriture, par exemple, n'entrent pas en ligne de compte pour la détermination des « dommages civils causés incidemment ». Par conséquent, un acte qui cause de simples désagréments ne peut être considéré comme une attaque. Si ce critère n'est pas sans intérêt, il peut y avoir des divergences de vues sur ce qui constitue un désagrément en matière d'interférence avec la cybertechnologie et les communications. Par exemple, s'il est sans doute possible de convenir que l'interruption d'un système de réservation en ligne cause de simples désagréments, il peut être plus difficile de parvenir à un consensus sur des questions telles que la perturbation de services bancaires. Il reste à voir comment ces interférences illicites seront considérées à l'avenir, en particulier dans la pratique des États.

84 M. Bothe *et al.*, *op. cit.*, note 79, p. 289.

85 C'est-à-dire des cyberopérations au moyen desquelles les services fournis par les serveurs ciblés sont rendus indisponibles pour leurs utilisateurs ou clients habituels.

86 M. N. Schmitt, « Wired Warfare », *op. cit.*, note 74, p. 377 ; Program on Humanitarian Policy and Conflict Research (Programme sur la politique humanitaire et de recherches sur les conflits), Harvard University, *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare,* 2010, commentaire de l'article 1(e), para. 7, disponible sur : http://www.ihlresearch.org/amw/aboutmanual.php (ci-après *Commentary on HPCR Manual on Air and Missile Warfare*) ; Michael N. Schmitt, « Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflict », dans National Research Council, *Proceedings of a Workshop on Deterring Cyber Attacks*, Washington, The National Academies Press, 2010, p. 155.

*Résumé*

En résumé, une cyberopération peut constituer une attaque au sens du DIH si elle fait des morts ou des blessés, ou cause des destructions ou des dommages physiques, mais aussi si elle interfère avec le fonctionnement d'un bien en perturbant le système informatique sous-jacent. Ainsi, si une cyberopération met hors d'usage un système de défense aérienne, interrompt le fonctionnement d'un réseau électrique ou empêche le système bancaire de fonctionner, elle constitue une attaque. Cependant, toutes les cyberopérations visant à perturber le fonctionnement d'infrastructures ne doivent pas être considérées comme des attaques. Lorsque l'opération n'est pas dirigée contre l'infrastructure physique dépendant du système informatique, mais vise essentiellement à bloquer la communication, elle est plutôt analogue au brouillage de signaux radio ou d'émissions de télévision – sauf, bien entendu, si elle fait partie d'une attaque telle que le blocage d'un système de défense aérienne. La différence tient au fait que dans certains cas, c'est la fonction de communication du cyberespace qui est seule visée, alors que dans d'autres c'est le fonctionnement du bien au-delà du cyberespace, dans l'univers physique. Si une interférence avec des systèmes informatiques qui cause des perturbations dans le domaine physique constitue une attaque, la question de l'interférence avec des systèmes de communication tels que le courrier électronique ou les médias, elle, n'est pas entièrement résolue.

## Le principe de distinction

Le principe de distinction veut que les parties à un conflit soient tenues, en tout temps, de faire la distinction entre civils et combattants et entre biens de caractère civil et objectifs militaires[87]. C'est là, de l'avis de la Cour internationale de Justice, un principe cardinal du droit international humanitaire[88]. Les attaques ne doivent être dirigées que contre des combattants ou des objectifs militaires. Cela signifie que, lors de la planification et de l'exécution de cyberopérations, les seules cibles autorisées au regard du DIH sont des objectifs militaires, par exemple des ordinateurs ou des systèmes informatiques qui apportent une contribution effective à des opérations militaires concrètes. Aucune attaque via le cyberespace ne peut être dirigée contre des systèmes informatiques utilisés dans des installations purement civiles.

Certains aspects du débat concernant les objectifs militaires dans le cyberespace sont préoccupants du point de vue de la protection civile. De fait, il semble que les cyberopérations seraient particulièrement appropriées lorsqu'il s'agit de prendre pour cible certains biens civils, parce qu'elles permettent aux

87 PA I, art. 48, 51 et 52; Jean-Marie Henckaerts et Louise Doswald-Beck (directeurs de publication), *Droit international humanitaire coutumier. Volume I: Règles* (ci-après « Étude sur le droit international humanitaire coutumier »), CICR/ Bruylant, Bruxelles, 2006, règles 1 à 10.

88 CIJ, *Licéité de la menace ou de l'emploi d'armes nucléaires*, *C.I.J. Recueil 1996,* Avis consultatif du 8 juillet 1996 (ci-après « Avis consultatif sur les armes nucléaires »), para. 78.

belligérants de toucher des cibles qu'il aurait été plus difficile d'atteindre jusque-là, telles que les réseaux financiers ou les réseaux de stockage de données médicales[89]. On a entendu dire que la cyberguerre pourrait conduire à une sorte de « liste de cibles élargie[90] » par rapport à la guerre classique. De plus, comme les cyberopérations peuvent mettre un bien hors d'état de fonctionner sans lui causer de dommage physique, quelques commentateurs ont avancé que le recours à des cyberopérations élargit l'éventail des cibles légitimes parce qu'il permet des attaques ayant des effets réversibles contre des biens qu'il serait autrement interdit d'attaquer[91]. Un autre argument a été avancé, selon lequel

> [l]e caractère potentiellement non létal des cyberarmes peut altérer l'évaluation de la licéité d'une attaque, ce qui peut entraîner des violations plus fréquentes du principe de distinction dans ce nouveau type de guerre que dans la guerre classique[92].

Dans ce contexte, il est important de rappeler les règles du DIH régissant les attaques contre des biens et de se pencher sur un certain nombre de problèmes juridiques particuliers qui pourraient résulter du recours aux attaques de réseaux informatiques.

Au regard du DIH, sont biens de caractère civil tous les biens qui ne sont pas des objectifs militaires[93]. Les objectifs militaires sont définis à l'article 52(2) du Protocole additionnel I comme étant

> [les] biens qui, par leur nature, leur emplacement, leur destination ou leur utilisation apportent une contribution effective à l'action militaire et dont la destruction totale ou partielle, la capture ou la neutralisation offre en l'occurrence un avantage militaire précis.

Selon l'article 52(3) du Protocole additionnel I, un bien qui est normalement affecté à un usage civil est présumé ne pas être utilisé en vue d'apporter une contribution effective à l'action militaire. Pour citer un exemple, si le fonctionnement d'une infrastructure civile particulièrement sensible, comme le sont la plupart des usines chimiques, dépend d'un réseau informatique fermé, ce réseau doit être présumé civil.

89 Michael N. Schmitt, « Ethics and Military Force: The *Jus in Bello* », Carnegie Council for Ethics in International Affairs, 7 janvier 2002, disponible sur : http://www.carnegiecouncil.org/studio/multimedia/20020107/index.html.

90 « Expanded target list » est l'expression utilisée par Eric Talbot Jensen, « Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations? », dans *American University International Law Review*, Vol. 18, 2002-2003, p 1149.

91 Mark R. Shulman, « Discrimination in the Law of Information Warfare », dans *Columbia Journal of Transnational Law,* 1999, pp. 963 et s.

92 Jeffrey T.G. Kelsey, « Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare », dans *Michigan Law Review,* Vol. 106, 2007-2008, p. 1439 [traduction CICR].

93 PA I, art. 52(1), qui relève du droit international coutumier ; Étude sur le droit international humanitaire coutumier, *op. cit.,* note 87, règle 9.

Comme l'indique clairement le libellé de l'article 52(2), il doit y avoir un lien étroit entre la cible potentielle et l'action militaire. Le terme « action militaire » renvoie aux capacités de combat de l'ennemi. Le lien en question est établi au moyen de quatre critères : nature, emplacement, destination et utilisation. Le mot « nature » désigne le caractère intrinsèque d'un bien, par exemple une arme. Les biens qui ne sont pas de nature militaire peuvent aussi apporter une contribution effective à l'action militaire de par leur emplacement particulier, leur destination ou leur utilisation en l'espèce.

À cet égard, il convient de mettre en évidence quatre questions qui peuvent être lourdes de conséquences pour les infrastructures civiles : d'abord, et surtout, le fait que la plupart des cyberinfrastructures internationales sont, dans la pratique, des infrastructures dites « à double usage » ; ensuite, la question de savoir si les usines qui produisent du matériel et des logiciels utilisés par l'armée deviennent des objectifs militaires ; le fait que l'on prenne pour cible des biens ayant ce que l'on appelle une « capacité de soutien de la guerre » ; et, enfin, les conséquences juridiques de l'utilisation de réseaux de médias sociaux à des fins militaires, par exemple pour recueillir des renseignements sur des cibles.

### *Les biens à double usage dans le cyberespace*

Les biens dits « à double usage » – expression qui ne figure pas telle quelle dans les dispositions du DIH – sont des biens qui servent à la fois à des fins civiles et militaires. En raison de leur utilisation à des fins militaires, ils deviennent des objectifs militaires au regard de l'article 52(2) du Protocole additionnel I, et des cibles légitimes pour une attaque. Parmi les exemples fréquemment cités figurent les secteurs d'une infrastructure civile qui approvisionnent l'armée pour ses opérations, telles les centrales électriques ou les réseaux électriques.

L'opinion qui prévaut actuellement est qu'un bien ne peut pas être à la fois civil et militaire. Dès lors qu'il sert à l'action militaire, il devient intégralement un objectif militaire (sauf si certains éléments « séparables » demeurent civils, par exemple différents bâtiments d'un hôpital)[94]. Contrairement à ce que proposait le CICR dans son projet de règles de 1956, qui, outre les matériels et installations purement militaires, mentionnait les moyens de communication et de transport « d'intérêt essentiellement militaire » ou les industries « essentielles pour la conduite de la guerre »[95], on considère généralement aujourd'hui que le

94 *The Commander's Handbook on the Law of Naval Operations*, Department of the Navy/Department of Homeland Security, USA, juillet 2007, para. 8.3 ; *Tallinn Manual*, *op cit.*, note 27, commentaire de la règle 39, para. 1.

95 Dans le Projet de Règles limitant les risques courus par la population civile en temps de guerre élaboré par le CICR, la liste (annexée aux règles) dressée par l'organisation avec l'aide d'experts militaires et donnée à titre de modèle, soumise à modification, se lisait comme suit : « I. Les catégories d'objectifs énumérées ci-dessous sont considérées comme présentant un intérêt militaire généralement reconnu : … 6) Les lignes et moyens de communication – tels que les rails, les routes, les ponts, les galeries, les canaux – qui sont *d'intérêt essentiellement militaire* ; 7) Les installations des stations de radiodiffusion et de télévision, les centres téléphoniques et télégraphiques *d'intérêt essentiellement militaire* ; 8) Les

bien devient un objectif militaire même si son utilisation à des fins militaires n'est que minime par rapport à son utilisation à des fins civiles. Par exemple, si une usine fournit un faible pourcentage du carburant utilisé dans des opérations militaires, même si ce n'est pas là sa raison d'être principale, elle devient un objectif militaire.

Les dangers que représente le cyberespace sont évidents : pratiquement toute la cyberinfrastructure internationale – c'est-à-dire ordinateurs, routeurs, câbles et satellites – sert à la fois aux communications civiles et aux communications militaires[96]. Un câble sous-marin qui transmet des communications militaires devient un objectif militaire – avec pour conséquence que (sous réserve d'autres règles du DIH, concernant la proportionnalité) il peut non seulement être la cible d'une cyberopération visant à interrompre la communication militaire, mais aussi être détruit. De même, un serveur contenant 5 % de données militaires deviendrait une cible légitime. Il est particulièrement important de garder ceci à l'esprit en cette ère de développement de l'informatique dématérialisée (ou informatique « en nuage ») où, en général, les utilisateurs ne savent généralement pas sur quels serveurs leurs données sont stockées ni quelles autres données sont stockées sur ces serveurs. Il semblerait qu'environ 98 % des communications du gouvernement américain utilisent des réseaux appartenant à des civils et exploités par des civils[97].

Le danger qu'une partie quelconque de la cyberinfrastructure puisse être prise pour cible est tout ce qu'il y a de plus réel. En effet, si dans certaines circonstances des États peuvent chercher à mettre hors d'usage des fonctions très précises de l'infrastructure militaire d'un adversaire, le fait que l'ensemble du cyberespace serve à des opérations militaires signifie que, dans un conflit armé, il sera du plus grand intérêt stratégique de porter atteinte aux réseaux de communication de la partie adverse et à son accès au cyberespace. Il s'agira d'empêcher l'adversaire d'accéder à des voies d'une importance critique dans le cyberespace, de détraquer ses principaux routeurs ou de perturber son accès à des nœuds de communication essentiels, et non pas seulement de juste cibler des systèmes

industries d'un intérêt essentiel pour la conduite de la guerre : a) les industries destinées à la fabrication d'armements … ; b) les industries destinées à la fabrication de fournitures et de matériel de guerre … ; c) les usines ou installations constituant d'autres centres de production et de fabrication essentielles pour la conduite de la guerre, telles que les industries métallurgiques, mécaniques, chimiques, *de caractère ou à destination nettement militaire* ; d) les installations de dépôt et de transport qui sont essentiellement destinées aux industries citées sous lettres a)- c) ; e) les installations productrices d'énergie *destinée essentiellement à la conduite de la guerre*, telles que des exploitations de charbon, de carburants, d'énergie atomique, de même que des usines à gaz ou des installations d'énergie électrique ayant principalement une destination militaire. » [Italique ajouté] Voir *Projet de Règles limitant les risques courus par la population civile en temps de guerre*, CICR, 1956, disponible sur : http://www.icrc.org/applic/ihl/dih.nsf/Treaty.xsp?action=openDocument&documentId=2131A46F908304BCC12563140043AB32 et, pour la liste annexée, http://www.icrc.org/dih/1a13044f3bbb5b8ec12563fb0066f226/b7e10d0c8054b9b8c12563bd002d95f9?OpenDocument (note de bas de page 3).

96 Voir aussi R. Geiss et H. Lahmann, *op. cit.*, note 61, p. 3.

97 Eric Talbot Jensen, « Cyber Warfare and Precautions Against the Effects of Attacks », dans *Texas Law Review*, Vol. 88, 2010, p. 1534.

informatiques spécifiques de l'infrastructure militaire[98]. Contrairement à ce qui se passe sur les théâtres d'opérations naturels, tels que la terre ou l'espace aérien, dans le cyberespace – théâtre d'opérations créé par l'homme – les belligérants ne concentreront pas leur action uniquement sur l'arme en mouvement mais sur les voies de transmission elles-mêmes[99]. Alors que dans l'espace aérien, par exemple, seul l'aéronef peut être considéré comme un objectif militaire, dans la cyberguerre, en revanche, les infrastructures physiques au moyen desquelles les cyberarmes (codes malveillants) se transmettent constituent des objectifs militaires.

Les conséquences de cette situation sur le plan humanitaire sont des plus préoccupantes en ce qui concerne la protection de la population civile. Dans un monde où une grande partie de l'infrastructure civile, des communications civiles, des finances, de l'économie et du commerce dépendent de la cyberinfrastructure internationale, il ne devient que trop facile pour les parties à un conflit de détruire cette infrastructure. Il n'est pas nécessaire de faire valoir qu'un système bancaire est utilisé pour l'action militaire, ou qu'un réseau électrique est un bien à double usage. La neutralisation des principaux câbles, nœuds, routeurs ou satellites dont dépendent ces systèmes pourra presque toujours être justifiée par le fait qu'ils servent à transmettre des informations militaires et, par conséquent, peuvent être considérés comme des objectifs militaires.

Selon le Manuel de Tallinn,

> les circonstances dans lesquelles le réseau Internet tout entier pourrait être attaqué [sont] si hautement improbables que ce risque, actuellement, est purement théorique. Au lieu de cela, le groupe international d'experts a estimé que, d'un point de vue juridique et pratique, la quasi-totalité des attaques contre l'internet devraient se limiter à certains segments discrets du réseau[100].

Il y est également fait mention des principes de précaution et de proportionnalité, qui devraient être respectés si l'internet entier ou de vastes secteurs de l'internet étaient pris pour cible. Toutefois, si ceci peut sembler rassurant à première vue, un problème subsiste : que l'internet puisse ou ne puisse pas être pris pour cible dans son intégralité, n'importe lequel de ses segments peut devenir une cible s'il est utilisé pour des communications militaires et si sa destruction ou sa neutralisation offre un avantage militaire précis (une fois encore, dans le respect des principes de proportionnalité et de précaution).

En outre, le cyberespace est résilient, en ce sens que si le flux d'informations ne peut pas passer par un canal, il existe de multiples voies et possibilités différentes, et les informations peuvent généralement être transmises par un autre chemin. Selon le Manuel de Tallinn,

98 US Department of Defense, *Quadrennial Defence Review Report*, février 2010, pp. 37-38, disponible sur : http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.
99 R. Geiss et H. Lahmann, *op. cit.*, note 61, p. 9.
100 *Tallinn Manual*, *op. cit.*, note 27, commentaire de la règle 39, para. 5 [traduction CICR].

> [l]es cyberopérations posent à cet égard des problèmes tout à fait particuliers. Prenons le cas d'un réseau qui sert à la fois à des fins militaires et civiles. Il peut être impossible de savoir sur quelle partie du réseau passeront les transmissions militaires, distinctes des transmissions civiles. En pareil cas, la totalité du réseau (ou du moins les éléments où la transmission est raisonnablement probable) est à considérer comme un objectif militaire[101].

Ceci aurait pour conséquence que, dans certaines circonstances, pratiquement tous les secteurs de l'internet pourraient être considérés comme des objectifs militaires, parce qu'ils constituent tous des voies possibles de transmission d'informations militaires.

L'interprétation large des biens à double usage en tant qu'objectifs militaires qui prévaut ne va déjà pas sans poser de problèmes dans l'univers physique[102]. Dans le cyberespace, les conséquences pourraient être exacerbées jusqu'à la situation extrême où il ne subsisterait rien de civil et où la règle essentielle selon laquelle la population civile jouit d'une protection générale contre les dangers dus aux opérations militaires deviendrait pratiquement vide de sens, sous réserve seulement des principes de proportionnalité et de précaution.

Enfin, si la plus grande partie de la cyberinfrastructure qui existe dans le monde est à double usage et peut être considérée comme un objectif militaire, se pose à la question fondamentale des limites géographiques du conflit armé. Le cyberespace est un espace véritablement sans frontières où des ordinateurs, où qu'ils soient, peuvent, à distance, être attaqués, manipulés ou transformés en moyens de guerre et objectifs militaires. Il faut garder à l'esprit que cela n'aurait pas pour seule conséquence que ces ordinateurs pourraient être piratés en retour par les systèmes informatiques pris pour cible. En théorie, en tant qu'objectifs militaires, ils pourraient être détruits par des moyens cinétiques. Par exemple, un réseau d'ordinateurs zombies, ou botnet, pourrait être utilisé pour lancer une attaque qui détruirait la cyberinfrastructure d'un adversaire. Pour mener une telle opération, la partie au conflit qui lancerait l'attaque contrôlerait à distance des milliers ou des millions d'ordinateurs à travers le monde, qui transmettraient le maliciel aux ordinateurs pris pour cible. Si l'utilisation de ce botnet avait pour effet que les millions d'ordinateurs impliqués dans le monde seraient considérés comme des objectifs militaires pouvant être attaqués, le résultat serait une sorte de cyberguerre totale. La conséquence logique, à savoir que tous ces ordinateurs à travers le monde deviendraient des cibles militaires, serait contraire aux fondements

101 *Ibid.*, commentaire de la règle 39, para. 3 [traduction CICR].

102 Voir aussi Marco Sassòli, « Legitimate Targets of Attacks under International Humanitarian Law », Background Paper prepared for the Informal High-Level Expert Meeting on the Reaffirmation and Development of International Humanitarian Law, Cambridge, 27-29 January 2003, HPCR, 2003, pp. 3-6, disponible sur : http://www.hpcrresearch.org/sites/default/files/publications/Session1.pdf ; William M. Arkin, « Cyber Warfare and the Environment », dans *Vermont Law Review*, Vol. 25, 2001, p. 780, décrivant les conséquences que les attaques aériennes de 1991 contre le réseau électrique irakien avaient eues pour la population civile, en mettant à mal non seulement la fourniture d'électricité, mais aussi les infrastructures de distribution et d'épuration de l'eau, d'assainissement et de santé ; R. Geiss et H. Lahmann, *op. cit.*, note 61, p. 16.

du droit de la neutralité dans les conflits armés internationaux (et principalement à la logique qui sous-tend ce droit, qui est d'épargner le pays tiers et ses habitants des effets des hostilités), ou à la délimitation géographique du champ de bataille dans les conflits armés non internationaux[103]. Dans un conflit armé international, le droit de la neutralité imposerait certaines limites au droit de l'État attaqué à se défendre en attaquant des infrastructures en territoire neutre[104]. Premièrement, l'État attaqué doit adresser une notification à l'État neutre et lui donner un délai raisonnable pour mettre fin à la violation ; deuxièmement, l'État attaqué n'est autorisé à prendre des mesures pour mettre fin à la violation de la neutralité que si cette violation constitue une menace sérieuse et immédiate pour sa sécurité et s'il n'existe pas d'autre mesure réalisable à temps pour répondre à cette menace. Ces restrictions sont relativement vagues, et pour qu'elles puissent véritablement protéger la population civile de l'État neutre, il faudrait probablement qu'elles fassent l'objet d'une interprétation étroite. Dans les conflits armés non internationaux, le droit de la neutralité ne s'applique pas. Cependant, ce serait éliminer complètement les limites géographiques du champ de bataille dans cette catégorie de conflits que de considérer que les hostilités se déroulent partout où un ordinateur, un câble ou un nœud est utilisé pour une action militaire (et constituerait donc normalement un objectif militaire).

En résumé, il apparaît clairement que, dans le cyberespace, le principe de distinction est de peu d'utilité pour la protection de la cyberinfrastructure civile et de toutes les infrastructures civiles qui en dépendent. Dans ce contexte, la principale protection juridique dont dispose l'infrastructure civile est celle qu'offre le principe de proportionnalité, qui sera examiné plus loin dans ce texte[105].

Le problème du double usage de la plupart des infrastructures dans le cyberespace est certainement le plus préoccupant, et les autres questions juridiques qui se posent semblent moins pressantes. Certaines d'entre elles seront néanmoins traitées dans les paragraphes qui suivent.

### *Les entreprises qui produisent des technologies de l'information utilisées pour des actions militaires*

L'équipement militaire faisant un grand usage de matériel informatique et de logiciels, les entreprises du domaine des technologies de l'information qui les

103 La question de la délimitation du champ de bataille dans les conflits armés non internationaux est sujette à controverse et dépasserait de loin la portée de cet article – mais les difficultés que présente la cyberguerre à cet égard semblent presque insolubles. Pour l'opinion du CICR, voir « Le droit international humanitaire et les défis posés par les conflits armés contemporains », XXXI[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge, Genève, 28 novembre – 1[er] décembre 2011, Rapport établi par le CICR, octobre 2011, pp. 21-22 ; pour un examen des facteurs géographiques dans la cyberguerre, voir *Tallinn Manual*, *op. cit.*, note 27, commentaire de la règle 21.

104 Ces limites découlent de l'article 22 du *Manuel de San Remo sur le droit international applicable aux conflits armés sur mer*, du 12 juin 1994, disponible sur : http://www.icrc.org/applic/ihl/dih.nsf/TRA/560?OpenDocument&.

105 *Commentary on HPCR Manual on Air and Missile Warfare*, *op. cit.*, note 86, commentaire de la règle 22(d), para. 7 ; *Tallinn Manual*, *op. cit.*, note 27, commentaire de la règle 39, para. 2 ; E. T. Jensen, « Unexpected Consequences from Knock-On Effects », *op. cit.,* note 90, p. 1157.

produisent pourraient être considérées comme des « objectifs militaires soutenant la guerre »[106] – au même titre que les fabriques de munitions. Ceci signifierait probablement qu'un certain nombre d'entreprises informatiques à travers le monde constitueraient des cibles légitimes, car nombreuses sont sans doute celles qui fournissent des éléments d'infrastructure informatique aux armées[107]. Eric Talbot Jensen, par exemple, se demande si la société Microsoft constituerait une cible légitime « étant donné le soutien qu'elle apporte à l'effort de guerre des États-Unis en facilitant les opérations militaires de ce pays ». Selon lui, « [l]e fait que la société et son siège fournissent un produit que l'armée juge essentiel à son fonctionnement, ainsi que le service après-vente pour ce produit, peut s'avérer suffisant pour que l'on conclue qu'il s'agit d'un bien à double usage ». Cela étant, il doute qu'une attaque de cette cible puisse procurer un avantage militaire précis[108].

L'exemple montre que le parallèle avec les usines de munitions ne devrait pas être poussé trop loin. Le critère pertinent de l'article 52.2 du Protocole additionnel I est que le bien doit, par son utilisation, apporter une contribution effective à l'action militaire. Or, premièrement, les entreprises ne sont pas, en tant que telles, des biens matériels mais des entités juridiques, si bien que la question serait plutôt de savoir si certains de leurs sites (en fait des bâtiments) sont devenus des objectifs militaires. Deuxièmement, il existe une différence entre les armes et les outils informatiques. Les armes sont, par nature, des objectifs militaires, ce que les systèmes informatiques génériques ne sont pas. Ainsi, on pourrait avoir à distinguer entre les usines qui mettent effectivement au point ce que l'on pourrait appeler des cyberarmes – c'est-à-dire des codes ou protocoles particuliers qui serviront à une attaque de réseau informatique précise (par exemple l'endroit où un virus spécifique tel que Stuxnet est mis au point) – et celles qui fournissent juste à l'armée du matériel informatique générique, que l'on pourrait comparer, par exemple, à l'approvisionnement alimentaire[109].

106 M. N. Schmitt, « Cyber Operations and the *Jus in Bello*: Key issues », *op. cit.*, note 61, pp. 8 et s.

107 Il était annoncé en septembre 2012 que le département américain de la Défense allait accueillir des entrepreneurs souhaitant proposer de nouvelles technologies pour la cyberguerre : S. Shane, *op. cit.*, note 3.

108 E. T. Jensen, « Unexpected Consequences from Knock-On Effects », *op. cit.,* note 90, pp. 1160 et 1168. Voir aussi E. T. Jensen, « Cyber Warfare and Precautions », *op. cit.*, note 97, p. 1544 : « Si une société d'informatique civile produit, entretient ou supporte les systèmes informatiques du gouvernement, il semble évident qu'un ennemi pourrait en conclure que cette société répond au critère de l'article 52 et peut être prise pour cible. » [Traduction CICR]

109 Le *Manuel de Tallinn* n'arrive pas non plus à une conclusion définitive sur cette question : « La difficulté surgit lorsqu'un établissement produit des articles qui ne sont pas spécifiquement destinés au secteur militaire mais qui sont néanmoins souvent utilisés à des fins militaires. Si les experts ont été unanimes à juger que la qualification ou non d'un tel établissement en tant qu'objectif militaire par utilisation dépendrait de la quantité, de la portée et de l'importance des acquisitions militaires, ils n'ont pas pas pu arriver à une conclusion définitive quant aux seuils précis à appliquer. » [Traduction CICR]

*Capacité de combat ou capacité de soutien de la guerre ?*

Dans la cyberguerre, où la tentation de prendre pour cible des infrastructures civiles est peut-être plus grande que dans la guerre classique, il est important de garder à l'esprit que, pour qu'un bien civil devienne un objectif militaire, il faut que sa contribution à l'action militaire soit véritablement dirigée contre la capacité de combat d'une partie au conflit. Si un bien contribue seulement à la capacité d'une partie au conflit en matière de « soutien de la guerre » (son effort de guerre général), il ne doit pas être considéré comme un objectif militaire.

Dans le manuel du commandement américain sur le droit des opérations navales intitulé *The Commander's Handbook on the Law of Naval Operations*, l'expression « apporter une contribution effective à l'action militaire » utilisée dans l'article 52(2) du Protocole additionnel I a été élargie et remplacée par « apporter une contribution effective à la capacité de l'ennemi en matière de combat ou de soutien de la guerre »[110]. Ceci concerne essentiellement des cibles économiques, qui peuvent apporter un soutien indirect à la capacité militaire de l'ennemi[111]. Une évaluation du droit effectuée en 1999 par le bureau du conseiller juridique du département de la Défense des États-Unis (*US Department of Defense's Legal Counsel*) concernant les cyberopérations concluait :

> … les infrastructures purement civiles ne doivent pas être attaquées à moins que la force attaquante puisse démontrer qu'un avantage militaire précis est attendu de l'attaque. … Dans un conflit armé de longue durée, les dommages causés à l'économie et aux capacités de recherche-développement de l'ennemi ont des chances de saper son effort de guerre, mais dans un conflit de courte durée et limité, il peut s'avérer difficile d'articuler un avantage militaire précis à attendre du fait d'attaquer des cibles économiques[112].

110 *The Commander's Handbook on the Law of Naval Operations*, *op. cit.*, note 94, para. 8.2 [traduction CICR].

111 Michael N. Schmitt, « Fault Lines in the Law of Attack », dans S. Breau et A. Jachec-Neale (directrices de publication), *Testing the Boundaries of International Humanitarian Law,* British Institute of International and Comparative Law, Londres, 2006, pp. 277-307. En ce qui concerne la logique qui sous-tend cette position, voir, par exemple, Charles J. Dunlap, « The End of Innocence, Rethinking Noncombatancy in the Post-Kosovo Era », dans *Strategic Review*, Vol. 28, été 2000, p. 9 ; Jeanne M. Meyer, « Tearing Down the Façade: A Critical Look at Current Law on Targeting the Will of the Enemy and Air Force Doctrine », dans *Air Force Law Review*, Vol. 51, 2001, p. 143. Voir J.T.G. Kelsey, *op. cit.*, note 92, p. 1447, qui préconise une nouvelle définition des objectifs militaires incluant certains services et infrastructures civils.

112 Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, mai 1999, p. 7, disponible sur : http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf [traduction CICR]. La position des États-Unis dans un récent rapport du Secrétaire général des Nations Unies est pour le moins ambiguë lorsqu'on y lit que les principes du *jus in bello* « interdisent les attaques contre des infrastructures purement civiles dont l'arrêt des services ou la destruction ne générerait aucun avantage militaire significatif ». Si ceci est censé impliquer que les attaques contre des infrastructures purement civiles ne seraient pas interdites si l'arrêt ou la destruction des services devait générer des avantages militaires significatifs, ce serait incompatible avec le DIH, qui n'autorise jamais les attaques contre des biens purement civils (Rapport du Secrétaire général, 15 juillet 2011, document des Nations Unies A/66/152, p. 17).

Ces théories ne tiennent pas compte des restrictions juridiques imposées par le droit international humanitaire. Le DIH n'autorise jamais les dommages à l'économie et aux capacités de recherche et de développement civiles de l'ennemi en elles-mêmes, quels que soient l'avantage militaire attendu et la durée du conflit. Si tel n'était pas le cas, il n'y aurait pas de limites à la guerre car la quasi-totalité de l'économie d'un pays peut être considérée comme apportant un soutien à la guerre[113]. Il est particulièrement important de le rappeler dans le contexte de la cyberguerre et de souligner les conséquences dévastatrices qu'une définition large des objectifs militaires pourrait avoir pour la population civile.

*Les médias et les réseaux sociaux*

Le Manuel de Tallinn se penche sur la question épineuse de l'utilisation des réseaux sociaux à des fins militaires[114] :

> Des conflits récents ont mis en évidence l'utilisation des réseaux sociaux à des fins militaires. Par exemple, Facebook a servi à organiser des opérations de résistance armée et Twitter à transmettre des renseignements d'intérêt militaire. Trois mises en garde s'imposent toutefois. La première est qu'il faut se rappeler que cette règle [à savoir qu'un bien servant à la fois à des fins civiles et militaires est un objectif militaire] s'applique sans préjudice du principe de proportionnalité et de l'obligation de prendre des précautions dans l'attaque …. La deuxième est que la licéité des cyberopérations contre des réseaux sociaux dépend de la question de savoir si ces opérations atteignent le niveau d'une attaque …. Si ce n'est pas le cas, la question de la qualification en tant qu'objectif militaire ne se pose pas. La troisième est que ceci ne veut pas dire que Facebook ou Twitter en tant que tels puissent être pris pour cible ; seuls ceux de leurs éléments qui sont utilisés à des fins militaires peuvent être attaqués [aussi longtemps que l'attaque respecte d'autres prescriptions du droit des conflits armés][115].

La qualification de réseaux sociaux tels que Facebook ou Twitter en tant qu'objectifs militaires poserait plusieurs problèmes. En effet, ces réseaux contiennent des quantités si énormes de données –la plupart absolument sans rapport avec les informations spécifiques qui devraient être ciblées – qu'il semblerait difficile d'en qualifier un d'objectif militaire. Se poserait aussi la question de savoir s'il est

113 M. Sassòli, *op. cit.*, note 102 ; Stephan Oeter, « Means and Methods of Combat », dans Dieter Fleck (directeur de publication), *The Handbook of Humanitarian Law in Armed Conflicts*, Oxford University Press, Oxford, 1995, para. 442.5.

114 On a pu lire, par exemple, que l'OTAN reconnaissait que des médias sociaux tels que Twitter, Facebook et YouTube contribuaient à sa procédure de choix de cibles en Libye, après vérification par rapport à d'autres sources : Graeme Smith, « How social media users are helping NATO fight Gadhafi in Libya », dans *The Globe and Mail*, 14 juin 2011 ; Tim Bradshaw et James Blitz, « NATO draws on Twitter for Libya Strikes », dans *The Washington Post*, 16 juin 2011.

115 *Tallinn Manual*, *op. cit.*, note 27, p. 135 [traduction CICR].

techniquement possible de n'attaquer que les éléments qui sont utilisés à des fins militaires parmi les données non structurées de ces réseaux.

Une question tout aussi difficile se pose en ce qui concerne les médias. On peut lire dans le Manuel de Tallinn :

> Un autre cas intéressant … concerne les informations publiées dans les médias. Si ces informations contribuent effectivement à l'image opérationnelle de l'ennemi, en priver ce dernier pourrait procurer un avantage militaire précis …. Certains membres du groupe international d'experts ont émis l'avis que la cyberinfrastructure supportant la transmission de ces informations pouvait constituer un objectif militaire, tout en appelant l'attention sur le fait que l'infrastructure ne pourrait être attaquée que conformément aux règles concernant l'attaque, notamment celles qui concernent la proportionnalité et les précautions dans l'attaque …. Ils ont relevé en particulier que cette dernière condition aboutirait généralement à l'obligation de ne mener que des cyberopérations visant à bloquer les émissions en question. D'autres experts ont estimé que le lien entre la contribution de la cyberinfrastructure et l'action militaire était trop distant pour que l'infrastructure soit qualifiée d'objectif militaire. Tous les membres du groupe international d'experts ont convenu que des évaluations de ce type ne pouvaient être que très contextuelles[116].

Même si telle ou telle information diffusée par un média peut apporter une contribution effective à l'action militaire, il ne faut pas en tirer la conclusion que soit l'entreprise médiatique responsable, soit la cyberinfrastructure transmettant l'information peut faire l'objet d'une attaque. En ce qui concerne les entreprises médiatiques, le fait d'accepter qu'elles soient prises pour cible pourrait être lourd de conséquences. Prenons une société de radiodiffusion internationale telle que la BBC. D'abord, l'expression « contribuer à l'image opérationnelle de l'ennemi » a un sens beaucoup trop large, plus large qu'apporter une contribution directe à l'action militaire de l'ennemi, comme cela est formulé dans l'article 52(2) du Protocole additionnel I. Ensuite, même si l'information diffusée par les médias contient des renseignements tactiques, par exemple sur des cibles précises, la proposition tendant à ce que l'entreprise médiatique elle-même puisse être prise pour cible est extrêmement problématique. Au-delà de l'entreprise elle-même, si toute la cyberinfrastructure par laquelle les informations sont transmises devait être considérée comme un objectif militaire, cela signifierait qu'une grande partie de la cyberinfrastructure de la planète pourrait être endommagée ou détruite – en gardant ici aussi à l'esprit, comme dans le cas des biens à double usage, que le fait de considérer un bien comme un objectif militaire a pour conséquence que ce bien peut aussi être visé par des moyens cinétiques, ce qui veut dire que le site physique depuis lequel et par lequel les informations sont transmises pour-

116 *Ibid.*, pp. 133-134 [traduction CICR].

rait lui-même être endommagé et détruit. Enfin, comme nous l'avons déjà vu, l'exemple des entreprises médiatiques met clairement en évidence le problème des limites géographiques du champ de bataille. De plus, dans un conflit armé international, le droit de la neutralité imposerait certaines limites à la capacité d'un État à prendre pour cible les infrastructures d'un État neutre[117].

## L'interdiction des attaques et des moyens et méthodes de combat frappant sans discrimination

Les attaques sans discrimination sont interdites[118]. Il s'agit des attaques :

- qui ne sont pas dirigées contre un objectif militaire déterminé ;
- dans lesquelles on utilise une méthode ou des moyens de combat qui ne peuvent pas être dirigés contre un objectif militaire déterminé ; ou
- dans lesquelles on utilise une méthode ou des moyens de combat dont les effets ne peuvent pas être limités comme le prescrit le DIH,

et qui sont, en conséquence, dans chacun de ces cas, propres à frapper indistinctement des objectifs militaires et des personnes civiles ou des biens de caractère civil. Les parties à un conflit, donc, « ne doivent jamais … utiliser des armes qui sont dans l'incapacité de distinguer entre cibles civiles et cibles militaires »[119].

Nous l'avons vu, le fait que la majeure partie du cyberespace puisse probablement être considérée comme à double usage ne peut que rendre difficile de séparer l'infrastructure militaire de l'infrastructure civile. Cependant, même lorsqu'il est possible de faire la distinction entre les infrastructures civiles et militaires, des attaques risquent néanmoins de frapper sans discrimination du fait de l'interconnectivité du cyberespace[120]. Celui-ci consiste en effet en d'innombrables systèmes informatiques connectés les uns aux autres partout sur la planète. Même si les systèmes informatiques militaires sont distincts des systèmes civils, ils sont souvent interconnectés avec des systèmes commerciaux civils dont ils dépendent intégralement ou partiellement. Il peut donc s'avérer impossible, si on lance une attaque informatique contre une infrastructure militaire, de limiter cette attaque et ses effets à cet objectif militaire. Les virus et les vers sont des exemples de méthodes d'attaque de réseaux informatiques qui pourraient entrer dans cette catégorie si leurs créateurs n'en restreignent pas les effets. Le recours à des vers qui se reproduisent et se propagent sans qu'on puisse les contrôler, risquant de porter gravement atteinte à des infrastructures civiles, constituerait une violation du DIH[121].

117 Voir, plus haut, « *Les biens à double usage dans le cyberespace* ».
118 Étude sur le droit international humanitaire coutumier, *op. cit.*, note 87, règle 12 ; PA I, art. 51(4).
119 CIJ, Avis consultatif sur les armes nucléaires, *op. cit.*, note 88, para. 78.
120 K. Dörmann, *op. cit.*, note 42, p. 5.
121 Le ver pourrait soit ne pas pouvoir être dirigé contre un objectif militaire déterminé (voir l'Étude sur le droit international humanitaire coutumier, règle 12(b)) ; PA I, art. 51(4)(b)), soit avoir des effets qui ne pourraient pas être limités comme le prescrit le DIH (voir l'Étude sur le droit international humanitaire coutumier, règle 12(c) ; PA I, art. 51(4)(c)).

Certains commentateurs jugent cette préoccupation exagérée et font valoir en particulier que, du fait que la plupart des cyberopérations ne seraient efficaces que si elles ciblaient des systèmes très spécifiques et extrêmement spécialisés, elles n'auraient pas d'effets nocifs sur d'autres ordinateurs. Ils citent l'exemple du virus Stuxnet, qui a été conçu très précisément pour être utilisé contre les installations nucléaires de la République islamique d'Iran[122].

De fait, si un virus est introduit dans un système militaire fermé ou est conçu de façon à ne pas pouvoir se propager à d'autres systèmes, il peut ne présenter aucun risque pour les infrastructures civiles extérieures. On peut tout à fait imaginer, cependant, qu'une partie à un conflit ne prenne pas de telles précautions ou mette au point des cyberarmes qui auraient des effets qu'elle n'aurait pas prévus sur les réseaux. Ce n'est pas parce qu'on peut concevoir des cyberarmes ne frappant pas sans discrimination que le risque d'attaques sans discrimination ne reste pas très élevé. Même le virus Stuxnet – selon ce qu'ont rapporté les médias – montre à quel point il est difficile de maîtriser les effets des virus ; il semblerait que ce virus n'était pas censé infecter d'autres ordinateurs que les systèmes pris pour cible dans les installations nucléaires visées, et pourtant, d'une façon ou d'une autre, il s'est répliqué en dehors de l'Iran[123]. Si le fait qu'il se soit propagé largement au-delà des intentions de ses créateurs n'a pas causé de dommages, il montre en revanche combien il est difficile de maîtriser la propagation des virus.

Les parties belligérantes ont donc une double responsabilité. Premièrement, elles ne doivent pas employer de cyberarmes de nature à frapper sans discrimination, telles que les virus ou les vers qui se répliquent sans qu'il soit possible de maîtriser cette propagation (au même titre que les armes bactériologiques, par exemple). L'emploi de telles armes devrait être interdit lorsque l'arme est examinée au cours de sa mise au point ou de son acquisition ; si elle ne peut jamais être utilisée sans frapper aussi bien des objectifs civils que militaires, elle est incompatible avec les prescriptions du DIH[124]. Deuxièmement, lors de chaque attaque, la partie attaquante doit vérifier si, dans les circonstances de l'espèce, la cyberarme employée peut être et est effectivement dirigée contre une cible militaire et si ses effets peuvent être limités au sens du DIH.

## Le principe de proportionnalité

Étant donné le caractère de « bien à double usage » de la majeure partie de la cyberinfrastructure, d'une part, et le risque de répercussions sur l'infrastructure civile qui existe – du fait de l'interconnectivité du cyberespace – même lorsque des ordinateurs ou des systèmes informatiques exclusivement militaires sont pris pour cible, d'autre part, on peut sérieusement craindre que des infrastructures civiles ne soient gravement touchées par des cyberopérations menées dans le

122 T. Rid, *op. cit.*, note 24.
123 D. E. Sanger, *op. cit.*, note 23.
124 Ceci découle de l'article 36 du PA I pour les États parties au Protocole, mais aussi de l'obligation générale qu'ont les belligérants de ne pas employer d'armes frappant sans discrimination.

cadre de conflits armés. Le principe de proportionnalité devient dès lors une règle cruciale pour la protection de la population civile.

Le principe de proportionnalité est formulé à l'article 51(5)(b) du Protocole additionnel I, qui relève du droit international coutumier[125]. Sont interdites

> « 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 ».

Comme cela a été précisé plus haut, un dommage causé à un bien signifie une détérioration portant atteinte à la valeur ou à l'utilité de ce bien[126]. Il est donc clair que les dommages à prendre en compte sont non seulement les dommages physiques que peut subir une infrastructure civile, mais aussi la mise hors d'état de fonctionner de cette infrastructure même en l'absence de tout dommage physique. Il a été avancé que « les cyberattaques peuvent changer l'importance donnée aux conséquences temporaires dans l'appréciation de la proportionnalité »[127], mais cet argument n'a aucun fondement juridique dans le DIH. Comme l'expliquent Geiss et Lahmann, toute autre interprétation aurait la conséquence suivante :

> Alors que la destruction d'un seul véhicule civil représenterait un « dommage collatéral » juridiquement pertinent, bien qu'assez insignifiant, le fait que des milliers ou des millions de foyers, d'entreprises et de services publics soient déconnectés de l'internet ou d'autres moyens de communication, ou que les transactions financières en ligne soient interrompues pour toute l'économie d'un pays, ainsi que les effets économiques et sociétaux correspondants, ne constitueraient pas, en soi, des éléments pertinents à intégrer dans le calcul de la proportionnalité[128].

Il faut toutefois avoir conscience que, lorsque des attaques de réseaux informatiques causent des dommages à des infrastructures civiles, par exemple en interrompant temporairement leur fonctionnement, le principe de proportionnalité est soumis à un certain nombre de limitations (comme c'est le cas également dans la guerre classique).

Premièrement, comme dans toutes les applications du principe de proportionnalité, il subsiste une certaine incertitude quant à ce qui peut être considéré comme un dommage excessif causé incidemment à des biens civils par rap-

125 Étude sur le droit international humanitaire coutumier, *op. cit.*, note 87, règle 14.
126 D'après la définition du *Concise Oxford Dictionary*.
127 Oona Hathaway *et al.*, « The Law of Cyber-Attack », dans *California Law Review*, Vol. 100, N° 4, 2012, p. 817.
128 R. Geiss et H. Lahmann, *op. cit.*, note 61, p. 17.

port à l'avantage militaire concret et direct attendu. Apparemment, il n'arrive pas souvent que les dommages causés incidemment à des infrastructures civiles soient jugés excessifs par rapport à l'avantage militaire escompté[129]. Cela ne veut pas dire que le principe de proportionnalité ne pose pas du tout de limites aux attaques, mais il reste à voir comment il sera interprété en ce qui concerne les cyberattaques.

D'une part, on peut faire valoir que les cyberopérations en étant encore à leurs débuts, on ne sait que peu de choses sur leur impact, et il ne peut être attendu des commandants qu'ils prévoient leurs effets ; il est également difficile de savoir, dans la cyberguerre, quels sont les pertes ou dommages causés incidemment que l'« on peut attendre ». D'autre part, cette incertitude est plutôt quantitative que qualitative. Précisément à cause de l'interconnexion des réseaux, les conséquences pour les infrastructures civiles sont évidentes. En d'autres termes, on doit s'attendre dans la plupart des cas à des dommages causés incidemment, même s'il est difficile d'estimer leur étendue exacte.

Deuxièmement, s'il est désormais pratiquement incontesté qu'il faut tenir compte des répercussions d'une attaque – c'est-à-dire de ses effets indirects secondaires et tertiaires – l'étendue de cette obligation fait encore débat[130]. Étant donné la formulation de l'article 51(5)(b) du Protocole additionnel I (« on peut attendre »), il est raisonnable d'estimer qu'il faut tenir compte des dommages prévisibles, même s'il s'agit de dommages collatéraux à long terme[131]. Dans le cyberespace, en raison de l'interconnexion des réseaux, il peut être plus difficile de prévoir les effets à attendre que lorsqu'on utilise un armement cinétique classique, mais, en même temps, il est d'autant plus indispensable de faire le maximum pour estimer ces effets. Concrètement, cela nous amène à la question des précautions à prendre dans les attaques. Étant donné l'interconnectivité des réseaux d'information et des systèmes qui en dépendent, quelles vérifications

129 Voir Louise Doswald-Beck, « Some Thoughts on Computer Network Attack and the International Law of Armed Conflict », dans Michael N. Schmitt et Brian T. O'Donnell (directeurs de publication), *Computer Network Attack and International Law*, International Law Studies, Vol. 76, 2002, p. 169: « … on a surtout connu des exemples … où soit la cible possible était de caractère militaire mais inutilisable en l'occurrence, soit la valeur du bien en tant qu'objectif militaire ne pouvait pas être vérifiée ». Voir aussi TPIY, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia* (Rapport final présenté au Procureur par le Comité chargé d'examiner la campagne de bombardements de l'OTAN contre la République fédérale de Yougoslavie, ci-après « Rapport final présenté au Procureur »), 13 juin 2000, para. 19. Au sujet du bombardement par les forces de l'OTAN du complexe industriel de Pancevo et d'une raffinerie de pétrole à Novi Sad pendant la guerre au Kosovo, en 1999 – bombardement qui avait causé le déversement d'environ 80 000 tonnes de pétrole brut dans le sol et avait libéré des tonnes d'autres substances toxiques –, le comité avait déclaré : « [i]l est difficile d'évaluer les valeurs relatives à attribuer à l'avantage militaire obtenu et aux dommages causés à l'environnement, et il est plus facile de parler d'appliquer le principe de proportionnalité que de l'appliquer dans la pratique. » [Traduction CICR]

130 Voir, par ex., *Commentary on HPCR Manual on Air and Missile Warfare*, *op. cit.*, note 86, commentaire de la règle 14, para. 4; Michael N. Schmitt, « Computer Network Attack: the Normative Software », dans *Yearbook of International Humanitarian Law*, La Haye, TMC Asser Press, 2001, p. 82.

131 *Tallinn Manual*, *op. cit.*, note 27, commentaire de la règle 51, para. 6 ; R. Geiss et H. Lahmann, *op. cit.*, note 61, p. 16.

peut-on attendre d'un commandant lorsqu'il évalue les répercussions que pourra avoir une attaque de réseau informatique[132] ?

## Le principe de précaution

Le principe de précaution, en droit international humanitaire, a deux composantes : les précautions dans l'attaque et les précautions contre les effets des attaques[133].

### *Précautions dans l'attaque*

Dans la conduite des opérations militaires, il faut veiller constamment à épargner la population civile, les personnes civiles et les biens de caractère civil[134]. Le DIH prescrit notamment de faire tout ce qui est pratiquement possible pour vérifier que les objectifs à attaquer sont des objectifs militaires[135] et de prendre toutes les précautions pratiquement possibles quant au choix des moyens et méthodes d'attaque en vue d'éviter et, en tout cas, de réduire au minimum les pertes en vies humaines dans la population civile, les blessures aux personnes civiles et les dommages aux biens de caractère civil qui pourraient être causés incidemment[136]. Il dispose en outre que les parties au conflit devront annuler ou interrompre une attaque s'il apparaît que celle-ci causera des « dommages collatéraux » excessifs[137].

Ainsi, les précautions peuvent comprendre des obligations telles que prendre des mesures pour réunir toutes les informations disponibles afin de vérifier la cible d'une attaque et les effets que pourrait avoir incidemment ladite attaque[138]. Dans la cyberguerre, les précautions peuvent consister notamment à cartographier le réseau de l'adversaire[139], ce qui, de toute façon, fera souvent partie de la mise au point des attaques de réseaux informatiques si elles sont conçues pour cibler un système informatique particulier. Si l'on ne dispose que d'informations incomplètes, comme cela peut être le cas dans le cyberespace en raison de son interconnectivité, il faudra peut-être limiter la portée de l'attaque aux seules cibles sur lesquelles on dispose de suffisamment de renseignements[140].

132 À distinguer de l'attaque sans discrimination, dont les effets ne peuvent pas être limités.
133 Voir PA I, arts. 57 et 58 ; Étude sur le droit international humanitaire coutumier, *op. cit.*, note 87, règles 15-24.
134 PA I, art. 57(1) ; Étude sur le droit international humanitaire coutumier, *ibid.*, règle 15.
135 PA I, art. 57(2)(a)(i) ; Étude sur le droit international humanitaire coutumier, *ibid.*, règle 16.
136 PA I, art. 57(2)(a)(ii) ; Étude sur le droit international humanitaire coutumier, *ibid.*, règle 17.
137 PA I, art. 57(2)(b) ; Étude sur le droit international humanitaire coutumier, *ibid.*, règle 19.
138 TPIY, Rapport final présenté au Procureur, *op. cit.*, note 129, para. 29. Dans son rapport final, le comité décrit l'obligation en ces termes : « Un commandant militaire doit mettre sur pied un système de renseignement efficace pour réunir et évaluer des informations concernant les cibles potentielles. Il doit aussi ordonner à ses hommes d'utiliser les moyens techniques disponibles pour identifier correctement les cibles au cours des opérations. Tant le commandant que les équipages effectivement engagés dans les opérations doivent avoir une certaine latitude pour déterminer lesquelles des ressources disponibles seront utilisées, et comment. » [Traduction CICR]
139 E. T. Jensen, « Unexpected Consequences from Knock-On Effects », *op. cit.*, note 90, p. 1185.
140 *Tallinn Manual*, *op. cit.*, note 27, règle 53, para. 6.

Le principe de précaution peut exiger des compétences techniques spéciales. Le Manuel de Tallin précise que,

> « [é]tant donné la complexité des cyberopérations, la forte probabilité de porter atteinte à des systèmes civils et la compréhension parfois limitée de la nature de ces opérations et de leurs effets qu'ont parfois ceux qui sont chargés de les approuver, les responsables de la planification des missions devraient, lorsque cela s'avère possible, pouvoir disposer de l'aide d'experts techniques pour déterminer si les mesures de précaution appropriées ont été prises »[141].

S'il n'a pas à disposition les compétences techniques nécessaires et, par conséquent, la capacité d'évaluer la nature de la cible ou les pertes ou les dommages qui pourraient être causés incidemment, l'attaquant pourrait devoir s'abstenir de lancer l'attaque.

Il est probable, cependant, que de nombreuses cyberattaques défensives seront des cyberopérations automatiques, préprogrammées contre des intrusions venant de l'extérieur[142]. Ces opérations de piratage en retour, ou « rétropiratage », sont automatiques et ciblent simplement les ordinateurs d'où provient l'intrusion. Comme elles s'attaquent à un problème technique, elles ne sont pas concernées par le caractère civil ou militaire des ordinateurs. En pareille situation, et du fait que les cyberattaques de ce type proviendront de milliers, voire de millions d'ordinateurs, les États devront évaluer soigneusement la licéité de ce rétropiratage automatique au regard du principe de précaution.

Considéré sous un autre angle, le principe de précaution pourrait, dans certains cas, entraîner une obligation d'avoir recours à la cybertechnologie quand elle est disponible. En effet, les cyberopérations pourraient causer incidemment moins de dommages à des personnes civiles ou des infrastructures civiles que les opérations cinétiques. Il pourrait être moins préjudiciable, par exemple, de perturber certains services utilisés à des fins militaires et civiles que de détruire complètement les infrastructures concernées. Cependant, la mesure dans laquelle il y aurait obligation d'avoir recours à une technologie plus perfectionnée – en l'occurrence la cybertechnologie – n'est pas entièrement définie. De fait, il n'existe pas encore de consensus international établissant que les parties belligérantes doivent en tout temps employer les armes les plus précises et les plus avancées technologiquement (le débat sur ce sujet portant essentiellement sur les munitions à guidage de précision)[143]. Néanmoins, le principe de précaution contient l'obligation non seulement de respecter les principes de distinction et de proportionnalité, mais

141 *Ibid.*, règle 52, para. 6 [traduction CICR].

142 Selon le PA I, art. 49, ces opérations défensives sont elles aussi des « attaques » qui doivent respecter les principes de distinction, de proportionnalité et de précaution.

143 Jean-François Quéguiner, « Precautions under the law governing the conduct of hostilities » (Précautions prévues par le droit régissant la conduite des hostilités), dans *Revue internationale de la Croix-Rouge*, Vol. 88, N° 864, décembre 2006, p. 801 ; *Commentary on HPCR Manual on Air and Missile Warfare*, *op. cit.*, note 86, commentaire de la règle 8, para. 2.

aussi prendre toutes les dispositions pratiquement possibles « en vue d'éviter et, en tout cas, de réduire au minimum » les pertes et dommages civils qui pourraient être causés incidemment. En pareils cas, le principe de précaution implique probablement que les commandants choisissent les moyens les moins nuisibles disponibles au moment de l'attaque pour réaliser leur objectif militaire[144].

### *Précautions contre les effets des attaques*

Le principe de précaution contre les effets des attaques impose aux parties au conflit, entre autres, les précautions suivantes : « Dans toute la mesure de ce qui est pratiquement possible, les Parties au conflit … s'efforceront … d'éloigner du voisinage des objectifs militaires la population civile, les personnes civiles et les biens de caractère civil soumis à leur autorité » et « prendront les autres précautions nécessaires pour protéger contre les dangers résultant des opérations militaires la population civile, les personnes civiles et les biens de caractère civil soumis à leur autorité »[145]. Cela signifie que les États sont tenus soit de maintenir les biens militaires à distance des personnes civiles et des biens de caractère civil, soit (en particulier si ce qui précède n'est pas réalisable) de prendre d'autres mesures pour protéger les personnes et les infrastructures civiles des dangers résultant des opérations militaires.

Comme le précise le Manuel de Tallinn, il peut s'agir « de séparer les cyberinfrastructures militaires et civiles ; d'isoler de l'internet les systèmes informatiques dont dépendent des infrastructures civiles critiques ; de sauvegarder ailleurs des données civiles importantes ; de prendre des dispositions à l'avance afin que des systèmes informatiques importants puissent être réparés rapidement si certains types de cyberattaques prévisibles se produisent ; de procéder à des enregistrement numériques de biens culturels ou spirituels importants pour faciliter leur reconstruction au cas où ils seraient détruits pendant un conflit armé ; et de prendre des mesures antivirus pour protéger les systèmes civils qui pourraient être endommagés ou détruits pendant une attaque contre une cyberinfrastructure militaire »[146].

De fait, il est souvent préconisé que les réseaux militaires et civils soient séparés[147]. Comme le recommande l'évaluation juridique du département américain de la Défense, « lorsqu'on a le choix, les systèmes militaires devraient être tenus séparés des infrastructures utilisées à des fins essentiellement civiles »[148]. Ceci, toutefois, est peu réaliste. Aux débuts de l'internet,

144 K. Dörmann, *op. cit.*, note 42 ; Michael N. Schmitt, « The Principle of Discrimination in 21st Century Warfare », dans *Yale Human Rights and Development Law Journal*, Vol. 2, 1999, p. 170 ; *Commentary on HPCR Manual on Air and Missile Warfare*, *op. cit.*, note 86, commentaire de la règle 32(b), para. 3, au sujet des armes ayant une plus grande précision ou moins de force explosive.

145 PA I, art. 58 ; Étude sur le droit international humanitaire coutumier, *op. cit.*, note 87, règles 22 et 24.

146 *Tallinn Manual*, *op. cit.*, note 27, commentaire de la règle 59, para. 3 [traduction CICR].

147 E. T. Jensen, *op. cit.*, note 97, pp. 1533-1569 ; Adam Segal, « Cyberspace Governance: The Next Step », Council on Foreign Relations, *Policy Innovation Memorandum N° 2*, 14 novembre 2011, p. 3, disponible sur : http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

148 Department of Defense Office of General Counsel, *op. cit.*, note 112, p. 7 [traduction CICR].

la construction ne tenait probablement pas compte de ces questions. Il existe bien entendu des réseaux militaires fermés, et des infrastructures civiles très sensibles sont également isolées des réseaux extérieurs. Mais, étant donné la faiblesse inhérente de la disposition prévoyant que les biens civils soient séparés des biens militaires (article 58(a) du Protocole additionnel I), qui n'oblige les États qu'à s'efforcer d'éloigner les biens civils du voisinage des objectifs militaires, et seulement dans toute la mesure de ce qui est pratiquement possible, il est très improbable que les États, dans leur pratique, interprètent cette règle comme les obligeant à isoler les réseaux militaires des réseaux civils. S'il est vrai que ce serait faisable en théorie, ce serait si compliqué pratiquement et si coûteux que ce serait considéré comme irréalisable au sens de l'article 58 du Protocole. Les gouvernements devraient créer leur propre matériel informatique et leurs propres logiciels à usage militaire et créer leurs propres lignes de communication militaires – y compris les câbles, routeurs et satellites – dans le monde entier[149].

En outre, la séparation des cyberinfrastructures militaire et civile repose sur le postulat que ces cyberinfrastructures sont distinctes et devraient le rester. Au sens strict, l'article 58 n'interdit pas le double usage : il repose sur le principe qu'une distinction est établie entre biens civils et biens militaires, même si certains biens civils sont utilisés comme objectifs militaires. Dans l'univers physique déjà, des infrastructures critiques sont en grande partie à double usage, notamment les réseaux électriques, mais aussi, dans bien des cas, les oléoducs, les centrales électriques et le réseau routier. Ce principe perd dans une certaine mesure son sens dans le cyberespace, où le problème n'est pas le fait que l'infrastructure civile et l'infrastructure militaire soient implantées au même endroit, mais qu'elles ne fassent qu'une[150].

La question, dès lors, est de savoir si, en vertu de l'article 58(c) du Protocole additionnel I, au moins certaines infrastructures civiles (telles que centrales nucléaires, usines chimiques, hôpitaux) devraient être protégées contre tout dommage en cas de cyberattaque, ce qui supposerait que les États prennent des mesures pour maintenir leur capacité de fonctionnement. Eric Talbot Jensen, par exemple, recommande que, pour remplir leur obligation aux termes de l'article 58, les États-Unis prennent un certain nombre de mesures comme cartographier les systèmes, réseaux et industries civils qui deviendront des objectifs militaires, faire en sorte que le secteur privé soit suffisamment protégé, établir ou maintenir des solutions de rétropiratage ou créer une réserve stratégique de capacité Internet[151]. La tendance de nombreux pays à protéger leur infrastructure critique va sans nul doute dans cette direction, bien qu'il soit peu probable que les gouvernements conçoivent cette protection sous forme de précautions passives au sens de l'article 58(c).

149 E. T. Jensen, *op. cit.*, note 97, pp. 1551-1552.
150 Voir aussi R. Geiss et H. Lahmann, *op.cit.*, note 61, p. 14.
151 E. T. Jensen, *op. cit.*, note 97, pp. 1563 et s.

## Conclusion

Comme nous l'avons vu dans l'introduction, les cyberopérations feront intervenir de nouveaux moyens et méthodes de combat dont les effets n'ont pas encore été expérimentés ou sont mal cernés. Il semble toutefois que l'utilisation militaire des technologies de l'information pose de sérieux problèmes en matière d'application du DIH, et mette à mal en particulier le principe même selon lequel biens civils et biens militaires peuvent et doivent être distingués les uns des autres dans un conflit armé. Si l'on veut parvenir à des positions claires sur ce que les États entendent faire pour respecter les principes de distinction, de proportionnalité et de précaution, cette question devrait être examinée de façon plus franche et honnête que cela n'a été le cas jusqu'à présent.

Étant donné les dangers que la cyberguerre représente pour les infrastructures civiles, un certain nombre de solutions sont proposées *de lege lata* et *de lege ferenda*. L'une des propositions est que les États fassent des déclarations de « refuges numériques », c'est-à-dire de cibles civiles qu'ils considéreront comme inattaquables dans la conduite des cyberopérations[152]. Si les parties parviennent à un accord sur ces refuges, ceux-ci seraient l'équivalent des zones démilitarisées prévues à l'article 60 du Protocole additionnel I. Cela exigerait le processus de dialogue et les mesures de confiance qui sont prônées actuellement, et qui dépassent le champ du présent article. Selon Adam Segal, « il est probable que l'on se mettra assez facilement d'accord sur certains éléments – les hôpitaux et les systèmes de données médicales – mais beaucoup moins sur d'autres, comme les systèmes financiers, les réseaux électriques et l'infrastructure Internet »[153]. Si c'est là une formule intéressante à étudier – et une voie qui pourrait bien être explorée à terme dans le cadre d'un dialogue international sur des mesures de confiance – ce ne serait probablement pas faire preuve de trop de pessimisme que d'être sceptique sur ses chances de se réaliser dans un proche avenir. Étant donné le caractère secret d'une bonne partie des manipulations et des infiltrations dont semble être actuellement le théâtre le cyberespace, on voit mal quelle confiance sera accordée à des accords ou des déclarations sur des cyberzones qui seraient interdites à tout usage militaire.

Une autre proposition a été formulée par Geiss et Lahmann : élargir, par analogie, la liste des « ouvrages et installations contenant des forces dangereuses » visés à l'article 56 du Protocole additionnel I[154]. Cela pourrait s'appliquer à des éléments de cyberinfrastructure spécifiques, tels que les principaux nœuds d'échange Internet ou les serveurs centraux dont dépendent des millions de fonctions civiles importantes. Tout comme les barrages, les digues et les centrales nucléaires de production d'énergie électrique, ils ne pourraient pas faire l'objet d'attaques même s'ils constituaient des objectifs mili-

152 A. Segal, *op. cit.*, note 147 [traduction CICR].
153 *Ibid.*
154 R. Geiss et H. Lahmann, *op. cit.*, note 61, p. 11.

taires, parce que les dangers que cela représenterait pour la population civile seraient toujours considérés comme pesant plus lourd que l'avantage militaire attendu d'une attaque. Cependant, Geiss et Lahmann reconnaissent aussi qu'il est improbable qu'une telle proposition trouve grâce aux yeux des États. En particulier, s'il est vrai que la neutralisation ou la destruction de cyberinfrastructures pourraient avoir des répercussions énormes, il serait difficile de faire valoir qu'elles seraient comparables au rejet d'émissions telles que des substances radioactives ou à la libération des eaux d'un barrage. Si, toutefois, elles avaient des effets catastrophiques comparables, la logique qui sous-tend l'article 56 du Protocole additionnel I pourrait fournir un argument persuasif pour protéger également les cyberinfrastructures.

Les défis que représente la cybersphère suscitent en outre la question de savoir si (certains) moyens et méthodes de cyberguerre devraient être totalement interdits ou réglementés par un traité international. Comme cela a été mentionné dans l'introduction, plusieurs États ont plaidé en faveur d'un nouveau traité sur ce sujet, même si les contours de ce qu'il conviendrait d'autoriser ou pas ne sont pas toujours très clairs. Un autre débat se déroule parallèlement parmi les experts de la cybersécurité et les milieux universitaires. Certains ont proposé de nouveaux traités relatifs à la cyberguerre[155], tandis que d'autres estiment qu'il devrait y avoir un type de traité sur le désarmement interdisant la totalité ou, au moins, une partie des cyberarmes[156]. D'autres encore répliquent qu'un traité ne serait pas applicable en raisons des difficultés d'attribution de responsabilité, qu'il serait techniquement impossible de faire la distinction entre les instruments de cyberguerre et de cyberespionnage, que les armes interdites pourraient être moins dangereuses que des armes classiques, et que les vérifications seraient impossibles[157].

155 Mark R. Shulman, « Discrimination in the Law of Information Warfare », dans *Columbia Journal of Transnational Law,* 1999, p. 964 ; Davis Brown, « A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict », dans *Harvard International Law Journal*, Vol. 47, N° 1, hiver 2006, p. 179 ; Duncan B. Hollis, « Why States Need an International Law for Information Operations », dans *Lewis and Clark Law Review*, Vol. 11, 2007, p. 1023.

156 Mary Ellen O'Connell, « Cyber Mania », dans *Cyber Security and International Law*, Meeting Summary, Chatham House, 29 mai 2012, disponible sur : http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf ; Misha Glenny, « We will rue Stuxnet's cavalier deployment », dans *Financial Times*, 6 juin 2012, citant l'expert russe de la lutte antivirus Eugen Kaspersky ; Scott Kemp, « Cyberweapons: Bold steps in a digital darkness? », dans *Bulletin of the Atomic Scientists*, 7 juin 2012, disponible sur : http://thebulletin.org/web-edition/op-eds/cyberweapons-bold-steps-digital-darkness ; Bruce Schneier, « An International Cyberwar Treaty Is the Only Way to Stem the Threat », dans *US News*, 8 juin 2012, disponible sur : http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/an-international-cyberwar-treaty-is-the-only-way-to-stem-the-threat ; Duncan Hollis, « An e-SOS for Cyberspace », dans *Harvard International Law Journal,* Vol. 52, N° 2, été 2011, qui expose des arguments en faveur d'un système d'e-SOS.

157 Herb Lin et Thomas Rid, « Think Again: Cyberwar », dans *Foreign Policy,* mars/avril 2012, p. 7, disponible sur : http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?print=yes&hidecomments=yes&page=full ; Jack Goldsmith, « Cybersecurity Treaties: A Skeptical View », dans Peter Berkowitz (directeur de publication), *Future Challenges in National Security and Law*, disponible sur : http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

Certains commentateurs proposent d'autres solutions, telles que le « multilatéralisme informel[158] » ou une organisation internationale de cybersécurité, du même genre que l'Agence internationale de l'énergie atomique, qui jouerait le rôle d'une plate-forme indépendante de coopération internationale dans le but d'élaborer des traités pour le contrôle des cyberarmes[159].

Il est difficile de savoir, à ce stade, où mèneront ces discussions, et surtout si les États sont disposés à débattre franchement des dangers réels de la cyberguerre et à prendre des mesures pour prévenir les scénarios catastrophe. Entretemps, si les parties choisissent des cyberarmes pendant un conflit armé, elles doivent avoir conscience du cadre juridique existant, qui impose de respecter un ensemble minimum de règles, quelles qu'en soient les limitations. Ces parties doivent instruire leurs forces en conséquence. Il est important d'encourager le débat sur ces questions, de sensibiliser les acteurs concernés à la nécessité d'évaluer l'impact humanitaire de l'élaboration des technologies, et de veiller à ce que celles-ci ne soient pas employées prématurément, dans des conditions ne garantissant pas le respect du droit.

Pour conclure, il ne fait aucun doute que le DIH s'applique à la cyberguerre. Toutefois, la mesure dans laquelle il apportera une protection suffisante à la population civile, en particulier en évitant que des infrastructures civiles ne soient endommagées, dépendra de la façon dont ses dispositions, dont les rédacteurs n'avaient pas envisagé ce type d'opérations, seront interprétées concernant lesdites opérations. Ce n'est que si elles sont interprétées en toute bonne foi et avec le plus grand soin, et dans ce cas seulement, qu'il sera possible de protéger les infrastructures civiles du risque d'être prises directement pour cible ou de subir des dommages qui pourraient être catastrophiques pour la population civile. Même alors, étant donné les faiblesses potentielles des principes de distinction, de proportionnalité et de précaution – et en l'absence d'une connaissance plus approfondie des capacités et effets offensifs des cyberopérations – il ne saurait être exclu que des règles plus strictes s'avèrent nécessaires.

158 A. Segal, *op. cit.*, note 108.

159 Eugene Kaspersky, « Der Cyber-Krieg kann jeden treffen », dans *Süddeutsche*, 13 septembre 2012, disponible sur : http://www.sueddeutsche.de/digital/sicherheit-im-internet-der-cyber-krieg-kann-jeden-treffen-1.1466845.