Volume 94 Sélection française 2012/2

REVUE INTERNATIONALE de la Croix-Rouge Sélection française

Débat humanitaire: droit, politiques, action

Guerre et nouvelles technologies

CICR

REVUE
INTERNATIONALE
de la Croix-Rouge

But et contenu

Créée en 1869, la *Revue internationale de la Croix-Rouge* est un périodique publié par le Comité international de la Croix-Rouge (CICR) qui entend favoriser la réflexion sur le droit international humanitaire, la politique et l'action en temps de conflit armé et d'autres situations de violence armée collective. En tant que revue spécialisée en droit humanitaire, elle cherche à promouvoir la connaissance, l'examen critique et le développement de ce droit, et elle contribue à la prévention de violations des règles protégeant les valeurs et les droits fondamentaux. La *Revue* offre une tribune pour discuter de l'action humanitaire contemporaine et analyser les causes et les caractéristiques des conflits, afin de favoriser la compréhension des problèmes humanitaires qui en découlent. Enfin, la *Revue* informe ses lecteurs sur les questions ayant trait au Mouvement international de la Croix-Rouge et du Croissant-Rouge et, en particulier, sur la doctrine et les activités du CICR.

Comité international de la Croix-Rouge

Organisation impartiale, neutre et indépendante, le Comité international de la Croix-Rouge (CICR) a la mission exclusivement humanitaire de protéger la vie et la dignité des victimes de conflits armés et d'autres situations de violence, et de leur porter assistance. Le CICR s'efforce également de prévenir la souffrance par la promotion et le renforcement du droit et des principes humanitaires universels. Créé en 1863, le CICR est à l'origine des Conventions de Genève et du Mouvement international de la Croix-Rouge, dont il dirige et coordonne les activités internationales dans les conflits armés et les autres situations de violence.

Équipe éditoriale

Rédacteur en chef: Vincent Bernard
Assistantes de rédaction: Elvina Pothelet, Mariya Nikolova et Gaetane Cornet
Conseiller spécial sur Guerre et nouvelles technologies : Raymond Smith
Assistante de publication: Claire Franc Abbas

Revue internationale de la Croix-Rouge
Avenue de la Paix 19
CH - 1202 Genève
Tél: +41 22 734 60 01
Fax: +41 22 733 20 57
Courriel: review@icrc.org

Volume 94 Sélection française 2012/2

INTERNATIONALE
de la Croix-Rouge
Sélection française

Guerre et nouvelles technologies

INTERNATIONALE

TABLE DES MATIÈRES

Cette publication rassemble une sélection d'articles parus dans la version originale en anglais (*International Review of the Red Cross*, Vol. 94, N° 886, Summer 2012).

Guerre et nouvelles technologies

Articles

Volume 94 Sélection française 2012/2

Rapports et documents

INTERNATIONALE

ÉDITORIAL – LA SCIENCE NE PEUT PAS ÊTRE PLACÉE AU-DESSUS DE SES CONSÉQUENCES

Dans la mythologie grecque, le mythe d'Icare illustre le désir de l'être humain d'aller toujours plus loin au risque de se heurter aux limites de sa condition. Il évoque aussi l'ambivalence de notre soif de connaissance et de progrès. Icare et son père Dédale cherchant à fuir leur ennemi en Crète pour gagner la Grèce, ce dernier a l'idée de fabriquer des ailes semblables à celles des oiseaux, confectionnées avec de la cire et des plumes. Grisé par le vol, Icare oublie les conseils de prudence de son père et s'approche trop près du soleil. La chaleur fait fondre la cire de ses ailes artificielles, elles se désagrègent et Icare périt, précipité dans la mer.

Le premier vol réussi d'un appareil à moteur est attribué aux frères Wright. Leur avion, le *Flyer*, parcourut quelques centaines de mètres le 17 décembre 1903, restant en l'air moins d'une minute. L'invention de l'avion ouvre alors d'immenses possibilités : la promesse d'abolir les distances entre les continents, les pays et les hommes, facilitant les échanges commerciaux, la connaissance du monde, mais aussi la compréhension et la solidarité entre les peuples.

S'il avait fallu à l'humanité des millénaires pour réaliser le rêve d'Icare, il ne faudra qu'une dizaine d'années pour perfectionner suffisamment l'invention afin de l'utiliser à des fins militaires, ce qui causera d'incalculables souffrances humaines. Le premier bombardement aérien aurait eu lieu le 1er novembre 1911 lors de la guerre italo-turque en Tripolitaine[1]. Le 5 octobre 1914, un avion français abat un avion allemand durant le premier duel aérien de l'histoire. La combinaison de nouvelles technologies permettra bientôt de perfectionner la technique du bombardement et, dans les décennies qui suivront, des pluies de bombes incendiaires détruiront des villes entières : Guernica, Coventry, Dresde, Tokyo... Le rêve d'Icare n'est pas loin d'entraîner toute l'humanité vers sa chute quand les bombardements d'Hiroshima et de Nagasaki ouvrent l'ère nucléaire. Un peu plus d'un siècle après le décollage du *Flyer*, des drones pilotés à des milliers de kilomètres de distance délivrent leur charge mortelle en Afghanistan, au Pakistan ou au Yémen. Il devient aussi techniquement possible de leur donner la capacité de décider de manière autonome quand utiliser leurs armes.

1 Sven Lindqvist, *Une histoire du bombardement*, La Découverte, Paris, 2012, p. 14.

Il y a encore peu de temps, seulement quelques générations en arrière, un être humain pouvait espérer au cours de sa vie entière être le témoin d'un ou peut-être deux changements techniques affectant directement son quotidien. Or, les progrès scientifiques et techniques ne suivent pas une courbe linéaire mais une courbe exponentielle. Nous sommes sans doute arrivés au point où cette courbe prend l'allure d'une ligne ascendante, presque verticale. La science a chaque jour de plus en plus d'emprise sur les sociétés, même les plus éloignées des centres d'innovation. Pourtant, le constat de l'auteur de sciences fiction Isaac Asimov reste plus que jamais d'actualité : « *Le plus triste aspect de notre vie moderne c'est que la science rassemble plus vite les connaissances que la société ne rassemble la sagesse* »[2].

Les progrès scientifiques et techniques fulgurants des dernières décennies ont permis l'apparition de moyens et méthodes de guerre inédits. Certaines de ces nouvelles technologies (tels que les drones d'observation ou de combat) sont déjà utilisées, tandis que d'autres (nanotechnologies, robots de combat ou armes à laser par exemple) sont encore au stade de l'expérimentation ou du développement. Outre les espaces terrestres, maritimes et aériens, les grandes armées reconnaissent également le besoin de disposer de capacités militaires dans « l'espace cybernétique »[3].

Ces développements laissent entrevoir la possibilité d'une nouvelle rupture dans la façon de mener la guerre ou d'utiliser la force hors du cadre d'un conflit armé. En effet, certaines technologies ne constituent pas seulement un prolongement des technologies précédentes (un avion plus rapide, un explosif plus puissant) : leur apparition peut modifier profondément la manière de faire la guerre, voire même bouleverser les rapports de force sur la scène internationale. Ainsi, la maîtrise de la guerre mécanisée et la tactique de la « *blitzkrieg* » aura donné un avantage décisif à l'Allemagne au début de la Seconde Guerre mondiale.

Il est difficile de délimiter précisément les moyens et méthodes que recouvre exactement l'expression « nouvelles technologies », qui fait pourtant l'objet de débats passionnés impliquant philosophes, juristes et militaires. De même, il paraît vain de déterminer une date précise à partir de laquelle une technique peut être considérée comme « nouvelle », puisque les progrès des sciences et des techniques sont, par définition, en constante évolution. Il s'agit plutôt ici d'essayer de distinguer des tendances générales caractérisant un certain nombre d'innovations technologiques relatives à la conduite de la guerre – et à l'usage de la force de façon plus générale – ces dernières années. Qu'est-ce qui distingue les drones, les systèmes d'armement automatisés, les armes

2 Isaac Asimov et Jason A. Shulman, *Isaac Asimov's Book of Science and Nature Quotations,* Blue Cliff Editions, Weidenfeld & Nicolson, New York, 1988, p. 281.

3 Les États-Unis d'Amérique disposent d'un cyber commandement opérationnel depuis mai 2010. Voir U.S. Department of Defense, « U.S. Cyber Command Fact Sheet », U.S. Department of Defense Office of Public Affairs, 25 mai 2010, disponible sur : http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf (dernière consultation juillet 2012).

nanotechnologiques ou encore la guerre cybernétique des moyens et méthodes de guerre « traditionnels » utilisés jusqu'à maintenant ? Afin de mieux circonscrire le champ d'étude, la *Revue internationale de la Croix-Rouge* (la *Revue*) a choisi d'étudier plus particulièrement les innovations technologiques qui s'inscrivent dans une ou plusieurs des trois tendances suivantes : premièrement, la tendance à l'automatisation de systèmes d'armement (tant offensifs que défensifs) et, par conséquent, la délégation d'un nombre croissant de tâches à la machine. Deuxièmement, les progrès quant à la précision, la persistance[4] et la portée des systèmes d'armement. Troisièmement, la capacité d'utiliser de moins en moins de force physique et/ou cinétique pour des effets équivalents, voire plus importants.

Des technologies qui relevaient encore hier de la science-fiction pourraient provoquer demain des catastrophes humanitaires inédites, tels des accidents technologiques majeurs ou la paralysie des systèmes de santé ou d'approvisionnement d'un pays par la destruction des réseaux informatiques dans le cadre d'une cyber-guerre. D'autres développements récents permettraient cependant non seulement de limiter les pertes civiles mais aussi d'épargner la vie des combattants. Certaines technologies améliorent ainsi la précision des armes ou facilitent la collecte de renseignements sur la nature de la cible. En outre, l'étude des « nouvelles technologies » et de la guerre ne se limite pas aux seules applications militaires, mais recouvre aussi de nouveaux moyens mis à disposition des organisations humanitaires, des journalistes ou encore des tribunaux : les technologies de la communication et de l'information permettent ainsi d'alerter le monde sur des violations du droit, mobiliser des volontaires ou encore communiquer directement avec les victimes de conflits. Les progrès en matière de cartographie et d'imagerie satellite, ou encore d'intervention chirurgicale à distance, peuvent aussi faciliter l'action humanitaire.

Comment appréhender l'accélération des développements technologiques de la guerre ? Faut-il y voir une évolution inéluctable et simplement se préparer à gérer les conséquences de leur usage ? Le philosophe allemand Hans Jonas évoque les risques inédits posés par la physique nucléaire ou la génétique : « La pratique collective, dans laquelle nous sommes entrés avec la technologie de pointe, est encore une terre vierge de la théorie éthique... Qu'est-ce qui peut servir de boussole ? L'anticipation de la menace elle-même ![5] »

Le développement de nouveaux moyens et méthodes de guerre ne doit pas seulement s'accompagner d'une réflexion éthique. Il s'inscrit aussi dans un cadre juridique. En vertu du droit international humanitaire, les États ont en effet l'obligation de vérifier la compatibilité avec le droit international de « l'emploi d'une nouvelle arme, de nouveaux moyens ou d'une nouvelle méthode de guerre », dès les stades de « l'étude, la mise au point, l'acquisition ou

4 Par exemple, certains drones ont la capacité de demeurer plus longtemps en vol que les avions, ce qui permet la surveillance prolongée d'une zone.

5 Hans Jonas, *Le principe responsabilité : Une éthique pour la civilisation technologique*, Édition du Cerf, Paris, 1990, Préface, p. 13.

l'adoption »[6]. De nombreux moyens ou méthodes de guerre ont déjà été interdits ou leur usage réglementé au cours de l'histoire. Les armes à laser aveuglantes ont ainsi été proscrites en 1995[7], avant même leur apparition sur les champs de bataille.

Si la science permet l'automatisation d'un nombre croissant de tâches dans le cadre de la conduite des hostilités, l'évaluation de leur licéité au regard du droit international humanitaire demeure, elle, bel et bien du ressort de l'humain. Or, certaines caractéristiques de ces nouvelles technologies posent des questions totalement inédites qui rendent plus complexe l'évaluation de la licéité d'une attaque. Tout d'abord, la possibilité de voir des machines commettre des actes de violence programmés implique de déléguer notre capacité de jugement, élément essentiel dans l'attribution de la responsabilité. Ensuite, notre recours croissant (voire notre dépendance) à la technologie entraîne inéluctablement une plus grande vulnérabilité vis-à-vis des incertitudes scientifiques et des risques de dysfonctionnement d'ordre technique. Dans quelle mesure peut-on prendre en compte l'étendue – encore incertaine – des conséquences de l'utilisation d'armes nanotechnologiques ? Quel degré d'incertitude est « acceptable » juridiquement ?

Par ailleurs, le recours croissant à la technologie dans la conduite des hostilités pose des questions complexes en matière de responsabilité, compte tenu du nombre de personnes – civiles et militaires – impliquées dans le processus allant de la conception à l'utilisation de l'arme en question. À qui doit être attribuée la responsabilité d'une attaque illégale par un robot ? Comment adapter les processus d'établissement des faits à la nature de plus en plus technique de la guerre ? Un dysfonctionnement technique avéré peut-il absoudre l'opérateur de sa « faute » ? Dans ce cas, le concepteur de la machine doit-il être tenu pour responsable ?

En ouverture de cette édition, Peter Singer, expert reconnu des nouvelles technologies de la guerre et auteur de *Wired for War*[8], pose les termes du débat dans son interview. À sa suite, plusieurs experts en matière éthique, juridique, scientifique et militaire se penchent sur les développements technologiques contemporains et sur leurs conséquences, ainsi que sur les questions qu'ils soulèvent en matière d'action et de droit humanitaire. Certaines de ces contributions illustrent également des sensibilités nationales différentes et la *Revue* a notamment sollicité des perspectives chinoise et étasunienne sur la « guerre cybernétique ».

6 Article 36 du Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole additionnel I), 8 juin 1977.

7 Protocole relatif aux armes à laser aveuglantes (Protocole IV à la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination de 1980), Genève, 13 octobre 1995.

8 Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, Penguin Books, New York, 2009.

Ces contributions illustrent la profonde ambivalence de ces « nouvelles technologies » en termes d'effets sur la guerre et ses conséquences. Dans les lignes qui suivent, nous soulignons quelques-unes des principales questions et paradoxes que ces nouvelles technologies soulèvent et qui seront débattues dans cette édition de la *Revue*.

Le brouillage de la notion traditionnelle de la guerre

À l'image de nos sociétés, les guerres aussi évoluent du fait des nouvelles technologies. Pour les quelques pays qui les possèdent, la principale évolution est sans doute la possibilité de commettre des actes de guerre sans pour autant mobiliser de conscrits, occuper des territoires et conduire de vastes opérations terrestres, comme cela était le cas lors des grandes guerres du XX^{e} siècle. Certaines technologies n'en demeurent pas moins extrêmement complexes et coûteuses à développer. Encore peu de nations sont capables de maîtriser aujourd'hui leur développement et de mener des opérations à distance.

Par ailleurs, de telles méthodes de guerre ne changent pas fondamentalement la cruelle escalade de la violence qui caractérise si souvent les conflits dits « asymétriques » opposant forces conventionnelles et groupes armés non-étatiques. Si l'usage de drones commandés à des milliers de kilomètres permet d'atteindre un ennemi incapable de riposter, ce dernier choisira souvent de compenser cette impuissance en attaquant intentionnellement la population civile.

Contrairement à ce qui est souvent affirmé, loin d'être désormais inconscientes de ces guerres lointaines, les populations des pays qui mènent ce type de guerre « high-tech » sont beaucoup mieux informées qu'autrefois. Pourtant, l'ennemi lointain est souvent perçu avant tout comme un criminel et non comme un belligérant dont les droits et obligations seraient régis par le droit humanitaire.

Il est possible que certaines nouvelles technologies (comme les drones, par exemple) rendent l'usage de la force sur le territoire d'États non-belligérants moins problématique, en rendant les questions de protection des forces militaires sans objet, éliminant ainsi les mesures de dissuasion traditionnelles à l'attaque de l'ennemi hors de la zone de combat. Cet obstacle à l'entrée perçu comme plus faible pourrait créer l'impression que le champ de bataille est « global ». Il est essentiel de rappeler que les attaques menées à l'aide de drones en dehors d'une situation de conflit armé ne sont pas régies par le droit humanitaire (qui permet l'usage de la force létale contre les combattants, tout du moins sous certaines conditions), mais par le droit international des droits de l'homme (qui limite beaucoup plus strictement les instances où l'usage de la force létale est autorisé).

Les effets entraînés par certaines nouvelles technologies devraient engendrer une réflexion sur ce que l'on entend par « usage de la force armée » comme seuil d'application du droit humanitaire (*jus in bello*), notamment dans

le contexte d'une cyber-attaque[9]. Il en va de même de la notion « d'acte d'agression », qui déclenche le droit de légitime défense conformément à la Charte des Nations Unies (*jus ad bellum*). Les coups bas et les cyber-attaques auxquels se livrent les États semblent correspondre davantage au sabotage ou à l'espionnage qu'aux conflits armés. Dès lors, les règles régissant (d'ailleurs peu et mal) l'espionnage et autres actes hostiles sous le seuil d'application du droit international humanitaire ne seraient-elles pas plus appropriées dans de telles situations ?

Les conflits récents montrent clairement que le déploiement de troupes et de moyens militaires conséquents reste essentiel quand l'objectif d'une opération est de contrôler le territoire. Toutefois, certaines nouvelles technologies permettent à ceux qui les maîtrisent de frapper leur ennemi avec des effets destructeurs considérables – tant dans le monde réel que virtuel – sans pour autant déployer de troupes. Une cyber-attaque n'implique pas l'invasion du territoire de l'adversaire mais, si l'on veut, de son espace virtuel. Autant de concepts et d'images de la guerre « traditionnelle » qui sont à repenser, pour éviter un brouillage des catégories juridiques existantes de conflits armés (internationaux et non-internationaux) au risque d'un affaiblissement de la protection que le droit humanitaire accorde aux victimes.

Portée, précision et distance morale

Si l'augmentation de la portée d'une arme a longtemps été faite au détriment de sa précision, l'usage de drones, de robots armés ou de la cybernétique permet aujourd'hui de réconcilier ces deux caractéristiques. L'augmentation de la portée de certaines armes nouvelles évite d'exposer directement les troupes au feu de l'adversaire. La précision des armes permet surtout de diminuer les charges nécessaires à la destruction de l'objectif militaire et de minimiser les dommages collatéraux. Ceci dit, elles requièrent souvent une grande précision du renseignement, qu'il est difficile de collecter à distance.

Ainsi, le recours aux drones ou aux robots se révèle particulièrement adapté à l'usage de la force par les pays soucieux d'épargner la vie de leurs soldats. En outre, maintenir les opérateurs de ces nouvelles armes éloignés du champ de bataille, dans un environnement familier, diminuerait de façon non négligeable leur exposition au stress ou à la peur, et réduirait ainsi les erreurs liées à des facteurs émotionnels. En revanche, l'augmentation de la distance physique entre la localisation de l'opérateur et sa cible augmenterait du même coup la distance morale entre parties au conflit. Ainsi, la multiplication des attaques conduites depuis des drones pilotés à distance alimente un débat sur la soi-disant « PlayStation mentality[10] » qui affecterait le jugement moral des

9 Voir l'article de Cordula Droege dans cette édition.

10 Le problème de la « PlayStation mentality » est décrit ainsi par Philip Alston : « Les jeunes militaires élevés aux jeux vidéo vont désormais tuer de vraies personnes à distance en usant un joystick.

opérateurs de drones et aggraverait le phénomène criminogène de « déshumanisation » de l'ennemi en temps de guerre. L'existence d'un tel phénomène est néanmoins contestée. Les opérateurs de drones pourraient être en fait davantage exposés moralement que les artilleurs ou les pilotes de bombardiers du fait de l'observation prolongée de leurs cibles et des dommages causés par les attaques.

Cela soulève aussi la question de la vision que se forment les joueurs de jeux vidéo de la réalité des guerres modernes : le plus souvent celle d'un monde sans loi où tous les coups sont permis pour vaincre l'ennemi. En collaboration avec plusieurs sociétés nationales de Croix-Rouge, le CICR a initié un dialogue avec les joueurs, les concepteurs et les producteurs de jeux vidéo, afin de produire des jeux qui intègrent le droit applicable en temps de conflit armé, offrant aux joueurs les mêmes dilemmes que ceux posés aux combattants sur les champs de bataille contemporains.

Certains observateurs voient dans le développement de systèmes d'armement autonomes la possibilité de mieux faire respecter le droit international humanitaire sur le champ de bataille. Un robot ne connaît ni la fatigue ni le stress, ni les préjugés ou la haine, autant de causes de crimes en temps de conflit. Toutefois, pour l'heure, il semble extrêmement difficile d'un point de vue technique de doter ces armes d'une capacité de distinction. Comme le relève Peter Singer dans la présente édition : « *A computer looks at an 80 year old woman in a wheelchair the exact same way it looks at a T-80 tank. They are both just zeros and ones* »[11]. Si les systèmes d'armement entièrement autonomes ne sont pas actuellement utilisés, certains commentateurs appellent dès à présent à une interdiction totale des armes autonomes[12]. Le CICR souligne pour sa part que le déploiement de tels systèmes « soulèverait tout un ensemble de problèmes fondamentaux du point de vue juridique, éthique et social, qui doivent être pris en compte avant que ces systèmes soient développés ou déployés »[13]. Jusqu'à quel point l'homme peut-il être sorti de la boucle du processus de décision d'utiliser ou non la force létale ?

Éloignés des conséquences humaines de leurs actions, quelle valeur cette génération de combattants donnera-t-elle au droit à la vie ? Comment les commandants et les hommes politiques resteront-ils à l'abri de la nature antiseptique des attaques létales par drones ? Tuer sera-t-il une option plus attractive que capturer ? Les standards de collecte de renseignements justifieront-ils une fiche de meurtres ? Le nombre de morts civiles collatérales acceptables augmentera-t-il ? ».Voir Philip Alston et Hina Shamsi, « A Killer above the law », dans *The Guardian*, 2 août 2010.

11 « Un ordinateur porte sur une femme de 80 ans dans une chaise roulante exactement le même regard que sur un char T-80. L'une et l'autre ne sont que des zéros et des uns. » (traduction CICR). Voir «Interview de Peter W. Singer», dans cette édition.

12 Voir l'article de Peter Asaro dans cette édition, ainsi que Noel Sharkey, « The evitability of autonomous robot warfare », dans *International Review of the Red Cross*, Vol. 94, N° 886, 2012, pp. 787-799.

13 CICR, « Le droit international humanitaire et les défis posés par les conflits armés contemporains », Rapport de la XXXIe Conférence de la Croix-Rouge et du Croissant-Rouge, Genève, 28 novembre – 1er décembre 2011, p. 45, disponible sur : http://www.rcrcconference.org/docs_upl/fr/31-int-conference-ihl-challenges-report-11-5-1-2-fr.pdf (dernière consultation juillet 2012).

Le dommage

Les progrès réalisés en termes de précision du ciblage sont à mettre en parallèle avec une tendance inverse, à savoir la difficulté de limiter dans le temps et l'espace les effets de certaines nouvelles armes. Cette tendance n'est certes pas nouvelle : on connaît par exemple les effets indiscriminés de l'arme atomique, qui s'étendent bien au-delà du point d'impact. Mais l'introduction de nanotechnologies dans les systèmes d'armement ou le recours à des attaques cybernétiques relancent ces questions. Comment prendre en compte dans le calcul de proportionnalité les effets dans le temps et l'espace de l'utilisation de nanotechnologies alors que ceux-ci demeurent encore largement inconnus ? À partir de quel degré d'incertitude scientifique peut-on considérer qu'une utilisation de ces matériaux serait contraire au principe de précaution ? Peut-on mesurer l'impact qu'une attaque lancée dans le monde virtuel peut avoir sur le monde réel ? En effet, compte tenu de toutes ces inconnues, les incidences auxquelles on ne pouvait pas « s'attendre[14] » deviennent de plus en plus nombreuses.

Par ailleurs, certains nouveaux moyens ou méthodes de guerre, tels que les armes à micro-ondes ou les cyber-attaques, visent souvent à la destruction d'informations. Les informations devraient-elles être à présent considérées comme un « bien civil » au sens du droit international humanitaire et leur destruction comme un dommage à un bien civil ? Aujourd'hui, en effet, seuls les dégâts physiques sont pris en compte dans la définition du dommage subi. Dans un monde de plus en plus dépendant de l'information, la destruction des données bancaires ou médicales des citoyens d'un pays aurait des conséquences dramatiques, ce qui appelle pour certains à une redéfinition de la notion de bien civil protégé. La position du CICR dans cette discussion se veut claire et pragmatique : « Si les moyens et les méthodes de la cyber-guerre produisent les mêmes effets dans le monde réel que les armes conventionnelles (destruction, perturbation, dégâts/dommages, blessés, morts), ils doivent être gouvernés par les mêmes règles que les armes conventionnelles »[15].

L'information et la transparence

Les innovations technologiques que nous observons ces dernières décennies semblent pointer vers deux conclusions contraires en matière d'accès à l'information et de transparence. D'un côté, il règne encore une certaine opacité

14 Ainsi, selon les articles 51(5)(b) et 57(2)(a)(iii) du Protocole additionnel I de 1977, une attaque indiscriminée est « une attaque dont on peut *attendre* qu'elle cause 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 » (nous soulignons).

15 Cordula Droege, CICR, citée par Pierre Alonso dans « Dans cyberguerre il y a guerre », *OWNI*, 29 novembre 2012, disponible sur : http://owni.fr/2012/11/29/dans-cyberguerre-il-y-a-guerre/ (dernière consultation novembre 2012).

sur les conséquences humanitaires réelles ou possibles de l'usage de certaines « nouvelles armes ». Si elles sont déployées dans le cadre d'opérations secrètes, le public n'aura que peu connaissance de l'impact de ces armes.

D'un autre côté, l'usage de nouvelles technologies permet de filmer ou d'enregistrer les opérations militaires et de révéler de possibles crimes de guerre. Cela peut être le fait des armées elles-mêmes (notamment dans le but d'assurer un « *rapport après action* ») ou des organisations internationales et des organisations non-gouvernementales. Par exemple, l'utilisation de l'imagerie satellite a déjà permis d'enquêter sur de possibles violations du droit dans le contexte de la bande de Gaza, de la Géorgie, du Soudan ou du Sri Lanka par exemple[16]. Ces dernières années, de nombreux crimes ont été aussi dévoilés dans des vidéos prises par les soldats eux-mêmes !

Finalement, le progrès technique a toujours permis des améliorations en matière médicale et humanitaire. Aujourd'hui l'utilisation de nouvelles technologies de communication ou de géolocalisation peuvent permettre de faciliter l'identification des besoins, le rétablissement des liens familiaux après une crise ou encore de suivre à la trace les déplacements de populations dans les régions les plus reculées[17].

Nos responsabilités

Si la technologie permet à l'homme de déléguer un certain nombre de tâches et même parfois de lui éviter de faire des erreurs, elle ne l'autorise en rien à déléguer sa responsabilité morale et légale de respecter les règles de droit applicable. L'utilisation de nouvelles technologies dans la conduite de la guerre peut toutefois rendre plus complexe l'attribution de la responsabilité en cas de violations du droit international humanitaire et ce, pour deux raisons. Premièrement, certaines nouvelles technologies s'accompagnent de difficultés d'ordre technique pour identifier les responsables. Le meilleur exemple de la complexification du processus d'identification et des compétences de plus en plus techniques qu'il requiert est certainement le recours à la cyber guerre. Une des caractéristiques des attaques dans le cyber espace est en effet leur caractère anonyme et la difficulté d'en localiser l'origine. De même, l'automatisation de certaines séquences de tirs de missiles dirigées par des ordinateurs affaiblit la notion de responsabilité. Deuxièmement, la délégation de certaines tâches militaires à des machines « intelligentes » a pour effet d'augmenter le nombre de personnes potentiellement impliquées dans le processus de réalisation, acquisition et utilisation de la machine, complexifiant ainsi la chaîne de responsabilité. En élargissant notre point de vue au-delà du seul champ

16 Voir l'article de Joshua Lyons dans cette édition.

17 Voir par exemple l'article de Patrick Meier, « Les nouvelles technologies de l'information et leur impact sur le secteur humanitaire », dans *Revue internationale de la Croix-Rouge*, Vol. 93, *Sélection française 2011/3*, pp. 225-254.

d'application du droit en temps de conflit, la responsabilité ne serait donc pas seulement à chercher du côté de la chaîne de commandement militaire ou des combattants qui utilisent ou utiliseront ces armes sur le champ de bataille. La responsabilité est aussi celle des scientifiques et des constructeurs qui développent ces nouvelles technologies, ainsi que des autorités politiques et des entreprises qui les commanditent.

Les États ont l'obligation de faire en sorte que l'emploi de nouvelles armes et de nouveaux moyens ou méthodes de guerre soit conforme aux règles du droit humanitaire. Toutefois, la société civile a aussi un rôle important à jouer. En effet, en informant sur les conséquences humanitaires des armes et en suscitant un débat autour de leur licéité, elle participe à la formation d'une véritable « conscience publique » internationale telle que mentionnée dans la « clause de Martens » :

> « Dans les cas non prévus par le présent Protocole ou par d'autres accords internationaux, les personnes civiles et les combattants restent sous la sauvegarde et sous l'empire des principes du droit des gens, tels qu'ils résultent des usages établis, des principes de l'humanité et des exigences de la conscience publique »[18].

La Cour internationale de Justice a d'ailleurs insisté sur l'importance de cette clause dans le cadre de son avis consultatif sur la *Licéité de la menace ou de l'emploi d'armes nucléaires*[19].

Depuis de nombreuses années, le CICR, rejoint aujourd'hui par de nombreuses organisations non-gouvernementales, contribue à l'émergence de cette « conscience publique ». Face à l'évolution constante et rapide des armes, le CICR a ainsi publié un *Guide relatif à l'examen de la licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre*[20] et contribue activement au développement de nouvelles règles internationales encadrant l'emploi des armes. Le dernier exemple de traité en date est la Convention sur les armes à sous-munitions du 30 mai 2008.

***

18 Art. 1(2) du Protocole additionnel I de 1977. Voir aussi le préambule de la Convention (IV) de La Haye de 1907 concernant les lois et coutumes de la guerre sur terre, et le préambule de la Convention (II) de La Haye de 1899.

19 La Cour internationale de Justice (CIJ) a estimé que la clause de Martens « continue indubitablement d'exister et d'être applicable » (para. 87) et qu'elle s'était « révélée être un moyen efficace pour faire face à l'évolution rapide des techniques militaires » (para. 78). La CIJ a également rappelé que la clause de Martens représente « l'expression du droit coutumier préexistant » (para. 84). Voir CIJ, *Licéité de la menace ou de l'emploi d'armes nucléaires*, Avis consultatif, La Haye, 8 juillet 1996.

20 CICR, *Guide de l'examen de la licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre*, CICR, Genève, 2007, disponible sur : http://www.icrc.org/fre/resources/documents/publication/p0902.htm (dernière consultation juillet 2012). Voir aussi Kathleen Lawand, « Reviewing the legality of new weapons, means and methods of warfare », dans *International Review of the Red Cross*, Vol. 88, N° 864, 2006, pp. 925-930.

REVUE INTERNATIONALE de la Croix-Rouge

« La Science trouve, l'Industrie applique, l'Homme s'adapte » : contrairement à ce qu'affirmait le slogan de l'Exposition Universelle de Chicago en 1933, nous ne sommes pas condamnés à subir le développement technologique en témoins impuissants. L'évolution scientifique et technologique ne signifie pas forcément « progrès » et la décision de donner à l'invention une application militaire doit donner lieu à une étude en profondeur de la mesure, y compris les conséquences positives et négatives résultant d'une exploitation de cette invention. De même, chaque décision de produire, acheter et enfin utiliser telle ou telle innovation technologique à des fins militaires est une responsabilité politique et sociétale d'autant plus importante qu'elle aura des répercussions directes sur des vies humaines. Les conséquences humanitaires des conflits armés ne sont pas virtuelles. Le débat au sein de la société civile et dans les communautés scientifique, militaire et politique que l'utilisation de certaines nouvelles technologies à des fins militaires suscite devrait être considéré comme un développement positif : cela témoigne de ce questionnement sur la compatibilité de ces nouvelles armes avec nos principes légaux et moraux.

De même que les frères Wright n'entrevoyaient sans doute pas encore tout le potentiel de l'avion, les possibilités militaires qu'offriraient bientôt les nouvelles technologies – et des combinaisons inédites de nouvelles technologies – sont encore largement inconnues. Toutefois, il est essentiel d'anticiper les conséquences humanitaires que leur usage pourrait entraîner. Le Comité international de la Croix-Rouge, présent dans les conflits du monde depuis un siècle et demi, peut malheureusement en témoigner : contrairement aux illusions d'un « progrès » sans fin que nourrissaient les hommes au début du XX^{e} siècle, l'histoire a démontré que la science ne peut pas être placée *au-dessus* de ses conséquences.

Vincent Bernard
Rédacteur en chef

REVUE INTERNATIONALE

Interview de Peter W. Singer*

Directeur de la 21st Century Defense Initiative, Brookings Institution

Peter W. Singer est directeur de la 21st Century Defense Initiative *à Brookings Institution, basée à Washington, D.C. Il est l'auteur de trois ouvrages récompensés par des prix, Corporate Warriors:* The Rise of the Privatized Military Industry, Children at War, *et* Wired for War: The Robotics Revolution and Conflict in the 21st Century[1]. *Il a été consultant auprès d'institutions aussi diverses que l'armée des États-Unis, le FBI et des organisations de défense des droits de l'homme.*

Dans cet entretien, Peter Singer explique dans quelle mesure et de quelle manière les nouvelles technologies changent notre façon de concevoir et de mener la guerre, ainsi que les effets qu'elles auront sur le travail des acteurs humanitaires. Il expose sa vision pour l'avenir, en analysant les défis éthiques et juridiques que pose l'accès à de nouvelles technologies avancées, ainsi que les opportunités qu'elles offrent.

: : : : : : : :

Parlez-nous un peu de votre parcours personnel. Comment et pourquoi en êtes-vous arrivé à travailler sur ce sujet ?

Comme je l'écris en introduction de mon livre *Wired for War*, lorsque je repense à mon enfance, mes jeux mélangeaient bribes et fragments de l'histoire militaire de ma famille et science-fiction. Comme beaucoup d'autres petits garçons, quand je ramassais un bâton, il se transformait en quelques secondes

* Cette interview a été réalisée à Washington D.C le 29 avril 2012 par Vincent Bernard, rédacteur en chef de la *Revue internationale de la Croix-Rouge*, Mariya Nikolova, assistante de rédaction, et Mark Silverman, chargé des affaires publiques et des relations avec le Congrès à la délégation du CICR à Washington. La version originale en anglais est publiée dans *International Review of the Red Cross*, Vol. 94, N° 886, été 2012, pp. 467-481.

en un fusil mitrailleur avec lequel j'allais défendre le quartier contre les nazis ou en un sabre laser avec lequel j'allais vaincre Dark Vador. Je me souviens que je prenais les vieilles médailles de mon grand-père pour les épingler sur mon pyjama, ou un modèle du jet que mon oncle avait piloté au Viet Nam et que je m'en servais pour protéger mes constructions de Lego. Et puis, comme pour beaucoup d'autres gosses, ces souvenirs sont peuplés d'artefacts de science-fiction : oui, il se peut que j'aie porté sur ma veste de pyjama les médailles remportées par mon grand-père pendant la Seconde Guerre mondiale, mais quand je sautais dans mon lit, c'était dans les draps de la Guerre des étoiles que je m'enfilais.

Dans son livre *Six armées en Normandie*[2], l'écrivain John Keegan écrit en substance : « J'ai grandi dans ce climat d'histoire militaire et de guerre, ce n'est pas de bon ton de le dire mais c'est la réalité ». Je pense qu'il y a quelque chose comme cela chez moi. Mais soyons clair. Les contacts que j'ai eus plus tard avec le côté bien réel de la guerre m'ont amené à réajuster ma vision des choses. Je me souviens d'être allé en Bosnie comme membre d'une équipe de chercheurs des Nations Unies, d'être arrivé à Mostar et d'avoir eu l'impression que les images des vieux livres de mon grand-père prenaient vie. Cependant, les vieilles photos du livre de mon grand-père ne restituaient pas l'odeur, les sentiments et les émotions qui sont dans l'air quand on est dans une guerre bien réelle... Quand on lit un livre, on n'a pas besoin de se demander où poser le pied la prochaine fois pour éviter les mines terrestres, ni d'essayer de passer là où passent les locaux pour ne pas marcher sur l'une d'elles.

Ce que je veux dire, c'est que j'ai été formé par l'imaginaire historique de la guerre dans lequel j'ai grandi, comme beaucoup d'autres, et qui a été plus tard tempéré par les expériences faites dans le monde réel. L'autre élément formateur vient de ce que je suis un universitaire travaillant sur des questions de politique publique, et j'ai toujours été frappé par le hiatus qui existe entre la façon dont nous pensons que le monde fonctionne et son mode de fonctionnement réel. C'est une constante dans mes recherches.

Par exemple, quand j'étais en Bosnie, je suis tombé sur une société américaine qui travaillait comme entreprise militaire privée. Cette notion n'existait pas alors dans nos études de la guerre et de la politique, et pourtant cette société existait bel et bien. Lorsque j'ai proposé de faire une thèse sur ce sujet, un professeur à Harvard m'a dit que pour imaginer de faire des recherches sur une idée aussi sotte, je ferais mieux de quitter l'université et de devenir scénariste. Cette thèse est finalement devenue mon livre *Corporate Warriors* (Sous-traitants de la guerre) et, dans l'intervalle, nous avons vu tous les problèmes que posait la présence d'acteurs non étatiques (d'entreprises) sur le champ de bataille.

1 Voir Peter W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry*, édition mise à jour, Cornell University Press, New York, 2007; *Children at War*, University of California Press, Berkeley C.A., 2006; et *Wired for War: The Robotics Revolution and Conflict in the 21st Century*, Penguin Books, New York, 2009.

2 Voir John Keegan, *Six armées en Normandie. Du jour J à la libération de Paris, 6 juin-25 août 1944*, Albin Michel, Paris, 2004.

De même, alors que je faisais des recherches sur les armées privées, j'en suis venu à étudier le cas de l'Afrique de l'Ouest, où l'on a assisté à un type de guerre que personne n'imaginait devoir exister. D'un côté, il y avait un gouvernement qui engageait une société privée pour qu'elle lui serve d'armée et, de l'autre, une société combattant une force rebelle essentiellement composée d'enfants enlevés. Aucun de ces deux aspects ne cadrait avec le schéma de pensée que nous appliquions à la guerre, et pourtant ils existaient bel et bien. Ce fut la genèse de mon livre suivant, *Children at War* (Enfants en guerre). Cette fois encore, je me suis heurté à un professeur qui m'a dit qu'elle ne croyait pas à l'existence d'enfants soldats. Aujourd'hui, bien sûr, cette réaction paraît stupide, mais on pensait de cette manière au début des années 90.

Mon dernier livre a enchaîné sur cette idée d'étudier de nouveaux acteurs, mais a essayé aussi d'ouvrir les yeux des gens. J'y examine la robotique et les répercussions très réelles qu'elle a eues sur les combats et, au-delà du champ de bataille, sur les questions politiques et éthiques. D'ores et déjà, les expériences faites avec ce livre ressemblent fort à celles que j'ai faites avec la thèse et le premier livre. À la fois les hauts gradés de la défense qui ne savaient pas que leurs militaires utilisaient cette technologie, *et* les organisations humanitaires qui continuent à la considérer comme une technologie de science-fiction ont une réaction qui semble « trop faible et trop tardive ».

Qu'est-ce que ces nouvelles technologies apportent sur le champ de bataille ? En quoi la robotique change-t-elle notre façon de percevoir la guerre aujourd'hui ?

Il y a cette idée – parfois au sein même des services de défense – qu'il s'agit d'une « technologie révolutionnaire » et l'on se méprend fréquemment sur le sens de l'adjectif. Une technologie révolutionnaire est une technologie qui change la donne au point de provoquer une rupture dans l'histoire. Comme la poudre, la machine à vapeur ou la bombe atomique.

Je vais exprimer clairement ma pensée : ces technologies ne règlent pas tous les problèmes de la guerre. On en discute trop souvent comme s'il s'agissait de solutions miracles. Donald Rumsfeld, par exemple, disait à propos de la technologie des réseaux informatiques qu'elle pourrait « dissiper le brouillard de la guerre ». Les nouvelles technologies sont souvent décrites de la même manière dans les milieux humanitaires, comme si elles pouvaient rendre la guerre moins dangereuse et plus propre. Il n'y a là rien de nouveau. Le poète John Donne prédisait en 1621 qu'avec les canons les guerres « arriveraient à leurs fins plus vite que par le passé et l'on éviterait les grandes effusions de sang[3] ». Nous avons vu qu'en se perfectionnant les canons ne rendaient pas les guerres moins meurtrières ni moins coûteuses. Et cette manière de penser persiste jusqu'à nos jours : beaucoup parlent des robots comme s'ils allaient résoudre les problèmes éthiques de la guerre.

3 John Donne, Sermon CXVII, prononcé à la cathédrale St. Paul le jour de Noël 1621, Jean i.8.

Les technologies révolutionnaires changent la donne – non pas parce qu'elles résolvent tous les problèmes – mais parce qu'elles nous obligent à nous poser des questions qui étaient inimaginables à l'échelle de l'individu, de l'organisation ou de la nation, une génération plus tôt. Certaines de ces questions touchent à ce qui était possible il y a une génération, par rapport à ce qui est possible aujourd'hui.

Tout récemment, je discutais avec un général de division de la capacité que l'on a aujourd'hui d'observer de près ce qui se passe sur le théâtre des opérations, mais grâce à un avion qui a décollé à quelque 11 000 kilomètres de là. Il n'imaginait pas avoir de telles capacités lorsqu'il était jeune officier et maintenant il commande toute une division grâce à cette capacité. Nous constatons que cela ouvre de nouvelles possibilités aux acteurs humanitaires, que des organisations non gouvernementales (ONG) pourraient avoir cette même capacité d'observer et d'établir l'existence de crimes, sans avoir à exposer qui que ce soit au danger.

Les technologies révolutionnaires amènent cependant aussi à s'interroger sur ce qui est juste et à se poser des questions auparavant inconcevables, des questions sur le bien et le mal jamais explorées dans le passé. Un général aujourd'hui peut être en mesure d'observer ce qui se passe sur le champ de bataille situé à 11 000 kilomètres de là, mais quelle incidence cela a-t-il sur la structure de son unité, sa tactique, sa doctrine, les cas et les lieux où il emploie la force, les règles qu'il applique dans telle ou telle situation ? De même, si le fait pour une organisation humanitaire de pouvoir observer à distance les atrocités commises sur un champ de bataille peut être un atout certain, cette capacité soulève également de multiples questions, par exemple sur le devoir d'action incombant à ceux qui observent, ou sur la question de savoir si la notion de guerre « sans pertes » s'applique aussi *mutatis mutandis* aux opérations humanitaires, et si la possibilité offerte de réduire les risques pour les travailleurs humanitaires en regardant simplement de loin ne va pas de pair avec une certaine dévalorisation de la vie de ceux qui se trouvent au sol.

C'est pourquoi je suis d'avis que certaines technologies changent la donne et la robotique entre dans cette catégorie. Lorsque je suis allé interroger des gens sur le terrain pour savoir à quelles avancées historiques leur faisait penser la robotique aujourd'hui, leurs réponses ont été révélatrices. Les ingénieurs m'ont répondu que les systèmes sans pilote, ou la robotique, leur rappelaient la voiture sans chevaux de 1910. Même les termes employés pour les décrire – voiture « sans chevaux » et systèmes « sans pilote » – démontrent que nous nous plaisons encore à essayer d'appréhender quelque chose par ce qu'il n'est *pas*, plutôt que par ce qu'il est. Si l'on choisit d'établir un parallèle entre la voiture « sans chevaux » et la robotique, on peut voir aussi quelles répercussions la robotique peut finir par avoir sur notre société, la conduite de la guerre et les questions de droit. Il n'y avait pas de « code de la route » par exemple avant la voiture sans chevaux.

D'autres – comme Bill Gates, le fondateur de Microsoft, par exemple – établissent un parallèle avec l'ordinateur de 1980. L'ordinateur à cette époque était un énorme engin encombrant qui ne pouvait remplir qu'un ensemble limité

de fonctions. Il a été mis au point par l'armée, qui était le principal client sur le marché et le principal chercheur dans ce domaine. Aujourd'hui les ordinateurs sont partout, à telle enseigne qu'on ne les appelle même plus des ordinateurs. Je conduis une voiture qui en compte plus d'une centaine. Là encore, si l'on choisit d'établir ce parallèle, il faut prendre en compte toutes les conséquences qu'a eues l'entrée dans l'ère de l'informatique. Qui, en 1980, aurait imaginé qu'un ordinateur pourrait donner lieu à des choses telles que la cyberguerre ou à de graves atteintes à la vie privée ?

Le dernier parallèle, qui inquiète certains savants, est avec la bombe atomique des années 1940. Le parallèle, disent-ils, tient au fait que, comme la physique nucléaire dans les années 1940, la robotique et l'intelligence artificielle sont aujourd'hui tellement à la pointe du progrès qu'elles attirent les cerveaux les plus brillants. Quand on voulait travailler comme scientifique sur ce qui était important dans les années 1940, on se dirigeait vers la physique nucléaire. De nos jours, on se dirige vers la robotique et l'intelligence artificielle. Mais les scientifiques, comme d'autres, s'inquiètent aussi de ce que tout cela signifie.

Les scientifiques d'aujourd'hui craignent de voir se reproduire ce qui s'est passé avec les cerveaux qui étaient derrière le *projet Manhattan*[4] et qui, après avoir créé cette technologie (la bombe atomique) qui a changé la donne, ont été dépassés par leur invention. Paradoxalement, beaucoup de ceux qui ont construit la bombe atomique ont été plus tard les fondateurs du mouvement moderne de limitation des armements. Mais le génie était déjà sorti de la boîte. Il y a des parallèles évidents à faire ici avec la robotique. Seulement, dans ce cas, le génie pourrait littéralement s'échapper tout seul de la boîte.

Vous écrivez dans votre livre que, malgré tout, ce sont encore des humains qui font la guerre pour le compte d'autres humains. La guerre est encore synonyme de souffrances humaines, de pertes de vies humaines et de conséquences pour les êtres humains. Qu'est-ce que la robotique va changer à la manière de partir en guerre et à la conduite de la guerre ?

La robotique a une incidence sur la psychologie et les aspects politiques de la guerre. Mais quelle que soit la technologie employée, la guerre est une entreprise humaine. Et c'est toujours vrai aujourd'hui, même avec cette technologie avancée. La technologie influe sur le regard que nous, le public, et surtout nos dirigeants portons sur la guerre et sur notre manière de l'interpréter, de décider quand elle se justifie et quand elle ne se justifie pas, et d'en évaluer les coûts, probables ou réels.

Cette incidence, à mon avis, c'est dans le rapport entre la technologie de la robotique, les démocraties et la guerre que nous la voyons le plus aujourd'hui. La plupart des démocraties ne connaissent plus la conscription. On n'a plus

4 Note du rédacteur : le « projet Manhattan » est le nom de code d'un projet secret de recherche-développement du gouvernement des États-Unis qui a mis au point la première bombe atomique pendant la Seconde Guerre mondiale.

de déclaration de guerre. La dernière fois que le Congrès des États-Unis, par exemple, a officiellement déclaré la guerre, c'était en 1942, contre les puissances mineures de l'Axe. Nous n'achetons plus de titres d'emprunt de guerre, nous ne payons plus d'impôts de guerre non plus. Pendant la Seconde Guerre mondiale, par exemple, les habitants des États-Unis ont acheté à titre individuel, autrement dit investi personnellement plus de 180 milliards de dollars en obligations de guerre. En fait, on s'investissait tellement dans l'effort de guerre que si l'on réunissait plus de 200 000 dollars, on pouvait choisir le nom de son navire. Au cours des dix dernières années de guerre, en revanche, les citoyens américains ont acheté pour zéro dollar d'obligations de guerre et, au lieu de payer un impôt de guerre, les 4 % les plus riches ont obtenu des allègements fiscaux. Et nous avons maintenant une technologie qui nous permet de mener des opérations que nous assimilions par le passé à des actes de guerre, sans avoir à nous préoccuper des conséquences politiques que peut avoir le fait d'envoyer nos fils et nos filles risquer leur vie au loin.

On constatait déjà un abaissement des obstacles à la guerre dans nos sociétés avant l'arrivée de cette technologie. Celle-ci pourrait bien, cependant, les réduire à néant. Ce n'est pas juste une notion de théorie politique. Cela tient à nos idéaux les plus anciens sur les démocraties, jugées préférables, plus honorables, plus réfléchies face à la guerre. Cela tient au rapport entre le public et ses guerres. On s'en aperçoit dans diverses opérations aujourd'hui même. Il y a eu par exemple plus de 350 frappes aériennes effectuées à l'intérieur du Pakistan qui n'ont pas été votées par le Congrès. Ces frappes n'ont pas été effectuées par l'armée américaine, mais par des opérations secrètes des services de renseignement, et n'ont pas le degré de transparence qu'aurait une action militaire. Ainsi, on peut mener une opération d'une échelle environ huit fois supérieure à celle du début des hostilités au Kosovo, sans que personne ne la conçoive comme « guerre ». Ne vous méprenez pas : en fait, j'approuve le but de beaucoup de ces opérations. Mais je m'inquiète des effets de la technologie sur notre façon de parler de la guerre et, partant, de la conceptualiser et de l'autoriser.

On constate également aujourd'hui que cette tendance – et à mon avis, cela change vraiment la donne – a aussi une incidence sur les opérations militaires menées au grand jour. La campagne de Libye en est une formidable illustration. Aux États-Unis, l'autorisation dont avait besoin l'armée pour employer la force au grand jour était régie par la loi sur les pouvoirs de guerre (*War Powers Resolution*), qui reconnaît qu'il y a parfois des situations d'urgence dans lesquelles le Président doit être en mesure de déployer des forces, mais qui ajoute qu'il doit obtenir dans les 60 jours l'approbation du Congrès. C'est une loi postérieure à la guerre du Viet Nam, conçue pour que des incidents tels que ceux du golfe du Tonkin ne se reproduisent plus. Pourtant, lorsque les 60 jours se sont écoulés, l'exécutif a tenu le raisonnement suivant : « Nous n'avons pas besoin d'autorisation parce que cela n'implique plus de risque pour les soldats américains, ni même de menace de risque ». En gros, l'argument était le suivant : nous n'avons plus de personnel en danger, donc nous n'avons plus besoin d'observer les dispositions de cette loi.

Pourtant, des actes que nous étions accoutumés à considérer comme des actes de guerre se poursuivaient. Nous continuions à faire sauter des ouvrages et des gens. À ce stade de l'opération, on s'était mis à utiliser des systèmes sans pilote et, passé ce délai de 60 jours, 146 frappes aériennes ont été effectuées avec des systèmes de classe Predator/Reaper, la toute dernière ayant eu raison de Kadhafi. Là encore, qu'il n'y ait pas de malentendu : j'ai approuvé cette opération, je n'avais aucune sympathie pour Kadhafi. Ce qui me gêne, c'est que, alors que notre intention était de faire ce que traditionnellement nous aurions appelé une « guerre », les trois pouvoirs et, au-delà, les médias et le public en avaient une perception tout autre. Nous créons des précédents lourds de conséquences sans nous demander où cela va nous mener à l'avenir.

En d'autres termes, nous estimons ne pas avoir à suivre les anciennes procédures d'autorisation parce que nous disposons maintenant de cette nouvelle technologie. Cela change notre façon de concevoir la guerre. En démocratie, la guerre signifiait naguère des gens exposés au danger, et des blessés et des morts sur le champ de bataille. La technologie nous permet maintenant de dissocier la guerre de ses conséquences, ou du moins nous amène à penser que l'on peut séparer les deux, ce qui change notre façon de délibérer de la guerre.

Cela ne s'applique pas seulement aux systèmes sans pilote et à la robotique. Cela vaut aussi pour nombre d'autres technologies nouvelles. Les cybertechniques en sont une bonne illustration. Les militaires peuvent entreprendre des opérations qui auraient pu être interprétées dans le passé comme des actes de guerre, mais qu'ils ne considèrent pas comme tels, soit parce qu'elles n'exposent personne au danger, soit parce qu'elles se déroulent trop vite – ou trop lentement, si l'on pense à certains types de sabotage informatique – pour cadrer avec notre conception traditionnelle de la guerre.

Vos propos s'appliquent-ils aussi à la manière dont des acteurs armés non étatiques font la guerre aujourd'hui ? D'un côté, on peut dire que peu d'acteurs armés non étatiques ont aujourd'hui suffisamment de ressources pour déployer des drones et lancer plus de 300 attaques sur plusieurs mois. De l'autre, on peut dire aussi que la prolifération des nouvelles technologies est en train de « démocratiser » la guerre en mettant des armes à la disposition de chacun. Quelles tendances voyez-vous se dessiner pour l'avenir ?

Premièrement, nous assistons certainement à un abaissement des obstacles à la guerre, pas seulement pour les États, mais pour des acteurs très divers. Ce n'est pas le cas seulement pour les technologies les plus perfectionnées. L'AK-47 en est un bon exemple – une technologie relativement simple peut être une avancée énorme en ce sens qu'un enfant soldat utilisant un AK-47 a tout d'un coup la puissance de feu d'un régiment de l'époque napoléonienne. Il n'est peut-être pas aussi professionnel, mais il peut faire autant de dégâts et de morts autour de lui, tout cela à cause d'un AK-47 dont il a appris le maniement en une demi-heure. Ainsi, la « démocratisation » de la guerre ne tient pas forcément uniquement à la disponibilité de technologies de pointe, mais simplement au fait que certaines technologies sont accessibles à tous.

Deuxièmement, nous constatons effectivement aujourd'hui que des acteurs très divers ont accès à des technologies nouvelles et avancées, en particulier parce qu'elles deviennent plus abordables et plus simples à utiliser. La gamme d'acteurs non étatiques qui utilisent la robotique va déjà des groupes d'activistes et de quasi-terroristes à des organisations criminelles, en passant par des groupes d'autodéfense (aussi connus sous le nom de milices des frontières), des organisations de médias et même des agents immobiliers. Ils se sont tous mis à la robotique, et lorsqu'on en arrive au point où l'on peut faire voler un microdrone à l'aide d'une application d'iPhone – ce qui est maintenant possible – tout d'un coup beaucoup de gens peuvent s'en servir.

Il en est de même pour les technologies informatiques et les cybercapacités. En même temps, il ne faut pas exagérer les risques et les craintes qui agitent déjà le monde des internautes et qui enflent et font gloser au point que l'on parle de cyberterrorisme. Nous n'avons pas encore vu aboutir une cyberattaque terroriste à grande échelle, ni une cyberopération militaire à grande échelle. En effet, du point de vue des terroristes en particulier, la conduite d'une cyberopération efficace, pour prendre l'exemple de Stuxnet, demande non seulement des compétences en informatique, mais aussi un investissement assez important et intelligent dans le renseignement, allié à des compétences dans nombre de domaines différents.

Prenons l'exemple de Stuxnet. Il ne s'agissait pas seulement de l'entrée par effraction dans un réseau informatique iranien, mais aussi de la conception d'un malware plutôt sophistiqué, ciblant des automates spécifiques produits par Siemens et fonctionnant dans une centrale nucléaire spécifique. Comment ces automates fonctionnent-ils ? Combien y en a-t-il et comment pénétrer à l'intérieur du système ? Seule une équipe composée de spécialistes du renseignement et d'ingénieurs a pu répondre à ces questions. Il a fallu pour cela réunir des compétences très différentes. Ce n'est pas le genre de choses que deux ados de 14 ans sirotant du Red Bull peuvent faire, ni que deux apprentis terroristes planqués dans un appartement de Hambourg sont capables d'imaginer.

C'est pourquoi je crains que, parfois, l'hystérie et le battage médiatique ne nous conduisent sur des terrains qui peut-être ne méritent pas une attention extrême, des milieux politiques comme des spécialistes de l'action humanitaire.

Poursuivons notre discussion sur la baisse des coûts de la guerre au sol. Si l'on considère l'engagement de leurs forces dans le monde, les États-Unis peuvent décider d'entrer en action si un autre pays n'a pas « le pouvoir ou la volonté » d'agir contre un danger les menaçant. Les frappes à l'aide de drones au Pakistan, au Yémen et en Somalie ont été expliquées par ce raisonnement. Que se passerait-il si un autre pays décidait que les États-Unis n'ont pas « le pouvoir ou la volonté » ?

Les milieux humanitaires ont un vrai problème face à ces attaques de drones : ils mélangent tactique et technologie. Prenons le cas de la frappe des États-Unis au Yémen qui a eu raison d'al-Awlaqi – affaire particulièrement contestée parce

qu'elle touche un citoyen des États-Unis. Qu'est-ce qui contrarie les milieux humanitaires ? Est-ce le fait que la frappe a été effectuée par un drone ou est-ce la frappe elle-même ? Autrement dit, que diraient ceux qui se plaignent des « attaques de drones » si l'on avait utilisé un F-16 avec pilote plutôt qu'un Reaper MQ9 ? Trouveraient-ils cela plus acceptable ? Évidemment non. La technologie influe sur les considérations politiques et sur les décisions qui sont prises, mais les questions de droit, elles, ne tiennent pas à la technologie elle-même. C'est généralement l'action elle-même et le poids que nous lui accordons qui détermine si un acte est légal ou non.

De même, il peut y avoir confusion entre l'utilisation de la technologie dans les zones où la guerre a été déclarée et son utilisation en dehors de ces zones. Par exemple, on nous interroge parfois sur l'usage militaire que font les États-Unis de ces systèmes mais, en fait, les questions visent les « frappes de drones » au Pakistan. L'usage militaire que font les États-Unis de ces systèmes n'est pas spécialement problématique du point de vue du droit humanitaire. Il se situe à l'intérieur de zones de guerre et s'inscrit dans une chaîne de commandement assez transparente. Il y a obligation de rendre des comptes, une hiérarchie qui réagit lorsque les choses tournent mal, remise de rapports aux échelons supérieurs et un système judiciaire qui peut être saisi de l'affaire.

Surtout, les questions relatives aux cibles sont beaucoup plus faciles à résoudre dans une zone de guerre transparente. La force qui nous anime, c'est l'action et non pas l'identité ; pour moi, c'est la clé. On n'a pas besoin de connaître le nom du tireur pour être une cible dans une zone de guerre. Si un sniper vous tire dessus, que vous pensiez que c'est Albert ou Ahmed derrière le fusil, cela n'a pas d'importance – c'est le fait qu'il vous tire dessus qui en a. Mais quand vous passez la frontière pour entrer, disons, au Pakistan, que l'opération ne s'inscrit plus dans le cadre du système militaire, avec ses troupes de soutien au sol, une chaîne de commandement claire et un système de justice militaire, mais qu'elle est menée à partir de renseignements de civils et que le choix des cibles ne repose plus sur l'action mais davantage sur une identité perçue et une menace probable, alors là les choses deviennent problématiques.

Ainsi, tous les aspects de votre opération, depuis le feu vert qui vous est donné jusqu'aux conséquences judiciaires en cas d'erreur (ou à dire vrai, l'absence de conséquences judiciaires dans la pratique), sont soumis à des règles fondamentalement différentes quand l'opération menée à l'aide de drones issus de la robotique cesse d'être une action militaire dans une zone de guerre pour devenir une opération secrète de l'autre côté de la frontière. Certains diraient que ce n'est pas ainsi que les choses devraient se passer mais, bien sûr, telle est la différence entre ce qui est et ce qui devrait être.

Les nouvelles technologies peuvent-elles servir aux milieux humanitaires ?

Il y a des parallèles à établir entre le monde humanitaire et les militaires pour ce qui est du potentiel des nouvelles technologies et des problèmes qui peuvent en résulter. La technologie donne aux milieux humanitaires des moyens qui

étaient inimaginables voilà seulement une génération, mais elle leur pose aussi des problèmes dont il aurait été inconcevable de se préoccuper il y a de cela une génération. Des moyens inimaginables, par exemple, de détecter les crimes de guerre et d'en établir l'existence. Quelqu'un qui commettrait un génocide aujourd'hui n'aurait que très peu de chances de s'en tirer sans que le monde l'apprenne.

De même, tant les petites organisations que les grandes ont les moyens de recueillir des informations sur les catastrophes naturelles, d'agir en conséquence et de localiser les populations qui ont besoin d'aide. Comparez les actions menées après le tsunami de 2004 et le tremblement de terre en Haïti en 2010. Quelques années seulement après le tsunami, les organisations humanitaires étaient capables d'échanger des informations pour localiser les gens et déterminer le type d'aide dont ils avaient besoin, grâce à Twitter, à la cartographie de crise et aux drones. Ces moyens sont stupéfiants.

En même temps se posent des questions fondamentales qui ne se posaient pas auparavant : quelles sortes de moyens un acteur humanitaire non gouvernemental devrait-il avoir ? Devrait-il avoir l'équivalent de sa propre force aérienne ? Quelles règles devraient en régir le fonctionnement ? D'autres questions touchant à la vie privée, à la propriété ou à la gestion de l'information se posent également. Et surtout, ces moyens éveillent dans certains cas de faux espoirs chez les humanitaires, comme chez les militaires, dont certains voient dans la robotique une solution technologique miracle. D'aucuns, par exemple, font valoir que le déploiement de drones de surveillance au Soudan ou en Syrie empêcherait les crimes de guerre. Nous savons déjà que des horreurs se produisent au Darfour ou à Damas. Il se peut que l'on en ait à présent une idée plus précise, que cela suscite une multiplication des réactions sur Twitter, mais est-ce que cela change la réalité sur le terrain ?

Pensez-y sous cet angle : Henry Dunant n'imaginait pas un monde dans lequel le CICR se creuserait la cervelle à propos de machines volantes sans personne dedans, qui traversent les frontières pour larguer des fusées qui ne manquent jamais leur cible parce qu'elles sont guidées par un faisceau lumineux amplifié. De son temps, l'organisation n'était même pas prête à appréhender des choses telles que des sous-marins. Les questions sur lesquelles l'organisation sera amenée à réfléchir à l'avenir seront très différentes de celles qui l'occupent maintenant.

Quelles sortes de conséquences humanitaires ces nouvelles technologies pourraient-elles avoir ?

La grande difficulté, quand on parle des conséquences humanitaires, est de faire la différence entre les technologies d'aujourd'hui et celles qui commencent à faire leur apparition.

Par exemple, certains prétendent que des drones ne peuvent pas faire de prisonniers. Eh bien, pendant la guerre du Golfe de 1991, l'US Navy utilisait un drone Pioneer pour localiser les cibles sur lesquelles devait tirer l'artillerie

navale. Il n'a pas échappé aux Irakiens que chaque fois que ce petit avion bruyant à hélices volait au-dessus d'eux, deux minutes plus tard, toutes les forces de l'enfer se déchaînaient. Le drone faisait de l'exploration pour un navire de guerre datant de la Seconde Guerre mondiale, qui tirait des obus de 16 pouces capables de tout raser dans un rayon grand comme un terrain de football. Les Irakiens ont compris que ce petit drone était de mauvais augure lorsqu'il s'approchait d'eux, si bien que la fois suivante, lorsqu'il les a survolés, plusieurs d'entre eux ont retiré leurs uniformes et agité des tee-shirts blancs. C'était la première fois dans l'histoire que des êtres humains se rendaient à un robot.

Cet épisode s'est produit en 1991. Derrière les technologies télécommandées comme le Pioneer et une grande partie de la robotique, il y a encore un homme aujourd'hui. Et elles ont déjà des conséquences massives, bien qu'il s'agisse de la première génération de cette technologie. Il n'est pas nécessaire d'attendre que la technologie devienne totalement autonome dans un monde de Terminator imaginaire pour que la robotique ait une incidence sur nos décisions de partir en guerre, et sur le choix du moment et du lieu. Elle en a déjà une maintenant, au Pakistan et en Libye. Mais souvent, soit nous faisons des amalgames, soit nous ignorons des questions encore plus importantes, alors que la technologie gagne sans cesse en autonomie et en intelligence. Actuellement, les questions tournent autour de l'utilisation de drones hors des zones de guerre, ou autour du fait que ces frappes sont télécommandées et des pertes civiles qu'elles occasionnent.

Peu à peu, le débat en vient cependant à porter sur des systèmes de plus en plus capables de prendre des décisions autonomes ; le point d'interface entre l'homme et ces machines ne se situe pas au moment de la bataille, mais plutôt dans les jours, semaines ou même années qui la précèdent, lorsque le système est programmé. Par exemple, nous avons déjà des logiciels d'acquisition d'objectifs, nous avons déjà des avions qui, non seulement peuvent décoller et atterrir tout seuls, mais qui peuvent aussi voler en toute autonomie pendant certaines parties de la mission. À l'avenir, on pourrait avoir un système autonome capable de transformer une mitrailleuse de calibre 50 en fusil à lunette.

Pourtant, au stade actuel, notre intelligence artificielle n'est pas capable de distinguer une pomme d'une tomate. N'importe quel bambin de deux ans sait faire la différence. Et qu'en est-il de l'intelligence affective ? Un ordinateur porte sur une femme de 80 ans dans une chaise roulante exactement le même regard que sur un char T-80. L'une et l'autre ne sont que des zéros et des uns. Des pans entiers de l'expérience humaine de la guerre risquent donc d'être transférés, modifiés ou déplacés à mesure que la technologie acquiert plus de capacités.

Lorsque j'ai fait le tour des organisations humanitaires pour les interviewer pour mon livre il y a quatre ans, aucune n'était prête ou disposée à parler de technologies comme le Predator. Le même phénomène se produit maintenant avec l'évolution actuelle des technologies. Les milieux humanitaires réagissent après coup à des choses qui existent déjà et sont utilisées. Il en résulte pour eux une perte d'influence, parce qu'ils ont trop attendu pour en tenir compte. La technologie suivante pointe déjà son nez.

Il est difficile de les en blâmer – il y a tellement d'autres choses qui se passent dans le monde que réfléchir à la robotique semble une perte de temps. Là encore, la technologie dont nous parlons aujourd'hui n'est pas du tout théorique, elle n'est pas conçue quelque part dans le désert dans des labos secrets dont personne ne connaît l'existence. Elle existe et on peut lire des articles là-dessus dans le magazine *Wired* [5] ou en entendre parler au journal télévisé, et pourtant on se laisse distancer. Il y a certainement des documents classés « secret défense » dans divers domaines, mais une grande partie des travaux est publique. Je travaille actuellement sur un projet qui a pour objet de recenser les technologies qui, à l'état d'ébauche aujourd'hui, changeront la donne, autrement dit les technologies qui sont aujourd'hui ce que le Predator était en 1995. Et n'oublions pas que les vols du Predator étaient publics en 1995. Ce n'était pas un secret.

Que peut faire la société civile internationale – et les milieux humanitaires en particulier – pour mieux réagir face aux défis que vous mentionnez ? Comment faire pour mieux anticiper ?

J'ai écrit un article intitulé « The Ethics of Killer Apps: Why is it so hard to talk about Science, Ethics and War »[6] (L'éthique du tueur et ses applications : pourquoi il est si difficile de parler de science, d'éthique et de guerre). J'y passe en revue les difficultés rencontrées face aux nouvelles technologies, et il en est une majeure que j'évoque et qui est la difficulté à passer d'un domaine à l'autre. Nous restons dans notre propre domaine de compétence, entourés de gens qui pensent comme nous, parlent notre langue, écrivent et lisent des revues spécialisées dans leur domaine uniquement, et nous nous attribuons mutuellement des récompenses pour cela.

Résultat : passer d'un domaine à l'autre, c'est dans une large mesure comme passer d'un pays à l'autre, d'une culture à l'autre. Si vous parlez la langue du droit humanitaire et que vous passez dans le monde de la science, c'est comme si tout le monde vous parlait finlandais. À son tour, lorsque le scientifique essaie de lire, d'écrire ou de parler à quelqu'un qui est dans le droit humanitaire, c'est comme si tout le monde s'adressait à lui en portugais. Et ce ne sont pas seulement les langues qui sont différentes – il y a une incapacité fondamentale à comprendre. Au fond, comme l'a expliqué l'une des personnes que j'ai interviewées, le scientifique va rarement entamer une discussion philosophique sur l'évolution des nouvelles technologies parce qu'il devrait alors « porter la casquette du philosophe », et qu'il « n'a pas cette casquette ». De même, on peut lire des tonnes d'articles dans les milieux du droit international sur des questions telles que les drones, écrits par des gens qui n'ont jamais vu un drone et n'ont jamais essayé non plus de parler à quelqu'un qui en a fait voler, en a conçus ou en a fait fonctionner. Il y a donc incapacité de communiquer, ce qui est à mon sens le problème majeur.

5 Disponible sur : http://www.wired.com/magazine/ (dernière consultation en juin 2012).

6 Peter W. Singer, « The Ethics of Killer Apps : Why is it so hard to talk about Science, Ethics and War », dans *Journal of Military Ethics*, Vol. 9, N° 4, 2010, pp. 299-312.

Pour le projet dont je parlais, nous interviewons des scientifiques de haut niveau, des directeurs de laboratoires militaires, des futurologues, des gens qui travaillent chez Google et d'autres sociétés de ce genre, et nous leur posons la question suivante : quelles sont les nouvelles technologies qui marqueront l'avenir ? Vont-elles être du genre de l'AK-47, que tout le monde peut avoir, ou de celui de la bombe atomique, que très peu d'acteurs peuvent acquérir ? Nous les interrogeons ensuite sur l'utilisation que l'armée fera de ces armes. Quel usage en fait-on dans les conflits sophistiqués dirigés contre des États, et dans les conflits plus rudimentaires de type insurrectionnel dans lesquels interviennent d'autres acteurs que l'État ? Comment pourrait-on utiliser ces technologies contre vous, et quelles en sont les faiblesses ? La dernière partie de ce projet consiste à réunir des éthiciens, des philosophes, des spécialistes du droit humanitaire, des responsables religieux et des gens des médias et à dire : voici les technologies qui, selon les scientifiques, vont s'imposer ; voici comment les militaires pensent les utiliser, quelle est votre opinion ? L'idée est alors d'essayer, pendant qu'il en est encore temps, de poser les questions qui, nous le savons, vont devenir d'actualité. C'est, à mon avis, la meilleure façon de procéder ; cela vaut mieux en tout cas que d'attendre d'être placé devant le fait accompli pour entamer la discussion. Préparez-vous.

Autre défaut que les milieux humanitaires devraient chercher à corriger : comme n'importe quel autre milieu, face aux grandes questions auxquelles ils veulent s'attaquer, ils se focalisent sur un aspect de la question et manquent souvent de jugement dans leurs efforts. Par exemple, pendant mes recherches sur les enfants soldats, j'ai découvert que le discours dans ce domaine portait de manière démesurée sur le recrutement par les armées occidentales de jeunes de 17 ans et demi – ce qui concernait quelques centaines de personnes qui n'étaient pas enlevées à leurs familles. À la lecture des rapports, on s'aperçoit que ce problème est traité avec la même profondeur, la même précision et la même énergie que celui des dizaines de milliers d'enfants de 12 ans et moins qui ont été enlevés de chez eux, drogués avec une poudre brune appelée *brown-brown*[7] et forcés de mettre le feu à un village. Il s'agit dans les deux cas de pratiques répréhensibles, à mon avis, mais la seconde est manifestement plus grave et devrait mobiliser une plus grande part de nos ressources limitées. Si nous voulons produire des effets et une synergie autour d'une question, il faut que nous sachions clairement sur quoi faire porter nos efforts.

Le même constat vaut aujourd'hui dans les discussions sur les armes et les technologies. Les lasers aveuglants ont beaucoup fait parler d'eux à une époque où le battage autour de ces armes n'était pas proportionné à leurs effets. De nouveau, qu'il n'y ait pas de malentendu : je ne dis pas que ces efforts n'en valent pas la peine, mais qu'il faut les faire en réfléchissant à la meilleure façon, pour la communauté internationale humanitaire, d'utiliser ses ressources pour obtenir l'impact maximum.

7 Mélange d'héroïne ou de cocaïne en poudre et de poudre de cartouches de fusil.

Je crains que notre préférence n'aille parfois à des questions qui peuvent paraître séduisantes ou davantage susceptibles d'intéresser les médias (et donc des donateurs), mais qui n'ont peut-être pas les mêmes conséquences que d'autres questions moins débattues publiquement. Par exemple, dans les années 1990, le pourcentage de travailleurs humanitaires par habitant était plus élevé dans les Balkans que dans des régions d'Afrique aussi troublées, sinon plus. Nous assistons aujourd'hui au même phénomène chez les militants préoccupés de technologie, et cela me préoccupe.

Constatez-vous dans vos recherches des différences dans la manière d'aborder les utilisations de la technologie d'un point de vue éthique ? Les démarches éthiques qui devraient précéder le déploiement de nouvelles technologies diffèrent-elles selon le contexte dans lequel on se trouve dans le monde (par exemple en Chine, en Russie et en Inde) ?

Absolument, parce que chacun est marqué par sa psychologie et sa culture ; cela a une grande influence sur le bien et le mal que nous pouvons penser de ces technologies. Les attitudes à l'égard de la robotique en sont un bon exemple. En Occident, le robot a été dès l'origine le serviteur mécanisé qui se réveille et puis se révolte, et il l'est toujours. Au sens littéral, le mot vient du terme tchèque pour « servitude » ; il a été employé pour la première fois dans les années 1920 dans une pièce de théâtre appelée *R.U.R : Rossum's Universal Robots*, dans laquelle ces nouveaux serviteurs mécaniques appelés « robota » deviennent intelligents et s'emparent du monde. Cette trame du méchant robot prêt à prendre le contrôle est encore présente aujourd'hui dans toute la science-fiction, mais aussi dans le monde politique. L'image d'un robot armé d'une mitrailleuse, même si c'est un système entièrement télécommandé, nous fait encore froid dans le dos.

En Asie, en revanche, on porte sur le robot – dans la science-fiction et ailleurs – un tout autre regard. Au Japon, le robot fait son apparition dans la science-fiction après la fin de la Seconde Guerre mondiale et il ne fait pas figure de méchant, mais presque toujours de gentil. Le robot est l'acteur humanitaire. *Astro Boy* en est un exemple. Cette idée rejoint certaines notions de la religion et de la culture. Dans le shintoïsme, par exemple, contrairement aux croyances occidentales, une pierre, un cours d'eau ont une âme, et un robot aussi. Il en résulte des attitudes très différentes à l'égard de la robotique selon les cultures, et des réticences plus ou moins grandes à les utiliser à la maison. Nous n'avons pas de robot baby-sitter en Occident de nos jours. Les robots destinés à servir de compagnons aux personnes âgées n'y sont pas commercialisés. Les Japonais en ont. En Corée du Sud, Samsung n'a pas seulement créé un robot armé d'une mitrailleuse, mais a également produit une publicité télévisée dans laquelle la société se vante d'avoir construit ce robot. Vous imaginez Apple faisant une publicité télévisée à sa gloire en Occident pour faire savoir qu'ils ont créé un robot armé d'une mitrailleuse ?

Les robots sont-ils en fait capables d'avoir un comportement éthique ? Peuvent-ils avoir pour effet de mieux faire respecter le droit de la guerre sur le terrain ou, au contraire, voyez-vous leur déploiement comme une menace ?

Nous voulons une réponse facile, oui ou non, ou, en termes de robotique, des questions formulées en zéros ou en uns. Je pense que cela montre exactement pourquoi les problèmes d'éthique ne seront pas résolus par la robotique. Parce qu'en fin de compte, ni la guerre ni l'éthique ne sont des domaines qui se réduisent à des zéros et des uns, même avec la robotique la plus perfectionnée.

On assiste déjà à une évolution des capacités permettant d'observer ou de respecter le droit international ou, plus important encore, de prendre sur le fait ceux qui sont en train de le violer. Ces améliorations auraient été impensables dans le passé. Je prendrai comme exemple une anecdote que m'a rapportée un officier de l'armée américaine en Irak. Ils avaient un drone qui volait au-dessus d'eux alors qu'ils menaient une opération au sol. Ils ont capturé un rebelle. Il a été placé sous la garde d'un soldant dans une ruelle adjacente. À un moment donné, le soldat a jeté un coup d'œil vers le bas de la rue, puis de l'autre côté ; il a vu que personne ne regardait et a rapidement balancé un coup de pied à la tête du prisonnier. Mais c'était sans compter le drone ; au centre de commandement, ils étaient tous en train de suivre la scène au moyen de l'avion qui la survolait. Le commandant a raconté qu'il a vu tous les regards se tourner vers lui d'un air interrogateur. Comment allait-il réagir ? Par le passé, il aurait été impossible d'établir la preuve que le prisonnier avait été maltraité. Or, grâce aux nouvelles technologies, tout le monde avait assisté en direct à cette maltraitance et regardait le commandant pour savoir ce qui allait se passer. Il a finalement puni le soldat.

Autre scénario qui illustre l'avantage de ces technologies : les robots peuvent se substituer aux soldats en milieu urbain. Dans ces opérations, les soldats doivent faire irruption dans une pièce et décider en quelques millièmes de seconde si les gens à l'intérieur sont des civils ou des ennemis. Cet homme-là tient-il un AK-47 ou un appareil photo ? Cet enfant tient-il en réalité un fusil ou un balai ? Ils savent que s'ils se trompent en ces quelques millièmes de seconde, ils risquent d'être tués. Aussi y a-t-il beaucoup d'erreurs commises. Comparez ce scénario à celui où ce sont des robots qui sont envoyés : ils peuvent détecter les gens, les observer et, s'ils ont un doute, ils peuvent attendre pour tirer. Si les gens tirent les premiers, aucune conséquence, personne ne meurt. C'est là le gros avantage de ces technologies.

Mais disons-le clairement : beaucoup de gens poussent ce raisonnement trop loin et prétendent que la technologie sera la solution miracle aux problèmes d'éthique. Nos âmes ne sont pas parfaites, nos machines non plus. Aussi ne devrait-on pas parler d'une technologie qui n'existe pas encore comme si elle existait réellement. On entend dire qu'on pourrait placer un « régulateur éthique » sur la technologie et que cela résoudrait les problèmes. Demandez à voir les plans d'un régulateur éthique. C'est ce qu'on appelle, en langage militaire, du *vapourware*, du vent. Il y a le *hardware* (le matériel), le s*oftware* (les logiciels) et le *vapourware*, pour ce qui n'existe pas.

Mais même si cela existait, ce ne serait pas une solution miracle. Imaginons que l'on soit capable de créer un ensemble de logiciels qui mette en œuvre les Conventions de Genève. En fait, ce ne serait pas encore suffisant dans la guerre moderne. Parce qu'on a deux problèmes. Premièrement, les Conventions de Genève ne se traduisent pas en un langage tranché de oui et de non dans toutes les situations, surtout dans le conflit moderne. Deuxièmement, il y a des acteurs qui font ce qu'on appelle du « *lawfare* », qui connaissent le droit de la guerre et qui le violent délibérément.

Je prends ces exemples du monde réel pour montrer combien il est faux de penser que la technologie va régler les guerres et les dilemmes de la guerre. À supposer même que la technologie soit inventée, que vous dirait-elle de faire devant un sniper qui vous tire dessus avec deux femmes assises devant lui et quatre enfants couchés sur lui, comme l'a fait un sniper du monde réel en Somalie ? Un sniper qui s'était revêtu d'une armure vivante de non-combattants ? Tirer ou ne pas tirer ? Que vous dirait-elle de faire si elle voyait un char avec des enfants assis dessus se livrer à une opération de nettoyage ethnique ? Que vous dirait-elle de faire devant une ambulance qui transporte à la fois des civils et des soldats blessés, ainsi que des munitions ? Que vous dirait-elle de faire à un civil contraint de tirer des roquettes depuis sa ferme sur une ville peuplée de civils pour ne pas être lui-même tué par un groupe armé local ? Tous ces cas se sont produits dans le monde réel, au cours de conflits récents. On pourrait passer des heures à en discuter – les pages de cette revue seraient pleines d'articles consacrés à ce que le droit dit et ne dit pas, et tous les juristes prendraient beaucoup de plaisir à argumenter sur ce qu'il convient de faire dans ce genre de situation. Alors penser que les dilemmes du conflit pourraient être aisément tranchés par un ensemble de logiciels qui n'existe pas encore, ce n'est pas raisonnable.

Bien entendu, dans la guerre, l'ennemi a aussi son mot à dire. Je veux dire par là qu'à mesure que les machines se perfectionneront, les gens en face deviendront de plus en plus ingénieux dans la recherche de moyens de les contourner. Je vous raconte une anecdote, qui ne manque pas de sel. Il existe un véhicule terrestre sans pilote qui est capable de mettre une mitrailleuse en position. J'en discutais avec un groupe de marines américains – pas seulement de l'avancée incroyable que cela représentait, mais aussi des réactions potentielles de la partie adverse. Et nous disions que la riposte la plus efficace, ce n'était pas une technologie archisecrète, mais plutôt un enfant de six ans armé d'une bombe de peinture aérosol parce que cela pose un dilemme inextricable.

Soit vous tirez sur un enfant de six ans qui, techniquement parlant, n'est pas armé, parce qu'il a une bombe de peinture aérosol, soit vous laissez un enfant de six ans marcher jusqu'à votre engin et le neutraliser. Il n'a qu'à vaporiser de la peinture sur les capteurs visuels. L'un des marines dans le public s'est mis à hurler : « Dans ce cas, on télécharge simplement une arme non létale, comme le pistolet Taser, et on s'en sert contre le petit gars ». J'ai répondu : « Voilà qui est intéressant. C'est une réponse passablement humanitaire que vous me donnez. » Sauf qu'il y a encore un problème. Vous avez trouvé une solution humanitaire et vous avez contourné le problème. Mais il reste une multitude de problèmes à résoudre.

Premièrement, combien va coûter le kit de mise à jour ? L'un des marines s'est écrié, en plaisantant à moitié, qu'avec leur système d'acquisition, cela risquerait de coûter quelques millions. Ainsi, la guerre se déplace maintenant sur le terrain de l'investissement, et à une projection de peinture de cinquante cents vous répondez par des mises à jour coûtant des millions de dollars. Ce n'est pas justifiable. La partie adverse a d'ores et déjà gagné, simplement parce qu'elle a recouru à cette tactique illicite et envoyé un enfant se battre à sa place. Deuxièmement, même si vous optez pour la solution non létale, vous allez avoir des ennuis. Quand la vidéo deviendra publique et montrera un robot utilisant un pistolet Taser contre un enfant de six ans, je pense que cela fera très mauvais effet et produira des remous. Je veux dire par là que, si avancée que soit votre technologie, vous ne pouvez pas vous débarrasser des dilemmes éthiques et juridiques qui vont de pair avec les tactiques et stratégies de la guerre.

Il semble que nous soyons fascinés par les robots, les acteurs humanitaires comme les militaires. Où cette fascination nous mènera-t-elle à l'avenir ?

Eh bien, on peut répondre par un métadéfi, puis par une métaquestion. Le métadéfi est essentiellement celui-ci : les technologies progressent à un rythme exponentiel. Dans le monde informatique, elles suivent la loi de Moore : la puissance des puces électroniques double tous les 18 mois. Parmi les applications civiles, voyez l'iPhone dont vous avez fait cadeau à votre enfant l'an dernier. Il semblait alors incroyablement à la pointe et puissant, et il est déjà dépassé une année après.

Du côté militaire, toute l'armée des États-Unis dans laquelle mon père a servi avait moins de puissance électronique à sa disposition qu'une simple carte d'anniversaire qui s'ouvre en jouant un petit air. Et pourtant nos politiques, les milieux des juristes et des éthiciens n'évoluent pas à un rythme exponentiel, mais plutôt glaciaire. Le fossé entre les deux s'élargit de plus en plus ; nous prenons de plus en plus de retard. C'est cela le métadéfi.

Quant à la métaquestion que soulève la robotique, elle se pose en ces termes : nous nous distinguons en tant qu'espèce par notre créativité ; nous sommes la seule espèce à avoir inventé le feu, les fusées qui nous ont transportés jusqu'à la lune, l'art, la littérature, le droit et l'éthique. C'est ce qui nous distingue comme espèce. Et maintenant nous sommes en train de créer non seulement des machines d'une technologie incroyable, mais une nouvelle espèce en puissance, peut-être à notre image, peut-être pas. Mais pour être honnêtes avec nous-mêmes, si nous créons cette technologie, ce n'est pas seulement pour progresser dans un sens positif, mais pour essayer de trouver le moyen de mieux nous entretuer, comme l'homme le fait depuis la nuit des temps. Ainsi le titre de mon livre, *Wired for War* (configurés pour la guerre), était un jeu de mots. Mais au final, la vraie question est la suivante : est-ce que ce sont nos machines qui sont programmées pour la guerre ou nous, les humains ?

Volume 94 Sélection française 2012/2

REVUE INTERNATIONALE

Émergence de nouvelles capacités de combat : les avancées technologiques contemporaines et les enjeux juridiques et techniques de l'examen prévu à l'article 36 du Protocole I

Alan Backstrom et Ian Henderson*

Alan Backstrom (Baccalauréat en Ingénierie et Master en Science de l'Ingénieur) est responsable qualité dans l'industrie automobile. Il dispose d'une vaste expérience de collaboration avec les fabricants d'équipements et les fournisseurs de systèmes, sous-systèmes et composants ; ses principaux domaines de compétence sont les techniques de validation de la conception, les analyses de garantie et les enquêtes après accident. Le colonel d'aviation Ian Henderson (AM, BSc, LLB, LLM, PhD) est conseiller juridique auprès de l'armée de l'air australienne.

* Le présent article a été rédigé à titre personnel et ne représente pas nécessairement les opinions du département australien de la Défense ou des forces armées australiennes. Les auteurs remercient les nombreux amis et collègues qui ont généreusement fait part de leurs commentaires sur une première ébauche de l'article.
La version originale en anglais de cet article est publiée sous le titre « New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews », dans *International Review of the Red Cross*, Vol. 94, N° 886, été 2012, pp. 483-514, et a été traduite en français par le CICR.

Résumé

La complexité croissante des systèmes d'armement exige de conduire de manière interdisciplinaire l'examen de licéité des armes prévu à l'article 36 du Protocole additionnel I des Conventions de Genève. Leurs concepteurs doivent connaître les principes du droit international humanitaire qui régissent l'emploi des armes. Les juristes, quant à eux, doivent savoir comment l'arme examinée sera utilisée dans les opérations, et ils doivent utiliser cette connaissance pour faciliter l'élaboration de directives opérationnelles judicieuses tenant compte des défis que les avancées technologiques posent au droit international humanitaire. Les informations relatives aux capacités d'une arme donnée sont souvent extrêmement confidentielles et « compartimentées ». Juristes, ingénieurs et opérateurs doivent donc travailler de manière coopérative et imaginative pour surmonter les limitations dues à la classification de sécurité et à la compartimentation de l'accès aux informations.

Mots-clés : arme, DIH, droit international humanitaire, droit des conflits armés, guerre, conduite de la guerre, Conventions de Genève, Protocole additionnel, examen de la licéité des armes, autonome, reconnaissance de cible, fiabilité.

: : : : : : :

L'article 36 du Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux[1] dispose que :

> « Dans l'étude, la mise au point, l'acquisition ou l'adoption d'une nouvelle arme, de nouveaux moyens ou méthodes 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 ».

À mesure que les armes deviennent techniquement plus complexes, il est de plus en plus difficile de satisfaire à l'exigence (apparemment simple) posée par le droit international. Si l'on demandait à un juriste de se prononcer sur la licéité

1 Ci-après « Protocole additionnel I ». Ouvert à la signature le 12 décembre 1977, 1125 U.N.T.S. 3, entré en vigueur le 7 décembre 1978. Voir, de façon générale, Justin McClelland, « The review of weapons in accordance with Article 36 of Additionnal Protocol I », dans *Revue internationale de la Croix-Rouge*, Vol. 85, N° 850, juin 2003, pp. 397-415 ; Kathleen Lawand, « Reviewing the legality of new weapons, means and methods of warfare », dans *International Review of the Red Cross*, Vol. 88, N° 864, décembre 2006, pp. 925-930 ; Comité international de la Croix-Rouge (CICR), *Guide de l'examen de la licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre – Mise en œuvre des dispositions de l'article 36 du Protocole additionnel I de 1977*, 2006, disponible sur : http://www.icrc.org/fre/assets/files/other/icrc_001_0902.pdf (toutes les références Internet ont été consultées en juin 2012). Pour une analyse plus détaillée de ce qui constitue (ou ne constitue pas) une « arme » aux fins de l'examen de licéité, voir Duncan Blake et Joseph Imburgia, « 'Bloodless Weapons'? The need to conduct legal reviews of certain capabilities and the implications of defining them as 'weapons' », dans *The Air Force Law Review*, Vol. 66, 2010, p. 157.

d'une épée, il n'aurait pas besoin de se préoccuper d'autres caractéristiques techniques que celles qui sont observables à l'œil nu. Les subtilités des méthodes de production et d'essais ne présenteraient aucun intérêt sur le plan du droit, et même un juriste serait capable de comprendre comment l'arme serait utilisée au combat. Il en va tout autrement pour certaines armes modernes, sans parler des armes encore en cours de développement. Par exemple, pour utiliser une arme guidée dotée d'une option de tir autonome, il faut comprendre les paramètres juridiques, la conception technique, les méthodes de conception et d'essais (ou de validation), ainsi que la manière dont l'arme en question pourrait être employée sur le champ de bataille[2]. Il y a toujours une part de vérité dans l'humour et, même s'il s'agit d'une boutade, nous nous souviendrons que l'on devient juriste quand on est mauvais en maths, ingénieur quand on est mauvais en orthographe – et soldat quand on ne comprend ni les maths ni l'orthographe !

Déterminés à abattre toutes ces barrières, nous adopterons une approche multidisciplinaire dans le présent article. Nous identifierons les problèmes juridiques essentiels associés à l'emploi des armes, nous relèverons les caractéristiques importantes des armes émergentes, puis nous analyserons la manière dont les essais et les évaluations techniques peuvent renseigner le processus d'examen juridique de ces armes. En combinant ces différentes méthodes, nous espérons établir un cadre général permettant de mieux comprendre les problèmes juridiques et techniques qui sont associés à la mise au point et à l'emploi d'une arme, qu'elle soit simple ou complexe.

Après un rapide examen des facteurs juridiques essentiels relatifs à l'emploi et à l'examen des armes, nous nous pencherons sur trois questions de fond. La première partie traite du processus d'autorisation de ciblage, indépendamment du choix de l'arme qui sera employée ; la deuxième examine certaines armes émergentes, ainsi que les problèmes juridiques posés par ces armes ; enfin, la troisième est consacrée aux questions d'ingénierie liées à l'évaluation de la licéité des armes nouvelles et, en particulier, comment l'examen d'armes d'une très grande complexité peut être facilité par la compréhension des processus de conception.

Facteurs juridiques essentiels

Les étapes-clés prévues par le droit international humanitaire[3] pour lancer une attaque sont les suivantes :

1) Recueillir des renseignements sur la cible.
2) Analyser ces renseignements pour déterminer si la cible constituera, au moment de l'attaque, une cible licite.

2 Voir Michael Schmitt, « War, technology and the law of armed conflict », dans Anthony Helm (éd.), *The Law of War in the 21st Century : Weaponry and the Use of Force*, Vol. 82, *International Law Studies*, 2006, p. 142.

3 Également appelé « droit des conflits armés ».

3) Considérer les effets pouvant être causés incidemment par l'arme et prendre toutes les précautions pratiquement possibles pour réduire au minimum de tels effets.
4) Évaluer la « proportionnalité » entre, d'une part, tous les effets incidents attendus et, d'autre part, l'avantage militaire escompté de l'attaque dans son ensemble (et non pas simplement de l'attaque spécifique menée avec une arme particulière)[4].
5) Tirer, lancer ou l'utiliser d'une autre manière, de telle sorte que ses effets soient dirigés contre la cible désirée.
6) Observer l'évolution de la situation, et annuler ou suspendre l'attaque si les effets incidents sont disproportionnés[5].

En outre, le type d'arme à employer doit être pris en compte. Il est particulièrement important dans le cadre du présent article de noter que certaines façons d'employer une arme par ailleurs licite pourraient produire un effet prohibé (par exemple, tirer de manière indiscriminée avec un fusil). L'examen de la licéité d'armes nouvelles (y compris les nouveaux moyens et méthodes de combat) repose sur certains facteurs juridiques essentiels. Il s'agit, d'une part, de chercher à établir si l'arme est elle-même interdite ou si son emploi est soumis à des restrictions par le droit international[6] et, d'autre part, si ce n'est pas le cas, il s'agit de déterminer si les effets de l'arme en question sont interdits ou limités par le droit international[7].

4 Voir, par exemple, la déclaration d'interprétation de l'Australie, selon laquelle, au sens des articles 51 et 57 du Protocole additionnel I, *op. cit*., note 1, l'avantage militaire doit être compris comme étant « l'avantage attendu de l'attaque militaire dans son ensemble, et non pas seulement des parties isolées ou particulières de cette attaque » – reproduit dans Adam Roberts et Richard Guelff, *Documents on the Laws of War*, 3e éd., Oxford University Press, Oxford, 2000, p. 500.

5 Voir *op. cit*., note 1, art. 57(2)(b) du Protocole additionnel I.

6 Les armes peuvent être purement et simplement interdites, ou interdites en fonction du but recherché ou de l'utilisation normale attendue, ou les manières de les employer peuvent être réglementées (c'est-à-dire que certains emplois peuvent être interdits). Une arme peut être totalement interdite par un instrument spécifique : par exemple, les armes biologiques sont interdites par la *Convention sur l'interdiction de la mise au point, de la fabrication et du stockage des armes bactériologiques (biologiques) ou à toxines et sur leur destruction*, ouverte à la signature le 10 avril 1972, 1015 U.N.T.S. 163, entrée en vigueur le 26 mars 1975. Une arme peut aussi faire l'objet d'une interdiction générale si, en toutes circonstances, elle est « de nature à causer des maux superflus », voir *op. cit*., note 1, art. 35(2) du Protocole additionnel I, et droit international coutumier. Nous pouvons comparer cela avec, par exemple, les armes à laser qui sont généralement licites mais sont interdites quand elles sont « spécifiquement conçues de telle façon que leur seule fonction de combat ou une de leurs fonctions de combat soit de provoquer la cécité permanente chez des personnes dont la vision est non améliorée », *Protocole relatif aux armes à laser aveuglantes* (*Protocole IV) annexé à la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination*, ouvert à la signature le 13 octobre 1995, 35 ILM 1218, entré en vigueur le 30 juillet 1998. Enfin, les armes incendiaires sont licites *per se*, mais, par exemple, « [i]l est interdit en toutes circonstances de faire d'un objectif militaire situé à l'intérieur d'une concentration de civils l'objet d'une attaque au moyen d'armes incendiaires lancées par aéronef », art. 2(2) du *Protocole sur l'interdiction ou la limitation de l'emploi des armes incendiaires (Protocole III) annexé à la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination,* ouvert à la signature le 10 avril 1981, 1342 U.N.T.S. 137, entré en vigueur le 2 décembre 1983.

7 CICR, *Guide de l'examen de la licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre – Mise en œuvre des dispositions de l'article 36 du Protocole additionnel I de 1977*, *op. cit*., note 1, p. 11.

Enfin, « les lois de l'humanité et les exigences de la conscience publique » doivent être gardées à l'esprit[8].

Du point de vue opérationnel, les points essentiels peuvent se résumer ainsi : il faut obtenir la reconnaissance correcte de la cible, déterminer la façon de donner l'autorisation de tir et, enfin, contrôler (ou limiter) les effets de l'arme.

Sur le plan juridique, les problèmes associés aux armes de conception relativement simple sont, eux aussi, relativement simples. Si nous reprenons l'exemple de l'épée, nous n'avons en fait à répondre qu'aux deux questions suivantes : a) s'agit-il d'une « arme prohibée »[9] ; b) si tel n'est pas le cas, la personne qui manie l'épée le fait-elle avec discrimination ? Ni les défauts de conception (si, par exemple, l'arme était mal équilibrée), ni les défauts de fabrication (si, par exemple, le métal était trop fragile) n'auront d'incidence sur l'analyse juridique ; en fait, ces défauts ne préoccuperont probablement que l'utilisateur de l'épée. S'agissant d'armes plus compliquées (les arbalètes, par exemple), la complexité de leur conception entraîne le risque que l'obligation de distinction ne puisse être respectée en raison des éléments suivants :

- erreurs de conception (si, par exemple, l'arme ne tire pas droit ou si le système de visée est défaillant par suite d'un défaut de conception) ; ou
- erreurs de fabrication (si, par exemple, l'arme ne tire pas droit ou si le système de visée est défaillant parce que l'arme n'a pas été fabriquée conformément à la conception, dans les limites de ce qui est tolérable).

Les erreurs de ce type sont susceptibles d'être amplifiées dans le cas des armes de longue portée (l'artillerie, notamment) ; de plus, la variabilité des lots de production constitue également désormais un élément important, toute variation étant amplifiée du fait de la plus longue portée de l'arme. Par ailleurs, les armes modernes sont dotées d'une variété de systèmes de visée qui ne dépendent pas seulement de l'opérateur (comme par exemple un système de guidage inertiel ou d'un guidage électro-optique ou par GPS). Enfin, comme nous le verrons plus bas, certaines armes ont la capacité de choisir elles-mêmes leur cible.

Dans le domaine de l'armement, la technologie progresse dans de nombreuses directions différentes. Or, rares sont les ouvrages accessibles au public qui traitent des voies de recherche et des capacités des armes en cours de développement[10]. Les armes émergentes dont nous parlerons ci-dessous ne sont donc mentionnées qu'à titre purement représentatif. De toute façon, aux fins de notre exposé, les capacités exactes ont moins d'importance que les modes opératoires considérés d'un point de vue général.

8 *Ibid.*

9 Étant donné qu'il n'existe aucune interdiction portant spécifiquement sur les épées, l'examen de licéité serait basé sur l'interdiction générale des armes qui sont « de nature à causer des maux superflus », conformément à l'art. 35(2) du Protocole additionnel I, *op. cit.*, note 1.

10 Voir Hitoshi Nasu et Thomas Faunce, « Nanotechnology and the international law of weaponry: towards international reglementation of nano-weapons », dans *Journal of Law, Information and Science*, Vol. 20, 2010, pp. 23-24.

Reconnaissance de cible et autorisation de tir

Nous nous intéresserons maintenant aux armes et systèmes d'armement qui, d'une part, possèdent un certain niveau de fonctionnalité leur permettant d'établir une distinction entre les différents types de cibles et qui, d'autre part, dans des circonstances appropriées, pourraient attaquer une cible sans qu'une intervention humaine soit nécessaire. Prenons l'exemple d'une mine terrestre non télécommandée. Une fois mis en place et armé, l'explosion de l'engin est déclenchée au moyen d'une plaque de pression, d'un fil de trébuchement, etc. Ces engins présentent un niveau de reconnaissance de cible très basique. Par exemple, une mine terrestre actionnée par pression explose quand un minimum de pression (correspondant en général à un poids de 15 kilogrammes) s'exerce sur la plaque de contact – il est donc fort peu probable que la mine soit déclenchée par une souris. Par ailleurs, une telle explosion ne requiert aucune autorisation humaine[11]. Des systèmes d'armes plus complexes (les mines anti-véhicule, par exemple) visent à faire la distinction entre des camions civils et des véhicules militaires tels que des chars[12]. Il est important de ne pas confondre les armes automatisées ou autonomes et les armes opérées à distance. Certes, les systèmes de combat « inhabités » (c'est-à-dire sans pilote à bord) suscitent de grands débats depuis quelque temps. Pourtant, il ne s'agit que de plateformes d'armement opérées à distance, et les problèmes juridiques sont bien plus liés à la manière dont ces systèmes sont utilisés qu'à leurs caractéristiques techniques[13]. Nous verrons qu'il convient de faire une distinction entre armes *automatisées* et armes *autonomes,* et nous examinerons brièvement les principaux problèmes juridiques qui sont associés à chaque type de système d'armement. Pour conclure, nous décrirons dans leurs grandes lignes certaines méthodes d'emploi licite de ces armes.

Armes automatisées[14]

> « Les armes automatisées – ou robots en langage courant – vont plus loin que les systèmes télécommandés. Elles ne sont pas dirigées à distance,

11 Bien sûr, c'est là précisément le problème que peuvent poser les mines terrestres. Les mines terrestres non télécommandées qui sont mises en place dans des zones fréquentées par des civils ne sont pas capables de distinguer les civils des combattants.

12 « Anti-vehicle mines, victim-activation and automated weapons », 2012, disponible sur : http://www.article36.org/weapons/landmines/anti-vehicle-mines-victim-activation-and-automated-weapons/ .

13 Sur la question de savoir comment ces systèmes opérés à distance sont, juridiquement parlant, des systèmes d'armement comme tous les autres et ne constituent pas une catégorie distincte et ne nécessitent pas d'être traités différemment au regard du droit international humanitaire, voir, de façon générale, *Denver Journal of International Law and Policy*, Vol. 39, N° 4, 2011 ; voir aussi Michael Schmitt, Louise Arimatsu et Tim McCormack (dir.), *Yearbook of International Humanitarian Law 2010*, Springer, Vol. 13, 2011.

14 À ne pas confondre avec les armes automatiques, qui sont des armes qui tirent plusieurs fois après l'activation du mécanisme de déclenchement : c'est le cas, par exemple, d'une mitrailleuse qui continue de tirer aussi longtemps que le déclencheur reste activé par le tireur.

> mais fonctionnent de façon autonome et indépendante, une fois lancées. C'est notamment le cas des mitrailleuses SG autonomes, des munitions autodirectrices et de certaines mines terrestres anti-véhicule. Bien que déployés par des humains, ces systèmes vont identifier ou détecter de façon indépendante un type de cible donné puis tirer ou exploser. Une mitrailleuse SG autonome par exemple fera feu ou non après vérification du mot de passe prononcé par un intrus potentiel »[15].

En bref, les armes automatisées sont conçues pour faire feu automatiquement sur une cible quand certains paramètres prédéterminés sont détectés. Les armes de ce type servent trois buts différents. Les mines permettent aux militaires d'interdire une zone donnée sans que les forces soient physiquement présentes. Les mitrailleuses SG autonomes libèrent des capacités de combat et peuvent fonctionner pendant de longues heures en accomplissant une tâche répétitive et fastidieuse sans risquer de sombrer dans le sommeil[16]. Enfin, les munitions autodirectrices offrent la possibilité de « tirer et fuir » et peuvent être considérées comme une extension des armes de type BVR [*beyond visual range* / au-delà de la portée visuelle][17].

Le principal problème juridique que posent les armes automatisées tient à leur capacité de discrimination entre les cibles licites (objectifs militaires), d'une part, et les cibles illicites (personnes civiles et biens de caractère civil), d'autre part[18]. La seconde préoccupation est de savoir quelle attitude adopter face aux blessures et aux dommages que ces armes sont susceptibles de causer incidemment aux personnes civiles et aux biens de caractère civil[19].

En ce qui concerne la capacité de discrimination, il vaut la peine de relever que les armes automatisées ne sont pas une nouveauté. Les mines, les pièges, et même une chose aussi simple qu'un pieu fiché au fond d'une fosse,

15 Jakob Kellenberger, Président du CICR, « Le droit international humanitaire et les nouvelles technologies de l'armement », XXXIV[e] Table ronde sur les sujets actuels du droit international humanitaire, San Remo, 8-10 septembre 2011, Discours d'ouverture, p. 5, disponible sur : http://www.icrc.org/fre/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm. Divers types d'armes automatisées et autonomes existant déjà sont brièvement évoquées (et d'autres références utiles sont mentionnées) dans Chris Taylor, « Future Air Force unmanned combat aerial vehicle capabilities and law of armed conflict restrictions on their potential use », Australian Command and Staff College, 2011, p. 6 (copie dans les dossiers des auteurs).

16 La Corée du Sud met actuellement au point des robots équipés de détecteurs de chaleur et de mouvement afin de repérer des menaces possibles. Dès qu'une menace est détectée, une alerte est envoyée à un centre de commandement, où le système de communication audio ou vidéo des robots peut être utilisé pour déterminer si la cible constitue ou non une menace. En ce cas, l'opérateur peut ordonner au robot d'utiliser son fusil ou son lance-grenades automatique de 40mm. « S. Korea deploys sentry robot along N. Korea border », dans *Agence France-Presse*, 13 juillet 2010, disponible sur : http://www.defensenews.com/article/20100713/DEFSECT02/7130302/S-Korea-Deploys-Sentry-Robot-Along-N-Korea-Border .

17 Une arme dite « amorcée par capteur » ou « à allumage par capteur » est une arme dont le mécanisme d'armement (l'allumage) est intégré à un système de détection de cible (le capteur).

18 *Stricto sensu*, les problèmes tels que celui des tirs fratricides ne relèvent pas du droit international humanitaire. De toute façon, d'autres moyens et méthodes (« blue-force trackers », corridors de sécurité et zones de restriction de tirs) sont adoptés pour réduire les tirs fratricides.

19 Voir *op. cit.*, note 1, art. 51(5)(b) et art. 57(2)(a)(iii) du Protocole additionnel I.

sont autant d'armes qui, une fois en place, n'exigent plus aucune intervention humaine, ni en termes de contrôle ni pour leur utilisation. Certaines de ces armes possèdent également une capacité de discrimination de par la manière dont elles sont conçues. Les mines anti-véhicule, par exemple, sont conçues pour n'exploser que si elles sont activées par un certain poids. La technologie des mines marines a été perfectionnée et aux anciennes mines de contact ont succédé des mines magnétiques et des mines acoustiques. Bien sûr, le problème de ces nouveaux engins est qu'ils ne sont pas capables de distinguer les objectifs militaires des biens de caractère civil qui correspondent aux critères d'activation[20]. L'une des façons de surmonter ce problème consiste à combiner plusieurs mécanismes de déclenchement (capteurs) et d'adapter cette combinaison pour atteindre des navires qui sont davantage susceptibles d'être des bâtiments de guerre ou d'autres cibles légitimes que des navires civils.

Les armes ayant vu augmenter tant leurs capacités que leur portée, il est devenu de plus en plus important de pouvoir effectuer l'identification au combat de l'ennemi à plus grandes distances. La reconnaissance de cibles non coopératives (également appelée « reconnaissance automatique de cible ») est la capacité d'utiliser la technologie pour identifier certaines caractéristiques distinctives du matériel ennemi, sans devoir observer visuellement ce matériel[21]. La combinaison de certaines technologies – telles que celles des radars, des lasers et de certains développements dans le domaine des télécommunications – avec celle des armes de type BVR aboutit à une capacité toujours croissante de déterminer si l'objet détecté est ami, inconnu ou ennemi, puis, le cas échéant, d'engager la cible. Cela dit, chaque avancée ne correspond pas à un problème unique, mais plutôt à « un continuum de problèmes de complexité croissante, allant de la reconnaissance d'une cible simple avec peu de fouillis d'échos jusqu'à la classification de cibles multiples dans un environnement de fouillis d'échos complexe comme par exemple les cibles au sol dans un environnement urbain »[22]. Des travaux de recherche importants sont en cours en vue de produire des systèmes intégrés où le repérage de cibles combinant trois types de capteurs (affectés au renseignement, à la surveillance et à la reconnaissance) se fait sans intervention humaine. Il sera ainsi possible d'obtenir des taux de détection plus élevés, une résolution accrue des images obtenues et, en fin de compte, une meilleure discrimination[23]. Si plusieurs capteurs sont intégrés, l'identification

20 Sauf si la mine est télécommandée.

21 Un exemple réside dans l'utilisation des rayons laser (ou d'un radar millimétrique) pour scanner un objet, suivie de l'utilisation d'algorithmes de traitement d'image pour comparer l'image obtenue aux modèles de cible en trois dimensions qui ont été préchargés. L'identification de la cible peut être basée sur des caractéristiques spécifiques avec jusqu'à 15 cm de résolution à une distance de 1000 mètres. Voir « Laser radar (LADAR) guidance system », Defense Update, 2006, disponible sur : http://defense-update.com/products/l/ladar.htm.

22 « RADAR Automatic Target recognition (ATR) and Non-Cooperative Target Recognition (NCTR) », OTAN, 2010, disponible sur : https://www.cso.nato.int/detail.asp?ID=6299

23 Voir Andy Myers, « The legal and moral challenges facing the 21st century air commander », dans *Air Power Review*, Vol. 10, N° 1, 2007, p. 81, disponible sur : http://www.raf.mod.uk/rafcms/mediafiles/51981818_1143_EC82_2E416EDD90694246.pdf .

peut être jusqu'à 10 fois plus performante et la géolocalisation jusqu'à 100 fois plus précise que dans le cas de capteurs uniques[24].

Dans le cas d'un engin aussi simple qu'une mine terrestre traditionnelle actionnée par pression, le mécanisme de déclenchement est purement mécanique. Si une pression égale ou supérieure à la pression prédéterminée est exercée, le mécanisme de déclenchement est activé et la mine explose. Ce type de mécanisme de détonation n'est pas capable de distinguer par lui-même les civils des combattants (ou d'autres cibles licites). De plus, le risque de causer incidemment des blessures au moment de la détonation ne figure pas parmi les éléments de l'équation « exploser/ne pas exploser ». Il est vrai que ce risque peut être pris en compte dans le cas des mines terrestres télécommandées, mais le mécanisme de détonation est alors d'une nature clairement différente. S'agissant des mines terrestres actionnées par pression, deux moyens principaux permettent de limiter le risque de causer incidemment des dommages : réduire au minimum le souffle de la déflagration et les projections d'éclats, ou ne placer les mines que dans des zones non habitées par des civils ou dont les habitants ont été prévenus de la présence de mines[25].

Le mécanisme de déclenchement des mines est cependant devenu progressivement plus complexe. Par exemple, certaines mines anti-véhicule sont conçues pour pouvoir faire la distinction entre véhicules amis et véhicules ennemis en utilisant un « catalogue de signatures ». Les mines conçues pour n'exploser que contre des cibles militaires et qui sont déployées en tenant compte des limitations prévues par leur conception, répondent aux préoccupations liées à la capacité de discrimination. Pour autant, le risque de causer incidemment des blessures et des dommages aux personnes et aux biens de caractère civil n'est pas entièrement écarté. À notre connaissance, il n'existe aucune arme dont les capteurs et/ou les algorithmes sont conçus pour détecter la présence de civils ou de biens de caractère civil à proximité de « cibles ». Par conséquent, si certaines armes prétendent pouvoir faire la distinction entre biens de caractère civil et objectifs militaires et ne « tirer » que sur des objectifs militaires, aucune de ces armes ne cherche en outre à savoir, avant de « tirer », si des biens de caractère civil se trouvent à proximité des objectifs militaires. Prenons l'exemple hypothétique d'un véhicule militaire qui se déplace à proximité immédiate d'un véhicule civil. Certaines mines terrestres seraient capables de faire la distinction entre les deux types de véhicules et d'exploser uniquement au moment du passage du véhicule militaire ; cependant, le risque de causer incidemment des dommages au véhicule civil ne constitue pas l'un des éléments de données intégrés dans

24 Note d'accompagnement, *Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence*, Bureau du Sous-Secrétaire à la Défense (Acquisition, technologie et logistique), ministère de la Défense des États-Unis, novembre 2008, p. 1.

25 Bien sûr, l'histoire montre que de nombreuses mines terrestres antipersonnel ont été posées soit sans tenir suffisamment compte du risque de victimes civiles, soit – pire encore – en ignorant délibérément ce risque. Par conséquent, une majorité d'États ont convenus d'interdire totalement l'emploi de mines terrestres antipersonnel non télécommandées. Voir CICR, « Mines terrestres antipersonnel », 2012, disponible sur : http://www.icrc.org/fre/war-and-law/weapons/anti-personnel-landmines/index.jsp.

l'algorithme « exploser/ne pas exploser ». D'un point de vue juridique, cela ne signifie pas que l'emploi de ces armes automatisées doit être interdit, mais que des restrictions doivent être imposées quant à la façon dont ces armes devraient être employées sur le champ de bataille.

Au problème de la capacité de discrimination vient donc s'ajouter celui du risque de causer incidemment des blessures aux personnes civiles et des dommages aux biens de caractère civil. Dans le cas des armes automatisées, deux moyens principaux permettent de gérer ce problème, à savoir : premièrement, contrôler la manière dont ces armes sont utilisées (par exemple, dans des zones où il est peu probable de trouver des personnes civiles ou des biens de caractère civil) et/ou, deuxièmement, maintenir une surveillance humaine. Ces deux points seront examinés ci-dessous, dans la section intitulée « Méthodes d'emploi licite des armes automatisées et des armes autonomes ». Une troisième option consiste à accroître la « capacité décisionnelle » du système d'armement, ce qui nous amène à parler maintenant des armes autonomes.

Armes autonomes

Les systèmes d'armement autonomes sont une combinaison sophistiquée de capteurs et de logiciels qui « peuvent analyser ou adapter leur fonctionnement en fonction d'un changement de circonstances »[26]. Une arme autonome est capable de surveiller une zone d'intérêt, de rechercher des cibles, d'identifier des cibles appropriées, de poursuivre une cible détectée (c'est-à-dire de l'attaquer) et, enfin, de faire un rapport sur le point d'impact de l'arme[27]. Ce type d'arme peut aussi jouer un rôle dans les domaines des renseignements, de la surveillance et de la reconnaissance. Par exemple, une arme autonome potentielle – connue sous le sigle WASAAMM pour *Wide Area Search Autonomous Attack Miniature Munition :*

> [s]erait un missile de croisière miniature intelligent, capable de rester en attente au-dessus d'une cible et de rechercher une cible spécifique, améliorant de manière significative le ciblage de cibles mouvantes ou éphémères. Une fois la cible acquise, le WASAAMM peut soit l'attaquer soit émettre un signal demandant l'autorisation de l'attaquer[28].

Les armes telles que le WASAAMM posent un certain nombre de problèmes techniques et juridiques[29]. La plupart des éléments de conception d'une telle arme

26 J. Kellenberger, *op. cit.*, note 15, p. 5.

27 Chris Anzalone, « Readying air forces for network centric weapons », 2003, diapositive n° 9, disponible sur : http://www.dtic.mil/ndia/2003targets/anz.ppt.

28 US Air Force, « Transformation flight plan », 2003, Annexe D, p. 11, disponible sur : http://www.au.af.mil/au/awc/awcgate/af/af_trans_flightplan_nov03.pdf [Traduction CICR].

29 Myers examine aussi certains aspects moraux comme, par exemple, la question de savoir s'il est « moralement correct qu'une machine soit capable de prendre une vie ». Voir A. Myers, *op. cit.*, note 23, pp. 87-88 [Traduction CICR]. Voir aussi CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, Rapport présenté à la XXXI[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge, 2011, p. 42, disponible sur :

ont toutes les chances de pouvoir être mis au point dans les vingt-cinq prochaines années ; par contre, la partie « autonome » de l'arme se heurte encore à de sérieux problèmes techniques. De plus, des questions restent en suspens quant au respect du droit international humanitaire et des règles d'engagement qui découlent de ces obligations[30]. Bien sûr, si le mode d'opération du WASAAMM était tel que le missile enverrait toujours un signal pour obtenir l'autorisation d'attaquer[31], cela réduirait de manière significative à la fois les difficultés techniques et les problèmes liés au respect du droit international humanitaire (et des règles d'engagement), mais pourrait-on, en ce cas, parler d'arme « autonome » ?

Dans un domaine lié aux armes autonomes, des assistants artificiels de renseignement font actuellement l'objet de travaux de recherche et de développement afin d'aider les opérateurs humains à écourter la boucle OODA (Observer, Orienter, Décider, Agir). Le but de ces systèmes d'aide à la décision est de résoudre le problème défini de la manière suivante :

> « des gains de temps en matière de collecte et de distribution d'informations peuvent être obtenus par le biais d'une mise en réseau correctement mise en œuvre; par contre, l'analyse des informations, la compréhension et la prise de décisions risquent de constituer de graves goulets d'étranglement et de ralentir le tempo opérationnel »[32].

Le public n'a accès qu'à très peu d'informations sur la manière dont ces systèmes d'aide à la décision pourraient opérer dans une zone de ciblage.

Ainsi, la question fondamentale se pose dans les termes suivants : « comment doit-on utiliser le traitement informatique pour automatiser des tâches traditionnellement assumées par des humains ? »[33]. En matière de reconnaissance automatique de cible, l'utilisation de capteurs couplés avec la puissance de calcul des ordinateurs afin de scanner périodiquement un terrain d'aviation pour détecter des changements, et déclencher ainsi une intervention humaine, a donné de

http://www.icrc.org/fre/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-fr.pdf . Les enjeux d'ordre moral sont aussi examinés dans Kenneth Anderson et Matthew Waxman, « Law and ethics for robot soldiers », dans *Policy Review*, 2012, disponible sur : http://ssrn.com/abstract=2046375. Voir, de façon générale, Peter Singer, « The ethics of killer applications: why is it so hard to talk about morality when it comes to new military technology? », dans *Journal of Military Ethics*, Vol. 9, N° 4, 2010, pp. 299-312.

30 *Ibid.*

31 Par exemple, le robot « Fire Shadow » du Royaume-Uni possédera une fonction « Man In The Loop (MITL) » qui permettra à un opérateur humain de prendre la main sur le guidage de l'arme et de modifier la trajectoire de l'arme ou d'abandonner l'attaque en cours et de revenir au mode de veille quand les conditions sont telles que des forces amies sont en danger, quand les conditions qui prévalent ne sont pas conformes aux règles d'engagement, ou quand une attaque pourrait causer des dommages collatéraux excessifs », voir « Fire Shadow: a persistent killer », Defense Update, 2008, disponible sur : http://defense-update.com/20080804_fire-shadow-a-persistent-killer.html [Traduction CICR] .

32 Shyni Thomas, Nitin Dhiman, Pankaj Tikkas, Ajay Sharma et Dipti Deodhare, « Towards faster execution of the OODA loop using dynamic décision support », dans Leigh Armistead (éd.), *The 3rd International Conference on Information Warfare and Security*, 2008, p. 42, disponible sur : http://academic-conferences.org/pdfs/iciw08-booklet-A.pdf [Traduction CICR] .

33 *Op. cit.*, note 24, p. 47.

meilleurs résultats que l'utilisation de capteurs tels que, par exemple, les radars à synthèse d'ouverture[34]. Une difficulté certaine tient à ce que le droit relatif au ciblage s'énonce d'ordinaire non pas sous forme de formules précises, comportant des variables en nombre limité, mais en termes généraux évoquant toute une gamme de faits infiniment variables. Voilà précisément la raison pour laquelle le jugement d'un commandant est souvent requis afin de déterminer si une attaque peut être lancée contre tel objectif ou telle personne de manière licite[35]. Comme le relève Taylor, c'est cette « nature extrêmement contextuelle » du ciblage qui empêche d'établir une simple liste de cibles licites[36]. Néanmoins, si un commandant était prêt à renoncer à certaines capacités théoriques, il pourrait être envisagé – dans un conflit armé particulier – de dresser la liste d'un sous-ensemble d'objectifs pouvant à tout moment être pris pour cible. Tant que la liste est tenue à jour et revue, il sera certainement possible, à tout moment donné, dans un conflit armé, de décider que les véhicules militaires, les sites radar, etc, peuvent être pris pour cible. En d'autres termes, un commandant pourrait choisir de limiter la liste de cibles relevant de la reconnaissance automatique, et de dresser une courte liste de cibles qui, par leur nature, sont clairement des objectifs militaires. Ce faisant, le commandant renoncerait cependant à soumettre à la reconnaissance automatique d'autres cibles dont seul un jugement plus nuancé permettrait de déterminer le statut d'objectifs militaires en raison de leur emplacement, de leur destination ou de leur utilisation[37].

L'étape suivante nous conduit à aller au-delà d'un système qui, de fait, est programmé pour fonctionner à la manière d'un commandant et qui apprenne quelle est la nature des opérations militaires et comment appliquer le droit aux activités de ciblage. À mesure que les systèmes de télécommunications deviennent plus complexes, « non seulement ils transmettent des informations, mais ils ont la capacité de collationner, analyser, diffuser et afficher des informations en prévision d'opérations militaires, et pendant la conduite de celles-ci »[38]. Quand un système est « utilisé pour analyser les données relatives aux cibles, puis pour fournir une solution ou un profil concernant cette cible»[39], alors « le système

34 *Ibid.*, pp. 47-48. Les systèmes automatiques de reconnaissance de cible ont fonctionné en laboratoire ; par contre, ils ne se sont pas révélés fiables après leur mise en service, quand ils ont eu à traiter des données réelles et non plus des « données contrôlées irréalistes pour évaluer la performance des algorithmes », *ibid.*, pp. 47 et 53 [Traduction CICR]. Bien que datant un peu, un article explique comment fonctionne ce type de reconnaissance de cible : Paul Kolodzy, « Multidimensional automatic target recognition system evaluation », dans *The Lincoln Laboratory Journal*, Vol. 6, N° 1, 1993, p. 117.

35 Voir C. Taylor, *op. cit.*, note 15, p. 9. Voir, de façon générale, Ian Henderson, *The Contemporary Law of Targeting: Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I*, Martinus Nijhoff, Leiden, 2009, pp. 45-50.

36 Voir C. Taylor, *ibid.*, p. 9 ; voir aussi I. Henderson, *ibid.*, pp. 49-50.

37 Voir *op. cit.*, note 1, art. 52(2) du Protocole additionnel I.

38 Voir J. McClelland, *op. cit.*, note 1, p. 405 [Traduction CICR]. Il faudrait éviter de minimiser l'importance des problèmes techniques (qui peuvent être aussi simples que les normes relatives aux métadonnées pour les données collectées par un capteur et la largeur de bande disponible pour la transmission de données mais peuvent devenir bien plus complexes), en particulier en ce qui concerne les données provenant de plusieurs capteurs. Voir, de façon générale, *Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence, op. cit.*, note 24, pp. 1-9.

39 Voir J. McClelland, *op. cit.*, note 1, p. 405 [Traduction CICR].

devrait raisonnablement correspondre à la signification de l'expression *moyens et méthodes de guerre,* car il constituerait une partie intégrante du processus de décision concernant le ciblage»[40].

À quoi pourrait donc ressembler un système n'exigeant pas de programmation détaillée, mais qui serait capable d'apprendre ? Supposons qu'un système d'intelligence artificielle scanne l'espace de combat à la recherche de cibles potentielles : nous le baptiserons AITRS (*Artificial Intelligence Target Recognition System*, ou Système d'intelligence artificielle pour la reconnaissance de cible). L'AITRS n'aurait pas besoin d'être préprogrammé : il apprendrait les caractéristiques de certaines cibles dont l'attaque a été précédemment validée[41]. Au fil du temps, l'AITRS serait de plus en plus capable d'exclure les cibles de faible probabilité, de repérer différents capteurs et d'appliquer des algorithmes pour déjouer les manœuvres de l'ennemi (camouflage, contre-mesures, etc.). Dans un premier cas, le processus aboutit à la présentation par l'AITRS à un opérateur humain d'une vue simplifiée de la zone de combat, n'indiquant que des cibles probables et leurs caractéristiques ; ces données sont ensuite analysées et une décision humaine doit intervenir (attaquer/ne pas attaquer). De façon significative, cependant, toutes les « informations brutes » (imagerie, imagerie multi-spectrale, enregistrement vocal des conversations interceptées, etc.) sont disponibles pour être examinées par un humain. Dans un deuxième cas, alors que ce même système d'intelligence artificielle pour la reconnaissance de cible présente à un opérateur humain une vue simplifiée de la zone de combat, indiquant des cibles probables identifiées, afin d'obtenir une autorisation d'attaquer, ce ne sont pas des « informations brutes », mais plutôt des données déjà analysées qui sont présentées au décideur humain[42]. Par exemple, l'opérateur humain pourrait voir apparaître sur un écran un symbole représentant un véhicule à moteur et accompagné des mentions suivantes :

- probabilité de présence à bord d'un humain : 99 % ;
- probabilité de concordance (corps) avec le colonel John Smith[43] : 75 % ;
- probabilité de concordance (voix) avec le colonel John Smith : 90 %[44].

40 *Ibid.*, p. 406.

41 Voir K. Anderson et M. Waxman, *op. cit.*, note 29, p. 10.

42 « Le fait de traiter automatiquement les données du capteur – soit pour réduire le volume d'informations essentielles et disposer d'un plus petit paquet de données soit pour décider d'aller ou non de l'avant – pourrait améliorer le temps de réaction », dans *Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence, op. cit.*, note 24, p. 43 [Traduction CICR].

43 Partons de l'hypothèse que le colonel Smith figure sur la liste de cibles prioritaires et fait l'objet d'une attaque licite (le problème des blessés, des malades, des personnes qui se rendent ou qui se trouvent hors de combat pour toute autre raison ainsi que le problème des dommages collatéraux n'étant pas pris en compte). Ce type d'attaque repose sur l'identification d'une cible, à savoir le colonel Smith. Ceci contraste avec les attaques basées sur des caractéristiques de la cible associées aux « forces ennemies » (déchargement d'explosifs, rassemblement en certains lieux et autres types de comportement). La deuxième attaque est une « frappe signature », la première est une « frappe personnalité ». Voir Greg Miller, « CIA seeks new authority to expand Yemen drone campaign », dans *The Washington Post*, 19 avril 2012, disponible sur : http://www.washingtonpost.com/world/national-security/cia-seeks-new-authority-to-expand-yemen-drone-campaign/2012/04/18/gIQAsaumRT_story.html.

44 Voir aussi l'exemple cité par A. Myers, ainsi que l'analyse du repérage par systèmes multicapteurs. A. Myers, *op. cit.*, note 23, p. 84.

Enfin, dans un troisième cas, c'est l'AITRS lui-même qui décide de lancer ou non une attaque : s'il est relié à un système d'armement, nous avons affaire à un système d'armement autonome.

Il ne semble pas que la technologie actuelle permette de programmer une machine afin qu'elle effectue les évaluations compliquées visant à déterminer si une attaque donnée serait licite alors que des dommages collatéraux sont prévus[45]. De fait, l'on pourrait même se demander par où commencer : en effet, mettre en balance l'avantage militaire escompté et les dommages collatéraux attendus équivaut à comparer des pommes et des oranges[46]. À l'heure actuelle, cela signifierait que tout système d'armement de ce type devrait être employé de manière telle que le risque de dommages collatéraux soit réduit[47]. Il est toutefois probable qu'un véritable AITRS ayant initialement fonctionné sous supervision humaine soit capable – en se basant sur les décisions prises par ses opérateurs humains – d'« apprendre » quels dommages collatéraux sont acceptables ou inacceptables[48].

Comme nous l'avons relevé dans la note de bas de page n° 46, les évaluations des dommages collatéraux ne consistent pas seulement à calculer et à comparer des chiffres (fonction parfaitement adaptée aux ordinateurs actuels). Il s'agit au contraire de procéder à une évaluation clairement qualitative, alors que les éléments que l'on compare ne sont pas même semblables. Comment une machine pourrait-elle un jour effectuer de tels jugements ? Peut-être pourrait-elle le faire non pas grâce à une programmation directe, mais plutôt en suivant la voie de l'intelligence artificielle? Non content d'apprendre ce que sont des cibles licites, notre hypothétique AITRS apprendrait donc aussi comment réaliser une évaluation de proportionnalité en procédant comme les humains, c'est-à-dire par le biais de l'observation, de l'expérience, de l'apprentissage (par le jeu des essais et des erreurs, dans les jeux de stratégie militaire, etc.). Un AITRS qui échoue à poser des jugements raisonnables (de l'avis du personnel chargé de sa formation) pourrait être traité comme le serait un jeune officier qui ne parvient jamais

45 CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, *op. cit.*, note 29, pp. 39-40 ; voir aussi William Boothby, *Weapons and the Law of Armed Conflict*, Oxford University Press, Oxford, 2009, p. 233.

46 Voir I. Henderson, *op. cit.*, note 35, pp. 228-229. De nombreuses facettes des opérations militaires exigent que les commandants exercent leur jugement – notamment, quand ils sont confrontés à certains problèmes juridiques. Après avoir déterminé l'avantage militaire attendu d'une attaque (qui ne constitue pas, en elle-même, une quantité exacte) lancée contre un centre de commandement et de contrôle, et après avoir estimé les pertes civiles et les dommages aux biens civils qui seraient causés incidemment lors de cette attaque, il faut comparer ces deux facteurs d'une manière ou d'une autre. L'évaluation ne sera sans doute ni objective ni mathématique ; elle aura clairement un caractère subjectif et sera différente d'une personne à l'autre. Nous dirons à ce propos que le fait d'interpréter et de respecter certains aspects du droit international humanitaire relève en partie de l'art – et non pas seulement de la pure science.

47 W. Boothby, *op. cit.*, note 45, p. 233.

48 Pour un point de vue contraire sur la question, voir Markus Wagner, « Taking humans out of the loop : implications for international humanitartian law », dans *Journal of Law Information and Science*, Vol. 21, 2011, p. 11, disponible sur : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1874039. Wagner conclut que les systèmes autonomes ne seront jamais capables de respecter le principe de proportionnalité.

tout à fait à gagner ses galons (peut-être resterait-il en fonction, mais sans être investi d'aucun pouvoir de décision). Par contre, un AITRS ayant fait ses preuves – en matière de théorie et dans des exercices sur le terrain – pourrait être promu et se voir accorder des degrés croissants d'autonomie, etc.

Un autre problème technique se pose, à savoir le manque de clarté de la norme d'identification requise pour déterminer si une personne ou un objet constitue une cible licite. La norme énoncée par le Tribunal pénal international pour l'ex-Yougoslavie est un « motif raisonnable de croire »[49]. Dans leurs règles d'engagement, deux États au moins ont adopté la norme de la « certitude raisonnable »[50]. Une troisième approche, présentée dans le *Manuel de San Remo sur les règles d'engagement*, consiste à exiger l'identification de la cible par des moyens visuels et/ou par certains moyens techniques[51]. Tant le commandant qui autorise le déploiement d'une arme autonome que l'opérateur qui en assure la surveillance devront savoir quelle norme a été adoptée pour respecter le droit international et l'ensemble des règles d'engagement spécifiques à chaque opération. À l'exigence d'un niveau particulier de certitude (le « motif raisonnable de croire » ou la « certitude raisonnable ») peut aussi venir s'ajouter l'exigence que l'identification se fasse par des moyens visuels et/ou par certains moyens techniques.

Une norme d'identification ne pourra sans doute être codée[52] dans un programme informatique que si elle est « traduite » en une confirmation quantifiable, exprimée sous la forme d'une probabilité statistique. Par exemple, le « motif raisonnable de croire » ne devrait plus être un concept subjectif, mais se transformer en quantité objective et mesurable (comme, par exemple, « un degré de confiance de 95 % »). De cette valeur repère et de l'expérience de terrain (y compris les données historiques) émergerait une équation empirique permettant de profiler une cible potentielle. De nouvelles données relatives à l'espace de bataille seraient ensuite comparées afin de quantifier (évaluer) la force de la corrélation par rapport au degré de confiance requis (dans le présent exemple, 95 %, ou davantage). Il convient cependant de quantifier – en tant que critère de validation distinct – l'incertitude des mesures associées aux données sur l'espace de bataille qui sont fournies par les capteurs.

49 « La Chambre de première instance pense que pareil bien [normalement affecté à un usage civil] ne doit pas être l'objet d'une attaque lorsqu'il n'y a pas lieu de croire, dans la situation où se trouve la personne envisageant l'attaque, et compte tenu des informations dont elle dispose, que ce bien est utilisé pour apporter une contribution effective à l'action militaire », TPIY, *Le Procureur c/ Stanislav Galic*, Affaire n° IT-98-29-T, Jugement et opinion (Chambre de première instance), 5 décembre 2003, para. 51.

50 International and Operational Law Department: The Judge Advocate General's Legal Centre & School (US Army), *Operational Law Handbook 2012,* « CFLCC ROE Card », p. 103, disponible sur: http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2011.pdf; CICR, *Customary IHL,* « Philippines : Practice Relating to Rule 16. Target Verification», 2012, disponible sur: http://www.icrc.org/customary-ihl/eng/docs/v2_cou_ph_rule16.

51 Voir les exemples de règles de la Série 3, intitulée « Identification des objectifs », dans Institut international de droit humanitaire, *Manuel de San Remo sur les règles d'engagement*, 2009, pp. 41-42, disponible sur: http://www.iihl.org/iihl/Documents/Sanremo%20ROE%20Handbook%20(French).pdf.

52 Là encore, seule l'intelligence artificielle permettrait d'adopter une méthode sans codage.

Par exemple, considérons que dans certaines circonstances opérationnelles une incertitude de mesure ait pour résultat une incertitude de plus ou moins 1 % et que, dans d'autres circonstances opérationnelles, l'incertitude soit de plus ou moins 10 %. Dans le premier cas, pour obtenir une certitude de 95 %, la corrélation ne devrait pas être inférieure à 96 %. Dans le second cas, toutefois, le degré de confiance requis ne pourrait jamais être atteint, l'incertitude de mesure empêchant d'atteindre le degré de confiance requis (95 %)[53].

Méthodes d'emploi licite des armes automatisées et des armes autonomes

« La plupart des armements en tant que tels ne seraient pas illicites ; la licéité de leur utilisation dans des conflits dépend des circonstances et de la manière dont ces technologies sont utilisées »[54]. Cela s'applique également aux armes automatisées et aux armes autonomes, à moins que ces armes ne soient un jour interdites par un traité (comme l'ont été, par exemple, les mines terrestres antipersonnel non télécommandées). Il existe divers moyens d'assurer l'emploi licite de telles armes.

> « [L]'absence de ce que l'on nomme ' un homme dans la boucle de surveillance' ne signifie pas nécessairement qu'il est impossible d'employer l'arme en accord avec le principe de distinction. Les phases de détection, d'identification et de reconnaissance de cible peuvent s'appuyer sur des données fournies par des capteurs capables de faire la distinction entre cibles militaires et cibles non militaires. En combinant plusieurs capteurs, la capacité de discrimination de l'arme est fortement accrue »[55].

Une méthode permettant de réduire le problème de la reconnaissance de cible et de la programmation consiste à ne pas essayer de mettre en œuvre toute la gamme des options de ciblage prévues par le droit. Par exemple, un système de reconnaissance de cible pourrait être programmé pour rechercher uniquement des cibles de haute priorité (systèmes mobiles de défense aérienne et lanceurs de missiles sol-sol, par exemple). Ces cibles sont, par nature, des objectifs militaires et sont donc relativement plus faciles à programmer en tant que cibles licites que des objets qui deviennent des objectifs militaires de par leur emplacement, destination ou utilisation[56]. Ces cibles pouvant être de haute priorité, le logiciel de ciblage pourrait être programmé de telle sorte que seules ces cibles soient

53 Dans le second cas, le système de ciblage risquerait d'entraîner le repérage par d'autres capteurs ou par un opérateur humain ; il serait uniquement programmé de manière à ne pas autoriser l'emploi d'une arme autonome.

54 Philip Spoerri, « Table ronde sur les nouvelles technologies de l'armement et le DIH – conclusions », dans *XXXIV^e table ronde sur les sujets actuels du droit international humanitaire*, San Remo, 8-10 septembre 2011, disponible sur : http://www.icrc.org/fre/resources/documents/statement/new-weapon-technologies-statement-2011-09-13.htm.

55 J. McClelland, *op. cit.*, note 1, pp. 408-409 [Traduction CICR].

56 Voir Lockheed Martin, « Low cost autonomous attack system », dans *Defense Update,* 2006, disponible sur : http://defense-update.com/products/l/locaas.htm.

attaquées, mais qu'une autre cible également licite mais de plus faible priorité et qui aurait été détectée la première, ne soit pas attaquée[57]. Si aucune cible de haute priorité n'est détectée, l'attaque pourrait être annulée ou être poursuivie mais contre d'autres cibles constituant par nature des objectifs militaires. L'adoption de ce type d'approche atténuerait la nécessité de résoudre des problèmes aussi difficiles que celui-ci : comment doit-on programmer un système autonome de telle sorte qu'il n'attaque pas une ambulance sauf si elle a perdu sa protection contre l'attaque du fait de son emplacement, de sa destination ou de son utilisation[58] ?

Une autre sauvegarde consisterait notamment à faire en sorte que l'arme soit « surveillée » et contrôlée à distance, ce qui permettrait de la désactiver si elle est jugée potentiellement dangereuse pour des objectifs non militaires[59]. Une telle surveillance n'aurait d'utilité sur le plan juridique (et opérationnel) que si les opérateurs procédaient à une véritable analyse, et ne se contentaient pas de faire confiance aux données fournies par le système[60]. En d'autres termes, l'opérateur doit « ajouter de la valeur ». Par exemple, s'il avait sous les yeux une icône indiquant qu'une cible hostile a été identifiée, l'opérateur ajouterait de la valeur au processus en considérant séparément les données, en observant la zone cible afin de détecter l'éventuelle présence de civils, ou en adoptant toute autre démarche qui ne consiste pas uniquement à autoriser ou à poursuivre une attaque sur la base de l'analyse fournie par le logiciel de ciblage. En d'autres termes, l'opérateur effectue une seconde vérification que la cible elle-même peut faire l'objet d'une attaque licite, ou s'assure que les autres précautions dans l'attaque sont prises (précautions consistant à réduire au minimum les dommages collatéraux, à veiller à ce que tout dommage collatéral qui subsiste respecte le principe de proportionnalité, à lancer un avertissement aux civils s'il y a lieu, etc.). Un problème se poserait si l'opérateur recevait d'importants volumes de données[61] car, en ce cas, sa capacité d'assurer une supervision de qualité risquerait d'être compromise par la surabondance d'informations[62]. L'un des moyens de gérer ce problème consisterait à programmer le logiciel de ciblage de manière telle qu'il ne donne la recommandation de tir que si la zone cible est exempte

57 Par exemple, un char T-72 pourrait être détecté mais ignoré, car constituant une cible de faible priorité; la procédure se poursuivrait en mode de recherche jusqu'au moment où un lance missile sol-air mobile SA-8 serait détecté et intercepté, *ibid.*

58 En partant de l'hypothèse que toutes les cibles de haute priorité sont clairement de nature militaire et qu'il serait donc plus facile de programmer des logiciels de reconnaissance de manière à ce qu'ils identifient ce type de cibles. Si des cibles de haute priorité étaient des ambulances employées abusivement comme véhicules de commandement et de contrôle, les problèmes de programmations subsisteraient. Voir *op. cit.*, note 37, ainsi que le texte d'accompagnement.

59 J. McClelland, *op. cit.*, note 1, pp. 408-409.

60 Voir *Report of Defense Science Board Task Force on Patriot System Performance: Report Summary*, Bureau du Sous-Secrétaire à la Défense (Acquisition, technologie et logistique), 2005, p. 2.

61 Ce cas se présenterait soit si un système unique devait traiter et afficher de gros volumes de données, soit si un opérateur unique devait surveiller de multiples systèmes.

62 CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains, op. cit.*, note 29, p. 39.

d'objectifs non militaires[63]. Dans d'autres circonstances, le logiciel de ciblage pourrait simplement détecter la présence d'une cible et d'objets non militaires, et de fournir non pas une recommandation de tir mais uniquement une solution de tir. En d'autres termes, le logiciel de ciblage identifierait la manière dont une cible donnée pourrait être frappée, mais resterait neutre sur la question de savoir si l'attaque doit ou non être poursuivie ; ainsi, le logiciel indiquerait clairement à l'opérateur qu'il existe d'autres éléments à prendre en compte avant le tir.

Deux autres aspects juridiques des armes automatisées et des armes autonomes (ainsi que des armes opérées à distance) appellent un examen plus approfondi. Ce sont, d'une part, les règles relatives à la légitime défense[64] et, d'autre part, la manière de tenir compte des risques courus par ses propres forces lors de l'évaluation de l'avantage militaire et des dommages collatéraux attendus d'une attaque.

La question de la légitime défense comporte deux aspects : la légitime défense nationale (c'est-à-dire, principalement, ce qu'un État peut faire en réponse à une attaque) et la légitime défense individuelle (c'est-à-dire, principalement, ce qu'un individu peut faire en réponse à une attaque)[65]. Avant qu'un conflit armé ne commence, le premier emploi illicite de la force contre un navire de guerre et un aéronef militaire d'un État peut être considéré comme équivalant à une attaque armée contre cet État, qui peut ainsi invoquer le droit de légitime défense nationale. La conclusion serait-elle la même si aucun équipage ne s'était trouvé à bord des navires de guerre ou des aéronefs militaires attaqués ? Imaginez une attaque lancée contre un navire de guerre qui, pour une raison quelconque, n'avait à son bord aucun membre de l'équipage au moment de l'attaque. Quand un navire de guerre est attaqué, qu'est-ce qui est important sur le plan juridique ? Est-ce simplement le fait qu'il s'agit d'un bâtiment militaire battant pavillon de l'État ? Est-ce le fait que toute attaque contre le navire de guerre risque aussi de mettre en danger l'équipage du navire ? Est-ce la combinaison de ces deux éléments ?

Deuxièmement, considérons les différentes sources juridiques régissant l'emploi de la force létale. Généralement parlant, la légitime défense individuelle permet à la personne A d'employer la force létale contre la personne B quand la personne B menace la vie de la personne A[66]. Le fait que les personnes A et B soient ou non des soldats ennemis qui s'affrontent importe peu. Si nous nous plaçons maintenant du point de vue du droit international humanitaire, le soldat A est autorisé à employer la force létale contre le soldat B simplement parce que le soldat B est un ennemi[67]. Il n'est pas nécessaire que le soldat B menace

63 J. McClelland, *op. cit.*, note 1, pp. 408-409.

64 Conversations entre Patrick Keane et Ian Henderson, 2011-2012.

65 Dans ce contexte, la légitime défense individuelle englobe aussi le fait de défendre une tierce partie contre une attaque illicite.

66 Le droit pénal interne varie d'une juridiction à l'autre, et la question est plus nuancée que cette simple explication.

67 À condition que le soldat B soit hors de combat. Il serait aussi licite, au regard du droit international humanitaire, que le soldat A tire sur la personne B s'il s'agissait d'un civil qui participe directement aux hostilités, mais l'espace ne nous permet pas d'aller plus loin dans l'exploration de ce thème.

directement le soldat A. De fait, le soldat B pourrait être endormi et le soldat A pourrait être en train d'opérer un aéronef armé piloté à distance. Néanmoins, le soldat A doit s'assurer, conformément à la norme juridique applicable, que la cible est bien un soldat ennemi. L'identification, non la menace, est ici ce qui compte avant tout. Pourtant, pendant les briefings sur les règles d'engagement, il est enseigné aux membres des forces armées qu'en période de conflit armé, ils peuvent non seulement faire feu sur un ennemi identifié, mais que rien, dans le droit international humanitaire (ni, d'ailleurs, dans aucun autre corpus juridique) ne les empêche de retourner le feu contre un contact non identifié[68] dans le cadre de la légitime défense individuelle[69]. Ce mantra bien connu ne peut pas être répété tel quel dans les briefings des opérateurs d'engins télépilotés. En toutes circonstances, sauf les plus exceptionnelles, l'opérateur d'un engin inhabité ne se trouvera pas personnellement mis en danger si l'engin est la cible de tirs. Cette question devra être soigneusement examinée par les rédacteurs des règles d'engagement et par les commandants militaires. En effet, de manière générale, le fait de retourner le feu pour protéger uniquement le matériel (et non des vies humaines) serait illégal selon le paradigme de la légitime défense individuelle[70]. Il en va différemment du paradigme du droit international humanitaire qui autoriserait sans doute l'emploi de la force létale pour protéger certains types de biens et de matériel contre l'attaque en invoquant l'argument selon lequel quiconque attaque les biens et le matériel est nécessairement soit un soldat ennemi, soit un civil qui participe directement aux hostilités[71].

De la même façon, comment traiter en droit international humanitaire un engin inhabité (télépiloté) lorsque l'on estime que l'« avantage militaire » attendu d'une attaque n'est pas évident? Certes, le risque couru par les assaillants est un élément qui peut légitimement être considéré comme faisant partie de l'évaluation de l'avantage militaire[72]; traditionnellement, cependant, ce risque a été considéré comme s'appliquant aux combattants, et non pas au matériel militaire. Il est effectivement logique que le risque de perte de matériel militaire soit aussi un élément à prendre en compte, mais en le considérant clairement comme moins important que le risque de pertes en vies humaines au sein de la population civile.

68 « Non identifié » car on ignore si la personne en train de tirer est un soldat ennemi, un civil, etc. L'exigence d'identifier la source (c'est-à-dire la localisation) de la menace demeure néanmoins.

69 Le concept de « légitime défense de l'unité » apporte peu à la présente analyse, car il s'agit d'une combinaison mêlant à la fois légitime défense nationale et légitime défense individuelle.

70 Le paradigme juridique de la légitime défense individuelle peut être invoqué pour protéger le matériel dans les cas où la perte de ce matériel mettrait directement des vies en danger.

71 En d'autres termes, aussi longtemps que je pense disposer d'au moins un argument juridique pour utiliser la force létale contre une *personne* (comme, par exemple, un ennemi combattant ou un civil qui participe directement aux hostilités), je n'ai pas à déterminer qui relève réellement de quelle catégorie. L'espace ne nous permet pas d'analyser pleinement ce point, ni une autre question intéressante, à savoir l'utilisation de la force pour protéger le matériel au nom de l'intérêt sécuritaire national en situation de légitime défense nationale en dehors d'un conflit armé.

72 I. Henderson, *op. cit.*, note 35, p. 199.

Pour conclure, nous dirons que le commandant a la responsabilité juridique de « veiller à ce que toutes les précautions utiles soient prises dans l'attaque »[73]. Quel que soit l'éloignement, dans le temps ou dans l'espace, du moment du lancement d'une attaque, la responsabilité individuelle et la responsabilité de l'État incombent aux personnes qui autorisent l'emploi d'un système d'armement autonome[74]. Il convient de relever que cela ne signifie pas qu'un commandant doit être automatiquement tenu responsable si quelque chose tourne mal. En temps de guerre, des accidents surviennent. La question qui se pose est de savoir qui pourrait être déclaré responsable, et non pas qui est coupable.

L'analyse qui précède a été centrée sur la cible visée par une arme. L'analyse qui suit portera sur les armes émergentes, qui mettent en relief le problème juridique de l'effet des armes, même quand la cible est une cible licite.

L'effet des armes

Armes à énergie dirigée

Les armes à énergie dirigée (ou « armes à faisceau d'énergie dirigée ») utilisent le spectre électromagnétique (en particulier de l'ultraviolet à l'infrarouge ainsi que la radiofréquence, y compris les micro-ondes) ou les ondes acoustiques pour mener des attaques[75]. En tant que moyen d'affaiblir la capacité de combat de l'ennemi, les armes à énergie dirigée peuvent être employées directement contre le personnel et le matériel de l'ennemi, ou indirectement en tant qu'armes anti-capteurs. Par exemple, les systèmes à laser pourraient être employés en tant qu'éblouisseurs dirigés contre la vision humaine (assistée ou non), les capteurs à infrarouge, et les capteurs spatiaux ou aériens[76]. Ces systèmes pourraient également être utilisés comme armes anti-matériel[77]. Les micro-ondes de forte puissance peuvent être employées contre les composants électroniques et l'équipement de télécommunications. Les lasers et les radars sont aussi employés pour détecter et suivre des cibles ainsi que pour fournir un guidage de cible à d'autres armes conventionnelles.

73 C. Taylor, *op. cit.*, note 15, p. 12 [Traduction CICR].

74 P. Spoerri, *op. cit.*, note 54.

75 Les armes à particules font aussi l'objet de recherches mais elles semblent aujourd'hui rester dans le champ de la théorie – voir Federation of American Scientists, « Neutral particle beam », 2012, disponible sur : http://www.fas.org/spp/starwars/program/npb.htm ; voir aussi Carlo Popp, « High energy laser directed energy weapons », 2012, disponible sur : http://www.ausairpower.net/APA-DEW-HEL-Analysis.html. Pour un bon survol de la question des armes à énergie dirigée dites « non létales » (y compris les armes acoustiques), voir Neil Davison, *« Non Lethal » Weapons*, Palgrave MacMillan, Basingstoke, 2009, pp. 143-219.

76 Des systèmes à laser pourraient être employés comme « éblouisseurs » contre des capteurs spatiaux ou aériens et les micro-ondes de forte puissance peuvent être employées contre les composants électroniques, voir *Defense Science Board Task Force on Directed Energy Weapons*, Bureau du Sous-Secrétaire à la Défense (Acquisition, technologie et logistique), ministère de la Défense des États-Unis, décembre 2007, pp. 2, 11 et 13.

77 Notamment contre des missiles et des équipements de déminage, ainsi qu'en tant qu'armes antisatellites, *ibid.*, p. 19.

Quand des armes à faisceau d'énergie dirigée sont employées contre les systèmes de communication ennemis, les problèmes juridiques ne sont pas significativement différents de ceux que pose l'emploi de moyens cinétiques. La cible (un système de télécommunications, par exemple) est-elle un objectif militaire licite et les effets incidents sur la population civile ont-ils été évalués ? Les armes à énergie dirigée ayant clairement le potentiel de réduire les effets collatéraux immédiats qui sont communément associés aux armes à forte puissance explosive (armes à effet de souffle et armes à fragmentation, par exemple)[78], le principal effet incident à prendre en compte réside donc dans les conséquences de second ordre de la mise à l'arrêt d'un système de télécommunications gérant le contrôle du trafic aérien ou les services d'intervention d'urgence. Bien qu'il soit courant de dire que, lors de l'évaluation de la licéité d'une attaque, les conséquences de second ordre sont à prendre en compte, il faut aussi comprendre correctement ce qui est « comptabilisé » en tant que dommage collatéral aux fins des évaluations de proportionnalité. C'est une erreur de croire que tout désagrément causé à la population civile doit être évalué. Il n'en est rien : outre les pertes humaines (morts et blessés), seuls les « dommages » causés aux biens de caractère civil doivent être pris en compte[79]. Dès lors, dans le cas d'une attaque lancée au moyen d'une arme à énergie dirigée contre un système de contrôle du trafic aérien, et qui aurait affecté à la fois le trafic aérien militaire et le trafic aérien civil[80], le risque que des aéronefs civils soient endommagés et, d'autre part, le risque de pertes civiles devraient être pris considération, mais non pas les simples désagréments, les perturbations de l'activité économique, etc.[81].

Des armes à énergie dirigée sont aussi en cours de développement en tant qu'armes non létales (on parle aussi d'« armes moins létales » ou d' « armes à létalité réduite »). Le but est de proposer un continuum de riposte plus vaste en vue d'une « escalade contrôlée » du recours à la force[82]. Tout un ensemble de raisons d'ordre opérationnel et juridique font qu'il est préférable d'avoir l'option de préserver la vie tout en obtenant la neutralisation (temporaire ou prolongée) de l'individu ciblé. Cela dit, les termes mêmes utilisés pour décrire ces armes sont de nature à causer des problèmes au-delà de toute contrainte particulière,

78 Comme d'autres armes à effet cinétique, telles que les « bombes béton » inertes.

79 Voir *op. cit.*, note 1, art. 51(5)(b) et art. 57(2)(a)(iii) du Protocole additionnel I.

80 Voir CICR, « Guerre informatique et DIH : quelques réflexions et questions », 2011, disponible sur : http://www.icrc.org/fre/resources/documents/feature/2011/weapons-feature-2011-08-16.htm.

81 L'espace ne permet pas un examen approfondi de ce point. D'autres facteurs mériteraient cependant d'être analysés, ce sont, d'une part, les effets sur des acteurs neutres et, d'autre part, tous les types d'effets de troisième ordre (comme, par exemple, l'effet sur les vols d'évacuation médicale) ; l'auteur se demande toutefois « si le CICR pourrait aussi s'employer à générer un consensus à l'échelon international sur la question de savoir si les civils ont un droit fondamental à l'information et à l'électricité, entre autres, tout comme ils ont droit à la vie et à la propriété », *ibid.*

82 Voir, de façon générale, ministère de la Défense des États-Unis, « Non-lethal weapons program », disponible sur : http://jnlwp.defense.gov ; James Duncan, « A primer on the employment of non-lethal weapons », dans *Naval Law Review*, Vol. XLV, 1998. Voir aussi Jürgen Altmann, « Millimetre waves, lasers, acoustics for non-lethal weapons? Physics analyses and inferences », dans DSF-Forschung, 2008, disponible sur : http://tocs.ulb.tu-darmstadt.de/204611717.pdf .

sur les plans du droit ou de la doctrine[83]. Les conséquences non intentionnelles des armes (dues notamment à l'ignorance de l'état de santé de la cible) peuvent aller jusqu'au décès ou à l'invalidité permanente de la cible. Ces conséquences sont utilisées pour stigmatiser le concept d'arme « non létale » ou « moins létale ». Le point important à retenir ici est que, lors d'un conflit armé et comme pour toute autre capacité de combat (y compris les armes à effet cinétique), l'emploi d'armes à énergie dirigée est régi à la fois par le droit international humanitaire, par l'ensemble des règles d'engagement applicables et par les instructions données par le commandement des combats[84].

Les armes non létales à énergie dirigée peuvent être employées conjointement avec des armes traditionnelles, létales. Par exemple, selon certaines sources :

> « Une autre arme … peut émettre des sons assourdissants et extrêmement irritants sur de grandes distances. Plus précisément, le dispositif de longue portée émet un faisceau d'ondes acoustiques à haute énergie, jusqu'à une distance pouvant atteindre cinq fois la longueur d'un terrain de football. Le dispositif ayant été installé dans un hangar proche de la piste d'atterrissage, un témoin qui se trouvait de l'autre côté de la piste a expliqué avoir eu l'impression que quelqu'un hurlait directement dans son oreille.
>
> Le dispositif 'a démontré son utilité pour dégager les rues et les toits pendant les opérations de bouclage et de perquisition … ainsi que pour faire sortir à découvert des tireurs embusqués ennemis, qui sont ensuite abattus par nos propres tireurs d'élite' : c'est ainsi que le système a été présenté dans un rapport des forces armées des États-Unis, dont une compagnie (*361st Tactical Psychological Operations Company*) a testé le dispositif en Irak»[85].

Ce type d'arme à énergie dirigée met en évidence deux problématiques essentielles associées à la technologie des armes non létales. Tout d'abord, de telles armes ont toutes les chances d'être employées contre une population civile (dans le cas décrit plus haut, le but était de dégager les rues et les toits)[86]. Ensuite, les armes non létales peuvent être employées conjointement avec des armes existantes pour obtenir un effet létal.

83 Voir *Defense Science Board Task Force on Directed Energy Weapons, op. cit.*, note 76, p. xii.

84 *Ibid.*, p. xiii.

85 Bryan Bender, « US testing nonlethal weapons arsenal for use in Iraq», dans *Boston Globe*, 5 août 2005, disponible sur : http://www.boston.com/news/nation/articles/2005/08/05/us_testing_nonlethal_weapons_arsenal_for_use_in_iraq/?page=full . L'arme en question (*Long Range Acoustic Device*) est décrite en détail dans J. Altmann, *op. cit.*, note 82, pp. 44-53. J. Altmann relève que, bien que décrit comme destiné aux interpellations ou aux avertissements, ce dispositif peut potentiellement être utilisé comme une arme, *ibid.*, p. 52. Pour une discussion sur les efforts déployés pour échapper à l'obligation juridique de l'examen des « armes » nouvelles en nommant différemment ces types de dispositifs acoustiques, voir N. Davison, *op. cit.*, note 75, pp. 102 et 205.

86 Des préoccupations quant à l'emploi d'armes non létales contre la population civile, ou contre « des individus avant d'avoir vérifié s'ils sont ou non des combattants » sont exprimées dans N. Davison, *op. cit.*, note 75, pp. 216-217.

Les autres armes à énergie dirigée incluent des systèmes dits « de refus actif »[87].

> L'une des armes testées avec succès est un rayon thermique … capable de « cuire » une personne en chauffant l'humidité qui se trouve dans la partie supérieure de la couche épidurale de la peau. Cette arme a été initialement mise au point aux États-Unis, à la demande du département de l'Énergie, pour protéger les installations nucléaires contre les intrus[88].

La « sensation irrésistible de chaleur sur la peau de l'adversaire [cause] un effet dissuasif immédiat »[89]. En effet, la sensation de chaleur provoque « une douleur intolérable et les mécanismes naturels de défense [du corps humain] prennent le dessus »[90]. L'« intense sensation de chaleur ne disparaît que si la personne sort de la trajectoire du rayon ou si l'émission du rayon est arrêtée »[91]. Étant donné que les lance-flammes et autres armes incendiaires sont seulement réglementés et non pas spécifiquement prohibés par le droit international humanitaire, il n'existe aucune raison juridique d'interdire l'emploi au combat de ce système de « refus actif »[92].

Lorsque les systèmes de « refus actif » sont utilisés comme une « clôture » invisible, il appartient évidemment à toute personne de décider de s'approcher ou non de la clôture et, ce faisant, de tenter de pénétrer par effraction[93]. Néanmoins, si des systèmes de « refus actif » sont pointés sur une personne ou un groupe dans le but de dégager une zone[94], ce type d'arme soulève une question sur laquelle il convient de se pencher : comment une personne faisant l'objet de ce type d'attaque peut-elle soit se rendre, soit choisir consciemment de quitter la zone, alors qu'elle ne peut pas voir le rayon[95], qu'elle ignore peut-être même que ce type de technologie existe, et qu'elle réagit au même moment à une douleur intolérable, semblable à la « sensation … [de] toucher une poêle à frire brûlante »[96] ? Le fait de réagir instinctivement à une douleur intolérable rend probablement une personne incapable de réfléchir rationnellement[97]. L'emploi de telles armes devra être précisément réglementé, en combinant une série d'éléments – tactiques, techniques et procédures, règles

87 *Defense Science Board Task Force on Directed Energy Weapons, op. cit.*, note 76, pp. 33 et 38. Pour plus de détails, voir « Active denial system demontrates capabilities at CENTCOM », United State Central Command, disponible sur : http://www.centcom.mil/press-releases/active-denial-system-demonstrates-capabilities-at-centcom.
88 B. Bender, *op. cit.*, note 85. Le système de « refus actif » est décrit en détail dans J. Altmann, *op. cit.*, note 82, pp. 14-28.
89 *Defense Science Board Task Force on Directed Energy Weapons, op. cit.*, note 76, p. 38.
90 *Ibid.*, p. 42.
91 *Ibid.*
92 J. Altmann, *op. cit.*, note 82, p. 27.
93 Conversation entre Patrick Keane et Ian Henderson, 14 avril 2012.
94 À la différence des armes à effet cinétique traditionnelles, dont l'effet désiré est de mettre l'adversaire hors de combat (en le blessant ou en le tuant).
95 Voir J. Altmann, *op. cit.*, note 82, p. 28.
96 *Defense Science Board Task Force on Directed Energy Weapons, op. cit.*, note 76, p. 42.
97 Courrier électronique échangé entre April-Leigh Rose et Ian Henderson le 24 avril 2012.

d'engagement – afin d'éviter que des souffrances excessives ne soient causées par l'emploi continu de l'arme uniquement dû au fait que la personne n'a pas quitté la zone cible[98]. À ce propos, nous relèverons que le système de « refus actif » a « passé avec succès les tests visant à établir son acceptabilité sous l'angle juridique, conventionnel et au regard des règles d'engagement du Commandement central des États-Unis »[99]. Nous rappellerons cependant que les obligations juridiques des États varient, et que tous les États n'emploient pas les armes de la même manière. Par conséquent, le résultat de l'examen juridique effectué par un État n'est pas déterminant pour les autres États[100]. Cet aspect peut être important dans le contexte de la vente de matériel de haute technologie, car les informations sur les capacités d'une arme donnée sont souvent classées comme extrêmement confidentielles et « compartimentées ». L'État procédant à l'examen juridique peut fort bien ne pas contrôler l'accès aux données nécessaires. Comme nous le verrons ci-dessous, cela amène parfois les juristes, les ingénieurs et les opérateurs à travailler ensemble de manière coopérative et imaginative, dans le but de surmonter le problème des limitations imposées par la classification de sécurité et la compartimentation de l'accès aux informations.

Une arme similaire, également à faisceau d'énergie dirigée, mais utilisant une technologie différente est « une lumière blanche de forte puissance, assez intense pour faire fuir dans la direction opposée tous les assaillants, sauf les plus déterminés »[101]. Il semble que les concepts d'utilisation de l'arme en question incluent le fait de l'employer pour identifier des forces hostiles, si l'on en croit la déclaration d'un haut responsable du projet, le colonel Wade Hall : « [s]i je vois que quelqu'un est prêt à supporter l'inconfort … , je sais ce qu'il a l'intention de faire – je le tue »[102]. De tels propos semblent inquiétants, mais il vaut la peine de se demander s'il y a vraiment une différence par rapport aux scénarios « traditionnels » d'avertissements et d'escalade de la force (tels que la sommation « Halte, ou je tire ») ou par rapport aux fusées éclairantes et aux éblouisseurs utilisés pour prévenir les véhicules et éviter qu'ils se rapprochent trop des convois militaires.

Lorsque les armes à énergie dirigée sont employées pour lutter contre les engins explosifs (souvent improvisés)[103], ce sont principalement les conséquences qu'il importe d'analyser. Si l'arme à énergie dirigée doit provoquer une explosion à une distance telle que les forces amies ne sont pas menacées, il est indispensable de chercher à savoir si des civils ou autres non-combattants se trouvent à proximité du lieu de l'explosion et risquent, de ce fait, d'être blessés ou tués[104].

98 J. Altmann recommande aussi d'étudier le risque pour la vue en raison de lésions potentielles de la cornée, voir J. Altmann, *op. cit.*, note 82, p. 28.

99 *Ibid.*, p. 38.

100 Voir J. McClelland, *op. cit.*, note 1, p. 411, qui relève ce point en réponse aux fabricants qui invoquent la légalité de leur produit.

101 B. Bender, *ibid.*

102 *Ibid.*

103 Voir *Defense Science Board Task Force on Directed Energy Weapons, op. cit.*, note 76, p. 40.

104 L'espace ne permet pas une analyse complète de ce sujet. Il convient cependant de noter que les problèmes sont différents si, au lieu de provoquer une explosion, la contre-mesure empêche la détonation du dispositif explosif.

Les cyber-opérations

Ce sont des opérations dirigées contre un ordinateur ou un système informatique par le biais de flux de données[105].

> « De telles opérations peuvent poursuivre des objectifs divers comme, par exemple, infiltrer un système informatique pour collecter, exporter, détruire, altérer ou encrypter des données, ou pour déclencher, détourner ou manipuler de toute autre manière des processus contrôlés par le système informatique infiltré. Toute une série de «cibles» dans le monde réel peuvent ainsi être détruites, altérées ou perturbées, comme les industries, les infrastructures, les télécommunications ou les systèmes financiers »[106].

Les cyber-opérations sont conduites au moyen de logiciels, de matériel informatique ou en combinant logiciels et personnel. Le virus STUXNET est un exemple récent de cyber-opération ayant été essentiellement conduite au moyen d'un logiciel. Une fois en place, le virus semble avoir opéré de façon indépendante, sans requérir aucune autre intervention humaine[107]. Ce virus peut être comparé à un logiciel conçu pour permettre à un téléopérateur d'exercer un contrôle sur un ordinateur, ce qui lui permet, entre autres, de charger ou de modifier des données dans l'ordinateur cible. Nous citerons enfin le piratage de cartes de crédit comme exemple non militaire de cyber-opération qui exige à la fois du matériel et des programmes informatiques.

L'application à la « cyber-guerre » de règles spécifiques du droit international humanitaire demeure un sujet de débat[108]. Néanmoins, aux fins du présent article, nous partons du principe que les exigences essentielles du droit international humanitaire – à savoir le respect des principes de distinction, de proportionnalité et de précaution – s'appliquent, au minimum, aux cyber-attaques ayant des conséquences sur le plan matériel (ainsi, le virus STUXNET a altéré les conditions de fonctionnement des centrifugeuses iraniennes servant à l'enrichissement de l'uranium, ce qui a ensuite provoqué des dommages matériels à ces centrifugeuses)[109]. Quatre aspects juridiques particuliers des cyber-armes méritent d'être mentionnés ici.

105 Sur la base de cette définition, une attaque cinétique visant à « mettre hors circuit » un système électronique (en lâchant une bombe sur le bâtiment où se trouve l'ordinateur, par exemple) ne constituerait pas une cyber-opération.

106 CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, *op. cit.*, note 29, p. 42.

107 Voir Angus Batey, « The spies behind your screen », dans *The Telegraph*, 24 novembre 2011 ; Jack Goldsmith, « Richard Clarke says Stuxnet was a United-Staes Operation », dans *LawFare: Hard National Security Choices*, 29 mars 2012, disponible sur: http://www.lawfareblog.com/2012/03/richard-clarke-says-stuxnet-was-a-u-s-operation/ .

108 Voir « Tallinn Manual on the International Law Applicable to Cyber Warfare », 2012, pp. 17-22, disponible sur : http://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf.

109 CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, *op. cit.*, note 29, pp. 36-37.

Premièrement, une cyber-arme présente la particularité de pouvoir être opérée par un civil[110]. Une telle « arme » a toutes les chances d'être éloignée du champ de bataille ; elle est technologiquement sophistiquée ; enfin, elle n'évoque pas immédiatement le risque de pertes en vies humaines. Le maniement d'une cyber-arme expose l'opérateur civil (en tant que civil participant directement aux hostilités) à la fois au risque de ciblage létal[111] et à d'éventuelles poursuites pénales pour avoir commis des actes non protégés par l'immunité du combattant dont jouissent les membres des forces armées[112]. Ces questions sont examinées en détail dans un récent article de Sean Watts qui lance notamment l'idée de l'éventuelle nécessité de repenser complètement la manière dont le droit relatif à la participation directe aux hostilités s'applique dans le domaine de la cyber-guerre[113]. L'on pourrait aussi se demander quelle formation de tels opérateurs civils pourraient avoir reçue quant aux règles pertinentes du droit international humanitaire[114].

Deuxièmement, les cyber-attaques peuvent avoir des conséquences dans le monde réel et non pas seulement dans le monde virtuel[115]. Lorsque la population civile est affectée – morts et blessés civils, dommages aux biens de caractère civil, ou combinaison de ces pertes et dommages – il convient d'examiner ces conséquences à la lumière du droit international humanitaire[116]. L'analyse de cette question que nous avons présentée à propos des attaques par arme à énergie dirigée est également applicable aux cyber-attaques. Une autre considération est apparentée : lorsque l'on peut raisonnablement attendre qu'un virus introduit dans un système militaire soit capable de s'infiltrer dans des systèmes civils et de causer des dommages aux infrastructures, ce dommage collatéral doit également être pris en considération[117]. L'on cite souvent l'exemple d'une possible cyber-attaque qui affecterait directement les civils et mettrait hors service une centrale électrique, soit simplement en provoquant sa fermeture, soit en la surchargeant, soit enfin en désactivant les dispositifs de sécurité, endommageant ainsi le matériel informatique. Toute infrastructure dont la gestion est assurée par un logiciel est susceptible de connaître un tel sort.

Troisièmement, les cyber-armes doivent être examinées non seulement au regard du droit international humanitaire, mais aussi de manière très significative

110 Voir Adam Segal, « China's cyber stealth on new frontline », dans *Australian Financial Review*, 30 mars 2012, disponible sur : http://afr.com/p/lifestyle/review/china_cyber_stealth_on_new_frontline_z6YvFR0mo3uC87zJvCEq6H . L'auteur fait référence aux « cyber-milices » d'entreprises technologiques recrutées par l'Armée Populaire de Libération chinoise.

111 Voir *op. cit.*, note 1, art. 51(3) du Protocole additionnel I.

112 Sur ces deux points, voir D. Blake et J. Imburgia, *op. cit.*, note 1, pp. 195-196.

113 Voir Sean Watts, « Combatant status and computer network attack », dans *Virginia Journal of International Law*, Vol. 50, N° 2, 2010, p. 391.

114 Voir J. Kellenberger, *op. cit.*, note 15 (la remarque concerne les armes opérées à distance).

115 CICR, « Guerre informatique et DIH : quelques réflexions et questions », *op. cit.*, note 80.

116 Voir *op. cit.*, note 1, art. 51(5)(b) et 57(2)(a)(iii) du Protocole additionnel I. Le fait de tenir compte ou non d'autres conséquences pour la population civile (perturbations, destruction d'infrastructures et d'équipements, etc.) constitue une décision politique.

117 Voir CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, *op. cit.*, note 29, p. 38.

au regard du *jus ad bellum*[118]. Comme le relèvent Blake et Imburgia, même si elle n'a pas d'effets cinétiques, une cyber-attaque pourrait tout de même aller à l'encontre de la Charte des Nations Unies ou, de manière générale, du droit international[119]; de plus, si elle équivaut à une « attaque armée », une cyber-attaque pourrait légitimer, au titre de la légitime défense, l'emploi de la force par l'État affecté.

Quatrièmement, de par la nature même de la cyber-guerre, il peut être difficile de déterminer qui est à l'origine d'une attaque, et les problèmes d'attribution de la responsabilité vont jusqu'au cœur de la responsabilité des États et individuelle[120].

Nanotechnologie et militarisation de la neurobiologie

> Il est difficile de définir une « nano-arme », mais le terme recouvre des objets et des dispositifs issus de la nanotechnologie qui sont conçus ou utilisés pour nuire à des êtres humains, ainsi que ceux qui causent des effets nuisibles à l'échelle nanométrique (si ces effets caractérisent la létalité de l'arme)[121].

Parmi le second type de nano-armes figurent les bombes DIME (*Dense Inert Metal Explosive*):

> Il s'agit d'un aérosol explosif composé de micro-éclats à très haute température contenant un alliage de tungstène et de métaux lourds appelé HMTA (*Heavy Metal Tungsten Alloy*), broyé et réduit en poudre. Les bombes DIME ont un très grand pouvoir létal, mais dans un rayon relativement restreint. À l'impact, la poudre de HMTA se transforme en poussière (dont les particules sont de taille encore plus minuscule). Sous l'effet de la résistance de l'air, l'aérosol perd très vite son inertie, mais il brûle et détruit, selon une angulation très précise, tout ce qui se trouve dans un rayon de 4 mètres. La poudre de HMTA est considérée comme étant extrêmement carcinogène et toxique pour l'environnement. Initialement mise au point par l'armée de l'air américaine, cette nouvelle arme a été conçue pour réduire les dommages collatéraux, lors de combats en zones urbaines, en limitant la portée de la force explosive[122].

118 L'on peut dire, pour simplifier, que le *jus ad bellum* est le droit qui réglemente le recours global à l'emploi de la force, alors que le *jus in bello* (le droit international humanitaire) réglemente les cas individuels d'emploi de la force en période de conflit armé. Voir Matthew Waxman, « Cyber attacks as 'Force' under UN Charter Article 2(4) », dans Raul Pedrozo et Daria Wollschlaeger (dir.), *International Law and the Changing Character of War*, *International Law Studies*, Vol. 87, 2011, p. 43; Sean Watts, « Low-intensity computer network attack and self-defense », dans *ibid.*, p. 59; Michael Schmitt, « Cyber operations and the *jus ad bellum* revisited », dans *Villanova Law Review*, Vol. 56, N° 3, 2011, pp. 569-605.

119 D. Blake et J. Imburgia, *op. cit.*, note 1, pp. 184-189. Ces éléments sont examinés plus en détail dans Michael Schmitt, *ibid.*, qui évoque également la situation actuelle, parlant des « failles dans le droit qui régit l'emploi de la force [qui] sont dues au fait que ce corpus juridique est antérieur à l'apparition des cyber-opérations » [Traduction CICR].

120 J. Kellenberger, *op. cit.*, note 15; CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, *op. cit.*, note 29, p. 42.

121 H. Nasu et T. Faunce, *op. cit.*, note 10, p. 23.

122 Il semble que le fait qu'une telle arme ait été employée lors d'opérations de combat réel reste affaire de

La « capacité [des bombes DIME] de causer des blessures incurables et des souffrances excessives (notamment en raison du fait qu'aucun éclat n'est de taille suffisante pour être facilement détecté ou retiré par le personnel médical) a alarmé les experts en médecine »[123]. L'autre préoccupation suscitée par les nanotechnologies vient de ce que les éléments et les produits chimiques qui, à l'échelle macroscopique, ne sont pas directement nuisibles pour les humains peuvent être chimiquement extrêmement réactifs à l'échelle nanométrique. Il faudra donc sans doute repréciser ce qu'est une « arme chimique » au regard du droit international humanitaire.

De la même façon, du fait des avancées actuelles dans la compréhension du génome humain et les neurosciences, il existe une possibilité très réelle de militarisation des connaissances acquises dans ces domaines[124]. Sur le plan du droit, l'une des conséquences réside dans la nécessité de réévaluer le bien-fondé du maintien d'une distinction juridique entre armes chimiques et armes biologiques. Étant donnée la manière dont ces armes peuvent être employées, il faudrait peut-être les considérer juridiquement comme constituant des éléments d'un « spectre continu de menaces biochimiques, car des chevauchements existent entre les deux Conventions – celle sur les armes biologiques et à toxines (CABT) de 1972 et celle sur les armes chimiques (CAC) de 1993 – quant aux agents dits de mi-spectre comme les toxines et les biorégulateurs »[125].

Des tensions opposées existent dans ce domaine. Les armes chimiques et les armes biologiques n'ont pas bonne presse, et cela n'a rien d'étonnant. En même temps, des recherches sont en cours afin de mettre au point des armes non létales telles que les armes biochimiques incapacitantes.

> « Bien qu'il n'en existe aujourd'hui aucune définition universellement acceptée, les agents biochimiques incapacitants peuvent être décrits comme étant des substances dont l'action chimique sur certains processus biochimiques et systèmes physiologiques, spécialement ceux qui

spéculation : voir, de façon générale, *Dense Inert Metal Explosive (DIME)*, Global Security, disponible sur : http://www.globalsecurity.org/military/systems/munitions/dime.htm.

123 H. Nasu et T. Faunce, *op. cit.*, note 10, p. 22. Outre l'article 35(2) du Protocole additionnel I, *op. cit.*, note 1, qui interdit de causer des maux superflus, voir aussi le *Protocole relatif aux éclats non localisables (Protocole I)* annexé à la *Convention sur certaines armes classiques* de 1980. Amnesty International estime que de nouvelles études sont nécessaires pour déterminer si l'emploi de munitions DIME est licite ou non en droit international. Amnesty International, « Dense Inert Metal Explosives (DIME) », dans *Fuelling conflict: Foreign arms supplies to Israel/Gaza*, 2009, disponible sur : http://www.amnesty.org/en/library/asset/MDE15/012/2009/en/5be86fc2-994e-4eeb-a6e8-3ddf68c28b31/mde150122009en.html#0.12 . Pour une discussion générale du Protocole relatif aux éclats non localisables (Protocole I) annexé à la Convention de 1980 sur certaines armes classiques, voir W. Boothby, *op. cit.*, note 45, pp. 196-199.

124 Voir, de façon générale, Mark Wheelis et Malcolm Dando, « Neurobiologie : étude de cas sur la militarisation imminente de la biologie », dans *Revue internationale de la Croix-Rouge*, N° 859, 2005, pp. 553-571. Voir aussi « Brain Waves 3: Neuroscience, conflict and security », dans *The Royal Society*, disponible sur : http://royalsociety.org/policy/projects/brain-waves/conflict-security, pour une discussion relative, entre autres, aux applications militaires potentielles des neurosciences et des neurotechnologies ainsi qu'aux problèmes juridiques actuels.

125 M. Wheelis et M. Dando, *ibid.*, p. 560.

> influent sur l'activité régulatrice supérieure du système nerveux central, créent un problème incapacitant (ils peuvent, par exemple, entraîner incapacité, désorientation, incohérence, hallucinations, sédation, perte de conscience). Ils sont aussi connus sous les noms d'agents chimiques incapacitants, d'agents biotechniques, d'agents calmants et, enfin, d'agents immobilisants »[126].

Il est essentiel de relever ici que, alors que les agents biologiques et chimiques traditionnels étaient employés contre des soldats ennemis ou des civils « non coopératifs » et seraient clairement considérés comme des armes, les agents modernes peuvent parfois être employés par un État pour « augmenter » les capacités de ses propres forces armées. Dans ce dernier cas, il y a bien moins de chances que les agents utilisés équivalent à des armes[127]. Par exemple :

> « [d]ans quelques dizaines d'années, nous assisterons à une augmentation des performances des troupes qui sera presque certainement le résultat de l'emploi de divers composés pharmaceutiques, et qui concernera plusieurs systèmes physiologiques, bien au-delà du cycle du sommeil. En réduisant la peur et la douleur et en augmentant l'agressivité, l'hostilité, les capacités physiques et la vigilance, l'on pourrait améliorer de manière significative les performances des soldats, mais cela risquerait aussi d'accroître notablement la fréquence des violations du droit humanitaire. Par exemple, il y a fort peu de chances que le fait de renforcer l'agressivité et l'hostilité de l'individu dans les situations de conflit ait pour résultat d'accroître la retenue et le respect des interdictions juridiques de la violence »[128].

Des préoccupations similaires ont déjà été exprimées à propos des armes télécommandées. Et, comme dans le cas de l'emploi d'armes à énergie dirigée pour disperser des rassemblements de civils, le risque existe que des civils soient « pacifiés » dans des territoires occupés par des produits chimiques inclus dans les distributions de vivres[129]. Il existe aussi – et peut-être est-ce encore plus inquiétant, car cela affecte directement la capacité de faire appliquer le droit international humanitaire, en particulier la responsabilité du commandement – la possibilité que les « souvenirs des atrocités commises [soient] effacés chimiquement lors des briefings après les opérations »[130].

126 Michael Crowley et Malcolm Dando, « Submission by Bradford Nonlethal Weapons Research Project to Foreign Affairs Select Committee Inquiry on Global Security: Non-Proliferation », 2008, pp. 1-2, disponible sur : http://www.brad.ac.uk/acad/nlw/publications/BNLWRP_FAC071108MC.pdf [Traduction CICR].
127 Une armure, par exemple, n'est pas considérée comme une arme.
128 M. Wheelis et M. Dando, *op. cit.*, note 124, pp. 562-563 [Traduction CICR].
129 *Ibid.*, p. 565.
130 *Ibid.*, p. 565 [Traduction CICR].

La nécessité de comprendre et d'intégrer les questions d'ingénierie dans le processus d'examen de la licéité des armes

La rapide présentation ci-dessus des armes émergentes montre que plus la complexité des armes augmente, plus les non-spécialistes ont de la peine à comprendre le mode de fonctionnement de chacune d'elles. La présente section de l'article se concentre sur les questions d'ingénierie. Nous nous efforcerons de montrer que la compréhension des enjeux techniques peut constituer l'un des éléments à prendre en compte lors l'examen juridique des armes nouvelles.

Pourquoi arrive-t-il qu'une arme ne fonctionne pas comme prévu ?

Plusieurs raisons peuvent expliquer qu'une arme ne fonctionne pas comme prévu ou de façon conforme aux « spécifications de conception du produit »[131]. Des spécifications techniques inadéquates, des défauts de conception, ou encore un contrôle de qualité défaillant au stade de la fabrication (variabilité des lots de production) figurent parmi ces raisons. D'autres facteurs peuvent aussi intervenir, notamment « l'âge de la munition, les conditions de stockage, les conditions environnementales au moment de l'usage et, enfin, les conditions sur le terrain »[132].

Un simple exemple d'anomalie de spécification, ou tout au moins d'une spécification qui ne sera pas considérée 100 % fiable, est celui d'une mine antivéhicule qui serait conçue pour ne pas exploser quand un humain pose le pied dessus. Par exemple, s'il s'agit d'une mine activée par pression, le poids pourrait être fixé comme devant être inférieur à 150 kg. Néanmoins :

> [l]a recherche biomécanique fournit de solides preuves montrant qu'un être humain peut très facilement exercer une pression qui est proche ou même supérieure à celle d'un poids de 150 kg. Par exemple, si un garçonnet de 8 ans pesant 30 kg et portant des chaussures dévale en courant du haut d'une colline, il exerce une force d'impact au sol de 146 kg ; une fillette de 9 ans pesant 40 kg qui dévale en courant, pieds nus, du haut d'une colline exerce une force de 167 kg ; un homme qui court exerce une force de 213 kg[133].

Autre cas de figure : la spécification serait correcte, mais une défaillance au niveau de la conception, du processus de fabrication ou de l'intégration de systèmes ne

131 L'étape des spécifications de conception du produit vise à définir ce qu'un produit devrait faire ; elle précède l'étape des spécifications techniques proprement dites qui porte sur la manière dont le produit fera ce qu'il est prévu qu'il fasse.

132 *Defense Science Board Task Force, Munitions System Reliability*, Bureau du Sous-Secrétaire à la Défense (Acquisition, technologie et logistique), ministère de la Défense des États-Unis, Washington, D.C., septembre 2005, p. 15, disponible sur : http://permanent.access.gpo.gov/lps72288/ADA441959.pdf [Traduction CICR].

133 « Anti-vehicle mines: discussion paper », Actiongroup *Landmine.de*, 2004, p. 5 (note de bas de page omise), disponible sur : http://www.landmine.de/fileadmin/user_upload/pdf/Publi/AV-mines-discussion-paper.pdf [Traduction CICR]

permettrait pas d'atteindre constamment le résultat voulu. Il pourrait s'agir d'un problème de qualité au niveau de l'ingénierie, la robustesse des processus mis en œuvre ayant été insuffisante : le produit serait donc défectueux et poserait de ce fait un problème de fiabilité.

Si une arme ne fonctionne pas comme prévu, les deux conséquences principales sont les suivantes :

- L'effet militaire désiré n'est pas obtenu. Si l'arme ne remplit pas sa fonction, les forces armées de l'utilisateur sont mises en danger. Si l'arme ne fonctionne pas de manière conforme aux spécifications, les civils et les biens de caractère civil sont mis en danger[134].
- Si des civils sont blessés ou tués, ou si des biens de caractère civil sont endommagés, la responsabilité peut être engagée[135]. La responsabilité de l'État peut être engagée en cas de fait internationalement illicite (c'est-à-dire en cas d'infraction au droit international humanitaire) et la responsabilité pénale peut être éventuellement imputée au commandant qui a autorisé l'emploi de l'arme, ou à la personne qui a employé l'arme, ou à l'un et à l'autre.

À mesure que les systèmes d'armes deviendront plus complexes, la compréhension de l'analyse de fiabilité devra devenir l'un des éléments du processus d'examen juridique.

Fiabilité : procédure de tests et d'évaluation

La procédure de tests et d'évaluation a pour but de fournir un moyen d'établir objectivement si un système (ou l'un de ses composants) fonctionne de manière fiable conformément aux spécifications. La fiabilité est la probabilité de fonctionnement correct, à un niveau de confiance donné, pendant un cycle de vie défini (mesuré en unités de temps, en cycles d'opération, etc.). Il est intuitivement simple de comprendre que la fiabilité constitue un facteur essentiel dans le fonctionnement d'une arme ; toutefois, le niveau de complexité n'est pas toujours immédiatement perçu par quiconque n'est pas familier avec les questions de fiabilité d'ingénierie[136]. La quantification de la fiabilité n'est pas une proposition à laquelle l'on peut répondre par « oui » ou par « non »[137] ; elle ne peut pas non plus s'obtenir par le biais d'un seul test « réussite ou échec », car elle est en fait « soumise aux limites de confiance statistique »[138]. Par exemple, afin de déterminer au niveau approprié de confiance

134 De telles défaillances ont des conséquences directes sur l'efficacité militaire ; elles ont aussi un impact négatif sur le moral, le soutien de l'opinion publique au niveau national, le soutien international, etc.

135 La responsabilité peut aussi être engagée quand les moyens ou méthodes de guerre utilisés contre les combattants sont illicites (ce qui peut se produire dans un scénario d'arme défectueuse où, par exemple, un coup de feu serait tiré contre un combattant déjà hors de combat).

136 Voir, de façon générale, *Defense Science Board Task Force, Munitions System Reliability*, *op. cit.*, note 132.

137 « Dis-moi simplement si ce produit est fiable ou non », demanderait le chef.

138 *Defense Science Board Task Force, Munitions System Reliability*, *op. cit.*, note 132, p. 15.

statistique que le taux de défaillance de la population d'une certaine arme est acceptable, il faut qu'un nombre minimum de tests aient été réalisés. Toutefois, les ressources étant toujours limitées, des pratiques d'ingénierie responsables doivent répondre à la question suivante : comment optimiser les ressources et établir le minimum requis pour parvenir à un taux de fiabilité acceptable ? Supposons qu'il serait trop long d'effectuer le nombre voulu de tests, ou que les frais à engager excéderaient le budget alloué. Une approche naïve consisterait simplement à réduire le nombre de tests pour se plier aux exigences budgétaires, en espérant que les essais effectués fourniront malgré tout quelques informations utiles. Or, rien ne dit que ce sera le cas. On peut imaginer que de tels essais ne fourniront que des conclusions trompeuses si les résultats obtenus n'atteignent pas le niveau de confiance requis. Les tests de certification exigent un certain niveau de confiance. Il est vrai qu'en ce qui concerne les composants d'armes non létales, le niveau de confiance statistique requis est parfois établi (à juste titre) à un niveau bas car leur défaillance n'a qu'un faible impact opérationnel et ses implications en termes de sécurité sont mineures ou nulles (dans le cas, par exemple, de la défaillance d'une balle traçante). Par contre, le système de reconnaissance de cible qui est monté sur une arme autonome peut exiger un niveau très élevé de confiance statistique pour réduire au minimum l'emploi d'armes létales contre des civils tout en assurant l'engagement de cibles ennemies. Si un niveau élevé d'assurance statistique est jugé nécessaire pour la sécurité des civils alors que des contraintes budgétaires empêchent de procéder aux tests requis, alors des limites appropriées devraient être imposées quant aux applications approuvées pour cette arme, jusqu'à ce que l'expérience de terrain permette de parvenir à un niveau de confiance approprié envers la fiabilité de l'arme.

Comment cela devrait-il être appliqué dans la pratique ? Les principales étapes de la procédure d'acquisition d'une arme sont bien décrites par McClelland, y compris les diverses étapes des « tests de démonstration », « tests de fabrication » et « essais en service »[139]. Comme le relève McClelland, il ne s'agit pas d'un processus juridique mais plutôt de l'un des éléments du processus d'acquisition. Ce sont néanmoins autant de points de prise de décision qui constituent « des étapes importantes pour l'apport de conseils juridiques formels »[140]. En effet, pour que les tests soient utiles, il faut que certaines questions, d'importance capitale, relatives au fonctionnement soient traduites en éléments testables, pouvant être mesurés de manière objective. De nombreux petits pays pourraient se contenter d'être de simples acheteurs d'armes prêtes à l'emploi[141], mais d'autres gouvernements sont

139 J. McClelland, *op. cit.*, note 1, p. 401. Ou encore, les essais peuvent avoir lieu aux stades de la conception et de l'acceptation initiale puis dans le cadre de l'évaluation opérationnelle.

140 *Ibid.*, p. 402.

141 Bien sûr, les acheteurs de systèmes d'armes « prêtes à l'emploi » doivent encore s'assurer de la licéité des armes acquises. Même dans le cas d'une arme dont la mise au point est terminée et qui a fait l'objet de tous les tests prévus, cette démarche peut être difficile pour les acheteurs d'armes de haute technologie. Il peut arriver, par exemple, que le fabricant refuse de donner suffisamment d'informations sur une arme de haute technologie utilisant un logiciel propriétaire crypté, alors que ces informations auraient permis à l'utilisateur final de juger en connaissance de cause les algorithmes utilisés et d'avoir confiance quant à la fiabilité ultime de l'arme.

engagés dans le processus de conception, de mise au point et d'essais d'armes dont la technologie est émergente. Certes, le niveau d'implication varie, mais il s'agit d'un choix pour les gouvernements[142]. Aussi, plutôt que de se borner à recevoir passivement les résultats des essais et autres données relatives aux armes, les gouvernements pourraient adopter une démarche proactive dans le cadre du processus d'examen juridique. Les juristes pourraient apporter leur contribution dès les phases d'essais et d'évaluation, en identifiant les problèmes au regard du droit, qui seraient ensuite traduits en éléments testables. Cela pourrait être l'une des façons de surmonter, en partie tout au moins, les difficultés en termes de sécurité et d'accès compartimenté que présentent les armes de haute technologie et dont nous avons parlé plus haut. Par exemple, il est justifié d'accorder davantage de confiance à la fiabilité dans le cas d'applications militaires impliquant des facteurs de risque plus élevés pour les civils. De telles informations pourraient servir de référence croisée avec des données relatives à la fiabilité de systèmes d'armes existants ; elles pourraient ainsi constituer une contribution au processus de prise de décisions, quand il s'agit de déterminer si une nouvelle procédure de ciblage peut être considérée comme licite.

Pour être suivies d'effet, les exigences juridiques doivent être exprimées en termes « testables, quantifiables, mesurables et raisonnables »[143]. Le défi à relever consistera notamment à combler le fossé qui sépare souvent les définitions des exigences techniques et la performance opérationnelle souhaitée. L'existence de ce fossé peut généralement être « attribuée à la terminologie employée pour définir le niveau de performance requis ainsi que les conditions et la manière dont cette performance [doit être] mesurée »[144]. C'est là, précisément, que des juristes travaillant avec des ingénieurs systèmes peuvent influencer le processus, de telle sorte que les tests, les démonstrations et l'analyse puissent être adoptés en tant que méthodes valables pour prévoir la performance réelle.

Une fois qu'un système a été mis en service, d'autres essais peuvent encore être réalisés pour obtenir davantage d'informations sur les capacités du système et s'assurer qu'il satisfait réellement aux exigences de l'utilisateur. Cette phase d'essais et d'évaluation est particulièrement critique, car c'est la seule phase qui est en lien avec l'emploi du système dans le « monde réel »[145].

142 Voir *Report on the Defense Science Board Task Force on Developmental Test & Evaluation*, Bureau du Sous-Secrétaire à la Défense (Acquisition, technologie et logistique), ministère de la Défense des États-Unis, mai 2008, pp. 6-7, disponible sur : www.acq.osd.mil/dsb/reports/ADA482504.pdf. Ce rapport a attiré l'attention sur la récente diminution de la participation du gouvernement des États-Unis aux tests de qualification (essais visant à vérifier la validité de la conception et sa conformité aux spécifications) ; peut-être plus inquiétant encore est le fait que l'accès du gouvernement aux données relatives aux essais ait été limité.

143 *Ibid.*, p. 38 [Traduction CICR]. Il est relevé dans le rapport que cette démarche pourrait initialement ne pas être facile. Voir, par exemple, *ibid.*, p. 39, une discussion des cas où cette démarche a été omise en ce qui concerne les exigences opérationnelles.

144 *Ibid.*, p. 41.

145 Par exemple, il a été constaté de manière empirique que certaines défaillances étaient dues à des « facteurs opérationnels qui n'avaient pas été pris en compte dans les essais réalisés aux fins de mise au point, validation et surveillance », *Defense Science Board Task Force, Munitions System Reliability*, *op. cit.*, note 132, p. 17 [Traduction CICR].

Si des spécialistes du droit fournissaient des critères juridiques cohérents à l'aune desquels une catégorie d'armes pourrait être évaluée, la conformité permanente de ces armes aux exigences du droit pourrait être prise en compte dans un processus déjà existant. Un autre domaine dans lequel la contribution des juristes serait utile est l'évaluation et l'analyse de l'intégration et de l'interaction de systèmes et de sous-systèmes. Quand il s'agit d'un système de systèmes, l'expérience militaire des États-Unis montre qu'il n'existe aucun

> « directeur de programme unique qui 'possède' la responsabilité de la performance ou de la vérification pour l'ensemble de multiples éléments constitutifs des systèmes ; il n'existe aujourd'hui aucun processus d'adjudication largement utilisé qui permettrait de facilement assigner la responsabilité des capacités [d'un système de systèmes], à l'exception près des systèmes de commandement et de contrôle »[146].

La situation est bien différente dans d'autres secteurs. Les principaux constructeurs automobiles, par exemple, utilisent des processus extrêmement sophistiqués de conception, de production, d'essais et de validation de qualité pour chaque composant d'un véhicule ; ils disposent ainsi d'une attribution de responsabilité détaillée pour chaque composant, système et produit tout entier (y compris pour les systèmes multiples). En travaillant avec les ingénieurs systèmes, les différentes instances du processus de contrôle de qualité pourraient identifier les problèmes juridiques critiques qui exigent à la fois la réalisation d'essais et l'attribution de responsabilité (par exemple, en cas de non-respect du droit international humanitaire) entre le fabricant de l'arme et les diverses parties prenantes militaires.

Fiabilité et reconnaissance automatique de cible

Les armes qui sont conçues pour exploser mais n'explosent pas comme prévu quand elles sont utilisées en opérations et sont laissées sur le terrain après la cessation des hostilités sont appelées « restes explosifs de guerre »[147]. De fait, la fiabilité des munitions est même définie comme « une mesure de la probabilité d'une explosion réussie »[148]. En raison des dangers que les engins non explosés font courir à la population civile, une réglementation juridique existe déjà en la matière[149]. L'on sait moins, cependant, que la fiabilité des armes, s'agissant de la reconnaissance automatique de cible, comporte un autre aspect important : le problème qui se pose n'est pas seulement celui d'une arme qui n'explose pas, mais également celui d'une arme qui se trompe de cible.

146 *Report on the Defense Science Board Task Force on Developmental Test & Evaluation*, *op. cit.*, note 142, p. 43 [Traduction CICR].
147 Voir *Defense Science Board Task Force, Munitions System Reliability*, *op. cit.*, note 132, p. 10.
148 *Ibid.*, p. 14 [Traduction CICR].
149 Par exemple, voir le chapitre sur les « Unexploded and abandoned weapons », dans W. Boothby, *op. cit.*, note 45, pp. 297-317.

Nous tenterons donc ici de déterminer s'il est raisonnable de conclure, sur la base de l'analyse des données de reconnaissance, qu'une cible donnée possède certaines propriétés ou caractéristiques ennemies et, le cas échéant, de préciser quand il est raisonnable de parvenir à une telle conclusion. Prenons le cas où la différence entre l'hypothétique caractéristique ennemie et les données de reconnaissance n'est ni assez forte pour que nous rejetions automatiquement la cible, ni assez faible pour que nous la validions facilement. Dans un tel cas, il faudrait effectuer une analyse statistique plus sophistiquée (des tests d'hypothèses, par exemple). Supposons qu'il a été prouvé par l'expérience qu'une concordance de 90 % entre les données de reconnaissance et les informations disponibles sur un certain type de cibles ennemies constituait un critère fiable pour confirmer une cible ennemie. Si la concordance était de 100 % ou de 30 %, nous pourrions possiblement en arriver à une conclusion acceptable en utilisant le sens commun. Supposons maintenant une concordance de 81 % entre les données. Certes, nous pourrions penser que nous sommes relativement près de 90 %, mais pourrions-nous pour autant penser que cela suffit pour valider la cible en tant que cible licite ? Que nous acceptions ou que nous rejetions les données pour décider qu'il s'agit d'une cible licite, nous ne pouvons pas être absolument certains de prendre la bonne décision. Nous sommes contraints d'admettre l'incertitude – et de la gérer. Plus nous resserrons les critères de validation des croisements de données, moins il y a de chances qu'un système automatique de reconnaissance prenne pour cibles à attaquer des cibles qui sont à épargner (des « non-cibles ») ; il y aura par contre davantage de chances que le système de reconnaissance échoue à identifier des cibles comme étant licites[150].

Le niveau auquel l'explosion d'une arme est censée se produire pourrait correspondre à un « taux de fonctionnement fiable de 95 % »[151]. Ce taux de fiabilité est celui des armes autonomes qui font feu contre une cible illicite par suite d'une erreur de classification, une fois sur vingt. Une telle « performance » serait-elle jugée acceptable quand l'enjeu consiste à distinguer les cibles licites des cibles protégées ? Nous voyons que si une arme est considérée sous cet angle, la meilleure façon de définir la fiabilité tient dans la question suivante : « l'arme remplit-elle la fonction qui lui a été assignée ? »[152]. En outre, « les capacités en termes d'amorçage et de guidage étant de plus en plus intégrées, la fiabilité de l'acquisition de cible devra être mesurée et évaluée »[153]. Il a été suggéré que ce qu'il faudrait, c'est un « niveau de probabilité très élevé pour l'identification de cible correcte … et un niveau de probabilité très bas pour le risque que des cibles amies ou des cibles civiles soient faussement identifiées comme des

150 Voir *Defense Science Board Task Force, Munitions System Reliability*, *op. cit.*, note 132, p. 28.
151 *Ibid.*, p. 11. Même ce niveau de fiabilité est basé sur des conditions contrôlées, et un niveau plus bas est autorisé dans les conditions propres aux opérations, de manière à prendre en compte des « facteurs environnementaux tels que le terrain et les conditions météorologiques », *ibid.*, Annexe III, *DoD Policy Memo on Submunition Reliability*, p. 1 [Traduction CICR].
152 *Ibid.*, p. 14.
153 *Ibid.*, p. 16.

cibles valables – c'est-à-dire, comme des cibles ennemies »[154]. Puisqu'il existe un compromis inhérent entre sensibilité et spécificité, il convient donc de tenir également compte de la manière dont une arme sera employée. Si, sur la base d'un examen indépendant, un opérateur humain donne l'autorisation de poursuivre l'attaque ou, au contraire donne l'ordre de l'abandonner, il fournit une protection supplémentaire contre une « fausse » reconnaissance ; en ce cas, un plus grand nombre de résultats faussement positifs générés par le système automatique de reconnaissance serait acceptable. Par contre, s'il s'agit d'une arme autonome, l'effet militaire d'un emploi correct contre des cibles ennemies identifiées doit être plus scrupuleusement mis en balance avec les risques courus par les civils. Nous remarquerons ici que l'un des buts des systèmes automatisés et des systèmes autonomes est justement de prendre en charge des volumes importants de données d'observation qui submergeraient un opérateur humain : lorsque les « observations [se comptent] par millions … même un très faible risque d'erreurs pourrait provoquer de regrettables incidents fratricides »[155]. La confiance envers la capacité d'un système autonome d'opérer dans le monde réel pourrait être accrue en déployant de tels systèmes en mode semi-autonome, c'est-à-dire qu'un opérateur humain devrait donner l'approbation finale de tir[156]. Une analyse rigoureuse des données post-mission permettrait de disposer à terme d'une évaluation statistiquement importante de la fiabilité de l'arme quant à l'identification correcte des cibles licites.

Un dernier point mérite d'être relevé à propos des essais :

> Le fait de parvenir ou non à de tels résultats [accroissement des capacités, efficience du personnel et réduction des coûts grâce à une utilisation bien plus large des systèmes autonomes] dépendra de la mise au point de méthodes entièrement nouvelles qui permettent « la confiance envers l'autonomie » par le biais des procédures de vérification et de validation des états quasi illimités des systèmes qui résultent des niveaux élevés d'adaptabilité et d'autonomie. En effet, le nombre d'états d'entrée pouvant être présentés à ces systèmes est si élevé que, non seulement, il est impossible de tester directement la totalité d'entre eux, mais qu'il n'est pas même possible d'en tester davantage qu'une insignifiante fraction. La mise au point de tels systèmes est donc intrinsèquement invérifiable par les méthodes actuelles et, par conséquent, il est impossible de certifier leur fonctionnement dans la totalité des applications (quelques applications, relativement mineures, faisant exception).
>
> Il est possible de mettre au point des systèmes ayant des niveaux élevés d'autonomie, mais c'est le manque de méthodes de vérification et de validation qui empêche l'autorisation de l'utilisation de tous les niveaux d'autonomie, à l'exception des plus bas. Des adversaires potentiels, néanmoins,

154 *Ibid.*, p. 23 [Traduction CICR].
155 Voir *Report of Defense Science Board Task Force on Patriot System Performance: Report Summary*, *op. cit.*, note 60, p. 2 [Traduction CICR].
156 Voir A. Myers, *op. cit.*, note 23, pp. 91-92.

> pourraient être prêts à déployer des systèmes ayant des niveaux d'autonomie bien plus élevés sans aucun besoin de procédures certifiables de vérification et de validation: ils pourraient de ce fait obtenir d'importants avantages, en termes de capacités, sur [nos] forces aériennes. Pour compenser cet avantage asymétrique, il faudrait mettre au point des méthodes (inexistantes à ce jour) permettant de disposer de procédures fiables en matière de vérification et de validation[157].

Dans le domaine de l'armement, la recherche se distingue clairement des essais. Cette recherche (par opposition au développement) devrait-elle être limitée ou entravée par des considérations juridiques ? De manière générale, hormis les contraintes budgétaires, rien n'empêche légalement la recherche de pousser l'étude d'armes potentielles aussi loin que le permettront les limites de la science et de l'ingénierie, notamment car les lois changent[158]. Les moments opportuns pour imposer des limites sur la base du droit se situent pendant les phases de production et de déploiement des armes. Bien sûr, certains pourraient avancer des arguments différents (et ils le font) en invoquant la morale et l'éthique[159]. C'est effectivement à ce niveau que de tels arguments sont le mieux défendus et débattus.

Conclusion

Face à la complexité technologique toujours plus grande des armes et des systèmes d'armes, il est important que les informaticiens, les ingénieurs et les juristes, notamment, dialoguent les uns avec les autres chaque fois qu'un État entreprend l'examen des armes prescrit par l'article 36 du Protocole additionnel I[160]. Ces examens ne peuvent pas être « compartimentés », chaque discipline se

157 Armée de l'air des États-Unis, « Technology horizons », disponible sur : http://www.af.mil/information/technologyhorizons.asp [Traduction CICR].

158 Voir les exemples de sous-marins et d'aéroplanes auxquels il est fait référence dans K. Anderson et M. Waxman, *op. cit.*, note 29, pp. 6-7. Bien que certains aspects du droit international humanitaire soient susceptibles de changer, cette évolution ne s'étendra probablement pas aux principes cardinaux que sont les obligations de distinction et de proportionnalité ainsi que l'interdiction de causer des maux superflus.

159 Voir Matthew Bolton, Thomas Nash et Richard Moyes, « Ban autonomous armed robots », Article 36, 5 mars 2012, disponible sur : http://www.article36.org/statements/ban-autonomous-armed-robots/ : « Bien que l'attribution d'un rôle accru aux robots dans les conflits semble être un phénomène impossible à arrêter, nous devons tracer une ligne rouge à ne jamais franchir : le ciblage entièrement autonome. Une première mesure en ce sens pourrait consister à reconnaître qu'une telle ligne rouge doit effectivement concerner tous les niveaux, de la technologie relativement simple des mines terrestres anti-véhicule (encore non interdites à ce jour), jusqu'à la plupart des systèmes complexes en cours de mise au point. Il ne faudrait pas pour autant ignorer les défis que rencontrera une telle prise de position. Par exemple, il faudra peut-être examiner la manière dont l'automatisation fonctionne dans le contexte de la défense antimissiles et dans d'autres contextes similaires. Cependant, certains fondamentaux paraissent solides. La décision de tuer ou de blesser ne devrait pas être laissée à des machines et, même si elle est parfois imparfaite, la distinction entre militaires et civils devrait uniquement être faite par des humains » [Traduction CICR].

160 Voir P. Spoerri, *op. cit.*, note 54.

penchant de manière isolée sur son propre domaine technique. Au contraire, les personnes qui conduisent l'examen juridique doivent montrer qu'elles possèdent « une compréhension technique de la fiabilité et de la précision de l'arme examinée »[161], ainsi que de la manière dont l'arme sera employée dans les opérations[162]. Bien sûr, cela ne signifie pas que chacun des spécialistes – juristes, ingénieurs, informaticiens et opérateurs – doit être compétent dans toutes les disciplines ; par contre, cela signifie que chacun d'entre eux doit posséder une compréhension suffisante des autres domaines pour repérer les interactions potentielles, mener des discussions fructueuses et évaluer ses propres décisions à l'aune de leur impact sur les autres domaines en développement.

Les responsables de la mise au point des armes doivent connaître les règles essentielles du droit international humanitaire qui régissent l'emploi des armes. De leur côté, les juristes qui apportent leur point de vue dans l'évaluation de la licéité doivent être particulièrement bien informés de la manière dont l'arme examinée sera employée dans les opérations ; ils doivent utiliser cette connaissance pour faciliter l'élaboration de directives opérationnelles cohérentes, tenant compte des défis que les avancées technologiques représentent pour le droit international humanitaire. De plus, toutes les parties doivent comprendre comment les méthodes d'essais et de validation, y compris les mesures de fiabilité, doivent être élaborées et interprétées – en termes non seulement de résultats opérationnels, mais aussi de respect du droit international humanitaire.

Les informations sur les capacités d'une arme donnée étant souvent extrêmement confidentielles et « compartimentées », les juristes, les ingénieurs et les opérateurs peuvent être appelés à travailler ensemble, de manière coopérative et imaginative, pour surmonter les limitations imposées par la classification de sécurité et la compartimentation de l'accès aux informations. Une approche à envisager consisterait à élaborer des paramètres juridiques clairement énoncés pouvant être utiles lors des essais de systèmes. Une autre approche pourrait consister à concevoir des ensembles d'équations entre des critères de validation multi-paramètres. De tels ensembles d'équations permettraient de procéder à des tests d'hypothèses tout en intégrant des données relatives à la fiabilité, des niveaux de confiance et des facteurs de risque, en utilisant des données d'entrée telles que l'avantage militaire escompté, les données relatives à la fiabilité de l'arme, le degré d'incertitude des mesures de reconnaissance et les facteurs de risque pour les civils.

161 K. Lawand, *op. cit.*, note 1, p. 929 [Traduction CICR].

162 CICR, *Guide de l'examen de la licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre - Mise en œuvre des dispositions de l'article 36 du Protocole additionnel I de 1977*, *op. cit.*, note 1, pp. 17-18.

Volume 94 Sélection française 2012/2

REVUE INTERNATIONALE

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.

Volume 94 Sélection française 2012/2

REVUE INTERNATIONALE

Une boîte de Pandore ? Les frappes de drones au regard du droit : *jus ad bellum*, *jus in bello* et droit international des droits de l'homme

Stuart Casey-Maslen*

Stuart Casey-Maslen est Directeur de recherches à l'Académie de droit international humanitaire et des droits humains à Genève, et spécialiste du droit des armes et du respect des normes internationales par les acteurs armés non étatiques.

Résumé

Les drones armés sont une grave menace pour l'interdiction générale de l'usage interétatique de la force et le respect des droits de l'homme. Sur le champ de bataille, en situation de conflit armé, l'utilisation de drones armés peut permettre le respect des règles de distinction et de proportionnalité, qui sont les règles fondamentales du droit international humanitaire (bien qu'il puisse s'avérer difficile de déterminer la responsabilité pénale internationale de leur usage illégal). Hors du contexte du champ de bataille, les frappes de drones constituent souvent une violation des droits de l'homme. Il est urgent de clarifier le régime juridique qui leur est applicable et de définir des limites pour empêcher la prolifération de cette technologie.

* L'auteur remercie Andrew Clapham, Nils Melzer et Bonnie Docherty pour leurs commentaires sur le projet de cet article, ainsi qu'Alice Priddy pour ses recherches sur le sujet. Tous les sites Internet indiqués en référence ont été consultés en octobre 2012, sauf indication contraire.
La version originale en anglais de cet article est publiée sous le titre « Pandora's box? Drone strikes under *jus ad bellum*, *jus in bello*, and international human rights law », dans *International Review of the Red Cross*, Vol. 94, N° 886, été 2012, pp. 597-625.

Mots-clés: conflit armé ; participation directe aux hostilités ; drone ; droits de l'homme ; droit international humanitaire ; maintien de l'ordre ; assassinat ciblé ; véhicule aérien sans pilote.

: : : : : : : :

> « *Some have called such operations 'assassinations'. They are not, and the use of that loaded term is misplaced. Assassinations are unlawful killings.* »
> (D'aucuns ont qualifié ces opérations d'« assassinats ». L'emploi de ce terme tendancieux est inapproprié, car il ne s'agit pas d'assassinats. Un assassinat est le fait de tuer illégalement.)
>
> Eric Holder, Procureur général des États-Unis, 5 mars 2012[1]

Depuis dix ans, l'utilisation de drones – véhicules aériens ou avions sans pilote[2] – à des fins militaires et antiterroristes connaît une croissance exponentielle[3]. On rapporte, par exemple, que l'administration de Barack Obama, Président des États-Unis, aurait autorisé en 2010 plus de deux fois plus de frappes de drones dans le nord-ouest du Pakistan qu'en 2009, « année durant laquelle les attaques de drones avaient déjà été plus nombreuses que pendant la totalité du mandat de George W. Bush »[4]. Le Pentagone aurait disposé de 7 500 drones début 2012, soit environ un tiers de la flotte aérienne militaire totale des États-Unis[5]. Leur utilisation par la police pour des opérations classiques de maintien de l'ordre à l'intérieur des États devrait aussi voir une augmentation mais à un rythme moins rapide[6].

1 Discours prononcé devant la faculté de droit de la Northwestern University de Chicago le 5 mars 2012, disponible sur : http://www.lawfareblog.com/2012/03/text-of-the-attorney-generals-national-security-speech/ .

2 Selon une loi fédérale des États-Unis adoptée en 2012, le terme « avion sans pilote » désigne un « avion fonctionnant sans possibilité d'intervention humaine directe à l'intérieur ou sur l'appareil ». Article 331(8) de la Loi de modernisation et de réforme de l'administration de l'aviation fédérale (FAA Modernization and Reform Act), promulguée par le Président des États-Unis le 14 février 2012 [traduction CICR].

3 US Department of Defence, « US Unmanned Systems Integrated Roadmap (Fiscal years 2009-2034) », Washington, D.C., 2009, p. 2, disponible sur : http://www.acq.osd.mil/sts/docs/DoD%20USRM%202013.pdf (« Feuille de route pour systèmes intégrés sans pilote »).

4 Peter Bergen et Katherine Tiedemann, « Hidden War, There Were More Drone Strikes – And Far Fewer Civilians Killed », *New America Foundation*, 22 décembre 2010, disponible sur : http://newamerica.net/node/41927 .

5 W. J. Hennigan, « New drone has no pilot anywhere, so who's accountable? », dans *Los Angeles Times*, 26 janvier 2012, disponible sur : http://www.latimes.com/business/la-fi-auto-drone-20120126,0,740306.story. On s'attend à ce que les drones atteignent les mêmes proportions dans la Royal Air Force (RAF) britannique au cours des 20 prochaines années. Nick Hopkins, « Afghan civilians killed by RAF drone », dans *The Guardian*, 5 juillet 2011, disponible sur : http://www.guardian.co.uk/uk/2011/jul/05/afghanistan-raf-drone-civilian-deaths. Le Général N. A. Schwartz, Chef d'État-major de l'US Air Force, aurait jugé « concevable » que le nombre de pilotes de drones dépasse celui de pilotes en cabine dans un proche avenir, mais prédit que les forces armées aériennes conserveront des pilotes traditionnels pendant encore au moins une trentaine d'années. Elisabeth Bumiller, « A Day Job Waiting for a Kill Shot a World Away », dans *The New York Times*, 29 juillet 2012, disponible sur : http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?p.wanted=all .

6 Voir, par exemple, « Groups Concerned Over Arming Of Domestic Drones », dans *CBSDC*, Washington, D.C., 23 mai 2012, disponible sur : http://washington.cbslocal.com/2012/05/23/groups-concerned-over-arming-of-domestic-drones/ ;Vincent Kearney, « Police in Northern Ireland consider using mini drones », dans BBC, 16 novembre 2011 , disponible sur : http://www.bbc.co.uk/news/uk-

Ce sont les États-Unis d'Amérique qui, les premiers, ont déployé un nombre significatif de drones[7] pour des opérations de surveillance et de reconnaissance dans des conflits armés, d'abord au Viet Nam dans les années 1960[8], puis en Bosnie-Herzégovine et au Kosovo dans les années 1990[9]. Plus récemment, en 2012, des informations indiquent que le régime syrien utiliserait des drones pour localiser les forces rebelles[10]. Mais bien qu'ils soient utilisés comme appareils de reconnaissance ou de surveillance (et certaines forces armées ne les utilisent que dans ces fonctions), les drones sont surtout connus pour servir à exécuter des assassinats ciblés, principalement hors des frontières, en lançant des explosifs sur des « terroristes » suspectés[11].

En même temps que les progrès scientifiques permettent de construire des drones plus gros et plus rapides, la miniaturisation ouvre la voie à des appareils de la taille d'un insecte, les « nanodrones »[12], qui pourraient aussi être utilisés pour des assassinats ciblés, éventuellement par empoisonnement. En février 2011, des chercheurs ont dévoilé un prototype de drone colibri volant à 17 km/h, capable de se poser sur un appui de fenêtre[13].

northern-ireland-15759537 ; BBC, « Forces considering drone aircraft », 26 novembre 2009, disponible sur : http://news.bbc.co.uk/2/hi/uk_news/england/8380796.stm ; Ted Thornhill, « New work rotor: helicopter drones to be deployed by U.S. police forces for the first time (and it won't be long before the paparazzi use them, too) », dans *Daily Mail*, 23 mars 2012, disponible sur : http://www.dailymail.co.uk/sciencetech/article-2119225/Helicopter-drones-deployed-U-S-police-forces-time-wont-long-paparazzi-use-too.html . La Loi de modernisation et de réforme de l'administration fédérale de l'aviation (US Federal Aviation Authority Modernization and Reform Act) de 2012 laisse plus de latitude aux forces de police locale de tous les États pour utiliser leurs propres drones.

7 L'Oxford English Dictionary donne de ce mot la définition suivante : *« a remote-controlled pilotless aircraft or missile »* (avion ou missile télécommandé, sans pilote). Le mot, en vieil anglais, désignait le bourdon (insecte). Au Pakistan, à cause de leur bruit qui ressemble à un bourdonnement d'insecte, les drones sont surnommés *machay* (les guêpes) par les Pachtounes. Jane Meyer, « The Predator war », dans *The New Yorker*, 26 octobre 2009, disponible sur : http://www.newyorker.com/reporting/2009/10/26/091026fa_fact_mayer .

8 David Cenciotti, « The dawn of the robot age: U.S. Air Force testing air-launched UCAVs capable to fire Maverick and Shrike missiles in 1972 », dans *The Aviationist* (blog), 14 mars 2012, disponible sur : http://theaviationist.com/2012/03/14/the-dawn-of-the-robot-age/ .

9 « Predator Drones and Unmanned Aerial Vehicles (UAVs) », dans *New York Times*, mise à jour du 5 mars 2012, disponible sur : http://topics.nytimes.com/top/reference/timestopics/subjects/u/unmanned_aerial_vehicles/index.html .

10 « Syrian forces use drone in attack on rebel city », dans *ABC News*, 12 juin 2012, disponible sur : http://www.abc.net.au/news/2012-06-12/52-killed-in-syria-as-troops-pound-rebels-strongholds/4064990 .

11 Selon Alston, un assassinat ciblé est « l'usage intentionnel, prémédité et délibéré de la force létale par un État ou ses agents agissant sous couleur du droit, ou par un groupe armé organisé dans un conflit armé, contre un individu déterminé qui ne se trouve pas physiquement sous la garde de l'agresseur ». Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston, Addendum, Study on targeted killings, rapport au Conseil des droits de l'homme ; document ONU A/HRC/12/21/Add.6, du 28 mai 2010, para. 1, disponible sur : http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf (ci-après « 2010 Study on Targeted Killings » [traduction CICR] . Selon N. Melzer, un assassinat ciblé cumule cinq éléments : usage de la force létale, intention, préméditation et volonté de tuer ; ciblage de personnes sélectionnées individuellement ; absence de garde physique ; et imputabilité du meurtre à un sujet du droit international. Nils Melzer, *Targeted Killings in International Law*, Oxford Monographs in International Law, Oxford University Press, Oxford, 2008, pp. 3-4.

12 J. Meyer, *op. cit.*, note 7.

13 Elisabeth Bumiller et Thom Shanker, « War Evolves With Drones, Some Tiny as Bugs », dans *The New York Times*, 19 juin 2011, disponible sur : http://www.nytimes.com/2011/06/20/world/20drones.html?p.wanted=1&_r=1&ref=unmannedaerialvehicles .

Cela préfigure aussi la robotisation de la guerre et les difficultés évidentes qu'il y aurait à établir la responsabilité pénale individuelle (voir plus loin). Un article de presse paru en 2011 à ce sujet alertait sur le fait que les États-Unis s'apprêtaient à déployer des drones entièrement autonomes, capables de déterminer une cible et de faire feu sans nécessité d'intervention humaine une fois l'engin lancé[14], ce qui représente potentiellement le plus grand défi au *jus in bello* depuis le développement des armes chimiques[15]. Une étude interne sur les drones publiée en 2011 par le Ministère de la défense du Royaume-Uni affirme que : « Si nous voulons, en particulier, permettre que des systèmes prennent des décisions indépendantes de toute intervention humaine, nous aurons beaucoup à faire avant de pouvoir montrer comment ces systèmes fonctionneront légalement »[16]. Dans un même ordre d'idées, le Département de la défense des États-Unis affirmait, en 2009 :

> Parce que le Département de la défense respecte le droit des conflits armés, l'emploi d'armes dans un appareil sans pilote pose de nombreuses questions qu'il faudra résoudre... Pendant longtemps encore, sans doute, la décision de déclenchement d'un tir ou de lancement d'un missile par un appareil sans pilote restera entièrement sous le contrôle d'un opérateur humain et ne sera pas entièrement automatisée. Plusieurs aspects de la séquence de tir seront entièrement automatisés, mais la décision de faire feu ne le sera probablement pas tant que toutes les questions relatives à la légalité, aux règles d'engagement et à la sécurité n'auront pas été étudiées exhaustivement et résolues[17].

Étant donné que les drones « sont promis à un bel avenir[18] » – les « drones tueurs » seraient en effet « l'avenir de la guerre[19] », de l'avis d'un ancien juriste de la CIA – le présent article s'intéresse à la légalité des frappes de drones à l'intérieur et

14 W. J. Hennigan, « New drone has no pilot anywhere, so who's accountable? », dans *Los Angeles Times*, 26 janvier 2012, disponible sur : http://www.latimes.com/business/la-fi-auto-drone-20120126,0,740306.story .

15 Emma Slater, « UK to spend half a billion on lethal drones by 2015 », dans *The Bureau of Investigative Journalism*, 21 novembre 2011, disponible sur : http://www.thebureauinvestigates.com/2011/11/21/britains-growing-fleet-of-deadly-drones/ .

16 Development, Concepts and Doctrine Centre, *The UK Approach to Unmanned Aircraft Systems*, Joint Doctrine Note 2/11, Ministry of Defence, 2011, p. 5-2, para. 503. Il est par ailleurs dit dans ce rapport : « On évalue diversement le temps qu'il faudra pour arriver à l'intelligence artificielle (par opposition aux systèmes automatisés complexes et intelligents), mais on semble s'accorder sur le fait qu'il faudra plus de 5 ans et moins de 15 ans, certains estimant même qu'il faudra beaucoup plus de temps ». *Ibid.*, p. 5-4, para. 508 [traduction CICR].

17 US Department of Defence, *op. cit.*, note 3, p. 10 [traduction CICR].

18 Voir E. Bumiller et T. Shanker, *op. cit.*, note 13. Selon le Département de la défense des États-Unis, « les systèmes sans pilote continueront de jouer un rôle central dans les diverses opérations de sécurité [des États-Unis], et plus particulièrement dans la Guerre contre le terrorisme ». US Department of Defence, *op. cit.*, note 3, p. iii (CICR).

19 Afsheen John Radsan, « Loftier Standards for the CIA's Remote-Control Killing », Statement for the House Subcommittee on National Security & Foreign Affairs, *Legal Studies Research Paper Series, Accepted Paper No. 2010-11*, William Mitchell College of Law, St. Paul, Minnesota (États-Unis), mai 2010, disponible sur : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1604745 .

hors des frontières[20], dans le cadre des conflits armés et dans celui du maintien de l'ordre. Il abordera les interactions entre le *jus in bello,* le *jus ad bellum* et les règles régissant le maintien de l'ordre, notamment le droit international des droits de l'homme. Il se conclura par une brève analyse des problèmes que l'utilisation de drones et robots de combat posera à l'avenir au droit international.

Avant de nous lancer dans une analyse plus détaillée, il serait utile de rappeler l'article 36 du Protocole additionnel I :

> 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.

Étant donné sa nouveauté, cette méthode de guerre consistant à lancer des missiles depuis des avions sans pilote commandés par des opérateurs, souvent civils, postés à des milliers de kilomètres, les États cherchant à construire ou à acquérir des drones devraient déjà les avoir soumis à un examen poussé. L'obligation énoncée à l'article 36 devrait s'imposer au moins à tous les États signataires du Protocole additionnel I de 1977, mais on pourrait aussi soutenir que l'obligation générale de « respecter et faire respecter » le droit international humanitaire devrait inciter chaque État, partie ou non au Protocole, à procéder à un tel examen juridique[21]. Or, quand bien même les quelque 70 États supposés posséder des drones auraient réalisé des études concernant la légalité de l'utilisation de drones de combat dans un conflit armé ou pour le maintien de l'ordre, ils ne les ont pas rendues publiques[22].

20 Les autres aspects de l'utilisation des drones comme la surveillance et la reconnaissance ne sont pas étudiés dans le présent article.

21 Curieusement, dans l'étude sur le droit international humanitaire coutumier réalisée par le Comité international de la Croix-Rouge (CICR) et publiée en 2005, l'article 36 n'est pas indiqué comme faisant partie du droit coutumier, apparemment en raison d'un manque d'application pratique par les États. Indépendamment de cette lacune, il est difficile de comprendre comment il est possible de respecter les obligations coutumières interdisant l'usage d'armes de nature à frapper sans discrimination ou à causer des maux superflus ou des souffrances inutiles (respectivement règles 71 et 70 de l'étude du CICR) si les capacités des armes n'ont pas été soumises au préalable à un examen juridique permettant de vérifier leur conformité au droit. Voir CICR, *Droit international humanitaire coutumier, Vol. I: Règles*, Jean-Marie Henckaerts et Louise Doswald-Beck (éds), Cambridge University Press, Cambridge, 2005 [ci-après « Étude du CICR sur le droit international humanitaire coutumier »]. Les États-Unis, par exemple, qui ne sont pas partie au Protocole, réalisent des études détaillées sur les armes avant leur mise en service. Voir, par exemple, US Department of Defence, *op. cit.*, note 3, p. 42.

22 Voir, par exemple, Peter Bergen et Jennifer Rowland (New America Foundation), « A Dangerous New World of Drones », dans *CNN*, 1er octobre 2012, disponible sur : http://newamerica.net/node/72125 . Ce n'est, en fait, qu'au début de 2012, dix ans après la première frappe de drone, que l'administration des États-Unis a officiellement admis l'existence de son programme secret d'utilisation de drones armés. Dans une discussion en ligne sur Google+ et YouTube, le Président Obama a dit, le 31 janvier 2012, que les frappes visaient « des gens qui sont recensés comme des terroristes actifs ». Voir, par exemple, le document posté par Al Jazeera le 31 janvier 2012, disponible sur : www.youtube.com/watch?v=2TASeH7gBfQ .

Drones et *jus ad bellum*

C'est le *jus ad bellum* qui régit le recours légal d'un État à la force armée, y compris les attaques de drones, contre un autre État ou contre des acteurs armés non étatiques d'un autre État sans le consentement de celui-ci[23]. L'article 2(4) de la Charte des Nations Unies, énonce que :

> Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies.

Cryer *et al.* voient dans cet article le « principe juridique fondamental régissant l'emploi de la force », qui « reflète le droit international coutumier »[24]. Toutefois, nul n'ignore l'article 51 de la Charte, qui dispose que :

> Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales[25].

La Cour internationale de justice a commenté la notion d'agression armée perpétrée par des groupes armés équipés par un État étranger dans l'affaire *Nicaragua* dans les termes suivants :

> La Cour ne voit pas de raison de refuser d'admettre qu'en droit international coutumier la prohibition de l'agression armée puisse s'appliquer à l'envoi par un État de bandes armées sur le territoire d'un autre État si cette opération est telle, par ses dimensions et ses effets, qu'elle aurait été qualifiée d'agression armée et non de simple incident de frontière si elle avait été le fait de forces armées régulières. Mais la Cour ne pense pas que la notion d'agression armée puisse recouvrir non seulement l'action de bandes armées dans le cas où cette action revêt une ampleur particulière, mais aussi une assistance à des rebelles prenant la forme de fourniture d'armements ou d'assistance logistique ou autre. On peut voir dans une telle assistance une menace ou un

23 Ainsi, comme le fait observer Noam Lubell, le cadre du *jus ad bellum* n'est pas conçu pour restreindre l'usage de la force à l'intérieur des propres frontières d'un État. Noam Lubell, *Extraterritorial Use of Force against Non-State Actors*, Oxford Monographs in International Law, Oxford University Press, Oxford, 2011, p. 8.

24 Robert Cryer, Hakan Friman, Darryl Robinson et Elizabeth Wilmshurst, *An Introduction to International Criminal Law and Procedure*, 2nd éd., Cambridge University Press, Cambridge, 2010, p. 322 [traduction CICR].

25 Charte des Nations Unies, article 51. Hormis la légitime défense et l'emploi de la force autorisé par le Conseil de sécurité de l'ONU, l'emploi de la force dans un autre État n'est légal qu'avec le consentement de celui-ci.

emploi de la force, ou l'équivalent d'une intervention dans les affaires intérieures ou extérieures d'autres États[26].

Le seuil à partir duquel il est déterminé qu'un État a commis une agression armée est donc assez élevé et dépasse le « simple incident de frontière » entre membres des forces armées de deux États (ou de groupes armés opérant dans un État avec un soutien limité d'un autre État). D'aucuns pourraient même faire valoir qu'une frappe de drone très limitée et très ciblée menée par un État contre des personnes se trouvant dans un autre État ne constituerait pas une agression armée au sens de la Charte des Nations Unies ou du droit coutumier en invoquant le principe très contesté de la légitime défense préventive[27]. Néanmoins, en l'absence de légitime défense, le recours à la force serait sans aucun doute contraire à l'interdiction générale de la menace ou de l'emploi de la force (et constituerait donc une violation du droit international à moins que l'État « victime » n'ait consenti à l'emploi de la force)[28]. Il est presque certain que des frappes de drones plus intensives conduites hors des frontières, ressemblant à un bombardement, constitueraient une agression armée contre un autre État, en l'absence d'autorisation donnée par le Conseil de sécurité ou d'une situation de légitime défense[29].

On peut toutefois soutenir qu'une attaque de drone, même isolée, est une attaque armée susceptible de constituer une agression. En effet, l'Assemblée générale des Nations Unies a décidé, dans sa résolution 3314 (XXIX), qu'un acte d'agression était constitué, entre autres, par : « Le bombardement, par les forces armées d'un État, du territoire d'un autre État, ou l'utilisation de toutes armes par un État contre le territoire d'un autre État »[30]. Cet argument est aussi étayé par l'affaire du stratège militaire de l'Organisation de libération de la Palestine tué en 1988 à son domicile à Tunis par neuf commandos israéliens, acte que le Conseil de sécurité de l'ONU a condamné comme « agression » perpétrée en violation flagrante de la Charte des Nations Unies[31].

Si une attaque isolée de drone constitue une « agression armée », l'État qui lance le drone devra justifier son action par référence à son droit naturel de légitime défense (à moins qu'il n'ait obtenu le consentement requis ou l'autorisation du Conseil de sécurité de l'ONU) ; à défaut, il risquerait de commettre un acte d'agression[32]. Cette situation porte à controverse lorsque la légitime défense est

26 Cour internationale de justice (CIJ), *Affaire des activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique)*, Jugement, CIJ Recueil 1986, para. 195.
27 Voir, par exemple, Antonio Cassese, *International Law*, 2nd éd., Oxford University Press, Oxford, 2005, pp. 357-363.
28 Au sujet des conditions détaillées pour que le consentement soit légal, voir, par exemple, *ibid*., pp. 370-371.
29 Voir, par exemple, *ibid*., pp. 158-159.
30 AG ONU, Rés. 3314 (XXIX) du 14 décembre 1974, annexe, article 3(b).
31 CS ONU, Rés. 611 du 25 avril 1988, adoptée par 14 voix avec une abstention (États-Unis d'Amérique).
32 L'acte d'agression est généralement défini comme l'emploi de la force armée par un État contre un autre État non justifié par la légitime défense ni autorisé par le Conseil de sécurité de l'ONU. Les actions pouvant être qualifiées d'actes d'agression sont explicitement influencées par la Résolution 3314 (XXIX) de l'Assemblée générale des Nations Unies du 14 décembre 1974. Selon l'article 8 *bis* du Statut de Rome de la Cour pénale internationale de 1998, adopté par la première Conférence de révision du

invoquée, non pas contre un autre État, mais contre un acteur armé non étatique se trouvant dans un autre État. Dans l'avis consultatif émis en 2004 par la Cour internationale de justice (CIJ) sur les *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, la Cour paraît sous-entendre que la légitime défense ne peut être invoquée que par un État vis-à-vis d'un autre État[33]. Une lecture plus attentive de ces *dicta* laisse toutefois penser que la Cour n'exclut pas entièrement la possibilité de légitime défense à l'égard d'un acteur armé non étatique commettant des actes « terroristes » lorsque l'État menacé n'exerce pas le contrôle effectif[34]. Plus tard, dans l'*Affaire des activités armées sur le territoire du Congo*, la Cour a évité la question de savoir si le droit international autorisait la légitime défense « pour riposter à des attaques d'envergure menées par des forces irrégulières »[35]. L'opinion individuelle dissidente du juge Kooijmans va plus loin que les *dicta* de la Cour dans l'affaire *Édification d'un mur*, le juge affirmant que :

> si l'on se trouve dans la situation où les attaques perpétrées par des forces irrégulières auraient pu, par leurs dimensions et leurs effets, être qualifiées d'agression armée eussent-elles été le fait de forces armées régulières, rien dans les termes de l'article 51 de la Charte n'empêche l'État victime d'exercer son droit *naturel* de légitime défense[36].

Le droit coutumier traditionnel régissant le droit de légitime défense des États est né d'un incident diplomatique survenu autrefois entre les États-Unis et le Royaume-Uni, lorsque plusieurs citoyens américains se portant au secours de rebelles – dans ce qui était alors la colonie britannique du Canada – furent tués alors qu'ils transportaient des hommes et du matériel depuis le territoire américain[37]. Selon la jurisprudence de l'affaire *La Caroline,* le droit de légitime défense ne peut être exercé qu'en cas de « nécessité immédiate, impérieuse, ne laissant

Statut de Rome tenue en 2010 à Kampala, le crime d'agression est défini comme étant la planification, la préparation, le lancement ou l'exécution par une personne en situation de commandement, d'un acte d'agression. Cet acte doit constituer une « violation manifeste » de la Charte des Nations Unies (article 8 *bis*, para. 1).

33 CIJ, *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, Avis consultatif, CIJ Recueil 2004, para. 139.

34 La Cour (para. 139) se réfère aux résolutions 1368 (2001) et 1373 (2001) adoptées par le Conseil de sécurité de l'ONU après les attentats perpétrés le 11 septembre 2001 contre les États-Unis, notant « qu'Israël exerce son contrôle sur le territoire palestinien occupé et que, comme Israël l'indique lui-même, la menace qu'il invoque pour justifier la construction du mur trouve son origine à l'intérieur de ce territoire, et non en dehors de celui-ci. Cette situation est donc différente de celle envisagée par les résolutions 1368 (2001) et 1373 (2001) du Conseil de sécurité, et de ce fait Israël ne saurait en tout état de cause invoquer ces résolutions au soutien de sa prétention à exercer un droit de légitime défense ». Dans les deux résolutions mentionnées, un paragraphe du préambule reconnaît « le droit naturel de légitime défense individuelle ou collective conformément à la Charte ».

35 CIJ, *Affaire des activités armées sur le territoire du Congo* (*République démocratique du Congo c. Ouganda*), CIJ Recueil 2005, para. 147.

36 *Ibid*., Opinion individuelle du juge Kooijmans, para. 29.

37 À ce sujet, voir Christopher Greenwood, « International Law and the Pre-emptive Use of Force: Afghanistan, Al-Qaïda, and Iraq », dans *San Diego International Law Journal*, Vol. 4, 2003, p. 17 ; N. Lubell, *op. cit*., note 23, p. 35 ; et Andrew Clapham, *Brierly's Law of Nations*, 7e éd., Oxford University Press, Oxford, 2008, pp. 468-469.

ni le choix des moyens ni le temps de la réflexion », et l'acte de riposte doit être proportionné « puisque l'acte justifié par la nécessité de légitime défense doit être limité par cette nécessité et être clairement contenu dans ces limites »[38]. On s'accorde largement à voir dans ces déclarations adressées en 1842 par le Secrétaire d'État des États-Unis aux autorités britanniques une description juste du droit coutumier de l'État en matière de légitime défense[39].

Pour que le recours à la force d'un État prétendant agir en situation de légitime défense soit reconnu légitime, il faut donc qu'il satisfasse à la fois aux critères de la nécessité et de la proportionnalité. À défaut, l'emploi de la force peut même constituer une agression. Dans un avis consultatif rendu en 1996 sur la *Licéité de la menace ou de l'emploi d'armes nucléaires,* la CIJ a déclaré que ces deux conditions interdépendantes constituaient une règle du droit international coutumier[40]. Selon le principe de nécessité, « l'État agressé (ou menacé d'agression imminente si l'on admet la légitime défense préventive) ne doit en l'occurrence pas avoir eu d'autre moyen pour arrêter l'agression que le recours à l'emploi de la force armée »[41]. La proportionnalité, en revanche, est un principe un peu plus abstrus, car si le terme comporte généralement l'idée d'un équilibrage (souvent entre concepts opposés), l'intention, dans le contexte qui nous occupe, est assez différente :

> L'exigence dite de la *proportionnalité* de l'action commise en état de légitime défense a trait... au rapport entre cette action et le but qu'elle se propose d'atteindre, à savoir... d'arrêter et de repousser l'agression... Il serait par contre erroné de croire que la proportionnalité doive exister entre le comportement constituant l'agression armée et celui qu'on lui oppose. Il se peut très bien que l'action requise pour stopper et rejeter l'agression doive prendre des proportions qui ne correspondent pas à celles de l'agression subie... Sa licéité ne doit donc se mesurer qu'à son aptitude à atteindre le résultat recherché. On peut d'ailleurs dire que les exigences de la « nécessité » et de la « proportionnalité » de l'action menée en légitime défense ne sont que les deux faces d'une même médaille[42].

38 Lettre de M. Webster, US Department of State, Washington, D.C., à Lord Ashburton, en date du 27 juillet 1842 [traduction CICR].

39 Voir, par exemple, A. Clapham, *op. cit.*, note 37, pp. 469-470.

40 « Ainsi que la Cour l'a déclaré dans l'affaire des *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. États-Unis d'Amérique*), il existe une 'règle spécifique bien établie en droit international coutumier' selon laquelle la légitime défense ne justifierait que des mesures proportionnées à l'agression armée subie, et nécessaires pour y riposter ». La Cour relève que cette double condition « s'applique également dans le cas de l'article 51 de la Charte, quels que soient les moyens mis en œuvre ». CIJ, *Licéité de la menace ou de l'emploi des armes nucléaires*, Avis consultatif, CIJ Recueil 1996, para. 41.

41 « Additif au huitième rapport sur la responsabilité des États, par M. Roberto Ago, Rapporteur spécial – Le fait internationalement illicite de l'État, source de responsabilité internationale (Première partie) », Extrait de l'Annuaire de la Commission du droit international, 1980, vol. II (1), Document ONU A/CN.4/318/Add.5-7, para. 120.

42 *Ibid.*, para. 121.

Ce point de vue, en particulier l'idée que l'efficacité avec laquelle la riposte réussit à faire cesser une agression armée détermine la proportionnalité[43], a été exprimé indirectement par la CIJ dans d'autres affaires. Dans l'affaire de 2003 *Plateformes pétrolières (Iran c. États-Unis d'Amérique)*, la Cour a conclu de la façon suivante :

> S'agissant de l'exigence de proportionnalité, la Cour, si elle avait conclu à la nécessité des attaques du 19 octobre 1987 en réponse à l'incident du *Sea Isle City* vu comme une agression armée commise par l'Iran, aurait pu considérer qu'elles y satisfaisaient. En revanche, l'attaque du 18 avril 1988 fut planifiée et menée dans le cadre d'une opération plus vaste baptisée opération « Praying Mantis »…. En réponse au mouillage, par un auteur non identifié, de la mine que devait heurter un seul navire de guerre américain, lequel, s'il fut gravement endommagé, ne sombra toutefois pas et dont l'équipage n'eut à déplorer aucune perte en vie humaine, ni l'opération « Praying Mantis » dans son ensemble, ni même le volet de celle-ci qu'a constitué la destruction des plates-formes de Salman et de Nasr ne sauraient être considérés, dans les circonstances de l'espèce, comme un emploi proportionné de la force au titre de la légitime défense[44].

Une incertitude demeure en ce qui concerne tant l'application de l'emploi de la force que le degré précis auquel il devient licite en situation de légitime défense[45]. Néanmoins, on peut supposer qu'un État qui utilise un drone armé dans une opération hors de ses frontières sans avoir obtenu le consentement de l'État sur le territoire duquel se trouve le « terroriste » visé ne peut revendiquer un droit de légitime défense que si la menace ou l'usage de la force à son encontre constitue une agression armée[46]. La menace d'une attaque « terroriste » isolée, plus limitée, ne serait donc pas suffisante. Cela peut avoir des incidences importantes, notamment dans le cas de l'utilisation par Israël de drones armés sur le territoire palestinien. Il semblerait aussi, en tout état de cause, que d'après l'article 51 de la Charte des Nations Unies, l'utilisation d'un drone armé par un État qui prétendrait agir en situation de légitime défense contre un autre État ou sur le territoire d'un autre État, devrait être notifié

43 Voir, par exemple, Elizabeth Wilmshurst, « Principles of international law on the use of force by states in self-defence », Chatham House Working Paper, octobre 2005, pp. 7, 8 et 10, disponible sur : http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/ilpforce.doc .

44 CIJ, *Affaire des plates-formes pétrolières, République islamique d'Iran c. États-Unis d'Amérique*, Arrêt, CIJ Recueil 2003, para. 77.

45 Y compris lorsqu'un droit de légitime défense est invoqué du fait d'attaques répétées de faible intensité par des acteurs non étatiques. Voir, à cet égard, l'étude du Rapporteur spécial « 2010 Study on targeted killings », *op. cit.*, note 11, para. 41.

46 Comme l'affirme Alston, « il n'arrive que très exceptionnellement qu'un acteur non étatique dont les activités n'engagent la responsabilité d'aucun État puisse mener une attaque armée de nature à créer un droit de riposter par l'emploi extraterritorial de la force ». Rapporteur spécial, « 2010 Study on Targeted Killings », *op. cit.*, note 11, para. 40 [traduction CICR].

immédiatement au Conseil de sécurité pour être licite[47]. À la connaissance de l'auteur, cela ne s'est encore jamais produit[48].

Les drones et le droit international humanitaire

Théoriquement, l'utilisation de drones sur le champ de bataille est relativement peu controversée au regard du *jus in bello* (sans préjudice du *jus ad bellum*) parce que, concrètement, il n'y a guère de différence entre l'utilisation d'un missile de croisière ou un bombardement aérien et l'utilisation d'un drone équipé d'armes explosives[49]. En effet, d'après le Rapporteur spécial des Nations Unies sur les exécutions extrajudiciaires, sommaires et arbitraires, « bien que, dans la plupart des circonstances, les assassinats ciblés violent le droit à la vie, dans les circonstances exceptionnelles d'un conflit armé, ils peuvent être licites »[50]. Que l'utilisation de drones armés constitue une agression ou un acte de légitime défense, si elle s'inscrit dans le contexte d'un conflit armé et satisfait au critère du lien *(nexus)* pertinent (voir, plus loin, le paragraphe sur le lien de belligérance), elle sera jugée au regard du droit applicable, le *jus in bello*[51]. Les frappes devront ainsi respecter au moins les règles du DIH applicables à la conduite des hostilités, notamment celles de la précaution dans l'attaque, de la distinction et de la proportionnalité, et ne pas utiliser d'armes dont l'usage n'est pas admis par le DIH. Nous examinerons ces règles une par une ci-dessous.

47 « Les mesures prises par des membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité ». Alston va plus loin en faisant valoir que la Charte des Nations Unies imposerait de demander l'accord du Conseil de sécurité. *Ibid*., para. 40.

48 De plus, même dans le cas d'opérations menées dans un État qui, dans les faits – et quoiqu'il s'en défende publiquement à intervalles réguliers – consent au moins implicitement à l'utilisation de drones sur son territoire, le fait d'utiliser des drones pour cibler des « terroristes » n'a pas la large faveur de l'opinion publique. Dans un entretien accordé à *Voice of America* le 31 janvier 2012, un porte-parole du Ministère des affaires étrangères du Pakistan a qualifié les frappes de missiles américains d'« illégales, contreproductives et inacceptables, perpétrées en violation de la souveraineté du Pakistan », alors même qu'il avait été dit que ces frappes avaient été exécutées avec l'aide des services de renseignement pakistanais. « Obama's drone strikes remark stirs controversy », *Voice of America*, 31 janvier 2012, disponible sur : http://www.voanews.com/content/pakistan-repeats-condemnation-of-drone-strikes-138417439/151386.html .

49 Les États-Unis font un usage soutenu des drones en Afghanistan depuis 2001 ; la toute première frappe aurait eu lieu durant l'invasion de novembre 2001 et qu'elle aurait eu pour cible une réunion de haut niveau d'Al-Qaïda à Kaboul. Voir, par exemple, John Yoo, « Assassination or targeted killings after 9/11 », dans *New York Law School Law Review*, Vol. 56, 2011/12, p. 58, citant lui-même James Risen, « A nation challenged : Al Qaeda, Bin Laden aide reported killed by US bombs », dans *The New York Times*, 17 novembre 2001, p. A1, disponible sur : http://www.nytimes.com/2001/11/17/world/a-nation-challenged-al-qaeda-bin-laden-aide-reported-killed-by-us-bombs.html. À partir d'avril 2011, les drones ont aussi été utilisés dans le conflit armé libyen, notamment lors de la célèbre attaque du convoi transportant le dirigeant libyen destitué Muammar Khadafi à la sortie de Syrte en octobre de cette même année.

50 « 2010 Study on Targeted Killings », *op. cit*., note 11, para. 10.

51 Ainsi, des actes qui sont illicites en vertu du *jus in bello* ne constitueraient pas nécessairement une riposte disproportionnée si l'on devait déterminer si des actes commis en situation de légitime défense sont licites au regard du *jus ad bellum*.

Les précautions dans l'attaque

Le respect des règles concernant les précautions à prendre lors des attaques et le respect des autres règles coutumières applicables à la conduite des hostilités, notamment les règles de la distinction (ou discrimination) et de la proportionnalité sont directement liés, de même que l'interdiction de l'utilisation de moyens ou de méthodes de guerre de nature à causer des maux superflus ou des souffrances inutiles. La plupart des règles concernant les précautions dans l'attaque, qui ont été codifiées dans le Protocole additionnel I de 1977, sont des règles coutumières qui s'appliquent dans les conflits armés non internationaux et les conflits armés internationaux, selon l'étude publiée en 2005 par le Comité international de la Croix-Rouge. Au cœur de ces règles se trouve l'obligation de « veiller constamment », dans la conduite des opérations, à « épargner la population civile, les personnes civiles et les biens à caractère civil ». À cet égard,

> « (t)outes les précautions pratiquement possibles doivent être prises 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 »[52].

L'article 57 du Protocole prévoit que ceux qui préparent ou décident une attaque doivent « prendre toutes les précautions pratiquement possibles quant au choix des moyens et méthodes d'attaque »[53].

On peut invoquer plusieurs raisons pour soutenir que les frappes de drones sont à même de satisfaire aux exigences de précaution dans l'attaque. Premièrement, un signal vidéo transmis par le drone permet de voir la cible « en temps réel », de sorte que l'on peut s'assurer de l'absence de civils à proximité de la cible jusqu'aux dernières minutes, voire aux dernières secondes[54]. Deuxièmement, il apparaît qu'au moins certaines des cibles des drones sont repérées à l'aide d'un dispositif de repérage apposé (ou peint) sur le véhicule, sur un bagage ou un équipement de la personne ciblée, voire sur la personne elle-même ou l'une des personnes ciblées. Troisièmement, dans certains cas (notamment sur le sol afghan) des forces armées postées à proximité sont aussi chargées de surveiller la cible. Quatrièmement, à l'exception de la version thermobarique des missiles Hellfire[55], la plupart des missiles lancés par des drones sont censés avoir

52 Étude du CICR sur le droit international humanitaire coutumier, *op. cit.*, note 21, règle 15.

53 Protocole additionnel I de 1977, article 57(2)(a)(ii).

54 Un ancien responsable des services antiterroristes à la Maison Blanche, resté anonyme, aurait en revanche affirmé « qu'il y a tellement de drones » dans le ciel pakistanais que des querelles ont éclaté pour savoir quels opérateurs à distance pouvaient se prévaloir de telle ou telle cible, provoquant des « problèmes de commandement et de contrôle ». Voir J. Meyer, *op. cit.*, note 7.

55 Selon le site Internet d'un fabricant d'armement des États-Unis, le missile air-sol Hellfire version AGM-114N est muni d'une tête thermobarique à charge métallique augmentée capable d'aspirer l'air hors d'une cave, de provoquer l'effondrement d'un bâtiment ou de produire, à l'extérieur, « un effet de souffle dans un rayon prodigieusement étendu ». « US Hellfire missile orders, FY 2011-2014 », dans

un rayon d'action moindre que les autres munitions classiques généralement tirées d'avions de combat. Ces facteurs ne suppriment pas le risque de faire des victimes civiles, mais ils constituent certainement des précautions pratiquement possibles permettant de réduire au minimum les pertes de vies humaines dans la population civile qui pourraient être causées incidemment[56].

On ne saurait toutefois nier qu'il y ait eu de sérieux échecs, comme l'opération menée en 2010 en Afghanistan durant laquelle 23 civils afghans ont été tués et 12 autres blessés par une attaque par drone[57]. En mai 2010, les forces armées américaines ont publié un rapport sur cet incident indiquant que la communication « d'informations inexactes et dénotant un manque de professionnalisme » par les opérateurs du drone Predator étaient à l'origine de la mort d'un groupe de civils composé d'hommes, de femmes et d'enfants visé par une attaque aérienne en février 2010[58]. D'après ce rapport, quatre officiers américains, dont un commandant de brigade et de bataillon, ont été réprimandés et deux officiers subalternes ont fait l'objet de mesures disciplinaires. Le Général Stanley A. McChrystal, qui a présenté des excuses au Président afghan Hamid Karzai après l'attaque, a annoncé une série de mesures de formation destinées à empêcher que de tels événements se reproduisent. Il a également demandé aux commandants de l'armée de l'air d'ouvrir une enquête sur les opérateurs du Predator[59].

Defence Industry Daily, 10 janvier 2012, disponible sur : http://www.defenseindustrydaily.com/US-Hellfire-Missile-Orders-FY-2011-2014-07019/.

56 On notera, cependant, la prudence dont fait preuve à cet égard Alston : « Les partisans des drones soutiennent que, puisque les drones offrent une capacité de surveillance supérieure et une plus grande précision que les autres armes, ils permettent de réduire le nombre de victimes et de blessés collatéraux parmi la population civile. C'est peut-être vrai dans une certaine mesure, mais c'est une image incomplète. La précision et la licéité d'une frappe dépendent des renseignements humains sur lesquels repose la décision de ciblage ». « 2010 Study on Targeted Killings », *op. cit.*, note 11, para. 81 [traduction CICR]. En effet, Daniel Byman avance l'argument suivant : « Réduire le nombre de victimes nécessite de disposer de services de renseignement de premier ordre. Les opérateurs doivent non seulement savoir où se trouvent les terroristes, mais aussi qui est avec eux et qui risque de se trouver dans le rayon de souffle. La surveillance n'est souvent pas exercée à un tel niveau, et l'utilisation délibérée par les terroristes d'enfants et d'autres civils comme boucliers humains rend plus probable encore la mort de civils dans l'opération. » Daniel L. Byman, « Do Targeted Killings Work? », *Brookings Institution*, 14 juillet 2009, disponible sur : http://www.brookings.edu/opinions/2009/0714_targeted_killings_byman.aspx.

57 « First Drone Friendly Fire Deaths », dans *RT*, 12 avril 2011, disponible sur : http://rt.com/usa/news/first-drone-friendly-fire/. En octobre 2011, le Département de la défense des États-Unis a conclu que des erreurs de communication entre membres du personnel militaire avaient été à l'origine, en avril de la même année, de la frappe au cours de laquelle deux soldats américains avaient été tués par erreur en Afghanistan. « Drone strike killed Americans », dans *RT*, 17 octobre 2011, disponible sur : http://rt.com/usa/news/drone-american-military-report-057/ .

58 Dexter Filkins, « Operators of Drones Are Faulted in Afghan Deaths », dans *New York Times*, 29 mai 2010, disponible sur : http://www.nytimes.com/2010/05/30/world/asia/30drone.html. Le rapport, signé du général de division T. P. McHale, établissait que les opérateurs du Predator au Nevada et des « postes de commandement inefficaces » de la zone n'avaient pas transmis au commandant de terrain des informations sur la présence de civils dans les camions. Selon des responsables militaires à Washington et en Afghanistan qui se sont exprimés sous le couvert de l'anonymat, des analystes des services de renseignement qui surveillaient le signal vidéo du drone ont à deux reprises envoyé des messages électroniques pour prévenir les opérateurs du drone et les postes de commandement au sol de la présence visible d'enfants.

59 *Ibid.*

La question du nombre de civils tués par des frappes de drones divise fortement[60]. Selon un article paru en mai 2012 dans *The New York Times,* l'administration Obama a opté pour une méthode de dénombrement des victimes civiles consistant à « compter effectivement comme combattants tous les hommes d'une zone de frappe en âge de servir... à moins que leur innocence soit expressément prouvée à titre posthume par des informations des services de renseignement »[61]. À la lumière de ces événements, l'« extraordinaire affirmation » du conseiller principal du Président Obama pour la lutte antiterroriste, John O. Brennan, selon laquelle il n'y aurait eu « aucune victime collatérale » au cours des 12 mois écoulés paraît d'une exactitude très discutable[62].

La règle de la distinction

Cette règle, que l'on peut considérer comme la plus fondamentale de toutes les règles du DIH, est beaucoup plus simple à appliquer dans un conflit armé international que dans un conflit ne présentant pas un caractère international. L'utilisation de drones de combat ne semble être confirmée jusqu'ici que dans deux conflits armés internationaux, celui auquel ont pris part les États-Unis et leurs alliés en Afghanistan (contre les forces talibanes, et non pas contre Al-Qaïda[63]) en 2001-2002[64], et celui qui a opposé les forces armées des États membres de l'OTAN à la Libye en 2011. Il est aussi avéré, par ailleurs, que des frappes de drones aient eu lieu en 2003-2004 lors de

60 Voir, par exemple, Chris Woods, « Analysis: CNN expert's civilian drone death numbers don't add up », dans *The Bureau of Investigative Journalism*, 17 juillet 2012, disponible sur : http://www.thebureauinvestigates.com/2012/07/17/analysis-cnn-experts-civilian-drone-death-numbers-dont-add-up/ .

61 Jo Becker et Scott Shane, « Secret 'Kill List' Proves a Test of Obama's Principles and Will », dans *New York Times*, 29 mai 2012, disponible sur : http://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?_r=1&pagewanted=all .

62 « Le Bureau du journalisme d'enquête » (*Bureau of Investigative Journalism*), qui suit le bilan des opérations, a recensé entre 63 et 127 victimes non activistes en 2011, d'après des « décomptes crédibles des médias », et une enquête de l'agence Associated Press a récemment établi qu'au moins 56 villageois et membres de milices tribales avaient été tués au cours des 10 frappes les plus importantes menées depuis août 2010. Toutefois, des analystes, des représentants du gouvernement américain et même de nombreux chefs de tribus reconnaissent que les drones sont de plus en plus précis. Sur les dix frappes qui ont eu lieu cette année, il n'y aurait eu, selon les organes d'information locaux, qu'un cas entraînant des victimes civiles. Dans tous les autres cas, 58 personnes tuées selon des estimations modérées, les victimes étaient des activistes ». Declan Walsh, Eric Schmitt et Ihsanullah T. Mehsud, « Drones at Issue as U.S. Rebuilds Ties to Pakistan », dans *New York Times*, 18 mars 2012, disponible sur : http://www.nytimes.com/2012/03/19/world/asia/drones-at-issue-as-pakistan-tries-to-mend-us-ties.html?pagewanted=all . Pour une défense argumentée des frappes de drones et de l'idée que le nombre de victimes dans la population civile serait largement exagéré, voir, par exemple, Gregory S. McNeal, « Are Targeted Killings Unlawful? A Case Study in Empirical Claims Without Empirical Evidence », dans C. Finkelstein, J. D. Ohlin et A. Altmann (éd.), *Targeted Killings, Law and Morality in an Asymmetrical World*, Oxford University Press, Oxford, 2012, pp. 326-346.

63 De l'avis de l'auteur, il est préférable de classer la lutte menée contre Al-Qaïda en Afghanistan depuis 2001 séparément, comme un conflit armé non international.

64 Le conflit contre les talibans a changé de caractère après la *Loya Jirga* qui a élu Hamid Karzai à la présidence en juin 2002. Sur la question de la qualification des conflits armés en Afghanistan, voir, par exemple Robin Geiss et Michael Siegrist, « Le conflit armé en Afghanistan a-t-il un impact sur les règles relatives à la conduite des hostilités ? », dans *Revue internationale de la Croix-Rouge*, Vol. 93, *Sélection française 2011/1*, en particulier pp. 66 et suiv.

l'attaque contre l'Iraq[65] qui faisait partie du conflit armé international opposant les États-Unis (et leurs alliés) au régime de Saddam Hussein.

Hormis ces exemples, il est clair que l'écrasante majorité des frappes de drones lors de conflits armés se sont produites lors de conflits non internationaux : elles ont été le fait des États-Unis et du Royaume-Uni en Afghanistan à partir de juin 2002[66], et des États-Unis au Pakistan[67], en Somalie[68] et au Yémen[69]. En Iraq, des drones non armés sont maintenant utilisés par le Département d'État américain à des fins de surveillance uniquement[70] ; des drones armés y ont été utilisés dans le passé, avec des résultats mitigés[71]. En Inde, les Forces spéciales indiennes utilisent des drones, mais qui ne seraient pas armés, pour repérer automatiquement les combattants maoïstes[72].

Cela étant, la règle de distinction qui s'applique – distinction entre les objectifs militaires légitimes et les civils et objets civils – est normalement celle qui régit la conduite des hostilités dans les conflits armés ne présentant pas un caractère international. Seuls des objectifs militaires légitimes, incluant les civils « qui participent directement aux hostilités », peuvent légitimement être pris pour cibles des attaques, selon les dispositions de l'article 3 commun aux quatre Conventions de Genève complétées par le droit international coutumier (et, le cas échéant, l'article 13(3) du Protocole additionnel II de 1977)[73].

65 Voir, par exemple, « Unmanned aerial vehicles (UAVs) », dans *GlobalSecurity.org*, modifié en dernier lieu le 28 juillet 2011, disponible sur : http://www.globalsecurity.org/intell/systems/uav-intro.htm .

66 L'Australie et le Canada utiliseraient des drones Heron non armés. Voir, par exemple, « Canada, Australia Contract for Heron UAVs », dans *Defense Industry Daily*, 17 juillet 2011, disponible sur : http://www.defenseindustrydaily.com/Canada-Contracts-for-Heron-UAVs-05024/ .

67 Voir, par exemple, « US drone strike kills '16' in Pakistan », dans *BBC*, 24 août 2012, disponible sur : http://www.bbc.co.uk/news/world-asia-19368433. Il n'est pas certain, par contre, que la situation au Pakistan soit aujourd'hui un conflit armé sous le droit international.

68 La première frappe de drone contre les forces d'Al-Shabaab aurait eu lieu fin juin 2011. Declan Walsh, « US begins drone strikes on Somalia militants », dans *The Guardian*, 1er juillet 2011, p. 18.

69 Voir, par exemple, Ahmed Al Haj, « Khaled Batis Dead: U.S. Drone Strike In Yemen Reportedly Kills Top Al Qaeda Militant », dans *Huffington Post*, 2 septembre 2012, disponible sur : http://www.huffingtonpost.com/2012/09/02/khaled-batis-dead_n_1850773.html ; Hakim Almasmari, « Suspected U.S. drone strike kills civilians in Yemen, officials say », dans *CNN*, 4 septembre 2012, disponible sur : http://edition.cnn.com/2012/09/03/world/meast/yemen-drone-strike/index.html .

70 Eric Schmitt et Michael S. Schmidt, « U.S. Drones Patrolling its Skies Provoke Outrage in Iraq », dans *The New York Times*, 29 janvier 2012, disponible sur : http://www.nytimes.com/2012/01/30/world/middleeast/iraq-is-angered-by-us-drones-patrolling-its-skies.html?pagewanted=all .

71 J. Meyer, *op. cit.*, note 7.

72 Nishit Dholabhai, « Scanner in sky gives fillip to Maoist hunt », dans *The Telegraph* (Inde), Calcutta, 16 janvier 2012, disponible sur : http://www.telegraphindia.com/1120117/jsp/nation/story_15015539.jsp .

73 Les États-Unis ne sont pas partie à ce protocole, contrairement à l'Afghanistan. Quand bien même les États-Unis adhéreraient au Protocole, ils feraient peut-être valoir que, d'après son article premier, cet instrument ne s'appliquerait qu'à l'Afghanistan et/ou que son application extraterritoriale aux attaques menées au Pakistan serait exclue. L'article premier dispose, en effet, que le Protocole s'applique « à tous les conflits armés... 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 le présent Protocole ». Pour avoir une vue plus complète de l'application du protocole en Afghanistan, au moins à tous les États parties à cet instrument, voir, par exemple, le projet Rule of Law in Armed Conflict (RULAC), Australia profile, Qualification of Armed Conflicts Section, notamment la note 2, disponible sur : http://www.geneva-academy.ch/RULAC/ .

Le *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire* du CICR est très contestable à certains égards. Personne ne semble prétendre que le DIH interdise de prendre pour cible les forces armées d'un État partie à un conflit armé non international en certaines circonstances[74]. Ce qui est beaucoup plus discutable, en revanche, c'est l'affirmation selon laquelle des membres (militaires) de groupes armés organisés qui sont partie à un tel conflit satisfont aussi aux critères requis du fait d'une prétendue « fonction de combat continue »[75]. Ceux qui exercent ainsi une fonction de combat continue peuvent, en principe, être visés à tout moment par une attaque (cette possibilité générale étant cependant soumise à la règle de la nécessité militaire). Alston fait ainsi observer que :

> la création d'une catégorie « fonction de combat continue » constitue, de fait, une détermination de statut contestable puisque, selon la formulation employée dans le traité, la participation directe est limitée « pendant la durée de l(a) participation », par opposition à « à tout moment »... La création de cette catégorie de fonction de combat continue accroît le risque que soit pris à tort pour cible quelqu'un qui, par exemple, s'est désengagé de sa fonction[76].

Identifier ces membres militaires, sur le plan juridique et pratique, est une difficulté supplémentaire. Le *Guide interprétatif du CICR* indique que :

> au regard du DIH, le critère décisif pour déterminer l'appartenance individuelle à un groupe armé organisé consiste à savoir si une personne assume, pour le groupe, une fonction continue impliquant sa participation directe aux hostilités (ci-après: « fonction de combat continue »). [Cette fonction]... établit plutôt une distinction entre, d'une part, les membres des forces combattantes organisées d'une partie non étatique et, d'autre part, les civils qui participent directement aux hostilités de manière purement spontanée, sporadique ou non organisée, ou qui assument des fonctions exclusivement non combattantes, par exemple de caractère politique ou administratif[77].

Les personnes qui participent aux hostilités d'une manière spontanée, sporadique ou non organisée ne peuvent être légitimement prises pour cible que pendant leur participation (mais elles peuvent, en d'autres temps, être arrêtées dans

74 Voir Nils Melzer, *Guide interprétatif sur la notion de participation directe aux hostilités dans le droit international humanitaire*», CICR, Genève, 2009, pp. 32-33 (ci-après Guide interprétatif du CICR).

75 *Ibid.*, pp. 29-30.

76 « 2010 Study on Targeted Killings », *op. cit.*, note 11, paras 65-66 [traduction CICR].

77 Guide interprétatif du CICR, *op. cit.*, note 74, p. 35. Selon N. Melzer, la fonction de combat continue « peut également se déduire d'un comportement concluant, par exemple lorsqu'une personne participe aux hostilités directement et de manière répétée, pour soutenir un groupe armé organisé dans des circonstances indiquant qu'une telle conduite constitue une fonction continue et non pas un rôle spontané, sporadique ou temporaire, assumé pendant la durée d'une opération particulière». *Ibid.*, p. 37 ; voir aussi Nils Melzer, « Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation In Hostilities », dans *New York University Journal of International Law and Politics*, Vol. 42, 2010, p. 890 (ci-après, « Keeping the Balance »).

une opération de maintien de l'ordre et poursuivies en vertu du droit national pour les infractions commises). Celles qui exercent des fonctions exclusivement non combattantes, par exemple à caractère politique ou administratif, ne peuvent légitimement être visées par des attaques à moins qu'elles ne participent directement aux hostilités, et seulement pendant le temps où elles exercent de telles activités[78]. En cas de doute quant à son statut, une personne doit être considérée comme un civil ne participant pas directement aux hostilités[79].

Sur cette base, l'usage de la force létale contre un militant d'Al-Qaïda en Afghanistan qui planifie, dirige ou exécute une attaque contre l'armée américaine, par exemple, serait donc, *a priori*, licite au regard de la règle de la distinction existant en DIH. Prendre pour cible son fils, sa fille, son épouse ou ses épouses ne le serait que si ces personnes participent directement aux hostilités (et seulement pendant la durée de leur participation)[80]. La légalité de l'attaque contre le militant, si l'on s'attend, par ailleurs, qu'elle tue ou blesse incidemment des civils, dépendra de la détermination établie au regard de la règle de la proportionnalité (voir, plus loin, la sous-section sur la proportionnalité de l'attaque).

Si une telle distinction n'est pas opérée durant l'attaque, celle-ci sera illicite et sera un fait constitutif de crime de guerre[81]. En mars 2012, le cabinet

78 Brigadier-General Watkin propose, quant à lui, d'élargir sensiblement la catégorie des personnes qui relèveraient de cette définition, en incluant notamment celles qui exercent exclusivement des fonctions « d'appui aux combattants », telles que les cuisiniers et le personnel administratif. Kenneth Watkin, « Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in the Hostilities' Interpretive Guidance », dans *New York University Journal of International Law and Politics*, Vol. 42, 2010, p. 692, disponible sur : http://www.law.nyu.edu/ecm_dlv1/groups/public/@nyu_law_website__journals__journal_of_international_law_and_politics/documents/documents/ecm_pro_065932.pdf . Voir N. Melzer, « Keeping the Balance », *op. cit.*, note 77, pp. 848-849.

79 Selon la recommandation VIII du Guide interprétatif du CICR : « Toutes les précautions pratiquement possibles doivent être prises au moment de déterminer si une personne est une personne civile et, en ce cas, si cette personne civile participe directement aux hostilités. En cas de doute, la personne doit être présumée protégée contre les attaques directes ». *Guide interprétatif du CICR*, *op. cit.*, note 74, p. 77. Voir également N. Melzer, « Keeping the balance », *op. cit.*, note 77, notamment pp. 874-877. Radsan affirme que : « Sauf dans des circonstances exceptionnelles, les services ne peuvent frapper que s'ils sont convaincus au-delà de tout doute raisonnable que leur cible est un combattant en action d'Al-Qaïda ou d'un groupe terroriste similaire. Les frappes de drones sont, en effet, des exécutions ne laissant aucune possibilité réaliste de recours devant les tribunaux par *habeas corpus* ou sous une autre forme de procédure ». A.J. Radsan, *op. cit.*, note 19, p. 3 [traduction CICR]. On peut regretter de voir l'auteur affirmer, plus loin : « Il existe, bien entendu, des exceptions à ce que je formule comme une règle générale concernant le ciblage par la CIA. Je résume ces exceptions sous l'étiquette de 'circonstances extraordinaires' ; par exemple une cible jouant un rôle irremplaçable dans Al-Qaïda, ou un opérateur de drone voyant une personne sur l'écran qui est probablement Ben Laden, mais sans en avoir la certitude absolue. Même dans ces cas, l'avantage militaire qu'il y aurait à tuer Ben Laden plutôt qu'un terroriste de second rang justifie parfois que l'on prenne aussi le risque de tuer ou blesser par erreur un paisible civil ». *Ibid.*, p. 5.

80 À cet égard, Melzer note que, selon la déclaration des États-Unis dans le contexte du Protocole facultatif relatif à la Convention relative aux droits de l'enfant concernant l'implication d'enfants dans les conflits armés, « 'participer directement aux hostilités' : i) s'entend d'actes immédiats et effectifs sur le champ de bataille susceptibles de causer un dommage à l'ennemi parce qu'il y a un lien de causalité direct entre ces actes et le dommage causé à l'ennemi ; et ii) ne s'entend pas d'actes de participation indirecte aux hostilités, comme la collecte et la transmission de renseignements militaires, le transport d'armes, de munitions et d'autres fournitures, ni du déploiement avancé ». Voir N. Melzer, « Keeping the balance », *op. cit.*, note 77, p. 888 et note 226.

81 À cet égard, les affirmations selon lesquelles les frappes de drones de la CIA ont souvent pris pour cible des cortèges funèbres ou les personnes venues au secours des victimes de frappes de drones sont

d'avocats britannique Leigh Day & Co et l'organisme de bienfaisance Reprieve ont engagé des poursuites contre le Ministre des affaires étrangères du Royaume-Uni, William Hague, au nom de Noor Khan, dont le père Malik Daud Khan avait été tué lors d'une frappe aérienne au Pakistan en 2011 « alors qu'il présidait un paisible conseil de sages tribaux »[82].

En 2009, les médias ont rapporté que les noms de quelque 50 barons de la drogue afghans soupçonnés de participer au financement des talibans avaient été ajoutés à la *Joint Integrated Prioritized Target List*, la liste des cibles terroristes approuvée par le Pentagone, déjà longue de 367 noms[83]. Les personnes qui cultivent, distribuent ou vendent des stupéfiants sont *a priori* des criminels ; toutefois, même s'ils financent délibérément ou non le terrorisme, ils ne participent pas directement aux hostilités en Afghanistan[84]. Diriger des frappes de drones contre des criminels serait donc contraire au droit.

La règle de la proportionnalité

Même lorsque la cible d'une opération est un objectif militaire légitime au regard du DIH, se pose la question de la proportionnalité, qui peut avoir des incidences sur le choix des moyens et méthodes de guerre pouvant légitimement être mis en œuvre, ou même empêcher le lancement d'une attaque. Une attaque qui ne respecterait pas la règle de la proportionnalité serait une attaque sans discrimination, selon le Protocole additionnel I de 1977[85]. Cette règle ne figure ni dans l'article 3 commun aux Conventions de Genève, ni dans le Protocole additionnel II de 1977, mais elle est considérée comme une règle coutumière du DIH applicable aux conflits armés internationaux comme aux conflits armés ne présentant pas un caractère international. La Règle 14 de l'étude du CICR sur le droit international humanitaire coutumier est ainsi formulée :

> Il est interdit de lancer des attaques dont on peut attendre qu'elles causent incidemment des pertes en vies humaines dans la population civile, des blessures aux personnes civiles, des dommages aux biens de caractère civil, ou une combinaison de ces pertes et dommages, qui seraient excessifs par rapport à l'avantage militaire concret et direct attendu.

extrêmement inquiétantes. Selon un rapport du *Bureau of Investigative Journalism* : « À l'issue de trois mois d'enquête et de récits recueillis auprès de témoins oculaires, il est apparu qu'au moins 50 civils avaient été tués lors de frappes consécutives à une attaque alors qu'ils portaient secours aux victimes. Plus de 20 civils ont également été délibérément ciblés lors d'attaques lancées sur des convois funèbres et les participants aux funérailles ». « Obama terror drones: CIA tactics in Pakistan include targeting rescuers and funerals », dans *Bureau of Investigative Journalism*, 4 février 2012, disponible sur : http://www.thebureauinvestigates.com/2012/02/04/obama-terror-drones-cia-tactics-in-pakistan-include-targeting-rescuers-and-funerals/ [traduction CICR].

82 « GCHQ staff could be at risk of prosecution for war crimes », dans *Gloucester Echo*, 13 mars 2012, disponible sur : http://www.thisisgloucestershire.co.uk/GCHQ-staff-risk-prosecution-war-crimes/story-15505982-detail/story.html.

83 J. Meyer, *op. cit.*, note 7.

84 Voir, à cet égard, « 2010 Study on Targeted Killings », *op. cit.*, note 11, para. 68.

85 Protocole additionnel I de 1977, articles 51(5)(b) et 57(2)(a)(iii).

La question, naturellement, est de savoir ce que l'on entend par « excessif ». Dans le commentaire publié par le CICR sur l'article 51(5) du Protocole additionnel I de 1977, d'où est extrait le texte énonçant la règle de la proportionnalité de l'attaque, il est dit que :

> La disproportion entre les pertes et dommages causés et l'avantage militaire attendu pose évidemment un problème délicat ; certaines situations ne laisseront subsister aucun doute, tandis que dans d'autres situations il y aura matière à hésitation. Dans de tels cas, c'est l'intérêt de la population civile qui doit primer[86].

La notion de ce qui est proportionné sera appréciée, cela va sans dire, très diversement par tel État et tel autre. Même entre des alliés militaires proches comme le Royaume-Uni et les États-Unis, les avis divergent sensiblement sur ce point. L'Afghanistan nous en donne un exemple éloquent en mars 2011, lorsque quatre civils afghans ont été tués et deux autres blessés par un drone de la Royal Air Force lors d'une attaque contre des « chefs insurgés » dans la province de Helmand, la première opération dans laquelle il a été confirmé qu'un avion Reaper du Royaume-Uni avait causé la mort de civils[87]. Dans un communiqué de presse, le porte-parole du Ministère de la défense du Royaume-Uni a dit ceci :

> « Un incident faisant des victimes parmi les civils est profondément regrettable et nous prenons toutes les mesures possibles pour éviter que de tels incidents se produisent. Le 25 mars, un appareil Reaper du Royaume-Uni a été chargé d'attaquer et de détruire deux camions. La frappe a entraîné la mort de deux insurgés et la destruction d'une quantité importante d'explosifs transportés dans les camions. Malheureusement, quatre civils afghans ont aussi été tués et deux autres blessés. Il existe des procédures rigoureuses, fréquemment revues à la lumière de l'expérience, qui ont pour but d'une part de minimiser le risque de morts accidentelles et d'autre part d'enquêter sur tout incident qui se produit malgré tout (traduction CICR). »

Une enquête a été menée par la Force internationale d'assistance et de sécurité (FIAS) pour déterminer s'il y avait des leçons à tirer de cet incident ou si des erreurs avaient été commises dans les procédures opérationnelles ; le rapport a indiqué que les équipages du Reaper avaient agi conformément aux procédures et aux règles d'engagement du Royaume-Uni[88].

Néanmoins, une « source », apparemment attachée au Ministère de la défense du Royaume-Uni, a fait savoir au quotidien britannique *The Guardian* que cette attaque « n'aurait pas eu lieu si nous avions su qu'il y avait aussi des civils à

86 Yves Sandoz, Christophe Swinarski et Bruno Zimmermann (éds), *Commentaire des Protocoles additionnels du 8 juin 1977 aux Conventions de Genève du 12 août 1949*, Comité international de la Croix-Rouge, Genève, 1987, paras. 1979-1980.
87 N. Hopkins, *op. cit.*, note 5.
88 *Ibid.*

bord des véhicules »[89]. Ainsi, bien que la cible (c'est-à-dire les insurgés se trouvant dans au moins un des camions pick-up) n'aurait probablement pas été illégitime au regard du DIH, il semble que le Royaume-Uni aurait estimé disproportionné de cibler les deux insurgés s'il avait su que des civils se trouvaient à bord des camions.

On comparera à l'exemple qui précède le cas de la mort du chef taliban, Baitullah Mehsud. Le 23 juin 2009, la CIA tuait Khwaz Wali Mehsud, un commandant taliban pakistanais de rang intermédiaire. Elle entendait utiliser sa dépouille comme « appât » pour tuer Baitullah Mehsud, censé assister aux funérailles. Parmi les quelque 5 000 personnes rassemblées pour la circonstance se trouvaient des combattants talibans mais aussi de nombreux civils. Les drones américains frappèrent de nouveau, tuant jusqu'à 83 personnes. Parmi les victimes, il y aurait eu 45 civils, dont 10 enfants et 4 chefs tribaux. Une attaque de ce type pose des questions très graves du point de vue de l'interdiction des attaques sans discrimination. Baitullah Mehsud en sortit indemne, mais succomba six semaines plus tard, ainsi que sa femme, à une nouvelle frappe de la CIA[90].

L'utilisation d'armes licites

Le droit coutumier interdit l'usage, dans les conflits armés internationaux et non internationaux, d'armes de nature à frapper sans discrimination ou à causer des maux superflus ou des souffrances inutiles[91]. En général, les missiles Hellfire normalement lancés par des drones ne paraissent pas enfreindre cette règle[92]. Comme nous l'avons dit plus haut, cependant, la prudence s'impose en ce qui concerne l'utilisation potentielle de missiles Hellfire thermobariques. Compte tenu de leur grand champ d'action et de leurs conséquences sur les êtres humains, ces missiles demandent à être examinés de plus près au regard de ces deux principes généraux relatifs à l'armement[93]. De surcroît, les drones n'étant que des plateformes, il arrive qu'ils soient équipés d'autres armes qui ne respectent pas forcément l'interdiction de l'usage d'armes illicites dans les conflits armés.

Lien avec le conflit

Faut-il considérer les frappes au Pakistan, en particulier celles qui visent des hommes soupçonnés d'appartenir à Al-Qaïda, comme s'inscrivant dans la

89 *Ibid.*

90 C. Woods et C. Lamb, *op. cit.*, note 81. D'après Meyer, la CIA a effectué 16 frappes de missiles tuant jusqu'à 321 personnes avant de réussir à atteindre Baitullah Mehsud. Voir J. Meyer, *op. cit.*, note 7.

91 Voir l'étude du CICR sur le droit international humanitaire coutumier, *op. cit.*, note 21, règles 70 et 71.

92 Étant donné que les frappes de drones se déroulent souvent dans des zones densément peuplées, si le rayon de souffle des missiles utilisés devait augmenter, il serait plus problématique de respecter l'interdiction concernant les attaques sans discrimination.

93 Les armes thermobariques compteraient « parmi les armes les plus horribles qui puissent se trouver dans l'arsenal d'une armée : la bombe thermobarique, explosif effroyable qui enflamme l'air au-dessus de sa cible, et vide ensuite de son oxygène toute personne ayant eu le malheur de survivre à l'explosion initiale ». Noah Shachtman, « When a gun is more than a gun », dans *Wired*, 20 mars 2003, disponible sur : http://www.wired.com/politics/law/news/2003/03/58094 (consultée en dernier lieu le 20 février 2012, la page n'est plus disponible).

conduite licite des hostilités dans le cadre du conflit armé en Afghanistan[94] ? Dans un échange en ligne du 31 janvier 2012, le Président Obama disait que les frappes de drones au Pakistan, effectuées par la CIA plutôt que par l'armée[95], étaient une « action ciblée, centrée sur des personnes répertoriées comme étant des terroristes actifs » et que les États-Unis ne se contentaient pas « de frapper à tort et à travers », mais visaient « des gens soupçonnés d'appartenir à Al-Qaïda vivant dans des zones montagneuses d'accès difficile le long de la frontière entre l'Afghanistan et le Pakistan »[96]. Un « terroriste » n'est cependant pas toujours quelqu'un qui est engagé dans un conflit armé (*a fortiori* les barons de la drogue évoqués plus haut). Il doit exister clairement un lien avec un conflit armé impliquant une partie non étatique clairement définie, et non un discours prônant une vague « guerre contre le terrorisme » mondialisée, dont l'administration américaine actuelle, d'ailleurs, cherche à se démarquer[97]. Comme le souligne Melzer,

> La question de savoir si un groupe participe ou non aux hostilités ne consiste pas seulement à savoir si ce groupe recourt à la violence armée organisée dans une situation coïncidant temporellement et géographiquement avec un conflit armé, mais si cette violence sert à aider l'un des belligérants contre un autre (lien de belligérance)[98].

Selon le Procureur général des États-Unis, Eric Holder, qui a évoqué la question des frappes de drones dans un discours prononcé en mars 2012, « la compétence juridique du gouvernement des États-Unis ne se limite pas aux champs de bataille d'Afghanistan ». M. Holder a déclaré que, dans certaines circonstances, « il serait licite d'employer la force meurtrière dans le cadre d'une opération menée dans un pays étranger contre un citoyen américain qui est un haut dirigeant d'Al-Qaïda ou de forces associées et qui planifie activement de tuer des Américains »[99]. Les circonstances évoquées sont notamment le fait qu'un examen approfondi a permis de déterminer que la personne fait peser une « menace imminente d'attaque violente contre les États-Unis », que

94 Lorsque, en revanche, des talibans pakistanais ou afghans planifient ou réalisent des incursions sur le territoire afghan, ou lorsque les États-Unis lancent des frappes de drones pour soutenir le Pakistan dans le conflit armé non international contre les talibans pakistanais, ces opérations sont clairement liées à un conflit armé spécifique.

95 Les drones de la CIA seraient commandés d'un bâtiment d'une banlieue proche de Langley (Virginie) où se trouve le siège de l'Agence. Voir D. Walsh, *op. cit.*, note 68.

96 Voir, par exemple, la vidéo « Obama discusses US use of drones in online Q&A », dans *The Guardian*, 31 janvier 2012, disponible sur : http://www.guardian.co.uk/world/video/2012/jan/31/obama-us-drones-video.

97 Voir, par exemple, N. Lubell, *op. cit.*, note 23, pp. 113, en particulier la note 5, et 114.

98 N. Melzer, « Keeping the balance », *op. cit.*, note 77, p. 841 [traduction CICR] ; voir également N. Melzer, *op. cit.*, note 11, p. 427.

99 La notion de « forces associées » devrait être précisée. Les États-Unis auraient une position juridique plus défendable s'ils restreignaient publiquement leur liste de personnes à éliminer aux dirigeants d'Al-Qaïda, au lieu d'y inclure toute personne soutenant publiquement ou en privé les objectifs de cette organisation ou adhérant à ses méthodes.

« sa capture n'est pas possible » et que « l'opération sera menée conformément aux principes applicables du droit de la guerre »[100].

S'il serait opportun de limiter la licéité des assassinats ciblés à ceux visant des hauts dirigeants d'Al-Qaïda ou de forces associées qui font peser « une menace imminente d'attaque violente contre les États-Unis », car cela nous laisse supposer qu'une frappe ne sera pas autorisée à moins que la menace d'attaque violente soit « imminente », cela laisse cependant subsister plusieurs questions. Premièrement, qu'est-ce qu'une menace « imminente » ? Deuxièmement, les hommes tués par les frappes de drones au Pakistan ne sont souvent pas des hauts dirigeants, mais des combattants de rang intermédiaire ou subalterne. Qu'en est-il de la légalité de ces frappes ? Ou bien les critères de restriction des frappes ne valent-ils que lorsqu'il s'agit de citoyens américains ? Ce qui voudrait dire, s'agissant d'étrangers, que « la chasse est ouverte »[101] ? Troisièmement, les États-Unis considèrent-ils une attaque contre des forces américaines en Afghanistan conduite par des combattants basés au Pakistan comme une attaque terroriste ? Bien que la définition du mot « terrorisme » soit toujours controversée, nombreux sont ceux qui soutiennent que ce qui caractérise et définit le terrorisme, c'est le fait de prendre pour cible des civils – et non des membres des forces armées d'un État[102] – dans l'intention d'influencer la politique du gouvernement sur un ou plusieurs sujets. Or ce n'est manifestement pas ainsi que le gouvernement des États-Unis comprend le mot « terrorisme ».

Le discours du Procureur général élude, une fois encore, la question de savoir si de telles frappes s'inscrivent dans un conflit armé : l'engagement verbal de conduire une opération « conformément aux principes applicables du droit de la guerre » ne signifie pas, en effet, que le DIH soit applicable selon le droit international. Dans l'affaire *Hamdan c. Rumsfeld*, la Cour suprême des États-Unis a rejeté l'assertion selon laquelle le conflit était une guerre globale contre Al-Qaïda à laquelle les Conventions de Genève ne s'appliquaient pas, et a déterminé, en l'espèce, que l'article 3 commun aux Conventions de Genève s'appliquait à Salim Ahmed Hamdan, ancien garde du corps et chauffeur d'Oussama Ben Laden capturé par les forces armées des États-Unis en Afghanistan en novembre 2001[103]. Cet arrêt ne signifie pas que toute personne affiliée à Al-Qaïda, où qu'elle se trouve dans le monde, soit impliquée dans un conflit armé non international contre les États-Unis, en tant que personne participant directement aux hostilités du fait de son adhésion, voire de son soutien indirect, à une idéologie violente[104].

100 « Attorney General Eric Holder defends killing of American terror suspects », dans *Daily Telegraph*, 6 mars 2012, disponible sur : http://www.telegraph.co.uk/news/worldnews/al-qaeda/9125038/Attorney-General-Eric-Holder-defends-killing-of-American-terror-suspects.html.

101 Radsan écrit : « Si la vie de citoyens non-américains a autant d'importance que celle de citoyens américains, le même système de procédure régulière (ou de 'précaution', pour reprendre un terme de DIH) devrait s'appliquer à tous. En d'autres termes, si les contrôles ne sont pas assez précis pour tuer des Américains, ils ne le sont pas non plus pour tuer des Pakistanais, des Afghans ou des Yéménites ». Voir A. J. Radsan, *op. cit.*, note 19, p. 10.

102 Voir, par exemple, le document de l'ONU « Un monde plus sûr : notre affaire à tous ; Rapport du Groupe de personnalités de haut niveau sur les menaces, les défis et le changement », New York, 2004, paras. 159-161.

103 Cour suprême des États-Unis, affaire *Hamdan c. Rumsfeld*, 29 juin 2006, pp. 67-69.

104 Voir, par exemple, M.E. O'Connell, « Seductive drones : learning from a decade of lethal operations », Notre Dame Legal Studies Paper No. 11-35, dans *Notre Dame Law School Journal of Law, Information*

Les frappes de drones et le droit international des droits de l'homme

Après avoir étudié l'application du DIH aux attaques de drones et ses effets dans une situation de conflit armé, nous verrons dans cette section quelles sont les implications du droit international des droits de l'homme en ce qui concerne l'usage de drones de combat. Le premier assassinat ciblé exécuté à l'aide d'un drone en dehors de la scène d'un conflit armé serait, semble-t-il, celui de six membres présumés d'Al-Qaïda dont Qaed Senyan Al-Harithi, plus connu sous le nom d'Abou Ali Al-Harithi, soupçonné d'avoir été l'instigateur du bombardement du navire américain *USS Cole* en octobre 2000[105]. Tous les six ont été tués le 3 novembre 2002 au Yémen par un ou peut-être deux missile(s) Hellfire[106] tiré(s) d'un drone commandé par la CIA (agence centrale de renseignement des États-Unis), détruisant la jeep à bord de laquelle les hommes se déplaçaient dans la province de Marib, dans le nord du Yémen, à environ 160 kilomètres à l'est de Sanaa[107]. Depuis lors, les assassinats ciblés à l'aide de drones sont devenus monnaie courante au Pakistan et, dans une moindre mesure, au Yémen et dans d'autres pays[108]. En septembre 2011, l'exécution au Yémen, par un drone de la CIA, d'Anwar Al-Awlaki, un religieux musulman radical d'ascendance yéménite, a suscité une polémique d'autant plus vive qu'il était citoyen américain[109]. Après l'échec de plusieurs frappes dirigées contre lui, sa famille avait engagé une bataille juridique en vue d'empêcher que les États-Unis exécutent sans procès un de leurs citoyens[110].

Dans la première sous-section, nous verrons comment le droit international des droits de l'homme régit l'emploi de la force dans une situation de

& Science, août 2011 ; également cité par Carrie Johnson dans « Holder spells out why drones target US citizens », *NPR*, 6 mars 2012, disponible sur : http://www.npr.org/2012/03/06/148000630/holder-gives-rationale-for-drone-strikes-on-citizens.

105 Voir N. Melzer, *op. cit.*, note 11, p. 3 ; « Sources : US kills Cole suspect », dans *CNN*, 4 novembre 2002, disponible sur : http://articles.cnn.com/2002-11-04/world/yemen.blast_1_cia-drone-marib-international-killers?_s=PM:WORLD.

106 Le missile AGM-114 Hellfire est un missile air-sol conçu initialement pour un usage antichar, qui peut être lancé d'une plateforme aérienne, navale ou terrestre. Voir, par exemple, Lockheed Martin, « HELLFIRE II Missile », sur le site de *Lockheed Martin*, non daté, disponible sur : http://www.lockheedmartin.com/us/products/HellfireII.html (consulté le 20 mars 2012). Le missile, dont le premier lancement téléguidé a eu lieu en 1978, tire son nom du fait qu'il était conçu pour être tiré d'hélicoptère et fonctionner de manière automatisée après lancement (HELicopter Launched FIRE-and-forget). « AGM-114A HELLFIRE missile », dans *Boeing*, disponible sur : http://www.boeing.com/history/bna/hellfire.htm.

107 Voir, par exemple, « CIA 'killed al-Qaeda suspects' in Yemen », dans *BBC*, 5 novembre 2002 ; et « US Predator kills 6 Al Qaeda suspects », dans *ABC News*, 4 novembre 2002, disponible sur : http://abcnews.go.com/WNT/story?id=130027&page=1. Selon l'article de *ABC News*, il ne restait plus du véhicule « que quelques débris dans le désert ».

108 Les forces israéliennes ont commis des assassinats ciblés de Palestiniens à l'aide de drones. Voir, par exemple, « Three killed in Israeli airstrike », dans *CNN*, 23 juin 2012, disponible sur : http://articles.cnn.com/keyword/gaza-strip ; « Gaza truce gets off to a shaky start », dans *CNN*, 23 juin 2012, disponible sur : http://articles.cnn.com/2012-06-23/middleeast/world_meast_israel-gaza-violence_1_gaza-truce-popular-resistance-committees-palestinian-medical-officials?_s=PM:MIDDLEEAST.

109 « Predator drones and unmanned aerial vehicles (UAVs) », dans *The New York Times*, mise à jour du 5 mars 2012.

110 « Obituary : Anwar al-Awlaki », dans *BBC*, 30 septembre 2011, disponible sur : http://www.bbc.co.uk/news/world-middle-east-11658920.

« maintien de l'ordre », en dehors d'un conflit armé, et dans la seconde nous analyserons son rôle et ses effets réels et potentiels dans un conflit armé, en tant qu'élément constitutif, avec le DIH, du *jus in bello*.

L'application des droits de l'homme au maintien de l'ordre

En droit international des droits de l'homme, deux principes importants régissent l'usage de la force dans le contexte du maintien de l'ordre : la nécessité et la proportionnalité. Bien que ces termes soient employés à la fois dans le contexte du *jus ad bellum* et dans celui du DIH, ils ont un sens précis nettement différent dans le contexte des droits de l'homme. Alston écrit :

> « Un meurtre d'État n'est légal que s'il doit être commis pour protéger la vie (la force létale étant ainsi *proportionnée*) et s'il n'existe aucun autre moyen, tel que la capture ou la neutralisation l'individu, d'empêcher cette menace de mort de se réaliser (la force létale étant ainsi *nécessaire*) »[111].

À cela s'ajoute que la menace de mort devant être écartée par le recours à la force létale doit être imminente[112]. Ainsi, pour ce qui est de la manière de réglementer l'usage intentionnel de la force létale, le droit international des droits de l'homme reprend généralement les critères fixés dans les Principes de base sur le recours à la force et l'utilisation des armes à feu par les responsables de l'application des lois de 1990 (« les Principes de base »[113]). La dernière phrase du 9e Principe de base précise : « Quoi qu'il en soit, [les responsables] ne recourront intentionnellement à l'usage meurtrier d'armes à feu que si cela est absolument inévitable pour protéger des vies humaines »[114].

Il existe toutefois deux objections à cette position générale. La première est que ces principes n'ont pas été conçus pour régir les actes des forces armées

111 « 2010 Study on Targeted Killings », *op. cit.*, note 11, para. 32 [traduction CICR]. Melzer souligne que, dans le « modèle » du maintien de l'ordre, « le critère de la proportionnalité ne consiste pas à savoir si l'usage de la force potentiellement létale est 'nécessaire' pour mettre fin à une menace concrète, mais s'il est 'justifié' compte tenu de la nature et de l'ampleur de cette menace ». N. Melzer, *op. cit.*, note 11, p. 115 [traduction CICR].

112 Selon le Principe 9 des Principes de base sur le recours à la force et l'utilisation des armes à feu par les responsables de l'application des lois, de 1990 : « Les responsables de l'application des lois ne doivent pas faire usage d'armes à feu contre des personnes, sauf en cas de légitime défense ou pour défendre des tiers contre une menace *imminente* de mort ou de blessure grave, ou pour prévenir une infraction particulièrement grave mettant sérieusement en danger des vies humaines, ou pour procéder à l'arrestation d'une personne présentant un tel risque et résistant à leur autorité, ou l'empêcher de s'échapper, et seulement lorsque des mesures moins extrêmes sont insuffisantes pour atteindre ces objectifs » [nous soulignons].

113 Adoptés par le huitième Congrès des Nations Unies pour la prévention du crime et le traitement des délinquants, tenu à La Havane (Cuba) du 27 août au 7 septembre 1990. Les États-Unis n'ont pas participé à cette réunion, mais une résolution de l'Assemblée générale des Nations Unies adoptée la même année a accueilli avec satisfaction les Principes de base et a invité les gouvernements « à les respecter et à les prendre en considération dans le cadre de leurs législations et de leurs pratiques nationales ». AG ONU, Rés. 45/166, A/45/PV.69, adoptée sans vote le 18 décembre 1990.

114 Le Principe 8 se lit comme suit : « Aucune circonstance exceptionnelle, comme l'instabilité de la situation politique intérieure ou un état d'urgence, ne peut être invoquée pour justifier une dérogation à ces Principes de base ».

en situation de conflit armé, lesquels continuent de relever du *jus in bello*. La seconde est que le seuil de l'emploi intentionnel de la force létale a été fixé en termes moins restrictifs par la jurisprudence domestique des États-Unis (en ce qui concerne les pouvoirs de police) et interprété, de même, d'une manière plus laxiste par la Commission interaméricaine des droits de l'homme (pour les opérations antiterroristes)[115]. Dans l'affaire *Tennessee v. Garner*[116], la Cour suprême des États-Unis a dit que :

> Lorsque le policier peut avoir des raisons de penser que le suspect fait peser une menace d'atteinte grave à l'intégrité physique sur sa personne ou sur d'autres personnes, il n'est pas déraisonnable, du point de vue constitutionnel, d'empêcher le suspect de s'échapper en employant la force meurtrière. Ainsi, si le suspect menace le policier avec une arme ou lorsque l'on peut avoir des raisons de penser qu'il a commis un délit grave consistant à infliger ou menacer d'infliger des atteintes graves à l'intégrité physique, la force mortelle peut être utilisée si elle est nécessaire pour empêcher sa fuite, après sommation si la situation le permet[117].

D'autres pays dont l'Australie et le Royaume-Uni défendent le critère plus rigoureux énoncé dans les Principes de base. Le Royaume-Uni, par exemple, a pour politique de tirer pour tuer en présence d'un suspect d'attentat-suicide, ce qui est tout à fait conforme à ce critère parce que l'attentat-suicide réunit la menace de mort et le critère de l'imminence, qui est un facteur associé à la gravité de la menace. À la suite de la mort de Jean-Charles de Menezes, un jeune homme

115 La Commission semble toutefois faire une confusion entre les situations dans lesquelles l'usage des armes à feu est permis (menace imminente de mort ou de blessure grave) et celles dans lesquelles l'emploi intentionnel de la force létale est admis. Elle cite, en effet, en alléguant que les responsables de l'application des lois peuvent aussi faire usage de la force meurtrière pour se protéger eux-mêmes ou pour protéger d'autres personnes contre une menace imminente de blessure grave, le 9e Principe de base, qui, comme nous l'avons vu, limite l'usage intentionnel de la force létale aux cas où cela est absolument inévitable pour protéger des vies. Certains auteurs influents semblent avoir commis la même erreur. Voir, par exemple, N. Melzer, « Keeping the balance », *op. cit.*, note 77, p. 903 ; N. Melzer, *op. cit.*, note 11, pp. 62 et 197 ; et N. Lubell, *op. cit.*, note 23, p. 238.

116 *Tennessee v. Garner*, 471 US 1, Appeal from the US Court of Appeals for the Sixth Circuit, No. 83-1035 (27 mars 1985). Dans cette affaire, un policier avait tué par balles un garçon de 15 ans qui ne portait aucune arme. Le suspect a été tué par balles dans l'arrière du crâne avec un revolver de calibre 38 chargé de balles à pointe creuse alors qu'il s'enfuyait d'une maison prétendument cambriolée. On a retrouvé sur lui de l'argent et des bijoux pour une valeur de 10 dollars qui auraient été volés dans la maison.

117 La Cour a cité avec approbation le Code pénal modèle selon lequel : « L'usage de la force létale ne peut être justifié... à moins i) que le motif de l'arrestation soit un crime ou un délit majeur *(felony)* ; ii) que la personne qui procède à l'arrestation soit autorisée à agir en tant qu'agent de la paix ou assiste une personne qu'elle croit autorisée à agir en tant qu'agent de la paix ; iii) que la personne qui agit pense que la force employée ne fait courir aucun risque d'atteinte à l'intégrité physique d'innocents ; et iv) que la personne qui agit pense 1) que le délit grave à l'origine de l'arrestation comporte des actes tels que l'utilisation ou la menace d'utilisation de force mortelle, ou 2) qu'il existe un risque important que la personne à arrêter commette des actes meurtriers ou attentant gravement à l'intégrité physique si son appréhension est différée ». American Law Institute, Model Penal Code, Section 3.07(2)(b) (Projet officiel, 1962), cité dans *Tennessee v. Garner*, *ibid.*, para. 166, note 7 [traduction CICR].

tué en juillet 2005 de sept coups tirés à bout portant par des agents de la Police Métropolitaine Londonienne qui l'avaient pris à tort pour un auteur d'attentat-suicide alors qu'il n'était pas armé[118], Lord Stevens, ancien commissaire de la police londonienne, a rendu publique, dans un journal britannique populaire, la politique qui avait été adoptée pendant qu'il était en exercice en 2002[119]. Il a révélé à ce quotidien que les équipes qu'il avait envoyées en Israël et dans d'autres pays[120] où des attentats-suicides avaient été commis après les attentats du 11 septembre 2001 aux États-Unis avaient appris une « terrible vérité », à savoir que le seul moyen d'empêcher un auteur d'attentat-suicide d'agir était de « détruire son cerveau immédiatement, irrémédiablement ». Jusque-là, les policiers tiraient sur le corps du délinquant, « normalement à deux reprises, pour le rendre incapable d'agir et le maîtriser »[121]. Sir Ian Blair, qui était Commissaire en 2005, a déclaré que « cela ne servait à rien » de viser un suspect à la poitrine car c'était l'emplacement le plus probable de la bombe et que cela la ferait détoner[122].

L'imminence est un aspect extrêmement important pour la question des frappes de drones, en particulier compte tenu du risque de subjectivité et du manque de transparence concernant les noms qui figurent sur la liste des personnes à éliminer des États-Unis[123]. Dans son discours prononcé en mars 2012, le Procureur général Eric Holder semblait vouloir unir deux régimes juridiques différents – l'un applicable à un paradigme de maintien de l'ordre et l'autre applicable aux conflits armés – lorsqu'il affirmait que l'autorisation de lancer un drone contre un citoyen américain serait subordonnée à « un examen approfondi » permettant de conclure que le citoyen en question faisait peser « une menace imminente d'attaque violente contre les États-Unis » et que sa « capture n'était pas possible ». En 2010, Koh déclarait que :

> [l]'administration actuelle estime – et cela s'est vérifié lors de mon mandat de conseiller juridique – que les pratiques de ciblage des États-Unis, y compris les opérations létales conduites à l'aide de véhicules aériens sans pilote,

118 Voir, par exemple, « De Menezes police 'told to shoot to kill' », dans *Daily Telegraph*, 3 octobre 2007, disponible sur : http://www.telegraph.co.uk/news/uknews/1564965/De-Menezes-police-told-to-shoot-to-kill.htm. Cet incident montre à quel point des erreurs fatales sont possibles même lorsqu'une surveillance directe et indirecte ininterrompue est exercée sur un terroriste suspect.

119 Cette politique portait le nom de code « Operation Kratos », d'après le demi-dieu grec Kratos dont le nom signifiait force ou pouvoir en grec ancien.

120 En Russie et à Sri Lanka, selon ses dires.

121 « Debate rages over "shoot-to-kill" », dans *BBC*, 24 juillet 2005, disponible sur : http://news.bbc.co.uk/1/hi/uk/4711769.stm. Lord Stevens a dit : « Nous vivons une époque marquée par un mal sans précédent, en guerre contre un ennemi d'une brutalité indicible, et il ne fait pour moi aucun doute que ce principe, plus que jamais, est le bon, bien que tout risque d'erreur ne soit, hélas, pas exclu... Et on se tromperait lourdement à vouloir revenir dessus » [traduction CICR].

122 L'utilisation d'armes moins meurtrières telles que le pistolet à impulsion électrique Taser n'est pas non plus recommandée en raison du risque de détonation des explosifs. Voir, par exemple, la note interne de la Metropolitan Police Authority intitulée « Counter Suicide Terrorism » (from the Clerk to the Metropolitan Police Authority to the Members of the MPA), Londres, 8 août 2005.

123 Voir « 2010 Study on Targeted Killings », *op. cit.*, note 11, para. 20. Il y a aussi un risque manifeste de considérer les assassinats ciblés comme un châtiment mérité pour des crimes passés. Voir, par exemple, au Pakistan, N. Melzer, *op. cit.*, note 11, p. 178.

> respectent *le droit applicable dans son intégralité*, y compris les lois de la guerre[124].

En mai 2012, *The New York Times* a révélé l'existence de « mardis de la terreur », lors desquels le Président désignait les personnes qui seraient éliminées par les États-Unis, généralement à l'aide de drones :

> Voilà l'ennemi à abattre, présenté sur un plateau par les services de renseignement : 15 personnes suspectées d'appartenir à Al-Qaïda au Yémen ayant des liens dans les pays occidentaux. Le portrait signalétique et la brève notice biographique des suspects feraient plutôt penser à l'annuaire d'une université. Plusieurs des suspects sont des Américains et deux sont très jeunes, notamment une jeune fille de dix-sept ans qui en paraît moins[125].

Les contraintes importantes que le droit international des droits de l'homme impose en ce qui concerne l'usage intentionnel de la force létale amènent Alston à conclure que:

> « En dehors du contexte des conflits armés, l'usage de drones pour des assassinats ciblés n'a quasiment aucune chance d'être légal. Un assassinat ciblé commis à l'aide d'un drone par un État sur son propre territoire, sur lequel il a la maîtrise, a très peu de chances de se situer dans les limites définies par les droits de l'homme pour ce qui concerne l'emploi de la force létale ».

Si l'État n'agit pas sur son propre territoire, poursuit Alston,

> « Il existe très peu de situations, en dehors du contexte des hostilités actives, dans lesquelles le critère de la légitime défense préventive... pourrait être respecté... En outre, la mort de toute personne autre que la cible (un membre de la famille ou d'autres personnes se trouvant dans les environs, par exemple) résultant de l'attaque d'un drone constituerait un cas de privation arbitraire de la vie au sens des droits de l'homme et pourrait entraîner la responsabilité de l'État et la responsabilité pénale individuelle des auteurs[126].

124 Discours de Harold Hongju Koh, Conseiller juridique du Département d'État des États-Unis, à la Réunion annuelle de l'*American Society of International Law*, Washington, D.C., 25 mars 2010, disponible sur : http:/www.state.gov/s/l/releases/remarks/139119.htm [nous soulignons ; traduction CICR].

125 J. Becker et S. Shane, *op. cit.*, note 61.

126 « 2010 Study on targeted killings », *op. cit.*, note 11, paras. 85 et 86 [traduction CICR].

Pour Lubell, par exemple, le meurtre d'Al-Harithi au Yémen en 2002 était illégal car il violait le droit à la vie inscrit dans le Pacte relatif aux droits civils et politiques de 1966[127].

Application du droit international applicable dans les conflits armés et en liaison avec eux

Outre le *jus ad bellum,* au regard duquel sera éventuellement déterminée la légalité de l'emploi de la force dans un autre État, le droit international des droits de l'homme sera la principale source de droit international pour déterminer si l'usage de drones en dehors d'une situation de conflit armé est légal. Dans une situation de conflit armé, pour les actes présentant le lien requis avec ce conflit, au minimum les droits non susceptibles de dérogation continueront de s'appliquer pleinement, tandis qu'il pourra être dérogé aux autres droits « dans la stricte mesure où la situation l'exige »[128]. Étant donné que les frappes de drones, à l'évidence, menacent avant tout la vie – même si elles peuvent porter atteinte directement ou indirectement à de nombreux autres droits de l'homme – l'analyse se concentrera sur ce droit « suprême » (terme employé par le Comité des droits de l'homme de l'ONU)[129].

Applicabilité des droits de l'homme dans les conflits armés

Dans un *dictum* souvent cité sur le droit à la vie inscrit dans le Pacte relatif aux droits civils et politiques de 1966, la CIJ a observé que :

> la protection offerte par le pacte international relatif aux droits civils et politiques ne cesse pas en temps de guerre, si ce n'est par l'effet de l'article 4 du pacte, qui prévoit qu'il peut être dérogé, en cas de danger public, à certaines des obligations qu'impose cet instrument. Le respect du droit à la vie ne constitue cependant pas une prescription à laquelle il peut être dérogé. En principe, le droit de ne pas être arbitrairement privé de la vie vaut aussi pendant des hostilités. C'est toutefois, en pareil cas, à la lex specialis applicable, à savoir le droit applicable dans les conflits armés, conçu pour régir la conduite des hostilités, qu'il appartient de déterminer ce qui constitue une privation arbitraire de la vie. Ainsi, c'est uniquement au regard du droit applicable dans les conflits armés, et non au regard des dispositions du pacte lui-même, que l'on pourra dire si tel cas de décès provoqué par l'emploi d'un certain type d'armes au cours d'un conflit armé doit être considéré comme une privation arbitraire de la vie contraire à l'article 6 du pacte[130].

127 N. Lubell, *op. cit.*, note 23, pp. 106, 177 et 254-255.
128 Comité des droits de l'homme, « Observation générale n° 29 : états d'urgence (article 4) », Doc. ONU CCPR/C/21/Ref.1/Add.11, 31 août 2001.
129 « Observation générale n° 6 : Le droit à la vie (article 6) », du 30 avril 1982.
130 CIJ, *Licéité de la menace ou de l'emploi d'armes nucléaires*, Avis consultatif, CIJ Recueil 1996, para. 25.

Plusieurs États ont fait valoir sans succès devant la Cour que le Pacte – et plus généralement les droits de l'homme – n'était pas applicable dans les situations de conflit armé. Ce point de vue n'est maintenant plus guère entendu et a été généralement discrédité[131].

Relation entre les droits de l'homme et le droit international humanitaire

En revanche, l'assertion de la Cour selon laquelle c'est le droit applicable aux conflits armés, en tant que *lex specialis,* qui permet de décider si le droit à la vie a été violé[132] reste largement soutenue. À la première lecture, la Cour paraît ainsi s'en remettre totalement au DIH. Il existe cependant plusieurs raisons de contester cette assertion. Selon Christian Tomuschat[133], cette déclaration de la Cour est « plutôt de courte vue[134] » puisque, sur la question dont elle était saisie, à savoir la licéité de la menace ou de l'emploi d'armes nucléaires, la Cour n'a pas réussi à « conclure de manière définitive » de son interprétation du DIH qu'une telle menace ou un tel emploi « serait licite ou illicite dans une circonstance extrême de légitime défense[135] ». Par ailleurs, Tomuschat et d'autres ont fait observer que l'appréciation des rapports entre le DIH et les droits de l'homme donnée par la Cour a été modifiée dans des décisions ultérieures[136], notamment dans l'avis consultatif Édification d'un mur (2004)[137] et dans l'arrêt rendu dans l'*Affaire des*

131 Toutefois, en ce qui concerne la position d'Israël et des États-Unis, voir, par exemple, N. Melzer, *op. cit.*, note 11, pp. 79-80. En ce qui concerne la Convention américaine des droits de l'homme, la Commission interaméricaine des droits de l'homme a spécifié que « les contours du droit à la vie peuvent changer dans le contexte d'un conflit armé, mais... la privation arbitraire de la vie reste une interdiction absolue. La Convention établit clairement que le droit à la vie ne peut être suspendu quelles que soient les circonstances, même dans les conflits armés et les états d'urgence légitimes ». Commission interaméricaine des droits de l'homme, « Report on Terrorism and Human Rights », OEA/Ser.L/V/II.116 (doc.5 rev.1 corr.), 22 octobre 2002, para. 86 [traduction CICR].

132 Pour une analyse de l'application de ce principe, voir, par exemple, Nancie Prud'homme, « *Lex specialis* : oversimplifying a more complex and multifaceted relationship ? », dans *Israel Law Review*, Vol. 40, N° 2, 2007.

133 Christian Tomuschat, « The right to life – legal and political foundations », dans C. Tomuschat, E. Lagrange et S. Oeter (éds), *The Right to Life*, Brill, Pays-Bas, 2010, p. 11.

134 Schabas la qualifie de « maladroite, dans le meilleur des cas ». Voir William A. Schabas, « The right to life », dans A. Clapham et P. Gaeta (éds), *Oxford Handbook of International Law in Armed Conflict*, Oxford University Press, à paraître. Lubell est encore plus sévère, qualifiant ce propos de la Cour « d'approche peut-être inepte ». N. Lubell, *op. cit.*, note 23, p. 240. Milanović préconise que l'on « cesse de se servir de *lex specialis* comme d'une formule magique résumant en deux mots les rapports entre le DIH et le droit international des droits de l'homme, car cela est source de confusion plus que de clarté ». N. Milanović, « Norm conflicts, international humanitarian law and human rights law », dans Orna Ben-Naftali (éd.), *Human Rights and Humanitarian Law*, Collected Courses of the Academy of European Law, Vol. XIX/1, Oxford University Press, Oxford, 2010, p. 6 [traduction CICR].

135 *Ibid.*, para. 105.

136 Voir aussi, sur ce point, Sir Daniel Bethlehem, « The relationship between international humanitarian law and international human rights law and the application of international human rights law in armed conflict », document non publié et non daté, de 2012, para. 39.

137 CIJ, *Conséquences juridiques de l'édification d'un mur dans le territoire palestinien occupé*, Avis consultatif, CIJ Recueil 2004. Au paragraphe 106, il est dit ceci : « Dans les rapports entre droit international humanitaire et droits de l'homme, trois situations peuvent dès lors se présenter : certains droits peuvent relever exclusivement du droit international humanitaire ; d'autres peuvent relever exclusivement des droits de l'homme ; et d'autres enfin peuvent relever à la fois de ces deux branches

activités armées sur le territoire du Congo (2005)[138]. De l'avis d'Alston, puisque aussi bien le DIH que les droits de l'homme sont applicables dans le contexte d'un conflit armé,

> c'est à la *lex specialis* applicable qu'il appartient de déterminer si un meurtre est légal... Dans la mesure où le DIH ne donne pas de règle, ou si la règle n'est pas claire et si son sens ne peut être déduit avec certitude des orientations contenues dans les principes du DIH, il convient de suivre les orientations données par les droits de l'homme[139].

L'auteur va même plus loin, comme d'autres avec lui. Milanović, par exemple, relève que la Cour a omis, dans l'arrêt de 2005 concernant l'affaire du Congo, de mentionner le DIH en tant que *lex specialis* comme elle l'avait fait dans les avis consultatifs Édification d'un mur et *Armes nucléaires,* et exprime l'espoir que cette omission était intentionnelle[140]. Dans un blog du *European Journal of International Law,* il écrit en 2011 :

> Il serait plus audacieux d'aborder la question de l'application conjointe du DIH et du DIDH (droit international des droits de l'homme) en se demandant s'il est possible que des assassinats respectent le DIH tout en demeurant arbitraires au regard du DIDH. Autrement dit, le DIDH peut-il, dans un conflit armé, imposer des conditions supplémentaires à celles du DIH pour qu'un meurtre soit licite ? Et est-ce que ces conditions, tout en étant plus rigoureuses que celles du DIH, peuvent l'être un peu moins que celles définies par la jurisprudence en matière de droits de l'homme développée dans et pour des situations normales... ?... Je pense que l'on peut répondre à toutes ces questions par une affirmation prudente[141].

Dans l'avis consultatif concernant les *Armes nucléaires*, la Cour précisait en effet que le droit applicable dans les conflits armés *(jus in bello)* ne se limitait pas au DIH[142]. Le sens de l'expression « privation arbitraire » confirme aussi qu'il serait exagérément simpliste d'interpréter le droit à la vie dans une situation de conflit

du droit international. Pour répondre à la question qui lui est posée, la Cour aura en l'espèce à prendre en considération les deux branches du droit international précitées, à savoir les droits de l'homme et, en tant que *lex specialis*, le droit international humanitaire ».

138 CIJ, *Affaire des activités armées sur le territoire du Congo* (*RDC c. Ouganda*), Arrêt, CIJ Recueil 2005, para. 216.

139 « 2010 Study on targeted killings », *op. cit.*, note 11, para. 29 [traduction CICR].

140 M. Milanović, *op. cit.*, note 134, p. 6.

141 M. Milanović, « When to kill and when to capture ? », dans *EJIL Talk!*, 6 mai 2011, disponible sur : http://www.ejiltalk.org/when-to-kill-and-when-to-capture/ [traduction CICR].

142 Ainsi, au paragraphe 42 de son avis consultatif, la Cour mentionnait les « exigences du droit applicable dans les conflits armés, dont en particulier les principes et règles du droit humanitaire ». Le droit applicable dans les conflits armés comprend bien, en effet, *en particulier* [sic] les principes et règles du droit humanitaire, mais il est moins limité puisqu'il comprend aussi des éléments du droit des droits de l'homme et du droit ('humanitaire') du désarmement. CIJ, *Licéité de la menace ou de l'emploi d'armes nucléaires*, Avis consultatif, CIJ Recueil 1996, para. 42.

armé sous le seul angle du respect du DIH. Pour ce qui est du Pacte relatif aux droits civils et politiques de 1966, l'expression renfermerait « des éléments d'illégalité et d'injustice, de caprice, et d'irrationalité[143] ».

Il y a cependant une limite claire à cette approche. Si les droits de l'homme ont beaucoup à apporter au DIH pour ce qui est de limiter la violence et de promouvoir l'humanité (par exemple en contribuant à une meilleure compréhension de ce qui constitue, concrètement, « les principes de l'humanité » et les « exigences de la conscience publique » dans l'application de la clause de Martens), notre propos n'est pas de laisser entendre que les droits de l'homme rendraient en quelque sorte généralement illicite une arme qui est généralement licite au regard du DIH. Lubell, par exemple, indique que les lois régissant le choix des armes relèvent à juste titre du DIH sans qu'il y ait interférence du droit des droits de l'homme[144]. (En fait, on pourrait même soutenir qu'une telle interférence risquerait d'affaiblir le DIH puisque le gaz lacrymogène et les balles expansibles, bannis par le DIH, en tant que méthode et moyen de guerre respectivement, pourraient en quelque sorte devenir légitimes puisque le droit international des droits de l'homme admet leur utilisation dans le maintien de l'ordre.)

Néanmoins, la perspective d'une influence accrue et croissante des droits de l'homme sur le contenu du *jus in bello*, considéré jusque-là comme le domaine exclusif du DIH, ne devrait pas être vue comme une menace, mais plutôt comme un contrepoids nécessaire à la plus grande agressivité démontrée par certains États face à ce qu'ils embrassent comme un nouveau modèle de droit dans le monde de l'après 11 septembre[145]. La modération n'est pas un signe de faiblesse – c'est un signe de force. En ce qui concerne les drones, la CIA se serait refusée à déployer des Predator pour des missions autres que la surveillance avant le 11 septembre. On rapporte aussi que, la semaine précédant les attentats d'Al-Qaïda contre les États-Unis, George Tenet, alors directeur de la CIA, aurait dit à propos des drones que « faire usage d'une arme de ce type serait une 'erreur impardonnable' de la part du Directeur des services de renseignement »[146]. On peut s'interroger sur la valeur prophétique de ces propos.

Conclusion

Les drones permettent aux États d'exécuter des assassinats avec efficacité, à peu de frais et en prenant le minimum de risques. Dans l'Affaire du détroit de Corfou[147], la CIJ a dit que :

143 Manfred Nowak, *U.N. Covenant on Civil and Political Rights*, CCPR Commentary, N. P. Engel, Kehl, 1993, p. 111. Voir également N. Melzer, *op. cit.*, note 11, p. 93.

144 N. Lubell, *op. cit.*, note 23, p. 242.

145 Une autre manière d'étudier l'attitude des États après les attentats du 11 septembre consisterait à appliquer les règles du DIH aux situations dans lesquelles devrait s'appliquer le droit international des droits de l'homme applicable aux opérations de maintien de l'ordre.

146 Daniel Benjamin et Steven Simon, *The Age of Sacred Terror*, Random House, New York, 2002, p. 345.

147 L'incident ayant donné naissance à l'affaire du Détroit de Corfou est la collision survenue dans ce détroit entre deux navires de la Royal Navy britannique, provoquant l'explosion de mines immergées (45 officiers de marine et hommes d'équipage ont trouvé la mort et 42 autres ont été blessés dans cet incident) ; à la suite de l'accident, la marine britannique a effectué des opérations de déminage dans le détroit, mais dans les eaux territoriales

> Le prétendu droit d'intervention ne peut être envisagé par elle que comme la manifestation d'une politique de force, politique qui, dans le passé, a donné lieu aux abus les plus graves et qui ne saurait, quelles que soient les déficiences présentes de l'organisation internationale, trouver aucune place dans le droit international. L'intervention est peut-être moins acceptable encore dans la forme particulière qu'elle présenterait ici, puisque, réservée par la nature des choses aux États les plus puissants, elle pourrait aisément conduire à fausser l'administration de la justice internationale elle-même[148].

Les assassinats ciblés commis par les États à l'aide de drones ou d'autres moyens ressemblent trop souvent à l'élimination de noms sur une liste de meurtres de la maffia. En effet, comme le fait observer Melzer : « En dernière analyse,... à l'aune des critères moraux communs à la plupart des sociétés, même les assassinats ciblés exécutés dans le cadre de l'ordre juridique actuel présentent souvent des caractéristiques qui les rapprochent plus des pratiques criminelles que d'une politique gouvernementale acceptable »[149]. Ou encore, selon les propos d'un ancien juriste de la CIA : « Le pouvoir du gouvernement de donner la mort doit être rigoureusement contrôlé, sous peine de se transformer en une tyrannie plus grave que le terrorisme »[150].

Ce contrôle suppose que les frappes de drones illicites entraînent la responsabilité juridique internationale individuelle et de l'État. Qui, cependant, doit être tenu pénalement responsable de la mort de civils tués soit en violation des règles de la distinction et de la proportionnalité dictées par le DIH, soit en violation des droits humains fondamentaux ? L'opérateur du drone ? Les « guetteurs » sur place (le cas échéant) ? Ceux qui désignent la cible comme objectif militaire (qui peuvent être des informateurs rémunérés) ? Le juriste qui autorise la frappe ? Toutes les personnes précitées ? Si la frappe est illicite, pourrait-on la considérer comme une entreprise criminelle commune selon le droit pénal international, ou considérer une ou plusieurs des personnes précitées comme complices d'un crime international ?

Plus préoccupante encore est la perspective de drones entièrement autonomes prenant des décisions de ciblage sur la base d'une série de vecteurs pro-

albanaises. La Cour a tenu l'Albanie pour responsable des explosions et a accordé des dommages et intérêts au Royaume-Uni, mais a jugé que les opérations de déminage étaient une violation de la souveraineté albanaise.

148 CIJ, *Affaire du détroit de Corfou (Royaume-Uni de Grande-Bretagne et d'Irlande du Nord c. Albanie)*, Arrêt (Fond), CIJ Recueil 1949, p. 35.

149 N. Melzer, *op. cit.*, note 11, p. 435.

150 A.J. Radsan, *op. cit.*, note 19, p. 8. Dans une étude du Ministère de la défense du Royaume-Uni (2011), il est dit ceci : « Il est essentiel, avant que les avions sans pilote ne soient partout (s'il n'est pas déjà trop tard), de mener une réflexion sur cette question et de veiller à ce que, en ôtant de son horreur à la guerre, ou du moins en la tenant à distance, nous ne risquions de perdre le contrôle de notre humanité et de rendre la guerre plus probable ». *The UK Approach to Unmanned Aircraft Systems*, Development, Concepts and Doctrine Centre, Joint Doctrine Note 2/11, Ministry of Defence, 2011, pp. 5-9 [traduction CICR]. Voir également Richard Norton-Taylor et Rob Evans, « The terminators : drone strikes prompt MoD to ponder ethics of killer robots », dans *The Guardian*, 17 avril 2011, disponible sur : http://www.guardian.co.uk/world/2011/apr/17/terminators-drone-strikes-mod-ethics.

grammés, potentiellement sans contrôle humain[151]. Qui, dès lors, doit être tenu responsable ? Le constructeur du drone ? Le programmeur du logiciel ? Pour le moment, les questions restent bien plus nombreuses que les réponses.

Par ailleurs, les groupes armés non étatiques finiront tôt ou tard par se procurer des drones ou en développer la technologie[152] (ou bien ils pirateront la commande d'un drone étatique dont ils prendront le contrôle)[153]. Ces groupes ne chercheront-ils pas activement à reprendre l'avantage ? Un chercheur attaché à la Brookings Institution a lancé en 2011 l'avertissement suivant :

> Croire que les drones resteront le domaine réservé de pays responsables, c'est méconnaître la longue histoire des techniques d'armement. Les groupes ou les États voyous hostiles aux États-Unis seront, un jour ou l'autre, capables de construire ou d'acquérir leurs propres drones et de les utiliser pour lancer des attaques sur notre sol ou sur nos soldats à l'étranger, ce n'est qu'une question de temps[154].

La boîte de Pandore a été ouverte, mais à n'en pas douter, l'avenir nous réserve des surprises bien pires encore.

151 Voici ce que dit un rapport de l'US Air Force datant de 2010 : « L'utilisation militaire de véhicules pilotés à distance est en plein essor car les forces armées de nombreux pays de par le monde leur trouvent des usages de plus en plus nombreux comme la surveillance, la frappe, la guerre électronique et autres. Ces véhicules comprennent des appareils à voilure fixe et à voilure tournante, des dirigeables, des avions hybrides et d'autres conceptions. Leurs capacités gagneront en autonomie, ce qui permettra aux pilotes à distance de déclarer globalement les buts de la mission et de laisser l'appareil s'adapter de façon autonome à l'environnement local pour répondre au mieux à ces objectifs... Même si l'homme doit rester maître des décisions de frappe dans l'avenir prévisible, le degré d'autonomie s'améliorera considérablement avec les technologies de pointe. Ces dernières pourront alors être exploitées en toute sécurité lorsque des méthodes appropriées de vérification et de validation ainsi que des normes techniques auront été établies et pourront servir à certifier ces systèmes hautement autonomes ». US Air Force Chief Scientist, « Report on technology horizons, a vision for Air Force science & technology during 2010-2030 », doc. AF/ST-TR-10-01-PR, Vol. 1, mai 2010, pp. 24-42. Voir également Tom Malinowski, Human Rights Watch, « A dangerous future of killer robots », dans *Washington Post*, 22 novembre 2012, disponible sur : http://www.hrw.org/news/2012/11/22/dangerous-future-killer-robots.

152 En octobre 2012, le chef du Hezbollah a prétendu que son groupe était à l'origine du lancement d'un drone abattu au-dessus du territoire israélien par les forces de défense israéliennes le 6 octobre. Cheikh Hassan Nasrallah a affirmé que le drone avait été construit en Iran et avait survolé des « sites sensibles » en Israël. « Hezbollah admits launching drone over Israel », dans *BBC*, 11 octobre 2012, disponible sur : http://www.bbc.co.uk/news/world-middle-east-19914441.

153 En juin 2012, des chercheurs des États-Unis ont pris le contrôle d'un drone en vol en piratant son GPS, pour relever un défi de 1 000 dollars lancé par le Département de la sécurité intérieure. Une équipe de l'Université du Texas à Austin a utilisé la technique du leurre qui consiste à faire passer le signal des pirates pour celui des satellites GPS. C'est peut-être cette technique qui a servi à abattre un drone américain en Iran en 2011. « Researchers use spoofing to 'hack' into a flying drone », dans *BBC*, 29 juin 2012, disponible sur : http://www.bbc.com/news/technology-18643134.

154 John Villasenor, « Cyber-physical attacks and drone strikes: the next homeland security threat », dans *The Brookings Institution*, 5 juillet 2011, disponible sur : http://www.brookings.edu/papers/2011/0705_drones_villasenor.aspx [traduction CICR].

Volume 94 Sélection française 2012/2

REVUE INTERNATIONALE

Droits de l'homme, automatisation et déshumanisation des prises de décisions létales : les systèmes d'armement autonomes doivent-ils être interdits ?

Peter Asaro*

Philosophe des technologies, le professeur Peter Asaro a mené des travaux sur l'intelligence artificielle, les réseaux de neurones, le traitement du langage naturel et la vision robotique. Il est chercheur associé au Centre de recherche sur l'internet et la société de la faculté de droit de l'université de Stanford, aux États-Unis, et vice-président du Comité international pour le contrôle des armes robotisées, dont il est cofondateur. Il est également directeur des programmes de 2e et 3e cycles à l'École d'études des médias de la *New School For Public Engagement*, à New York City, États-Unis.

Résumé

Le présent article passe en revue la littérature consacrée récemment aux systèmes d'armement autonomes et à leur éventuelle interdiction internationale. Répondant aux commentateurs qui estiment que cette prohibition serait contestable à plusieurs titres, l'article montre qu'une telle interdiction trouverait son fondement théorique dans les normes relatives aux droits de l'homme et dans les principes humanitaires, non seulement moraux mais aussi juridiques. Ainsi, l'une des exigences implicites du droit international humanitaire, qui régit les conflits armés, est l'exercice d'un jugement humain. Cette exigence

* La version originale en anglais de cet article est publiée sous le titre « On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making », dans *International Review of the Red Cross*, Vol. 94, N° 886, été 2012, pp. 687-709.

figure implicitement dans trois principes cardinaux – distinction, proportionnalité et nécessité militaire – qui sont énoncés dans des traités internationaux tels que les Conventions de Genève de 1949 et qui sont fermement établis en droit international coutumier. Des principes similaires sont aussi implicites dans le droit international relatif aux droits de l'homme qui garantit, en toutes circonstances, certains droits fondamentaux à tous les êtres humains, indépendamment de leurs origines nationales ou de la législation locale. J'estime pour ma part qu'il existe une obligation spécifique qui s'applique à toute une gamme de systèmes automatisés et autonomes. Cette obligation découle de deux droits fondamentaux de la personne humaine – le droit à la vie et le droit à un procès équitable – et des conditions restreintes dans lesquelles il peut être dérogé à ces droits. Les individus et les États en temps de paix et en situation de conflit armé, les combattants, les organisations militaires et les États sont tenus de ne déléguer en aucun cas à des machines ou à des processus automatisés ni l'autorité ni la capacité d'employer la force létale si la légitimité morale et juridique d'un tel acte n'a pas été préalablement établie par un humain. Je soutiens qu'il serait bon que cette obligation soit établie comme norme internationale et que cela soit formalisé par un traité, avant que ne commencent à apparaître divers systèmes d'armes automatisées et d'armes autonomes susceptibles de menacer gravement les droits fondamentaux de tout individu.

Mots-clés : robots ; drones ; systèmes d'armement autonomes ; automatisation ; décisions létales ; droits de l'homme ; maîtrise des armements.

: : : : : : :

En septembre 2009, Jürgen Altmann, Noel Sharkey, Rob Sparrow et moi-même avons créé le Comité international pour le Contrôle des Armes robotisées (*International Committee for Robot Arms Control – ICRAC*)[1]. Nous avons publié peu après une déclaration de mission qui contenait un appel au débat sur une éventuelle interdiction internationale des systèmes d'armement autonomes :

> « Étant donné le rythme rapide du développement de la robotique militaire et les dangers pressants que ces avancées font peser sur la paix et la sécurité internationale, ainsi que sur les civils en temps de guerre, nous demandons à la communauté internationale d'entamer d'urgence un débat sur l'établissement d'un régime de maîtrise des armements visant à réduire la menace que ces systèmes représentent. Nous proposons que le débat porte sur l'interdiction de la mise au point, du déploiement et de l'emploi de systèmes d'armement autonomes télépilotés ; des machines ne devraient pas être autorisées à prendre la décision de tuer des êtres humains »[2].

1 Voir www.icrac.net [Sauf mention contraire, tous les sites internet ont été consultés en août 2013]

2 Jürgen Altmann, Peter Asaro, Noel Sharkey et Robert Sparrow, *Mission Statement of the International Committee for Robot Arms Control*, 2009, disponible sur : http://icrac.net/statements/ [Traduction CICR].

Depuis lors, philosophes, juristes, officiers militaires, décideurs politiques, scientifiques et roboticiens se sont emparés de cette question. Au départ, les débats étaient surtout centrés sur l'incapacité, pour les systèmes d'armement autonomes existant déjà, de satisfaire aux exigences du droit international humanitaire (DIH) ; la possibilité que les futures technologies leur confèrent cette capacité a donné lieu à diverses conjectures. Deux questions retenaient alors particulièrement l'attention. D'une part, les systèmes armés autonomes sont-ils (ou seront-ils) capables de respecter les principes de distinction et de proportionnalité, comme l'exigent les Conventions de Genève ? D'autre part, sera-t-il possible d'imputer à quiconque la responsabilité des dommages ou des pertes que de tels systèmes pourraient causer de manière illicite ? À l'issue des discussions initiales, l'attention a commencé à se porter sur la question de savoir si le DIH a besoin d'être complété par un traité international interdisant explicitement ces technologies. Bien que la grande majorité du public et un certain nombre de spécialistes – universitaires, juristes, officiers militaires et ingénieurs – sont aujourd'hui d'avis que les systèmes létaux ne devraient pas être autonomes, certains commentateurs estiment qu'il pourrait être prématuré, inutile et même immoral d'établir une interdiction des systèmes d'armement autonomes au niveau international[3]. Je considère pour ma part que leur position est erronée et que nous devons agir sans tarder afin interdire ces systèmes. Je pense en effet que nous sommes tenus, pour des raisons d'ordre moral et juridique, d'empêcher toute délégation de l'autorité létale à des systèmes non humains et non supervisés. Il importe en outre que, dans nos travaux de recherche en science et en ingénierie, ainsi que dans l'affectation de nos ressources de développement, nous poursuivions l'objectif d'accroître la performance éthique des décideurs humains. Le présent article exposera donc un fondement théorique pour une interdiction internationale des systèmes d'armement autonomes reposant sur le droit international des droits de l'homme (DIDH) et sur le droit international humanitaire (DIH). Outre leur consécration et leur protection par un corpus juridique important (tant au plan international qu'interne), les droits humains ont également un statut moral, indépendant du droit en vigueur. Il est donc possible d'y puiser des conseils judicieux quant à l'extension du droit afin de répondre aux défis posés par les technologies émergentes. Je présenterai l'argument selon lequel une interdiction internationale des systèmes d'armement autonomes peut être fermement établie sur le principe que l'autorité de décider d'employer la force létale ne peut pas être légitimement déléguée à un processus automatisé ; cette autorité doit rester la responsabilité d'un agent humain qui est tenu de prendre une décision réfléchie et informée.

3 Ronald C. Arkin, *Governing Lethal Behavior in Autonomous Robots*, CRC Press, 2009 ; Gary Marchant, Braden Allenby, Ronald C. Arkin, Edward T. Barrett, Jason Borenstein, Lyn M. Gaudet, Orde F. Kittrie, Patrick Lin, George R. Lucas, Richard M. O'Meara et Jared Silberman, « International governance of autonomous military robots », dans *Columbia Science and Technology Law Review*, 30 décembre 2010, disponible sur : http://ssrn.com/abstract=1778424 ; Kenneth Anderson et Matthew C. Waxman, « Law and ethics for robot soldiers », dans *Policy Review*, 28 avril 2012, disponible sur : http://ssrn.com/abstract=2046375 .

Ce principe a des incidences sur plusieurs corpus juridiques, notamment le droit interne, le DIDH et le DIH. Étant donné que l'intérêt que suscite actuellement la mise au point de systèmes d'armement autonomes est principalement motivé par des applications militaires, je traiterai donc les incidences de ce principe sous l'angle du DIH. Ce même principe s'appliquerait toutefois à l'usage de systèmes d'armement autonomes par les États à des fins de police intérieure, de contrôle des mouvements de foule, de surveillance des frontières, de garde de prisonniers, ainsi que pour assurer la sécurité d'installations et du territoire, ou pour mener d'autres activités potentiellement meurtrières. Ces systèmes pourraient aussi être employés par des individus ou par des organisations pour toute une gamme d'utilisations relevant de la sécurité et impliquant l'emploi de la force. Je me focaliserai donc sur l'un des droits fondamentaux de la personne humaine – le droit à la vie – tout en sachant que des arguments similaires peuvent être invoqués à propos des décisions automatisées qui dérogent à d'autres droits humains, ou en empêchent l'exercice. Je pense notamment à l'automatisation de certaines activités (arrestation, détention et restriction de mouvement ; localisation, surveillance et poursuite ; déportation ; expulsion et saisie ; refus d'accès aux soins médicaux, interdiction de tenir des réunions publiques, suppression de la liberté de la presse et de la liberté d'expression, suppression des droits de vote ; et, enfin, suppression d'autres droits civils, politiques, économiques, sociaux et culturels)[4].

Les systèmes d'armement autonomes

Un emploi accru de technologies hautement automatisées a été observé lors de récents conflits armés. Les drones armés pilotés à distance, utilisés dans un certain nombre de pays, notamment par les forces armées des États-Unis, en sont l'exemple le plus frappant. Ces aéronefs de combat sont capables d'effectuer de nombreuses procédures de vol automatisées très sophistiquées (par exemple, des opérations entièrement automatisées de décollage et d'atterrissage, des approches GPS autonomes ou le maintien en orbite à une altitude prédéfinie autour d'une cible localisée par GPS). Ces aéronefs possèdent aussi de nombreuses capacités en matière de collecte et de traitement automatisés des images. Bien qu'ils soient hautement *automatisés*, ces systèmes ne sont pas considérés comme *autonomes*, car ils sont encore placés sous la supervision et le contrôle direct d'un opérateur humain[5]. De plus, bien que ces systèmes soient porteurs d'armes dotées de cer-

4 Les droits de l'homme actuellement reconnus en droit international sont notamment, mais non exclusivement, les droits proclamés dans la Charte internationale des droits de l'homme des Nations Unies, composée de la Déclaration universelle des droits de l'homme, du Pacte international relatif aux droits civils et politiques et du Pacte international relatif aux droits économiques, sociaux et culturels.

5 Le terme « autonome » est utilisé en ingénierie pour qualifier un système qui fonctionne sans supervision ni contrôle direct d'un opérateur humain. Le terme « automatisé » s'applique à un système ou processus non supervisé, impliquant des opérations répétitives, structurées, de routine, effectuées avec peu de retour d'information (comme les lave-vaisselle), au contraire des systèmes ou processus

taines capacités automatisées (dans le cas, par exemple, des missiles guidés par laser et des bombes guidées par GPS), toutes les décisions de ciblage et de tir sont encore sous le contrôle direct d'un humain. Le présent article se développe autour des ramifications que peut avoir, sur les plans du droit et de l'éthique, l'automatisation des décisions de ciblage et de tir. Nous pouvons définir un « système d'armement autonome » comme étant tout système qui est capable de sélectionner sa cible et d'employer une force potentiellement meurtrière, sans aucune supervision ni aucune implication humaines directes dans la prise de décisions létales[6]. Si l'on s'en tient à cette définition, les aéronefs pilotés à distance utilisés aujourd'hui – tels que les drones de type *Predator* et *Reaper* – ne sont pas des systèmes d'armement autonomes. Néanmoins, il apparaît de plus en plus clairement que les activités qui, aujourd'hui, sont encore placées sous contrôle humain pourraient être automatisées dans un avenir proche, permettant ainsi l'élimination de toute intervention humaine directe pour sélectionner les cibles et décider d'employer la force létale contre elles. Il convient de relever que les aéronefs pilotés à distance ne sont pas le seul sujet de préoccupation. De nombreux systèmes déjà utilisés sur terre, en mer et sous la mer pourraient, eux aussi, être armés. De plus, certains systèmes défensifs fixes (tels que les tours de tir et les sentinelles) et divers modes opératoires des cyber-attaques pourraient être automatisés et devenir ainsi capables d'utiliser la force létale sans qu'aucun humain ne soit directement impliqué dans la sélection des cibles ou dans l'autorisation d'employer la force létale contre une cible donnée.

Certes, il existe divers exemples d'armes et de pratiques militaires qui se passent probablement d'intervention humaine directe dans la prise de décisions létales. Toutefois, la nouvelle vague de capacités technologiques a suscité, tant au sein de la communauté du droit international que parmi les militaires de carrière, de vives inquiétudes et interrogations quant à la légitimité morale et juridique de ces systèmes. Ainsi, comme l'a déclaré Jakob Kellenberger, alors président du Comité international de la Croix-Rouge (CICR), lors de la Conférence de San Remo (Italie) en septembre 2011 :

> « robotisés » ou « autonomes » (comme les voitures sans conducteur, par exemple), qui opèrent, quant à eux, dans des environnements ouverts, dynamiques et non structurés, sur la base d'informations provenant de différents capteurs. Tous ces systèmes – malgré les distinctions ci-dessus et bien qu'ils restent tributaires des données imprédictibles fournies par les capteurs – obéissent, d'une part, à des instructions algorithmiques presque entièrement fixes et déterministes et, d'autre part, à des calculs de probabilité étroitement circonscrits (parfois utilisés à des fins d'apprentissage et de correction d'erreurs).

6 Je préfère utiliser le terme de « système d'armement autonome » plutôt que celui d'« arme autonome », de manière à signifier que chacun de ces systèmes peut être réparti entre divers éléments disparates qui, néanmoins, fonctionnent ensemble pour constituer un système d'armement autonome. Par exemple, un ordinateur se trouvant presque n'importe où dans le monde pourrait recevoir des données transmises par un drone de surveillance et utiliser ces informations pour lancer et diriger une frappe effectuée à l'aide d'un système d'armes téléguidées se trouvant dans un tout autre point du globe, tout cela sans intervention ni supervision humaines : cet ordinateur constituerait ainsi un « système d'armement autonome ». En d'autres termes, les différents éléments qui composent ces systèmes – à savoir, les capteurs, les moyens autonomes de ciblage et de prise de décision, et l'arme elle-même – n'ont pas besoin d'être directement attachés les uns aux autres ou de se trouver au même endroit : il suffit qu'ils soient connectés par des réseaux de communication.

> Un système [d'armement] véritablement autonome serait doté d'une intelligence artificielle qui devrait être capable de mettre en œuvre le DIH. Bien que ce domaine suscite un grand intérêt et que la recherche soit largement financée, ces systèmes n'ont pas encore été adaptés aux armements. Développer de tels systèmes est un tel défi en termes de programmation que ce sera peut-être impossible. Il est clair que le déploiement de tels systèmes représenterait une véritable révolution conceptuelle et un changement qualitatif majeur dans la conduite des hostilités. Mais il soulèverait aussi tout un ensemble de problèmes fondamentaux du point de vue légal, éthique et sociétal, et ces problèmes doivent être pris en compte avant que ces systèmes ne soient développés ou déployés. Un robot pourrait être programmé de façon à se comporter de façon plus éthique et plus prudente qu'un être humain sur le champ de bataille. Mais que faire si, du point de vue technique, il est impossible de réaliser une programmation fiable d'un système d'armement autonome de façon à garantir qu'il respecter le DIH sur le champ de bataille ? ... Cela étant, l'application de règles juridiques préexistantes à une technologie nouvelle soulève la question de savoir si ces règles sont suffisamment claires au vu des caractéristiques spécifiques – et peut-être sans précédent – de cette technologie, et également au vu de l'impact humanitaire qu'elle peut avoir dans un avenir prévisible. Dans certaines circonstances, les États choisiront, ou ont déjà choisi, d'adopter des règles plus spécifiques[7].

Ainsi, comme Jakob Kellenberger l'a clairement indiqué, de graves interrogations subsistent quant à savoir si les technologies autonomes seront techniquement capables de se conformer aux dispositions actuelles du DIH. Nombreux sont les militaires qui reconnaissent que la technologie évolue dans le sens d'une autonomie accrue des systèmes d'armes létales ; toutefois, la plupart d'entre eux (y compris certains décideurs politiques du Bureau du Secrétaire à la Défense des États-Unis) expriment de graves préoccupations éthiques :

> S'il est essentiel d'imposer des limites aux armes autonomes pour assurer des engagements éthiques, la tâche la plus difficile consiste à créer des armes autonomes « à sûreté intégrée ». L'environnement en temps de guerre, dans lequel les systèmes militaires opèrent, est à la fois confus et compliqué et, malgré cela, les systèmes autonomes doivent être capables de fonctionner de façon appropriée. L'adaptation de l'ennemi, la dégradation des communications, les risques pour l'environnement, la présence de civils sur le champ de bataille, les cyber-attaques, les dysfonctionnements, et les tensions en période de guerre sont autant d'éléments qui introduisent la possibilité que les systèmes autonomes soient confrontés à des situations non anticipées et

7 Jakob Kellenberger, « Discours d'ouverture», Le droit international humanitaire et les nouvelles technologies de l'armement, XXXIV[e] table ronde sur les sujets actuels du droit international humanitaire, San Remo, Italie, 8-10 septembre 2011, pp. 5-6, disponible sur : http://www.icrc.org/fre/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm .

> que, par conséquent, ils agissent d'une façon qui n'a pas été voulue. Même les algorithmes relativement sophistiqués ne sont pas à l'abri d'une défaillance quand ils rencontrent une situation échappant aux paramètres intégrés lors de leur conception car, à la différence des êtres humains, ils ne possèdent pas l'intelligence contextuelle que l'on nomme parfois « bon sens » ou « sens commun ». La complexité des ordinateurs modernes vient encore compliquer le problème, car il est d'autant plus difficile d'anticiper tous les dysfonctionnements possibles ou tout comportement émergent, susceptible de survenir quand un système est mis en service[8].

Même dotés d'intelligence artificielle, les systèmes autonomes doivent être préprogrammés et ils n'ont, au mieux, que des capacités très limitées en termes d'apprentissage et d'adaptation. Il sera donc difficile, voire impossible, de concevoir des systèmes capables de fonctionner malgré le « brouillard » et les tensions qui caractérisent le temps de guerre. Si l'on examine les incidences que cela peut avoir pour la protection des civils dans les conflits armés, diverses questions d'ordre éthique et juridique apparaissent. Tout d'abord, comment sera assuré le respect, exigé par le DIH, des principes de distinction, de proportionnalité et de nécessité militaire ? Ensuite, en cas d'emploi de la force létale, comment pourra-t-on établir les responsabilités et faire en sorte que les auteurs rendent compte de leurs actes ?

Maintes inquiétudes d'ordre éthique et sociétal sont suscitées par l'emploi de systèmes d'armement autonomes. Ces préoccupations sont notamment dues aux problèmes de la guerre asymétrique et de la redistribution des risques (qui pèsent non plus sur les combattants, mais sur les civils), ainsi qu'à la crainte de voir s'abaisser le seuil au-delà duquel les nations décident de livrer une guerre[9]. En effet, les systèmes d'armement autonomes tendent à éloigner de la zone de conflit les combattants qui les utilisent et à réduire les risques de pertes humaines pour ceux qui les possèdent. Ils ont donc pour effet de réduire les coûts et les risques politiques d'une guerre, ce qui pourrait se traduire par un abaissement général du seuil de l'entrée en guerre. Par ailleurs, les systèmes d'armement autonomes sont également susceptibles de provoquer de l'instabilité et de l'insécurité aux niveaux régional ou mondial, d'alimenter la course aux armements, de proliférer et tomber aux mains d'acteurs non étatiques, ou encore de provoquer l'escalade de certains conflits en l'absence d'intentions politiques humaines. La force létale pourrait être employée sans supervision humaine par des systèmes dotés de cette capacité, même dans des situations où les dirigeants politiques et les chefs militaires n'auraient pas jugé une telle action appropriée ; l'on verrait ainsi des conflits éclater ou escalader de manière involontaire, en dehors de tout contrôle humain direct[10]. Ces systèmes font donc peser une grave menace sur la

8 Paul Scharre, « Why unmanned », dans *Joint Force Quarterly*, N° 61, 2e trimestre 2011, p. 92 [Traduction CICR].

9 Peter Asaro, « How just could a robot war be ? », dans Adam Briggle, Katinka Waelbers et Philip A. E. Brey (dir.), *Current issues in computing and philosophy*, IOS Press, Amsterdam, 2008, pp. 50-64, disponible sur : http://peterasaro.org/writing/Asaro%20Just%20Robot%20War.pdf.

10 L'on pourrait se référer par analogie au *Flash Crash* (« krach éclair ») du 6 mai 2010, au cours duquel les

stabilité internationale, ainsi que sur la capacité des instances internationales à gérer les conflits.

S'agissant de l'acceptabilité juridique des systèmes d'armement autonomes au regard du DIH existant[11], la question essentielle paraît être celle de savoir si ces systèmes seront ou non capables de respecter les principes de distinction et de proportionnalité[12]. Tant la complexité de ces systèmes que notre incapacité de prévoir comment ils pourraient se comporter dans des contextes opérationnels complexes nous placent devant une difficulté supplémentaire : comment tester et vérifier qu'un système d'armement autonome venant d'être conçu satisfait aux prescriptions du DIH, tel qu'exigé par l'article 36 du Protocole additionnel I[13] ? De manière plus générale, nous devrions également savoir comment « encadrer » les innovations technologiques, l'évolution étant de plus en plus rapide en ce qui concerne les nouvelles armes et les nouvelles tactiques[14].

Un autre motif de préoccupation tient au fait que l'opérateur de ces systèmes d'armement autonomes peut ne pas être identifiable. En d'autres termes, d'une part, aucun être humain ne pourrait être tenu responsable des actes commis dans une situation donnée par un système d'armement autonome et, d'autre part, un tel système pourrait agir de manière si imprévisible qu'il serait injuste de tenir l'opérateur responsable des actes commis[15]. Ces systèmes pourraient donc exclure la possibilité d'établir toute responsabilité pénale individuelle, celle-ci

systèmes de courtage automatique à haute fréquence se sont emballés et ont provoqué une baisse de 1000 points de l'indice des cours (Dow Jones) : cette baisse de 9 % en moyenne des valeurs cotées a été la plus violente que la Bourse de New York ait connue jusqu'alors. Voir sur *Wikipedia*, l'article consacré au *Flash Crash* du 6 mai 2010, disponible sur : http://fr.wikipedia.org/wiki/2010_aux_%C3%89tats-Unis.

11 Noel Sharkey, « Death strikes from the sky : the calculus of proportionality », dans *IEEE Technology and Society Magazine*, Vol. 28, No. 1, 2009, pp. 16-19 ; Noel Sharkey, « Saying 'No !' to lethal autonomous targeting », dans *Journal of Military Ethics*, Vol. 9, N° 4, 2010, pp. 369-383 ; Markus Wagner, « Taking humans out the loop : implications for the international humanitarian law », dans *Journal of Law Information and Science*, Vol. 21, 2011, disponible sur : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1874039 ; Matthew Bolton, Thomas Nash et Richard Moyes, « Ban autonomous armed robots », 5 mars 2012, Article36.org, 5 mars 2012, disponible sur : http://www.article36.org/statements/ban-autonomous-armed-robots .

12 Voir, en particulier, les articles 51 et 57 du Protocole additionnel I. *Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977*, 1125 UNTS 3, entré en vigueur le 7 décembre 1978. Voir http://www.icrc.org/applic/ihl/dih.nsf/Article.xsp?action=openDocument&documentId=1C05636226FBEE14C12563BD002C24B0 (article 51 – Protection de la population civile) et http://www.icrc.org/applic/ihl/dih.nsf/Article.xsp?action=openDocument&documentId=9FBD35598315A3E8C12563BD002C25A3 (article 57 – Précautions dans l'attaque).

13 Le texte intégral de l'article 36 du Protocole additionnel I (Armes nouvelles) est le suivant : « 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 ». Voir : http://www.icrc.org/applic/ihl/dih.nsf/Article.xsp?action=openDocument&documentId=39C6B917F5E974F5C12563BD002C22BE .

14 Richard M. O'Meara, « Contemporary governance architecture regarding robotics technologies : an assessment », dans Patrick Lin, Keith Abney et George Bekey, *Robot Ethics*, MIT Press, Cambridge, MA, 2011, pp. 159-168.

15 Robert Sparrow, « Killer Robots », dans *Journal of Applied Philosophy*, Vol. 24, N° 1, 2007, pp. 62-77.

exigeant la capacité de porter des jugements moraux ainsi que la détermination d'une intention criminelle (*mens rea*)[16]. Des systèmes d'armement autonomes placés sous la supervision ou le commandement d'opérateurs humains pourraient commettre des atrocités ou causer une tragédie. Deux notions fondamentales – la responsabilité du commandant et l'obligation de superviser les personnes placées sous ses ordres – se trouveraient alors gravement sapées. Les opérateurs humains seraient à l'abri de poursuites alors que, dans d'autres circonstances, les actes commis auraient été considérés comme des crimes de guerre. Il apparaît donc de plus en plus important que, d'une part, les États soient tenus responsables de la conception et de l'emploi des systèmes d'armement autonomes et que, d'autre part, des règles soient imposées au niveau international.

Nous sommes aujourd'hui à la croisée des chemins. Il nous faut décider quelle attitude nous entendons adopter, en tant que communauté internationale, vis-à-vis de ces systèmes. Allons-nous les traiter comme de nouvelles extensions de technologies anciennes, ou comme un changement qualitatif vers un nouveau genre de technologie ? Tels qu'ils sont aujourd'hui, le DIH et le DIDH permettent-ils de répondre aux défis posés par les technologies létales des systèmes autonomes ou ont-ils besoin d'être modifiés et de faire l'objet d'extensions mineures ou de révisions majeures ? Une interdiction des systèmes d'armement autonomes est-elle souhaitable ou risque-t-elle de venir perturber la mise au point d'armes nouvelles qui seraient mieux à même de respecter les normes morales et juridiques ?

J'estime pour ma part que les systèmes d'armement autonomes représentent un changement qualitatif de la technologie militaire, précisément parce qu'ils suppriment l'exercice du jugement humain dans l'engagement de la force létale. Ces systèmes menacent de saper les droits de l'homme du fait de l'absence de tout jugement et examen critique de la part d'un opérateur humain. Il existe donc de bonnes raisons de clarifier le DIH et le DIDH en codifiant explicitement l'interdiction de l'emploi de systèmes d'armement autonomes. Ces raisons résistent d'ailleurs à toutes les critiques formulées jusqu'ici à leur encontre. Une telle clarification et une telle codification permettraient notamment :

1) d'éviter diverses « pentes glissantes » menant vers des systèmes d'armement autonomes, en imposant une limite de principe qui départage ce qui peut être automatisé et ce qui ne peut pas l'être ;
2) d'orienter les futurs investissements dans le développement technologique vers des conceptions davantage centrées sur l'humain et capables d'améliorer le respect des normes éthiques et juridiques dans les conflits armés ;
3) d'éliminer le risque que les nouvelles technologies entraînent une déstabilisation plus radicale des normes éthiques et juridiques régissant les conflits armés et, enfin ;
4) d'établir le principe juridique selon lequel les processus automatisés ne satisfont pas aux exigences morales à respecter quand une vie humaine est en jeu.

16 M. Wagner, *op. cit.*, note 11, p. 5.

Il serait donc souhaitable que la communauté internationale prenne des mesures visant à établir une interdiction internationale des systèmes d'armement autonomes en se fondant sur les normes de protection des droits de l'homme ainsi que sur d'autres normes qui protègent l'individu.

La prise de décisions létales

Afin de développer l'argument selon lequel leur emploi est moralement et juridiquement inadmissible, nous devrons clarifier en quoi les systèmes d'armement autonomes ne remplissent pas les conditions nécessaires et suffisantes dans lesquelles il est permis de tuer pendant un conflit armé. La notion de « système d'armement autonome » doit également être affinée. Il suffit toutefois, à ce stade, de définir que la catégorie des systèmes d'armement autonomes regroupe l'ensemble des systèmes automatisés qui peuvent utiliser la force létale en l'absence de toute décision spécifique, consciente et délibérée d'un opérateur, contrôleur ou superviseur humain.

Certes, ces systèmes ne sont pas sans précédents. Des précurseurs de divers types ont déjà été utilisés dans des conflits armés, notamment les mines et autres dispositifs déclenchés par les victimes, ainsi que certains missiles guidés et quelques systèmes automatiques de défense. En un certain sens, ces systèmes sont eux-mêmes moins des « armes » que des systèmes automatisés qui sont dotés d'armes ou qui contrôlent des armes. Ils constituent donc un défi pour les modes de pensée traditionnels dans le domaine des armes et de la maîtrise des armements, qui ont tendance à se concentrer essentiellement soit sur l'arme en tant qu'outil ou instrument, soit sur les effets destructeurs de cette arme. Au contraire, les systèmes d'armement autonomes nous forcent à penser en termes de « systèmes » qui pourraient réunir toute une variété de configurations de capteurs, de traitement de l'information et de déploiement d'armements, et ils nous obligent à nous concentrer sur la façon dont est prise la décision d'employer la force létale[17].

Il existe, au sein des forces armées des États-Unis, une ligne politique qui consiste à suivre un modèle prévoyant « un homme dans la boucle » (*human-in-the-loop*) en cas d'emploi de la force létale. Cette expression est utilisée dans le domaine de l'ingénierie des facteurs humains pour indiquer qu'un être humain fait partie intégrante du système. S'agissant de l'utilisation de la force létale, le système déterminant est celui qui inclut le cycle de prise de décisions au cours duquel intervient la décision de recourir à la force létale. Dans le jargon militaire, ce cycle de prise de décisions est appelé « chaîne de frappe » et, selon l'armée de l'air des États-Unis, comporte six phases : *find, fix, track, target, engage, assess*

17 Au sens de l'article 36 du Protocole additionnel I aux Conventions de Genève, les systèmes d'armement autonomes doivent faire l'objet d'un examen de licéité. L'obligation porte en effet sur « toute nouvelle arme, nouveau moyen ou nouvelle méthode de guerre ». Le fait de doter une arme existante (déjà autorisée) de moyens autonomes de ciblage ou de tir constitue une nouvelle manière d'utiliser cette arme.

(trouver-fixer-suivre-cibler-engager-évaluer)[18]. Un débat s'est engagé récemment sur l'opportunité d'adopter un modèle intégrant « un homme dans la boucle », l'opérateur humain supervisant un ou plusieurs systèmes qui automatisent un grand nombre de tâches des six phases de ce cycle. Ce changement de paradigme paraît créer une position intermédiaire entre le contrôle humain direct du modèle « un homme dans la boucle » et un système d'armement entièrement autonome. Néanmoins, l'élément décisif qui détermine si un système donné est, ou n'est pas, un système d'armement autonome réside dans sa capacité à automatiser soit l'étape « cibler » soit l'étape « engager » en l'absence de tout contrôle humain direct. Nous pouvons donc dire que tout système qui est capable de sélectionner des cibles et d'employer la force potentiellement létale en l'absence de volonté délibérée et d'examen spécifique de la part d'un agent humain entre dans la catégorie des « systèmes d'armement autonomes ».

Cette définition reconnaît que, sur les plans de l'éthique et du droit, le problème fondamental consiste à établir soit la présence d'un lien de causalité entre la prise de décision automatisée et l'emploi d'une arme ou de la force létale, soit, inversement, l'absence de rapport causal entre la décision humaine et le fait qu'un système automatisé contrôle directement le recours à la force létale. Ainsi, le problème central, sur les plans moral et juridique, réside dans le fait que des humains puissent abandonner leurs propres responsabilités dans la prise de décisions pour les déléguer à des systèmes autonomes conçus pour tuer.

Il convient cependant de relever que l'inclusion d'un humain dans le processus de prise de décisions létales constitue une exigence nécessaire, mais non pas suffisante. Pour être légitime, ce processus doit remplir trois autres conditions : d'une part, l'opérateur humain (qui prend la décision d'employer la force létale après avoir vérifié que la cible est légitime) doit disposer de suffisamment de temps pour réfléchir. D'autre part, cet opérateur doit avoir reçu une formation appropriée et être bien informé. Enfin, il doit être tenu responsable et répondre de ses actes. Certes, il serait facile de placer des personnes insuffisamment formées devant un écran sur lequel défile une liste de cibles désignées et de demander à ces « opérateurs » de vérifier les cibles avant d'appuyer sur un bouton pour donner l'autorisation d'employer la force létale contre ces cibles. Ces « opérateurs » ne feraient pas mieux que des automates s'ils étaient contraints de prendre rapidement des décisions, sans avoir le temps de réfléchir, ou sans avoir accès à des informations pertinentes et suffisantes sur la base desquelles ils pourraient prendre une décision valable, ou s'ils étaient soumis à des tensions extrêmes sur les plans physique et émotionnel. Nous tenons généralement compte de ce genre de facteurs quand nous évaluons la validité d'une décision prise par un individu. Si un opérateur est placé dans de telles conditions, nous sommes moins enclins à le tenir responsable tant des décisions prises que de toute conséquence fortuite pouvant en avoir résulté, même s'il devra tout de même répondre de ses

18 Julian C. Cheater, « Accelerating the kill chain via future unmanned aircraft », Blue Horizons Paper, Center for Strategy and Technology, Air War College, avril 2007, p. 5, disponible sur : http://www.au.af.mil/au/awc/awcgate/cst/bh_cheater.pdf .

actes. Puisque ces facteurs diminuent la responsabilité de l'individu qui prend la décision, la conception et l'emploi de systèmes qui augmentent la probabilité que la prise de décisions se déroule de cette façon constituent en eux-mêmes des actes irresponsables. À mon avis, si l'on se place du point de vue de l'éthique de l'ingénierie et de la conception, le fait de concevoir délibérément des systèmes qui excluent l'intervention d'agents qui puissent répondre de leurs actes et être tenus responsables est en lui-même non éthique, irresponsable et immoral. Au moment d'établir les critères à l'aune desquels nous évaluons la prise de décisions létales, nous devrions éviter toute confusion entre, d'une part, les « circonstances atténuantes » que nous accordons aux humains qui agissent dans des conditions difficiles et, d'autre part, les idéaux auxquels nous rattachons les critères utilisés. De plus, le fait que lors de la prise de telles décisions, la performance d'un humain puisse être ramenée au niveau de celle d'un système autonome ne signifie pas que nous devions aussi abaisser les critères à l'aune desquels nous jugerons ces décisions.

Certes, le libellé détaillé de la définition des systèmes d'armement autonomes devant figurer dans un traité international sera nécessairement choisi au terme d'un processus de négociations. Néanmoins, la pierre angulaire d'un tel traité devrait être l'établissement du principe selon lequel des vies humaines ne peuvent pas être supprimées sans une décision informée et réfléchie, prise par un humain, quant à chacune de ces vies, ce principe s'appliquant dans chaque cas, sans exception, d'emploi de la force létale. Dès lors, tout système automatisé qui exclut les humains du processus de prise de décisions létales ne respecte pas ce principe et doit être interdit. Une telle proposition a un caractère novateur dans le domaine du contrôle des armes, car elle ne vise pas une arme particulière, mais plutôt la manière dont est prise la décision d'utiliser cette arme. Les traités de limitation des armements précédents ont essentiellement porté sur des armes spécifiques et sur leurs effets, ou sur le caractère intrinsèquement indiscriminé d'une arme donnée. Une interdiction des systèmes d'armement autonomes devra, au contraire, se concentrer sur la délégation de l'autorité d'employer la force létale à un processus automatisé qui n'est placé sous aucune supervision humaine directe et qui échappe à tout contrôle discrétionnaire.

« Meurtre légal » et nécessité d'un jugement humain

Pour qu'il soit légal de tuer pendant un conflit armé, cet acte doit être en accord avec les règles du DIH. En particulier, les parties à un conflit armé sont tenues de respecter les principes de distinction et de proportionnalité. La capacité des systèmes d'armement autonomes de respecter ces principes suscite de nombreux débats. La conjecture la plus ambitieuse consiste à dire que nous serons peut-être capables de programmer les systèmes d'armement autonomes de manière telle que, demain, ils seront capables de se conformer aux dispositions du DIH, ainsi qu'aux règles d'engagement et aux ordres du commandant

s'appliquant spécifiquement à une mission donnée[19]. Les promoteurs de cette idée (qui s'appuie sur la tradition dite de la « programmation par contraintes ») affirment que le DIH pourrait être traduit en règles de programmation définissant strictement quelles actions sont prohibées dans une situation donnée. Ainsi, un hypothétique « dispositif de contrôle éthique » pourrait empêcher un système d'armement autonome de mener une action qui, selon ce dispositif, est explicitement prohibée par le DIH. Ronald C. Arkin estime que les systèmes d'armement autonomes pourraient choisir de se sacrifier dans des situations où nous ne nous attendrions pas à ce que des humains le fassent. Ces systèmes pourraient dès lors commettre beaucoup moins d'erreurs et de manquements que des soldats humains et seraient donc plus aptes à respecter les règles du DIH.

En première analyse, cette proposition paraît assez convaincante et même J. Kellenberger lui a reconnu un certain attrait :

> À l'occasion du débat sur ces nouvelles technologies, il nous faut voir également quels sont les avantages qu'elles pourraient apporter si elles contribuaient à une meilleure protection. Respecter les principes de distinction et de proportionnalité signifie qu'il faut prendre certaines précautions dans l'attaque, comme indiqué à l'article 57 du Protocole additionnel I. Cet article prévoit notamment l'obligation pour un attaquant 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. Dans certains cas, les cyberopérations ou le déploiement d'armes télécommandées ou de robots pourraient faire incidemment moins de victimes civiles et causer moins de dommages aux biens de caractère civil que l'emploi d'armes classiques. Des précautions accrues devraient également être possibles dans la pratique, du fait simplement que ces armes sont déployées depuis suffisamment loin et souvent, avec suffisamment de temps pour que la cible soit choisie avec soin et que le moment de l'attaque soit décidé de façon à minimiser l'impact sur la population civile et les biens de caractère civil. On pourrait considérer que dans de telles circonstances, l'application de cette règle voudrait qu'un commandant évalue s'il peut obtenir le même avantage militaire en utilisant ces moyens et méthodes de guerre, s'ils sont applicables[20].

Assurément, le fait de renforcer la protection des personnes et des biens civils dans les futurs conflits armés serait avantageux. Nous devons toutefois éviter de tirer trop vite des conclusions qui conduiraient à autoriser l'emploi de systèmes d'armement autonomes. Cet argument apparemment simple repose sur

19 R. C. Arkin, *op. cit.*, note 3, pp. 71-91.
20 J. Kellenberger, *op. cit.*, note 7, p. 6.

un grand nombre d'hypothèses, et nous risquerions de nous laisser induire en erreur et d'en oublier la raison d'être et la signification du DIH.

Pendant un conflit armé, le but ultime du DIH est de protéger les personnes qui ne participent pas, ou ne participent plus, directement aux hostilités et de restreindre le recours à certains moyens et méthodes de guerre. Il est tentant de penser que de tels objectifs peuvent être objectivement et facilement mesurés. Nous aimerions pouvoir croire que le principe de distinction est semblable à une règle de tri qui permettrait de scinder le monde en deux catégories : les civils d'un côté, les combattants de l'autre. Nous voudrions croire en l'existence d'une règle, aussi complexe fût-elle, qui permettrait d'attribuer définitivement chaque individu à l'une ou l'autre de ces deux catégories[21], mais les choses sont bien plus compliquées que cela. Je prendrai ici pour exemple la difficulté de définir le sens de l'expression « civil participant aux hostilités ». Le CICR a établi un ensemble de lignes directrices, soigneusement formulées, visant à définir ce qui constitue « un acte de participation directe aux hostilités », en conséquence duquel un civil perd les protections que le DIH octroie normalement aux civils[22]. Ces lignes directrices précisent dans quelles conditions il est possible de conclure qu'un civil constitue une cible légitime. Ces conditions sont les suivantes : 1) seuil de nuisance, 2) rapport direct de cause à effet et 3) lien de belligérance. Chacune de ces trois conditions est explicitée dans le Guide interprétatif du CICR mais, pour les fins du présent article, il suffira de les résumer brièvement :

> Pour qu'un acte spécifique atteigne le niveau de nuisance requis pour constituer une participation directe aux hostilités, il doit être de nature à nuire aux opérations militaires ou à la capacité militaire d'une partie à un conflit armé. En l'absence d'effets nuisibles sur le plan militaire, le seuil peut également être atteint si un acte est susceptible d'infliger des pertes en vies humaines, des blessures ou des destructions à des personnes ou à des biens protégés contre les attaques directes. Dans ces deux cas, les actes atteignant le niveau de nuisance requis ne peuvent constituer une participation directe aux hostilités que s'ils satisfont en outre aux exigences de relation directe de causalité et de lien de belligérance.
>
> L'exigence de causation directe est satisfaite lorsque l'on peut raisonnablement attendre de l'acte spécifique en question (ou d'une opération militaire concrète et coordonnée dont cet acte fait partie intégrante) qu'il cause directement – en une seule étape causale – des effets nuisibles atteignant le seuil requis. Néanmoins, des actes satisfaisant à l'exigence de causation directe et atteignant le seuil de nuisance requis ne constitueront une par-

21 Il existe en effet, dans la littérature sur les armes autonomes, une tendance à se référer à la notion de « discrimination » plutôt qu'au principe de distinction (ce qui renvoie à la notion de « tâche de discrimination » dans les domaines de la psychologie cognitive et de l'intelligence artificielle). Voir, à ce sujet, le point de vue de Noel Sharkey dans cette édition.

22 Nils Mezler, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, Genève, 2010, disponible sur : http://www.cicr.org/fre/assets/files/other/icrc_001_0990.pdf .

ticipation directe aux hostilités que si le troisième critère – celui du lien de belligérance – est également rempli.

Afin de satisfaire à l'exigence du lien de belligérance, un acte doit être spécifiquement destiné à causer directement des effets nuisibles atteignant le seuil requis, à l'avantage d'une partie à un conflit armé et au détriment d'une autre. En règle générale, les effets nuisibles causés n'ont pas le lien de belligérance requis pour constituer une participation directe aux hostilités dans les cas suivants: a) dans le cadre de la légitime défense individuelle ou de la défense d'autrui contre les actes de violence interdits par le DIH; b) dans l'exercice du pouvoir ou de l'autorité sur des personnes ou sur un territoire; c) en tant qu'élément des troubles civils contre une telle autorité; d) lors de situations de violence entre civils.

Appliqués conjointement, les trois critères requis – seuil de nuisance, causation directe et lien de belligérance – permettent d'établir une distinction fiable entre, d'une part, les activités constituant une participation directe aux hostilités et, d'autre part, les activités qui, bien qu'elles se produisent dans le contexte d'un conflit armé, n'entrent pas dans le cadre de la conduite des hostilités et, par conséquent, n'entraînent pas, pour les personnes civiles, la perte de protection contre les attaques directes. Toutefois, même quand un acte spécifique constitue une participation directe aux hostilités, le type et le degré de la force utilisée pour le réprimer doivent être en conformité avec les règles et les principes du DIH et de toute autre branche applicable du droit international[23].

Ces lignes directrices tentent de définir la voie à suivre pour déterminer qui est une cible légitime et qui ne l'est pas. Pourtant, elles ne sont pas même appelées « règles » : ce ne sont que des lignes directrices destinées à aider un agent moral à franchir de multiples étapes d'interprétation et de jugement. Pour être à même de déterminer si un individu spécifique, dans des circonstances spécifiques, remplit chacune des trois conditions énoncées, cet agent moral doit être parvenu à un degré élevé de compréhension d'une situation complexe. Il doit notamment avoir apprécié les implications, aux niveaux tactique et stratégique, du préjudice potentiel, ainsi que le statut d'autres individus potentiellement menacés, la nature des structures causales, ainsi que les relations et implications causales directes des actions d'un individu en particulier et, enfin, la situation socioculturelle et l'état psychologique de l'individu pour que ses intentions et actions puissent être qualifiées d'« actions militaires » et ne pas être considérées, par exemple, comme relevant de l'exercice de l'autorité publique ou de la légitime défense.

Que veulent vraiment dire ceux qui déclarent que nous pouvons transcrire les règles du DIH dans un programme informatique ? S'agit-il simplement de prendre des règles juridiques qui ont été élaborées pour régir des actions humaines et de les traduire en codes programmés pour imposer des contraintes

23 N. Mezler, *op. cit.*, note 22, pp. 48-67.

aux actions d'une machine ? Le prochain Protocole additionnel aux Conventions de Genève devrait-il être écrit directement en code informatique ? Le DIH ne comporte-t-il pas des éléments qui ne peuvent pas être programmés ? Il est tentant d'aborder ce problème sous son aspect technique, de voir les décisions et les actions d'un combattant comme une « boîte noire », de comparer le soldat humain au soldat robot, et de prétendre que celui des deux qui commet le moins d'erreurs au regard du DIH est le soldat « le plus éthique ». Cette stratégie d'argumentation a souvent été utilisée dans l'histoire de l'intelligence artificielle.

Deux questions se posent en fait ici. La première est de caractère empirique : quand il en va de la vie ou de la mort de personnes humaines, peut-on attendre d'une machine, d'un ordinateur ou d'un processus automatisé qu'ils prennent chacune de ces décisions à un niveau de « performance » jugé acceptable ? La seconde question est d'ordre moral : peut-on admettre que de telles décisions de vie ou de mort soient prises par une machine, un ordinateur ou un processus automatisé ? Si nous ne parvenons pas à démontrer qu'une machine ne devrait pas prendre de telles décisions, nous n'aurons plus qu'à nous demander si (et quand) des programmeurs de talent seront à même de concevoir un jour un système informatique doté de ces capacités et, au minimum, quand allons-nous permettre à des machines de prendre de telles décisions.

L'histoire de l'intelligence artificielle est instructive à cet égard. Elle nous indique en effet que, de manière générale, un tel problème ne peut pas être résolu par le calcul numérique, mais que si nous arrivons à le définir très précisément et à le simplifier, nous avons quelques chances de succès. Cela dit, nous pourrions aussi établir une comparaison entre, d'une part, le genre de problèmes que l'intelligence artificielle a su résoudre (dans le jeu d'échecs, par exemple) et, d'autre part, le genre de problèmes rencontrés dans l'application du DIH. Certes, les exigences posées par le DIH constituent en un certain sens des « règles », mais elles sont bien différentes des règles des échecs dans la mesure où, pour être appliquées de façon appropriée en toute situation donnée, elles requièrent une grande part de jugement interprétatif. De plus, le contexte dans lequel s'appliquent les règles du DIH, la nature et la qualité des informations disponibles, ainsi que les diverses interprétations pouvant se trouver en concurrence ou en conflit peuvent grandement varier, tant tout au long d'un conflit donné que d'un jour à l'autre, voire d'une heure à l'autre.

Nous pourrions vouloir ajouter que l'intelligence est exclusivement humaine, mais si quelqu'un est un jour capable de la définir de manière suffisamment spécifique, ou de la réduire à l'exécution de telle ou telle tâche concrète, alors il sera peut-être possible de programmer un ordinateur pour qu'il remplisse « mieux » cette même tâche. Ce faisant, nous modifions nécessairement la définition de l'intelligence, qui n'est plus considérée comme une aptitude complexe mais comme la capacité d'accomplir une tâche spécifique. Peut-être n'est-il pas si important (malgré les incidences sur les plans sociétal et culturel) de redéfinir l'intelligence pour tenir compte des dernières avancées en informatique ? Par contre, quand il s'agit de moralité et de suppression de vies humaines, voulons-nous vraiment redéfinir le sens du qualificatif « moral » de manière à le rendre applicable aux

systèmes d'armement autonomes ? Quels lendemains préparerions-nous en donnant à des systèmes automatisés l'autorité de décider de la vie ou de la mort d'êtres humains ? En l'absence de tout jugement humain, comment pouvons-nous avoir l'assurance que ces décisions ne seront pas prises de manière arbitraire ?

L'automatisation des règles du DIH déprécierait probablement le rôle qu'elles jouent en réglementant le comportement éthique des divers protagonistes. Les risques liés à une telle évolution expliquent peut-être aussi pourquoi les développeurs s'efforcent de conserver « dans la boucle » des humains à qui il incombe de lever les ambiguïtés et de passer les décisions au crible d'une appréciation morale. Comme l'a déclaré Sir Brian Burridge, qui a commandé les forces aériennes du Royaume-Uni (RAF) en Irak de 2003 à 2005 :

> Au regard du droit des conflits armés, il subsiste l'exigence d'évaluer la proportionnalité et, dans ce cadre, une attente demeure, celle que l'humain se trouvant au bout de la chaîne de transmission accomplisse la dernière évaluation en appréciant la situation sur la base d'un jugement rationnel. Les conflits postmodernes nous mettent face … à des champs de bataille ambigus, non linéaires. Dès lors, nous ne pouvons pas « sortir de la boucle » l'opérateur humain, le commandant, l'analyste – tous ceux qui luttent contre l'ambiguïté. Le débat sur le maintien de « l'homme dans la boucle » doit aller bien au-delà de cela[24].

De par sa nature même, le DIH – dont le but est de réguler le comportement des êtres humains et des organisations humaines pendant les conflits armés – présume que les combattants sont des êtres humains. En ce sens, le DIH est anthropocentrique. Malgré tous les efforts déployés par ses auteurs pour que le DIH soit clair et précis, son application ne peut pas être effective dans une situation donnée sans passer par des niveaux d'interprétation multiples. Le DIH complète ses règles par des orientations heuristiques auxquelles les agents humains doivent se conformer ; il demande explicitement aux combattants d'examiner de façon raisonnée les implications de leurs actions ; enfin, en faisant explicitement appel à leur humanité, le DIH demande aux combattants de faire preuve de compassion et d'exercer leur jugement. Ce faisant, le droit n'impose pas d'effectuer un calcul spécifique, mais il impose aux combattants le devoir d'évaluer de manière réfléchie le coût potentiel en vies humaines et en biens des diverses modalités d'action dont ils disposent.

La justice ne peut pas être automatisée

De par sa nature même, le droit est incomplet. Il reste soumis à l'interprétation et peut toujours faire l'objet d'un examen ultérieur. Aussi bien intentionnées

24 Brian Burridge, « UAVs and the dawn of post-modern warfare: a perspective on recent operations », dans *RUSI Journal*, Vol. 148, N° 5, octobre 2003, pp. 18-23 [Traduction CICR].

que puissent être les lois et les règles de droit, et même si leur élaboration a été approfondie et réfléchie, aucun régime juridique n'est, et ne peut être, parfait. En évolution constante, ce système est conçu de telle manière que la charge d'en gérer l'application dans le monde des affaires humaines incombe à des institutions créées par l'homme. Afin de permettre le bon fonctionnement du système judiciaire, un certain nombre d'agents humains – juges, procureurs, avocats, témoins, jurés – s'engagent dans des processus complexes d'interprétation et de jugement. Les uns et les autres participent activement à l'évaluation des concordances pouvant exister entre un ensemble de règles abstrait et une situation concrète donnée. Le droit à une procédure régulière porte essentiellement sur l'obligation, pour ceux qui « disent le droit », de rendre compte publiquement de cette démarche délibérative.

Certes, il pourrait exister un jour un programme informatique destiné à remplacer les agents humains et à automatiser leurs décisions. J'estime toutefois que cela porterait fondamentalement atteinte au droit à une procédure régulière, qui consiste essentiellement à permettre, d'une part, de mettre en cause les règles et la pertinence de leur application dans une circonstance donnée et, d'autre part, de faire appel à la rationalité et à la compréhension humaines suffisamment informées. Arrive-t-il que des humains occupant de telles fonctions commettent des fautes ? Oui, bien sûr, cela arrive. Cependant, la compréhension, la rationalité et le jugement humains valent davantage que tout ensemble concevable de règles fixées ou que tout système informatique. De plus, les arguments avancés dans un cas donné, la possibilité d'interjeter appel afin de renverser les décisions judiciaires, ainsi que les diverses façons dont les opinions et la jurisprudence renseignent l'interprétation des lois, font apparaître que tout jugement juridique exige la mise en regard de perspectives différentes, incompatibles et même parfois contradictoires, dont il importe ensuite de tirer les enseignements. Les systèmes informatiques ou algorithmiques actuels ne possèdent pas une telle « compétence », et rien ne dit qu'ils la posséderont un jour.

Plus important encore, le jugement humain est un élément constitutif du système judiciaire. En d'autres termes, un système de justice, quel qu'il soit, ne peut s'appliquer à des êtres humains que s'il est fondé sur la raison humaine. La justice, en tant que telle, ne peut pas être déléguée à des processus automatisés. Bien sûr, dans le cadre des procédures administratives et juridiques, l'automatisation de diverses tâches est de nature à aider les humains qui, ainsi, seront mieux à même de poser leurs jugements, ou de le faire avec une plus grande efficacité. Par contre, l'automatisation ne peut pas exonérer les humains de l'obligation d'examiner les éléments de preuve, de délibérer sur des interprétations alternatives et de se former une opinion basée sur des informations suffisantes. De manière générale, les efforts visant à automatiser la justice administrative n'ont pas amélioré la performance humaine – ils l'ont même fortement dégradée[25]. Automatiser ces aspects essentiels du jugement humain dans les procé-

25 Danielle Keats Citron, « Technological due process », dans *Washington University Law Review*, Vol. 85, 2008, pp. 1249-1292.

dures judiciaires équivaudrait à déshumaniser la justice, et une telle perspective devrait être rejetée par principe.

Si j'affirme que l'on devrait rejeter par principe l'automatisation du raisonnement humain dans les procédures judiciaires, c'est parce qu'il n'existe encore, à mon avis, aucun système automatisé (quel que soit son niveau de performance) que nous pourrions accepter en tant que substitut d'un être humain. En somme, quand un système judiciaire, un État ou ses agents sont appelés à prendre des décisions touchant aux droits fondamentaux de la personne humaine, les agents et les fonctionnaires de l'État à qui appartient la décision finale doivent être eux-mêmes humains. Des motifs non seulement moraux mais également juridiques peuvent être avancés à l'appui de ce principe. En effet, indépendamment de son statut sur le plan éthique, ce principe est un élément constitutif et essentiel du système de justice lui-même.

Au sein de chaque armée, du commandant en chef au simple soldat, il existe de nombreux niveaux de délégation de l'autorité. Toutefois, à chacun de ces niveaux se trouve un humain à qui incombent à la fois l'autorité et la responsabilité du recours à la force. La responsabilité du supérieur hiérarchique ne permet pas d'éviter l'obligation morale et juridique de déterminer si l'emploi de la force est approprié dans une situation donnée. Cette obligation peut être transférée à un autre agent humain responsable, le supérieur qui délègue son autorité étant alors tenu de superviser la conduite de son subordonné. Dans la mesure où les systèmes d'armement autonomes ne sont pas des agents humains responsables, cette autorité ne peut pas leur être déléguée.

En ce sens, le respect du principe de distinction peut être vu non seulement comme l'obéissance à une règle qui demande de distinguer les combattants des civils, mais aussi comme la prise en compte des vies humaines qui risqueraient d'être perdues en cas d'emploi de la force létale. Il est donc nécessaire qu'un être humain prenne une décision basée sur des informations suffisantes avant d'ôter la vie d'autrui. Cette exigence apparaît plus nettement quand il s'agit de respecter le principe de proportionnalité. Il faut en effet, dans ce cas, mettre en balance la valeur de vies humaines (qu'il s'agisse de civils ou de combattants) et la valeur d'objectifs militaires. Or, aucune de ces valeurs n'est fixe et, d'une certaine façon, elles découlent précisément des jugements éthiques qui entrent dans les calculs de proportionnalité.

Voilà donc pourquoi l'on ne saurait prétendre qu'un système d'armement autonome serait moralement supérieur à un soldat humain, au motif qu'il pourrait être technologiquement capable de commettre moins d'erreurs en accomplissant une tâche de discrimination, ou de trouver des moyens de neutraliser des cibles militaires réduisant de façon optimale le risque de provoquer des pertes et des dommages disproportionnés. Cela ne signifie nullement qu'il n'est pas désirable de poursuivre de tels buts. S'il existait vraiment des technologies qui soient capables de faire la différence entre civils et combattants mieux que tout être humain, ou mieux que le combattant « moyen », ces technologies devraient alors être déployées non pas pour pouvoir se passer de tout jugement humain, mais pour aider les combattants à respecter le principe de distinction. De même, s'il

existait une technologie capable de déterminer la marche à suivre pour détruire un objectif militaire en causant un minimum de dommages collatéraux et en réduisant au maximum les pertes et les dommages disproportionnés, cette technologie pourrait être employée par des combattants humains, tenus de prendre en connaissance de cause la décision d'employer la force létale dans une situation donnée.

Tout processus automatisé – aussi performant soit-il, et même si sa performance excède notablement celle d'un humain – devrait être soumis au contrôle d'un opérateur humain avant de pouvoir légitimement utiliser la force létale. Cette exigence est requise sur le plan technologique pour ce qui est de l'avenir prévisible car, pendant quelque temps encore, les robots n'atteindront pas le niveau de performance des êtres humains. Surtout, c'est une exigence morale, et dans de nombreux cas importants, juridique. J'affirme donc que, de manière générale, nous avons le devoir de ne pas autoriser des systèmes d'armement autonomes à faire usage de la force létale si aucune supervision et aucun contrôle direct ne sont exercés par un humain.

Deux stratégies sont utilisées aujourd'hui pour défendre l'argument selon lequel les systèmes d'armement autonomes pourraient constituer un moyen de guerre moralement ou juridiquement supérieur à ceux qui sont aujourd'hui déployés dans les conflits armés. Cet argument se présente sous de nombreuses variantes, que je range pour ma part en deux catégories : 1) les arguments pragmatiques, axés sur les défaillances du processus de prise de décisions létales pendant les conflits armés, et insistant sur les possibles/hypothétiques améliorations technologiques à attendre de l'automatisation de ces décisions[26] ; 2) les arguments insistant sur le fait que si de tels systèmes permettent de réduire de manière générale les risques encourus par les combattants et/ou les civils (la diminution du nombre de victimes venant le confirmer), il existe un impératif moral enjoignant de les utiliser. Ces mêmes arguments ont été avancés dans le passé pour promouvoir les armes de précision[27] ainsi que, plus récemment, pour promouvoir les drones de type *Predator* et certaines armes létales commandées à distance[28].

Les armes plus précises sont-elles plus « morales » que les armes de moindre précision ? Imaginons que nous nous trouvons devant le choix suivant : attaquer une cible militaire en utilisant des munitions à guidage de précision, et donc avec un faible risque de dommages collatéraux, ou attaquer la même cible en lançant un « tapis de bombes », avec un niveau élevé de probabilité (sinon de certitude) que les dommages collatéraux seront importants. Il est assez facile de défendre l'argument selon lequel les munitions à guidage de précision seraient préférées par tout individu placé devant un tel choix. Voilà précisément, toutes choses étant égales par ailleurs, le type de décision morale et légale que nous

26 Ronald C. Arkin, « Governing lethal behavior: embedding ethics in a hybrid deliberative/reactive robot architecture », Georgia Institute of Technology, Technical Report GUT-GVU-07-11, 2007, p. 11.

27 Human Rights Watch, « International humanitarian law issues in the possible U.S. invasion of Iraq », dans *The Lancet*, 20 février 2003.

28 Bradley Jay Strawser, « Moral Predators: the duty to employ uninhabited aerial vehicles », dans *Journal of Military Ethics*, Vol. 9, N° 4, 2010, pp. 342-368.

devons prendre aujourd'hui. Bien sûr, l'expression « toutes choses étant égales par ailleurs » peut être un grand fourre-tout dans lequel chacun glissera ce qu'il voudra. Certes, au moment de décider de la manière d'engager une cible, l'opérateur devrait préférer l'arme la plus précise. Fort bien, mais l'arme choisie n'est pas éthiquement étrangère à cette décision. En fin de compte, c'est l'opérateur humain qui choisit d'utiliser (ou non) l'arme qu'il juge la plus « morale » ; même la plus précise des armes peut être utilisée de manière illégale et immorale. Tout ce qu'apporte la précision, c'est la possibilité, pour l'utilisateur de l'arme, d'opter pour une façon d'agir plus éthique : elle ne détermine ni ne garantit l'adoption d'un tel comportement.

L'argument ci-dessus peut paraître purement sémantique, mais la distinction qui est faite est cruciale. Nous ne mettons pas fin à nos responsabilités morales en recourant à des technologies plus précises. Par contre, comme dans le cas d'autres systèmes automatisés (tels que le régulateur de vitesse ou le pilotage automatique d'un véhicule), nous continuons à tenir l'opérateur responsable tant du système qu'il gère que de la décision ultime d'enclencher ou de désenclencher le système automatisé ; l'opérateur est ultimement responsable de la pertinence de ses choix. En effet, la plupart du temps, comme nous l'avons vu dans l'emploi des munitions à guidage de précision et des drones de combat, ces technologies augmentent en fait le fardeau moral qui pèse sur l'opérateur, à savoir : faire en sorte que les cibles soient correctement sélectionnées et que les civils soient épargnés. Dès lors, à mesure que nos technologies gagnent en sophistication, nous devrions les concevoir de telle manière que leur perfectionnement améliore notre conduite morale.

Il y a quelque chose de profondément étrange dans l'idée que l'on pourrait accroître la moralité de la conduite de la guerre en automatisant celle-ci (à tel point que l'humain n'y jouerait plus aucun rôle) ou, tout au moins, en automatisant les décisions de recours à la force létale. La stratégie rhétorique visant à rendre ces arguments plus convaincants consiste à mettre l'accent sur les défaillances morales des humains en temps de guerre. Les actes dictés par la peur ou le désespoir et les erreurs commises sous l'effet du stress ou de la contrainte et dans le « brouillard de la guerre » sont montrés du doigt. L'étape suivante consisterait donc à proposer une solution technologique susceptible d'éliminer de telles défaillances. L'idée pourrait être séduisante, mais aucune technologie de ce type n'existe encore. Par ailleurs, deux points cruciaux n'ont pas été relevés à propos des nouveaux types de technologies automatisées que nous voyons apparaître. Premièrement, en éloignant les soldats des risques immédiats de la guerre (ce que font les systèmes opérés à distance, sans pour autant automatiser les décisions létales), nous pouvons aussi leur éviter de subir une grande part des pressions psychologiques évoquées plus haut, et donc de commettre les erreurs qui s'ensuivent. Deuxièmement, si un système automatisé était capable de meilleures performances que les humains dans les tâches de discrimination ou dans les calculs de proportionnalité, il pourrait tout aussi facilement remplir une fonction consultative auprès des décideurs humains. De tels systèmes automatisés assisteraient et renseigneraient les opérateurs

sans qu'il soit nécessaire de leur transférer l'autorité de recourir à la force létale en l'absence de toute décision (basée sur des informations suffisantes) prise par un humain[29].

Arguments contre l'interdiction des systèmes d'armement autonomes

Dans une note d'orientation publiée récemment, Anderson et Waxman ont présenté un examen critique des propositions d'interdiction des systèmes d'armement autonomes[30]. Ils concluent qu'il est important d'établir des normes internationales relatives à l'emploi des systèmes d'armement autonomes, mais qu'une interdiction ne constitue pas la meilleure option. Tant l'argumentation que beaucoup de conclusions présentées par ces auteurs soulèvent néanmoins de nombreux problèmes. Leur argumentation repose essentiellement sur deux postulats :

> Dans la recherche de solutions aux dilemmes juridiques et éthiques qui accompagnent ces technologies émergentes, il est capital de reconnaître que l'évolution de ces technologies est inéluctable et qu'elle se fera de manière progressive. La politique des États-Unis visant à résoudre ces dilemmes devrait être élaborée en partant de ces postulats. Étant donné le développement et le déploiement (certains, mais graduels) de ces systèmes, ainsi que les avantages humanitaires liés à la précision que présentent quelques-uns d'entre eux, certaines mesures proposées – telles que des traités d'interdiction – sont à la fois impossibles à implanter et contestables sur le plan de l'éthique[31].

Nous avons ici plusieurs arguments contre la proposition d'un traité international d'interdiction. Les auteurs insistent tout d'abord sur les deux postulats de départ : l'apparition de ces technologies est inévitable, et leur développement sera progressif. Ils n'apportent cependant aucun élément de preuve ni aucun argument à l'appui de l'une et l'autre de ces hypothèses, alors qu'il existe de solides raisons de les rejeter. Ils avancent ensuite l'argument selon lequel certains de ces systèmes pourraient présenter des avantages sur le plan humanitaire et que, par conséquent, les mesures visant à les interdire sont à la fois « impossibles à implanter » et « contestables sur le plan de l'éthique ». Je viens d'expliquer pourquoi il n'est pas « contestable sur le plan de l'éthique » d'affirmer que même les plus précis des systèmes d'armement autonomes mettent en péril les droits de l'homme. Je m'intéresserai donc maintenant aux deux postulats préliminaires d'Anderson et Waxman, ainsi qu'à leur éventuelle incidence

29 Peter Asaro, « Modeling the moral user : designing ethical interfaces for tele-operation, dans *IEEE Technology & Society*, Vol. 28, N° 1, 2009, pp. 20-24, disponible sur : http://peterasaro.org/writing/Asaro%20Modeling%20Moral%20User.pdf .

30 K. Anderson et M. C. Waxman, *op. cit.*, note 3, p. 13. [Traduction CICR]

31 *Idem*, p. 2.

sur la mise en œuvre d'une interdiction internationale des systèmes d'armement autonomes.

Les systèmes d'armement autonomes sont-ils inévitables ?

Pourquoi devrions-nous partir du principe que les systèmes d'armement autonomes sont inévitables ? Qu'est-ce que cela pourrait réellement signifier ? En tant que philosophe et historien des sciences et des technologies, je rencontre souvent des déclarations sur le caractère « inéluctable » des découvertes scientifiques ou des innovations technologiques. La popularité de cette assertion est due en grande partie au caractère rétrospectif de toute démarche historique et au fait que, pour réfléchir à la possible évolution des technologies, nous nous basons sur ce que nous avons pu comprendre dans le passé. En d'autres termes, il paraît facile aujourd'hui pour nous d'affirmer que l'invention de l'ampoule électrique, ou du téléphone, ou de n'importe laquelle des technologies était inéluctable, puisqu'elle a bel et bien eu lieu… Il est difficile d'imaginer ce que serait le monde sans ces inventions. Pourtant, un examen attentif des détails historiques révèle que, le plus souvent, le succès d'une technologie a été extrêmement tributaire de toute une série de facteurs. Dans la plupart des cas, l'adoption de la technologie n'a pas été garantie par le succès de l'innovation. De fait, les moyens et les manières de son éventuelle utilisation dépendent toujours d'une grande variété de forces qui s'exercent aux niveaux sociétal et culturel. Assurément, il suffit de se pencher sur les nombreux grands « couacs » de la technologie et, par exemple, sur la succession d'échecs enregistrés par la commercialisation de l'ampoule électrique avant son premier succès, pour se rendre compte que les technologies pouvant être qualifiées d'« inévitables » ou d'« inéluctables » sont très rares, voire inexistantes. Même le succès de l'ampoule électrique doit beaucoup à l'innovation et au développement des services d'électricité, et son adoption généralisée s'explique par la mise au point d'une foule d'autres appareils électriques (les grille-pain, par exemple). Désormais bien plus rapide, l'évolution des technologies reste un phénomène toujours aussi dynamique et imprédictible.

Peut-être Anderson et Waxman veulent-ils dire que le développement de ces technologies aura fort probablement lieu ? Voilà qui est plus plausible. En effet, des systèmes rudimentaires peuvent déjà exécuter les fonctions essentielles d'un système d'armement autonome ; ils seraient néanmoins incapables de satisfaire aux normes juridiques internationales en vigueur exigeant le respect des principes de distinction et de proportionnalité[32]. Mais même en ignorant les limitations juridiques existantes, le fait que nous soyons capables de construire des technologies létales autonomes ne signifie pas nécessairement que nous les utiliserons. D'aucuns pourraient prétendre que divers types de systèmes d'armement autonomes peuvent déjà être fabriqués et que, dès lors, c'est leur

32 M. Wagner, *op. cit.*, note 11, pp. 5-9.

adoption qui est « inéluctable ». Un tel argument équivaudrait cependant à dissimuler d'importants éléments qui différencient l'invention d'une technologie et son adoption généralisée au sein de la société. Il existe certainement des motivations très solides pour adopter ces technologies, y compris le désir de réduire les risques courus par les militaires et de diminuer les frais et le personnel mobilisé dans diverses opérations et capacités militaires.

Ou alors, peut-être Anderson et Waxman veulent-ils dire que nous devrions partir du postulat qu'il est inévitable que soient mis au point des systèmes d'armement autonomes capables de respecter les règles exigeant un certain degré de discrimination et de proportionnalité. Ce postulat n'est cependant qu'une affirmation empirique relative aux capacités de technologies encore non existantes, et qui sont mesurées à l'aune de critères encore non définis. Sur un plan purement empirique, nous ignorons si ces technologies verront ou non le jour et si nous parviendrons à nous mettre d'accord sur des critères acceptables pour en évaluer les performances. Dès lors, pourquoi devrions-nous croire que le développement de ces technologies est inéluctable[33] ?

La question cruciale est donc la suivante : ces nouvelles technologies peuvent-elles déjà, ou pourront-elles, satisfaire aux exigences du droit international ? Je répondrai que cela est loin d'être certain. Les arguments affirmant la supériorité éthique des soldats robots ressemblent étrangement à ceux que l'on a entendus aux premiers temps de l'intelligence artificielle selon lesquels les ordinateurs finiraient par battre nos grands maîtres humains au jeu d'échecs. Et voilà qu'avec un retard de quarante ans par rapport aux prédictions initiales, l'ordinateur *Deep Blue* d'IBM a réussi à battre Gary Kasparov. Entre le jeu d'échecs et le DIH, il existe toutefois d'importantes différences qui méritent d'être relevées. Les échecs sont un jeu assez bien défini, basé sur un ensemble de règles et qui se prête à l'analyse informatique. Il n'est question dans ce jeu ni d'interprétation, ni de normes sociales. Bien qu'il ait lui aussi des règles, le droit international est autre chose que le jeu d'échecs. Pour pouvoir être appliqué aux situations du monde réel, le droit, quel qu'il soit, nécessite interprétation et jugement. Certes, les précédents historiques et les normes établies facilitent ces activités d'interprétation et de jugement mais ils ne les déterminent pas de manière stricte. Le corpus constitué par la jurisprudence, les procédures, les plaidoiries et les appels est apte à défendre de vieux principes ou à établir de nouveaux précédents. Ce faisant, il établit des normes et des principes, même si le sens de ces normes et principes continue d'évoluer au fil du temps.

Prétendre avec insistance que les systèmes d'armement autonomes sont inévitables est donc un argument assez pernicieux. D'une part, un tel postulat ferait apparaître l'établissement d'une interdiction comme automatiquement

33 Prenons, à titre de comparaison, le cas des voitures électriques, une technologie qui existe déjà depuis une centaine d'années. Malgré la récente popularité des voitures hybrides (essence-électricité) et les très bonnes performances de certaines voitures électriques, bien peu de gens seraient prêts à soutenir l'argument selon lequel notre transition vers la voiture électrique est inévitable. Or, la technologie dont nous parlons est non seulement « possible », mais elle existe déjà !

impossible à respecter ou à mettre en œuvre. En d'autres termes, si l'on admet que les systèmes prohibés existeront et seront utilisés, à quoi bon les interdire ? Bien sûr, ces systèmes n'existent pas et ne sont pas utilisés aujourd'hui. De fait, même s'ils étaient déjà utilisés, une interdiction pourrait empêcher leur usage ultérieur. Loin d'être impossible à respecter ou à mettre en œuvre, une interdiction pourrait contribuer de manière assez efficace à infléchir les trajectoires de l'innovation vers des systèmes plus utiles et véritablement conformes à l'éthique. Il semble évident que la catégorie des systèmes d'armement autonomes peut être définie de façon suffisamment claire. Nous pourrons donc débattre ensuite de la manière dont un traité s'appliquerait (ou ne s'appliquerait pas) à certains cas « limites » (blindages réactifs, systèmes de défense antimissile balistique ou systèmes de surveillance, par exemple). Il est peu probable qu'une interdiction vienne prohiber tout recours, sans exception, à l'automatisation dans les conflits armés. Elle devrait, par contre, établir une norme internationale selon laquelle il est illicite d'employer des systèmes qui prennent des décisions létales de manière automatisée. Les traités internationaux d'interdiction des mines terrestres et des armes à sous-munitions n'ont peut-être pas fait entièrement disparaître les mines terrestres et les armes à sous-munitions, ni supprimé leur emploi dans les conflits armés. Toutefois, depuis que ces traités existent, il est plus difficile, pour les fabricants, de produire ces armes de façon profitable et, pour les militaires, de les employer sans répercussions au sein de la communauté internationale.

Il apparaît en outre que si l'on prend pour postulat de départ le caractère inévitable des systèmes d'armement autonomes, leur acceptabilité est nécessairement tenue pour acquise. Pourtant, en définitive, ce qui compte, c'est de savoir quels critères internationaux seront utilisés pour déterminer l'acceptabilité de ces systèmes. En d'autres termes, quelles sont les normes de conduite qui seront jugées acceptables par la communauté internationale ? Accepter de postuler que le développement et l'emploi de ces technologies sont inéluctables empêche tout nouveau débat sur le bien-fondé et la pertinence de la démarche qui consiste à étudier, développer et employer ces technologies. Bref, comme dans le cas de toute autre technologie, ni la mise au point ni l'emploi de systèmes d'armement autonomes ne sont inévitables. Certes, de tels systèmes sont réalisables ; s'ils ne l'étaient pas, il n'y aurait aucun besoin de les interdire. Néanmoins, leur développement nécessite encore d'importants investissements. Même si nous ne parvenons pas à empêcher la création de certaines technologies, nous pourrons toujours défendre notre position quant à l'acceptabilité morale et juridique de leur emploi. Il ne suffit pas qu'une technologie existe pour que son emploi soit acceptable.

Les conséquences d'un développement progressif des systèmes d'armement autonomes

Permettez-moi de revenir au second postulat d'Anderson et Waxman, à savoir que le développement des systèmes d'armement autonomes ne sera pas brusque

mais progressif. Quelle contribution ce postulat est-il censé apporter à l'argumentation de ces auteurs ? Toutes les technologies connaissent, d'une manière ou d'une autre, ce type de développement. Pourquoi cela devrait-il modifier notre façon d'appréhender les implications éthiques et juridiques de telles innovations ? Anderson et Waxman tentent-ils simplement de dissiper la crainte d'un grand bond technologique à l'issue duquel des robots remplaceraient les soldats humains ? À mesure que ces auteurs développent leur argumentation, nous comprenons mieux ce qu'ils veulent dire : la transition vers les systèmes d'armement autonomes ne sera pas brutale ; elle se fera « à petits pas », chacun de ces pas étant soigneusement examiné. Il s'agit là d'une inversion assez habile de l'argument de la « pente glissante ». Anderson et Waxman ne disent pas que ces technologies sont dangereuses parce qu'elles nous encouragent à déléguer toujours davantage d'autorité aux systèmes automatisés (ce qui, à terme, nous amènerait à doter les robots de l'autorité – illégitime mais réelle – de cibler et de tuer des êtres humains). Ces systèmes seront légitimes parce que chaque étape de leur mise au point nous aura paru acceptable. En quelque sorte, nous devrions accepter la conclusion de cette ligne de raisonnement au motif que nous avons pu l'atteindre grâce à une série d'ajustements moraux, dont aucun n'est apparu, en lui-même, trop détestable.

Il serait plus sensé de considérer ce processus comme une pente glissante qui nous mène à un résultat qui nous paraît inacceptable. Nous devrions, dès lors, rechercher avec davantage de soin un principe sous-jacent que nous pourrions invoquer afin de stopper notre périlleuse glissade vers une conclusion indésirable. Or, une limite fondée sur des principes existe, et nous pouvons l'imposer aux systèmes d'armement autonomes. Cette prescription peut être énoncée ainsi : un être humain doit être impliqué de manière significative chaque fois que la décision d'employer la force létale doit être prise. Nous pourrions, certes, assouplir cette règle en faisant intervenir divers systèmes technologiques de contrôle partagé et de contrôle hiérarchique. Nous pourrions aussi concevoir les systèmes d'armement autonomes de manière telle que la règle imposée soit au contraire plus claire, et que les décisions létales soient mieux informées[34].

De la nécessité d'établir des normes

Les conclusions d'Anderson et Waxman sont erronées en ce qui concerne les implications d'une interdiction des systèmes d'armement autonomes. Par contre, ces auteurs ont raison sur deux points, à savoir la signification de l'établissement de normes visant à régir l'emploi de ces systèmes et la nécessité d'imposer certaines contraintes :

> Les États-Unis doivent néanmoins agir avant que les attentes internationales relatives à ces technologies se durcissent, sous l'influence de ceux qui souhai-

34 P. Asaro, *op. cit.*, note 29, pp. 20-24 .

> teraient imposer des interdictions irréalistes, ineffectives ou dangereuses, ou de ceux qui préféreraient peu de contraintes, ou pas de contraintes du tout[35].

Anderson et Waxman prennent donc acte ici du fait que ces technologies ouvrent effectivement un nouvel espace moral. Nul ne sait à ce stade ce que la communauté internationale acceptera en tant que nouvelles normes applicables à la conduite des hostilités à l'ère de la robotique et de l'automatisation. Ces auteurs ont aussi raison d'affirmer que les États-Unis – à la fois superpuissance et chef de file dans le développement de ces nouvelles technologies – sont mieux placés que quiconque pour créer des précédents et établir les normes qui façonneront l'avenir des conflits armés. Par contre, Anderson et Waxman n'ont pas montré en quoi il serait irréaliste d'interdire les systèmes d'armement autonomes ; ils n'ont pas non plus apporté la moindre preuve qu'une telle interdiction serait inefficace ou immorale. Examinons donc tour à tour chacune de ces thèses.

Comment devons-nous comprendre l'argument selon lequel une interdiction des systèmes d'armement autonomes serait irréaliste ? Cela signifie-t-il qu'une telle interdiction serait difficile à implanter dans la pratique ? Tous les traités de maîtrise des armements présentent des défis de mise en œuvre. L'interdiction des systèmes d'armement autonomes ne devrait pas être exceptionnellement plus difficile que d'autres à mettre en application – elle n'est donc pas irréaliste. Devons-nous plutôt comprendre qu'il serait politiquement difficile de rallier un soutien suffisant pour une telle interdiction ? D'après mon expérience personnelle, je pense qu'une telle interdiction trouverait un soutien auprès de nombreux individus (en particulier parmi les officiers militaires et les responsables politiques, mais aussi parmi les ingénieurs et les dirigeants de l'industrie de la défense). De par ma pratique du dialogue avec le public, je sais aussi que les systèmes d'armement automatisés, au même titre que les risques potentiels qui leur sont liés, suscitent des appréhensions morales, fortes et largement répandues. Je dirai donc *a minima* qu'une interdiction n'est pas irréaliste dans la mesure où elle est susceptible d'obtenir un large soutien de la part du public et des autorités.

En fait, la seule raison de considérer qu'une telle interdiction est irréaliste serait d'accepter le premier postulat (non démontré) d'Anderson et Waxman proclamant le caractère inéluctable des systèmes d'armement autonomes. Il est vrai que si nous acceptons comme une fatalité le développement de ces systèmes, toute tentative visant à empêcher que l'inévitable se produise paraît effectivement irréaliste. Il n'y a toutefois rien d'inévitable dans le développement d'une technologie émergente, dont les capacités n'existent pas encore, et au sujet de laquelle aucune norme n'a encore été établie.

Anderson et Waxman anticipent également un argument contre les systèmes d'armement autonomes, fondé sur un principe moral :

35 K. Anderson et M. C. Waxman, *op. cit.*, note 3, p. 2. [Traduction CICR]

> Une deuxième objection, d'ordre moral, consiste à dire que le retrait de tout agent moral humain de la « boucle de tir » constitue simplement une erreur en soi. Une machine, aussi performante fût-elle, ne peut pas totalement remplacer la présence d'un véritable agent moral, c'est-à-dire d'un être humain possédant une conscience et la faculté de jugement moral (malgré les imperfections de la nature humaine). D'ailleurs, le titre du présent document est délibérément provocateur puisqu'il assimile « robot » à « soldat », alors que c'est précisément ce que l'on ne devrait jamais tenter de faire.
>
> Il s'agit là d'un argument auquel il est difficile de répondre, car il s'arrête sur un principe moral que l'on ne peut qu'accepter ou refuser[36].

L'objection dont parlent Anderson et Waxman s'appuie sur ce qui est censé être une sorte de principe en soi[37]. Ces auteurs supposent dès lors que la seule raison d'accepter ce principe serait de se fier à ses propres intuitions morales. À mon avis, les arguments présentés plus haut dans le présent article ont clairement démontré que le principe moral au nom duquel nous nous opposons aux systèmes d'armement autonomes est en fait contenu de manière implicite dans le DIH et s'exprime à travers ses diverses formulations et exigences anthropocentriques. Ce principe est en outre implicite dans la structure même des lois et de l'administration de la justice (droit à une procédure régulière, notamment). Si la présence d'un humain est requise, c'est en tant qu'« agent juridique », indépendamment de la nécessité qu'il soit un « agent moral ».

Ce n'est pas uniquement parce que la décision de tuer est lourde à prendre (bien qu'elle le soit, assurément). La décision de tuer un humain ne peut être légitime que si elle est non arbitraire. Or, en l'absence de contrôle, de supervision et de responsabilité exercés par un humain, il n'y a aucun moyen de garantir le caractère non arbitraire de l'emploi de la force. Tuer sans que s'exercent la raison, le jugement et la compassion d'un humain est donc immoral – et devrait être illégal.

Conclusions

Afin de préserver la moralité humaine, la dignité, la justice et le droit, nous ne pouvons pas accepter qu'un système automatisé prenne la décision de tuer un humain. Nous devrions, afin de respecter ce principe, prohiber les systèmes d'armement autonomes. Quand il est question de vie ou de mort, chaque cas mérite d'être examiné avec attention et considération par un humain, étant donné le poids moral que porte en soi la suppression d'une vie humaine.

À mesure qu'elle progresse, la technologie permet à l'humanité d'exercer sur le monde un contrôle toujours plus étendu. Ce nouveau contrôle s'accompagne d'une responsabilité accrue. Bien sûr, cela semble évident

36 *Idem*, p. 11.
37 M. Bolton, T. Nash et R. Moyes, *op. cit.*, note 11.

dans le cas des technologies qui influencent le bien-être de la population et la protection de l'environnement, mais cela vaut également pour les technologies militaires. Le développement de technologies militaires avancées n'implique pas nécessairement que celles-ci peuvent être utilisées (et seront utilisées) avec davantage de prudence et de manière plus éthique, même si une telle possibilité existe. Mais les nouvelles capacités s'accompagnent d'un risque de régression sur les plans de l'éthique et de la moralité, plutôt que d'un potentiel de progrès. En définitive, la technologie déterminera la nature des progrès que nous ferons sur le plan moral dans la manière de conduire les hostilités. L'impact sera plus profond que le simple fait de donner aux combattants la possibilité de conduire des guerres peu coûteuses en vies humaines. Cela va au-delà des exigences du DIH et du DIDH. En choisissant les armes et les tactiques avec lesquelles nous nous engageons dans un conflit armé, nous opérons également un choix moral quant au monde dans lequel nous souhaitons vivre et pour lequel nous voulons nous battre, et quant aux conditions légitimes dans lesquelles nous pouvons faire advenir ce monde. Au moment de ces choix, nous devons résister aux arguments voulant que « la fin justifie les moyens ». Nous devons aussi reconnaître que les moyens mobilisés pour opérer des changements dans le monde, ou pour résister à de tels changements, deviennent ainsi un aspect de ce monde. Si nous souhaitons vraiment construire un monde dans lequel les conflits armés seront à la fois inutiles et inacceptables, nous devrons, pour y parvenir, adopter un processus permettant que chaque nouvelle innovation technologique vienne élever, et non abaisser, nos principes moraux.

La communauté internationale devrait entamer des discussions sur l'élaboration d'un traité d'interdiction des systèmes d'armement autonomes. Dans la mesure où de tels systèmes n'existent pas encore, le fait de les interdire contribuerait à infléchir le développement des technologies militaires de demain en l'axant non pas sur ce que l'on nomme les « systèmes éthiques », mais sur des systèmes qui soient capables de réellement améliorer le comportement éthique des humains dans les conflits armés. Ceux qui s'opposent à une telle interdiction basent leur argumentation tant sur des affirmations infondées de l'inévitabilité de ces technologies que sur des allégations mensongères concernant des technologies éthiquement évoluées. Aussi longtemps que les capacités potentielles de ces technologies resteront incertaines, leur émergence aura lieu dans un champ de normes éthiques et juridiques évoluant rapidement. Bien sûr, nous aimerions pouvoir faire confiance à la promesse de guerres plus éthiques, rendues possibles par ces hypothétiques systèmes d'armement autonomes. La réalité est malheureusement différente : ces systèmes peuvent aussi dégrader nos conceptions et nos critères en matière de conduite éthique ; en nous incitant à poursuivre la mise au point d'une technologie improbable qui menace nos droits humains au niveau fondamental, ils risquent en outre de nous amener à ne plus chercher à améliorer le raisonnement moral humain par le biais des technologies. Ces systèmes risquent aussi de nous dissuader de continuer à renforcer et à améliorer le DIH et le DIDH afin qu'ils soient à même de relever de façon appropriée et moralement acceptable les défis posés par ces nouvelles technologies.

Volume 94 Sélection française 2012/2

REVUE INTERNATIONALE

Au-delà de « Call of Duty » : pourquoi les joueurs de jeux vidéo ne feraient-ils pas face aux mêmes dilemmes que les soldats ?

Ben Clarke, Christian Rouffaer et François Sénéchaud*

Ben Clarke est professeur agrégé à l'université de Notre-Dame d'Australie et était conseiller auprès de l'Unité relations avec la société civile du Comité international de la Croix-Rouge (CICR).
Christian Rouffaer est conseiller auprès de l'Unité relations avec les forces armées, CICR.
François Sénéchaud est chef de la Division de l'intégration et de la promotion du droit, CICR.

Résumé

Les jeux vidéo donnent aux joueurs une fausse idée de ce que les soldats sont autorisés à faire durant une guerre. Ils peuvent aussi avoir un impact sur la façon dont les combattants se comportent dans les conflits armés actuels. Bien qu'ils offrent à des millions de joueurs un moyen extrêmement divertissant de s'évader de la réalité, certains jeux vidéo donnent l'impression que des actes interdits, tels que la torture ou les exécutions extrajudiciaires, sont normaux. Les auteurs soutiennent qu'une meilleure intégration du droit international humanitaire pourrait permettre de mieux faire connaître les règles de la guerre à des millions de

* Nous tenons à remercier Helen Durham, Alexandra Boivin, Neil Davidson, Ray Smith et Vincent Bernard pour leur précieuse contribution. Les opinions exprimées dans cet article sont celles des auteurs et ne reflètent pas nécessairement le point de vue du CICR. Tous les sites Internet indiqués en référence ont été consultés en 2012, sauf indication contraire.
La version originale en anglais de cet article est publiée sous le titre « Beyond the Call of Duty: why shouldn't video game players face the same dilemmas as real soldiers ? », dans *International Review of the Red Cross*, Vol. 94, N° 886, été 2012, pp. 711-737.

joueurs, y compris des recrues potentielles et des soldats déployés, offrant ainsi l'espoir que cette branche du droit soit mieux respectée sur les futurs champs de bataille.

Mots-clés : jeux vidéo, influence, comportement, effet nuisible, applicabilité, défis, messages, obligation, initiative, banalisation.

: : : : : : : :

Tandis que je scrute l'horizon à la recherche de cibles, une rivière de feu traverse le ciel nocturne et des lueurs dansantes illuminent la ville de rouge et de blanc. Je vois du phosphore blanc tout autour de nous. Ce truc tue tout ce qu'il touche. Nos obus de 155 mm, en alternance avec le phosphore blanc et les explosifs brisants, affaiblissent les positions ennemies avant l'attaque. Dans un instant, nous quitterons la sécurité de notre véhicule blindé pour initier le boulot sanglant des fantassins, fouillant les maisons et tuant les méchants. Nous devons avancer. Nous ne pouvons pas laisser les terroristes se replier et se regrouper. Nous avons établi une tête de pont dans la ville et nous devons exploiter ce succès en pénétrant le plus profondément possible en territoire ennemi. Nous avons pour instructions de nous emparer du quartier général ennemi, une grande maison au bout de la rue. Le succès de la campagne repose entièrement sur nos épaules.

Notre chef d'escouade se tourne vers nous, nous lance rapidement quelques ordres et se dirige vers l'entrée arrière. Je jette une grenade vers le bâtiment municipal. Quand elle explose, la fumée et les débris envahissent la rue. Nous tirons quelques salves de M 203 pour faire bonne mesure. L'explosion nous sert d'écran de fumée. Tandis que nous avançons, un membre de notre équipe est abattu par le tir d'un sniper provenant d'un bâtiment sur notre gauche. On dirait un hôtel. Je demande un drone. Presque immédiatement, il lâche sa charge meurtrière sur le bâtiment, ne laissant qu'un tas de décombres. Pas besoin de se préoccuper d'éventuels occupants ou dégâts collatéraux : toute la ville n'est habitée que par de dangereux terroristes sans foi ni loi et peut être détruite. Tout être humain que notre équipe rencontre constitue une cible. Les mines antipersonnel sont un bon moyen de sécuriser les rues et les bâtiments dont nous nous sommes emparés. Pendant quatre heures consécutives, nous entrons dans les maisons, tuant quiconque entre dans notre ligne de mire, et récupérons les plaques d'identité de nos victimes comme autant de trophées. Les ennemis blessés, en général, essaient de se défendre, et même si ce n'est pas le cas, ils reçoivent deux balles comme les autres. Après tout, la reddition n'est pas une option. Seuls les chefs ennemis sont capturés vivants : les morts ne peuvent pas donner de renseignements, même sous la torture. Chaque ennemi que j'abats d'un tir dans la tête à l'aide de mon fusil d'assaut M4 Busmaster – avec le silencieux que j'ai obtenu pour avoir tué 100 ennemis – me permettent de progresser plus vite dans le classement du jeu[1].

1 Récit fictif inspiré de l'expérience des auteurs et d'un récit de la bataille de Fallouja, dans David Bellavia, *Fallouja*!, Nimrod, Paris, 2009.

Les jeux vidéo[2] offrent aux joueurs la possibilité d'« utiliser » les armes les plus récentes contre des combattants ennemis sur des champs de bataille actuels. Mais malgré leur réalisme, tant au niveau des images que des sons, ces jeux présentent souvent des conflits armés auxquels ne s'appliquent aucune loi, où les actions sont sans conséquences. Ils envoient ainsi des messages négatifs aux joueurs au sujet de l'existence de normes humanitaires s'appliquant aux conflits armés réels et de la nécessité de les respecter. Pourquoi les joueurs ne peuvent-ils pas se procurer des jeux vidéo qui reflètent véritablement les dilemmes des combattants modernes ? Les jeux vidéo peuvent-ils être utilisés pour produire une influence positive qui permettrait de renforcer la connaissance et le respect de la loi ? Pourquoi les joueurs ne pourraient-ils pas être récompensés lorsqu'ils respectent les règles qui régissent l'usage de la force et le traitement réservé aux personnes tombées aux mains de l'ennemi et être sanctionnés en cas de violations de ces mêmes règles ?

***

Avec des centaines de millions de joueurs actifs (« *gamers* ») dans le monde[3], l'industrie du jeu vidéo est devenue un phénomène mondial qui transcende les différences sociales, culturelles et géographiques, ainsi que les classes d'âge et de revenu. Bien que la grande majorité des jeux vidéo ne montrent pas de situations de combat ni même d'ailleurs aucune forme de violence, ceux qui le font représentent un segment extrêmement lucratif, bien qu'étroit, du marché des jeux vidéo[4]. De Rio de Janeiro à Ramallah, des enfants et des adultes – y compris des soldats et des nouvelles recrues – sont captivés par cette forme de divertissement « militaire » appelé « *militainment* » (voir les chiffres cités dans le présent article)[5].

Les liens entre les jeux vidéo et le droit international humanitaire (DIH) constituent un domaine de recherche relativement nouveau et fragmenté, cou-

2 Dans cet article, nous désignons par « jeux vidéo » des jeux de tir en vue subjective ayant pour cadre des situations de combat – notamment des champs de bataille actuels tels que l'Irak, l'Afghanistan, le Liban, la Somalie et le Levant – où les joueurs tirent sur des cibles ennemies. L'industrie du jeu électronique utilise le terme « jeux de tir en vue subjective » pour désigner ce type de jeux, mais comme cet article est destiné à un lectorat plus large, nous avons préféré utiliser le terme « jeux vidéo ».

3 D'après une société, Spil Games, ses jeux en ligne compteraient 130 millions d'utilisateurs actifs mensuels. Elle estime qu'en 2010, 510 millions de personnes jouaient en ligne (*Spil Games, 2010 State of Gaming Report*). Selon une estimation, ce secteur a généré au moins 70 milliards de dollars américains en 2011. Voir IDATE, *World Video Games Market Data & Forecasts 2011-2015*, 17 janvier 2012.

4 Au moment de la publication de cet article, les jeux vidéo les plus populaires étaient : *Call of Duty: Black Ops II, Madden NFL 12, Halo 4, Assassin's Creed 3, Just Dance 4, NBA 2K13, Borderlands 2, Call of Duty: Modern Warfare 3, Lego Batman 2: DC Super Heroes* et *FIFA 12*. Vous trouverez les chiffres actuels des ventes pour les différentes plateformes (jeux) sous « 10 best selling videogames in 2012 », dans *Market Watch,* 10 janvier 2013, disponible sur : http://www.marketwatch.com/story/10-best-selling-videogames-in-2012-2013-01-10 (dernière consultation janvier 2013).

5 Le « *militainment* » a été décrit comme une « guerre adaptée à un usage récréatif » et un « divertissement à thème militaire célébrant le département de la défense (américaine) ». Voir Roger Stahl, *Militainment, Inc. – War, Media and Popular Culture*, Routledge, New York, 2009, p. 6 ; vous pouvez également visionner le documentaire « *Militainment, Inc: militarism and pop culture* » sur : http://watchdocumentary.org/watch/militainment-inc-e2-80-93-militarism-and-pop-culture-video_7baee6f62.html.

vrant divers points de vue. Il existe peu de documentation à ce sujet centrée sur le DIH. En conséquence, cet article est en grande partie prospectif. Il a pour but de mettre en évidence l'impact potentiel de ces jeux sur la perception qu'ont les joueurs du cadre normatif qui régit l'usage de la force. Nous nous concentrons sur les jeux de tir en vue subjective qui ont pour cadre des situations de combat, c'est-à-dire les jeux où les joueurs tirent sur des cibles ennemies sur des champs de bataille actuels, comme l'Irak, l'Afghanistan, le Liban, la Somalie et d'autres contextes du Levant[6]. Comme cet article ne traite pas de la question de la représentation de la violence en soi, il ne prend pas en compte les jeux vidéo dont les scénarios sont plus fictifs, comme le médiéval-fantastique ou les guerres futuristes se déroulant dans l'espace. Dans la première section, nous décrivons l'influence potentielle des jeux vidéo sur la perception qu'ont les joueurs des règles applicables sur les champs de bataille réels. La deuxième section étudie l'applicabilité du DIH et du droit international des droits de l'homme aux situations contemporaines représentées dans les jeux vidéo. Dans la troisième section, nous tournons notre attention vers les défis que constituent pour les normes humanitaires les jeux qui sont vendus comme une expérience « réelle » du combat, mais représentent en fait des champs de bataille où ne règne pour ainsi dire aucune loi. Dans la dernière section, nous présentons l'initiative lancée par le Comité international de la Croix-Rouge (CICR) conjointement avec diverses Sociétés nationales, et visant à collaborer avec l'industrie du jeu vidéo afin de l'encourager à introduire des innovations permettant de mieux intégrer le DIH et le droit international des droits de l'homme dans ces jeux. Nous relevons que, par le biais de cette initiative, les jeux vidéo – avec leur large portée et leur capacité de transmettre des connaissances et des compétences – peuvent devenir d'importants outils de promotion des normes humanitaires[7].

Influence des jeux vidéo

Les jeux vidéo et les comportements violents

Dire que la technologie influe sur les méthodes de guerre est un truisme. À notre sens, la technologie a également un impact sur la façon dont nous imaginons la guerre. Depuis toujours, l'image de la guerre a été façonnée par des chansons, des récits, des pièces de théâtre et des films héroïques et épiques. Aujourd'hui, des millions de personnes ont un accès direct à des films et des

6 Il existe différentes plateformes de jeux vidéo, les plus courantes étant les ordinateurs et les consoles. Dans cet article, le terme « jeux vidéo » désigne les deux.

7 Cela vaut également pour les programmes de simulation de l'armée qui représentent des champs de bataille contemporains. Les forces armées les utilisent de plus en plus pour illustrer les lois des conflits armés à l'intention du personnel militaire. Étant donné leur fonction pédagogique, ces simulateurs sont plus susceptibles d'intégrer le DIH que les jeux vidéo commerciaux, mais leur public est beaucoup plus restreint. C'est pourquoi cet article se concentre principalement sur les jeux vidéo commerciaux.

REVUE INTERNATIONALE de la Croix-Rouge

Figure 1: Il s'agit ici d'une photo réelle prise durant les combats à Fallouja. © Anja Niedringhaus / Keystone.

Figure 2: Dans *ArmA II*, les joueurs combattent dans des environnements réalistes. Cette scène, entre autres, ressemble fortement aux images filmées durant des opérations militaires réelles. © Bohemia Interactive

jeux vidéo de plus en plus réalistes, élaborés avec la contribution d'anciens militaires qui ont servi dans des conflits actuels[8]. Dans certains cas, la représentation des conflits armés dans les jeux vidéo est si réaliste qu'il est difficile de faire la distinction entre de réelles images de la guerre et le jeu (figures 1 et 2)[9]. Par rapport aux films, les jeux vidéo apportent une nouveauté sans précédent : les joueurs sont les participants actifs d'une simulation de guerre. Contrairement aux spectateurs passifs de médias conventionnels tels que les films, les joueurs décident eux-mêmes d'avoir ou non recours à la force. Du fait de cette évolution, 59 % des participants à un sondage du gouvernement australien ont déclaré que les jeux vidéo devraient être classifiés différemment des autres médias, précisément car le joueur est invité à participer aux actes de violence, et ne se contente plus de les regarder[10].

Dans le cadre de cette même enquête, 63 % des personnes ont répondu qu'elles pensaient que les jeux vidéo violents incitent leurs utilisateurs à commettre des violences dans la vie réelle. Bien que cette impression largement répandue soit révélatrice, les recherches menées dans ce sens ne sont pas concluantes. La documentation scientifique est divisée au sujet de l'influence des jeux vidéo sur les comportements humains, en particulier lorsque la question est posée de la façon suivante : « La pratique des jeux vidéo peut-elle induire des comportements violents ?[11] ». Bien que rien ne permette de le prouver de manière décisive, l'intérêt des médias pour ces questions est régulière-

8 Le réalisme croissant des jeux vidéo ayant pour cadre des champs de bataille modernes a attiré l'attention sur la collaboration des milieux commerciaux et militaires, qui travaillent ensemble au développement de jeux. Voir par exemple : « Documentary - Official Call of Duty Black Ops 2 », disponible sur : http://www.youtube.com/watch?feature=player_embeded&v=Gm5PZGb3OyQ.

9 Les caractéristiques d'un « jeu vidéo réaliste ayant pour cadre un conflit armé » sont floues et quelque peu subjectives. Certains jeux comprennent des armes réalistes et des environnements de combat, mais des caractéristiques irréalistes (par ex. les joueurs peuvent ressusciter).

10 Département du procureur général du gouvernement australien, *Community Attitudes To R18+ Classification Of Computer Games*, rapport, novembre 2010, disponible sur : www.ag.gov.au

11 Pour une illustration du débat scientifique voir : Anderson, *et al.*, qui affirment l'existence d'un lien causal entre les jeux violents et les comportements violents : Craig A. Anderson, Akiko Shibuya, Nobuko Ihori, Edward L. Swing, Brad J. Bushman, Akira Sakamoto, Hannah R. Rothstein et Muniba Saleem, « Violent video game effect on aggression, empathy and prosocial behaviour in eastern and western countries: a meta-analytic review », dans *Psychological Bulletin,* Vol. 136, N° 2, pp. 151-173. Pour Ferguson, le lien n'est pas avéré et il faudrait s'intéresser à d'autres facteurs (par ex. la pauvreté et la violence domestique), voir Christopher J. Ferguson, « Media violence effects: confirmed truth or just another X-file? », dans *Journal of Forensic Psychology*, Vol. 9, N° 2, avril-juin 2009, pp. 103-126. C'est également la conclusion à laquelle arrive le rapport *Summary of violent computer games and aggression – an overview of the research 2000-2011*, Conseil suédois des médias, Stockholm, 2012, disponible sur : http://www.statensmedierad.se/upload/_pdf/Summery_Violent_Computer_Games.pdf, et la décision rendue dans l'affaire *Brown, Governor of California, et al. v. Entertainment Merchants Association et al.,* demande d'ordonnance de *certiorari* adressée à la Cour d'appel des États-Unis pour le neuvième circuit, N° 08–1448, affaire débattue le 2 novembre 2010. Dans la décision rendue le 27 juin 2011 (ci-après, « affaire Brown »), la Cour suprême des États-Unis a relevé, à la majorité, que : « Les études psychologiques visant à démontrer l'existence d'un lien entre l'exposition aux jeux vidéo violents et les effets négatifs sur les enfants ne prouvent pas que cette exposition pousse les mineurs à se comporter de manière agressive. Les effets prouvés sont minimes et ne peuvent pas être différenciés des effets produits par les autres médias… » [traduction CICR]. (J. Scalia, p. 13, qui a rendu l'opinion de la Cour, à laquelle Kennedy, Ginsburg, Sotomayor et Kagan, JJ., ont adhéré. Alito a exprimé un avis convergent auquel C. J. Roberts a adhéré. J. Thomas et J. Breyer ont exprimé des opinions divergentes.)

ment stimulé par des révélations établissant que des tueurs ont utilisé des jeux vidéo pour s'entraîner[12].

Quand il s'agit de définir l'impact psychologique d'un stimulus spécifique sur un individu, les scientifiques butent contre un certain nombre d'obstacles qui les empêchent de tirer des conclusions qui s'appliquent à une population dans son ensemble. Plusieurs facteurs entraînent des différences d'une personne à l'autre, notamment le patrimoine génétique, l'environnement social et le niveau de violence dans la société d'une personne en particulier. L'accès aux armes, la pauvreté et les violences familiales constitueraient aussi des facteurs essentiels dans la décision de recourir à la violence armée. De plus, la plupart des recherches scientifiques sur les causes des comportements violents sont menées dans des pays développés où la violence est plus limitée et sévèrement punie. Comme l'accès à Internet et aux jeux vidéo n'est plus réservé aux pays privilégiés[13], des recherches scientifiques menées par exemple à Nairobi ou dans les favelas de Rio de Janeiro pourraient donner des résultats très différents des recherches actuelles, souvent conduites aux États-Unis[14]. Quoi qu'il en soit, si les chercheurs n'ont pas établi de lien de causalité entre les jeux violents et les comportements violents, ils n'ont pas non plus exclu tout lien.

Jeux vidéo, formation et acquisition de compétences

Il ne fait pratiquement aucun doute que les jeux vidéo constituent un moyen efficace de transmettre des connaissances et des compétences. Selon une récente étude francophone[15], plus de 50 % des joueurs déclaraient jouer entre une et quatre heures par jour, et plus de 90 % avaient joué à des jeux comprenant des

12 Des événements tragiques, notamment les tueries commises par des hommes armés à Columbine, Virginia Tech et Sandy Hook ont accru l'inquiétude du public. Comme le tueur norvégien Anders Breivik, plusieurs tueurs américains jouaient régulièrement à *Call of Duty*. Les observations de la police au sujet des similitudes entre le mode opératoire du tireur de Sandy Hook, Adam Lanza, et les méthodes utilisées dans un jeu vidéo auquel il jouait souvent sont particulièrement révélatrices. Voir Dave Altimari et Jon Lender, « Sandy Hook shooter Adam Lanza wore earplugs », dans *Hartford Courant*, 6 janvier 2013, disponible sur : http://articles.courant.com/2013-01-06/news/hc-sandyhook-lanza-earplugs-20130106_1_police-cars-lauren-rousseau-newtown (dernière consultation le 10 janvier 2013).

13 En 2008, quelque 31,68 millions de personnes à travers le monde jouaient en ligne, dont environ 3 millions à des jeux de tir en vue subjective. Ces chiffres ne tiennent pas compte de celles qui jouaient hors ligne, sur PlayStation ou sur téléphone portable. Au Moyen-Orient en 2010, 64 millions jouaient en ligne ou sur PlayStation. En 2012, on estimait à 211,5 millions le nombre de *gamers* aux États-Unis. Voir « Mobile gamers now represent the largest gamer segment », dans *NPD*, 5 septembre 2012, disponible sur : https://www.npd.com/wps/portal/npd/us/news/press-releases/pr_120905/. En Turquie, en 2012, quelque 21,8 millions de personnes jouaient à des jeux vidéo sur ordinateur, sur téléphone portable ou sur console. Voir « Infographic 2012 », dans *NewZoo*, 21 juin 2012, disponible sur : http://www.newzoo.com/infographics/infographic-turkey/.

14 Rien qu'aux États-Unis, plus de 200 études ont été réalisées sur la violence dans les médias. Au cours des 80 dernières années, ces études sont progressivement passées du cinéma à la télévision, pour se concentrer aujourd'hui sur les jeux vidéo.

15 Gaël Humbert-Droz, « Les jeux vidéos et le droit international », 2012. Cette enquête a été publiée sur les forums suivants : jeuxvideo.com, FantabobShow, DpStream, BF-France (battlefield France). Elle n'est plus disponible en ligne (les auteurs en possèdent une copie).

scènes réalistes de violence armée. La répétition des actions est essentielle à l'acquisition d'automatismes. Connue des chefs militaires depuis l'Antiquité, cette technique, communément appelée « *drill* », est institutionnalisée dans la formation militaire. Lorsqu'ils jouent pendant des heures, répétant régulièrement les mêmes actions et scénarios, les utilisateurs de jeux vidéo se concentrent sur l'objectif à atteindre. Les méthodes qu'ils utilisent sont simplement un moyen d'atteindre leur but. Inévitablement, les joueurs tirent des enseignements de leurs propres actions, ainsi que des images qui apparaissent sur l'écran.

Lorsqu'ils se comportent comme prévu par le scénario du jeu vidéo, les joueurs sont récompensés symboliquement par un bonus, une médaille, des améliorations apportées à leur équipement ou leur arsenal, ou par le passage au niveau supérieur. Ces récompenses, associées aux hormones produites par le cerveau, font naître un sentiment de satisfaction et de plénitude vis-à-vis des actions effectuées et des compétences acquises[16]. Bien sûr, un joueur exposé régulièrement à des scènes de torture dans un jeu, qui doit éventuellement commettre lui-même des actes de torture[17] (pour passer au niveau suivant) et qui est ensuite récompensé pour l'avoir fait, ne commettra pas nécessairement des actes de torture dans la réalité. Cependant, cette personne aura peut-être davantage tendance à considérer la torture comme un comportement acceptable. Une étude réalisée par la Croix-Rouge américaine, bien que ne mentionnant pas les jeux vidéo, fournit des indications importantes sur ce que les Américains pensent de certains actes souvent présents dans les jeux vidéo, notamment la torture[18]. Par exemple, 59 % des jeunes interrogés considéraient qu'il était acceptable de torturer des soldats ou des combattants ennemis capturés pour obtenir des renseignements militaires importants (contre 51 % des adultes). Seuls respectivement 45 % et 40 % ont répondu que cette conduite n'était acceptable en aucune circonstance.

Les forces armées sont conscientes de l'utilité des jeux vidéo et des environnements virtuels pour la formation et l'acquisition de compétences, ce qui les a amenées à collaborer avec le secteur commercial au développement de jeux. Cette collaboration entre l'industrie du jeu vidéo et les militaires n'est pas

16 Voir par exemple, Douglas A. Gentile, « Video games affect the brain – for better and worse », dans *The Dana Foundation,* 23 juillet 2009, disponible sur : http://www.dana.org/news/cerebrum/detail.aspx?id=22800.

17 On trouve par exemple, des scènes de torture dans *Call of Duty: World at War.* Voir « Call of Duty: Modern Warfare 2 », dans *Wikia*, disponible sur : http://callofduty.wikia.com/wiki/Call _of_Duty:_Modern_Warfare_2. Dans *Call of Duty: Black Ops,* le joueur doit participer à des actes de torture (son avatar doit frapper un détenu au visage, alors que des éclats de verre ont été introduits dans sa bouche). Dans *Call of Duty: Modern Warfare* 3, le supérieur du joueur torture un commandant somalien avant de lui tirer une balle dans la tête (figure 4). Bien que la présence d'actes de torture dans le scénario de ces jeux ne laisse certainement personne indifférent, leur raison d'être est peu claire.

18 Plus de deux jeunes sur cinq (41 %) pensent qu'il est parfois acceptable que l'ennemi torture des prisonniers américains capturés, contre seulement 30 % des adultes. Plus de la moitié des jeunes (56 %) et 29 % des adultes estiment qu'il est parfois acceptable de tuer des prisonniers ennemis en représailles si l'ennemi a tué des prisonniers américains. Brad A. Gutierrez, Sarah DeCristofaro et Michael Woods, « What Americans think of international humanitarian law », dans *Revue internationale de la Croix-Rouge*, Vol. 93, N° 884, décembre 2011, pp. 1009-1034.

nouvelle[19] et ces interactions à double sens prennent différentes formes. Les concepteurs de jeux de guerre commerciaux conseillent les forces armées pour que les jeux qu'elles utilisent à des fins de recrutement soient plus divertissants, tandis que des militaires en service ou à la retraite améliorent le réalisme des scénarios et des scènes des jeux commerciaux[20]. Par ailleurs, des images de conflits armés réels sont adaptées pour être utilisées tant dans les logiciels d'entraînement au combat que dans les jeux vidéo commerciaux. L'intérêt des militaires pour les jeux vidéo n'est pas difficile à comprendre. Selon une étude, le personnel militaire américain et les recrues potentielles jouent davantage aux jeux vidéo que le reste de la population[21]. Une étude de la marine américaine relative à l'efficacité des jeux éducatifs est arrivée à la conclusion que certains jeux pouvaient constituer un outil efficace pour former divers groupes de sujets à différentes tâches, dans des domaines tels que les mathématiques, les comportements, l'électronique et l'économie[22]. Des programmes de simulation sur ordinateur ont également été développés pour aider les vétérans à se réinsérer dans la société[23] et aider les victimes de traumatismes[24]. L'outil de recrutement le plus efficace de l'armée américaine constitue un autre exemple d'utilisation des jeux vidéo à des fins d'influence : un jeu vidéo multi-joueurs[25]. Dans *America's Army,* les joueurs mènent – avec d'autres internautes – des opérations militaires imaginaires, principalement dans des contextes urbains qui

19 Pour un bref historique de l'entreprise collective que forment les médias et les milieux militaires pour créer des situations de conflit virtuelles, voir : Robin Andersen et Marin Kurti, « From *America's Army* to *Call of Duty*: doing battle with the military entertainment complex », dans *Democratic Communique,* Vol. 23, N° 1, 2009, p. 45, disponible sur : http://journals.fcla.edu/demcom/article/view/76373/74027. Voir aussi Tony Fortin, « Jeux vidéo et monde militaire, un couple inséparable ? », dans *Rue89,* 22 septembre 2012, disponible sur : http://www.rue89.com/2012/09/22/jeux-video-et-monde-militaire-un-couple-inseparable-235526.

20 Par exemple, en 2002, la société Bohemia Interactive, qui a créé le jeu vidéo *ArmA II,* a conçu un système de simulation de champ de bataille pour les forces armées américaines. *Virtual Battlespace* (*VBS*) 1 et 2 sont maintenant utilisés par les forces armées, notamment le corps des marines des États-Unis (et plusieurs autres armes des forces armées américaines), les forces armées britanniques, australiennes, néo-zélandaises et canadiennes, ainsi que l'OTAN. Voir aussi, « US Army's new virtual simulation training system », dans *Defence Talk*, 30 mai 2011, disponible sur : http://www.defencetalk.com/army-virtual-simulation-training-system-34543/.

21 Des recherches menées par l'armée américaine suggèrent que 75 % du personnel masculin engagé dans l'armée américaine peut jouer à des jeux vidéo au moins une fois par semaine, contre 40 % de la population américaine dans son ensemble. B.W. Knerr, « Virtual media for military applications », Paper 21, *Current Issues in the Use of Virtual Simulations for Dismounted Soldier Training Data,* 2006. L'étude ne précise pas le type de jeu en question (par ex. jeu de tir à vue subjective ou jeu de rôle).

22 Robert T. Hayes, « The effectiveness of instructional games: a literature review and discussion », Naval Air Warfare Center Training Systems Division, Orlando, 2005, p. 6, disponible sur : http://handle.dtic.mil/100.2/ADA441935.

23 « US war woe: suicide kills more soldiers than combat », dans *RT*, 23 décembre 2011, disponible sur : http://www.rt.com/news/us-soldiers-suicide-combat-487/.

24 Voir Laurin Biron, « Virtual reality helps service members deal with PTSD », 11 juin 2012, disponible sur : http://www.defensenews.com/article/20120611/TSJ01/306110003/Virtual-Reality-Helps-Service-Members-Deal-PTSD. Voir, en général, Jane McGonigal, *Reality Is Broken: Why Games Make Us Better and How They Can Change the World,* Penguin Press, New York, 2011 (ce travail postdoctoral étudie comment utiliser le pouvoir des jeux pour résoudre des problèmes réels).

25 Les jeux multi-joueurs ont pour cadre un champ de bataille ouvert à tous. Des dizaines de personnes connectées à Internet luttent pour s'emparer du drapeau de l'ennemi ou éliminer les autres joueurs.

ressemblent aux conditions de combat en Irak et en Afghanistan. Selon des chercheurs du *Massachussetts Institute of Technology* (MIT), ce jeu en ligne gratuit serait un outil de recrutement plus efficace que toutes les autres formes de publicité de l'armée américaine réunies[26]. En plus d'être un vecteur utile pour communiquer des informations d'un intérêt évident pour les recrues potentielles (par ex. équipement, salaires ou perspectives de carrière), ce jeu permet d'inculquer des valeurs militaires[27].

Les forces armées américaines ou occidentales ne sont pas les seules à recourir aux jeux vidéo pour produire une influence. *Under Siege* (*Tahta al-Hisar*)[28], un jeu vidéo développé et produit à Damas, en Syrie, déroge au scénario traditionnel selon lequel des soldats américains combattent dans des pays musulmans. Destiné aux jeunes Arabes, *Under Siege*, dont l'action se déroule pendant la deuxième Intifada, offre une perspective moyen-orientale de ce conflit. Les joueurs jouent le rôle d'un jeune Palestinien face à l'occupation israélienne. Le jeu vidéo du Hezbollah, *Special Forces 2 – Tale of the Truthful Pledge*, qui fait suite à *Special Force* (2003), adopte une approche semblable. La seconde édition représente le conflit armé entre Israël et le Hezbollah en s'appuyant sur des phases clés du conflit armé de 2006[29].

Une autre forme d'interaction, indirecte celle-là, entre l'armée et le monde des jeux vidéo concerne la nouvelle génération d'opérateurs d'aéronefs sans pilote télécommandés (drones), qui mettent à profit des années d'expérience des jeux vidéo pour remplir leur nouvelle fonction dans les opérations de combats[30]. Cela a suscité un débat au sujet de l'effet de cette expérience sur leurs attitudes et leurs comportements. La question de savoir si les pilotes de drones ont une « mentalité Playstation » a généré un débat animé au sein des cercles militaires. Des officiers de haut rang ont exprimé leurs craintes que les jeux vidéo influent sur les perceptions relatives aux comportements acceptables en situation de guerre, notamment les perceptions des *gamers* expérimentés recrutés pour piloter à distance, loin du champ de bataille, des drones armés[31]. Cette question demande à être approfondie par des chercheurs indépendants des gouvernements et des forces armées.

Philip Alston, alors Rapporteur spécial des Nations Unies sur les exécutions extrajudiciaires, sommaires ou arbitraires, a formulé la question de la façon suivante :

26 Jeremy Hsu, « For the U.S. military, video games get serious », dans *Live Science*, 19 août 2010, disponible sur : http://www.livescience.com/10022-military-video-games.html.

27 Un exemple est la notion de héros : on trouve des biographies de « vrais héros » de l'armée américaine sur le site Internet de *America's Army* : http://manual.americasarmy.com/index.php/Real_Heroes.

28 Kim Ghattas, « Syria launches Arab war game », dans *BBC News*, 31 mai 2002, disponible sur : http://news.bbc.co.uk/2/hi/middle_east/2019677.stm.

29 Tom Perry, « Hezbollah brings Israel war to computer screen », dans *Reuters*, 16 août 2007, disponible sur : http://www.reuters.com/article/2007/08/16/us-lebanon-hezbollah-game-idUSL1662429320070816.

30 Peter W. Singer, « Meet the Sims... and shoot them », dans *Foreign Policy*, mars 2010, disponible sur : http://www.foreignpolicy.com/articles/2010/02/22/meet_the_sims_and_shoot_them.

31 Air Marshall Brian Burridge, « Post-modern warfighting with unmanned vehicle systems: esoteric chimera or essential capability? », dans *RUSI Journal*, Vol. 150, N° 5, octobre 2005, pp. 20-23.

> « Les jeunes militaires qui ont grandi en jouant aux jeux vidéo tuent aujourd'hui de vrais êtres humains à distance, à l'aide de joysticks. Loin des conséquences que produisent leurs actes sur le plan humain, comment ces nouveaux combattants pourront-ils accorder de la valeur au droit à la vie ? Comment les commandants et les responsables politiques pourront-ils eux-mêmes résister face à la nature faussement aseptisée des attaques de drones ? Tuer sera-t-il une option plus attrayante que capturer ? Quels seront les standards applicables à la collecte de renseignements pour justifier la décision de tuer ? Le nombre acceptable de morts civiles 'collatérales' augmentera-t-il ?[32] »

Les jeux vidéo et les facteurs influençant le comportement des combattants

Au sujet des jeux vidéo et de leur influence potentielle sur le comportement, il est instructif de comparer les mécanismes qui influent sur le comportement des combattants dans la vie réelle et les mécanismes présents dans les jeux vidéo. Sur la base de recherches empiriques et d'une étude de la littérature, le CICR a identifié plusieurs facteurs qui jouent un rôle crucial dans le conditionnement du comportement des combattants dans les conflits armés. Une étude a été menée en 2004[33] dans le but d'identifier les causes des violations du DIH. Elle se concentrait principalement sur des facteurs psychosociologiques universellement présents dans tout groupe de combattants armés participant à une guerre, tels que l'influence du groupe, l'insertion dans une structure hiérarchique et le désengagement moral[34]. Il est intéressant (ou inquiétant) de relever que la plupart de ces facteurs sont aussi présents dans les jeux vidéo. Concernant le comportement des combattants, l'étude a révélé que :

> « Les combattants sont soumis à des phénomènes de comportement de groupe qui entraînent la dépersonnalisation, la perte de l'indépendance et un fort conformisme. Cette réalité est favorable au processus de dilution de la responsabilité individuelle du combattant dans la responsabilité collective de son unité de combat. … Les combattants sont également soumis à un processus de déplacement de leur responsabilité individuelle vers la responsabilité de leurs supérieurs hiérarchiques. Les violations du DIH peuvent découler des ordres donnés par cette autorité, mais elles semblent le plus souvent liées à l'absence d'ordres explicites de ne pas violer le droit ou à l'autorisation implicite d'adopter des comportements répréhensibles. …

32 Philip Alston et Hina Shamsi, « A killer above the law », dans *The Guardian*, 2 août 2010, disponible sur : http://www.guardian.co.uk/commentisfree/2010/feb/08/afghanistan-drones-defence-killing [traduction CICR].

33 Daniel Muñoz-Rojas et Jean-Jacques Frésard, « Origines du comportement dans la guerre : comprendre et prévenir les violations du DIH », dans *Revue internationale de la Croix-Rouge*, Vol. 86, N° 853, mars 2004, pp. 169-188 (ci-après « l'étude »).

34 « Le désengagement moral est un processus complexe, et les actes malveillants sont toujours le produit d'interactions entre des influences personnelles, sociales et environnementales », *ibid*., p. 177. « Non seulement le désengagement moral est graduel, mais il détermine aussi des comportements qui puisent dans les actions passées la force nécessaire pour justifier les actions futures. », *ibid*, p. 180.

> Les combattants qui ont participé aux hostilités et ont été soumis à des situations traumatiques et de violence … sont, à court terme, amenés à perpétrer, eux aussi, des violations du DIH. … Le fossé observé entre reconnaissance et application des normes est le résultat d'une série de mécanismes conduisant au désengagement moral du combattant et à la perpétration de violations du DIH. Le désengagement moral des combattants se fait principalement en ayant recours 1) aux justifications des violations[35] et 2) à la déshumanisation de l'ennemi »[36].

Plusieurs parallèles peuvent être établis entre les conclusions de cette étude et les jeux vidéo qui ont pour cadre des champs de bataille actuels. Sur les cinq causes de violations recensées dans l'étude, au moins quatre se retrouvent dans les jeux vidéo, à savoir le caractère criminogène qui fait partie de la nature de la guerre, la définition des buts de guerre, les raisons d'opportunité et les raisons psychosociologiques. Évidemment, les raisons liées à la personnalité des individus (la cinquième cause recensée des violations) ne peuvent pas être généralisées ici.

L'étude a identifié le « caractère criminogène »[37] comme une partie de la nature de la guerre. Dans les jeux vidéo, il découle de l'idée que les champs de bataille sont des lieux d'où les civils ou les combattants hors de combat sont absents. Par conséquent, les joueurs ont l'impression que l'ensemble du champ de bataille est un champ de tir à ciel ouvert, où aucune précaution n'est nécessaire. De l'avis des auteurs, en décidant de supprimer tout civil de leurs produits, les développeurs de jeux vidéo favorisent la même impression : tout être vivant est un ennemi et le tuer est la seule option ; il n'y a aucune limite à l'usage de la force. Cette impression est renforcée par l'exemple que donnent parfois d'autres personnages des jeux vidéo. Par exemple, lorsqu'un chef d'escouade dans un jeu commet des actes de torture ou des exécutions extrajudiciaires, les joueurs y voient le signe que ce type de comportement est implicitement autorisé[38].

35 Les combattants ont recours à différentes justifications, notamment en se considérant non comme des bourreaux, mais comme des victimes, en soutenant qu'au vu des circonstances, certains actes répréhensibles sont admissibles, voire nécessaires, en invoquant les violations commises par l'ennemi et en attribuant le blâme aux victimes elles-mêmes, ou en niant, en minimisant ou en ignorant les conséquences de leurs actes en ayant recours à des euphémismes pour désigner leurs opérations et les conséquences de ces opérations, *ibid.*, pp. 178-180.

36 *Ibid.*, pp. 174-177. « On nie l'humanité de l'autre en lui attribuant des traits de caractère, des intentions … méprisables », parfois en l'assimilant à des insectes nuisibles ou à des virus qu'il faut éradiquer. « … [N]on seulement le combattant aura moins de peine à s'en prendre à lui, mais il pourra même rationaliser ses comportements les plus extrêmes et se convaincre qu'ils sont justifiés et nécessaires », *ibid.*, pp. 179-180.

37 *Ibid.*, p. 169.

38 « Les hommes ordinaires se soumettent de leur plein gré à une autorité lorsqu'ils l'estiment légitime, et ils se considèrent alors comme les agents de cette autorité. … Ce principe … est encore renforcé lorsque l'on parle de combattants insérés dans une hiérarchie militaire, généralement plus contraignante qu'une autorité civile. … Bien que, dans ces conditions, un individu commette des actes qui semblent contraires à sa conscience, on aurait tort d'en conclure que son sens moral a disparu : la vérité est qu'il a radicalement changé d'objectif. L'intéressé ne porte plus de jugement de valeur sur ses actions. Ce qui le préoccupe désormais, c'est de se montrer digne de ce que l'autorité attend de lui. », *ibid.*, pp. 174-175.

La « définition des buts de guerre » (ou « objectifs de campagne ») des jeux vidéo tend à justifier les résultats, quelles que soient les méthodes utilisées. Comme dans un conflit armé réel, les ennemis sont généralement diabolisés et déshumanisés, ce qui justifie leur meurtre. Le non-respect du droit par l'ennemi est également présenté comme une justification autorisant les joueurs à utiliser toutes les méthodes de guerre à leur disposition pour remplir leur mission.

Dans les conflits armés réels, de nombreux combattants violent les règles simplement parce que la guerre est l'expérience ultime et qu'ils ont la possibilité de le faire. Ces raisons d'opportunité se reflètent dans le plaisir de transgresser les règles, qui se trouve au cœur de nombreux types de jeux vidéo, et notamment nombre de ceux qui ont pour cadre des champs de bataille contemporains. Comme l'ont relevé certains développeurs de jeux vidéo, les joueurs ont tendance à abattre des civils simplement parce qu'ils en ont la possibilité. Pour les combattants comme pour les joueurs, le sentiment d'opportunité est renforcé par un sentiment d'impunité. Dans la plupart des jeux vidéo, les violations ne sont pas suivies de sanctions.

Enfin, comme dans les conflits armés réels, les raisons psychosociologiques telles que l'obéissance à l'autorité, l'influence du groupe et le désengagement moral sont toutes illustrées dans la liberté de décision restreinte dont dispose le joueur. Par exemple, dans un passage de *Call of Duty: Black Ops,* le joueur doit regarder son propre personnage introduire des éclats de verre dans la bouche d'un ennemi capturé et doit ensuite frapper le détenu au visage par le biais de l'ordinateur ou de la console. Sans autre alternative que d'obéir ou de quitter le jeu, le joueur doit justifier comme il le peut cet acte de torture afin de se distancer des faits et de poursuivre sa vie. Ce mécanisme n'est que trop connu de nombreux combattants participant à des conflits armés réels.

Applicabilité du DIH et du droit international des droits de l'homme aux jeux vidéo

Une multitude de normes juridiques s'appliquent aux jeux vidéo. Avant de s'intéresser au DIH, il est important de relever que les joueurs, les concepteurs de jeux et les distributeurs peuvent invoquer tout un éventail de protections applicables à leurs activités respectives, garanties par le droit international des droits de l'homme. Ces protections vont de la liberté d'expression[39] au droit à la

39 Selon l'article 19 du Pacte international relatif aux droits civils et politiques, entré en vigueur le 23 mars 1976 (adopté le 16 décembre 1966), « toute personne a droit à la liberté d'expression ; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix ». D'autres instruments internationaux et régionaux contiennent des dispositions semblables, notamment : l'article 19 de la Déclaration universelle des droits de l'homme, l'article 10 de la Convention européenne des droits de l'homme, l'article 9 de la Charte africaine des droits de l'homme et des peuples et l'article 13 de la Convention américaine relative aux droits de l'homme.

propriété[40], au droit à l'intimité et à la vie de famille[41] et au droit de jouer[42]. La liberté d'expression, par exemple, a été invoquée avec succès à de nombreuses reprises devant les tribunaux américains pour faire valoir la légalité des jeux vidéo qui contiennent des scènes violentes, notamment la torture et l'exécution sommaire de captifs[43]. Cependant, ce droit a des limites[44], que les législateurs de divers pays ont utilisées pour interdire des jeux qui contiennent des violences physiques extrêmes, des violences sexuelles ou d'autres types de contenus jugés offensants. Le fait que des dispositions spécifiques du droit international des droits de l'homme[45], du droit d'auteur et de la propriété intellectuelle[46] et du

40 Le droit à la propriété figure à l'article 17 de la Déclaration universelle des droits de l'homme ; à l'article 1 du Protocole I de la Convention européenne des droits de l'homme ; à l'article 21 de la Convention américaine relative aux droits de l'homme ; et le plus explicitement à l'article 14 de la Charte africaine des droits de l'homme et des peuples.

41 L'article 17 du Pacte international relatif aux droits civils et politiques garantit le droit à la protection contre toute immixtion arbitraire de l'État concernant l'utilisation d'ordinateurs et d'Internet dans un cadre privé.

42 Les articles 1 et 31 de la Convention relative aux droits de l'enfant, entrée en vigueur le 2 septembre 1990 (adoptée le 20 novembre 1989).

43 Par exemple, les tentatives de persuader les tribunaux américains d'interdire ou d'imposer des restrictions aux jeux qui comportent des scènes violentes aboutissent rarement. Le facteur décisif est généralement de savoir si la liberté d'expression s'applique ou non aux jeux. Voir : *American Amusement Machine Association v. Kendrick*, CA7 2001, 244. F. 3d 572, 577 (les jeux vidéo sont protégés sur la base de la liberté d'expression : aucune raison impérieuse n'a été présentée pour la restriction demandée) ; *Benoit v. Nintendo of America, Inc.*, 2001, Cour de district des États-Unis pour le district de la Louisiane (même si la mort d'un enfant au cours d'une crise d'épilepsie a été provoquée par une exposition à la violence dans *Mortal Kombat*, les dialogues du jeu vidéo étaient protégés à moins de constituer une incitation à la violence, ce qui n'était pas le cas) ; *Video Software Dealers Association v. Schwarzenegger*, en 2009, la Cour d'appel des États-Unis pour le neuvième circuit a confirmé le verdict de 2005 de la Cour de district (la législation restreignant la vente de jeux vidéo violents aux mineurs était anticonstitutionnelle. Pour l'appel devant la Cour suprême, voir affaire *affaire Brown, op. cit.*, note 11) ; *Entertainment Software Association v. Granholm* 2005, Cour de district pour le district est du Michigan (jeu violent protégé en vertu de la liberté d'expression, preuves de dommages insuffisantes) ; et *Entertainment Software Association; Entertainment Merchants Association v. Minnesota*, 2008, Cour d'appel des États-Unis pour le huitième circuit (injonction accordée contre la loi interdisant la vente ou la location de jeux vidéo violents aux mineurs : la liberté d'expression et l'absence de preuve de dommages ont été décisives).

44 La liberté d'expression peut être soumise à des restrictions en vertu du droit national afin de protéger les droits et la réputation d'autrui, la sécurité nationale, l'ordre public, la santé publique ou la morale. Voir l'article 19(3), du Pacte international relatif aux droits civils et politiques.

45 En plus des traités mentionnés ci-dessus, les autres instruments applicables aux jeux vidéo incluent : la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants, entrée en vigueur le 26 juin 1987 (adoptée le 10 décembre 1984), le Protocole facultatif à la Convention relative aux droits de l'enfant concernant l'implication d'enfants dans les conflits armés, entrée en vigueur le 12 février 2002 (adoptée le 25 mai 2000. L'inclusion de ce protocole parmi les instruments de DIH ou de droit international des droits de l'homme est controversée) ; et la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes, entrée en vigueur le 3 septembre 1981 (adoptée le 18 décembre 1979).

46 À l'exception des jeux que leurs créateurs mettent gratuitement à disposition, les logiciels de jeux vidéo sont généralement protégés par des droits d'auteur, des traités internationaux sur le droit d'auteur ou d'autres sujets, et le droit de la propriété intellectuelle. Les accords internationaux sur le droit d'auteur comprennent : la Convention de Berne pour la protection des œuvres littéraires et artistiques de 1886 ; la Convention universelle sur le droit d'auteur de 1952 ; le Traité de l'OMPI sur le droit d'auteur de 1996 ; et l'Accord de l'Organisation mondiale du commerce sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) de 1994.

droit national soient les principales sources de droit applicables à la conception, à la vente et à l'utilisation de jeux vidéo[47] ne prête pas à controverse et n'est pas l'objet du présent article. Un point plus pertinent pour le sujet traité ici est la question de l'applicabilité, aux champs de bataille virtuels créés par l'industrie du « *militainment* », des règles relatives à l'usage de la force et au traitement des personnes aux mains de l'ennemi contenues dans le DIH et le droit international des droits de l'homme.

Il va sans dire que les jeux vidéo appartiennent au domaine de l'imaginaire. Ils n'impliquent pas une participation à un conflit armé réel. C'est également le cas des technologies de simulation de combat utilisées à des fins d'entraînement militaire. Néanmoins, deux questions demandent réponses. Premièrement, les règles du DIH et du droit international des droits de l'homme s'appliquent-elles aux situations décrites dans les jeux vidéo ? Et, deuxièmement, les États ont-ils une obligation particulière de garantir que le contenu des jeux vidéo soit conforme aux règles relatives à l'usage de la force et au traitement des personnes tombées aux mains de l'ennemi ?

Toute opération sur un champ de bataille est menée dans un cadre juridique structuré par le droit international (DIH et droit des droits de l'homme) et la législation nationale. Bien que les jeux vidéo ne soient que virtuels, nous arguons ici que, par souci de réalisme, les règles de DIH et des droits de l'homme relatives à l'usage de la force devraient être appliquées aux scènes des jeux vidéo qui se déroulent sur des champs de bataille réalistes (de la même manière que les lois de la physique y sont appliquées). D'ailleurs, les jeux vidéo ne sont pas le seul contexte où ce cadre juridique peut influencer une situation, même hors du cadre d'un conflit armé. Un autre exemple important est la formation et la planification militaires. À chaque fois que les commandants militaires forment leur personnel, ou planifient des opérations avec leurs états-majors, ils doivent tenir compte du droit applicable. Il n'est certainement pas attendu d'eux d'attendre que l'opération soit en cours pour tenir compte de la loi.

L'applicabilité du DIH ou des droits de l'homme (ou des deux) à la situation représentée dans un jeu vidéo, dépend de la qualification du scénario comme conflit armé, ou non. Chaque jeu doit être examiné séparément. Comme le DIH ne s'applique que durant les conflits armés, il n'est pas pertinent si la situation présentée dans un jeu correspond à des tensions internes, telles que des émeutes ou des manifestations, n'atteignant pas le seuil d'intensité requis pour un conflit armé. Dans ces situations, le régime pour l'application des lois[48], qui relève du droit inter-

47 Le droit national peut s'appliquer à diverses activités associées aux jeux vidéo. La législation nationale relative au droit d'auteur, à la propriété et à la vie privée, ainsi que le droit pénal (par ex. les infractions liées à l'incitation à la haine raciale, à la fourniture de soutien à une organisation terroriste, etc.) peuvent régir la création, la distribution et l'utilisation des jeux vidéo. Pour les infractions « conseillées » par le biais d'un jeu vidéo, voir *R. c. Hamilton,* Cour suprême du Canada, 29 juillet 2005, 2 R.C.S. 432, 2005 CSC 47.

48 Le régime d'application de la loi (droit international des droits de l'homme) est l'ensemble des règles qui régissent l'usage de la force par les autorités de l'État pour maintenir ou rétablir la sécurité, la loi et l'ordre publics.

national des droits de l'homme, établit les règles applicables à l'usage de la force, aux armes à feu, aux arrestations, à la détention, aux fouilles et aux saisies durant les opérations de police[49]. Par exemple, le droit international des droits de l'homme prévoit que les armes à feu ne peuvent pas être utilisées contre une personne, à moins que celle-ci ne représente une menace imminente pour la vie et qu'il n'y ait pas d'alternative[50]. Lorsque la situation décrite atteint l'intensité d'un conflit armé, le DIH et le droit international des droits de l'homme s'appliquent tous les deux. Le DIH contient les règles que les combattants doivent suivre lorsqu'ils planifient et mènent des opérations militaires (par ex. règles ou principes de distinction, de proportionnalité et de précaution). Le régime s'appliquant à la conduite des hostilités, qui relève du DIH[51], permet de tuer des cibles légitimes[52]. Lorsque le scénario d'un jeu vidéo ne permet pas de déterminer clairement si la situation atteint l'intensité d'un conflit armé[53] – et donc si le DIH s'applique – le droit international des droits de l'homme reste applicable, notamment le régime d'application des lois

49 Ces règles figurent dans des traités (par ex. Pacte international relatif aux droits civils et politiques ; Convention internationale sur l'élimination de toutes les formes de discrimination raciale ; Convention relative aux droits de l'enfant) et des instruments non contraignants (par ex. Ensemble de règles minima pour le traitement des détenus ; Code de conduite pour les responsables de l'application des lois ; Déclaration des principes fondamentaux de justice relatifs aux victimes de la criminalité et aux victimes d'abus de pouvoir ; Ensemble de principes pour la protection de toutes les personnes soumises à une forme quelconque de détention ou d'emprisonnement ; Principes fondamentaux relatifs au traitement des détenus ; Principes de base sur le recours à la force et l'utilisation des armes à feu par les responsables de l'application des lois ; Déclaration sur l'élimination de la violence à l'égard des femmes).

50 Principes de base sur le recours à la force et l'utilisation des armes à feu par les responsables de l'application des lois, adoptés par le huitième Congrès des Nations Unies pour la prévention du crime et la justice pénale, La Havane, Cuba, du 27 août au 7 septembre 1990, en particulier les dispositions 5, 9 et 10.

51 Frida Castillo relève que « pour déterminer quel DIH s'applique dans une situation donnée, il est nécessaire de vérifier quels instruments ont été ratifiés par l'État en question. Alors que les Conventions de Genève de 1949 ont été universellement ratifiées, ce n'est pas le cas d'autres traités de DIH, notamment le Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés non internationaux du 8 juin 1977 (PA II). Là aussi, il est donc nécessaire de vérifier si les États parties au conflit ont ratifié les instruments applicables. Les règles considérées comme coutumières, par contre, s'appliquent à tous les États. » [traduction CICR]. Rapport de Frida Castillo, *Playing by the Rules: Applying International Humanitarian Law to Video and Computer Games,* TRIAL, Pro Juventute, Genève, octobre 2009, p. 3, note de bas de page 1.

52 Les combattants et les civils qui participent directement aux hostilités, pendant la durée de cette participation. Voir PA I, articles 48 et 51(3), ainsi que les règles 1 et 6 de l'Étude du CICR sur le droit international humanitaire coutumier. CICR, *Droit international humanitaire coutumier, Vol. I : Règles*, Jean-Marie Henckaerts et Louise Doswald-Beck (dir.), Bruylant, Bruxelles, 2006 (ci-après, « Étude du CICR sur le droit coutumier »).

53 Alors que tout recours à la force armée entre deux États constitue un conflit armé international, pour que le degré d'intensité d'un conflit armé non international soit atteint, il faut un « conflit armé prolongé » atteignant un certain niveau d'intensité et où les parties sont organisées. Concernant le critère d'intensité, les facteurs pertinents mentionnés dans la jurisprudence incluent : le nombre, la durée et l'intensité des différents affrontements ; le type d'armes utilisées ; le nombre de victimes ; l'étendue des destructions. Voir entre autres : Tribunal pénal international pour l'ex-Yougoslavie (TPIY), *Le Procureur c. Ramush Haradinaj, Idriz Balaj, Lahi Brahimaj*, Affaire n° IT-04-84-T, Jugement (Chambre de première instance I), 3 avril 2008, para. 49. Les facteurs indicatifs en matière d'organisation incluent : l'existence d'une structure de commandement, de règles de discipline et d'un quartier général ; le fait que le groupe contrôle un territoire délimité ; la capacité de planifier, de coordonner et de mener des opérations militaires. Voir entre autres, TPIY, *ibid*., para. 60.

mentionné ci-dessus ainsi que l'interdiction, en particulier, de la torture, de la privation arbitraire de la vie et des traitements cruels et dégradants[54].

Pour répondre à la seconde question, à savoir si les États ont l'obligation de garantir que le contenu des jeux vidéo soit conforme aux règles régissant l'usage de la force, prenons l'exemple théorique suivant : un jeu vidéo permet aux joueurs de commettre des actes de torture et d'autres infractions graves ou des violations sérieuses du DIH dans un conflit armé virtuel. Les joueurs ne sont pas informés que ces actes sont interdits. Parfois, ils sont même récompensés pour avoir adopté ce type de comportement dans le jeu. À des fins de simplicité, laissons de côté les dispositions de la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants. Le jeu engage-t-il l'obligation des États, découlant des traités de DIH, de respecter et de faire respecter le DIH[55], et d'en diffuser les règles[56] aussi largement que possible[57] ? Il ne fait aucun doute que les États doivent, au moins, veiller à ce que leurs outils de formation militaire (y compris les jeux vidéo utilisés, soit pour le recrutement, soit pour la formation) ni ne permettent, ni n'encouragent les comportements illicites sans sanctions appropriées. Dans le meilleur des cas, pour honorer leurs obligations, les États devraient pleinement intégrer dans les outils de formation militaire, les règles applicables à l'usage de la force. Autrement dit, ces outils devraient permettre au personnel militaire de respecter le droit et de se former au respect du droit[58]. Les obligations imposées aux États de « respecter et faire respecter »

54 Le DIH et le droit international des droits de l'homme contiennent des interdictions communes qui doivent être respectées en tout temps durant un conflit armé, notamment les interdictions relatives à la discrimination, aux exécutions sommaires, aux viols, à la torture et aux traitements cruels et dégradants. Ces deux régimes juridiques incluent en outre des dispositions relatives à la protection des femmes et des enfants ; établissent des droits fondamentaux pour les personnes soumises à un processus de justice pénale ; et régissent des aspects du droit à la nourriture et à la santé.

55 Article 1 commun aux quatre Conventions de Genève de 1949 ; Convention pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne, Genève, le 12 août 1949 (ci-après, CG I) ; Convention pour l'amélioration du sort des blessés, des malades et des naufragés des forces armées sur mer, Genève, le 12 août 1949 (ci-après, CG II) ; Convention relative au traitement des prisonniers de guerre, Genève, le 12 août 1949 (ci-après, CG III) ; Convention relative à la protection des personnes civiles en temps de guerre, Genève, le 12 août 1949 (ci-après, CG IV). Voir aussi la règle 139 de l'Étude du CICR sur le droit coutumier, qui établit que « [c]haque partie au conflit doit respecter et faire respecter le droit international humanitaire par ses forces armées ainsi que par les autres personnes ou groupes agissant en fait sur ses instructions ou ses directives ou sous son contrôle ».

56 CG I art. 47, CG II art. 48, CG III art. 127 et CG IV art. 144 énoncent tous : « Les Hautes parties contractantes s'engagent à diffuser le plus largement possible, en temps de paix et en temps de guerre, le texte de la présente Convention dans leurs pays respectifs, et notamment [si possible] à en incorporer l'étude dans les programmes d'instruction … civile, de telle manière que les principes en soient connus de l'ensemble de la population ». Voir aussi CG III art. 39 et 41, CG IV art. 99, PA I art. 83, PA II art. 19.

57 Au sujet de l'obligation de diffusion continue, voir Claude Pilloud, Yves Sandoz et Bruno Zimmermann (dir.), *Commentaire du Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977*, CICR, 1987 (commentaire de l'article 80), para. 3290.

58 Le nombre de mots limité de cet article ne nous permet pas de procéder à une étude détaillée de la pratique des États quant à la portée de ces obligations dans le contexte des outils de formation et des conséquences du non-respect de ces obligations. Il serait utile de mener une recherche approfondie sur ces points importants.

le DIH et de le diffuser aussi largement que possible, et d'honorer leurs obligations découlant des traités[59] sont très générales et s'appliquent en tout temps[60]. Même si ces règles devraient, logiquement, s'appliquer aux jeux vidéo commerciaux vendus ou distribués sur le territoire souverain des États, la pratique des États ne va pas dans ce sens.

En conclusion, il est important de relever que les questions visant à déterminer si les États ont l'obligation de veiller à ce que les règles relatives à l'usage de la force, ainsi qu'au traitement des personnes tombées aux mains de l'ennemi, soient bien intégrées dans les jeux vidéo ne sont pas purement théoriques. Les scènes de violations du droit ne sont pas rares dans les jeux vidéo. Une étude suisse de 2009 consacrée aux jeux vidéo populaires[61] a recensé les violations du DIH les plus fréquentes. Elles comprenaient des violations des principes de distinction et de proportionnalité ; la destruction massive de biens de caractère civil et/ou des blessures ou la mort de civils sans nécessité militaire ; et des attaques intentionnellement dirigées contre des civils ou des biens de caractère civil, y compris des bâtiments religieux[62]. Cette étude a révélé que, le plus souvent, les traitements cruels, inhumains ou dégradants et les actes de torture dans les jeux vidéo étaient infligés dans le cadre d'interrogatoires[63].

Cette même étude a montré que les attaques directes contre des civils ne participant pas directement aux hostilités étaient courantes[64]. Les victimes – le plus souvent des otages ou des civils présents dans un village – n'étaient pas de simples victimes collatérales : elles étaient directement visées. Dans un seul jeu ce comportement était sanctionné[65]. En fait, le non-respect du principe de distinction était présent dans différents jeux, qui contenaient par exemple l'utilisation de munitions, notamment d'obus de chars et d'armes à sous-munitions[66], qui frappent sans discrimination[67] lorsqu'elles sont utilisées dans des zones densément peuplées. Dans le jeu *Medal of Honour Airborne*, des armes qui ne

59 Ces dispositions sont fondées sur la règle coutumière *pacta sunt servanda*, telle qu'elle figure à l'article 26 de la *Convention de Vienne sur le droit des traités*, conclue à Vienne le 23 mai 1969, Recueil des traités vol. 1155, p. 331.

60 Selon le commentaire de l'article 1 de la CG I, p. 27, « s'il veut tenir son engagement solennel, [l'État] doit nécessairement préparer d'avance, c'est-à-dire dès le temps de paix, les moyens juridiques, matériels ou autres permettant, le moment venu, d'assurer une application loyale ». Voir aussi : Commentaire du PA I, p. 41 ; Commentaire de la CG IV, p. 21 ; Commentaire de la CG III, p. 24 ; Commentaire de la CG II, p. 25. Selon l'article 1(1) du PA I, ce respect est requis « en toutes circonstances ».

61 F. Castillo, *op. cit.*, note 51.

62 Dans un seul jeu, *Call of Duty 4 (Modern Warfare),* l'attaque d'une église a mis un terme à la mission (échec). L'attaque de mosquées n'a jamais ce type de conséquence. *Ibid*., p. 24.

63 Dans de nombreux cas, l'interrogatoire se termine par une exécution extrajudiciaire. *Ibid*., p. 42.

64 *Ibid*., p. 42.

65 *Tom Clancy Rainbow 6 Vegas.* Voir *ibid.,* p. 37.

66 Par exemple, *World in Conflict* et *Frontlines: Fuel of War.* Voir *ibid.*, pp. 30-31. La Convention sur les armes à sous-munitions de mai 2008 (ouverte à la signature depuis le 3 décembre 2008) interdit aux États parties d'utiliser des armes à sous-munitions. Par ailleurs, leur utilisation dans des situations où des civils et des combattants seraient frappés sans discrimination est toujours interdite.

67 Pour le droit applicable, voir la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination (entrée en vigueur le 2 décembre 1983), Recueil des traités vol. 1342, p. 137.

permettent pas de faire la distinction entre combattants et civils au sol sont utilisées lors d'opérations aériennes en zone urbaine[68]. Plusieurs jeux permettaient aussi aux joueurs d'abattre des soldats blessés hors de combat ou de regarder d'autres le faire[69]. Souvent, les conséquences que subissent les joueurs qui prennent des civils pour cibles ou adoptent d'autres comportements qui constitueraient des infractions dans un conflit armé réel sont incohérentes[70].

Les auteurs du présent article ont recensé, dans les jeux vidéo, divers autres exemples de comportements qui constitueraient des violations dans un conflit armé réel, notamment les tirs dirigés contre des unités médicales portant l'emblème protecteur de la croix rouge, du croissant rouge ou du cristal rouge et l'usage abusif de cet emblème ; la destruction de biens de caractère civil qui semble disproportionnée ; l'utilisation de mines antipersonnel ; le fait de s'emparer des plaques d'identité des combattants ennemis décédés ; l'utilisation d'armes lourdes dans des zones densément peuplées sans égard pour les règles relatives aux précautions à prendre en cas d'attaque ; et les attaques dirigées contre des biens de caractère civil qui peuvent entraîner la mort d'innombrables civils invisibles[71]. Ces deux derniers problèmes sont illustrés dans le jeu vidéo *Battlefield 3*. Dans une scène, un étage complet d'un hôtel de plusieurs étages est détruit pour tuer un seul sniper.

Défis pour les normes humanitaires

Le simple fait de jouer à un jeu vidéo ne signifie pas que le joueur va commettre des violations du DIH ou du droit international des droits de l'homme. Au risque d'énoncer une évidence, un joueur ne commet pas un acte criminel en pressant un bouton pour permettre à un personnage de jeu vidéo de procéder à des actes de torture ou à une exécution sommaire : les jeux vidéo sont imaginaires. De plus, il n'est ni nécessaire, ni possible d'engager des poursuites contre les joueurs dans ces circonstances. Les conflits armés sont, par définition, des environnements violents où les participants ou les combattants peuvent avoir recours à un certain degré de force pour obliger l'ennemi à se rendre. La représentation des violences dans les jeux vidéo n'est donc pas, en soi, le problème. Cependant, à notre sens, les jeux vidéo posent deux grands défis aux normes humanitaires. Le premier est leur tendance à banaliser les violations du droit. Le second, non moins important, est l'effet nuisible qu'ils risquent de produire sur la perception qu'ont les joueurs (qui incluent des combattants actuels et potentiels, des faiseurs d'opinion, des législateurs, des décideurs et le grand public) du cadre normatif.

68 F. Castillo, *op. cit.*, note 51, pp. 34 et 42.

69 *Ibid.*, pp.15-16 et 42. Les jeux concernés incluent : *Call of Duty 5 (World at War), Call of Duty: Modern Warfare 3, ArmA II, Call of Duty: Modern Warfare 2, Call of Duty: Black Ops*. Voir aussi : *24 heures chrono – le jeu*.

70 Par exemple, dans les jeux *Call of Duty*, la torture de prisonniers n'entraîne aucune sanction, alors que dans d'autres, tirer sur des civils provoque la fin de la partie.

71 Par exemple les jeux *Call of Duty* se déroulant à Paris et Téhéran.

Messages transmis par les jeux vidéo et défis humanitaires

Dans ce débat, il est tout d'abord nécessaire d'étudier de plus près les messages que transmettent les jeux vidéo, afin de mieux comprendre leur effet potentiellement nuisible sur la perception et le respect des règles fondamentales du DIH – en particulier celles qui régissent l'usage de la force et l'obligation d'épargner les civils et les combattants hors de combat. Cette section présente plusieurs messages transmis par les jeux vidéo, ainsi que les efforts constructifs déployés par l'industrie du jeu vidéo pour résoudre le problème de perception.

Plusieurs messages transmis par les jeux vidéo sont particulièrement inquiétants, précisément car ils reflètent et renforcent certaines idées qui constituent un défi direct au DIH. Les principaux exemples incluent notamment : la guerre est une zone de non-droit ; la fin justifie les moyens ; les moyens et les méthodes de guerre sont illimités ; tout être vivant sur un champ de bataille doit être abattu sans distinction ; les plaques d'identité sont des trophées ; et le personnel et les infrastructures sanitaires peuvent être attaqués.

La guerre est une zone de non-droit

Dans de nombreux jeux vidéo, il est normal d'infliger des blessures ou de causer la mort, et il s'agit souvent de la seule option possible. L'impunité est la norme et le droit applicable à la situation représentée dans le jeu est rarement, voire jamais, reconnu ou appliqué, ce qui provoque notamment une absence d'humanité. Dans les conflits armés contemporains, la difficulté de faire respecter les valeurs humanitaires n'est pas due à une absence de règles, mais au non-respect desdites règles. Améliorer le respect, la mise en œuvre et l'application du DIH est l'éternel défi de la communauté internationale et une priorité constante du CICR. Cette responsabilité incombe aux parties à un conflit, étatiques ou non, mais requiert aussi des actions de la part des États en temps de paix. De plus, des sanctions de nature disciplinaire ou pénale doivent être adoptées[72].

La fin justifie les moyens

Dans certains jeux vidéo, les joueurs doivent assister ou participer à des scènes réalistes de torture et/ou de meurtre de prisonniers ennemis pour pouvoir progresser[73]. Dans la réalité, ce type de comportement est strictement interdit en tout

72 CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* XXX[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge, octobre 2007, CICR, pp. 35-36, disponible sur : http://www.bibliomines.org/fileadmin/tx_bibliodocs/30IC_8-4_IHLchallenges_Report_Annexes_FRA_FINAL.pdf.

73 Dans *Call of Duty: Black Ops*, les joueurs regardent un de leurs supérieurs exécuter froidement des prisonniers de guerre. Contraints de s'agenouiller et de supplier le bourreau de les épargner, tous les prisonniers reçoivent une balle dans la tête, sauf le dernier, qui est exécuté à l'aide d'un couteau. Dans une autre scène de *Call of Duty: Black Ops,* le joueur doit participer à un acte de torture (son personnage doit frapper au visage un détenu après que des éclats de verre ont été introduits dans sa bouche).

temps, en vertu à la fois du droit international des droits de l'homme[74] et du DIH[75]. Dans de nombreux jeux vidéo, les combattants ennemis sont représentés comme des bandits perfides qui violent les règles les premiers. Ils sont souvent qualifiés de « terroristes » qui méritent un traitement brutal, notamment des exécutions sommaires ou des tortures. Un défi récent au DIH a été la tendance des États à qualifier de « terroriste »[76] tout acte de guerre commis à leur encontre par des groupes armés, en particulier dans les conflits armés non internationaux. Cela a provoqué une confusion entre les actes de guerre licites, notamment commis par des insurgés contre des cibles militaires dans leur pays, et les actes de terrorisme[77].

Les moyens et les méthodes de guerre sont illimités

Dans de nombreux jeux vidéo, les armes à la disposition des joueurs comprennent des engins explosifs activés par la présence ou la proximité de l'ennemi, ou en cas de contact. Sur un champ de bataille et en termes juridiques, ces engins seraient considérés comme des mines antipersonnel[78]. De nos jours, quelque 160 pays se sont engagés à éliminer ces armes de leur arsenal militaire. Depuis l'adoption de la Convention d'Ottawa il y a 15 ans, des progrès sensibles ont été accomplis face au problème humanitaire posé par ces mines, qui continuent de tuer et de blesser longtemps après la fin des conflits. Cependant, il reste de grands défis, en particulier en termes de déminage et d'atténuation des souffrances de centaines de milliers de blessés et de leurs familles. En 2009, à la deuxième Conférence d'examen de la Convention d'Ottawa, les États ont adopté un plan d'action qui contient des engagements fermes à améliorer les activités dans les domaines de l'assistance aux victimes, de la destruction des stocks et du déminage[79].

74 Article 7 du Pacte international relatif aux droits civils et politiques, article 3 de la Convention européenne des droits de l'homme, article 2 de la Convention contre la torture.

75 L'article 3 commun aux quatre Conventions de Genève de 1949 interdit les actes de torture ou les traitements cruels, inhumains, dégradants ou humiliants. Voir aussi les articles 50, 51, 130 et 147, respectivement, des quatre Conventions de Genève ; PA I art. 75, PA II art. 4, et la règle 90 de l'Étude du CICR sur le droit international coutumier.

76 Il n'existe pas de définition universellement adoptée du « terrorisme ». Voir PA II, art. 4(2)(d). De plus, les deux Protocoles additionnels aux Conventions de Genève interdisent les actes visant à répandre la terreur parmi la population civile. Voir PA I art. 51(2) et PA II art. 13(2). Pour une discussion sur le DIH et le terrorisme, voir CICR, « Droit international humanitaire : questions et réponses », 2011, disponible sur : http://www.icrc.org/fre/resources/documents/faq/terrorism-faq-050504.htm.

77 Voir CICR, *op. cit.*, note 72, pp. 6-7. Le DIH distingue essentiellement deux catégories de personnes dans les conflits armés : les membres des forces armées et les civils. Alors que ces derniers sont protégés en toutes circonstances, sauf s'ils participent directement aux hostilités et pendant la durée de cette participation, les premiers ne sont protégés contre les attaques qu'une fois hors de combat (pour cause de maladie, de blessure, de reddition ou de capture). Dans les conflits armés contemporains, les fonctions civiles et les fonctions militaires deviennent floues. Un exemple est la participation d'organismes civils (par ex. le programme des drones de la CIA) aux opérations militaires. Cela met en évidence une autre difficulté liée à la distinction entre les civils et les militaires : le problème des civils qui participent directement aux hostilités.

78 Article 2 de la Convention sur l'interdiction de l'emploi, du stockage, de la production et du transfert des mines antipersonnel et sur leur destruction, 18 septembre 1997.

79 Sur les mines antipersonnel, voir par exemple le site web du CICR : http://www.icrc.org/fre/war-and-law/weapons/anti-personnel-landmines/index.jsp.

Tout être vivant sur un champ de bataille doit être abattu sans distinction

Dans de nombreux jeux de tir subjectif, l'usage de la force ressemble à un sport. Au lieu de chasser du gibier, les joueurs chassent des êtres humains virtuels. Comme, le plus souvent, les champs de bataille virtuels ne contiennent aucun civil, tout être vivant est un ennemi[80]. Lorsqu'ils sont blessés, les combattants ennemis continuent généralement de se battre, ce qui justifie de les tuer. Le DIH distingue essentiellement deux catégories de personnes dans les conflits armés : les combattants et les civils. Tandis que ces derniers sont protégés en toutes circonstances, sauf s'ils participent directement aux hostilités et pendant la durée de cette participation, les premiers sont protégés s'ils sont hors de combat pour cause de maladie, de blessure, de capture ou de reddition. Dans les conflits armés contemporains, les fonctions civiles et militaires sont brouillées. De plus, le problème des civils qui participent directement aux hostilités s'est ajouté à la difficulté qu'il y a à différencier les civils et les militaires[81].

Les plaques d'identité sont des trophées

Dans de récents jeux vidéo[82], les joueurs doivent s'emparer des plaques d'identité des combattants ennemis qu'ils ont tués afin de valider ces morts et être récompensés. En situation de guerre, de nombreuses personnes disparaissent, laissant leur famille et leurs amis dans l'angoisse et l'incertitude car leur corps ne peut pas être identifié. Le DIH et le droit international des droits de l'homme exigent des parties à un conflit armé qu'elles prennent des mesures pour faire en sorte d'éviter les disparitions. Par exemple, tous les combattants devraient porter des documents d'identité adéquats[83] afin que leur sort puisse être documenté. Le DIH permet de prélever une des plaques d'identité pour la transmettre au Bureau national de renseignements ou à l'Agence centrale de recherches. L'autre

80 Une exception est une scène tirée de *Call of Duty: Modern Warfare II*, qui inclut le meurtre collectif de civils dans un aéroport (bien que cette scène ne se déroule pas à proprement parler sur un champ de bataille). Les joueurs peuvent participer à ce massacre sans subir aucune sanction.

81 Pour la notion de « participation directe aux hostilités », voir aussi Nils Melzer, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, Genève, 2009.

82 Notamment *Call of Duty: Modern Warfare 3* et *Call of Duty: Black Ops 2*.

83 La carte d'identité est le principal document permettant d'établir le statut et l'identité des personnes tombées aux mains de la partie adverse, et les États doivent en délivrer à toute personne susceptible de devenir prisonnier de guerre (CG III, art. 17). La carte doit indiquer au moins les noms et prénoms de son détenteur, sa date de naissance, son numéro matricule ou indication équivalente, son grade, son groupe sanguin et son facteur rhésus. Elle peut également porter les informations facultatives suivantes : description, nationalité, religion, empreintes digitales ou photo du détenteur, ou date d'expiration. Par ailleurs, les autorités doivent délivrer des cartes d'identité spécifiques pour le personnel militaire effectuant des tâches spéciales ou pour certaines catégories de civils. Les autorités peuvent compléter les mesures ci-dessus en fournissant des plaques d'identité (CG I, art. 16 ; CG II, art. 19), qui seront portées en permanence autour du cou sur une chaîne ou une lanière. Ces plaques, simples ou doubles, doivent être faites, si possible, d'un matériau inoxydable solide, résistant aux conditions du champ de bataille. Les inscriptions qu'elles portent sont semblables à celles qui figurent sur la carte d'identité et devraient être indélébiles et ineffaçables.

Figure 3: Dans le jeu *Crysis 2*, les joueurs peuvent attaquer une ambulance en toute impunité. Les attaques contre les ambulances n'entraînent ni avertissement, ni sanction. © CICR, Thierry Gassmann.

moitié devrait rester sur le corps afin de faciliter son identification. En 2003, le CICR a organisé une conférence internationale pour s'attaquer à cette tragédie invisible et chercher des moyens d'aider les familles et les communautés touchées. En 2006, l'Assemblée générale des Nations Unies a adopté la Convention internationale pour la protection de toutes les personnes contre les disparitions forcées.

Le personnel et les infrastructures sanitaires peuvent être attaqués

Un autre message qu'envoient certains jeux vidéo est qu'il est normal de prendre directement pour cible du personnel et des infrastructures de santé et que cela n'a aucune conséquence (figure 3)[84]. Cette impression est renforcée quand le personnel médical, dans les jeux vidéo, a un rôle et des armes offensives, notamment des lance-grenades[85]. Dans les conflits armés réels,

84 L'emblème de la croix rouge est devenu synonyme de « soins de santé » dans les jeux vidéo à la sortie de *Doom*, en 1993. Dans *ArmA II*, les emblèmes de la croix rouge, du croissant rouge et du cristal rouge sont clairement visibles (figure 5). Les véhicules blindés portant un emblème ne transportent pas d'armes, uniquement des équipements médicaux. Cependant, les unités d'« intelligence artificielle » contrôlées par le jeu ne font pas la distinction entre les personnes et les objets portant l'emblème protecteur et les autres. Dans le jeu *Crisis 2*, les joueurs peuvent attaquer une ambulance en toute impunité, sans recevoir ni avertissement, ni sanction.

85 Dans les jeux multi-joueurs, chaque joueur choisit une classe ou une fonction. En plus des snipers, des grenadiers ou des ingénieurs, on trouve souvent du personnel infirmier ou des médecins de guerre qui ont pour fonction de soigner ou de ressusciter leurs camarades. Le personnel infirmier, parfois habillé

des milliers de blessés et de malades sont privés de soins de santé efficaces quand les hôpitaux sont endommagés par des armes explosives ou quand les combattants y pénètrent de force, quand les ambulances sont détournées et quand les membres du personnel de santé sont menacés, enlevés, blessés ou tués. Le problème est si aigu dans les guerres d'aujourd'hui que le CICR a lancé une campagne mondiale, « Les soins de santé en danger », afin de faire connaître ce problème humanitaire[86].

Innovations de l'industrie du jeu vidéo visant à répondre aux défis humanitaires

Ces dernières années, les concepteurs de jeux ont pris plusieurs initiatives pour répondre à certaines des préoccupations mentionnées ci-dessus, ce qui démontre une envie de « bien faire »[87]. Les innovations comprennent : la suppression des civils des jeux vidéo, l'introduction de règles et de sanctions, le renforcement du principe de distinction, la possibilité d'opter pour autre chose que tuer, la suppression des emblèmes de la Croix-Rouge et du Croissant-Rouge et l'inclusion d'avertissements et de restrictions de cibles pour les joueurs.

Suppression des civils des jeux vidéo

Ayant observé que les joueurs tirent sur des civils innocents « simplement parce qu'ils en ont la possibilité », les créateurs de *Battlefield 3* ont décidé de supprimer tous les civils de leur jeu et de contourner ainsi la question de la distinction[88]. Cependant, cette solution plutôt radicale a pour résultat des représentations irréalistes des conflits urbains, notamment des combats qui se déroulent dans des centres villes vides de tout civil[89].

de blanc et portant souvent une croix rouge (ou d'une autre couleur), est généralement muni d'armes de petit calibre et a des capacités offensives de faible portée, mais efficaces, lorsqu'il a des fonctions de combat. Ces jeux envoient plusieurs messages inexacts au sujet des règles de la guerre (par ex. que des personnes ayant un rôle offensif peuvent porter des emblèmes protecteurs et que les attaques contre le personnel médical sont acceptables).

86 Voir CICR, *Health care in danger: a sixteen-country study*, CICR, Genève, 2011, disponible (en anglais uniquement) sur : http://www.icrc.org/eng/assets/files/reports/4073-002-16-country-study.pdf. Les États et les Sociétés nationales de la Croix-Rouge et du Croissant-Rouge ont adopté à l'unanimité une résolution sur cette question lors de la XXXI[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge. Voir résolution 5, « Les soins de santé en danger : respecter et protéger les soins de santé », document établi par le CICR, adopté à la XXXI[e] Conférence internationale de la Croix-Rouge et du Croissant-Rouge, Genève, 28 novembre-1[er] décembre 2011, disponible sur : http://www.rcrcconference.org/docs_upl/fr/R5_HCiD_FR.pdf.

87 Voir par exemple les changements entre les versions 1 et 3 de *Battlefield*. Dans la dernière version, les joueurs n'ont pas à assister à des actes de torture ou à en commettre.

88 Alec Meer, « Why you can't shoot civilians in *Battlefield 3* », interview de Patrick Bach, directeur général de DICE, dans *Rock, Paper Shotgun*, 30 août 2011, disponible sur : http://www.rockpapershotgun.com/2011/08/30/why-you-cant-shoot-civilians-in-battlefield-3/.

89 Bien qu'aucun civil ne soit visible dans le jeu, il est difficile d'imaginer qu'un conflit armé puisse se dérouler dans le centre de Téhéran (*Battlefield 3*) ou de Paris (*Call of Duty: Modern Warfare 3* et *Battlefield 3*) sans qu'aucun civil ne soit présent.

Introduction de règles et de sanctions

Dans une tentative de refléter la réalité des champs de bataille, certains concepteurs de jeux vidéo ont introduit des règles et des sanctions dans le scénario. Ainsi, ils ont intégré des aspects du droit applicable durant un conflit armé réel. Dans certains jeux, les personnages sont pénalisés s'ils tuent des civils. Par exemple, dans *Under Ash*, produit par Dar al-Fikr, les créateurs syriens de *Under Siege*, un joueur qui abat des civils perdra des points ou sera éliminé. Dans *Rainbow Six: Vegas*, le joueur qui commet des meurtres « excessifs » de civils est sanctionné en perdant sa fonction de commandement[90]. Dans *ArmA II*, les joueurs peuvent tirer sur des civils désarmés, mais s'ils persistent, ils seront finalement abattus par des soldats de leur propre camp[91].

Renforcement du principe de distinction

Dans *Call of Duty: Modern Warfare 3*, la majorité des soldats ennemis porte des uniformes et des emblèmes distincts et se comporte en général conformément au DIH. Lorsqu'ils ne sont pas en uniforme, les combattants ennemis portent des armes bien visibles et sont prompts à blesser le joueur, ce qui évite toute confusion au sujet des personnages qui constituent, ou non, des cibles légitimes[92].

Possibilité de choisir d'autres options que tuer

Bien que le DIH autorise l'usage de la force létale contre des combattants ennemis et des objectifs militaires[93], les parties à un conflit armé sont libres d'atteindre leurs objectifs militaires sans recourir à la force létale. Dans une tentative de mieux refléter la réalité, certains jeux incluent des options autres que tuer l'ennemi pour atteindre certains objectifs. Par exemple, dans le jeu du Hezbollah *Special Force 2*, les objectifs incluent la capture des soldats ennemis. *ArmA II* est le seul jeu, à la connaissance des auteurs, qui comprenne une option « reddition » pour les joueurs ou les soldats ennemis[94] et, dans *Under Siege*, le héros sauve des Palestiniens blessés par l'ennemi.

90 F. Castillo, *op. cit.*, note 51, p. 37.

91 Les joueurs ont notamment la possibilité, au lieu d'avoir recours à la force létale contre leurs alliés, d'arrêter et de traîner en justice les soldats qui commettent des crimes de guerre. Le défi, pour les concepteurs, est de trouver des moyens d'intégrer ces changements sans nuire au rythme du jeu.

92 Contrairement aux premières versions de ces jeux, *Call of Duty 4* et *Halo 3* intègrent aussi des changements pour éviter tout usage inadéquat des emblèmes. Par exemple, l'emblème de la croix rouge n'est plus utilisé dans ces jeux pour indiquer comment les joueurs peuvent se rétablir et remplir leur barre d'énergie.

93 Toujours sous réserve des principes de distinction, de proportionnalité et de précaution.

94 En contradiction avec le DIH, dans les jeux vidéo, en règle générale, personne ne se rend aux combattants ennemis. L'obligation de libérer l'ennemi s'il ne peut pas être détenu est entièrement absente. Comme relevé ci-dessus, dans les jeux testés par le CICR, les blessés, généralement, luttent ou essaient de se défendre avec une arme à feu. D'autres se contentent d'attendre jusqu'à ce que leur adversaire les tue. Dans d'autres scènes (injouables), des combattants blessés sont abattus alors qu'ils tentent de se rendre.

Figure 4: Exécution sommaire d'un captif dans *Call of Duty: Modern Warfare II*. Pour progresser dans le jeu, les joueurs doivent regarder cette scène qu'ils ne peuvent pas jouer. Ni sanctions, ni avertissements, ni conséquences n'accompagnent cette scène. © CICR, Thierry Gassmann.

Suppression des emblèmes de la Croix-Rouge et du Croissant-Rouge

Dans certains jeux vidéo, les emblèmes protecteurs de la Croix-Rouge et du Croissant-Rouge sont remplacés par d'autres (généralement des croix bleues, vertes ou blanches)[95]. Toutefois, même si les emblèmes protecteurs sont remplacés par d'autres symboles, le personnel médical et les volontaires qui accomplissent des tâches médicales doivent quand même être respectés et protégés en tout temps, à moins qu'ils ne commettent, en dehors de leur fonction humanitaire, des actes nuisibles à l'ennemi[96].

Avertissements et restrictions des cibles

Une autre innovation dans la conception des jeux est l'ajout d'avertissements pour les joueurs qui commettent des actes qui pourraient être considérés comme des violations du DIH s'ils étaient accomplis dans un conflit armé réel. Dans *Call of Duty: Modern Warfare 3*, les concepteurs ont fait de grands efforts pour éviter que des

95 Une exception est *ArmA II*, qui inclut trois des emblèmes distinctifs du Mouvement de la Croix-Rouge et du Croissant-Rouge.

96 Lorsqu'ils portent et utilisent des armes légères pour se défendre ou pour protéger les blessés et les malades dont ils ont la charge, les membres du personnel médical ne perdent pas la protection à laquelle ils ont droit. Les blessés et les malades dont ils s'occupent restent protégés même si le personnel médical lui-même ne l'est plus. Voir : PA I, art. 13 ; et règles 25 et 28 de l'Étude du CICR sur le droit coutumier (voir aussi p. 116 du commentaire de la règle 25, dans l'Étude du CICR sur le droit coutumier, *op. cit.*, note 52).

Figure 5 : Les emblèmes de la croix rouge, du croissant rouge et du cristal rouge sont rarement représentés dans les jeux vidéo actuels. *ArmA II* constitue une exception. Sur cette capture d'écran, un médecin soigne un combattant blessé à côté d'un poste de santé et d'un véhicule portant respectivement les emblèmes de la croix rouge et du cristal rouge. © Bohemia Interactive.

civils et des biens de caractère civil constituent des cibles (une caractéristique de la première version)[97]. Lorsque des biens de caractère civil se transforment en objectifs militaires, le jeu explique pourquoi. Quand des civils se trouvent dans la ligne de mire du joueur, un commandant invisible annonce que ce sont des civils et ordonne au joueur, soit de s'abstenir de tirer, soit de viser avec soin. Si le joueur décide de tuer un civil, la mission échoue instantanément et le jeu explique pourquoi[98].

Initiative du CICR

Sur la base de son expérience sur le terrain et de recherches[99], le CICR est arrivé à la conclusion que, si l'on veut modifier les comportements, il est préférable de modifier les conditions environnementales qui l'influencent plutôt que d'essayer de changer directement les opinions, les attitudes ou les points de vue. En conséquence, les activités du CICR visent à prévenir les souffrances humaines causées par les conflits armés ou d'autres situations de violence en favorisant un environnement propice au respect de la vie et de la dignité des personnes touchées par les conflits armés et

97 Pour plusieurs scènes posant problème dans la version 1 de *Call of Duty – Modern Warfare 3*, voir F. Castillo, *op. cit.*, note 51, pp. 23-25.

98 Ces innovations laissent penser que des consultants militaires et/ou juridiques ont participé à la conception du jeu. Voir aussi : Dave Their, « The real soldier behind the 'Call of Duty' games », dans *The Washington Post*, 19 octobre 2010. Disponible sur : http://www.aolnews.com/2010/10/19/the-real-soldier-behing-the-call-of-duty-games/.

99 D. Muñoz-Rojas et J.-J. Frésard, *op. cit.*, note 33.

d'autres situations de violence, et au respect des activités humanitaires. Concernant les jeux vidéo et les comportements individuels, il n'existe pas de preuves scientifiques concluantes quant à l'existence d'un lien entre les violations du DIH qui se produisent dans la réalité et celles qui sont décrites dans les jeux vidéo. Néanmoins, il est admis que l'utilisation très répandue des jeux vidéo pourrait rendre les joueurs insensibles à l'existence même de règles régissant l'usage de la force.

Au vu de la capacité des jeux vidéo de transmettre des messages positifs et négatifs sur les comportements qui sont autorisés durant les conflits armés, le CICR est inquiet que certains jeux vidéo banalisent les comportements odieux tels que la torture et les exécutions sommaires (figure 4). Les nouveaux jeux continuent à autoriser les joueurs à accomplir, sans aucune sanction, des actes qui constitueraient des violations du DIH s'ils se produisaient dans un conflit armé réel. En 2011, le CICR a invité les États et les Sociétés nationales de la Croix-Rouge et du Croissant-Rouge à un exposé sur les jeux vidéo qui représentent des conflits armés contemporains. Un bref film, présentant des scènes de certains des jeux vidéo les plus populaires, notamment les franchises *Medal of Honor*, *Call of Duty* et *ArmA*, a suscité une discussion animée, d'abord dans le cadre de cette manifestation puis en ligne, sur l'intégration des règles du DIH dans les jeux vidéo. En soulevant ces préoccupations, le CICR a souligné qu'il ne propose pas d'interdire toute représentation de violence dans les jeux vidéo. Il n'appelle pas non plus à renforcer la réglementation relative à l'industrie du jeu vidéo. Aussi paradoxal que cela puisse paraître, le CICR n'est pas partisan de jeux vidéo où les violations seraient interdites. Des violations se produisent sur les champs de bataille réels et peuvent donc aussi être commises dans les jeux vidéo. Par contre, l'institution plaide en faveur de champs de bataille qui reflètent la réalité. Certains jeux récents, notamment *ArmA II* (voir figure 5), font un grand pas dans cette direction. Il s'agit de présenter les opérations militaires soumises au droit et d'inclure des civils et des biens de caractère civil afin que les principes de distinction et de proportionnalité puissent être correctement compris et respectés. Les joueurs qui jouent des fonctions de combat devraient faire face aux mêmes dilemmes et défis que les vrais combattants. Les personnages qui violent les règles dans les jeux vidéo devraient être soumis à des sanctions et châtiments au même titre que les vrais combattants.

Au vu des mesures positives déjà prises par certains concepteurs pour intégrer des aspects des règles régissant l'usage de la force, le CICR, avec plusieurs Sociétés nationales de la Croix-Rouge, cherche à collaborer avec l'industrie dans le but d'influencer les principaux jeux vidéo. L'objectif général est de voir ce secteur adopter un changement de comportement pour finalement inclure, dans les nouveaux jeux ou les nouvelles versions de ceux existant déjà, des sanctions en cas de violations des règles de la guerre lorsque les paramètres du jeu permettent de commettre ces violations.

Depuis sa création en 1863, le CICR a acquis une vaste expérience directe des conflits armés et d'autres situations de violence armée. Grâce à ses démarches auprès des autorités gouvernementales, des groupes armés non étatiques, des militaires, de la police, etc. en faveur de l'adoption de mesures préventives favorisant le respect du droit, le CICR peut offrir des conseils utiles à l'industrie du

jeu vidéo. Avec les Sociétés nationales de la Croix-Rouge et du Croissant-Rouge concernées, il a engagé un dialogue avec les producteurs de jeux, les concepteurs et les joueurs, au sujet de la création de jeux plus réalistes qui intègrent le droit et proposent donc aux joueurs des dilemmes semblables à ceux que les soldats rencontrent sur les champs de bataille actuels. Le contenu des jeux vidéo publiés d'ici décembre 2013 permettra d'évaluer le succès de cette initiative.

Le but n'est pas de gâcher le plaisir des joueurs, par exemple en interrompant le jeu par des fenêtres pop-up énumérant des dispositions juridiques ou faisant la morale aux joueurs sur les règles de la guerre. Le but est plutôt que les règles régissant l'usage de la force soient intégrées dans les jeux afin que les joueurs puissent avoir une expérience vraiment réaliste et qu'ils doivent appliquer directement les principes de distinction (en vérifiant la nature des cibles), de proportionnalité (en optant pour la conduite qui causera le moins de dommages collatéraux aux civils et à leurs biens) et de précaution (en décidant si les attaques peuvent être lancées ou si elles doivent être reportées ou annulées). Par conséquent, les personnes et les objets protégés par le DIH doivent être inclus pour que le jeu reflète la réalité des conflits armés.

Par exemple, une approche plus réaliste de la question du respect des unités médicales et de l'utilisation des emblèmes protecteurs serait de conserver les emblèmes de la Croix-Rouge et du Croissant-Rouge dans les jeux vidéo, de mettre en évidence leur rôle protecteur et indicatif[100] et d'introduire des sanctions pour les joueurs qui attaquent le personnel médical, les moyens de transport médicaux et les hôpitaux qui portent l'emblème. Des sanctions devraient également s'appliquer en cas d'usage abusif de l'emblème (par ex. si un joueur transporte des armes jusqu'au front dans des ambulances ou lance des attaques depuis les ambulances [crime de perfidie])[101].

Les initiatives déjà prises par l'industrie prouvent que ces modifications sont possibles. Dans une enquête menée auprès des joueurs, la plupart des personnes interrogées étaient favorables à l'idée qu'un joueur qui respecte les règles de la guerre dans un jeu en soit récompensé[102]. Au contraire, ceux qui violent les

100 Voir CICR, *Étude sur l'usage des emblèmes : problèmes opérationnels et commerciaux et autres problèmes non opérationnels*, CICR, Genève, 2011.

101 L'art. 37 du PA I interdit la perfidie ou le fait de faire appel, « avec l'intention de la tromper, à la bonne foi d'un adversaire pour lui faire croire qu'il a le droit de recevoir ou l'obligation d'accorder la protection prévue par les règles du droit international applicable dans les conflits armés ». Les exemples comprennent : « Feindre l'intention de négocier sous le couvert du pavillon parlementaire, ou feindre la reddition ; feindre une incapacité due à des blessures ou à la maladie ; feindre d'avoir le statut de civil ou de non-combattant ; feindre d'avoir un statut protégé en utilisant des signes, emblèmes ou uniformes des Nations Unies, d'États neutres ou d'autres États non parties au conflit ». Le Statut de Rome de la Cour pénale internationale (ci-après, « Statut de Rome »), ouvert à la signature le 17 juillet 1998, Recueil des traités vol. 2187, p. 3 (entré en vigueur le 1er juillet 2002), inclut parmi les crimes de guerre le fait d'utiliser indûment les emblèmes distinctifs et, ce faisant, de causer la perte de vies humaines ou des blessures graves et le fait de diriger intentionnellement des attaques contre les bâtiments, le matériel, les unités et les moyens de transport sanitaires, et le personnel utilisant les signes distinctifs prévus par les Conventions de Genève. Voir art. 8(2)(b)(vii) et (xxiv) et (e)(ii) du Statut de Rome.

102 G. Humbert-Droz, *op. cit.*, note 15. Selon cette enquête francophone, la plupart des joueurs n'avaient que peu de connaissances sur le DIH. L'intérêt pour l'intégration du DIH dans les jeux vidéo était faible.

règles devraient être sanctionnés. Les bonnes ventes des nouveaux jeux qui ont intégré des règles de la guerre démontrent que l'intégration du droit ne nuit pas au succès commercial des jeux vidéo[103].

Conclusion

Cet article appelle à concevoir des jeux vidéo plus réalistes où les joueurs font face aux mêmes dilemmes que les combattants. Au vu des mécanismes présents dans les jeux vidéo et de leur valeur pédagogique, les auteurs soutiennent que les joueurs devraient être récompensés lorsqu'ils respectent le droit et sanctionnés en cas d'infraction. Indiscutablement, les jeux vidéo représentent un vecteur important qui peut favoriser la connaissance ou, inversement, le non-respect, des règles applicables à l'usage de la force et au traitement des personnes aux mains de l'ennemi. De l'avis des auteurs, leur portée dépasse de loin celle des programmes classiques d'éducation et de formation au DIH et au droit international des droits de l'homme[104]. Ceux qui ont des doutes au sujet de l'importance des jeux vidéo pour la diffusion des normes humanitaires n'ont qu'à regarder la taille de l'industrie du jeu vidéo ; la connaissance limitée du DIH et du droit international des droits de l'homme qu'ont les amateurs de jeux vidéo[105] et le grand public[106] ; le grand nombre de militaires recrutés par le biais de jeux vidéo ; et le taux supérieur à la moyenne de joueurs parmi le personnel militaire en service[107]. Plusieurs questions relatives aux jeux vidéo doivent être approfondies. Le risque que les opérateurs de drones fassent leur travail avec une « mentalité PlayStation » et l'impact possible des jeux sur la prise de décisions durant les opérations militaires constituent des problématiques importantes, tout comme la nature et la portée des obligations des États découlant du DIH et du droit international des droits de l'homme concernant les jeux vidéo commerciaux. Les auteurs espèrent que d'autres personnes s'inspireront de cet article pour étudier plus en profondeur ces questions, ainsi que d'autres points relatifs à la relation entre jeux vidéo et normes humanitaires.

103 Par exemple, en 2012, *Call of Duty: Modern Warfare 3* (dont les concepteurs ont fait de grands efforts pour éviter que des civils et des infrastructures civiles constituent des cibles – une caractéristique de la première version), a atteint la huitième place des 10 meilleures ventes de jeux et la deuxième position des jeux de tir subjectif en situation de combat (*Call of Duty: Black Ops 2* étant numéro un). Voir « 10 best selling videogames in 2012 », *op. cit.,* note 4.

104 Selon McGonigal, des dizaines, voire des centaines de millions de personnes jouent à des jeux vidéo chaque année (voir Jane McGonigal, « Le jeu peut rendre le monde meilleur », TED Talk, filmé en février 2010, disponible sur : http://www.ted.com/talks/jane_mcgonigal_gaming_can_make_a_better_world.html. Voir aussi : Entertainment Software Association, *Sales, Demographic and Usage Data: Essential Facts about the Computer and Video Game Industry*, 2011, Entertainment Software Association, Washington, D.C., 2011, disponible sur : http://www.theesa.com/facts/pdfs/ESA_EF_2011.pdf.

105 Voir G. Humbert-Droz, *op. cit.,* notes 15 et 102.

106 Voir B.A. Gutierrez, S. DeCristofaro et M. Woods, *op. cit.,* note 18, p. 1038 (« …de nombreux Américains n'ont jamais rien appris sur les Conventions de Genève, si ce n'est peut-être qu'elles existent … Aux États-Unis, deux jeunes sur cinq et un adulte sur trois pensent que les soldats américains détenus à l'étranger peuvent être torturés… » [traduction CICR]).

107 Voir B.W. Knerr, *op. cit.,* note 21.

Volume 94 Sélection française 2012/2

REVUE INTERNATIONALE

Attester de l'espace les violations du droit international humanitaire : examen critique de l'analyse géospatiale des images satellite durant les conflits armés à Gaza (2009), en Géorgie (2008) et au Sri Lanka (2009)

Joshua Lyons*

Joshua Lyons est l'analyste d'imagerie satellite de Human Rights Watch. Avant d'occuper ces fonctions, il était analyste principal du Programme Opérationnel pour les applications satellitaires des Nations Unies (UNOSAT). Il est titulaire de maîtrises en relations internationales de la London School of Economics (LSE) et en science de l'information géographique de l'University College London (UCL).

Résumé

Depuis le lancement du premier capteur satellite commercial à très haute résolution en 1999, la technologie spatiale est de plus en plus prise en considération et sollicitée pour permettre l'identification à distance d'éventuelles violations des droits de l'homme et

* La version originale en anglais de cet article est publiée sous le titre « Documenting violations of international humanitarian law from space: a critical review of geospatial analysis of satellite imagery during armed conflicts in Gaza (2009), Georgia (2008), and Sri Lanka (2009) », dans *International Review of the Red Cross*, Vol. 94, N° 886, été 2012, pp. 739-763.

du droit international humanitaire. Comme le montrent les trois cas de conflits armés décrits dans cet article - à Gaza, en Géorgie et au Sri Lanka - l'analyse des images satellite a permis de fournir aux enquêteurs des éléments de preuve indépendants, vérifiables et convaincants de violations graves du droit international humanitaire. L'article évoque aussi les limites importantes de cette analyse fondée sur l'imagerie satellite, sans oublier les difficultés plus générales, d'ordre technique, analytique et politique, auxquelles sera confrontée à l'avenir la communauté humanitaire et des droits de l'homme pour réaliser des analyses à partir de données acquises par satellite.

Mots-clés : imagerie satellite, conflit armé, droit international humanitaire, DIH, Gaza, Géorgie, Sri Lanka, technologie spatiale, droits de l'homme, géospatiale, GEOINT, Human Rights Watch, HRW, Richard Goldstone, UNOSAT, Ossétie du Sud, évaluation des dommages, Tigres de l'Eelam Tamoul, LTTE, rapport Goldstone, Israël, FDI, Nations Unies, ONU, UNITAR, IMINT.

: : : : : : : :

La publication de certaines images, recueillies par les services de renseignement des États-Unis, pour étayer des soupçons sur l'existence de fosses communes à Srebrenica en 1995 et au Kosovo en 1999 a clairement montré comment les techniques d'observation par satellite pouvaient être utilisées afin d'identifier à distance des violations potentielles du droit international humanitaire (DIH)[1]. La première démonstration utilisant des sources publiquement disponibles remonte à la publication commerciale, en mars 2000, d'images de la ville de Grozny recueillies par le satellite Ikonos, un mois après que l'armée russe ait occupé la ville au cours de la seconde guerre de Tchétchénie[2]. Comme le montrent les images 1 et 2, la destruction presque totale de plusieurs milliers de bâtiments dans le centre de Grozny a été établie de façon irréfutable par des documents imagés très détaillés. Les conséquences de ce fait étaient aussi spectaculaires qu'évidentes : l'imagerie satellite commerciale permettrait désormais aux enquêteurs internationaux de recueillir des éléments de preuve en cas d'allégations de crimes de guerre, à distance de la zone de conflit, pendant les hostilités actives, et sans plus dépendre de la nécessité traditionnelle d'obtenir une autorisation officielle d'une ou de plusieurs parties au conflit.

1 Yahya A. Dehqanzada et Ann M. Florini, « Secrets for sale - how commercial satellite imagery will change the world », Carnegie Endowment for International Peace, février 2000, disponible sur : http://carnegieendowment.org/2000/03/01/secrets-for-sale-how-commercial-satellite-imagery-will-changeworld/4jgy (toutes les références Internet ont été consultées entre mars et juin 2012). Voir aussi Lt Col. Peter L. Hays, « Transparency, stability, and deception: military implications of commercial high-resolution imaging satellites in theory and practice », présenté à la conférence annuelle de l'International Studies Association, Chicago, 21-24 février 2001, disponible sur : http://isanet.ccit.arizona.edu/archive/hays.html.

2 Images fournies par GeoEye 2012. En 2003, les Nations Unies décrivaient Grozny comme « la ville la plus détruite au monde ». Voir « Scars remain amid Chechen revival », dans *BBC News*, 3 mars 2007, disponible sur : http://news.bbc.co.uk/2/hi/programmes/from_our_own_correspondent/6414603.stm.

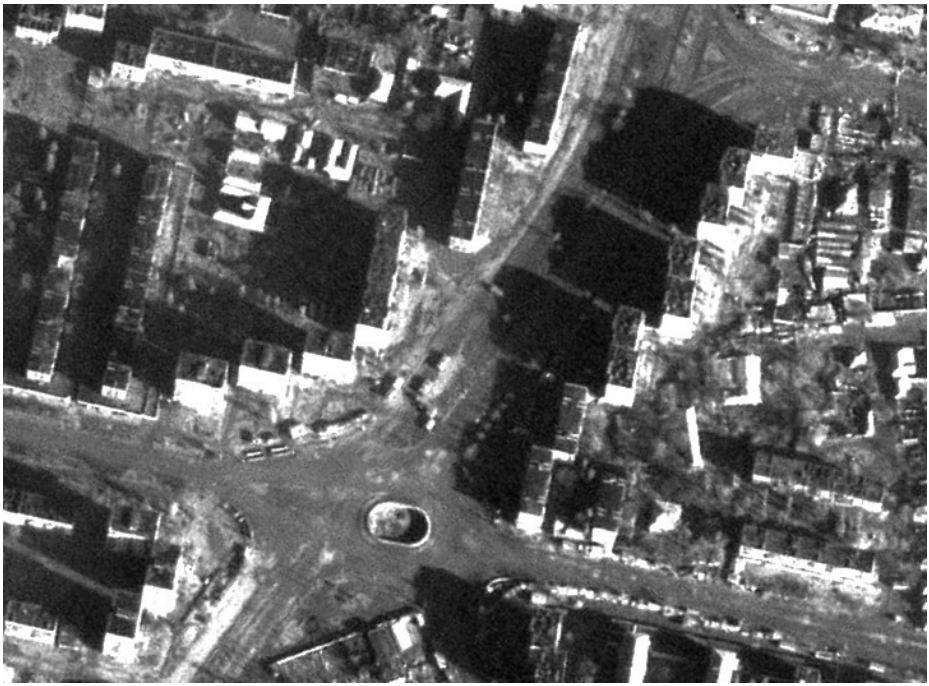

Image 1 : Le centre de Grozny (place Minutka) le 16 décembre 1999 (Image © GeoEye).

Depuis que les images satellite à très haute définition sont devenues disponibles pour la première fois sur le marché, à la fin de l'année 1999[3], le potentiel de cette technologie spatiale pour le suivi et l'analyse objective des faits qui surviennent sur le terrain en période de conflit armé, et en particulier comme source de preuves pour de graves violations du DIH, apparaît de plus en plus clairement.

Au cours des treize dernières années, le nombre de capteurs satellite commerciaux et à utilisation duale[4] a rapidement augmenté pour dépasser la dizaine, offrant une capacité de surveillance et d'analyse à distance qui a été employée avec succès dans un nombre de cas certes modeste mais croissant, couvrant tout le spectre des conflits, des conflits traditionnels entre États et guerres civiles aux cas de contre-insurrection et de violence intercommunautaire organisée.

L'analyse détaillée des images satellite disponibles sur le marché peut, dans des circonstances bien précises, jouer un rôle important de planification et

3 Grâce au satellite Ikonos, qui utilise des technologies de l'armée des États-Unis sur lesquelles le secret a été levé. On entend généralement par « images à très haute résolution » celles qui présentent une résolution spatiale (la taille minimale d'un pixel) inférieure ou égale à un mètre de diamètre. Ce seuil permet d'identifier visuellement un grand nombre d'objets terrestres, comme de petits véhicules de transport de personnes, des abris de fortune pour réfugiés et des dégâts aux bâtiments.

4 Les systèmes de satellite à utilisation duale sont mis au point, financés et contrôlés par des accords bilatéraux passés entre des entreprises privées et des services de renseignement nationaux ou des agences militaires.

Image 2 - Le même site après l'occupation russe, le 16 mars 2000 (Image © GeoEye).

de vérification dans le processus d'enquête. Elle peut fournir des indications précieuses sur les données spatiales et temporelles du conflit, elle peut aider à identifier des zones ou des incidents spécifiques exigeant un examen supplémentaire, et elle peut aider à corroborer, ou à contester, des témoignages dont la fiabilité est incertaine.

Avant tout, l'analyse des données recueillies par satellite peut fournir des éléments de preuve indépendants, vérifiables et incontestables de graves violations du DIH couvrant, par exemple, le recours disproportionné à la force, ou sans discrimination dans des zones civiles, les attaques visant délibérément des sites humanitaires ou culturels protégés, l'utilisation de civils comme boucliers humains, la destruction d'installations contenant des forces dangereuses ou l'absence de mesures de précaution pour protéger les civils des effets des attaques[5].

Toutefois, pour chaque cas dans lequel les images satellite ont indéniablement joué un rôle important et dynamique dans l'observation des conflits armés et l'élucidation de crimes de guerre potentiels, on compte aussi de nombreux cas dans lesquels ces données ont fourni des résultats peu concluants, ambigus et parfois trompeurs ou erronés. Ces cas reçoivent en général une publicité bien

5 Questions couvertes par les articles 51, 53, 56 et 57 du Protocole additionnel I aux Conventions de Genève du 12 août 1949, par les articles 11, 15 et 16 du Protocole additionnel II, et par les règles correspondantes du droit international humanitaire coutumier.

moindre, ce qui crée une perception déformée de l'efficacité générale de la technologie spatiale, et peut, de ce fait, susciter des attentes excessives au sein de la communauté humanitaire internationale.

L'un des objectifs importants de ce domaine nouveau de la recherche humanitaire appliquée devrait être une vision plus autocritique des limites inhérentes à l'analyse des images satellite, ainsi que des conséquences politiques et juridiques potentielles que peut entraîner un travail analytique incomplet, erroné, ou trompeur sur des zones de conflit. Étant donné l'intérêt croissant que suscite ce domaine et le recours potentiel à ces possibilités techniques par les institutions humanitaires et les organisations non gouvernementales (ONG), il est indispensable de mener un débat plus rigoureux et de procéder à un échange ouvert d'enseignements tirés de l'expérience et de pratiques optimales.

Les applications de base de l'analyse des images satellite pour le droit international humanitaire

Si l'on en croit l'expérience concrète acquise par les agences des Nations Unies et les organisations internationales et non gouvernementales dans les années 2000, le contrôle par satellite et les analyses des données recueillies par cette voie sont utilisés à deux niveaux. Il peut s'agir, d'une part, d'apporter un soutien direct à des enquêtes de terrain classiques sur des allégations de crimes de guerre ou, d'autre part, de se substituer à ces enquêtes de terrain. La distinction entre ces deux niveaux dépend généralement de la quantité et de la pertinence des données satellite disponibles et surtout du degré général d'accès (en termes politiques et matériels) aux zones concernées et aux personnes faisant l'objet de l'enquête.

L'analyse des images à l'appui des enquêtes de terrain

Lorsqu'il est possible d'enquêter directement et efficacement sur le terrain, l'analyse des données recueillies par satellite peut offrir une série de mesures d'appui analytique et technique aux enquêtes traditionnelles en améliorant la planification, la qualité et l'exactitude générales du travail de terrain. L'analyse des données satellite peut, plus spécifiquement, avoir un effet démultiplicateur sur le travail d'enquête, par exemple en identifiant et en évaluant les sites intéressants avant le déploiement d'une mission, ce qui peut permettre d'économiser beaucoup de temps et de ressources. Dans bien des cas, la couverture et l'analyse détaillée par imagerie peuvent produire une estimation quantitative plus précise du nombre total de personnes ou des infrastructures touchées lorsque des violations présumées se sont produites des mois, voire des années plus tôt en laissant peu de preuves matérielles, ou lorsque les estimations sont fondées sur les témoignages de survivants d'un échantillon réduit et potentiellement non représentatif des communautés touchées.

Les enquêteurs ont plus fréquemment recouru aux données recueillies par satellite et aux analyses de ces données pour dégager des éléments de preuve

permettant de confirmer des incidents signalés ou des affirmations émanant de sources dont la crédibilité n'est pas établie. Une couverture spatiale et temporelle suffisante d'imagerie satellite qui peut être acceptée et servir de référence à titre d'ensemble de données objectives peut offrir un tableau opérationnel général de la situation sur le terrain. Ce tableau d'ensemble contribue à éclairer les faits survenus lorsque des rapports ou témoignages multiples et contradictoires donnent un tableau controversé ou incertain des événements et des sites pertinents.

Du fait de la capacité des capteurs satellite à fournir des images détaillées en temps réel ou presque (en principe dans les 12 à 24 heures), cette technique est devenue la norme utilisée *de facto* pour évaluer rapidement des événements qui ont été signalés, mais n'ont pas encore pu être vérifiés sur le terrain de manière indépendante. Dans ce contexte, on constate une tendance intéressante, des agences et organisations chargées de l'analyse des images satellite à ne rendre publics que les cas « réussis » de confirmation positive de résultats attendus ou d'événements signalés. Bien qu'aucune étude systématique n'ait été entreprise pour établir le nombre d'allégations dont la fausseté a pu être rapidement démontrée par l'analyse rapide de l'imagerie satellite, il est presque certain que ce nombre est largement sous-estimé. Cette tendance probable de ne pas signaler tous les cas où les conclusions ont contredit des affirmations ou des craintes de crimes de guerre potentiels est compréhensible, étant donné le caractère émotionnel des faits invoqués, mais elle tend néanmoins à sous-estimer la gamme des avantages potentiels que l'imagerie peut offrir aux enquêteurs.

C'est ainsi qu'en 2008, durant le conflit en Géorgie, une agence des Nations Unies demanda une collecte rapide d'images satellite pour vérifier les affirmations lancées par le ministère géorgien des Affaires étrangères, selon lesquelles le port de Poti, sur la mer Noire, terminal pétrolier important, avait été « dévasté » par un raid aérien des forces russes[6]. Or, étonnamment, les images recueillies révélèrent peu de signes d'un bombardement aérien, et encore moins de dommages majeurs infligés aux infrastructures portuaires ou aux bâtiments résidentiels civils adjacents. L'analyse des images permit en revanche d'identifier six navires de la marine géorgienne coulés dans le port, vraisemblablement par des troupes d'élite russes qui auraient occupé les lieux plusieurs heures durant[7].

Dans un autre cas, toujours pendant le conflit géorgien, des informations faisant état de destructions massives et délibérées de sites du patrimoine culturel dans la région de Tskhinvali conduisirent des responsables géorgiens à demander aux Nations Unies une évaluation urgente par satellite. Les analyses montrèrent que, si trois monuments religieux au moins avaient probablement été détruits, la majorité des sites en question ne semblaient pas avoir subi le moindre dommage. Au grand soulagement des responsables géorgiens, les faits ne semblaient pas

6 « Russian jets attack Georgian town », dans *BBC News*, 9 août 2008, disponible sur : http://news.bbc.co.uk/2/hi/europe/7550804.stm.

7 Analyse d'images satellite réalisée par le Programme Opérationnel pour les applications satellitaires de l'UNITAR (UNOSAT). La carte d'ensemble peut être consultée sur : www.unitar.org/unosat/node/44/1262.

suggérer une campagne délibérée, de la part des milices sud-ossètes, de destruction systématique des monuments historiques géorgiens dans la région, comme on l'avait redouté dans un premier temps[8].

L'analyse des images satellite en tant que source principale

La deuxième application de l'analyse des images recueillies par satellite est sans doute plus importante : il s'agit du cas dans lequel ces images sont une source principale de preuves directes de violations graves du DIH. L'analyse des images satellite peut être utilisée lorsque les enquêtes sur le terrain et l'interrogation des témoins sont impossibles, généralement à cause du manque de sécurité, de mesures d'interdiction gouvernementales ou de l'impossibilité matérielle d'accéder aux zones en question. Dans de telles circonstances, l'imagerie satellite a fait ses preuves comme unique moyen permettant de recueillir de manière indépendante, objective et systématique des preuves significatives de crimes de guerre, comme cela a été démontré pour la première fois au sujet de la ville de Grozny pendant la deuxième guerre de Tchétchénie, en 2000. Comme nous le verrons dans les cas de la Géorgie (2008) et de Sri Lanka (2009), c'est précisément la combinaison d'une couverture d'imagerie pertinente et d'un manque durable d'accès physique aux zones de conflit qui rend l'analyse des données satellite cruciale pour la compréhension générale des conflits et pour le travail d'enquête à leur sujet.

Trois études de cas : Gaza (2009), la Géorgie (2008) et Sri Lanka (2009)

Ces trois cas ont été choisis en raison de l'importance relative qu'a prise l'analyse de l'imagerie satellite dans ces conflits, en apportant un soutien significatif ainsi que des preuves principales directes à l'appui d'enquêtes sur des violations alléguées du DIH. Bien que ces cas soient, à bien des égards, des illustrations parlantes de l'importance plus vaste et du potentiel à long terme de la technologie satellitaire pour ce type d'activité, nous examinerons aussi les limitations critiques ainsi que les défis qui furent identifiés à cette occasion.

Gaza (2009)

Juste après le début de l'opération militaire israélienne « plomb durci » à la fin du mois de décembre 2008, le Programme Opérationnel pour les applications satellitaires des Nations Unies (UNOSAT) de l'Institut des Nations Unies pour la formation et la recherche (UNITAR) lançait des activités de surveillance par satellite et d'évaluation des dommages sur Gaza, afin de soutenir les opérations

8 Source : correspondance et notes non publiées de l'auteur. Voir « Satellite damage assessment for cultural heritage monuments, South Ossetia, Georgia », UNITAR, disponible sur : http://www.unitar.org/unosat/node/44/1265.

d'urgence humanitaires en cours sur le terrain. Une série de documents détaillés axés sur l'évaluation des dommages furent rendus publics[9], et les données obtenues par satellite furent transmises à des organisations humanitaires telles que le Comité international de la Croix-Rouge ainsi qu'à des organismes de défense des droits de l'homme comme Human Rights Watch, pour leurs propres activités.

Dans les jours suivant le retrait des troupes israéliennes de Gaza, les analyses des Nations Unies fondées sur les données recueillies par satellite avaient abouti à une liste de plus de 3800 sites ayant subi des dommages sur la bande de Gaza, dont près de 2700 bâtiments endommagés, 187 ensembles de serres détruits et 930 cratères d'impact sur des routes importantes et des champs ouverts ou cultivés[10]. Sur la base des signes spécifiques des dommages, de la détection des forces de défense israéliennes (FDI) au sol et des déplacements de véhicules associés, il fut en général possible d'attribuer les dommages aux frappes aériennes de la force aérienne israélienne (FAI), aux tirs d'artillerie lourde ou aux opérations de démolition par les chars et bulldozers des FDI[11].

Après la mise sur pied par le Conseil des droits de l'homme, en avril 2009[12], de la Mission d'établissement des faits de l'Organisation des Nations Unies sur le conflit de Gaza, le chef de la Mission, le juge Richard Goldstone, commanda des analyses supplémentaires des images recueillies par satellite à l'appui du travail d'enquête de la Mission[13]. Les cartes et les documents connexes fournirent à la Mission Goldstone une vision d'ensemble de l'ampleur relative et de la distribution spatiale des dommages dans la bande de Gaza. Comme le déclara publiquement Richard Goldstone après l'achèvement du rapport officiel de la Mission d'établissement des faits de l'Organisation des Nations Unies sur le conflit de Gaza[14] :

Nous avons commandé ... un rapport complet sur les données recueillies par satellite, qui figure dans notre rapport. Il s'agit d'un document de 34 pages contenant des photographies prises par satellite de Gaza avant et après la campagne des Forces de Défense Israéliennes. Nous l'avons utilisé pour confirmer ou infirmer un grand nombre des informations que nous avons reçues concernant les dommages[15].

9 Voir les documents disponibles sur : http://www.unitar.org/unosat/maps/PSE.

10 « Satellite-based Gaza damage assessment overview », UNOSAT, disponible sur : http://unosat-maps.web.cern.ch/unosat-maps/PS/Crisis2008/UNOSAT_GazaStrip_Damage_Review_19Feb09_v3_Lowres.pdf.

11 *Ibid.* L'attribution aux diverses composantes de l'armée israélienne n'a pas toujours été possible avec le même degré de certitude, selon la complexité de l'environnement et le degré de dommages détectés.

12 Résolution 60/251 de l'Assemblée générale des Nations Unies, 3 avril 2009.

13 « Satellite image analysis in support to the United Nations Fact Finding Mission on the Gaza Conflict », UNITAR/UNOSAT, 31 juillet 2009, disponible sur : http://www2.ohchr.org/english/bodies/hrcouncil/specialsession/9/docs/UNITAR_UNOSAT_FFMGC_31July2009.pdf.

14 Rapport de la Mission d'établissement des faits de l'Organisation des Nations Unies sur le conflit de Gaza, doc. Nations Unies A/HRC/12/48, 25 septembre 2009, disponible sur : http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G09/158/67/PDF/G0915867.pdf?OpenElement.

15 « Goldstone transcript: righteous in our generation », *Rabbibrian's Blog*, disponible sur : http://rabbibrian.wordpress.com/2009/10/23/goldstone-transcript-righteous-in-our-generation/.

Le rapport d'établissement des faits a utilisé tout un éventail d'informations quantitatives dérivées des images satellitaires, concernant le moment des attaques israéliennes, pour corroborer les informations données par les témoins oculaires et, plus important encore, comme preuves principales invoquées dans les conclusions juridiques faisant état d'infractions graves à la Quatrième Convention de Genève par les forces israéliennes[16].

La section du rapport consacrée aux cas d'« attaques délibérées contre la population civile » cite à plusieurs reprises les chiffres de l'UNOSAT sur le nombre de bâtiments endommagés dans les quartiers résidentiels de Gaza et sur la période au cours de laquelle ces dommages ont été infligés. Ces données ont été utilisées pour confirmer les témoignages de familles concernant des incidents qui s'étaient vu donner une large publicité, comme la mort de 23 membres de la famille al-Samouni dans le quartier de Zeytoun du gouvernorat de Gaza[17].

C'est dans la section du rapport consacrée à la « destruction d'équipements industriels, de moyens de production alimentaire, d'installations d'approvisionnement en eau, de stations d'épuration des eaux usées et de logements » que la Mission s'appuie le plus sur l'analyse d'images satellite[18]. Outre des observations détaillées sur ce qui apparaît comme une volonté délibérée des forces israéliennes de viser plusieurs installations industrielles importantes, l'analyse des images réalisée par les Nations Unies a fourni les seules informations complètes sur l'ampleur de la destruction des complexes de serres dans l'ensemble de la bande de Gaza, au sujet de laquelle la Mission a conclu qu'elle « ne pouvait être justifiée par la volonté d'atteindre un quelconque objectif militaire »[19].

Qui plus est, une multiplication des attaques israéliennes contre des bâtiments commerciaux et résidentiels dans de nombreux endroits de la bande de Gaza a été observée dans les derniers jours du conflit, juste avant le cessez-le-feu et le retrait des forces terrestres des FDI. Les données quantitatives tirées des images qui illustrent cette tendance soulèvent des questions directes sur la stratégie de définition des cibles des FAI ainsi que sur la question de la nécessité opérationnelle. Dans le cas de Rafah, par exemple, un changement très net dans le choix des cibles des FAI a été observé au cours de la dernière semaine du conflit. Entre le 27 décembre 2008 et le 10 janvier 2009, les frappes aériennes des FAI ont été concentrées sur des terrains déserts le long du « couloir de Philadelphie » longeant la frontière, officiellement pour détruire les tunnels souterrains reliant la bande de Gaza à l'Égypte. Toutefois, pendant la dernière semaine du conflit précédant le cessez-le-feu proclamé par Israël le 18 janvier 2009, tout indique que les frappes aériennes des FAI se sont concentrées non plus sur les tunnels, mais sur la destruction de plus de 500 bâtiments situés le long de la frontière[20].

16 Rapport de la Mission d'établissement des faits de l'ONU, *op. cit.*, note 14, para. 1006.
17 *Ibid.*, pp. 156 et 169.
18 *Ibid.*, pp. 200-204 et 209-213.
19 *Ibid.*, para. 1021.
20 « Satellite image analysis in support to the United Nations Fact Finding Mission on the Gaza Conflict », UNITAR/UNOSAT, 27 avril 2009, pp. 6-13.

Des schémas similaires de destruction massive de bâtiments dans les derniers jours du conflit ont été identifiés grâce aux images satellite de plusieurs quartiers dans les gouvernorats de Gaza et de Gaza Nord, y compris la zone d'Al-Atatra, qui a vu plus de 55 % de tous ses bâtiments détruits pendant les trois derniers jours du conflit[21].

Comme le conclut le rapport de la Mission dans ses conclusions juridiques à ce sujet :

> Ayant comparé les résultats de sa propre enquête sur le terrain avec les images satellitaires d'UNOSAT et les témoignages publiés de soldats israéliens, la Mission conclut qu'outre les destructions étendues d'habitations prétendument rendues nécessaires par les opérations au cours de leur progression, les forces armées israéliennes se sont livrées à une autre vague de destruction systématique de bâtiments civils au cours des trois derniers jours de leur présence à Gaza, alors qu'elles savaient que leur retrait était imminent. Le comportement des forces armées israéliennes à cet égard était contraire au principe de la distinction entre objectifs civils et objectifs militaires et constitutive de l'infraction grave de « destruction … de biens, non justifiée … par des nécessités militaires et exécutée … sur une grande échelle de façon illicite et arbitraire »[22].

De manière générale, l'analyse des données recueillies par satellite a clairement rempli une fonction d'investigation importante, qui a contribué à structurer et à focaliser le travail de la Mission, à renforcer la crédibilité des témoignages recueillis grâce à une confirmation indépendante et à fournir des éléments de preuve indépendants principaux, directement cités dans certaines des conclusions juridiques du rapport de la Mission.

Nous reviendrons plus en détail sur cette question dans la suite de cet article, mais il est important de reconnaître les limites importantes - et dans certains cas criantes - de l'applicabilité, dans le cas de Gaza, de l'analyse des images satellite. L'absence systématique de données GPS précises sur des bâtiments importants dans la totalité du territoire a eu pour conséquence l'impossibilité de localiser, sur les images satellite, plusieurs usines, écoles et hôpitaux d'intérêt direct pour les enquêtes de la Mission. Plus problématique encore, l'impossibilité de fournir des informations pertinentes sur des violations potentielles du DIH commises par le Hamas, dont le déploiement de ses forces dans des zones peuplées sans avoir pris toutes les précautions pratiquement possibles pour réduire au minimum les dommages pour la population civile, ou le crime de guerre consistant à utiliser délibérément les civils comme boucliers humains. C'est là une lacune importante qui a des conséquences directes pour le suivi et l'analyse des conflits asymétriques de manière générale. Il n'a pas non plus été possible de fournir des informations pertinentes sur l'emploi potentiel par les forces israé-

21 *Ibid.,* pp. 14-22.
22 Rapport de la Mission d'établissement des faits de l'ONU, *op. cit.,* note 14, paras. 53 et 1006.

liennes de certains systèmes d'armement dont l'usage est restreint, comme les armes au phosphore blanc. Ces limites à l'utilisation des données satellite durant le conflit à Gaza seront examinées de manière plus détaillée plus loin, dans la section « Les satellites à la rescousse ? ».

La Géorgie (2008)

Après l'attaque militaire lancée par la Géorgie contre les forces sud-ossètes et russes à Tskhinvali du 7 au 9 août 2008, et le retrait subséquent des forces géorgiennes de la ville le 13 août 2008, les Nations Unies ont lancé un projet de surveillance et d'évaluation des dommages par satellite à la demande de plusieurs agences et organisations[23]. Sur la base de rapports initiaux faisant état de tirs d'artillerie nourris de l'armée géorgienne et de tirs de roquettes Grad contre des positions ossètes, les nouvelles images furent axées dans un premier temps sur la ville de Tskhinvali; il devint cependant vite évident qu'une évaluation plus large, au-delà des limites de la ville, serait nécessaire pour couvrir une deuxième vague de violences qui semblait se dérouler au nord et à l'est de la ville.

Grâce aux enseignements tirés du suivi des incendies criminels après les élections au Kenya en janvier 2008[24], il a été possible d'utiliser les données satellite provenant de capteurs environnementaux pour repérer et surveiller le déclenchement de grands incendies dans des endroits multiples en Ossétie du Sud juste après le retrait des forces géorgiennes. Bien que les capteurs environnementaux employés[25] n'aient pas pu distinguer les dommages concrets infligés aux bâtiments, ni déterminer la source des feux, il a été possible de déduire raisonnablement, à partir du moment et du lieu, que l'apparition soudaine et simultanée d'incendies à plusieurs endroits ne pouvait guère avoir des causes accidentelles ou naturelles. L'explication plus raisonnable était que ces feux représentaient une campagne d'incendies criminels dirigée contre des villages habités par des populations de souche géorgienne, interprétation confirmée par les témoins oculaires ainsi que par les photographies prises sur place par les chercheurs de Human Rights Watch présents en Ossétie du Sud au moment des attaques[26].

Le contrôle quotidien des sites où les feux faisaient rage permit de mettre à jour ce qui apparaissait comme un schéma d'incendies criminels, commençant le 10 août juste au nord de Tskhinvali, puis gagnant rapidement en nombre et en étendue le 12 août, jusqu'à toucher les villages à population de souche géorgienne de Kekhvi, au nord, et d'Eredvi, à l'est. Les incendies continuèrent à

23 Projet exécuté par UNITAR/UNOSAT en 2008.

24 On trouvera un exemple de carte des incendies criminels à l'adresse http://www.unitar.org/unosat/node/44/1035.

25 Données sur les incendies fournies par deux satellites MODIS de la NASA, Aqua et Terra, qui fournissent ensemble des données sur des incendies probablement actifs à l'intérieur d'une zone d'une superficie d'environ 1 km^2, de deux à quatre fois par jour.

26 Basé sur des échanges de correspondance internes aux Nations Unies. Voir aussi Human Rights Watch, *Georgia: satellite images show destruction, ethnic attacks,* 28 août 2008, disponible sur : http://www.hrw.org/news/2008/08/27/georgiasatellite-images-show-destruction-ethnic-attacks.

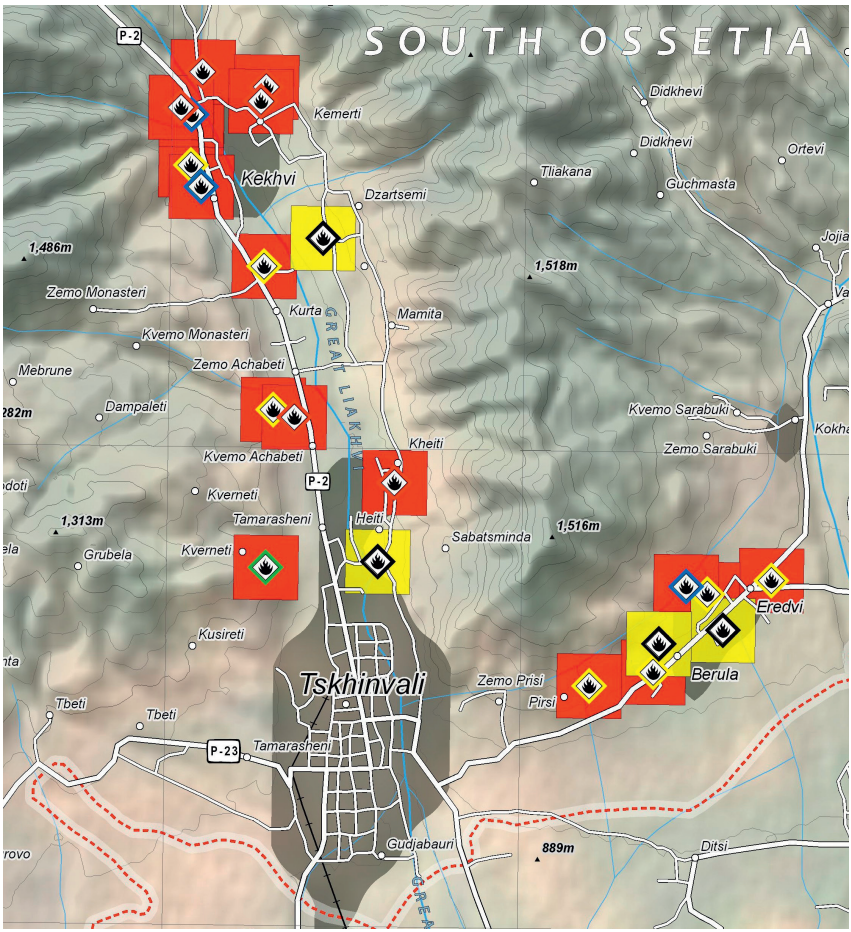

Image 3 : Carte des attaques incendiaires soupçonnées en Ossétie du Sud (Image © UNITAR/UNOSAT).

brûler les jours suivants, et il devint possible de repérer, à partir de la répartition de l'ensemble des feux détectés, deux groupes distincts d'attaques incendiaires suspectées, le premier centré sur les villages à population de souche géorgienne situés le long de la route principale (route P-2) et de la rivière Liakhvi, au nord de Tskhinvali, et le deuxième le long d'une route secondaire à l'est de Tskhinvali, entre les villages de Pirsi et d'Eredvi (voir image 3).

L'analyse des données satellitaires à très haute définition recueillies le 19 août 2008 fournit des preuves supplémentaires de la campagne d'incendies criminels, avec des images spectaculaires d'au moins huit bâtiments en proie aux flammes. Comme le montre l'image 4, un immeuble résidentiel situé dans le village de Kurta était de toute évidence en feu, dégageant un nuage de fumée noire. Les images des satellites montraient aussi des centaines de petits bâtiments d'habitations portant des signes clairs de dégâts causés par le feu, comme l'absence de toiture en présence de murs porteurs intacts, ce qui s'explique parfaitement

REVUE INTERNATIONALE de la Croix-Rouge

Image 4 : Immeuble résidentiel en proie aux flammes après une attaque incendiaire dans le village de Kurta (Ossétie du Sud) (Image © DigitalGlobe).

par le mode de construction caractéristique de la région, avec des murs en pierre et des toits en bois.

Une évaluation rapide des dommages infligés aux villages touchés dans la région fut effectuée à l'aide des images recueillies par satellite le 19 août. Les résultats de l'évaluation furent rendus publics sous forme de cartes, assorties de chiffres sur le nombre de bâtiments détruits ou gravement endommagés pour chaque village. Pour les premiers résultats couvrant le premier groupe de dommages aux bâtiments - y inclus la ville de Tskhinvali en direction du nord jusqu'au village de Kekhvi - un total de 1050 bâtiments détruits ou gravement endommagés furent dénombrés. Pour le deuxième groupe de dommages situé à l'est de Tskhinvali entre les villages de Pirsi et d'Eredvi, 300 bâtiments supplémentaires détruits ou gravement endommagés furent recensés[27].

27 « Village damage summary: Kekhvi to Tskhinvali, South Ossetia, Georgia », UNITAR, 28 août 2008, disponible sur : http://www.unitar.org/unosat/node/44/1258. Les données chiffrées sur les dégâts aux bâtiments sont toutes basées sur les images finales recueillies après la fin du conflit le 19 août 2008.

Pour la majeure partie de ces dommages identifiés aux bâtiments, et spécifiquement pour les dommages situés à l'extérieur du périmètre urbain principal de Tskhinvali, il fut généralement possible d'attribuer les dommages à l'une des forces militaires en présence, avec un risque limité de confusion avec les dégâts causés par d'autres forces militaires. Les dommages aux bâtiments causés par des incendies criminels concentrés au nord et à l'est de Tskhinvali purent être attribués avec certitude aux milices sud-ossètes qui menaient une campagne massive de nettoyage ethnique de la région des habitants de souche géorgienne.

Au vu de l'ampleur et de la durée prolongée des attaques incendiaires sur une période de dix jours, il semblait probable, à première vue tout au moins, que les Russes - qui étaient à l'époque la Puissance occupante en Ossétie du Sud[28] - aient systématiquement manqué à leur devoir d'empêcher les milices de lancer des attaques contre les civils et les bâtiments résidentiels, et qu'ils étaient donc responsables de violations graves de plusieurs articles de la Quatrième Convention de Genève[29].

Au vu de la complexité bien établie des combats au sol entre les forces géorgiennes et russes/sud-ossètes à Tskhinvali entre le 7 et le 12 août, il était évident qu'une évaluation des dommages à l'intérieur de la ville à partir des observations par satellite présentait des difficultés considérables sur le plan technique comme sur le plan politique, en termes d'exactitude comme en termes d'attribution potentielle à telle ou telle force. L'évaluation préliminaire pour l'ensemble de la ville, à partir des images recueillies le 19 août 2008, identifiait au total 230 bâtiments touchés. Sur ce nombre, 175 étaient complètement détruits et 55 autres gravement endommagés[30]. Les dommages étaient répartis de manière à peu près uniforme dans toute la ville, avec de nombreuses petites poches de destruction presque totale, dont la pire était le vieux quartier juif de la ville, comptant plus de 25 bâtiments détruits dans un périmètre très réduit[31].

L'examen des types de dommages identifiés grâce aux images satellite suggérait fortement que la plupart d'entre eux avaient été probablement causés par des tirs d'artillerie, mais le schéma de répartition des dommages aux bâtiments évoquait plutôt les types de dégâts habituellement causés par des tirs groupés de

Comme des incendies toujours actifs ont été détectés dans les villages le 22 août 2008, il est probable que le nombre de bâtiments endommagés dans les quatre villages à population de souche géorgienne situés à l'est de Tskhinvali (de Pirsi à Eerie) ait été supérieur à 300.

28 Rapport de la Mission d'enquête internationale indépendante sur le conflit en Géorgie (IIFFMCG), Conseil de l'Union européenne, 2009, paras. 19-28, disponible (en anglais) sur : http://www.ceiig.ch/pdf/IIFFMCG_Volume_I.pdf.

29 Les images recueillies le 19 août ont permis d'identifier de multiples concentrations de chars d'assaut russes et autres véhicules de transport lourds dans les villages au nord de Tskhinvali au moment des attaques incendiaires, ce qui suggère fortement que les forces russes ont appuyé passivement la campagne ossète de pillage et de destruction de biens dans les villages à population de souche géorgienne.

30 Les chiffres relatifs aux dégâts sont tirés de l'évaluation initiale de l'UNOSAT, terminée le 22 août 2008.

31 Voir le rapport de terrain concernant la destruction du quartier juif dans : Catherine Belton, « Tskhinvali bears scars of military maelstrom », dans *Financial Times,* 18 août 2008, disponible sur : http://www.ft.com/cms/s/0/06946f30-6cbb-11dd-96dc-0000779fd18c.html#axzz1tedp35Eb.

roquettes Grad[32]. Malgré les dénégations de toutes les parties quant à la responsabilité des dommages signalés aux immeubles résidentiels, l'évaluation des images satellite suggérait que l'on pouvait, de prime abord, imputer aux forces géorgiennes un usage sans discrimination de l'artillerie lourde, et en particulier de roquettes Grad, contre des quartiers densément peuplés de la ville au cours de leur offensive destinée à prendre Tskhinvali dans la matinée du 8 août 2008.

Sur la base des conclusions des vérifications effectuées sur le terrain après le conflit au Liban en 2006[33], qui montraient que les dommages aux bâtiments avaient été d'autant plus sous-évalués que les dégâts étaient peu graves, l'hypothèse a été faite, au moment de l'évaluation initiale, que les dommages aux bâtiments dans le milieu urbain de Tskhinvali avaient probablement été sous-estimés. Toutefois, un élément a été mal compris au cours de l'évaluation concernant Tskhinvali, à savoir l'ampleur potentielle de la sous-estimation des graves dommages aux bâtiments causés par les obus de chars et d'artillerie tirés à courte portée dans les flancs des bâtiments.

En septembre 2008, une ONG russe, Charta Caucasica, dont le siège est situé dans la république d'Ossétie du Nord, a publié un examen critique de l'évaluation des dommages à Tskhinvali réalisée par les Nations Unies sur la base de l'imagerie satellite. En se fondant sur une enquête réalisée sur place, l'ONG a publié des images des emplacements et des types de dégâts que l'évaluation des Nations Unies n'avait pas réussi à identifier. Bien que son enquête critique sur le terrain n'ait pas été rigoureuse et n'ait pas tenté d'aboutir à des estimations statistiques concernant les erreurs par action ou omission, les observations qu'elle contenait suggéraient fortement que l'ensemble des dégâts infligés aux bâtiments dans la ville avaient été gravement sous-estimés en raison de l'incapacité générale d'identifier, à partir des images satellite disponibles, les impacts de tirs d'artillerie et de roquettes dans les flancs de bâtiments élevés, pour la plupart des immeubles résidentiels[34].

Les photographies prises au sol de bâtiments portant des cratères clairement identifiables d'impacts latéraux et des marques d'explosions furent présentées en parallèle avec des images annotées des mêmes bâtiments tels qu'ils figuraient sur les cartes des Nations Unies réalisées à partir des images satellite. Les images 5 et 6 montrent l'emplacement exact de bâtiments endommagés non identifiés sur les images satellite et les photos correspondantes des mêmes sites, vus du sol. La conclusion générale tirée par Charta Caucasica était que l'imagerie satellite n'était guère appropriée pour effectuer une évaluation précise de l'éventail complet des dommages à l'intérieur de la ville, à cause de l'angle limité de prise de vues et de la résolution spatiale du capteur utilisé[35]. Ces graves limitations auraient dû être mieux comprises et anticipées, et des avertissements et notes explicatives auraient dû accompagner les cartes produites.

32 Informations fondées sur la correspondance personnelle de l'auteur avec des interlocuteurs au sein des Nations Unies.
33 Validation interne sur le terrain commandée par UNITAR/UNOSAT dans le sud et l'est du Liban après le conflit avec Israël, septembre-octobre 2006.
34 Disponible sur : http://www.caucasica.org/analytics/detail.php?ID=1387.
35 *Ibid.*

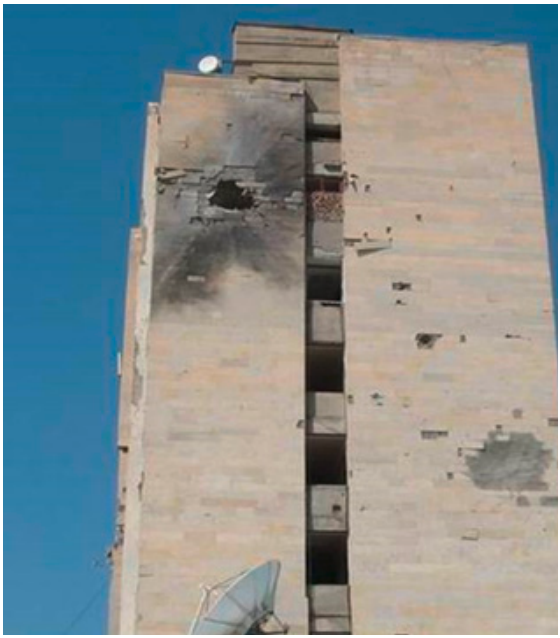

Image 5 : Photographie prise au sol d'un bâtiment endommagé présentant un cratère d'impact latéral à Tskhinvali (septembre 2008) (image reproduite avec l'autorisation de l'ONG Charta Caucasica).

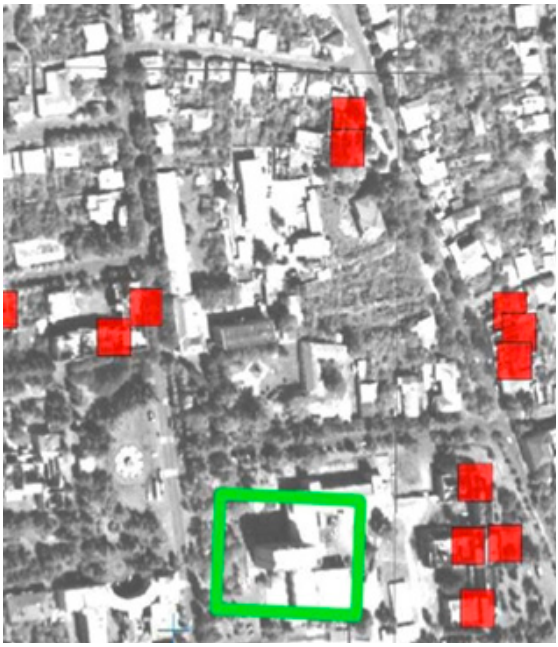

Image 6 : Image satellite montrant le bâtiment figurant sur l'image 5 (en vert) entouré de bâtiments touchés, dont les dommages ont été identifiés grâce aux images satellite (en rouge) (UNITAR/UNOSAT) (image © DigitalGlobe).

Sri Lanka (2009)

Les analyses d'images satellite réalisées par les Nations Unies pendant la guerre civile au Sri Lanka faisaient suite à une demande directe formulée en janvier 2009 par l'équipe de pays des Nations Unies à Colombo, qui souhaitait estimer le nombre de civils tamouls déplacés pris au piège à l'intérieur des trois zones de sécurité délimitées par le gouvernement dans le district de Mullaittivu[36]. Des images satellite furent aussi réunies et analysées durant les cinq derniers mois du conflit, afin de permettre le contrôle des mouvements massifs de civils, d'évaluer les incidents d'artillerie signalés à l'intérieur de ces zones, et d'identifier les dégâts aux bâtiments et les cratères d'impact causés par les tirs d'artillerie et les frappes aériennes. Du fait de la sensibilité politique des négociations entre l'équipe de pays des Nations Unies et les autorités sri-lankaises concernant l'accès de l'aide humanitaire à la zone de conflit, les rapports fondés sur les données acquises par satellite n'ont pas été rendus publics. Toutefois, le gouvernement sri-lankais a été dûment informé de leur préparation à l'époque ainsi que des conclusions générales de l'analyse pendant le déroulement des négociations[37].

Une seconde phase d'analyse s'est déroulée pour soutenir directement le Groupe d'experts chargé par le Secrétaire général de l'ONU d'étudier la question de la responsabilité du Sri Lanka (ci-après « le Groupe d'experts ») en 2010[38]. Recourant à une méthodologie proche de celle utilisée par la mission Goldstone à Gaza, le Groupe d'experts s'est appuyé sur l'analyse des images satellite pour corroborer les témoignages individuels concernant les bombardements de sites protégés. Le Groupe s'est aussi penché sur l'analyse des images satellite pour fournir, chaque fois que cela était possible, une analyse principale de l'attribution aux responsables du bombardement de lieux situés au sein des zones de sécurité qui, à l'époque, accueillaient des milliers de civils.

Un travail d'analyse supplémentaire a été effectué sur les sites de frappes aériennes et les sites visés par l'aviation sri-lankaise, ainsi que sur le champ d'action et la portée potentiels des mortiers et des batteries d'artillerie lourde de l'armée sri-lankaise en relation avec les zones identifiées de bombardements indiscriminés. Les conclusions de l'analyse furent soumises au Groupe d'experts lors de nombreuses séances d'information, puis sous forme d'un rapport définitif[39], qui fut partiellement incorporé dans le rapport final du Groupe d'experts au Secrétaire général, publié en mars 2011[40].

36 Projet exécuté par UNITAR/UNOSAT en 2009.

37 La communication d'un rapport aux médias britanniques par une ambassade étrangère, et la publication accidentelle par la suite d'un deuxième rapport, survenues toutes deux en avril 2009, ont déclenché une petite crise diplomatique, le gouvernement sri-lankais accusant les Nations Unies d'« espionnage ». Voir l'interprétation d'un câble de l'ambassade des États-Unis, disponible sur : http://wikileaks.org/cable/2009/05/09COLOMBO484.html#.

38 Rapport du groupe d'experts du secrétaire général des Nations Unies sur la question des responsabilités relatives aux événements au Sri Lanka, Nations Unies, 31 mars 2011, disponible (en anglais) sur : http://www.un.org/News/dh/infocus/Sri_Lanka/POE_Report_Full.pdf.

39 « Geospatial Analysis in Support to the Secretary-General's Panel of Experts on Sri Lanka », document Nations Unies non publié, 17 janvier 2011.

40 Rapport du groupe d'experts du secrétaire général, *op. cit.*, note 38.

Image 7 : Évaluation par imagerie satellite des dommages subis par l'hôpital de Vallipunam au Sri Lanka (UNITAR/UNOSAT).

Le Groupe d'experts souhaitait avant tout réaliser des évaluations détaillées des dommages infligés à une série de bâtiments médicaux et humanitaires protégés au sein de la zone de conflit, à la fois pour confirmer les dates des bombardements signalés et pour attribuer ces attaques à l'une des parties au conflit si cela était possible. La totalité des dix bâtiments médicaux, humanitaires et religieux examinés pour le Groupe[41] montraient des indications claires de graves dégâts résultant probablement de tirs d'artillerie indirects. En outre, les sept bâtiments médicaux et le centre d'aide humanitaire des Nations Unies semblaient avoir fait l'objet de tirs d'artillerie alors qu'ils étaient encore opérationnels et occupés par des civils en quête d'assistance humanitaire.

Les dommages identifiés sur les images satellite allaient de petits cratères d'impact relevés sur les toits des bâtiments et dans des cours à ciel ouvert, jusqu'à des cas d'effondrement total de la structure. Tous les sites examinés étaient soit clairement marqués comme des sites humanitaires protégés avec des emblèmes médicaux placés sur le toit, clairement visibles du ciel[42], soit faciles à distinguer en tant que sites culturels protégés de par leur architecture caractéristique. Comme le montre l'image 7, l'évaluation soumise au Groupe d'experts concernant les dégâts subis par l'hôpital Vallipunam, situé à l'extrémité sud de la première zone

41 Il s'agissait de sept hôpitaux, du centre de distribution des Nations Unies et de deux sites culturels/religieux (le temple de New Housing Colony Kandaswamy à Puthukkudiyiruppu et le temple de Kumara Kanapathi Pillaiyar, dans la division de Mullivaykkal West, à l'intérieur de la zone de sécurité 2).

42 L'emblème de la Croix-Rouge était en général clairement visible sur les images des satellites commerciaux utilisées dans le rapport.

de sécurité, indiquait clairement que l'enceinte de l'établissement avaient été gravement endommagée par des tirs d'artillerie, et ce plusieurs jours différents[43].

S'agissant de l'attribution des responsabilités, même s'il ne faisait guère de doute que les sites protégés examinés avaient été endommagés par des tirs d'artillerie répétés, aucun signe indubitable ne permettait d'attribuer la responsabilité des dégâts, et encore moins de répondre aux allégations selon lesquelles ces structures auraient été délibérément prises pour cible. Les dégâts causés par des tirs de mortier de petit et moyen calibre auraient pu être le fait soit des Tigres de libération de l'Eelam tamoul (LTTE) ou de l'armée sri-lankaise. Cela ne signifie pas qu'il était impossible d'utiliser les images disponibles pour attribuer la responsabilité des dommages, mais uniquement que cela n'était pas possible sur la base des indications fournies par les témoins oculaires présents sur les sites, telles que fournies au Groupe d'experts.

Cependant, une fois que l'étendue de l'évaluation fut élargie pour couvrir des zones étendues comprenant les sites protégés, il devint possible de tirer des conclusions bien argumentées sur l'identité probable des forces responsables de l'attaque. Des évaluations détaillées portant sur des zones situées à l'intérieur des zones de sécurité 1 et 2, ainsi que sur le centre de Puthukkudiyiruppu, permirent d'identifier un total de 1525 sites spécifiques de dommages[44]. Sur ce total, plus de 200 bâtiments permanents avaient été détruits ou gravement endommagés, tandis que 230 cratères d'impact supplémentaires furent recensés sur les toits de bâtiments permanents, et 1020 cratères d'impact supplémentaires dans des espaces ouverts (champs, plages, etc.).

L'analyse de ces zones de bombardements plus étendues aboutit à la conclusion que les dommages aux sites protégés n'étaient en fait pas le résultat de tirs d'artillerie isolés ou mal dirigés, mais qu'ils s'inscrivaient dans un schéma de tirs beaucoup plus étendus, que l'on peut décrire comme des bombardements de zone. Étant donné la quantité de munitions déployées sur des zones si étendues et les ressources largement épuisées des forces des LTTE, il ne faisait guère de doute que seule l'armée sri-lankaise était capable d'un tir d'artillerie aussi massif et soutenu. Des cartes détaillées ainsi que des données chiffrées sur ces zones de bombardement, illustrant de manière incontestable un recours disproportionné et sans discrimination à la force militaire par l'armée sri-lankaise dans des zones densément peuplées où se trouvaient des dizaines de milliers de civils tamouls déplacés, furent remises au Groupe d'experts[45].

Un examen détaillé des dommages probablement causés par des frappes aériennes durant une période de cinq mois permit d'identifier plus de 130 endroits différents où de tels dommages pouvaient être directement attribués à l'aviation

43 Les cartes d'évaluation concernant les sites protégés ont été publiées dans le rapport du Groupe d'experts du Secrétaire général, *op. cit.*, note 38.

44 On entend par là des cratères d'impact individuels sur les toits des bâtiments, dans des terrains à ciel ouvert, dans des zones humides et des routes, ainsi que des bâtiments permanents montrant des signes de dégâts plus graves que des cratères d'impact limités sur le toit (c'est-à-dire une destruction partielle ou totale).

45 « Geospatial analysis », *op. cit.*, note 39.

sri-lankaise[46]. La grande majorité de ces frappes aériennes visaient des lieux où des signes montraient une activité récente des LTTE[47], en dehors des zones de sécurité, et à l'écart des concentrations de tentes abritant des civils. Néanmoins, plus de dix cratères d'impact de frappes aériennes furent identifiés à proximité immédiate de concentrations de tentes abritant des civils et d'un hôpital en fonctionnement. L'endroit d'une frappe aérienne à l'intérieur de la zone de sécurité 2, en particulier, fut attesté à l'époque dans un rapport interne de l'ONU daté du 2 avril 2009[48]; il s'agissait des premières preuves émanant de sources indépendantes de frappes aériennes par le gouvernement à l'intérieur de la zone de sécurité 2, malgré l'interdiction explicite de tels actes et les dénégations du gouvernement sri-lankais à ce sujet[49]. Un journaliste qui était parvenu à se procurer ce rapport à Colombo réalisa un reportage évoquant ses principales conclusions, qui fut diffusé par la chaîne de télévision britannique Channel 4 ITN le 21 avril 2009. Le silence des autorités sri-lankaises à la suite de cette émission fut interprété, à l'époque, comme une confirmation tacite des conclusions du rapport[50].

Une analyse détaillée des batteries d'artillerie sri-lankaises situées dans l'ensemble de la zone de conflit constituait l'une des contributions importantes à l'enquête du Groupe d'experts. Le contrôle régulier de l'emplacement et de l'orientation des obusiers et des fosses à mortiers permit de constater que l'armée sri-lankaise orienta à plusieurs reprises son artillerie vers la zone de sécurité 2, puis vers la zone de sécurité 3, en suivant les mouvements des civils et des forces des LTTE lorsque celles-ci furent contraintes à gagner les parties méridionales d'une île-barrière à la fin du mois d'avril et au début du mois de mai 2009. Ces conclusions furent présentées au Groupe d'experts comme des preuves irréfutables du fait que l'armée sri-lankaise avait, tout au long des derniers mois du conflit, installé, maintenu et mis à niveau une capacité militaire opérationnelle lui permettant d'effectuer des tirs d'artillerie importants sur ces zones de sécurité, qui a l'époque accueillaient un grand nombre de civils[51].

Comme le montre l'image 8, des images ont aussi permis d'attester que l'armée sri-lankaise avait installé des batteries d'artillerie sur les territoires d'une école primaire et du principal hôpital de Puthukkudiyiruppu[52].

46 À la fin du mois de janvier 2009, les LTTE ne disposaient plus d'aucune capacité aérienne.

47 Parmi les exemples spécifiques de sites, on peut citer la construction de bermes défensives en terre et de tranchées, des activités de construction à proximité immédiate d'un couvert forestier dense près du front des combats, des formations armées visibles le long de routes et de plages et des petites embarcations partiellement enterrées sur les plages.

48 « Satellite-Detected Damages and IDP shelter Movement Report for March 2009 », document à diffusion interne aux Nations Unies, 2 avril 2009. Ce rapport précise que le site de frappe aérienne identifié se trouvait dans une partie de la zone de sécurité 2 où aucune tente servant d'abri aux civils n'était visible.

49 « Sri Lanka admits bombing safe zone », dans *Al-Jazeera,* 2 mai 2009, disponible sur : http://english.aljazeera.net/news/asia/2009/05/20095141557222873.html.

50 Vidéo disponible sur : http://link.brightcove.com/services/player/bcpid1529573111?bclid=20223644001&bctid=20379565001.

51 Voir les cartes d'analyse de la chronologie des tirs d'artillerie dans l'annexe au rapport du Groupe d'experts, *op. cit*., note 38.

52 Il est peu probable que ces établissements publics aient été en fonctionnement au moment des faits;

Image 8 : L'hôpital de Puthukkudiyiruppu (partiellement détruit) avec des mortiers de l'armée sri-lankaise visibles sur le territoire de l'hôpital en bas à gauche (17 juin 2009) (Image © GeoEye).

Contrairement à Gaza, où aucune preuve significative d'éventuelles violations du DIH commises par le Hamas durant le conflit n'a pu être produite, un ensemble significatif, bien qu'incomplet, d'éléments de preuve irréfutables a été réuni à l'encontre des Tigres de libération de l'Eelam tamoul pendant les dernières phases de la guerre civile. Non seulement il a été possible d'identifier des cas dans lesquels les LTTE avaient tactiquement déployé des installations d'artillerie à proximité de civils, utilisant apparemment ceux-ci comme des boucliers humains (ce qui constitue un crime de guerre), mais il fut également possible d'établir que les LTTE avaient à plusieurs reprises érigé des fortifications militaires (essentiellement des bermes et des tranchées) à proximité immédiate d'établissements médicaux, de sites religieux et d'autres abris remplis de civils, en violation du droit international, faisant ainsi courir à des civils des risques inutiles d'attaque militaire par les forces armées sri-lankaises.

Les preuves les plus flagrantes et complètes réunies contre les LTTE concernaient le positionnement délibéré de centaines de véhicules lourds, soupçonnés de contenir du matériel militaire, à l'intérieur de zones densément peuplées par des civils, ce qui revenait à utiliser ceux-ci comme des boucliers humains contre une

toutefois, l'école a été démolie par la suite et, à la fin de l'année 2010, il n'y avait aucun signe de reconstruction de l'hôpital.

attaque potentielle tout en les exposant au risque d'explosion du contenu des véhicules. Au matin du 16 mai 2009, à la fin du conflit, une énorme explosion de véhicules lourds des LTTE se produisit, entraînant la destruction totale par le feu d'une zone de près de 36 000 m^2 et détruisant quelque 200 tentes servant d'abri. Du fait de l'incertitude au sujet de la population civile estimée à l'intérieur de la zone de sécurité 3 au moment des faits, il ne fut pas possible d'estimer le nombre potentiel de morts ou de blessés civils causés par cette explosion[53].

Les satellites à la rescousse ?

Comme l'ont montrée les trois études de cas de Gaza, de la Géorgie et de Sri Lanka, l'analyse des images satellite peut souvent fournir des preuves indépendantes et irréfutables pour soutenir directement des enquêtes sur des crimes de guerre. Cependant, l'utilisation de l'imagerie à des fins de la vérification du respect du DIH se heurte à une série de limitations techniques, de difficultés d'analyse et de restrictions politiques, qu'il est impératif de mieux comprendre afin de ne pas nourrir des attentes excessives à l'égard de ce domaine passionnant de recherche appliquée dans le domaine de l'humanitaire.

Les limitations d'ordre technologique

Les capteurs électro-optiques des satellites présentent une limitation évidente : ils ne peuvent percer ni les nuages, ni un couvert forestier dense, et ils ne peuvent fonctionner de nuit, ce qui limite leur capacité d'évaluer ou de contrôler des conflits armés dans de nombreuses régions du monde, en termes géographiques comme en termes saisonniers. Si, par exemple, la guerre civile au Sri Lanka s'était achevée pendant la mousson orientale à la fin de l'année 2008 plutôt que durant la saison sèche au début de 2009, la couverture nuageuse constante n'aurait pas permis d'utiliser les capteurs électro-optiques aux fins d'une analyse détaillée du conflit.

Il existe une option alternative de plus en plus fiable dans de telles circonstances, à savoir la nouvelle génération de capteurs radar dits à synthèse d'ouverture, ou capteurs SAR, qui ne présentent pas les mêmes limitations liées aux conditions météorologiques que les capteurs électro-optiques traditionnels. Comme les capteurs SAR cartographient activement, ou illuminent le terrain au moyen d'ondes radar, il est aisé de recueillir des données pendant la nuit, à travers des nuages épais, et même, dans certaines circonstances, à travers une végétation dense. En matière d'enquête, les applications pertinentes pourraient inclure par exemple l'identification de zones de dommages importants aux bâtiments et d'effets sur l'environnement liés au conflit, ainsi que la localisation de

53 Cette explosion a été détectée par les capteurs de surveillance des incendies déjà utilisés pendant le conflit géorgien (2008).

concentrations importantes de civils déplacés, sur terre comme sur mer[54], ou encore le suivi de forces militaires classiques[55]. Malgré ces avantages considérables en termes de capacités, l'application pratique de données SAR à des fins de recherche par des institutions civiles et des ONG sur d'éventuelles violations du DIH a été limitée par plusieurs facteurs importants. L'interprétation et les méthodes de traitement traditionnelles des images employées couramment pour les images électro-optiques ne peuvent être aisément transposées à l'analyse des données SAR, du fait de la complexité des signatures radar. Les analystes dotés de ces compétences spécialisées sont encore essentiellement employés par les armées et les services de renseignement nationaux et de ce fait moins disponibles pour des recherches équivalentes dans le domaine civil. Les accords juridiques concernant le fonctionnement des capteurs SAR à très haute résolution étant encore souvent à utilisation duale (civile et militaire), les données sont non seulement nettement plus coûteuses, mais aussi potentiellement soumises à des restrictions politiques lorsqu'elles concernent des zones sensibles[56].

L'une des limites fréquentes, mais souvent mal comprise, des satellites à très haute résolution (qu'ils utilisent des capteurs électro-optiques ou SAR) est qu'ils ne récoltent pas des images de manière automatique et continue dans le monde entier; mais qu'ils sont plutôt utilisés pour des tâches précises au-dessus de zones qui présentent un intérêt particulier pour des raisons commerciales, politiques ou humanitaires. De ce fait, des conflits peu connus ou inattendus qui se produisent dans des zones isolées peuvent souvent échapper aux capteurs commerciaux durant des semaines ou des mois, ce qui fait que les images obtenues par la suite ne permettent pas de déceler des éléments de preuve pertinents relatifs au conflit. Au cours des cinq dernières années, les Nations Unies se sont heurtées à de multiples reprises à des cas où des demandes d'analyse d'images satellite d'incidents précis n'ont jamais été suivies d'effet, en raison de l'absence de couverture pertinente[57].

Les conflits asymétriques auxquels prennent part des forces irrégulières, comme à Gaza ou au Sri Lanka, continueront à présenter d'importantes difficultés techniques et analytiques. Du fait des limites de résolution des capteurs des satellites civils, il restera très difficile d'identifier les mouvements ou les actes de groupes

54 Les capteurs SAR sont particulièrement adaptés à la surveillance de la circulation des navires sur des étendues d'eau ouvertes, ce qui serait utile pour réaliser des études détaillées sur des circuits potentiels de traite d'êtres humains, ainsi que sur des déplacements de population forcés à grande échelle par voie maritime.

55 Rob Dekker *et. al.,* « Change detection tools », dans Bhupendra Jasani *et. al.* (éd.), *Remote Sensing from Space - Supporting International Peace and Security,* Springer, 2007, pp. 119-140.

56 Le capteur SAR allemand TerraSAR-X est soumis à la loi de 2007 relative à la sécurité des données recueillies par satellite, qui limite l'accès des civils aux données radar recueillies au-dessus de zones désignées comme sensibles. À l'heure où ces lignes sont écrites, on ignore dans quelle mesure cette politique a vraiment restreint dans la pratique l'accès aux données concernant des zones de conflit. Voir « German national data security policy for space-based earth remote sensing systems », 2010, disponible sur : http://www.oosa.unvienna.org/pdf/pres/lsc2010/tech-02.pdf. Voir aussi « PPP between DLR and Infoterra the SatDSiG-German Satellite Data Security Act », 2008, disponible sur: http://www.gwu.edu/~spi/assets/docs/PPP_DLR_SatDSiG-Datenpolicy_Bernhard.pdf.

57 Selon l'expérience de l'auteur au sein de l'UNITAR/UNOSAT (2005-2012).

insurgés irréguliers ou peu armés, qui ne possèdent pas ou ne sont pas en mesure de déployer des forces militaires conventionnelles ni des équipements aisément identifiables par satellite. Les petites unités de guérilla à l'œuvre dans des milieux urbains, sous camouflage ou sous un couvert végétal dense resteront en grande partie invisibles, ce qui pose un problème général de déséquilibre, puisque les actes des forces armées régulières sont suivis de manière nettement plus intensive[58].

La capacité de l'analyse des images satellite à identifier l'emploi de systèmes d'armement interdits restera limitée. C'est ainsi qu'en Géorgie, aucune preuve significative de l'emploi d'armes à sous-munitions par les forces russes dans la ville de Gori et aux alentours n'a pu être recueillie au moyen des images satellite, malgré des rapports de terrain détaillés de Human Rights Watch qui mentionnaient le moment approximatif et le lieu des attaques signalées[59]. Des questions fondamentales concernant l'emploi d'obus d'artillerie au phosphore blanc à Gaza par les FDI n'ont pas pu recevoir de réponse parce que l'imagerie ne permettait pas de se prononcer clairement; de ce fait, aucune conclusion n'a pu être tirée quant à l'éventuelle licéité de leur emploi.

L'une des limites les plus importantes aux évaluations de dommages au moyen des satellites demeure l'incapacité chronique de détecter les dégâts causés par les tirs au sol dus à des chars, à des roquettes et à des tirs d'artillerie à trajectoire tendue. Dans le cas de Tskhinvali, le nombre de bâtiments endommagés qui n'ont pas été recensés pour cette raison pourrait s'élever à plusieurs centaines pour l'ensemble de la ville, ce qui entraîne le risque de donner l'impression d'un biais politique contre les forces sud-ossètes, tout simplement parce que les dégâts causés par les incendies volontaires dont elles sont responsables ont été identifiés plus aisément et plus précisément. On peut conclure sans risque de se tromper que les cartes d'évaluation des dommages publiées à l'époque par les Nations Unies contenaient des degrés inégaux d'exactitude, les omissions étant concentrées précisément dans les parties de la ville les plus touchées par les bombardements du gouvernement géorgien pendant son offensive au début du mois d'août 2008. Malheureusement, il est peu probable que cette limitation spécifique soit surmontée dans un avenir proche, malgré les améliorations techniques que devraient connaître les capteurs.

58 Les seules informations recueillies concernant des actes potentiellement illégaux du Hamas à Gaza ont été l'identification et l'analyse par l'UNOSAT de dégâts causés à un mur de rétention d'une usine de traitement des eaux usées qui ont entraîné un écoulement massif sur une longueur de plus de 1200 mètres. Le rapport Goldstone est parti du principe que la responsabilité de cet événement incombait aux forces israéliennes, mais on ne dispose d'aucun témoignage direct et les éléments de preuve matériels sont très minces. Le gouvernement israélien a conclu, après avoir étudié la question, que même si une frappe aérienne accidentelle ne pouvait être entièrement exclue, cet acte aurait aussi pu être commis par le Hamas dans le cadre d'un plan défensif afin de gêner les déplacements des chars des FDI dans cette zone. Un tel acte pourrait constituer une violation du droit international coutumier tel que reflété dans l'article 56 du Protocole additionnel I et dans l'article 15 du Protocole additionnel II, qui interdisent la destruction d'installations contenant des forces dangereuses. Voir « Gaza operation investigations: an update », dans *Israeli Ministry of Foreign Affairs,* janvier 2010, para. 150‑164, disponible sur : http://www.mfa.gov.il/NR/rdonlyres/8E841A98-1755-413D-A1D2-8B30F64022BE/0/GazaOperationInvestigationsUpdate.pdf.

59 Basé sur la correspondance interne aux Nations Unies de l'auteur avec Human Rights Watch, août-septembre 2009.

Les difficultés de l'analyse : résultats ambigus, non concluant ou incertains

Il est essentiel de comprendre que les analyses détaillées des images satellite peuvent souvent aboutir à des conclusions ambiguës, grevées d'incertitude, voire politiquement contestées ou erronées. Rappelons, à titre d'exemple, les interprétations, largement discréditées, des images satellite présentées par le secrétaire d'État américain Colin Powell au Conseil de sécurité de l'ONU concernant la présence alléguée d'installations de fabrication d'armes chimiques et biologiques dans la période qui conduisit à la seconde guerre du Golfe[60]. Les analystes peuvent faire des erreurs ou, à partir de la même image, aboutir à des conclusions très divergentes; ils peuvent même modifier leurs conclusions sans en être conscients pour répondre aux attentes des utilisateurs ou des organisations. Cas de figure plus fréquent encore, les événements qui se déroulent sur le terrain peuvent être d'une grande complexité et rendre difficile la production d'informations pertinentes et significatives sur le conflit armé à partir des images fournies par les satellites.

Pendant la guerre civile au Sri Lanka, l'un des principaux défis fut la difficulté de confirmer les rapports faisant état de tirs de mortier à l'intérieur des zones de sécurité, qui constituaient de toute évidence une question éminemment pertinente pour l'enquête du Groupe d'experts. Les tactiques de survie, consistant à creuser des puits familiaux, des latrines, des abris contre les bombes, de même que la mobilité des tentes et les débris laissés sur place ont eu pour effet cumulatif de dissimuler fortement les signes caractéristiques de l'impact d'obus de mortier de petit et moyen calibre. Il est donc probable que les preuves de tirs d'artillerie aient été davantage masquées dans certaines zones en fonction du nombre relatif d'abris civils sous tente, avec pour résultat que c'est dans les zones de plus forte densité de population que les preuves de bombardements étaient les moins nombreuses.

Les incertitudes dans l'interprétation des images sont courantes dans des milieux complexes ou peu familiers, où la couverture temporelle des images disponibles n'est pas suffisante pour constater et reconstituer une série d'événements précis sur le terrain. De telles circonstances peuvent conduire à des interprétations multiples, dont chacune peut être également probable, laissant sans réponse des questions qui présentent un intérêt humanitaire direct. La comparaison de deux images satellite recueillies sur une zone donnée (avant et

60 Le rapport établi en 2004 par le Sénat des États-Unis sur les données de renseignement dont disposaient les États-Unis au sujet de l'Irak avant la guerre indique que, lorsque les analystes des images satellite parvenaient à des conclusions divergentes sur le sens à donner aux mouvements de véhicules à l'Institut Amiriyah des Sérums et des Vaccins, aucun mécanisme ou processus d'examen n'était prévu pour résoudre ces divergences, ce qui a eu pour effet d'inclure dans la présentation du Général Powell une interprétation erronée d'activités « inhabituelles ». Il semble, en outre, que les analystes pourraient avoir formulé leurs conclusions sur les emplacements des unités mobiles supposées de production d'agents d'armes biologiques de manière qu'elles correspondent aux renseignements fallacieux fournis par l'agent informateur dit « Curve Ball ». Voir « Report on the US Intelligence Community's Prewar Intelligence Assessments on Iraq », Sénat des États-Unis, 7 juillet 2004, pp. 244–256, disponible sur : http://web.mit.edu/simsong/www/iraqreport2-textunder.pdf.

après un événement) peut donner lieu à des scénarios ambigus en termes de causalité. L'objectif, en pareil cas, est de déterminer précisément ce qui s'est produit sur le terrain entre ces deux instantanés statiques. Lorsque l'analyse dépend d'une série d'images chronologiques très limitée - surtout si l'image « de référence » a été enregistrée des mois, voire des années plus tôt - il est probable que de multiples événements complexes se trouvent en quelque sorte amalgamés en une seule image statique éminemment ambiguë, qui est de peu d'utilité.

Pour prendre un exemple, l'une des questions fondamentales auxquelles l'on cherche à donner une réponse grâce à l'imagerie satellite, lorsque des informations font état de l'avancée de forces rebelles vers un camp de réfugiés, est de savoir si le camp a été attaqué ou non. Même si l'image prise après les faits supposés montre que les tentes servant d'abris ont disparu, elle ne contient pas nécessairement assez de détails pour établir avec un degré de confiance suffisant si les forces rebelles ont détruit les abris au cours d'une attaque, ou si les abris ont été démontés en toute hâte par les résidents fuyant avant l'attaque redoutée. Dans de telles circonstances complexes et faiblement documentées, le manque relatif d'images satellite suffisantes conduira généralement à des conclusions ambiguës et incertaines[61].

Comme le montrent les trois études de cas, il est souvent extrêmement ardu, voire potentiellement trompeur, d'attribuer une attaque à l'une des forces en présence en se fondant sur un examen limité aux signes de dommages relevés dans les images disponibles. Ainsi, les petits cratères d'impact identifiés sur les toits des hôpitaux ou dans les champs au Sri Lanka auraient pu, s'ils avaient été tirés de leur contexte plus large, être attribués à l'une ou l'autre des parties au conflit. Même pour des faits de plus grande ampleur, comme l'explosion massive qui a marqué les dernières heures de la guerre civile au Sri Lanka, les images peuvent contenir des indices ambigus ou peu significatifs ne permettant pas d'attribuer la responsabilité à l'une des parties.

Les restrictions politiques et l'avenir

Depuis que le gouvernement des États-Unis a décidé, en 1994, d'autoriser la commercialisation de techniques essentiellement militaires, l'accès public aux images satellite à très haute résolution et la prolifération de capteurs nouveaux toujours plus performants ont progressé sans interférence ou restriction politique majeure[62]. Il reste cependant une exception notable qui continue à limiter les effets de l'imagerie satellite sur des zones de conflit importantes au Moyen-Orient. En 1997, le gouvernement des États-Unis a promulgué une loi interdisant

61 Un risque clairement associé au recours de plus en plus fréquent à l'imagerie satellite par la communauté humanitaire et par les ONG est que des groupes pourraient, par manque d'expérience, par excès de zèle ou par désir de confirmer leurs attentes, publier des informations sans tenir compte de ce facteur d'incertitude ou sans le communiquer de façon adéquate aux utilisateurs finaux, ce qui risque d'entraîner des erreurs de jugement par précipitation, à l'exemple de la présentation au Conseil de sécurité des Nations Unies, en février 2003, d'interprétations d'images satellite par Colin Powell, à l'époque secrétaire d'État des États-Unis.

62 Voir Y.A. Dehqanzada et A.M. Florini, *op. cit.,* note 1.

la vente ou la diffusion d'images satellite d'une résolution spatiale inférieure à deux mètres récoltées au-dessus d'Israël, de la bande de Gaza, de la Cisjordanie, du Plateau du Golan, ainsi que d'une zone tampon de cinq kilomètres à l'intérieur des frontières avec l'Égypte, la Syrie et le Liban[63].

Cette restriction a été ressentie de manière directe pendant le conflit à Gaza en 2009, car elle a contraint les prestataires de services satellite commerciaux à dégrader systématiquement les images recueillies au-dessus de la bande de Gaza à 25 % à peine de leur résolution originale. Toute l'activité de contrôle et d'analyse réalisée par les Nations Unies pour la communauté humanitaire au sujet de Gaza - et en particulier pour la mission Goldstone - était fondée sur des images de qualité dégradée, ce qui a fortement compromis le degré général de précision et de fiabilité. Bien qu'aucune tentative n'ait été faite pour quantifier ces conséquences, ce fait a presque certainement entraîné une sous-estimation systématique de presque toutes les formes de dommages aux bâtiments et aux infrastructures dans l'ensemble de la bande de Gaza.

Bien que, juridiquement, cette restriction ne s'applique qu'aux capteurs des satellites américains, les gouvernements des États-Unis et d'Israël ont, jusqu'à une date récente, réussi à passer des accords bilatéraux avec les sociétés de satellites européennes et asiatiques pour qu'elles appliquent des restrictions similaires[64]. L'une des conséquences visibles des tensions diplomatiques récentes entre la Turquie et Israël est que les satellites turcs GökTürk-1 et GökTürk-2, qui doivent être déployés prochainement, pourraient commencer en 2013 à capter et à diffuser des images d'une résolution spatiale inférieure à un mètre de l'ensemble des territoires israéliens et palestiniens[65]. Si tel devait être le cas, on ne saurait exclure que la restriction imposée par les États-Unis soit révisée, voire abandonnée.

L'une des conséquences politiques potentielles de l'emploi des technologies satellites pour la surveillance et l'analyse des conflits est la volonté croissante que manifestent un grand nombre d'États membres des Nations Unies appartenant au Groupe des 77 de limiter la production et la publication de recherches basées sur l'imagerie satellite concernant des dossiers brûlants en matière de droits de l'homme et de DIH. Certains programmes des Nations Unies ont de fait subi des pressions résultant de directives récentes adoptées par leur organisation qui restreignent de plus en plus la diffusion publique d'informations acquises par satellite sur les conflits armés et sur les grandes situations d'urgence humanitaire[66].

63 National Defence Authorisation Act for Fiscal Year 1997, Gouvernement des États-Unis, 23 septembre 1996, Sec. 1064.

64 « Turkey dismisses Israel's concerns over satellite », dans *Reuters,* 11 mars 2011, disponible sur : http://www.reuters.com/article/2011/03/11/turkey-israel-satellites-idUSLDE72A1VM20110311. Voir aussi « Götürk - project of reconnaissance and surveillance satellite system », Turkish Air Force, disponible sur : http://www.hvkk.tsk.tr/EN/IcerikDetay.aspx?ID=167&IcerikID=154.

65 *Ibid.*

66 Basé sur des échanges de correspondance internes aux Nations Unies et sur des entretiens privés avec des collègues des Nations Unies (2005-2012).

Il est difficile de dire si ces tentatives politiques, au sein du système des Nations Unies, de restreindre l'emploi des technologies satellite auront un effet négatif, à long terme, sur la capacité des Nations Unies de mener des enquêtes. En revanche, il ne fait aucun doute qu'à brève échéance, la communauté humanitaire et des droits de l'homme, au sens large, fera de plus en plus souvent appel aux compétences techniques et analytiques nécessaires pour mener ses propres activités indépendantes de surveillance et d'analyse des conflits par satellite.

Volume 94 Sélection française 2012/2

REVUE INTERNATIONALE

RAPPORTS ET DOCUMENTS

Le droit international humanitaire et les nouvelles technologies de l'armement, XXXIVe table ronde sur les sujets actuels du droit international humanitaire, San Remo, 8-10 septembre 2011

Discours d'ouverture de Jakob Kellenberger, Président du CICR, et Conclusions par Philip Spoerri, Directeur du droit international et de la coopération au CICR

: : : : : : :

Discours d'ouverture de Jakob Kellenberger, Président, Comité international de la Croix-Rouge*

Les nouvelles technologies et les nouvelles armes ont révolutionné la conduite de la guerre depuis des temps immémoriaux. Il suffit de se rappeler l'invention du chariot, de la poudre à canon, de l'aéronautique ou de la bombe nucléaire pour comprendre combien les nouvelles technologies ont modifié la façon dont on fait la guerre.

* Disponible sur : http://www.icrc.org/fre/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm

Depuis la Déclaration de Saint-Pétersbourg de 1868 qui a interdit l'emploi de projectiles de moins de 400 grammes, la communauté internationale s'est efforcée de réglementer les nouvelles technologies utilisées dans la conduite de la guerre. Et le droit international humanitaire moderne s'est à de nombreux égards développé en réponse aux nouveaux défis posés par l'émergence d'armes nouvelles.

La Déclaration de Saint-Pétersbourg a interdit un type d'arme précis, mais elle a aussi établi un certain nombre de principes généraux sur lesquels allait reposer plus tard toute l'approche adoptée par le droit international humanitaire face aux nouveaux moyens et méthodes de guerre. Elle dit en effet que le seul but légitime que les États doivent se proposer, durant la guerre, est l'affaiblissement des forces militaires de l'ennemi, et que ce but serait dépassé par l'emploi d'armes qui aggraveraient inutilement les souffrances des hommes mis hors de combat ou voudraient leur mort inévitable.

C'est dans cet esprit que la réglementation des moyens et méthodes de guerre s'est développée tout au long des 150 dernières années, en suivant deux voies : par l'adoption, d'une part, de **règles et principes généraux s'appliquant à tous les moyens et méthodes de guerre**, partant du principe que les lois de l'humanité imposent des limites quant à leur choix et leur emploi ; et par la conclusion, d'autre part, d'**accords internationaux interdisant ou limitant l'emploi de certaines armes**, telles que les armes chimiques et biologiques, les armes incendiaires, les mines antipersonnel ou encore les armes à sous-munitions.

Les règles et principes généraux protègent les combattants contre les armes qui sont de nature à causer des blessures superflues ou des souffrances inutiles, mais ils ont aussi été établis dans le but de protéger les civils des effets des hostilités. C'est ainsi, par exemple, que les moyens et méthodes de guerre dont les effets sont indiscriminés sont interdits.

Partant de ces interdictions générales essentielles, le droit international humanitaire a été conçu de façon suffisamment souple pour pouvoir s'adapter aux évolutions technologiques, y compris à celles qui étaient inenvisageables à l'époque. Et il ne fait aucun doute que le droit international humanitaire s'applique aux nouvelles armes et à toutes les nouvelles technologies utilisées pour la guerre. L'article 36 du Protocole additionnel I le reconnaît explicitement quand il dit que dans l'étude, la mise au point ou l'adoption d'une nouvelle arme ou d'une nouvelle méthode de guerre, les États parties ont l'obligation de déterminer si l'emploi en serait interdit, dans certaines circonstances ou en toutes circonstances, par une règle du droit international qui leur est applicable.

Cela étant, l'application de règles juridiques préexistantes à une technologie nouvelle soulève la question de savoir si ces règles sont suffisamment claires au vu des caractéristiques spécifiques – et peut-être sans précédent – de cette technologie, et également au vu de l'impact humanitaire qu'elle peut avoir dans un avenir prévisible. Dans certaines circonstances, les États choisiront, ou ont déjà choisi, d'adopter des règles plus spécifiques.

Notre époque est celle des technologies de l'information, et on le voit, ces technologies sont aussi utilisées pour se battre. Ce n'est pas entièrement nouveau, mais la multiplication des nouvelles armes ou méthodes de guerre qui dépendent

de ces technologies semble exponentielle. Les mêmes progrès des technologies de l'information qui nous permettent d'avoir des conversations vidéo sur nos téléphones portables permettent également de construire des drones plus petits, moins chers et plus polyvalents. La même technologie qui nous permet de commander à distance l'air conditionné de notre maison permet également de plonger dans le noir une ville située à l'autre bout du monde.

La table ronde de cette année va nous permettre de regarder de plus près certaines des technologies qui commencent tout juste à être utilisées pour faire la guerre, ou qui sont susceptibles de l'être, et à en discuter. Je pense en particulier à la cybertechnologie, aux systèmes d'armement télécommandés et aux armes robotisées.

Je commencerai par la « **guerre informatique** ».

On s'interroge beaucoup aujourd'hui sur les problèmes juridiques que pose la guerre informatique, ou « cyberguerre ». Quand je parle de guerre informatique, je fais référence aux moyens et méthodes de guerre qui font appel aux technologies de l'information et qui sont employés dans un contexte de conflit armé. Le potentiel militaire du cyberespace commence à peine à être exploré. Nous savons, à partir de certaines cyberopérations qui ont été menées, qu'une partie au conflit peut « attaquer » les systèmes informatiques d'une autre partie, en s'y infiltrant ou en les manipulant. L'infrastructure informatique dont dépend l'arsenal militaire de l'ennemi peut ainsi être endommagée, désorganisée ou détruite. Mais les infrastructures civiles peuvent aussi être touchées, soit parce qu'elles sont directement visées ou parce qu'elles sont incidemment endommagées ou détruites alors que ce sont les infrastructures militaires qui sont visées.

Au jour d'aujourd'hui, nous ne savons pas avec précision quelles pourraient être les conséquences d'une guerre informatique du point de vue humanitaire. Techniquement parlant, des cyberattaques contre le contrôle du trafic aérien et d'autres modes de transport, des barrages ou des centrales nucléaires, sont possibles. De telles attaques auraient très vraisemblablement des conséquences humanitaires de grande ampleur. Elles pourraient faire de nombreuses victimes civiles et d'énormes dégâts. Bien sûr, il est pour l'instant difficile de connaître le degré de probabilité de cyberattaques d'une telle gravité, mais nous ne pouvons pas nous permettre d'attendre qu'il soit trop tard pour prévenir les pires scénarios.

Du point de vue humanitaire, le principal problème que posent les cyberopérations dans un contexte de guerre vient du fait que le cyberespace est interconnecté ; il est de ce fait même difficile de limiter les effets de ces attaques aux seuls systèmes informatiques militaires. Même si certaines infrastructures informatiques militaires sont sécurisées et indépendantes des infrastructures civiles, beaucoup d'infrastructures militaires dépendent d'ordinateurs ou de réseaux informatiques civils. Dans de telles conditions, comment l'attaquant peut-il prévoir les répercussions de son attaque sur les systèmes informatiques civils ? Il est fort probable que le système ou le réseau informatique dont dépend l'infrastructure militaire soit le même que celui dont dépend l'hôpital voisin ou le réseau d'approvisionnement en eau.

Une autre raison pour laquelle il est difficile d'appliquer les règles du droit international humanitaire au cyberespace vient du fait qu'il repose sur une architecture numérique. La numérisation garantit l'anonymat et complique l'attribution de telle ou telle conduite. C'est ainsi que dans la plupart des cas, il s'avère difficile, sinon impossible, d'identifier l'auteur d'une attaque. Comme le DIH est basé sur l'attribution de responsabilité à des personnes et à des parties à un conflit, cela pose d'énormes problèmes. En effet, s'il est impossible d'identifier l'auteur d'une opération et, de ce fait, d'établir le lien entre l'opération et le conflit armé, il est extrêmement difficile de déterminer l'applicabilité ou non du DIH à l'opération en question.

La deuxième innovation technologique dont nous parlerons à cette table ronde concerne les **systèmes d'armement télécommandés**.

Les systèmes d'armement télécommandés constituent une étape supplémentaire d'une stratégie de longue date qui consiste à éloigner de plus en plus les soldats de leurs adversaires et du champ de bataille.

Les drones – ou véhicules aériens sans pilote (UAV : *unmanned aerial vehicles*) – constituent l'exemple le plus marquant de ces nouvelles technologies, qu'ils soient armés ou non. Leur nombre s'est accru à un rythme exponentiel ces dernières années. De la même façon, les véhicules terrestres sans pilote sont de plus en plus présents sur les champs de bataille. Ils vont du robot qui sert à détecter et à détruire des bombes au bord des routes, jusqu'au robot qui inspecte les véhicules à l'approche d'un poste de contrôle.

Un des principaux arguments avancés pour défendre l'investissement dans ces nouvelles technologies est qu'elles préservent la vie des combattants. Un autre argument est que les drones, en particulier, ont une meilleure capacité de surveillance aérienne en temps réel et qu'ainsi les belligérants peuvent attaquer avec plus de précision les objectifs militaires, réduisant de ce fait les victimes civiles et les dommages aux biens de caractère civil. En d'autres termes, ils peuvent faire preuve de davantage de précaution dans l'attaque.

On peut néanmoins s'inquiéter de la façon dont ces systèmes sont dirigés et par qui. Pour commencer, ils sont parfois commandés par des civils, qui peuvent être des employés de sociétés privées. Ce cas pose la question du statut et de la protection de ces opérateurs ; il conduit aussi à se demander si leur formation et leur responsabilité sont suffisantes au vu des décisions qu'ils prennent, lesquelles sont des questions de vie ou de mort. En second lieu, des études ont montré que si on déconnecte une personne, en l'éloignant notamment (physiquement ou émotionnellement) d'un adversaire potentiel, il lui est plus facile de le prendre pour cible et de commettre des abus. L'historien militaire John Keegan appelle cela la « dépersonnalisation de la bataille ».

Enfin, je voudrais dire quelques mots des **armes robotisées**.

Les **armes automatisées** – ou robots en langage courant – vont plus loin que les systèmes télécommandés. Elles ne sont pas dirigées à distance, mais fonctionnent de façon autonome et indépendante, une fois lancées. C'est notamment le cas des mitrailleuses SG autonomes, des munitions autodirectrices et de certaines mines terrestres antivéhicule. Bien que déployés par des humains, ces sys-

tèmes vont identifier ou détecter de façon indépendante un type de cible donné puis tirer ou exploser. Une mitrailleuse SG autonome par exemple fera feu ou non après vérification du mot de passe prononcé par un intrus potentiel.

Le problème majeur que posent les systèmes automatisés est leur capacité à respecter le niveau de discrimination exigé par le DIH. Cette capacité de discrimination va entièrement dépendre de la qualité et de la diversité des capteurs et de la façon dont le système est programmé. Jusqu'à présent, la façon dont ces systèmes pourraient faire la différence entre un civil et un combattant, ou entre un combattant blessé ou hors de combat et un combattant actif, n'est pas claire. Et la façon dont ces armes pourraient évaluer la perte accidentelle en vies humaines, les blessures infligées aux civils ou les dégâts pour des objets civils, et ainsi respecter le principe de proportionnalité, ne l'est pas plus.

Une autre étape consisterait à déployer des **systèmes d'armement autonomes**, c'est-à-dire des systèmes d'armement qui peuvent analyser ou adapter leur fonctionnement en fonction d'un changement de circonstances. Un système véritablement autonome serait doté d'une intelligence artificielle qui devrait être capable de mettre en œuvre le DIH. Bien que ce domaine suscite un grand intérêt et que la recherche soit largement financée, ces systèmes n'ont pas encore été adaptés aux armements. Développer de tels systèmes est un tel défi en termes de programmation que ce sera peut-être impossible. Il est clair que le déploiement de tels systèmes représenterait une véritable révolution conceptuelle et un changement qualitatif majeur dans la conduite des hostilités. Mais il soulèverait aussi tout un ensemble de problèmes fondamentaux du point de vue légal, éthique et sociétal, et ces problèmes doivent être pris en compte avant que ces systèmes ne soient développés ou déployés. Un robot pourrait être programmé de façon à se comporter de façon plus éthique et plus prudente qu'un être humain sur le champ de bataille. Mais que faire si, du point de vue technique, il est impossible de réaliser une programmation fiable d'un système d'armement autonome de façon à garantir qu'il respecte le DIH sur le champ de bataille?

À l'occasion du débat sur ces nouvelles technologies, il nous faut voir également quels sont les avantages qu'elles pourraient apporter si elles contribuaient à une **meilleure protection**. Respecter les principes de distinction et de proportionnalité signifie qu'il faut prendre certaines **précautions dans l'attaque**, comme indiqué à l'article 57 du Protocole additionnel I. Cet article prévoit notamment l'obligation pour un attaquant 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. Dans certains cas, les cyberopérations ou le déploiement d'armes télécommandées ou de robots pourraient faire incidemment moins de victimes civiles et causer moins de dommages aux biens de caractère civil que l'emploi d'armes classiques. Des précautions accrues devraient également être possibles dans la pratique, du fait simplement que ces armes sont déployées depuis suffisamment loin et souvent, avec suffisamment de temps pour que la cible soit choisie avec soin et que le

moment de l'attaque soit décidé de façon à minimiser l'impact sur la population civile et les biens de caractère civil. On pourrait considérer que dans de telles circonstances, l'application de cette règle voudrait qu'un commandant évalue s'il peut obtenir le même avantage militaire en utilisant ces moyens et méthodes de guerre, s'ils sont applicables.

Le monde des nouvelles technologies n'est pas un monde virtuel et ne relève pas non plus de la science-fiction. Dans les conflits armés, les nouvelles technologies peuvent tuer et causer des dommages très réels. Conscient de leurs conséquences possibles du point de vue humanitaire, le CICR considère qu'il est important d'encourager le débat sur ces questions, d'attirer l'attention sur la nécessité d'évaluer l'impact humanitaire des technologies naissantes, et de veiller à ce que celles-ci ne soient pas utilisées de façon prématurée dans des circonstances où le respect du droit ne peut être assuré. La préoccupation qui a conduit à la Déclaration de Saint-Pétersbourg est tout aussi impérieuse aujourd'hui qu'elle l'était alors.

REVUE INTERNATIONALE de la Croix-Rouge

Conclusions par Philip Spoerri, Directeur du droit international et de la coopération, Comité international de la Croix-Rouge*

Lors de cette conférence, les groupes d'experts ont abordé une myriade de nouvelles technologies : armes à impulsions, drones, robots, technologie des satellites, armes spatiales et cybertechnologie. Certaines d'entre elles sont déjà déployées sur les champs de bataille modernes, d'autres relèvent encore de la science-fiction.

Les discussions ont fait ressortir bon nombre de grands thèmes qui donnent à réfléchir et demanderaient des recherches et des réflexions plus approfondies. Il ne m'est guère possible de résumer tous ces thèmes, mais je voudrais souligner cinq aspects qui semblaient récurrents.

Premièrement, nos discussions ont révélé un certain degré **d'incertitude quant aux faits**. On ne sait pas toujours clairement ce qui est techniquement possible dans les théâtres de guerre d'aujourd'hui, et encore moins ce qui le sera à l'avenir et quand. On ne sait pas non plus exactement quel est l'impact humanitaire des armes qui *sont déjà* déployées, comme les drones ; de celles qui sont *prêtes à être déployées*, comme les cyberattaques ; ou de celles qui pourraient être déployées à l'avenir, comme les robots autonomes. Dans quelle mesure cette incertitude entrave-t-elle notre capacité à s'assurer que les nouvelles technologies utilisées dans la conduite de la guerre sont toutes conformes au droit international humanitaire ? Même si l'incertitude eu égard aux spécificités et à l'impact de certaines de ces technologies n'est pas sans poser un problème quant au droit applicable à ces technologies, il n'y a pas lieu, me semble-t-il, de surestimer ce problème.

Dans la guerre informatique (cyberguerre), par exemple, l'anonymat et l'interconnexion des réseaux informatiques du monde entier semblent soulever des questions très graves sur l'évolution du droit international humanitaire dans l'infosphère. Des échanges plus nombreux entre scientifiques et juristes sont nécessaires pour que la clarté puisse être faite sur ces questions. Par ailleurs, il ne semble y avoir aucun doute sur le fait que les cyberattaques sont d'ores et déjà possibles et peuvent avoir des effets dévastateurs sur les civils et l'infrastructure civile, en provoquant par exemple la désorganisation des systèmes de contrôle aérien ou des réseaux d'approvisionnement en électricité ou en eau. La plupart d'entre nous comprennent peu ou prou comment fonctionne la technologie de l'information, et pourtant, nous connaissons déjà un certain nombre de choses et nous sommes déjà capables de dire quels effets seraient licites ou non, s'ils se produisaient. La plupart d'entre nous ne savent pas comment piloter des avions, mais connaissent les effets des bombardements aériens. En ce sens, *nous devrions nous concentrer sur les effets de la technologie que nous observons aujourd'hui dans la conduite de la guerre* (« *dans le monde réel* »), et il est probable que nous serions en mesure de donner des avis motivés sur l'applicabilité du droit

* Disponible sur : http://www.icrc.org/fre/resources/documents/statement/new-weapon-technologies-statement-2011-09-13.htm

international humanitaire et la légalité des moyens et méthodes spécifiques de la conduite de la guerre dans le cyberespace.

Deuxièmement, le fait que **les nouvelles technologies éloignent les combattants toujours plus du champ de bataille** a été un sujet de discussion récurrent. De nombreux intervenants ont souligné que le fait que les combattants soient éloignés les uns des autres n'est pas fondamentalement nouveau. Pourtant, il ressort aussi clairement qu'une des caractéristiques communes aux nouvelles technologies examinées est qu'elles agrandissent la distance, que ce soit au moyen de systèmes d'armements télécommandés, de cyberarmes ou de robots.

Les conséquences de ces moyens et méthodes de guerre à distance nécessitent une réflexion plus poussée. Tout d'abord, quel est l'impact de leur utilisation sur la définition, l'étendue du champ de bataille ? D'aucuns ont fait valoir que si les drones pouvaient être utilisés ou les cyberattaques lancées de partout dans le monde, le monde entier deviendrait alors un champ de bataille. Cela reviendrait à adhérer au concept de « champ de bataille mondial » avec pour conséquence que l'utilisation des règles relatives à l'emploi de la force causant incidemment des pertes en vies humaines dans la population civile et des dommages civils au regard du principe de proportionnalité relevant du droit international humanitaire s'étendrait bien au-delà de la portée acceptée à ce jour. Le CICR n'adhère pas à cette notion.

Les moyens et méthodes de guerre à longue distance soulèvent aussi quelques questions quant à la relation entre, *d'une part, l'emploi des nouvelles technologies de manière à garder les combattants hors d'état de nuire, en limitant leur exposition au combat direct, et d'autre part leur impact humanitaire pour la population civile.* Il est sans doute impossible de dire si l'éloignement des combattants par rapport au champ de bataille constituera en soi un risque accru pour les civils. Il est à craindre que, vu l'aversion au risque de bon nombre de sociétés et de gouvernements pour la vie de leurs militaires, la tendance vers des « guerres sans victime » conduira à choisir des armes en fonction de cette seule préoccupation, et ce, même au détriment des règles du droit international humanitaire qui protège les civils contre les effets des hostilités. À l'instar des bombardements à haute altitude qui pourraient être plus sûrs pour les combattants, mais aussi dans certaines circonstances indiscriminés et illégaux, il importe que les nouvelles technologies, bien que protectrices pour les troupes, soient toujours testées quant à leur compatibilité avec le droit humanitaire et en particulier quant à leurs possibles effets indiscriminés ou disproportionnés. Il faut, cependant, que nous ayons une meilleure compréhension des effets de ces technologies, notamment de leur précision et de leurs effets connexes, non seulement en termes technologiques abstraits mais surtout par rapport à leur utilisation concrète.

Cela m'amène à un troisième point, à savoir un certain **manque de transparence quant aux effets de certaines armes sur la population civile** – non pas sur leur effet potentiel futur, mais sur l'effet des technologies déjà utilisées. Il existe, par exemple, une controverse sur les effets des drones : personne ne semble connaître avec certitude les pertes de vies parmi la population civile, les blessures aux civils et les dommages aux infrastructures civiles qui ont été

provoqués par des attaques de drones. Sans connaissance objective, il est extrêmement difficile d'apprécier la licéité de ces armes ou la manière dont elles sont utilisées dans des conditions particulières. Il serait bon à cet égard que l'enregistrement des conséquences humanitaires liées à l'utilisation des nouvelles technologies soit transparent, il tiendrait alors compte non seulement des spécificités techniques abstraites mais intégrerait aussi la manière concrète dont les technologies sont utilisées.

Mais comme nous avons pu l'entendre, les **nouvelles technologies peuvent effectivement être aussi des outils qui contribuent à une plus grande transparence, favorisant la mise en évidence et l'enregistrement des violations ainsi que les enquêtes y afférentes.** Nous avons entendu un exposé très intéressant en rapport avec les images satellites utilisées par l'UNITAR (Institut des Nations Unies pour la formation et la recherche) pour enquêter sur les violations perpétrées lors des conflits armés. D'autres technologies viennent à l'esprit : par exemple, la technologie de l'ADN, qui peut quelquefois compléter les méthodes traditionnelles de la science médico-légale, ou des dispositifs simples, comme des caméras de téléphone portable, qui ont servi à enregistrer des violations. Les limites liées à l'utilisation d'images pour illustrer ou prouver des violations lors d'un conflit armé, en particulier des crimes de guerre, n'est pas chose nouvelle, et il est bien connu que les images parlent rarement d'elles-mêmes. Mais les nouvelles technologies – avec des moyens traditionnels, en particulier les récits de témoins – peuvent contribuer à découvrir certaines violations, et cela mérite assurément d'être salué.

Le quatrième thème récurrent portait sur la **responsabilité et l'obligation redditionnelle en matière de déploiement de nouvelles technologies.** Il reste à voir si les nouvelles technologies permettront de réduire notre capacité à déterminer la responsabilité et l'obligation redditionnelle en cas de violations. Pour commencer, rappelons que les parties aux conflits sont liées par le droit international humanitaire (États et groupes armés) et que le droit pénal international lie les individus. Comme nombre d'intervenants l'ont signalé, je ne suis pas convaincu que nous en ayons fini avec l'obligation de répondre de nos actes lors de l'utilisation d'armes autonomes. Même si l'intelligence artificielle devait être activée et les systèmes autonomes être déployés dans les conflits armés, les robots ne seraient-ils pas dans une certaine mesure toujours actionnés par l'homme ? Si tel est le cas, la personne en question – et la partie au conflit – sont responsables de la décision prise, quelle que soit la distance temporelle et spatiale avec laquelle l'arme aurait pu être déployée lors de l'attaque. Cela me fait penser au poème de Goethe « l'apprenti sorcier » *(Der Zauberlehrling)* qui a mis en marche un balai par la capacité destructrice de l'intelligence artificielle et des drones (UAV = *unmanned aerial vehicules,* véhicules aériens sans pilote). L'apprenti et le magicien lui-même portaient sans doute une part de responsabilité et le magicien fut finalement contraint de mettre sa maison en ordre. Dans le cyberespace, par contre, la répartition des responsabilités semble pouvoir être juridiquement contestée si l'anonymat est la règle plutôt que l'exception.

Enfin, le thème le plus récurrent a été peut-être que la **technologie n'est, en soi, ni bonne ni mauvaise. Elle peut être une source de bien et de progrès ou au pire entraîner des conséquences désastreuses**. Cela est vrai dans la plupart des cas. Mais quand il s'agit de transposer cette affirmation aux technologies de l'armement, cela signifie que la plupart des armements en tant que tels ne seraient pas illicites ; la licéité de leur utilisation dans des conflits dépend des circonstances et de la manière dont ces technologies sont utilisées.

Cela dit, certaines armes ne sont jamais licites et elles ont été interdites, citons par exemple les armes à laser aveuglantes ou les mines terrestres. Il en est de même pour les nouvelles technologies : la licéité des nouveaux moyens et des nouvelles méthodes de conduite de guerre dépendra surtout de leur utilisation, mais il n'est pas exclu que certaines armes seront considérées comme indiscriminées par nature ou susceptibles de causer des dommages ou des souffrances superflus, auquel cas, elles devront être interdites. C'est pourquoi le principe énoncé à l'article 36 du Protocole I additionnel aux Conventions de Genève au titre duquel les États ont l'obligation de vérifier, lors de l'élaboration de nouveaux moyens et de nouvelles méthodes de guerre, si leur emploi serait compatible avec le droit international humanitaire est si capital.

Nous sommes capables de tirer les leçons du passé – par exemple de l'expérience du déploiement de la bombe nucléaire – mais nous avons du mal à anticiper les problèmes et les catastrophes auxquels nous pourrions avoir à faire face à l'avenir. De l'avis de certains, les robots ou autres nouvelles technologies pourraient signifier la fin de la guerre. Si des robots se battent contre des robots dans l'espace sans entraîner d'autre effet sur l'homme que de possibles pertes économiques, nous reviendrions au temps des chevaliers qui se battaient en duel dans un pré carré loin de la ville, bref, nous serions dans un conte de fées sans rapport avec la guerre. Un tel scénario est assurément plus qu'improbable, il nous faut donc nous concentrer sur un scénario plus réaliste selon lequel les technologies utilisées dans les conflits armés serviront à nuire à l'ennemi, et le dommage qu'elles causeront ne se limitera pas à des objectifs purement militaires, il touchera les civils et les infrastructures civiles.

N'ayons donc pas exagérément peur de ce qui risque de ne pas se produire – tel a été le credo de nombreux orateurs, ici à San Remo. Restons néanmoins vigilants et ne manquons pas l'occasion de rappeler, chaque fois que cela est nécessaire, que les règles fondamentales du droit international humanitaire ne sont pas juste un code moral flexible. Ce sont des règles contraignantes, et à ce jour, le seul outil juridique dont nous disposons pour réduire ou limiter, au moins dans une certaine mesure, le coût humain de la guerre. Une réunion multidisciplinaire, telle cette table ronde, constitue un excellent moyen pour avancer vers cet objectif.

REVUE
INTERNATIONALE
de la Croix-Rouge

La version originale de la *Revue internationale de la Croix-Rouge* est publiée en anglais quatre fois par an, au printemps, en été, en automne et en hiver.

Une sélection annuelle d'articles est publiée au niveau régional en arabe, chinois, espagnol, français et russe.

Les articles publiés dans la *Revue* sont accessibles gratuitement en ligne sur le site: www.icrc.org/fre/resources/international-review

Présentation des manuscrits

La *Revue internationale de la Croix-Rouge* sollicite des articles sur des sujets touchant à la politique, à l'action et au droit international humanitaires. La plupart des numéros sont consacrés à des thèmes particuliers, choisis par le Comité de rédaction, qui peuvent être consultés sur le site web de la *Revue* dans la rubrique «Futurs thèmes de la *Revue internationale de la Croix-Rouge*». Les contributions portant sur ces sujets sont particulièrement appréciées.

Les articles peuvent être rédigés en anglais, arabe, chinois, espagnol, français et russe. Les articles choisis sont traduits en anglais, si nécessaire.

Les articles ne doivent pas avoir été publiés, présentés ou acceptés ailleurs. Ils font l'objet d'un examen collégial; la décision finale de les publier est prise par le rédacteur en chef. La *Revue* se réserve le droit d'en réviser le texte. La décision d'accepter, de refuser ou de réviser un article est communiquée à l'auteur dans les quatre semaines suivant la réception du manuscrit. Les manuscrits ne sont pas rendus aux auteurs.

Les articles peuvent être envoyés par courriel à:
review@icrc.org

Règles de rédaction
L'article doit compter entre 5 000 et 10 000 mots. Les textes plus courts peuvent être publiés dans la section «Commentaires et opinions».

Pour de plus amples informations, veuillez consulter les Informations à l'intention des auteurs et les Règles de rédaction, notes de bas de page, citations et questions de typographie sur le site web de la *Revue*:
www.icrc.org/fre/resources/international-review

Sélection française

Dès 2011, la *Revue internationale de la Croix-Rouge* publiera deux à quatre sélections françaises thématiques par année. Leurs contenus rassembleront une sélection d'articles parmi ceux figurant dans les quatre numéros annuels de la version anglaise de la *Revue internationale de la Croix-Rouge* (*International Review of the Red Cross*).

Les commandes de Sélection française doivent être faites via le eShop du CICR, à l'adresse suivante:
https://shop.icrc.org/publications/international-humanitarian-law.html

Photo de couverture: des habitants afghans regardent un robot durant une opération de déminage.
© Umit Bektas, Reuters

Recherche de photos:
Fania Khan Mohammad, CICR

Guerre et nouvelles technologies

Volume 94 Sélection française 2012/2

REVUE
INTERNATIONALE
de la Croix-Rouge

CICR
ISSN 1560-7755
4191/001

www.icrc.org/fre/resources/international-review