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.