

Les facteurs permettant de déterminer les conséquences juridiques liées à l'utilisation de systèmes militaires toujours plus autonomes

Tim McFarland*

Tim McFarland est candidat au doctorat à l'*Asia Pacific Centre for Military Law* (centre Asie Pacifique de droit militaire) à la Faculté de droit de l'Université de Melbourne. Il poursuit ses études de troisième cycle au sein de l'équipe de recherche travaillant sur le projet portant sur les technologies de guerre émergentes et leurs enjeux par rapport au droit des conflits armés.

Résumé

Cet article identifie cinq facteurs permettant de déterminer les conséquences juridiques de l'utilisation de systèmes militaires autonomes. Il soutient que les systèmes présentant des enjeux juridiques sont ceux qui sont programmés pour « prendre des décisions » réglementées par le droit. Ce faisant, ils transfèrent le contrôle ainsi que la responsabilité de ces décisions loin de ceux qui sont traditionnellement considérés comme étant les décideurs, vers les personnes chargées de développer et de déployer ces systèmes. L'article suggère également qu'il peut y avoir des limites dans la mesure où les règles du droit international humanitaire peuvent réglementer de manière adéquate la relation modifiée entre les soldats et leurs systèmes d'armement de plus en plus autonomes.

Mots clés : DIH, systèmes d'armement autonomes, mise au point d'armes, droit relatif aux armes, technologie militaire.



* L'auteur aimerait remercier ses supérieurs, le Professeur Tim McCormack et le Dr Rain Liivoja, ainsi que le Colonel d'aviation Ian Henderson, pour leurs commentaires constructifs sur différentes versions de cet article. La recherche relative à cet article a été soutenue par le programme de financement du *Australian Research Council's Discovery Project*.

Introduction

Il est de notoriété publique que plusieurs États mettent au point activement des systèmes militaires qui recourront à des technologies avancées afin de soutenir, de compléter, voire de remplacer les soldats humains dans des fonctions de combat. Les efforts de développement actuellement en cours ont notamment permis de créer des engins capables de reproduire quelques-unes des fonctions assurées, entre autres, par les pilotes de chasse¹ et les sentinelles², et il semble inévitable que les capacités de ces systèmes militaires continueront de se développer dans des secteurs habituellement du domaine réservé des opérateurs humains. Ces systèmes, communément appelés « autonomes³ », promettent de grands changements opérationnels dans la conduite des hostilités au cours des prochaines décennies. Cette perspective suscite par conséquent l'intérêt des juristes travaillant dans le champ des conflits armés.

Au-delà de la difficulté habituelle à obtenir des informations fiables sur les développements militaires, les analyses juridiques initiales des systèmes proposés ont relevé deux enjeux importants auxquels sont confrontés ceux qui tentent de faire coïncider ces systèmes avec le droit international humanitaire (DIH). D'abord, le sujet abordé est un sujet extrêmement technique, dont il peut découler des problèmes juridiques liés à la nature d'un ensemble de technologies, en particulier celles ayant trait à la robotique et à l'intelligence artificielle. En plus de constituer des sujets spécialisés allant bien au-delà du domaine traditionnel d'expertise des juristes, l'état des connaissances dans ces domaines avance rapidement. Ainsi, toute analyse juridique détaillée présente le risque de devenir obsolète avant même d'avoir pu être menée à son terme. Ensuite, à quelques exceptions près, les systèmes utilisés jusqu'à présent semblent ne posséder qu'une très faible capacité d'autonomie, généralement en-deçà du seuil nécessaire pour soulever des questions juridiques importantes. Les plans publiés ne fournissent que des descriptions générales des formes que prendront les systèmes plus avancés, des technologies qui les piloteront et de la manière dont ils seront utilisés. Les engins qu'il est possible d'évaluer aujourd'hui, comme le système d'arme de combat rapproché Phalanx (*Phalanx Close-In Weapon System*)⁴ ou les missiles utilisant un système de guidage terminal dynamique et des technologies similaires⁵, ne sont que le prélude des capacités qui pourront être observées dans les systèmes autonomes futurs.

- 1 Lockheed Martin, « UCLASS », disponible sur : <https://www.lockheedmartin.com/en-us/capabilities/autonomous-unmanned-systems.html> (toutes les références Internet ont été vérifiées en octobre 2018).
- 2 Kumagai, « A Robotic Sentry for Korea's Demilitarized Zone », *IEEE Spectrum*, 1^{er} mars 2007, disponible sur : <http://spectrum.ieee.org/robotics/military-robots/a-robotic-sentry-for-koreas-demilitarizedzone>.
- 3 Il ne s'agit pas ici d'armes télécommandées telles que les véhicules aériens sans pilote ou les drones, actuellement utilisés dans plusieurs conflits. Ces appareils sont contrôlés manuellement par des opérateurs humains dans le respect de leurs fonctions essentielles. S'il est vrai que les véhicules autonomes n'ont généralement pas d'équipage, cet article ne traite que des enjeux découlant de la capacité de la machine à « prendre des décisions » de façon autonome.
- 4 Raytheon, « Phalanx Close-In Weapon System (CIWS) », disponible sur : www.raytheon.com/capabilities/products/phalanx/.
- 5 Pour un aperçu de ces technologies, voir Groupe consultatif pour la recherche et les réalisations aérospatiales, Organisation du Traité de l'Atlantique Nord (OTAN), *Precision Terminal Guidance for Munitions*, Rapport consultatif n° AGARD-AR-342, février 1997, disponible sur : www.cso.nato.int/Pubs/rdp.asp?RDP=AGARD-AR-342.

En grande partie en raison de l'incertitude qui entoure les capacités potentielles de systèmes hautement autonomes, de nombreuses questions importantes demeurent sans réponse quant à leur comptabilité avec le DIH existant. Il est essentiel que ces questions soient traitées dans un avenir proche ; l'ampleur des changements attendus dans la conduite des hostilités nécessite à tout le moins d'effectuer une enquête préventive. De plus, le fait que les échéances liées à leur développement ne soient pas connues introduit un certain degré d'urgence. Par ailleurs, il s'agit d'une opportunité tout à fait inhabituelle pour les juristes de se préparer à l'avènement d'une nouvelle technologie militaire, voire d'influencer le développement de nouveaux systèmes avant leur déploiement, plutôt que de tenter de remédier à leur mauvaise utilisation après coup.

Cet article jette les bases d'une analyse systématique des questions pouvant se poser en termes du DIH, en raison de l'utilisation de systèmes militaires autonomes. Il ne s'agit pas ici d'effectuer une analyse juridique exhaustive, mais seulement d'offrir une discussion sur certains aspects, susceptibles d'être les plus importants, liés à l'autonomie des engins, ainsi que de proposer des orientations afin d'identifier les problèmes juridiques potentiels, dans le but de livrer à ceux qui le souhaiteraient une base qui leur permettra d'approfondir chacun de ces enjeux plus en détail. La caractéristique essentielle de cette approche est de centrer l'analyse juridique sur les décisions et les actions des personnes développant et travaillant avec des systèmes autonomes, plutôt que sur les capacités opérationnelles de ces engins. Mais avant toute chose, deux choix terminologiques doivent être expliqués.

Premièrement, alors que la plupart des discussions et des questions juridiques les plus controversées portent spécifiquement sur les armes autonomes, cet article fait référence de manière plus générale aux « systèmes militaires autonomes ». Dans ce contexte, le terme « système » peut désigner tout élément matériel ou tout logiciel, ou tout ensemble fait de composants matériels et/ou de logiciels qui effectuent une tâche définie. Un avion qui n'a pas d'équipage ou une arme telle qu'une tourelle, est un système aux fins de cet article, mais il en est de même pour un réseau de capteurs répartis sur une large zone, ou pour une « cyber-arme⁶ », ou encore pour un logiciel d'analyse de données qui accompagne un commandant dans ses prises de décisions. Le terme « système » peut, *grosso modo*, être considéré comme un synonyme de « moyens de guerre⁷ », dans la mesure où cette expression est utilisée dans divers instruments juridiques⁸. Ce choix a été opéré en raison du fait que, tel qu'expliqué

6 Une cyberarme est un logiciel et/ou du matériel « utilisé, conçu ou destiné à être utilisé [traduction CICR] » pour conduire « une cyber opération offensive ou défensive raisonnablement susceptible de blesser ou de tuer des personnes, ou d'endommager ou de détruire des biens » : Michael N. Schmitt (dir.), *Manuel de Tallinn sur l'applicabilité du droit international à la guerre cybernétique*, Cambridge University Press, Cambridge, 2013, pp. 106 (Règle 30), 141 (Règle 41).

7 Il est possible que l'utilisation d'un système militaire autonome puisse également faire référence à une méthode de guerre, par exemple lorsque le processus menant à la décision d'employer le système est en cause, ou lorsque le système détient plus d'un mode d'opération. Pour un exemple du second cas, voir : *ibid.*, p. 142, par. 4-5.

8 Voir, par exemple, Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977, 1125 UNTS 3, entré en vigueur le 7 décembre 1978, Titre III.

ci-dessous, les technologies en question sont susceptibles d'être intégrées à du matériel et à des logiciels militaires qui ne seraient normalement pas considérés comme de l'armement, mais qui pourraient tout de même influencer les opérations de combat de manière similaire aux capacités autonomes d'une arme. Par exemple, lorsque vient le temps de prendre une décision de mise à feu, un système de renseignement, de surveillance et de reconnaissance (RSR) autonome, utilisant des capteurs montés sur des drones, des satellites, des navires ou toute autre plateforme permettant de collecter et de traiter des informations sur des cibles potentielles avant de les fournir à un opérateur d'armes humain, peut jouer un rôle similaire à celui d'un système de prise de décisions autonome intégré au système d'armement lui-même.

Deuxièmement, contrairement à ce qui semble devenir une pratique courante, cet article ne fait pas de distinction entre les systèmes « automatisés » et les systèmes « autonomes ». De manière très générale, les systèmes sont décrits comme étant « automatisés » lorsqu'ils ne peuvent exécuter que des tâches rudimentaires en l'absence d'assistance extérieure, ou lorsqu'ils sont enfermés dans une routine opérationnelle répétitive et rigide définie par des procédures programmées de manière permanente. Ils sont au contraire dénommés « autonomes » lorsqu'ils peuvent recevoir des instructions de niveau supérieur et lorsqu'ils exercent un certain degré de « choix », ou sont dotés de la capacité de « prendre des décisions », afin de déterminer la manière d'exécuter ces instructions⁹. Cet article soutient qu'une telle distinction est artificielle, qu'elle manque de précisions et qu'elle est de ce fait inutile dans le cadre d'une analyse juridique. Les capacités précises propres à chacun des systèmes ne tombent pas clairement dans des catégories données ; au contraire, ces capacités existent dans un continuum de plusieurs dimensions et il faut s'attendre à ce que les capacités des systèmes dépassent les limites des définitions actuelles, lorsque les technologies pertinentes se seront davantage développées. Ainsi, les juristes qui souhaitent dégager des principes juridiques durables devraient éviter de les formuler en termes de catégories qui sont susceptibles de changer, et l'approche présentée ici évite justement ce piège. De plus, la distinction repose sur des notions anthropomorphiques d'engins prenant des décisions, exerçant un pouvoir discrétionnaire et accomplissant, en quelque sorte, davantage que la simple exécution d'un programme. Bien que ces termes offrent des métaphores utiles à des fins techniques, d'un point de vue juridique ils ne décrivent pas de manière fidèle le fonctionnement réel des systèmes en question, et peuvent se révéler trompeurs s'ils sont employés dans le cadre d'une discussion juridique. Tous les systèmes pouvant être décrits comme « automatisés » ou « autonomes » ne sont encore que des engins, construits ou programmés dans le but de décharger un opérateur de certaines décisions ou actions qui, autrement, auraient été effectuées manuellement. Ce point est discuté plus en détails ci-dessous.

La principale conclusion présentée ici tient au fait que les juristes devraient évaluer les systèmes « autonomes », non pas selon leur capacité à agir avec un certain

9 Il existe, cependant, un important désaccord à propos des définitions précises, même au sein de la communauté technique ; voir, par exemple, l'analyse in M. Shane Riza, *Killing Without Heart: Limits on Robotic Warfare in an Age of Persistent Conflict*, Potomac Books, Washington, DC, 2013, p. 13.

degré d'indépendance, ni même selon qu'ils affichent ou non certains comportements semblables à ceux de l'être humain, mais selon les décisions qui leur sont déléguées et la manière dont les opérateurs humains s'en remettent à eux. À cet égard, les systèmes qui devraient intéresser les juristes sont ceux qui dispensent les humains de prendre des décisions ou des actions qui sont réglementées par le droit et qui, ce faisant, transfèrent un certain contrôle et une certaine part de responsabilité liés à ces décisions d'un opérateur manuel vers une autre partie. Partie qui pourrait être celle qui définit le comportement du système ou celle qui est responsable de son utilisation.

Cet article est composé de trois sections. La première aborde trois aspects de l'autonomie des engins, lesquels sont pertinents dans le cadre d'une analyse juridique des systèmes militaires proposés. La deuxième analyse deux aspects des propositions de développement qui ont été présentées par des organisations militaires. La troisième expose, quant à elle, en quoi les développements proposés sont en lien avec le DIH et propose des orientations aux personnes souhaitant analyser des questions juridiques spécifiques : se rappeler que la responsabilité pour les décisions ayant un impact juridique important incombe aux humains, comprendre que la nature de ces décisions change lorsqu'on travaille avec des systèmes autonomes et veiller à ce que les questions juridiques et techniques soient distinguées.

Aspects de l'autonomie des engins, importants pour une analyse juridique

Une évaluation rationnelle des conséquences de la création d'armes « autonomes » doit se fonder sur une compréhension claire de ce qu'est réellement l'autonomie d'un engin. Dans le cadre d'une analyse juridique, il n'est pas essentiel d'étudier dans le détail les moyens techniques permettant d'aboutir à un comportement autonome. Il est bien plus important de définir avec précision de quelle manière les capacités autonomes affecteront les interactions entre ces systèmes et le reste du monde, en particulier en ce qui concerne les interactions avec les opérateurs, les superviseurs et ceux qui sont soumis aux effets de ces systèmes.

Malheureusement, alors que le principe d'autonomie peut ne pas sembler ambigu de prime abord, il est difficile de saisir pleinement la notion à l'aide d'une seule définition¹⁰. En effet, ce concept comporte plusieurs significations, assez différentes, se retrouvant dans divers domaines d'étude. Dans le cas présent, il est utilisé dans un sens strictement technique, mais même au sein de la littérature technique relative à l'autonomie des engins, il semble exister presque autant de définitions que d'auteurs qui s'essayent à le définir. Il est néanmoins possible d'affirmer que la plupart des définitions portent essentiellement sur deux aspects interdépendants de l'autonomie. Certaines définitions se concentrent sur la manière dont un opérateur interagit avec le système : selon ces définitions, les systèmes autonomes sont ceux pouvant opérer « sans aucune forme de contrôle extérieur sur de longues périodes de

10 Voir, par exemple, l'analyse *in* Henry Hexmoor, Christiano Castelfranchi et Rino Falcone, « A Prospectus on Agent Autonomy », *in* Henry Hexmoor, Christiano Castelfranchi et Rino Falcone (dir.), *Agent Autonomy*, Kluwer, Boston, MA, 2003, p. 3.

temps [traduction CICR]¹¹ ». D'autres formulent le problème au regard des capacités inhérentes au système : l'autonomie est alors « la capacité d'un système de choisir et de décider, avec certaines limites qui lui sont propres, son propre comportement [traduction CICR]¹² ». Évidemment, ces définitions, comme d'autres, ne font que couvrir une partie des facettes de l'autonomie des engins et ne présentent un intérêt que pour certains objectifs spécifiques ; les juristes souhaitant mener une enquête doivent donc également déterminer quels aspects sont pertinents dans le cadre qui est le leur. Au lieu de fournir une autre définition (qui serait inévitablement incomplète), cette section tente d'orienter le lecteur en présentant une vue d'ensemble de la façon dont l'autonomie des engins est atteinte en pratique, pour discuter ensuite des aspects des systèmes autonomes susceptibles d'être les plus importants au plan juridique dans un contexte militaire. Il s'agit également des aspects qui devraient être gardés à l'esprit par les juristes qui étudient les propositions de développement. En particulier, tel qu'expliqué ci-dessous, il est inexact de considérer ce processus comme relevant simplement du développement de l'armement¹³.

La façon dont l'autonomie est atteinte

L'analyse débute par une explication basique de la façon dont fonctionne un système d'armement autonome. Les concepteurs représentent généralement les systèmes autonomes comme étant composés de deux éléments principaux : la « centrale », qui est le système, ou le processus, devant être contrôlé, et le « contrôleur », qui est le dispositif régissant directement le comportement de la « centrale »¹⁴. Le terme « centrale » est repris du domaine du génie chimique ; dans un contexte militaire, il s'agit de l'installation qui, si elle n'est pas capable de fonctionner de manière autonome, serait directement contrôlée par un humain, à l'image d'un véhicule ou d'une tourelle. Le contrôleur d'un système autonome est composé du matériel et du logiciel qui, tout en suivant un programme fourni par un développeur, gèrent le véhicule, l'arme ou tout autre dispositif¹⁵. Les schémas 1 et 2 fournissent un aperçu conceptuel de la façon

- 11 George A. Bekey, *Autonomous Robots: From Biological Inspiration to Implementation and Control*, MIT Press, Cambridge, MA, 2005, p. 1. De la même façon, « un système doté d'un haut degré d'autonomie est un système pouvant être négligé sur une longue période de temps sans interaction [traduction CICR] » : Michael A. Goodrich et Alan C. Schultz, « Human-Robot Interaction: A Survey », *Foundations and Trends in Human-Computer Interaction*, vol. 1, n° 3, 2007, p. 217.
- 12 Charles François (dir.), *International Encyclopedia of Systems and Cybernetics*, vol. 1, K. G. Saur, Munich, 2004, p. 51. De la même façon, « l'autonomie est une capacité (ou un ensemble de capacités) permettant qu'une action particulière d'un système soit automatique ou, au sein de limites programmées, de s'"auto-gérer" [traduction CICR] » : Defense Science Board, *The Role of Autonomy in DoD Systems*, US Department of Defense (département de la Défense des États-Unis), juillet 2012, p. 1, disponible sur : www.acq.osd.mil/dsb/reports/AutonomyReport.pdf.
- 13 La pertinence quant à la catégorisation des systèmes autonomes en tant qu'armes est également abordée Hin-Yan Liu, « Categorization and Legality of Autonomous and Remote Weapons Systems », *Revue internationale de la Croix-Rouge*, vol. 94, n° 886, 2012, p. 627.
- 14 Voir, par exemple, Zdzislaw Bubnicki, *Modern Control Theory*, Springer, Berlin et New York, 2005, pp. 3-4.
- 15 Pour une introduction générale aux systèmes de contrôle général, voir Panos J. Antsaklis, Kevin M. Passino et S. J. Wang, « An Introduction to Autonomous Control Systems », *IEEE Control Systems*, vol. 11, n° 4, 1991, p. 5.

dont ces composantes fonctionnent ensemble dans des systèmes commandés manuellement ainsi que dans des systèmes autonomes. Les flèches pleines représentent les interactions typiques entre les différents éléments. Ces schémas ne se rapportent pas à des systèmes d'armement spécifiques ; ils ne font que décrire la fonctionnalité générique de chaque type de système.

Il est désormais possible de discuter de plusieurs aspects concernant l'autonomie des machines afin d'éclairer une analyse juridique.

Schéma 1 : Système d'armement manuel

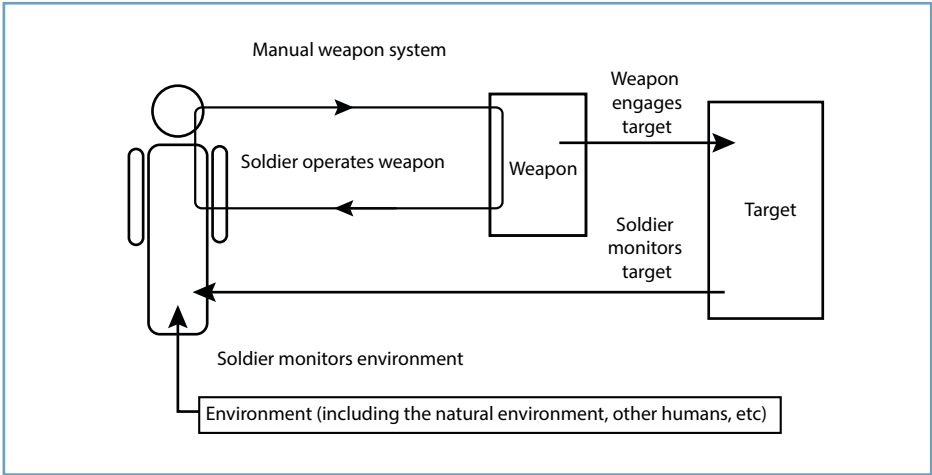
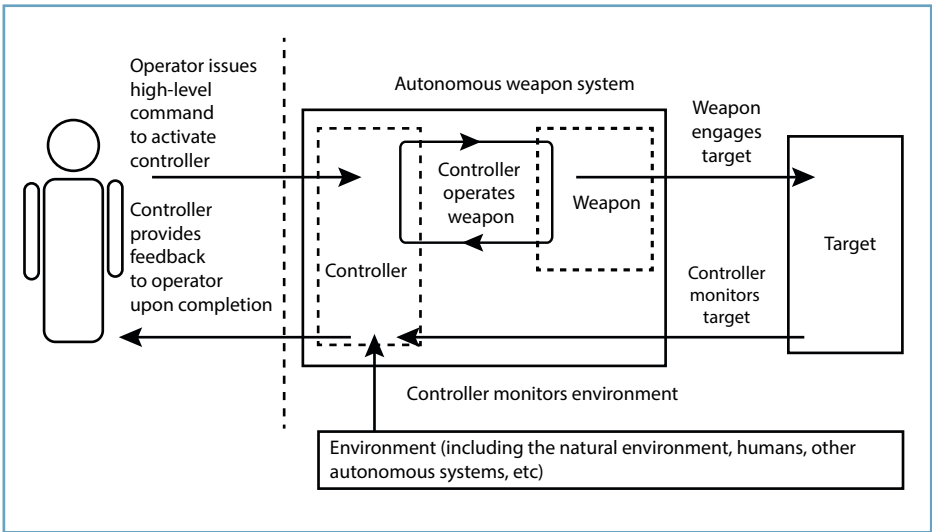


Schéma 2 : Système d'armement autonome



L'autonomie n'est ni fixe ni uniforme

Les juristes ont pour habitude de désigner les armes autonomes comme étant une catégorie distincte de dispositifs qui pourraient être aisément différenciées des systèmes non-autonomes et de se référer au « degré » d'autonomie qu'un système particulier présente, comme si de tels degrés d'autonomie étaient des propriétés intrinsèques à chaque système particulier¹⁶. Cette distinction simpliste ne reflète pas l'éventail des capacités des systèmes existant aujourd'hui et ne correspond pas au développement des feuilles de route¹⁷ rendues publiques par différentes forces armées. En réalité, on peut s'attendre à ce que les niveaux d'autonomie que présentent les systèmes militaires proposés varient de manière complexe.

De la même manière que la répartition des tâches entre un opérateur et un système autonome varie, les degrés d'autonomie possibles fluctuent considérablement. Ainsi, il faut s'attendre à ce que le comportement d'un système varie en fonction de la tâche spécifique qui doit être exécutée et des circonstances dans lesquelles il est exploité. Établir les degrés de contrôle exercés par un opérateur humain et par un système de contrôle informatique vis-à-vis d'une action particulière, que ce soit ou non à des fins juridiques, peut s'avérer être un processus complexe. L'objectif des brèves descriptions faisant l'objet de cette section n'est pas de fournir au lecteur toutes les connaissances techniques nécessaires afin d'entreprendre une telle démarche, elles servent plutôt à démontrer la nature subjective du contrôle des tâches dans un environnement où des humains doivent interagir avec des systèmes autonomes avancés.

Le degré de contrôle informatique

L'autonomie des engins n'est pas une caractéristique se définissant par « tout ou rien » ; il existe plutôt un continuum allant d'un contrôle humain complet exercé sur une fonction à un contrôle complet exercé par la machine. De nombreuses manières de décrire ce continuum ont été proposées¹⁸. L'une des plus connues, qui reconnaît dix degrés d'automatisation, est reproduite dans le tableau 1. Une fois encore cependant, ces « degrés » sont simplement des façons de décrire des étapes d'un continuum ; en réalité, il n'existe pas de degrés distincts pour l'autonomie des machines.

Le *US National Institute of Standards and Technology* a mis au point une taxonomie légèrement plus complexe, à savoir le cadre ALFUS¹⁹ (*Autonomy Levels for Unmanned Systems* : Degrés d'autonomie pour les systèmes sans pilote [traduction

16 Voir, par exemple, Markus Wagner, « Taking Humans Out of the Loop: Implications for International Humanitarian Law », *Journal of Law, Information and Science*, vol. 21, n° 2, 2011.

17 Voir, par exemple, Army Capabilities Integration Center, *US Army, Robotics Strategy White Paper*, 19 mars 2009, disponible sur : www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA496734 ; US Air Force, *Unmanned Aircraft Systems Flight Plan 2009-2047*, 18 mai 2009, disponible sur : www.fas.org/irp/program/collect/uas_2009.pdf.

18 Peter A. Hancock et Stephen F. Scallen, « Allocating Functions in Human-Machine Systems », in Robert R. Hoffman, Michael F. Sherrick et Joel S. Warm (dir.), *Viewing Psychology as a Whole: The Integrative Science of William N Dember*, American Psychological Association, Washington, DC, 1998, p. 521.

19 NIST Engineering Laboratory, National Institute of Standards and Technology, *Autonomy Levels for Unmanned Systems*, 16 juin 2010, disponible sur : www.nist.gov/el/isd/ks/autonomy_levels.cfm.

CICR]). Le cadre ALFUS qualifie les niveaux d'autonomie à l'aide d'un modèle tridimensionnel, qui fonctionne en termes de complexité de la mission, de complexité environnementale et d'indépendance vis-à-vis d'un opérateur humain, chacun de ces trois facteurs étant eux-mêmes décomposés en séries de considérations d'un niveau inférieur.

Tableau 1 : Les dix degrés d'automatisation de Sheridan et Verplank

Contrôle humain à 100%	<ol style="list-style-type: none"> 1. L'humain accomplit tout le travail jusqu'au point où il le cédera à l'ordinateur afin qu'il le mette en œuvre. 2. L'ordinateur aide en déterminant les options. 3. L'ordinateur aide à déterminer les options et en suggère une, que l'humain n'est pas obligé de suivre. 4. L'ordinateur sélectionne l'action et l'humain peut choisir de l'exécuter ou non. 5. L'ordinateur sélectionne l'action et la met en œuvre si l'humain l'approuve. 6. L'ordinateur sélectionne l'action et informe l'humain avec un délai suffisamment long pour qu'il puisse l'arrêter s'il le souhaite. 7. L'ordinateur accomplit l'entièreté du travail et informe systématiquement l'humain de ce qu'il a fait. 8. L'ordinateur accomplit l'entièreté du travail et informe l'humain de ce qu'il a fait seulement si l'humain le demande explicitement. 9. L'ordinateur accomplit l'entièreté du travail et informe l'humain de ce qu'il a fait seulement s'il estime²⁰ que l'humain devrait en être informé.
Contrôle informatique à 100%	<ol style="list-style-type: none"> 10. L'ordinateur accomplit l'entièreté du travail s'il décide que cela devrait être fait et informe l'humain seulement s'il estime que l'humain devrait en être informé.

Source : Thomas B. Sheridan et William L. Verplank, *Human and Computer Control of Undersea Teleoperators: Technical Report*, Massachusetts Institute of Technology, 1978, pp. 8–17.

D'autres organisations ont proposé des taxonomies alternatives aux degrés d'autonomie destinées à remplir divers objectifs, à l'image du modèle à huit niveaux de la NASA pour son outil SMART²¹ (*Spacecraft Mission Assessment and Re-planning Tool*) et du modèle à onze niveaux de la *US Army Science Board* découlant de son étude sur les problèmes d'interface « homme-robot²² ».

Il n'est pas nécessaire de s'appesantir davantage sur ces modèles relativement détaillés. Il est simplement important de souligner qu'il est inutile de tenter de décrire

20 En l'espèce, « décider » n'implique pas une capacité de prise de décision similaire à celle d'un humain ; cela signifie seulement que l'action est initiée par l'ordinateur en fonction de sa programmation plutôt qu'en réponse à une commande provenant de l'opérateur humain.

21 Ryan W. Proud, Jeremy J. Hart et Richard B. Mrozinski, *Methods for Determining the Level of Autonomy to Design into a Human Spaceflight Vehicle: A Function Specific Approach*, NASA Johnson Space Center septembre 2003, p. 4, disponible sur : www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA515467.

22 US Army Science Board, *Ad-hoc Study on Human Robot Interface Issues*, septembre 2002, p. 16, disponible sur : www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA411834.

un engin comme étant autonome, semi-autonome ou contrôlé manuellement, comme s'il s'agissait de catégories distinctes et objectives. L'autonomie est un phénomène en constante variation.

Les méthodes d'interaction « homme-machine » et la répartition des tâches

Même les systèmes hautement autonomes, qui n'ont pas nécessairement besoin d'une contribution humaine significative dans l'accomplissement des tâches qui leur sont assignées, vont opérer aux côtés d'autres entités, qui peuvent aussi bien être humaines qu'électroniques, et devront échanger des informations avec ces entités afin de recevoir des instructions, de coordonner leurs efforts, de rapporter les résultats, etc. L'étude de l'interaction « homme-machine » et, plus récemment, celle de l'interaction « homme-robot », sont des domaines multidisciplinaires qui ont fait l'objet d'une attention considérable et croissante au cours des deux dernières décennies, à mesure que se développaient les capacités informatiques et robotiques²³. Plusieurs paradigmes alternatifs ont émergé dans le but de décrire comment cette interaction peut être structurée et comment les tâches peuvent être réparties entre les différentes entités, avec des retombées sur les rôles que jouent les humains. De manière très générale, lorsqu'ils travaillent avec des systèmes autonomes, les humains peuvent occuper des rôles de contrôle ou de collaboration et peuvent échanger ces rôles au cours de l'exécution d'une série de tâches. Par exemple, une taxonomie répertorie cinq rôles pouvant être exercés par les humains lorsqu'ils œuvrent avec des robots : superviseur, opérateur, mécanicien, pair et spectateur²⁴. Ces rôles peuvent ne pas être statiques ; un paradigme de conception, désigné comme étant une interaction à initiative mixte, « se réfère à une stratégie d'interactions flexible dans laquelle chaque agent peut contribuer à la tâche en accomplissant ce qu'il sait faire le mieux » [traduction CICR]²⁵. Dans le paradigme de l'initiative mixte, les rôles respectifs de l'homme et de l'ordinateur (ou du robot) sont rarement déterminés à l'avance, mais sont « négociés » en fonction de l'évolution des circonstances. Selon les moments, l'opérateur humain ou la machine peut détenir un contrôle direct sur une tâche, pendant que l'autre l'assiste, ou bien ils peuvent travailler de manière indépendante.

L'interaction entre l'homme et le robot est un champ de recherche actif recelant sans cesse de nouveaux principes émergents. Bien qu'il soit raisonnable de supposer que les humains continueront collectivement d'exercer un contrôle élevé sur les armes robotisées employées lors d'un conflit armé, les juristes devraient faire preuve de prudence au moment d'évaluer les rôles et le degré de contrôle exercés par certaines personnes en particulier.

23 Pour un aperçu, voir M. Goodrich et A. Schultz, *op. cit.* note 11.

24 Jean Scholtz, « Theory and Evaluation of Human Robot Interactions », in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, Hawaii, 6-9 janvier 2003.

25 Marti A. Hearst, « Trends & Controversies: Mixed-Initiative Interaction », *IEEE Intelligent Systems*, vol. 14, n° 5, 1999, p. 14.

Les variations relatives aux fonctions

Il est fréquent de parler de l'autonomie comme étant la caractéristique d'un système dans son ensemble, mais, en pratique, les technologies contribuant à une capacité d'exploitation autonome seront, et sont, appliquées à des sous-systèmes spécifiques faisant partie du matériel et des logiciels militaires. En ce qui concerne les systèmes robotiques, le développement se déroule de façon différente dans les domaines de la navigation autonome, du ciblage autonome et de toute autre fonctionnalité requérant un système d'armement avancé. Alors que des systèmes dotés d'une plus grande capacité d'exploitation autonome seront développés au cours des prochaines années, il n'y a aucune raison de penser que toutes leurs fonctionnalités seront sujettes au même degré de supervision humaine directe ; il est probable que certaines fonctionnalités, notamment celles pour lesquelles l'analyse coût/bénéfice de l'automatisation sera, d'une certaine manière, plus favorable, seront fabriquées de façon à être « plus autonomes » que d'autres. Un système peut donc fonctionner simultanément à plus d'un « degré » d'autonomie par rapport à des tâches différentes, et les juristes examinant de tels systèmes devront évaluer leur comportement, ainsi que les degrés d'implication humain et informatique, en lien avec des fonctionnalités spécifiques, lesquelles pourront porter, entre autres, sur la planification, la navigation ou l'autorisation de tirs.

En examinant de plus près par exemple la procédure de ciblage en six étapes, utilisée par la *Australian Defense Force*²⁶, il se pourrait que des systèmes d'armement dotés de la capacité de localiser et d'observer de manière autonome des cibles potentielles, voire peut-être de prendre certaines précautions afin de minimiser les dommages collatéraux, ne soient pas considérés comme étant fiables lorsque vient le temps de libérer une arme de manière autonome. Dans de tels cas, un opérateur humain ou d'autres systèmes autonomes pourraient s'avérer nécessaires afin d'évaluer si la cible est bien un objectif militaire et si les dommages collatéraux attendus pourraient être excessifs par rapport à l'avantage militaire attendu²⁷. Si un tel système se trouvait impliqué dans un incident faisant l'objet d'une enquête dont l'objectif serait de déterminer ce qui a pu conduire au ciblage d'un civil, il serait important d'établir à quel stade une erreur a pu se glisser. Une fois ceci établi, il resterait alors à constater quels étaient les degrés de contrôle humain et informatique, dans le but de déterminer si un opérateur humain exerçait à ce moment-là un contrôle tel qu'il puisse être tenu pour pénalement responsable. Des considérations similaires seraient également applicables dans une situation de « système à systèmes » impliquant une communication entre différents systèmes possédant différents degrés d'autonomie.

26 Ian Henderson, *The Contemporary Law of Targeting*, Martinus Nijhoff, Boston, MA, et Leiden, 2009, p. 237.

27 Pour une discussion plus détaillée sur la manière dont un équilibre entre contrôle humain et exploitation autonome peut être atteint à différentes étapes du processus de ciblage, voir Mark Roorda, « NATO's Targeting Process: Ensuring Human Control Over and Lawful Use of "Autonomous" Weapons », Amsterdam Center for International Law Research Paper n° 2015-06, 2015, disponible sur : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2593697.

Les variations en fonction des circonstances

Alors que les fonctions d'un système autonome se réfèrent aux tâches que le système accomplit, les circonstances renvoient aux situations dans lesquelles il exécute ces tâches. Tel que mentionné ci-dessus, même lorsqu'un concepteur a déterminé qu'une fonction appartenant à un système particulier sera soumise à un certain degré de contrôle par ordinateur, ce niveau peut varier en fonction des circonstances, lesquelles peuvent consister en :

- la phase d'une mission, telle que la planification, l'initiation, la mise en œuvre ou la conclusion ;
- un événement perturbateur, par exemple lorsqu'un véhicule aérien sans pilote (UAV : *unmanned aerial vehicle*, aussi appelé drone), habituellement contrôlé à distance, peut être programmé afin de retourner de manière autonome à la base, de voler en cercle ou même de se défendre, dans l'éventualité où il viendrait à perdre contact avec l'opérateur ;
- une opportunité inattendue surgissant en cours de mission.

Le département américain de la Défense (*US Department of Defense*) résume cette variabilité comme suit : « L'élément clé tient au fait que les agents humains et informatiques échangeront leurs initiatives et leurs rôles respectifs selon les phases et les échelons de la mission, afin de s'adapter aux nouveaux événements, aux perturbations et aux opportunités survenant cependant que les situations évoluent [traduction CICR]²⁸ ».

Résumé

L'autonomie des engins est un phénomène fortement plus nuancé que ne le laisseraient supposer les images populaires des robots tel que *Terminator*. Il s'agit d'un ensemble de technologies en rapide évolution, certaines n'en étant encore qu'à leurs balbutiements, et il ne fait aucun doute que de nombreuses questions cruciales verront le jour, parmi lesquelles deux en particulier présentent un intérêt pour les juristes étudiant ce domaine. Premièrement, les capacités autonomes d'un engin affectent principalement de manière directe ses superviseurs et ses opérateurs, mais pas nécessairement (dans le cas d'une arme) ceux contre qui il est dirigé. Notamment, le rôle de l'opérateur est modifié de manière importante mais n'est pas éliminé ; il n'existe pas d'autonomie « complète » au sens d'un engin qui opérerait de manière totalement indépendante de tout être humain. Deuxièmement, la forme précise de la relation entre l'opérateur et la machine est susceptible de varier selon les différents systèmes, le moment et les tâches à effectuer. Les juristes doivent se garder de tirer des conclusions en se fondant uniquement sur le fait qu'une arme soit décrite comme étant « autonome ». Il est possible de se faire une idée de la complexité potentielle des relations entre un système autonome et ses opérateurs ainsi qu'avec ses superviseurs en examinant l'*Autonomous Systems Reference Framework* (le cadre de référence des systèmes autonomes [traduction CICR]) récemment proposé par le *US Defense*

28 Defense Science Board, *op. cit.* note 12, p. 27.

*Science Board*²⁹. Il s'agit d'une méthode qui, lors de la phase de conception du système, attribue des fonctions et des responsabilités à l'ordinateur ou à l'un des nombreux opérateurs ou superviseurs humains. Ce cadre de référence examine de quelle façon l'autonomie vient soutenir chacun des différents utilisateurs humains d'un système particulier au sein d'une hiérarchie militaire, comment la communication entre ces utilisateurs peut être facilitée, comment la répartition des tâches entre les humains et les machines peut varier au cours d'une mission, de même que plusieurs autres facteurs.

L'autonomie ou la relation entre la machine et l'opérateur

Dans le cadre de la robotique en général et plus particulièrement dans celui des propositions de systèmes militaires autonomes, l'autonomie fait référence à une capacité et non pas à une technologie spécifique, à un dispositif particulier ou à un certain comportement. Il s'agit simplement de la capacité d'un système à remplir ses fonctions, quelles qu'elles soient, tout en nécessitant moins d'interactions avec un opérateur humain que le requerrait un système manuel. L'autonomie s'intéresse donc à la relation entre le système et son opérateur humain, et non à la nature de la tâche exécutée par ce système ou à la manière dont il la réalise. Tel que discuté plus haut, cette relation s'inscrit dans un spectre passant du contrôle humain complet à un contrôle complet (et efficace) de la machine sur des tâches spécifiques, le tout en fonction du degré de capacité autonome présent dans le système.

Lorsqu'un système ou un processus manuel est remplacé par un système détenant un certain niveau d'autonomie, d'une certaine manière le contrôleur « se met à la place » de l'opérateur humain du système manuel. La compréhension de l'opérateur (ou du développeur du système) relative à la manière de contrôler le système est transcrite dans un logiciel et programmée dans le contrôleur. Les moyens physiques à l'aide desquels l'opérateur manipule le système sont convertis en un ensemble d'actionneurs³⁰ que le contrôleur peut activer. Une forme de capteur ou un mécanisme de rétroaction, à travers lequel le contrôleur peut surveiller le système, est fourni. Le contrôleur peut également être doté d'autres capteurs lui permettant d'observer les facteurs environnementaux pertinents. Le contrôleur manipule les informations provenant de tous ces capteurs en fonction de sa programmation et génère des signaux de sortie qui sont envoyés aux actionneurs afin de réguler le système. Ce processus est synthétisé dans le paradigme bien connu du « sentir-penser-agir », souvent utilisé comme la définition opérationnelle d'un robot³¹.

29 *Ibid.*, p. 24.

30 Un actionneur est tout simplement un dispositif à travers lequel un contrôleur commande une centrale. Un exemple serait un moteur électrique pivotant une tourelle sur la base d'un signal provenant du système de contrôle du logiciel de base de la tourelle.

31 « Sentir-penser-agir » réfère au processus continu par lequel un robot perçoit son environnement, utilise cette information pour « prendre des décisions » en fonction de sa programmation puis agit par rapport à ces décisions ; voir, par ex., G. A. Bekey, *op. cit.* note 11, p. 2.

Les propositions de développement militaire abordent souvent l'autonomie suivant les termes de la boucle OODA (Observer, Orienter, Décider, Agir)³², qui correspond au modèle du cycle récurrent de prise de décision d'un combattant, conceptualisé par le Colonel John Boyd de la *US Air Force*. Le modèle OODA décrit les processus mentaux et physiques impliqués lors de l'observation de l'environnement, ainsi que dans la réponse aux changements qui résultent de la poursuite de certains objectifs. Un objectif ambitieux peut renfermer un ensemble de tâches secondaires, chacune détenant sa propre boucle OODA devant être complétée afin de poursuivre l'objectif global. Dans un système manuel, toutes les étapes d'une boucle sont complétées par un être humain : observer l'environnement pour en dégager les informations brutes, s'orienter par rapport à l'environnement en traitant cette information afin de former un modèle fiable, prendre une décision basée sur ce modèle et agir en fonction de cette décision. Au regard de la boucle OODA, le développement de systèmes autonomes permet d'assigner une partie ou la totalité de la boucle à un engin afin de parvenir à un certain avantage opérationnel, tel qu'une plus grande vitesse, une meilleure endurance, un coût moindre, ou encore une diminution des risques pour l'opérateur. Un système hautement autonome est un système pouvant exécuter la plupart ou la totalité des boucles OODA nécessaires à l'accomplissement de l'objectif final, en utilisant seulement les instructions de haut niveau de l'opérateur comme ligne directrice dans l'étape de la prise de décision d'une boucle, de sorte que l'humain le « plus proche » agit comme un commandant. Un système détenant un niveau d'autonomie inférieur est uniquement capable d'exécuter les boucles de niveau inférieur, voire seulement certaines composantes de ces boucles, et doit travailler de pair avec un opérateur humain afin d'atteindre un objectif élevé, faisant ainsi de cette personne un collaborateur. À titre d'exemple un système de ce type pourrait être un récepteur d'alerte radar : un système simplifié pourrait n'être capable que de détecter une menace potentielle et émettre un avertissement à un opérateur humain, alors qu'un système plus autonome pourrait être à-même de mettre en œuvre des contre-mesures, telles que tirer des balles ou des leurres, sans qu'une intervention humaine ne soit nécessaire.

Le fait que l'autonomie ait une influence sur la relation entre l'opérateur et la machine renferme trois incidences importantes pour les juristes.

Premièrement, les systèmes autonomes effectueront tout ou partie des tâches de la mission, en lieu et place des humains, sans pour autant les exécuter différemment des humains. Rien dans le concept d'autonomie des engins ne présuppose nécessairement qu'un système autonome exécute une tâche de manière différente de celle dont un humain ou une équipe d'humains l'exécuterait manuellement. Cela ne signifie pas, évidemment, que les futurs systèmes autonomes fonctionneront de

32 Voir, par exemple, *US Air Force*, *op. cit.* note 17, p. 16. La boucle OODA peut être considérée comme une autre expression de la boucle « sentir-penser-agir ». Certains ouvrages portant sur l'interaction « homme-machine » font également référence à une boucle de type OODA afin de décrire quatre types de fonctions pouvant être réalisées par un système autonome : l'acquisition de données, l'analyse de données, la prise de décision et la mise en œuvre d'actions. Voir, par exemple, Raja Parasuraman, Thomas B. Sheridan et Christopher D. Wickens, « A Model for Types and Levels of Human Interaction with Automation », *IEEE Transactions on Systems, Man and Cybernetics*, vol. 30, n° 3, 2000, p. 288.

la même manière qu'un système équivalent opéré par un humain ; l'« endurance » des systèmes ne nécessitant pas une interaction humaine constante, la capacité à intégrer rapidement des données provenant de diverses sources et la capacité à prendre de plus grands risques que le ferait un système en équipe, entre autres, amélioreront substantiellement leur performance. Cependant, de telles différences, bien que primordiales sur le plan opérationnel, sont plutôt secondaires en ce qui concerne la question de l'autonomie. Les drones, par exemple, permettent déjà un haut niveau d'endurance sans forcément présenter des capacités associées à un haut niveau d'autonomie et sans soulever les mêmes enjeux juridiques. Les capacités partagées entre les systèmes télécommandés et les systèmes autonomes sèment souvent la confusion quant à la distinction entre ces deux catégories de machines, puisque toutes deux sont capables de « se substituer » aux humains de manière différente et évoquent des images d'engins pouvant combattre sans présence humaine. Il est cependant important pour les juristes de garder à l'esprit cette distinction, puisque ces deux catégories soulèvent des questions juridiques différentes. Les drones d'aujourd'hui, ainsi que les dispositifs similaires, étendent la portée et les capacités physiques des combattants humains, tout comme le feront les systèmes autonomes. Cependant, ces derniers modifieront en outre les processus de décision menant à l'activation d'une arme.

Par conséquent, l'analyse juridique des systèmes autonomes proposés doit reposer sur le principe selon lequel les nouvelles qualités du système sont susceptibles de se retrouver dans les processus d'activation d'une arme attachée au système. Il n'est pas nécessaire de tenter d'attribuer un quelconque niveau de performance à un système uniquement en raison du fait qu'il est décrit comme ayant une certaine capacité d'autonomie pour mener à bien des opérations ; la seule chose qui peut être affirmée sans contredit sur cette base est que l'implication directe, totale ou partielle, de l'opérateur humain dans la ou des boucle(s) OODA du système s'en trouvera réduite ou supprimée. Le simple fait de réaffecter la tâche d'un humain à un ordinateur n'altère pas nécessairement la réalisation de cette tâche.

Deuxièmement, si des décisions et des actions spécifiques faisant l'objet d'obligations juridiques doivent être transférées d'opérateurs humains vers des systèmes autonomes, il est alors important d'examiner comment ces décisions et ces actions peuvent être attribuées aux personnes responsables, et si ces dernières sont celles qui sont effectivement concernées par les règles juridiques existantes. Lorsque des obligations juridiques sont assumées par un opérateur humain, assisté par un système autonome ou travaillant à ses côtés, il convient de se demander si cet opérateur occupe toujours le rôle prévu par le droit.

Troisièmement, il est inexact de décrire les systèmes autonomes comme étant des engins « indépendants [traduction CICR] »³³ opérant « sans contrôle humain [traduction CICR] »³⁴ ; la relation entre l'homme et la machine n'est pas rompue, elle est seulement modifiée. Les choix effectués par les concepteurs de matériel et

33 M. Wagner, *op. cit.* note 16, p. 159.

34 Gary E. Marchant et al., « International Governance of Autonomous Military Robots », *Columbia Science and Technology Law Review*, vol. 12, 2011, p. 273.

de logiciel dans la phase de création façonneront les comportements des systèmes à partir du moment de leur conception. Les planificateurs de mission et d'autres individus imposeront également des contraintes à chaque mission ; par exemple, dans le cas d'un drone autonome, un plan de vol doit être établi à l'avance précisant la zone devant être couverte ainsi que la durée de la mission (et le drone doit être conçu dans le but d'adhérer à ce plan), tandis que les décisions sur la quantité de carburant et sur les armes à transporter guideront et limiteront ce qui peut arriver au cours d'une opération³⁵. Ainsi, la main de l'homme assure toujours un certain degré d'orientation, malgré un éventuel défaut de supervision directe.

Les systèmes autonomes demeureront toujours des machines

Les juristes doivent éviter de tomber dans le piège en anthropomorphisant les systèmes autonomes. Il est indéniable que les systèmes d'armes sophistiqués d'aujourd'hui sont de simples machines exécutant des instructions codées dans un logiciel et il est possible d'avancer ici que les futurs systèmes hautement autonomes envisagés par leurs concepteurs ne seront rien de plus que cela. Certes, ils seront plus complexes et disposeront de plus de capacités à bien des égards ; ils seront probablement en mesure d'utiliser des informations provenant de sources se trouvant hors de portée des systèmes actuels ainsi que de traiter ces informations même lorsque confrontés à une plus grande incertitude. De surcroît, ils fonctionneront efficacement dans des environnements plus chaotiques et plus exigeants. De telles améliorations ne seront toutefois rendues possibles que grâce aux améliorations des logiciels et matériels contrôlés par le système ; elles n'apporteront pas un changement fondamental à la nature du système au point qu'il devrait être considéré comme étant autre chose qu'une machine commandée par un ordinateur. Les capacités et les limites du système dépendront encore, directement ou indirectement, d'actions et de décisions humaines.

Actuellement, dans les systèmes d'armement automatisés, les contrôleurs fondés sur des logiciels sont essentiellement des ordinateurs spécialisés, qui exécutent des programmes permettant de contrôler l'arme en lieu et place d'un opérateur humain. Ces contrôleurs, bien qu'ils puissent être hautement sophistiqués tant dans leur conception que dans leurs objectifs, demeurent néanmoins des ordinateurs à programmes enregistrés, c'est-à-dire une catégorie d'appareils dont font également partie des éléments ordinaires, tels que des ordinateurs personnels. La caractéristique fondamentale des ordinateurs à programmes enregistrés réside dans le fait que les instructions sont entrées par un programmeur humain, enregistrées dans la mémoire de la machine, puis utilisées afin de déterminer son fonctionnement³⁶. À moins d'un changement technologique majeur, les systèmes autonomes de demain emploieront essentiellement la même technologie ; les systèmes seront toujours contrôlés par un logiciel écrit par des développeurs humains.

35 William Boothby, « How Far Will the Law Allow Unmanned Targeting to Go? » in Dan Saxon (dir), *International Humanitarian Law and the Changing Technology of War*, Martinus Nijhoff, Boston, MA, et Leiden, 2013, p. 56.

36 William Aspray, « The Stored Program Concept », *IEEE Spectrum*, vol. 27, n° 9, 1990, p. 51.

Le fait que des programmes même très complexes ne soient que de simples ensembles d'instructions prédéfinies est souvent occulté à l'occasion des discussions portant sur les systèmes d'armement sophistiqués. Pour un observateur extérieur, il n'est effectivement pas toujours évident de percevoir qu'une machine complexe exécute simplement des instructions plutôt que de fonctionner de manière indépendante. Même les systèmes détenant une capacité de niveau inférieur sont souvent dirigés par des programmes ayant des instructions de type « si < X arrive > alors < fait l'action A > sinon < fait l'action B > » ; et cela peut laisser croire que le système lui-même « choisit » entre deux voies d'action alternatives, alors qu'en fait le choix a été préparé à l'avance par la personne ayant écrit le programme ; l'expression de la volonté de cette personne attendait simplement dans la mémoire du système que le signal précédemment déterminé soit déclenché. Par exemple, imaginons qu'un drone autonome possède des caméras et un programme de reconnaissance d'images associant les personnes se trouvant dans son champ de vision à une base de données contenant des photos d'insurgés connus, une instruction du type « si < image de la caméra correspond à image de la base de données à plus de 95 % de probabilité > alors < viser et tirer > sinon < continuer à chercher > » laisserait à penser que le drone sélectionne lui-même ses cibles, alors qu'en réalité, les cibles et les conditions dans lesquelles ces dernières doivent être attaquées ont préalablement été sélectionnées par les développeurs du système.

Si cette référence à la technologie informatique est introduite ici c'est parce qu'il est fondamental que les juristes ne se laissent pas induire en erreur par des références à des machines « intelligentes » ayant la capacité de « choisir » ou d'accomplir une opération « vraiment autonome³⁷ ». Aucun ordinateur n'est capable de choisir lui-même s'il doit exécuter ou non un programme sauvegardé dans sa mémoire, ni de décider discrétionnairement d'accomplir ou non une instruction spécifique se trouvant dans un programme ; une telle apparence de « choix » ne peut qu'être la résultante d'instructions intégrées dans le logiciel par des êtres humains. Fondamentalement, la seule fonction d'un ordinateur est d'exécuter le logiciel dont il est doté, quel qu'il soit.

Lorsqu'il est possible de démontrer qu'un ordinateur exécute des instructions explicites de bas niveau, encodées dans un logiciel par un développeur, il est facile de constater que l'ordinateur n'agit pas de manière suffisamment indépendante pour soulever des difficultés sur le plan juridique. Cependant, cela peut ne pas être aussi évident lorsqu'un système détenant des capacités plus avancées est « formé » pour adopter une conduite déterminée associée à une action importante, telle que la manipulation d'une arme³⁸. Des défis similaires se présentent lorsque des

37 Voir, par exemple, Chantal Grut, « The Challenge of Autonomous Lethal Robotics to International Humanitarian Law », *Journal of Conflict and Security Law*, vol. 18, n° 1, 2013, p. 5.

38 Dans ce cadre, « former » signifie exposer un système artificiellement intelligent à des ensembles d'exemples de données, représentant les tâches auxquelles il sera confronté ainsi que les réponses exactes à fournir, dans le but d'induire des comportements produisant des résultats optimaux pour ces tâches. La formation est essentiellement de nature inductive, car les situations « réelles » rencontrées par un système formé différeront inévitablement, à certains égards, des exemples auxquels il a été formé et, dès lors, est sujette aux erreurs.

opérateurs ou des commandants humains ne fournissent à un système autonome que des objectifs de mission de haut niveau, laissant le soin au système d'accomplir une série de tâches secondaires de niveau inférieur. Évidemment, l'intelligence artificielle et l'apprentissage automatique sont des domaines complexes qui vont bien au-delà de la portée de cet article³⁹, mais, aux fins d'une analyse juridique, il n'est pas nécessaire, ni même souhaitable, de se plonger dans les détails d'algorithmes spécifiques. Les juristes devraient plutôt reconnaître que le développement d'un système artificiellement intelligent n'est en réalité qu'un exercice de développement de logiciel, qui ne diffère pas du niveau d'activité humaine nécessaire pour le développement d'un programme plus simple, de bas niveau. Dans les deux cas, le développeur conçoit un comportement souhaité pour le système et écrit un programme destiné à conférer ce comportement au système. La distinction se trouve dans les algorithmes employés dans le programme : au lieu de coder directement les actions de type « < cible correspond à ces paramètres > alors < feu > », comme le ferait le développeur d'un programme plus simple, le développeur d'une machine « intelligente » écrit un programme dont la fonction est de formuler un ensemble optimal d'actions à effectuer en réponse à des stimuli environnementaux rencontrés au cours d'une mission. Il y a, dans un certain sens, un niveau d'abstraction supplémentaire entre le développeur et la manipulation de l'arme, dans la mesure où le développeur n'avait peut-être pas à l'esprit la séquence précise des événements conduisant à l'activation de l'arme, au moment de programmer la machine. Ce séquençage peut émaner des données avec lesquelles le système a été formé, néanmoins le résultat final de l'exécution du système consiste toujours en une règle signalant au système de tirer, à l'image d'un programme plus simple composé de règles fixes. Ce niveau d'abstraction supplémentaire complique le processus d'harmonisation entre des résultats et des commandes spécifiques provenant d'un humain, mais cela ne change rien au fait que l'ordinateur exécute uniquement des instructions formulées par son développeur.

Afin d'éviter toute confusion, il convient de souligner ici que les affirmations selon lesquelles des systèmes « intelligents » pourraient prendre leurs propres « décisions » sont propres à induire en erreur. Bien que ces systèmes ne puissent pas être programmés avec des réponses précises prédéterminées pour chacune des situations qu'ils rencontrent, ils sont tout de même programmés suivant un certain schéma afin de générer une réponse et ils opèrent ainsi en fonction de leur programmation, indépendamment du fait que les comportements spécifiques qu'ils adoptent aient été envisagés, ou auraient pu avoir été envisagés, au moment de leur développement ou de leur déploiement. Une telle machine n'est encore qu'un instrument répondant à la volonté de ses développeurs et de ceux qui sont responsables de son utilisation dans certaines situations ; elle n'a pas précisément les caractéristiques d'un objet capable de prendre des décisions de manière indépendante. Par exemple, les drones ayant la capacité de naviguer de manière autonome peuvent être aptes à répondre à des situations survenant en cours de vol qui ne sont pas spécifiquement prévues par leur logiciel, mais leur comportement correspond toujours aux règles qui ont été

39 Pour un aperçu général voir, par exemple, Stuart Russell et Peter Norvig, *Artificial Intelligence: A Modern Approach*, Prentice Hall, Englewood Cliffs, NJ, 2009.

programmées pour qu'ils répondent à des événements inattendus. Le comportement n'émane pas des machines elles-mêmes, mais bien de la volonté de leurs développeurs.

Aspects des propositions de développement militaire, importants dans le cadre d'une analyse juridique

L'autonomie s'étendra au-delà des systèmes d'armement

Tel qu'indiqué dans l'introduction, cet article traite des systèmes militaires autonomes, pas uniquement des armes. Même dans le cadre d'une analyse spécifiquement axée sur le DIH, il est nécessaire de tenir compte des effets qu'ont les capacités autonomes de systèmes qui ne peuvent en eux-mêmes conduire aucun acte d'hostilité, mais qui peuvent tout de même avoir un impact sur une décision ou une action susceptible d'avoir des conséquences juridiques.

Le meilleur exemple d'une telle capacité se trouverait dans un système RSR autonome qui localise, identifie et suit les cibles potentielles. Le Département de la Défense des États-Unis, par exemple, a récemment annoncé une initiative pilote de recherche sur l'autonomie (*Autonomy Research Pilot Initiative, ARPI*) qui « cherche à promouvoir le développement de la science et de la technologie innovantes et transversales, afin de mettre en place des systèmes autonomes aptes à répondre aux exigences futures relatives aux système et mission du Département de la Défense [traduction CICR]⁴⁰ ». L'appel d'offres de l'ARPI identifie le RSR comme étant l'un de ses défis techniques :

En augmentant le niveau de perception, de raisonnement et d'intelligence des machines sur les plateformes RSR, il est possible d'atteindre un équilibre plus efficace en termes de charge de travail. Cela inclut la gestion et le contrôle en boucle fermée des ressources RSR afin qu'elles s'adaptent à leur milieu et aux circonstances de la mission, dans le but de collecter des données appropriées et pertinentes [traduction CICR]⁴¹.

Des initiatives préliminaires en ce sens sont déjà en cours ; aux États-Unis, l'Agence pour les projets de recherche avancée de défense (*Defense Advanced Research Projects Agency, DARPA*) participe au programme *Military Imaging and Surveillance Technology (MIST)* visant à « développer une capacité optique RSR fondamentalement nouvelle, capable de fournir des images 3D en haute résolution afin de localiser et d'identifier une cible à des distances beaucoup plus grandes que ce qui est présentement possible avec les systèmes optiques existants [traduction CICR]⁴² ».

40 Department of Defense, *Autonomy Research Pilot Initiative (ARPI) Invitation for Proposals*, novembre 2012, p. 1, disponible sur : www.auvac.org/uploads/publication_pdf/Autonomy%20Research%20Pilot%20Initiative.pdf.

41 *Ibid.*, p. 4.

42 Voir : www.darpa.mil/program/military-imaging-and-surveillance-technology.

Des systèmes développés dans le cadre de ce programme seraient capables d'identifier et de reconnaître de manière automatique des cibles potentielles⁴³.

La motivation à poursuivre cette ligne de recherche au sein de l'ARPI vient du fait que

L'espace de combat actuel génère une augmentation sans précédent des données de renseignement, de surveillance et de reconnaissance (RSR). L'analyste affecté au traitement, à l'exploitation et à la diffusion peut être dépassé quand vient le moment d'intégrer et d'analyser ces différentes saisies de données (imagerie, vidéo, communication et données RSR humaines) tout en essayant de localiser les cibles, d'en déduire les sources, et de fournir une rétroaction sur l'analyse (en temps réel ou postérieurement à celle-ci) [traduction CICR]⁴⁴.

Il est possible d'en déduire que l'augmentation de l'« intelligence » des plateformes RSR sera utilisée afin d'effectuer un certain traitement des données brutes avant de communiquer le résultat à un humain, plaçant ainsi le système RSR en position d'influencer la perception qu'aura l'opérateur humain sur l'espace de combat. Un tel traitement des données de capteurs a une incidence évidente sur l'impact qu'un système RSR avancé peut avoir sur une décision de tirer ou d'effectuer une autre action, ce qui implique d'importantes conséquences juridiques.

Bien que légèrement plus éloignés des opérations de combat, mais avec tout de même une certaine influence secondaire sur leurs résultats, doivent être mentionnés les véhicules autonomes qui transportent des marchandises, des provisions et même des personnes. Il existe de nombreux exemples d'efforts employés afin d'automatiser les opérations de réapprovisionnement, à l'image du programme *Autonomous Aerial Cargo/Utility System* (AACUS) du *US Office of Naval Research*⁴⁵. Suite au succès de l'hélicoptère de ravitaillement de marchandises sans pilote K-MAX⁴⁶ en Afghanistan, l'objectif du programme AACUS a été « le développement de capacités autonomes avancées visant à permettre la livraison rapide de marchandises par des systèmes à décollage et à atterrissage verticaux (ADAV) sans, ou potentiellement avec, pilote [traduction CICR]⁴⁷ ». Le programme produira un système qui pourra être installé dans des avions adaptés afin de répondre aux appels d'unités déployées, en planifiant son itinéraire de manière autonome (mais sous une certaine supervision), en évitant les obstacles et les intempéries, et en choisissant un point de débarquement approprié

43 Strategic Technology Office, DARPA, « Military Imaging and Surveillance Technology – Long Range (MIST-LR) Phase 2 », Broad Agency Announcement no DARPA-BAA-13-27, 12 mars 2013, p. 6, disponible sur : www.fbo.gov/index?s=opportunity&mode=form&id=78b0ddb382678fa9ace985380108f89&tab=core&_cview=0.

44 Department of Defense, *op. cit.* note 40, p. 4.

45 Office of Naval Research, « Autonomous Aerial Cargo/Utility System Program », 27 septembre 2013, disponible sur : www.onr.navy.mil/en/Science-Technology/Departments/Code-35/All-Programs/aerospace-research-351/Autonomous-Aerial-Cargo-Utility-AACUS.aspx.

46 Lockheed Martin Corporation, « K-MAX », disponible sur : www.lockheedmartin.com/us/products/kmax.html.

47 Mary Cummings et Angelo Collins, *Autonomous Aerial Cargo/Utility System (AACUS): Concept of Operations*, Office of Naval Research, p. 2, disponible sur : www.onr.navy.mil/~media/Files/Funding-Announcements/BAA/2012/12-004-CONOPS.ashx.

pour acheminer l'approvisionnement et, le cas échéant, évacuer des victimes⁴⁸. Bien que des véhicules tels que ceux contrôlés par des systèmes de type AACUS ne transporteront pas d'armes, ils demeureront néanmoins des éléments imposants se déplaçant rapidement, qui devront effectuer des opérations se déroulant à proximité de personnes et d'autres véhicules, et qui pourraient éventuellement transporter des matières dangereuses ou présenter d'autres dangers⁴⁹. Ils introduisent donc un risque juridique, par exemple s'ils sont utilisés pour transporter des soldats blessés.

La présence de capacités autonomes au sein de systèmes auxiliaires aux opérations de combat nécessitera dès lors d'avoir une vision plus large de l'autonomie, et non pas de la considérer comme étant simplement une propriété d'un nouveau type d'arme. En outre, tel qu'examiné dans la section suivante, la capacité dont dispose l'AACUS et d'autres systèmes similaires de négocier directement avec d'autres systèmes sans pilote⁵⁰ peut compliquer la tâche consistant à identifier quels systèmes sont pertinents pour une enquête particulière.

Les systèmes autonomes collaboreront entre eux

Tel que discuté ci-dessus, les systèmes autonomes altèrent la relation existant entre l'arme et l'opérateur. La relation entre des systèmes autonomes distincts est d'égale importance. La plupart des feuilles de route relatives à leur développement, publiées par des organisations militaires et gouvernementales, indiquent clairement que les systèmes autonomes doivent collaborer entre eux⁵¹. Cette interopérabilité peut prendre plusieurs formes.

De nombreux projets de recherche en cours, qu'ils soient militaires ou civils, sont axés sur le comportement de groupes de robots qui coopèrent de façon décentralisée. Ces groupes sont communément appelés des « essaims », qui fonctionnent ensemble, comme un seul système, dans la poursuite d'un certain objectif. Le programme de l'armée américaine *Micro Autonomous Systems and Technology* (MAST) en est un exemple⁵², il vise à créer des « systèmes de plateformes mobiles autonomes équipées de capteurs miniatures permettant d'explorer et de localiser des cibles rapidement, discrètement et de manière efficace [traduction CICR]⁵³ ». Il s'agit d'équipes de petits véhicules aériens et terrestres qui seront utilisés par des soldats afin d'explorer et de cartographier des environnements complexes, tels que des zones urbaines ou des grottes. La possibilité d'équiper des essaims avec des armes a également été soulevée⁵⁴.

48 *Ibid.*

49 Anthony Finn et Steve Scheduling, *Developments and Challenges for Autonomous Unmanned Vehicles: A Compendium*, Springer, Berlin, 2010, p. 156.

50 M. Cummings et A. Collins, *op. cit.* note 47, p. 2.

51 Voir, par exemple, *US Department of Defense, Unmanned Systems Integrated Roadmap FY2011-2036*, n° 11-S-3613, 2011, pp. 49-50.

52 US Army Research Laboratory, « Micro Autonomous Systems and Technology (MAST) », 25 février 2011, disponible sur : www.arl.army.mil/www/default.cfm?page=332.

53 MAST, « Research Thrusts », disponible sur : www.mast-cta.org.

54 Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*, Penguin Press, New York, 2009, p. 229.

Une forme de collaboration quelque peu différente entre les systèmes autonomes est utilisée dans des projets de développement tels que le programme Hydra de la DARPA⁵⁵. Le programme Hydra « vise à développer un réseau sous-marin de charges utiles et de plateformes sans pilote [traduction CICR]⁵⁶ ». Il s'agit d'un système de plateformes submersibles sans pilote, qui serait utilisé pour lancer une variété de drones et de véhicules sous-marins sans pilote (UUVs) à proximité d'opérations ennemies. Bien qu'il n'en soit encore qu'à ses débuts, ce programme envisage un système où le « navire principal » submersible interagirait directement avec les charges utiles de ses drones et de ses UUVs ; par exemple, des UUVs accosteraient et se rechargeraient à partir du navire principal, collecteraient des renseignements utiles à leur mission, et transfèreraient ensuite les informations acquises durant la mission au navire principal afin de les envoyer aux autorités⁵⁷.

Ces projets, tout comme d'autres projets similaires, de même que les tactiques et les stratégies qui y seront associées, s'inscrivent dans un courant général qui tend à relier plus étroitement les composantes, autrefois disparates, d'une force militaire. L'expression la plus connue de cette tendance est probablement la doctrine de la guerre réseau-centrique (NCW)⁵⁸, une approche de la conduite des hostilités qui met l'accent sur l'importance de partager l'information entre les éléments de la force, dans le but d'exploiter au mieux cette information et les capacités de la force. Si elle s'est développée à l'origine aux États-Unis, des approches similaires d'interconnexion des systèmes militaires sont menées, ou du moins ont été proposées, par l'OTAN⁵⁹, l'Australie⁶⁰, le Royaume Uni⁶¹ et dans d'autres pays. L'un des avantages escomptés d'un tel partage d'information se trouve la possibilité d'atteindre un degré d'opération décentralisée, ou d'« auto-synchronisation », tel que deux entités ou plus puissent interagir directement et coordonner leurs efforts sans avoir à recourir à une structure hiérarchique de commandement et de contrôle traditionnelle⁶². Lorsque certains de ces systèmes intégrés ont des degrés significatifs d'autonomie, le partage

55 Federal Business Opportunities, « Hydra », 22 août 2013, disponible sur : www.fbo.gov/index?s=opportunity&mode=form&id=4cc32f06144bd6f3eba18655135d6155&tab=core&_cvview=1.

56 DARPA Tactical Technology Office, « Hydra », disponible sur : www.darpa.mil/Our_Work/TTO/Programs/Hydra.aspx.

57 John Keller, « DARPA Considers Unmanned Submersible Mothership Designed to Deploy UAVs and UUVs », *Military & Aerospace Electronics*, 23 juillet 2013, disponible sur : www.militaryaerospace.com/articles/2013/07/darpa-uuv-mothership.html.

58 Voir, de manière générale, David S. Alberts, John J. Garstka et Frederick P. Stein, *Network Centric Warfare*, 2^e éd. révisée, Department of Defense Command and Control Research Program, 1999.

59 OTAN, « NATO Network Enabled Capability », 27 octobre 2010, disponible sur : www.nato.int/cps/de/SID-815535E4-57782C82/natolive/topics_54644.htm.

60 M. P. Fewell et Mark G. Hazen, *Network-Centric Warfare: Its Nature and Modelling*, Defence Science and Technology Organisation, September 2003, disponible sur : <http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/3310/1/DSTO-RR-0262%20PR.pdf>.

61 Ministère britannique de la Défense, *Network Enabled Capability*, JSP 777, 2005, disponible sur : http://webarchive.nationalarchives.gov.uk/20121026065214/http://www.mod.uk/NR/rdonlyres/E1403E7F-96FA-4550-AE14-4C7FF610FE3E/0/nec_jsp777.pdf.

62 D. S. Alberts, J. J. Garstka et F. P. Stein, *op. cit.* note 58, p. 175 ; pour une analyse plus complète portant sur le statut de l'auto-synchronisation, voir B. J. A. van Bezooijen, P. J. M. D. Essens et A. L. W. Vogelaar, « Military Self-Synchronization: An Exploration of the Concept », in *Proceedings of the 11th International Command and Control Research and Technology Symposium*, Cambridge, 26-28 septembre 2006, disponible sur : www.dodccrp.org/events/11th_ICCRTS/html/papers/065.pdf.

d'information ne sera pas nécessairement conduit, ou directement supervisé, par un humain, de sorte que si les renseignements collectés par un système autonome sont utilisés lors d'une action agressive par un autre système autonome, tous les systèmes impliqués pourraient faire partie d'une enquête judiciaire.

Alors que des concepts, tels que le NCW, ne sont pas intrinsèquement liés au développement des capacités autonomes dans les systèmes militaires, ils proposent une idée du type d'environnement dans lequel de tels systèmes avancés seraient susceptibles d'opérer et du degré d'intégration entre systèmes militaires qui pourrait devenir la norme. Les juristes devraient être conscients que si la tendance se maintient, ce qui semble être le cas, il deviendra de plus en plus difficile de séparer un système autonome d'un autre pour déterminer leur participation dans un incident. Un tel développement pourrait potentiellement compliquer les processus d'examen des nouveaux systèmes d'armes, ainsi que le processus de détermination de la responsabilité des personnes impliquées dans le développement ou l'exploitation de ces systèmes. En effet, les tentatives aux fins d'établir des distinctions entre des systèmes séparés, tel qu'entre des systèmes létaux et non létaux, peuvent devenir de plus en plus artificielles. Chaque appareil faisant partie d'un « système de systèmes » présentera à la fois un comportement individuel, en tant que système en soi, et un comportement de groupe, en tant que composant d'un réseau plus vaste.

Autonomie et DIH

Les conséquences juridiques liées à l'utilisation de systèmes militaires autonomes

En dépit de l'ampleur des changements qui vont survenir dans la composition des forces armées⁶³ et dans la pratique des conflits, il est encore possible de se demander en quoi la perspective d'utiliser des armes autonomes dans les conflits armés présente un intérêt particulier au plan juridique. Des machines innovantes possédant des degrés de sophistication très variés, la plupart trop complexes pour qu'un non-spécialiste puisse les comprendre en détail, ont été employées au combat depuis des millénaires, et l'application des principes juridiques en vigueur vis-à-vis de leur utilisation a rarement soulevé de difficultés. En effet, les systèmes, incluant les armes, détenant une capacité d'opération autonome plus limitée sont déjà utilisés au combat sans qu'aucune assertion sérieuse à l'effet que leur utilisation serait illégale n'ait été avancée. Ainsi, pourquoi une arme plus autonome soulèverait-elle des problèmes juridiques majeurs ? En d'autres termes, en quoi l'utilisation d'une arme autonome pourrait-elle affecter la capacité d'un État à respecter ses obligations découlant du DIH ou affecter la capacité d'un tribunal à juger d'éventuelles violations de ce droit ?

63 Sharon Gaudin, « U.S. Military May Have 10 Robots per Soldier by 2023 », Computerworld, 14 novembre 2013, disponible sur : www.computerworld.com/s/article/9244060/U.S._military_may_have_10_robots_per_soldier_by_2023.

La réponse, ainsi que la distinction juridique fondamentale entre des systèmes autonomes et d'autres systèmes militaires complexes, se trouve dans le fait que l'autonomie de la machine affecte le processus de décision relatif à l'exécution d'une action, alors que d'autres systèmes ne produisent un effet qu'une fois qu'une décision a été prise⁶⁴. Cela ne signifie pas, comme cela a été suggéré ailleurs⁶⁵, que des systèmes suffisamment autonomes prendront eux-mêmes des décisions. Au contraire, les deux aspects critiques, discutés ci-dessous, sont i) le fait que certaines décisions actuellement prises au cours d'un conflit armé seraient détournées des décideurs traditionnels et seraient plutôt prises, en réalité, par les personnes qui définissent le comportement du système autonome et celles chargées de son utilisation ; et ii) que, ce faisant, la nature de ces décisions en serait modifiée.

L'autonomie réaffecte les décisions opérationnelles

Une machine autonome exploite un logiciel qui se rapproche du processus de décision menant à la réalisation d'une action, ou d'une certaine partie de celle-ci, suivi d'un autre logiciel qui dirige la machine pour mettre en œuvre cette décision. En d'autres termes, la personne qui aurait normalement eu à décider d'accomplir ou non un acte en particulier, est partiellement ou totalement déchargée de cette décision, ou bien la personne qui aurait normalement été en mesure d'initier ou d'empêcher la commission d'un acte se retrouve en partie ou complètement écartée de cette possibilité. Certains éléments de cette décision sont incorporés de manière effective dans un logiciel écrit par des personnes qui n'auraient normalement pas contribué de manière significative à la décision de mener à bien l'acte en question. Se posent alors plusieurs questions juridiques nouvelles. Par exemple, les systèmes d'armement autonomes doivent-ils être conçus de manière à ce que ceux qui sont responsables de la planification d'une attaque exercent le même contrôle qu'ils seraient en mesure d'exercer sur les soldats humains ? Est-il possible que les développeurs d'armes, ou toute autre personne qui aiderait à déterminer le comportement d'un système d'armement autonome, soient tenus pénalement responsables de violations du DIH ? Dans quelle mesure est-il licite d'automatiser une fonction, telle qu'une analyse de proportionnalité, alors que le droit prévoit la responsabilité d'êtres humains pour cette fonction ?

Actuellement, lorsqu'ils travaillent avec des systèmes opérant à des degrés d'autonomie inférieurs, les opérateurs sont seulement déchargés des décisions d'un niveau inférieur, qui n'impliquent pas de conséquences juridiques importantes en elles-mêmes. Par exemple, un missile « tir et oublie », qui esquive de manière autonome toute tentative d'interception lors du trajet vers sa cible, ne libère pas de ce fait l'opérateur ayant appuyé sur le bouton de « mise à feu » de toute décision pouvant se révéler significative au plan juridique. Cependant, lorsqu'un système

64 Il est entendu que cet aspect peut soulever de nouvelles questions portant sur certains enjeux tels que ce que constitue une « décision » aux fins d'une analyse légale, et quelles conditions doivent être remplies pour qu'une décision soit considérée comme étant sous le contrôle immédiat d'un système autonome.

65 Armin Krishnan, *Killer Robots: Legality et Ethicality of Autonomous Weapons*, Ashgate, Farnham, 2009, p. 33.

opère avec un degré d'autonomie supérieur, le système de contrôle de la machine est susceptible d'émuler des décisions plus importantes. Lorsqu'un système RSR autonome ou un système de ciblage relié à une arme joue un rôle substantiel dans la sélection d'une cible ou dans la recommandation de tirer (un exemple étant le radar au sol du système de missile Patriot)⁶⁶, l'opérateur d'armes humain, s'il existe une personne pouvant raisonnablement être considérée comme tel, n'effectue plus toutes les étapes du processus mental conduisant à faire feu sur la cible. De ce fait, il n'est plus le seul, ou même le principal, décideur contribuant à la prise de décision de tirer. Sur le plan juridique, la machine en elle-même ne peut pas être considérée comme étant un décideur⁶⁷, de sorte que la décision est partiellement ou entièrement attribuable aux personnes responsables du comportement du système autonome (en gardant à l'esprit que l'identification de ces individus et de ces organisations peut s'avérer une entreprise complexe en soi) et aux personnes responsables de la décision d'utiliser l'arme.

L'autonomie modifie le caractère des décisions

Le fait que la prise de décisions opérationnelles passe des mains des ceux qui les prenaient traditionnellement à celles de ceux qui sont chargés de définir le comportement des systèmes autonomes modifie nécessairement la nature de ces décisions et ce, de trois manières interdépendantes.

Premièrement, les décisions acquièrent de plus en plus un caractère général. En effet, les décisions prises par des humains « sur le terrain » à propos de situations spécifiques sont remplacées ou complétées par des instructions programmatiques qui ont été fournies auparavant à une machine. Les décisions relatives à des actes précis dans des situations spécifiques sont donc remplacées par des choix, pour ainsi dire politiques, plus généraux, et applicables à la gamme de situations correspondant aux paramètres précédemment fournis à la machine.

Deuxièmement, le moment de la prise de décisions change. Les décisions consistant à déterminer s'il faut exécuter une action et comment, via un système autonome, sont en réalité prises au moment où le comportement visé est programmé dans la machine et lorsque la décision est prise d'utiliser l'arme, et non au moment où la situation se présente dans un conflit. Ce point est important d'abord car cela peut avoir des conséquences sur le champ d'application temporel du DIH⁶⁸ et ensuite car cela revient à prendre pour acquis que les situations dans lesquelles l'engin sera amené à se déployer à l'avenir ne différeront pas de celles envisagées à l'époque où il a été développé et testé.

66 Raytheon, « Patriot », disponible sur : www.raytheon.com/capabilities/products/patriot/.

67 Autrement dit, les machines ne sont pas des sujets de DIH et, bien entendu, la possibilité qu'elles puissent le devenir à l'avenir est peu crédible.

68 Pour une discussion portant sur une telle question, voir Tim McFarland et Tim McCormack, « Mind the Gap: Can Developers of Autonomous Weapons Systems be Liable for War Crimes? », *U.S. Naval War College International Law Studies*, vol. 90, 2014, p. 361, disponible sur : www.usnwc.edu/getattachment/ed8e80adb622-4fad-9a36-9bedd71afebe/Mind-the-Gap-Can-Developers-of-Autonomous-Weapons.aspx.

Troisièmement, les informations sur le fondement desquelles les décisions sont prises sont modifiées. Les décisions mises en œuvre via un système autonome ne peuvent pas être basées sur une observation directe (ni même indirecte) de la situation à laquelle se rapporte la décision ; au contraire, elles doivent être basées sur toute l'information acquise grâce à l'expérience et à l'anticipation, disponibles au moment où la machine a été programmée, puis, lorsque la décision est prise d'utiliser l'arme, confirmées.

L'un des résultats de ces changements réside dans le fait que le lien causal entre une décision spécifique prise par un humain et une action spécifique (ou répétée) ou un résultat spécifique, à l'image d'une cible quelconque vers laquelle des tirs sont effectués, peut être affaibli, dans la mesure où la décision est adoptée partiellement ou entièrement via un système autonome.

Les changements dans la nature des décisions tels que décrits ci-dessus se produisent si les actions sont explicitement programmées dans une machine, ou si des technologies d'intelligence artificielle sont utilisées afin de permettre à la machine d'adapter son comportement de manière dynamique. Mais dans tous les cas les développeurs de la machine, ou ceux à qui ils répondent, exercent un contrôle sur le comportement du système ; contrôle qui s'exerce en définissant un objectif et en dotant le système des moyens lui permettant d'atteindre cet objectif.

L'identification des enjeux juridiques

Un tel changement dans les prises de décisions militaires est fondamental, dans la mesure où l'application du DIH prend en considération la prise de décision. En cherchant à « limiter les effets des conflits armés pour des raisons humanitaires⁶⁹ », le droit cherche à guider les décisions, ainsi que les actions qui en résultent, des personnes prises individuellement ainsi que celles des parties au conflit, prises collectivement. Des objections juridiques à l'utilisation d'engins autonomes dans un conflit armé ont plus de chances d'être soulevées lorsque les technologies de l'autonomie et le DIH interviennent sur la même décision ; c'est-à-dire lorsque l'utilisation d'une arme ou d'un autre système possédant la capacité de mener des opérations autonomes modifie un processus décisionnel, ou le résultat d'une décision, au-delà de ce qui est permis en vertu du DIH, ou lorsqu'elle est de nature à entraver l'application du droit. Considérant les faibles degrés d'autonomie présents dans les systèmes d'armements actuels, un tel scénario demeure hypothétique. Certaines hypothèses plausibles peuvent toutefois être formulées : peut-être que si un système RSR autonome fournissait directement des informations à un système d'armement autonome, de telle manière que les commandants humains ne pourraient pas vérifier leur exactitude en toute indépendance avant d'activer une arme, cela pourrait être considéré comme une violation de l'obligation de prendre des précautions dans l'attaque.

69 CICR, « La guerre et le droit international humanitaire », Genève, 2012, disponible sur : <https://www.icrc.org/fre/war-and-law/overview-war-and-law.htm>.

Cela peut sembler vague, mais considérant les nombreuses formes que peuvent prendre systèmes autonomes et les nombreuses applications qui peuvent en résulter, ainsi que le stade embryonnaire de leur développement, il s'agit probablement du maximum qui puisse être avancé avec certitude. Les orientations suivantes peuvent toutefois être utiles afin d'identifier les enjeux juridiques.

Les décideurs juridiques continueront d'être des humains

De par sa nature et sa forme, Le DIH est anthropocentrique. L'un de ses objectifs principaux étant « d'adoucir [...] les maux irréparables de la guerre, de supprimer les rigueurs inutiles et d'améliorer le sort des militaires blessés sur les champs de bataille⁷⁰ », il met nécessairement l'accent sur les personnes : celles manipulant les armes et celles sujettes aux effets de ces armes. L'évolution du droit est motivée par la nécessité de réglementer et de rendre compte des décisions et des actions prises par des êtres humains, ainsi que par la nécessité de soulager les souffrances humaines inutiles.

Ce rappel peut sembler banal, mais il est nécessaire dans ce contexte. L'émergence d'une nouvelle technologie, en particulier lorsqu'elle est considérée par certains comme annonçant une « révolution dans les affaires militaires [traduction CICR]⁷¹ », attire naturellement l'attention sur ses particularités et sur les possibilités dont elle est porteuse. Il est souvent tentant d'aborder la technologie (ou les appareils qui l'utilisent) comme étant le point de référence du droit, plutôt que de ramener son attention sur les personnes. Dans certains cas, cela est opportun ; lorsqu'une technologie ou un appareil est censé produire un ensemble d'effets limités et bien définis sur la conduite des hostilités et sur les personnes concernées, il peut s'avérer utile de considérer que cette technologie ou cet appareil produit un effet juridique. Les armes à laser aveuglant, par exemple, ont un effet limité et bien défini dont il est facile de vérifier la compatibilité avec le droit des conflits armés, et dont il est aisé de constater qu'elles dépassent les limites fixées par ce droit ; dans un cas comme celui-ci, il est naturel pour les juristes de mettre ces armes au cœur de leur réflexion car elles présentent un effet indésirable bien identifié qu'il convient de réglementer⁷². Ce n'est toutefois pas le cas avec les systèmes autonomes.

L'ajout de capacités autonomes à des systèmes militaires nouveaux ou déjà existants présente un enjeu d'ordre différent. La capacité d'un système à effectuer, à un certain niveau, des opérations autonomes ne correspond pas en tant que telle à un effet facilement déterminable pouvant être apprécié en fonction des exigences du DIH. Tel que mentionné précédemment, un système de contrôle autonome n'affecte directement que la relation entre l'arme et l'opérateur. Il affecte donc le comportement de l'opérateur et non le comportement de l'arme contrôlée. De plus, considérant la

70 Convention pour l'amélioration du sort des militaires blessés dans les armées en campagne, 22 août 1864 (entrée en vigueur le 22 juin 1865), Préambule.

71 P. W. Singer, *op. cit.* note 54, p. 203.

72 Protocole additionnel (IV) à la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination (Protocole relatif aux armes à laser aveuglantes), 1380 UNTS 370, 13 octobre 1995 (entré en vigueur le 30 juillet 1998).

variabilité liée aux temps et aux fonctions de ce qui peut être qualifié d'autonomie d'une machine, il est difficile de formuler des affirmations générales portant sur le comportement d'un opérateur ou d'un développeur (ses réflexions et ses actions) en fonction d'un événement particulier survenant sur le champ de bataille. Il est simplement possible d'affirmer que les juristes doivent porter leur attention sur ce comportement, afin de déterminer où les enjeux juridiques sont susceptibles de survenir. Les technologies qui permettent à une machine d'atteindre une capacité d'opération autonome se contentent seulement de fixer ces objectifs.

Distinction entre les enjeux techniques et les enjeux juridiques

Parmi les enjeux les plus fréquemment soulevés par les auteurs du domaine juridique, figurent notamment les préoccupations relatives à la question de savoir si un système autonome proposé répondra à un certain standard de performance jugé nécessaire afin de se conformer au droit. Ces préoccupations ont jusqu'à présent eu trait le plus souvent aux principes juridiques de distinction et de proportionnalité⁷³.

En ce qui concerne la distinction, par exemple, plusieurs auteurs ont soutenu qu'aucun système robotique existant ne pouvait opérer une distinction fiable entre un combattant et un civil, une lacune pouvant être attribuée, entre autres, aux limites de l'efficacité des systèmes de capteurs⁷⁴, à l'incapacité du logiciel de contrôle à suffisamment bien « comprendre » le contexte et le comportement humain, ainsi qu'à la difficulté de trier ce qui est pertinent de ce qui ne l'est pas, à partir d'informations non pertinentes dans des situations complexes⁷⁵. Des arguments similaires sont utilisés afin de démontrer que les robots ne peuvent juger si une attaque proposée répondrait aux exigences de la proportionnalité, certains auteurs soulignant le plus souvent la nature qualitative et subjective du problème⁷⁶.

D'autres auteurs soulignent des limites plus générales concernant la faculté des systèmes robotiques à fonctionner de manière fiable dans un conflit. Asaro évoque les « capacités très limitées en termes d'apprentissage et d'adaptation » des systèmes autonomes afin de justifier pourquoi « [i]l sera [...] difficile, voire impossible, de concevoir des systèmes capables de fonctionner malgré le “brouillard” et les tensions qui caractérisent le temps de guerre⁷⁷ ». D'autres notent la difficulté de prédire de manière fiable le comportement de systèmes autonomes complexes⁷⁸.

73 Voir, par exemple, C. Grut, *op. cit.* note 37 ; Peter Asaro, « Droits de l'homme, automatisation et déshumanisation des prises de décisions létales : les systèmes d'armement autonomes doivent-ils être interdits ? », *Revue internationale de la Croix-Rouge*, vol. 94, n° 886, Sélection française 2012/2, p. 489 ; M. Wagner, *op. cit.* note 16.

74 Voir, par exemple, Benjamin Kastan, « Autonomous Weapons Systems: A Coming Legal “Singularity”? », *Journal of Law, Technology and Policy*, n° 1, 2013, p. 60.

75 M. S. Riza, *op. cit.* note 9, pp. 129-132.

76 Voir, par exemple, Noel E. Sharkey, « The Evitability of Autonomous Robot Warfare », *Revue internationale de la Croix-Rouge*, vol. 94, n° 886, 2012, p. 789.

77 P. Asaro, *op. cit.* note 73, p. 495.

78 A. Finn et S. Scheding, *op. cit.* note 49, p. 36 : « Au fur et à mesure que le degré d'autonomie augmente, il devient de plus en plus difficile de prédire l'état de l'ensemble du système [traduction CICR] ». Voir également la discussion portant sur la responsabilité des développeurs à la p. 183.

Il ne fait aucun doute que nombre de ces arguments peuvent sembler pertinents, considérant l'état actuel des technologies. Toutefois, lorsqu'une objection à l'utilisation de systèmes autonomes est présentée comme étant une déclaration sur l'aptitude d'un tel système à fonctionner suivant un standard requis par le DIH dans une situation donnée, cette affirmation, bien qu'elle soit exacte, ne touche qu'à un ensemble spécifique des capacités de la machine et ne vaut donc que pour un certain moment dans le temps ; suivant l'évolution de la technologie, l'objection peut venir à disparaître. Les juristes devraient donc se garder de faire des déclarations générales sur la légalité des systèmes autonomes sur la base de ce type d'arguments. Une telle objection servirait de fondement pour une décision juridique (peut-être à titre indicatif lors du processus d'examen des armes d'un État), seulement dans un cas où il serait possible de s'attendre à ce qu'une telle lacune de la machine perdure, comme cela pourrait être le cas s'il était possible d'identifier un facteur susceptible d'empêcher directement des systèmes dotés d'une certaine autonomie de fonctionner en conformité avec le DIH, ou encore dans un cas où un aspect inhérent à la nature de l'autonomie des machines violerait le DIH. Des exemples provenant de champs se situant en dehors du domaine de l'autonomie des machines pourraient inclure l'interdiction de la perfidie (en raison de la nature de l'acte) et de l'utilisation du gaz sarin (en raison de son effet intrinsèquement indiscriminé). Si de tels facteurs ne peuvent être identifiés, il semblerait plus approprié de déclarer simplement qu'un système particulier pourrait ou ne pourrait pas être utilisé dans une situation spécifique. De ce fait, il est recommandé que les investigations portant sur la licéité des systèmes autonomes incluent une question de qualification : si le système peut être développé, même de manière hypothétique, pour fonctionner dans une situation donnée aussi efficacement qu'un système non-autonome (que ce soit un humain ou autre), existerait-il une quelconque base légale afin de s'objecter à son utilisation ? Si la réponse est un « non » sans équivoque, alors l'objection est davantage un enjeu technique qui doit être résolu avant de pouvoir utiliser le système de manière licite, ou alors il s'agit d'un moyen destiné à limiter les situations dans lesquelles le système peut être utilisé jusqu'à ce que cet enjeu soit surmonté. Par exemple, si un système autonome de ciblage pouvait être développé afin de distinguer les combattants des civils d'une manière aussi fiable, voire davantage, que ne le font des soldats humains sans assistance, serait-il juste de s'objecter à son utilisation ? Certains avancent que les objections liées à l'utilisation de systèmes autonomes qui se basent sur la difficulté à prédire leur comportement en toutes circonstances, ou sur la possibilité d'erreurs informatiques et de dysfonctionnements se produisant après leur activation, pourraient également tomber dans cette catégorie. La possibilité de dysfonctionnements, en particulier, n'est pas propre aux systèmes autonomes ; elle est, au contraire, une préoccupation devant être abordée par rapport à tout système militaire recourant à un ordinateur pour une partie de son opération.

Si, toutefois, la réponse est « oui » (c'est-à-dire qu'indépendamment de l'efficacité d'un système autonome son usage ne répond pas aux règles du DIH actuelles), les juristes devront alors se pencher de plus près sur la question, afin de déterminer comment le développement du système autonome devrait être limité, ou dirigé, ou encore de quelle manière le droit devrait être développé. Cela pourrait être le cas

si, par exemple, il est observé que le droit requiert un certain degré de contrôle humain direct pour chaque attaque ou chaque acte de violence individuel ; si tel est le cas, il serait inacceptable de placer une attaque sous l'entier contrôle d'un système autonome, et ce indépendamment de la qualité de performance du système.

Conclusion

Même à cette étape de développement préliminaire, il semble probable que l'utilisation de systèmes militaires suffisamment autonomes puisse tester les limites du DIH au travers plusieurs de ses aspects fondamentaux. L'innovation des systèmes autonomes vient du fait qu'ils réaffectent les décisions opérationnelles et ce faisant modifient leur nature. Dans le cas d'un conflit armé, les décisions prises par des combattants individuels en fonction de la situation seraient remplacées par des choix plus généraux, effectués par des personnes définissant en amont le comportement des systèmes autonomes.

La variabilité attendue du degré d'autonomie dans les systèmes proposés, la variété probable des applications et la possibilité de systèmes autonomes collaborant directement entre eux sont des éléments qui se conjuguent et qui viennent grandement complexifier les approches analytiques relatives au comportement d'engins spécifiques lors de situations données. Il est recommandé que les juristes abordent plutôt les capacités des machines comme étant les résultantes de décisions prises par des développeurs d'armes et qu'ils concentrent leur attention sur le rôle que jouent ces développeurs et le personnel opérationnel, lesquels déploient et travaillent avec des systèmes autonomes. En particulier, les nouvelles conséquences juridiques liées aux capacités autonomes ne se rapportent pas à la manière dont une machine remplit correctement ses fonctions, mais seulement à la manière dont ses développeurs et ses opérateurs, le cas échéant, sont impliqués dans le résultat.