



# Assemblée générale

Distr. générale  
14 juillet 2025  
Français  
Original : anglais

---

## Conseil des droits de l'homme

### Soixantième session

8 septembre-3 octobre 2025

Points 3 et 5 de l'ordre du jour

Promotion et protection de tous les droits de l'homme,  
civils, politiques, économiques, sociaux et culturels,  
y compris le droit au développement

Organes et mécanismes chargés des droits de l'homme

## **Incidences sur les droits de l'homme des technologies nouvelles et émergentes dans le domaine militaire**

## **Rapport du Comité consultatif du Conseil des droits de l'homme**



## I. Introduction

### A. Mandat

1. Le présent rapport a été demandé par le Conseil des droits de l'homme dans sa résolution 51/22, par laquelle celui-ci a prié le Comité consultatif du Conseil des droits de l'homme de réaliser une étude dans laquelle il examinerait les incidences sur les droits de l'homme des technologies nouvelles et émergentes dans le domaine militaire.
2. À sa vingt-neuvième session, le Comité consultatif a créé un groupe de rédaction composé des membres suivants : Buhm-Suk Baek (Président), Nadia Amal Bernoussi, Milena Costas Trascasas, Alessandra Devulsky, Jewel Major, Javier Palummo (Rapporteur), Vasilka Sancin, Vassilis Tzevelekos, Catherine Van de Heyning, Frans Viljoen et Yue Zhang.

### B. Portée de l'étude

3. Dans la présente étude, le Comité consultatif examine l'ensemble du cycle de vie des technologies nouvelles et émergentes dans le domaine militaire. Il s'intéresse à la manière dont le droit international des droits de l'homme éclaire la prise de décisions relative à la collecte et à la gestion des données, à la transparence, au principe de responsabilité, à la non-discrimination et à la protection des droits. Il décrit les cadres juridiques internationaux applicables à la conception, à la mise au point, au déploiement et à la surveillance de ces technologies, et leur double usage potentiel (militaire et civil).
4. L'étude contient une analyse des modalités selon lesquelles les traités internationaux existants, le droit international coutumier et les instruments de droit non contraignant, notamment les Principes directeurs relatifs aux entreprises et aux droits de l'homme, peuvent contribuer à réglementer la mise au point et l'utilisation de ces technologies. Elle souligne l'importance et la complémentarité du droit international humanitaire et du droit international des droits de l'homme à cet égard.
5. On trouvera également dans l'étude une analyse des incidences sur les droits de l'homme que les technologies nouvelles et émergentes peuvent avoir dans le domaine militaire, compte tenu des débats menés sous l'égide de l'ONU, des contributions des parties prenantes, notamment les 22 réponses à un questionnaire<sup>1</sup>, et des travaux de recherche documentaire sur l'état actuel de ces technologies, ainsi que des nouvelles préoccupations qu'elles suscitent du point de vue des droits de l'homme. L'analyse repose sur une approche prospective qui prend en compte les scénarios auxquels pourraient donner lieu les nouvelles technologies. On trouvera, dans la dernière partie, des recommandations sur les mesures à prendre.

### C. Cadre conceptuel et normatif

#### 1. Technologies nouvelles et émergentes, domaine militaire et double usage

6. Aux fins du présent rapport, l'expression « domaine militaire » désigne les activités liées à la défense et l'environnement opérationnel dans lequel agissent les forces armées, y compris les forces de sécurité. L'expression « technologies nouvelles et émergentes » désigne les technologies qui sont en cours d'élaboration ou ont récemment été déployées, et qui se caractérisent souvent par leur potentiel de transformation. Fruit des progrès accomplis dans plusieurs domaines, notamment l'intelligence artificielle (IA), les neurosciences, la biotechnologie, la nanotechnologie et la robotique, les technologies nouvelles et émergentes dans le domaine militaire ne sont pas toujours synonymes d'« armes » ; si certaines armes peuvent en contenir, toutes les technologies nouvelles et émergentes dans le domaine militaire ne sont pas des armes. Eu égard à leur double usage, il est difficile d'en trouver qui ne fassent pas appel à l'innovation, de même que les innovations technologiques ne sauraient

<sup>1</sup> Voir <https://www.ohchr.org/en/hr-bodies/hrc/advisory-committee/human-rights-implications>.

se limiter à un usage strictement militaire<sup>2</sup>. L'expression « technologies à double usage » désigne les innovations qui ont des applications dans le domaine civil comme dans le domaine militaire et qui peuvent être utilisées à des fins commerciales, publiques ou militaires<sup>3</sup>. Le cadre conceptuel du présent rapport doit donc être considéré comme ouvert, ces différentes catégories étant difficiles à définir avec précision.

7. Si les armements militaires ont de tout temps incorporé de nouvelles technologies, les avancées numériques actuelles, en particulier l'IA, représentent un bond en avant considérable. Ce changement de paradigme survient dans un contexte de fracture technologique et de rapports de force déséquilibrés, caractérisé par le fait que les technologies militaires mises au point dans certaines parties du monde peuvent être déployées dans des États qui ont peu d'influence sur cette phase de mise au point. Par exemple, les États du Sud mondial sont souvent exclus du développement et de la gouvernance des technologies nouvelles et émergentes dans le domaine militaire, alors que leurs populations en subissent parfois les effets de manière disproportionnée.

8. Les technologies nouvelles et émergentes dans le domaine militaire posent aux États et aux autres acteurs des problèmes considérables au regard du respect du droit international des droits de l'homme. Fondamentalement, leur utilisation comporte un risque de déshumanisation de l'emploi de la force : elle renforce les tendances consistant à réduire, par un étiquetage et un ciblage algorithmiques, les vies humaines à de simples points de données, affaiblit, voire exclut les considérations morales et éthiques propres au jugement humain<sup>4</sup> et augmente le risque d'emploi arbitraire et disproportionné de la force. Cette déshumanisation est incompatible avec les principes des droits de l'homme, notamment les droits à la vie, à l'intégrité corporelle, à la non-discrimination et à la dignité humaine, qui comptent parmi les fondements du droit international des droits de l'homme et de nombreux systèmes juridiques nationaux. En outre, les technologies nouvelles et émergentes dans le domaine militaire peuvent, s'agissant des droits de l'homme, toucher différents groupes de personnes de différentes manières<sup>5</sup>.

9. L'une des principales préoccupations soulevées par ces technologies porte sur le point de savoir dans quelle mesure l'être humain en conserve véritablement le contrôle. Cette question concerne en particulier les technologies impliquant l'emploi de la force, notamment les systèmes d'armes autonomes et d'autres systèmes armés automatisés. Ces technologies reposent sur l'automatisation et la prise de décisions autonome, ce qui risque de réduire le contrôle humain et d'entraver l'application du principe de la responsabilité. Elles peuvent être à l'origine de graves violations des droits de l'homme, notamment de menaces contre les droits à la vie, à la liberté d'expression, à la protection de la vie privée et à la non-discrimination, ainsi que de violations de l'interdiction d'infliger des mauvais traitements. L'ensemble de leur cycle de vie doit s'inscrire dans un cadre solide de protection des droits de l'homme, au sein duquel les avancées technologiques ne portent pas atteinte à ces droits et les victimes ont accès à des mécanismes de responsabilisation et de réparation.

10. Les technologies nouvelles et émergentes dans le domaine militaire, qu'il s'agisse de biens ou de matériel informatique et de logiciels, sont considérées comme étant à double usage et susceptibles d'être utilisées à des fins commerciales, publiques ou militaires, ce qui représente un défi supplémentaire. Sachant qu'il se peut que ces technologies soient déployées hors de tout cadre juridique, les nouvelles préoccupations qu'elles suscitent sur le plan des droits de l'homme doivent être levées avant qu'elles ne deviennent opérationnelles, en particulier dans les situations de conflit. Les risques sont exacerbés par le rôle central que joue le secteur privé dans la mise au point de ces technologies. Les entreprises ont donc un

<sup>2</sup> Voir [https://www.ires.ma/sites/default/files/docs\\_publications/international-conference\\_-military-technologies-vis-a-vis-human-rights-concerns\\_-summary-report.pdf](https://www.ires.ma/sites/default/files/docs_publications/international-conference_-military-technologies-vis-a-vis-human-rights-concerns_-summary-report.pdf).

<sup>3</sup> Marcello Ienca et Effy Vayena (2018), « Dual use in the 21st century », *Swiss Medical Weekly*, vol. 148, n° 4748 ; Marcus Schulzke (2019), « Drone proliferation and the challenge of regulating dual-use technologies », *International Studies Review*, vol. 21, n° 3.

<sup>4</sup> Christof Heyns (2017), « Autonomous weapons in armed conflict and the right to a dignified life », *South African Journal on Human Rights*, vol. 33, n° 1.

<sup>5</sup> Voir la Conférence internationale de la Croix-Rouge et du Croissant-Rouge, résolution 34IC/24/R2.

rôle primordial à remplir en matière de prévention des violations des droits de l'homme et des atteintes à ces droits.

## **2. Cadres juridiques internationaux applicables à l'ensemble du cycle de vie des technologies nouvelles et émergentes dans le domaine militaire**

11. Le droit international, qu'il repose sur des normes conventionnelles ou coutumières, s'applique à la mise au point et à l'utilisation des technologies nouvelles et émergentes dans le domaine militaire, et les États sont tenus de s'y conformer. Ces derniers ont en outre l'obligation positive de veiller au respect de ce droit lorsque ces technologies sont utilisées par des acteurs non étatiques relevant de leur juridiction. L'ensemble du cycle de vie des technologies nouvelles et émergentes dans le domaine militaire est régi par de multiples cadres juridiques internationaux<sup>6</sup> qui s'appliquent de manière complémentaire et se renforcent mutuellement<sup>7</sup>.

12. Le droit international des droits de l'homme joue un rôle essentiel dans la réglementation des technologies nouvelles et émergentes dans le domaine militaire et s'applique aussi bien en temps de paix qu'en période de conflit armé. Il est impossible, même en cas de conflit armé, de déroger à certains droits de l'homme, notamment le droit à la vie<sup>8</sup>, l'interdiction des mauvais traitements, de l'esclavage et de la servitude, ainsi qu'aux principes de légalité, de non-rétroactivité et de liberté de pensée, de conscience et de religion<sup>9</sup>.

13. La Charte internationale des droits de l'homme et d'autres principaux traités internationaux relatifs aux droits de l'homme font partie des instruments essentiels qui s'appliquent aux technologies nouvelles et émergentes dans le domaine militaire. Ces technologies pouvant être utilisées pour assurer une surveillance de masse et mettre en œuvre des pratiques discriminatoires, les principes de transparence et de responsabilité sont, de ce point de vue, primordiaux. Certains droits ayant trait notamment à la protection de la vie privée, à la liberté d'expression et à la non-discrimination, mais également à la santé, à la culture et au travail, doivent être préservés lors des phases de conception, de mise au point et de déploiement. De même, l'utilisation de ces technologies doit être assortie d'une interdiction des mauvais traitements. La question de la non-discrimination est particulièrement importante, car ces technologies peuvent renforcer les préjugés dont sont victimes les groupes marginalisés ou vulnérables si les algorithmes ne sont pas correctement conçus et contrôlés. Les États doivent veiller à ce que la mise au point et l'utilisation des technologies nouvelles et émergentes dans le domaine militaire soient conformes au droit international des droits de l'homme et prévoir des recours utiles en cas de violation. Les entreprises concernées doivent appliquer les normes pertinentes, conformément aux Principes directeurs, éviter les violations des droits de l'homme et prévenir activement les risques que leurs activités pourraient faire peser sur les droits de l'homme.

14. Le droit international humanitaire joue également un rôle fondamental dans la réglementation des technologies nouvelles et émergentes dans le domaine militaire. Si certains traités réglementent ou interdisent expressément certaines armes, les Conventions de Genève et leurs Protocoles additionnels s'appliquent à toutes les formes de guerres et d'armes, y compris, comme l'a indiqué la Cour internationale de Justice, les armes qui n'ont pas encore été mises au point<sup>10</sup>. L'article 36 du Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I) oblige les parties à déterminer si l'étude, la mise au point, l'acquisition ou l'adoption d'une nouvelle arme, de nouveaux moyens ou d'une nouvelle méthode de guerre serait interdite par les dispositions du Protocole ou par toute autre règle du droit international.

<sup>6</sup> D'autres domaines du droit international (par exemple, le droit de l'environnement et le droit du travail) sont également concernés. Différents groupes d'États ont également adopté des déclarations, pris des engagements et adhéré à des codes de conduite.

<sup>7</sup> Haut-Commissariat des Nations Unies aux droits de l'homme (2011), *La protection juridique internationale des droits de l'homme dans les conflits armés* (publication des Nations Unies).

Voir aussi la résolution 51/22 du Conseil des droits de l'homme.

<sup>8</sup> Voir Comité des droits de l'homme, observation générale n° 36 (2018).

<sup>9</sup> Voir Comité des droits de l'homme, observation générale n° 29 (2001).

<sup>10</sup> Cour internationale de Justice, *Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif*, C.I.J. Recueil 1996, p. 226, par. 86.

Bien que cette disposition ne lie officiellement que les parties à ce Protocole, certains États non parties procèdent également à un examen de la légalité des armes.

15. 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 vise à interdire ou à limiter l'emploi de certains types d'armes considérées comme causant des souffrances inutiles ou injustifiables aux combattants ou comme frappant les civils sans discrimination. Les Protocoles additionnels à la Convention régissent l'utilisation d'armes en particulier et la mise au point de technologies d'armement en appliquant trois principes fondamentaux du droit international humanitaire : a) le droit des Parties à un conflit armé de choisir des méthodes ou moyens de guerre, qui n'est pas illimité ; b) la protection des personnes civiles contre les effets des hostilités ; c) l'interdiction d'infliger des blessures superflues ou des souffrances inutiles aux combattants. En outre, le Groupe d'experts gouvernementaux sur les technologies émergentes dans le domaine des systèmes d'armes létaux autonomes a réaffirmé que le droit international humanitaire continuait de s'appliquer pleinement à la mise au point et à l'utilisation potentielles de tels systèmes<sup>11</sup>.

16. Le droit international humanitaire demeure essentiel pour protéger les civils des effets des conflits armés dans un contexte de progrès technologiques rapides, et il incombe donc aux États de faire respecter ce droit, quelles que soient les avancées de la science et de la technologie<sup>12</sup>. Même si les États ne sont pas parties aux traités susmentionnés, ils restent liés par le droit international coutumier, dont plusieurs normes relèvent du *jus cogens*. Les États doivent également respecter leur devoir de diligence, c'est-à-dire qu'ils doivent tout mettre en œuvre pour prévenir la violation d'une obligation internationale, notamment en adoptant les réglementations et les mesures voulues, et exercer un devoir de vigilance auprès des opérateurs publics et privés<sup>13</sup>. Il convient cependant de noter que l'exercice de la diligence raisonnable relève d'une obligation de moyens et non de résultat.

17. Il incombe au premier chef à chaque État de veiller à ce que l'évolution des technologies nouvelles et émergentes dans le domaine militaire ne porte pas atteinte au droit international<sup>14</sup>. Par conséquent, les États doivent procéder à des évaluations complètes visant à déterminer la manière dont des normes juridiques internationales particulières s'appliquent à ces technologies. Les institutions nationales des droits de l'homme ont, à cet égard, un rôle important à jouer<sup>15</sup>. Il est essentiel que chaque État procède en temps utile à l'examen de sa législation nationale afin de recenser et éliminer toute incohérence avec le droit international.

18. Malgré les cadres juridiques existants, les progrès rapides des technologies nouvelles et émergentes dans le domaine militaire constituent un défi pour leur adoption et suscitent des débats quant à l'application du droit international, s'agissant notamment de la prise de décisions fondée sur l'IA, des systèmes d'armes autonomes, des systèmes automatisés et des programmes militaires augmentant les capacités physiques et cognitives des combattants. Face à la nouvelle donne que représentent l'IA et d'autres technologies nouvelles et émergentes, les parties prenantes doivent veiller à se mettre en conformité avec les normes et règles juridiques internationales<sup>16</sup>.

<sup>11</sup> CCW/GGE.1/2023/2, par. 21 a).

<sup>12</sup> Le droit conventionnel est également applicable à cet égard (par exemple, le Protocole additionnel I aux Conventions de Genève de 1949).

<sup>13</sup> Cour internationale de Justice, *Usines de pâte à papier sur le fleuve Uruguay (Argentine c. Uruguay)*, Jugement, C.I.J. Recueil 2010, p. 14, par. 197.

<sup>14</sup> Comité international de la Croix-Rouge (2016), *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons* (Genève).

<sup>15</sup> Contribution de Digital Rights Alliance.

<sup>16</sup> Voir <https://committees.parliament.uk/writtenEvidence/120290/pdf/>.

## II. Incidences sur les droits de l'homme

### A. L'intelligence artificielle, technologie clef dans le domaine militaire

19. Dans le domaine militaire, l'intelligence artificielle est une technologie clef qui améliore les capacités opérationnelles de diverses fonctions. Il est important de faire la distinction entre les technologies fondées sur l'intelligence artificielle, c'est-à-dire les outils et systèmes qui font appel à l'IA pour étayer la prise de décisions humaine, et les systèmes autonomes tels que les systèmes d'armes autonomes, qui peuvent fonctionner avec une intervention humaine limitée, voire sans aucune intervention humaine. Si l'IA peut faciliter la prise de décisions, tous les systèmes faisant appel à cette technologie ne sont pas autonomes. De même, un système autonome n'est pas forcément fondé sur l'IA. Cette section portera plus particulièrement sur le rôle de l'IA en tant qu'outil d'amélioration soumis au contrôle humain.

20. Si l'IA a commencé à être mise au point il y a plusieurs décennies et qu'elle est considérée comme une technologie émergente déjà ancienne, ce n'est que depuis peu qu'elle occupe une place centrale dans l'amélioration de l'autonomie des systèmes d'armes, l'aide à la prise de décisions militaires et dans les chaînes d'approvisionnement militaires. Les progrès informatiques récents ont renforcé son rôle dans ces domaines<sup>17</sup>.

21. L'IA fait de plus en plus partie intégrante des activités militaires, notamment dans les domaines de l'analyse du renseignement, de la planification des scénarios, de la logistique et de la prise de décisions opérationnelles. Les systèmes d'IA peuvent fonctionner selon divers degrés d'autonomie : le renforcement de l'autonomie a pour corollaire une diminution de la surveillance et du contrôle humains. L'IA peut faciliter la prise de décisions, par exemple en traitant rapidement de grandes quantités de données, et supplanter le jugement humain dans certains scénarios prédéterminés tels que les situations stressantes. Son utilisation soulève toutefois certaines préoccupations relatives aux droits de l'homme, notamment en ce qui concerne la liberté d'expression, la protection de la vie privée et la non-discrimination. Par exemple, elle pourrait prendre à tort un équipement d'assistance aux personnes handicapées pour une arme, en violation des principes de non-discrimination<sup>18</sup>. Des biais algorithmiques pourraient également entraîner une discrimination fondée sur la race ou le genre. Il est essentiel de faire respecter la dignité humaine, telle qu'elle est définie par le droit international des droits de l'homme, tout au long du cycle de vie d'un système d'IA si l'on veut garantir la valeur égale de chaque être humain<sup>19</sup>.

22. L'IA peut restreindre le contrôle humain et la capacité d'exercer un jugement moral ou juridique sur les résultats fournis par cette technologie. La principale difficulté consiste à déterminer si et dans quelle mesure le droit international exige un contrôle humain dans les domaines du ciblage, de la détention, de l'utilisation des armes et de la préservation de la dignité humaine. Il s'agira notamment de respecter des cadres juridiques tels que la Déclaration universelle des droits de l'homme, qui dispose que tous les êtres humains sont « doués de raison et de conscience et doivent agir les uns envers les autres dans un esprit de fraternité ».

23. Le manque de transparence du processus de prise de décision par l'IA constitue un autre problème majeur. De fait, de nombreux systèmes fonctionnent tels des « boîtes noires », ce qui remet en cause les principes de transparence et de recours utile en matière de droits de l'homme. L'intégration de l'IA, en particulier lorsqu'elle s'accompagne de fonctions d'apprentissage automatique, peut perturber l'application des cadres de responsabilité existants, qui sont fondés sur l'action humaine. Il est essentiel de définir clairement les responsabilités, ce qui est difficile lorsque l'IA fonctionne de manière très autonome ou que son raisonnement est opaque. L'application du principe de responsabilité suppose à la fois des mesures préventives et des évaluations a posteriori des violations éventuelles du droit

<sup>17</sup> Stefka Schmid, Thea Riebe et Christian Reuter (2022), « Dual-use and trustworthy? », *Science and Engineering Ethics*, vol. 28, n° 2.

<sup>18</sup> A/HRC/49/52, par. 54.

<sup>19</sup> Recommandation de l'Organisation des Nations Unies pour l'éducation, la science et la culture sur l'éthique de l'intelligence artificielle.

international. Les principaux mécanismes internationaux de responsabilisation s'appliquent tant à la responsabilité pénale individuelle qu'à la responsabilité des États.

24. Une autre préoccupation relative aux droits de l'homme tient au fait que les technologies nouvelles et émergentes dans le domaine militaire, en particulier celles qui ont recours à l'IA, consomment de grandes quantités d'énergie, génèrent d'importantes émissions de carbone et dépendent fortement de matières premières telles que le nickel, le cobalt et le graphite, ce qui présente des risques à long terme, notamment pour le droit à un environnement propre, sain et durable. Il sera essentiel, au fur et à mesure que ces technologies seront perfectionnées, de remédier à leurs effets sur l'environnement et les droits de l'homme.

## **B. Les systèmes d'armes autonomes et leur incidence sur l'intervention humaine et l'application du principe de responsabilité**

25. Les systèmes d'armes autonomes peuvent prendre des décisions moyennant une intervention humaine limitée, voire sans aucune intervention humaine. Les systèmes d'armes létaux autonomes, qui sont un sous-ensemble des systèmes d'armes autonomes, se distinguent par leur capacité à exécuter de manière autonome des décisions susceptibles de conduire à l'emploi de la force létale. La définition des systèmes d'armes autonomes pose un problème juridique imputable aux différents niveaux d'intervention et de contrôle humains possibles. L'absence de consensus entre les États sur une définition juridique de ces systèmes complique un peu plus leur réglementation<sup>20</sup>.

26. Contrairement aux systèmes de prise de décisions automatisés qui fonctionnent sur la base de commandes et de critères prédéfinis, les systèmes d'armes autonomes sont conçus pour fonctionner à des niveaux d'autonomie élevés, ce qui soulève des questions juridiques complexes quant à leur conformité avec le droit international. Ces systèmes posent, par exemple, des problèmes particuliers en ce qui concerne la dignité humaine, le contrôle humain et la transparence, et ont une incidence sur le droit à la vie, le droit de disposer de recours utiles et le droit à la protection de la vie privée<sup>21</sup>. S'agissant du droit international humanitaire, les principales difficultés ont trait aux principes de distinction, de proportionnalité et de précaution dans l'attaque, ainsi qu'à l'obligation de procéder à l'examen de la légalité des armes.

27. Les partisans de l'interdiction des systèmes d'armes autonomes affirment que ceux-ci pourraient violer la clause de Martens de la Convention de 1907 pour le règlement pacifique des conflits internationaux, qui dispose que les armes doivent être conformes aux « principes de l'humanité et [aux] exigences de la conscience publique »<sup>22</sup>. Or, ils voient souvent cette clause comme une base de réglementation plutôt que comme une interdiction<sup>23</sup>. À l'inverse, les opposants à cette interdiction peuvent aller jusqu'à remettre en cause la valeur juridique de cette clause<sup>24</sup>.

28. Malgré le consensus sur la nécessité de maintenir un contrôle humain sur les systèmes d'armes autonomes, il n'existe pas de règles ni de normes internationales particulières garantissant un contrôle humain véritable sur l'emploi de la force<sup>25</sup>. Diverses propositions ont permis de déterminer les éléments concrets d'un contrôle humain, notamment les restrictions relatives à l'utilisation de ces systèmes et à l'environnement opérationnel. Il a été

<sup>20</sup> Voir [https://docs-library.unoda.org/Convention\\_on\\_Certain\\_Conventional\\_Weapons\\_-Group\\_of\\_Governmental\\_Experts\\_on\\_Lethal\\_Autonomous\\_Weapons\\_Systems\\_\(2023\)/CCW\\_GGE1\\_2023\\_CRP.1\\_0.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf).

<sup>21</sup> Contribution de Privacy International.

<sup>22</sup> Rupert Ticehurst (1997), « *The Martens clause and the laws of armed conflict* », *International Review of the Red Cross*, n° 317.

<sup>23</sup> Voir <https://blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons/>.

<sup>24</sup> Paul Scharre (2018), *Army of None: Autonomous Weapons and the Future of War* (New York, W. W. Norton & Company).

<sup>25</sup> Voir <https://www.ejiltalk.org/what-level-of-human-control-over-autonomous-weapon-systems-is-required-by-international-law/>.

suggéré d'adopter certaines mesures telles que des restrictions concernant les cibles et l'obligation de mettre en œuvre une surveillance humaine et des mécanismes de responsabilisation pour remédier à l'imprévisibilité et aux risques inhérents à la mise au point, au déploiement et à l'utilisation de ces systèmes<sup>26</sup>. Au sein du Groupe d'experts gouvernementaux, dont les travaux portent à la fois sur les technologies autonomes et les technologies de l'IA, la question de ce qui constitue un « contrôle humain significatif » fait toujours débat, et aucun consensus ne s'est encore dégagé à ce sujet. En revanche, la nécessité de maintenir un certain degré d'intervention humaine fait l'objet d'un large consensus. Par ailleurs, la question des droits de l'homme reste largement absente des débats du Groupe d'experts gouvernementaux<sup>27</sup>.

29. L'intégration de l'IA et des technologies autonomes dans ces nouveaux systèmes pose des problèmes juridiques particuliers au regard du droit international. Dans le régime juridique actuel, le déploiement de l'IA peut compliquer la détermination de la responsabilité et le respect de l'obligation de rendre des comptes en cas de violation du droit international. Le manque de transparence des processus de ciblage fondés sur l'IA peut créer des zones d'ombre et rendre plus difficile l'attribution de la responsabilité pénale individuelle pour les crimes de guerre ou l'attribution de la responsabilité des États en cas de violation du droit international. Si la responsabilité pénale individuelle est abondamment examinée dans la doctrine et au sein de l'ONU, les débats sur les problèmes posés par les systèmes d'armes autonomes s'agissant de la responsabilité des États n'en sont encore qu'à leurs balbutiements<sup>28</sup>. Pour aborder cette question, il faut déterminer clairement les responsabilités imputables aux concepteurs de ces technologies, aux opérateurs et aux commandants militaires, ainsi que les obligations mises à la charge des États par le droit international, y compris au titre des Principes directeurs. Il est essentiel de préciser davantage ces aspects sur le plan juridique, car chaque technologie nouvelle et émergente présente des difficultés particulières à différents niveaux de responsabilité.

30. En outre, l'attribution d'un comportement aux fins de l'établissement de la responsabilité des États en droit international dans le contexte des systèmes d'armes autonomes soulève des questions juridiques fondamentales qui méritent un examen approfondi. Si les États membres du Groupe d'experts gouvernementaux ont estimé par consensus que tout fait internationalement illicite perpétré par un État, y compris en cas d'utilisation potentielle de systèmes d'armes létaux autonomes, engage sa responsabilité internationale, ils n'ont pas donné de précisions concernant l'attribution de cette responsabilité en cas de violation du droit international<sup>29</sup>. Il a été souligné dans le premier projet de texte soumis par le Président que le comportement des organes d'un État – par exemple de ses agents ou de toute personne faisant partie de ses forces armées – lui était imputable, y compris les actes et omissions liés à l'utilisation de ces systèmes<sup>30</sup>.

31. En particulier, il importera de savoir si et dans quelles circonstances le comportement d'un système d'armes autonome donné peut ou doit être imputé à l'État et si le régime actuel de la responsabilité internationale des États, qui repose sur le paradigme de l'action humaine, permet d'attribuer la responsabilité dans le contexte de ces systèmes<sup>31</sup>. Si les États ont des

<sup>26</sup> Ibid., Vincent Boulanin *et al.* (2020), *Limits on Autonomy in Weapon Systems* (Stockholm, Stockholm International Peace Research Institute et CICR) et CCW/GGE.1/2023/WP.6.

<sup>27</sup> Voir CCW/GGE.1/2020/WP.6, CCW/GGE.1/2023/WP.2/Rev.1 et CCW/GGE.1/2024/WP.10.

<sup>28</sup> Robin Geiß (2021), « State control over the use of autonomous weapon systems », in *Military Operations and the Notion of Control Under International Law*, Rogier Bartels *et al.*, dir. publ. (La Haye, Asser Press) et Lutiana Valadares Fernandes Barbosa (2024), *Autonomous Weapons Systems and the Responsibility of States: Challenges and Possibilities* (Boca Raton, Floride, États-Unis d'Amérique, et Abingdon, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, CRC Press).

<sup>29</sup> CCW/GGE.1/2022/2, par. 19.

<sup>30</sup> Voir <https://documents.unoda.org/wp-content/uploads/2022/07/CCW-GGE.1-2022-CRP.1.docx>.

Voir aussi CCW/GGE.1/2022/WP.2 et Alisha Anand Ioana Puscas (2022), « Proposals related to emerging technologies in lethal autonomous weapons systems » (Institut des Nations Unies pour la recherche sur le désarmement).

<sup>31</sup> Articles sur la responsabilité de l'État pour fait internationalement illicite (Annuaire de la Commission du droit international 2001, vol. II (Deuxième partie), voir A/CN.4/SER.A/2001/Add.1 (Deuxième partie), p. 26), Rebecca Crootof (2016), « War torts », *University of Pennsylvania Law*

obligations positives en matière de droits de l'homme, qui les engagent à veiller à ce que ces technologies respectent le droit international et à prendre des mesures préventives pour en minimiser les risques, le cadre fixé par ces obligations pourrait ne pas suffire, à lui seul, à établir la responsabilité des États lorsque de tels systèmes ont un degré d'autonomie supérieur aux capacités de prévision de l'être humain qui en est responsable. La difficulté consiste à déterminer dans quelles circonstances les actions menées par ces systèmes d'armes doivent être assimilées au comportement de l'État qui les déploie, et donc engager sa responsabilité en droit international. Il est essentiel de répondre à ces questions si l'on veut garantir l'application du principe de responsabilité et le respect du droit international.

32. L'intégration de capacités autonomes dans les systèmes d'armes faisant appel à l'IA pose des problèmes particuliers au regard de l'examen de la légalité des armes. Les systèmes d'armes autonomes interagissent avec leur environnement, d'où la nécessité de procéder à des essais faisant appel à de multiples scénarios. Plus l'on aura recours à l'IA, plus il faudra accorder d'attention à la compatibilité de ces systèmes avec les normes juridiques. Si la sélection et la révision des données algorithmiques sont essentielles, un examen complet de la légalité des systèmes d'armes autonomes intégrant des systèmes d'IA devrait tenir compte des obligations mises à la charge des États par le droit international des droits de l'homme, notamment les droits à la vie, à l'intégrité, à la non-discrimination et à la protection de la vie privée, ainsi que les principes de transparence et de responsabilité, sans oublier les risques de conséquences involontaires<sup>32</sup>. Il faudrait préciser la nature du devoir de diligence afin d'éliminer les préjugés et les discriminations involontaires, en particulier lorsqu'ils sont susceptibles de porter atteinte aux droits garantis par le droit international. Des juristes devront être associés à cette démarche dès la phase de conception de ces systèmes d'armes, ce qui permettra de traiter ces questions et de mettre en place des garanties contre le risque de violation des droits de l'homme. Néanmoins, des interrogations demeurent quant à la compatibilité de la prise de décisions automatisée avec les principes des droits de l'homme<sup>33</sup>, et il est important de souligner que la question de savoir si les systèmes d'armes autonomes peuvent être fabriqués et utilisés d'une manière qui soit pleinement conforme à toutes les prescriptions du droit international fait l'objet d'intenses débats.

33. L'introduction dans le domaine militaire de technologies nouvelles et émergentes, comme celles utilisées dans les systèmes d'armes autonomes, remet en cause le droit international existant et souligne la nécessité d'instaurer de nouvelles règles pour réglementer et, le cas échéant, interdire ces technologies si elles ne peuvent satisfaire aux normes juridiques internationales. Le Groupe d'experts gouvernementaux envisage une double approche consistante, d'une part, à interdire les armes incompatibles avec le droit international humanitaire et, d'autre part, à réglementer les autres. Cette approche est conforme aux appels lancés par le Secrétaire général et la Présidente du Comité international de la Croix-Rouge en faveur de l'adoption de nouvelles règles internationales pour protéger l'humanité<sup>34</sup>. Dans son rapport établi en application de la résolution 78/241 de l'Assemblée générale, la première portant sur les systèmes d'armes létaux autonomes, le Secrétaire général a exhorté les États à conclure, d'ici à 2026, un instrument juridiquement contraignant en vue d'interdire les systèmes qui fonctionnent sans supervision ou contrôle humain et ne peuvent être utilisés conformément au droit international humanitaire et à réglementer tous les autres types de systèmes d'armes autonomes<sup>35</sup>. En revanche, les États restent partagés sur la question de savoir si ces réglementations devraient être juridiquement contraignantes ou facultatives<sup>36</sup>. Par ailleurs, un débat sur le droit international des droits de l'homme et les systèmes d'armes autonomes est nécessaire.

---

*Review*, vol. 164, n° 6 et Valadares Fernandes Barbosa, *Autonomous Weapons Systems and the Responsibility of States*.

<sup>32</sup> Tobias Vestner Altea Rossi (2021), « Legal reviews of war algorithms », *International Law Studies*, vol. 97.

<sup>33</sup> Voir A/HRC/23/47.

<sup>34</sup> Voir <https://www.icrc.org/en/document/joint-call-un-and-icrc-establish-prohibitions-and-restrictions-autonomous-weapons-systems>.

<sup>35</sup> A/79/88, par. 90.

<sup>36</sup> Ibid., par. 63 à 86.

### C. Technologies d'amélioration des capacités humaines dans le domaine militaire

34. Bien qu'elles ouvrent de nouvelles perspectives en ce qui concerne les stratégies non létales et la réduction du stress en situation de conflit, les technologies d'amélioration des capacités physiques et cognitives soulèvent d'importantes questions éthiques, juridiques, sociétales et opérationnelles. Leurs effets sur les valeurs militaires, les dilemmes opérationnels, l'application du droit militaire et le consentement éclairé, notamment, figurent parmi les préoccupations exprimées. En outre, chaque type d'amélioration, qu'il soit d'ordre génétique, biologique ou cybernétique, comporte des risques en matière de droits de l'homme et d'éthique. Les avancées similaires observées dans le secteur civil, notamment sur le lieu de travail, montrent que ces technologies ont des répercussions profondes et sont par nature ambivalentes<sup>37</sup>.

35. Les progrès de l'IA élargissent le champ des possibilités offertes par les technologies d'amélioration des capacités de l'être humain, car cette technologie joue un rôle essentiel dans les traitements médicaux et la rééducation des troubles physiques et cognitifs dans des contextes civils<sup>38</sup>. Jusqu'à présent, l'amélioration des capacités humaines visait en priorité à assurer la réussite de la mission, parfois au détriment du bien-être des combattants. Dans ce contexte, il peut être difficile pour les soldats et les médecins militaires de recourir de façon autonome à des traitements neurotechnologiques (par exemple, administrer des pilules ou installer des implants neuronaux ou des neuroprothèses). Il est essentiel de garantir la transparence et le respect de la dignité humaine et du droit à la santé, notamment l'autonomie de prise de décisions et l'état de santé des combattants aux capacités améliorées dès lors qu'ils ne sont plus en service actif<sup>39</sup>.

36. Dans le domaine militaire, l'adoption de technologies telles que les interfaces cerveau-ordinateur est censée améliorer les capacités cognitives par la fusion de l'intelligence humaine et de l'intelligence de la machine. Si le développement de la robotique et des neurotechnologies, telles que les interfaces cerveau-ordinateur, offre des perspectives prometteuses dans le domaine des soins de santé, leur utilisation dans le contexte militaire soulève des difficultés particulières, notamment eu égard à l'application des lois relatives à la responsabilité et à l'exercice d'un contrôle humain sur les opérations militaires et la prise de décisions. Les interfaces cerveau-ordinateur et d'autres neurotechnologies de pointe pourraient également être détournées à des fins d'interrogatoires coercitifs dans le cadre d'hostilités. Le recours à de telles méthodes pourrait violer les droits de l'homme en ce qu'elles pourraient provoquer des dommages psychologiques ou être constitutives d'actes de torture, même en l'absence de violence physique<sup>40</sup>.

37. L'intégration de nouvelles technologies d'amélioration des capacités de l'être humain dans les activités militaires soulève de vives inquiétudes quant aux implications juridiques et aux violations potentielles des droits de l'homme auxquelles ces technologies pourraient donner lieu, du fait des risques qu'elles présentent, notamment en ce qui concerne le droit à la protection de la vie privée, l'obtention nécessaire du consentement libre et éclairé, et les atteintes à long terme qu'elles pourraient causer à l'intégrité physique et mentale des combattants. Les États et les entreprises ont le devoir de remédier à ces risques conformément aux dispositions applicables du droit international<sup>41</sup>.

<sup>37</sup> Timo Istace et Milena Costas Trascasas (2024), « Between science-fact and science-fiction », Research Brief (Genève, Académie de droit international humanitaire et de droits humains).

<sup>38</sup> Yuval Shany et Tal Mimran (2022), « Integrating privacy concerns in the development and introduction of new military or dual use technologies », in *The Rights to Privacy and Data Protection in Times of Armed Conflict*, Asaf Lubin et Russel Buchan, dir. publ. (Tallinn, NATO CCDCOE Publications) et Margaret Kosal et Joy Putney (2023), « Neurotechnology and international security », *Politics and the Life Sciences*, vol. 42, n° 1.

<sup>39</sup> Sebastian Sattler *et al.* (2022), « Neuroenhancements in the military » *Neuroethics*, vol. 15, n° 1.

<sup>40</sup> Charles N. Munyon (2018), « Neuroethics of non-primary brain computer interface », *Frontiers in Neuroscience*.

<sup>41</sup> Voir A/HRC/57/61.

38. En outre, les asymétries de pouvoir propres au domaine militaire, conjuguées aux conséquences à long terme des pratiques de collecte, de traitement et de conservation des données à caractère personnel, peuvent entraîner des violations du droit à la protection de la vie privée qui ne se manifesteront que bien plus tard. Par exemple, l'utilisation de ces technologies à des fins coercitives pourrait porter profondément atteinte à la dignité et à l'autonomie des soldats. Quant aux applications non coercitives, elles soulèvent de graves questions éthiques concernant le consentement et les effets à long terme sur la santé. Ces considérations devraient conduire à ce qu'on interdise expressément toute utilisation à des fins coercitives de ces technologies et qu'on mette en place des moratoires ou des restrictions sur leurs usages non coercitifs, afin qu'elles ne soient pas détournées<sup>42</sup>.

#### **D. Maintien de l'ordre et contrôle aux frontières**

39. Les technologies telles que la surveillance par l'IA, la modélisation prédictive et les systèmes biométriques sont de plus en plus utilisées par les autorités chargées du contrôle aux frontières et les forces de l'ordre. Si ces outils sont souvent loués pour leur capacité à renforcer la sécurité publique, parce qu'ils permettent d'optimiser les interventions d'urgence, d'organiser des passages sécurisés et sans encombre aux frontières, et contribuent à prévenir la criminalité, ils présentent également de graves risques pour les droits de l'homme<sup>43</sup>.

40. Les applications biométriques dans ce domaine visent à vérifier l'identité des personnes lors du contrôle d'accès et à les identifier lors de leur l'arrestation ou de leur placement en détention. Ces systèmes ne sont pas infaillibles. Pourtant, on ne s'est guère penché sur les effets, du point de vue des droits de l'homme, que pourrait avoir leur utilisation dans le domaine militaire, en particulier sur les groupes vulnérables, notamment les personnes handicapées, les personnes âgées, les enfants, les personnes d'ascendance africaine, les migrants et d'autres personnes historiquement ou structurellement victimes de discrimination. Il est à craindre que leur application ne renforce les inégalités, du fait de biais et d'un profilage discriminatoire qui résultent souvent de préjugés ancrés de longue date dans les pratiques de collecte, de traitement et de conservation des données. En matière de gestion des migrations, la diversité des données biométriques, sous l'effet des différences culturelles, peut accentuer ces biais. Par exemple, les technologies biométriques telles que la reconnaissance faciale pourraient violer le droit à la non-discrimination, car elles ont tendance à commettre des erreurs lors de l'identification des personnes issues de peuples autochtones ou d'ascendance africaine, en particulier les femmes. Elles peuvent également porter atteinte au droit à la protection de la vie privée si les gouvernements et les entreprises diffusent des données biométriques sans le consentement des personnes concernées. Étant donné l'importance accordée aux droits à la protection de la vie privée, à l'égalité et à la non-discrimination, qui sont expressément définis dans le droit international des droits de l'homme, il est essentiel de procéder à des évaluations de l'incidence de ces technologies sur les droits de l'homme et d'examiner la manière dont elles risquent de creuser les inégalités existantes<sup>44</sup>.

41. Les systèmes de surveillance optique, notamment aérienne, mobilisent aujourd'hui des moyens sans précédent qui permettent de surveiller, d'enregistrer et de suivre à distance les personnes dans bas l'espace public, y compris aux frontières, au moyen de technologies telles que les drones et la reconnaissance faciale. Ces progrès font peser de graves risques sur les droits de l'homme, notamment le droit à la liberté de circulation, le droit d'association et de réunion, le droit au respect de la vie privée et le droit à la non-discrimination.

42. Depuis quelques années, les systèmes d'armes autonomes retiennent de plus en plus l'attention. Si l'on met particulièrement en avant leur utilisation dans les conflits armés, il est de plus en plus évident que leur emploi est également envisagé pour la gestion des frontières et le maintien de l'ordre. Une telle évolution suscite de vives inquiétudes relatives aux droits de l'homme, notamment en ce qui concerne les droits à la vie, à l'intégrité corporelle et à la dignité. Contrairement aux militaires intervenant dans des conflits armés, dans le cadre

<sup>42</sup> Ibid., par. 80 b).

<sup>43</sup> Matias Leese *et al.* (2022), « Data matters », *Geopolitics*, vol. 27, n° 1.

<sup>44</sup> Voir A/HRC/51/17.

desquels l'emploi de la force est principalement régi par le droit international humanitaire, les forces de l'ordre peuvent recourir à la force seulement lorsque cela est inévitable, strictement nécessaire et dans la mesure exigée par l'accomplissement de leurs fonctions<sup>45</sup>.

## E. Guerre cognitive

43. La guerre cognitive vise à contrôler les pensées et les perceptions d'un adversaire dans le but d'influencer ses décisions et ses actions<sup>46</sup>. Ancrée dans la désinformation militaire, elle marque un nouveau cap stratégique qui a pu être franchi grâce au pouvoir transformateur de l'IA. Les technologies avancées permettent d'exercer une influence psychologique à grande échelle grâce au ciblage des capacités intellectuelles à l'insu de la personne visée et avec une précision accrue. Elles procurent des avantages stratégiques en permettant de modifier les perceptions et d'exploiter les vulnérabilités liées à la prise de décisions.

44. Si, à elle seule, la guerre cognitive ne suffit pas à l'emporter sur l'adversaire, elle peut permettre de le dominer lorsqu'elle est associée à des opérations physiques ou informationnelles comme la désinformation pilotée par l'IA. Les non-combattants, notamment les civils, sont de plus en plus exposés aux stratégies de guerre cognitive, ce qui soulève de graves préoccupations quant à la protection des droits de l'homme dans ce domaine. De telles tactiques pourraient porter atteinte aux droits de l'homme, notamment le droit à la protection de la vie privée (en raison de la collecte de données et du profilage), le droit à la liberté d'opinion et d'expression (en raison de la manipulation et de la désinformation), le droit d'accéder à des informations véridiques et le droit à l'intégrité psychologique. En outre, les opérations cognitives ciblées risquent d'aggraver la discrimination fondée sur l'appartenance ethnique, la religion, le genre ou l'affiliation politique, ce qui pourrait constituer une violation du droit à la non-discrimination.

45. Le développement rapide de l'IA modifie profondément la diffusion de l'information, faisant de la cognition humaine un champ essentiel de la confrontation militaire. En outre, des simulations de réalité virtuelle, dans des conditions de stress aigu, sont utilisées pour l'entraînement au combat, et les données recueillies contribueront à la préparation des combattants. Ces évolutions soulignent l'importance des enjeux de la concurrence entre les États dans le domaine cognitif<sup>47</sup>.

## F. Convergence potentielle de l'intelligence artificielle et des technologies biologiques, notamment les armes biologiques

46. Désormais partie intégrante des sciences de la vie, l'IA permet des avancées biotechnologiques qui contribuent à relever des défis mondiaux tels que la sécurité alimentaire et l'accès à l'eau potable. Toutefois, l'intégration de l'IA dans la biotechnologie, notamment sous la forme d'armes biologiques améliorées par l'IA, peut présenter de graves risques pour les droits de l'homme. La mise au point, la fabrication, l'acquisition, le transfert, le stockage et l'emploi des armes biologiques sont interdits par la Convention sur les armes biologiques. Cette interdiction est générale et s'applique quelles que soient les technologies utilisées, y compris donc aux armes biologiques améliorées par l'IA.

47. L'intégration de l'IA à la biologie synthétique, qui consiste à reprogrammer des organismes à des fins précises, pourrait faciliter la création d'organismes entièrement nouveaux dont les caractéristiques seraient taillées sur mesure. Elle présente le risque d'un développement imprévu et dangereux d'agents biologiques pouvant conduire à de nouvelles formes de menaces biologiques<sup>48</sup>. En outre, si l'IA peut faciliter l'accès à l'information et la

<sup>45</sup> Code de conduite pour les responsables de l'application des lois.

<sup>46</sup> Jean-Marc Rickli, Federico Mantellassi et Gwyn Glasser (2023), « Peace of mind », Policy Brief n° 9 (Genève, Geneva Centre for Security Policy).

<sup>47</sup> Voir <https://www.act.nato.int/activities/cognitive-warfare/>.

<sup>48</sup> Anshula Sharma *et al.* (2020), « Next generation agents (synthetic agents) », in *Handbook on Biological Warfare Preparedness*, S. J. S Flora et Vidhu Pachauri, dir. publ. (Londres, Elsevier).

diffusion des connaissances, elle peut également accroître les risques liés à la biosécurité en autorisant le transfert d'informations sensibles à des acteurs malavés ou malveillants<sup>49</sup>.

48. Les armes biologiques améliorées par l'IA peuvent porter atteinte aux droits à la vie, à l'intégrité, à la santé et à un environnement propre, sain et durable. Elles pourraient en outre poser des problèmes de biosécurité et de biosûreté, notamment en ce qui concerne la détection d'une attaque et l'attribution de son origine, lorsqu'elles sont délibérément conçues pour échapper aux systèmes de détection existants. Il serait ainsi difficile de déceler l'attaque d'un adversaire et d'y riposter. Par ailleurs, les armes biologiques pourraient être conçues de façon à imiter les épidémies d'origine naturelle, de sorte qu'il serait difficile de les imputer à tel ou tel adversaire et d'en déterminer l'origine, ce qui empêcherait d'y réagir de manière appropriée et pourrait entraver l'exercice du droit à un recours utile<sup>50</sup>.

49. Pour éliminer ces risques, il est indispensable d'adopter une approche multidimensionnelle fondée sur les droits de l'homme, notamment en faisant respecter le droit international des droits de l'homme et en appliquant les cadres internationaux tels que la Convention sur les armes biologiques, en mettant en œuvre une coopération multilatérale et en investissant dans la biosécurité et la recherche sur les technologies défensives.

## G. Intelligence artificielle et systèmes de commandement et de contrôle nucléaires

50. Si les États dotés d'une capacité nucléaire ont conscience, dans une certaine mesure, des risques associés à l'intégration de l'IA dans les systèmes de commandement et de contrôle nucléaires à des fins d'appréciation de la situation et de détection des menaces, la recherche d'un avantage stratégique dans un contexte nucléaire en constante évolution, conjuguée à la crainte d'être à la traîne de l'innovation en matière d'IA, pourrait favoriser l'adoption précipitée et prématurée de ces technologies<sup>51</sup>. Il est important de faire la distinction entre l'utilisation qui est faite des systèmes d'IA pour apprécier la situation et détecter les menaces, et celle qui pourrait en être faite lors de la prise de décisions concernant les armes nucléaires. Actuellement, il semble que l'IA soit surtout utilisée dans les systèmes de commandement, de contrôle et de communication nucléaires pour la détection précoce des menaces, la collecte de renseignements et l'aide à la décision. S'il existe bien, selon les informations disponibles, un système automatique conçu pour être utilisé en cas de frappe décapitante, celui-ci est antérieur aux progrès actuels de l'IA. La fiabilité de l'IA et ses effets sur ces systèmes sont une source de préoccupation, en particulier si des progrès futurs conduisent les acteurs à être plus fortement tributaires des décisions prises par cette technologie<sup>52</sup>.

51. Il est plus difficile d'intégrer une IA avancée basée sur l'apprentissage profond que d'appliquer des modèles existants fondés sur des règles. Les principales préoccupations à cet égard ont notamment trait à la fiabilité, à la transparence, à la vulnérabilité aux attaques adverses et au défaut d'alignement des modèles à grande échelle utilisés pour des fonctions critiques, telles que la prise de décisions liée aux armes nucléaires<sup>53</sup>. Les modèles d'apprentissage profond sont par nature opaques, d'où la difficulté à interpréter les processus décisionnels les concernant, ce qui peut donner lieu à des résultats imprévisibles et compliquer le contrôle humain. En outre, l'accélération des cycles de décision due à l'IA, qui fonctionne à des vitesses supérieures aux capacités humaines, pourrait réduire le temps disponible pour prendre une décision de riposte nucléaire, au point qu'il serait difficile pour

<sup>49</sup> Zhaohui Su *et al.* (2021), « Addressing biodisaster X threats with artificial intelligence and 6G technologies », *Journal of Medical Internet Research*, vol. 23, n° 5 et Renan Chaves de Lima *et al.* (2024), « Artificial intelligence challenges in the face of biological threats », *Frontiers in Artificial Intelligence*.

<sup>50</sup> Connor O'Brien, Kathleen Varty et Anna Ignaszak (2021), « The electrochemical detection of bioterrorism agents », *Microsystems and Nanoengineering*, vol. 7, n° 1.

<sup>51</sup> Voir <https://warontherocks.com/2024/12/beyond-human-in-the-loop-managing-ai-risks-in-nuclear-command-and-control/>.

<sup>52</sup> Alice Saltini (2023), « AI and nuclear command, control and communications » (Londres, European Leadership Network).

<sup>53</sup> Ibid.

un humain d'exercer un contrôle efficace. Cette situation soulève de profondes préoccupations quant au respect de la dignité humaine et des droits de l'homme, notamment les droits à la vie, à l'intégrité, à la non-discrimination, à la santé et à un environnement sain.

52. En outre, le risque que les systèmes d'IA interprètent à tort des activités anodines ou des fausses alertes comme des menaces pourrait provoquer une escalade involontaire. Un autre sujet de préoccupation est le biais d'automatisation, selon lequel les opérateurs humains risquent de se fier de manière excessive aux décisions prises par les systèmes d'IA, même lorsque l'intuition humaine, l'expérience acquise par la formation ou d'autres renseignements recommanderaient d'adopter une autre ligne de conduite. On risquerait alors de commettre des erreurs de jugement dont les conséquences seraient extrêmement graves. Les activités malveillantes dans le domaine des technologies de l'information et des communications (TIC) visant des systèmes basés sur l'IA pourraient permettre à des adversaires de s'infiltrer, de désactiver, de manipuler ou d'altérer les réponses, provoquant des incertitudes et des erreurs d'appréciation ou des actions involontaires<sup>54</sup>. En outre, sachant que l'entraînement des systèmes d'IA nécessite de vastes ensembles de données, des adversaires pourraient corrompre ces données, ce qui entraînerait des processus décisionnels erronés, voire des violations du droit de l'homme à la non-discrimination.

53. L'intégration de l'IA dans les systèmes de commandement et de contrôle nucléaires comporte des risques importants auxquels il convient de remédier avec soin en s'appuyant sur des évaluations des risques, des garanties techniques, des considérations éthiques et des cadres juridiques solides. La rapidité des progrès dans le domaine de l'IA nécessite de prendre les devants et d'adopter une approche dynamique qui permette de renforcer les mécanismes propres à garantir un déploiement responsable et sûr des systèmes d'IA, dans le respect du droit international des droits de l'homme.

## H. Armes à énergie dirigée

54. Les armes à énergie dirigée sont des systèmes qui émettent des formes concentrées d'énergie dans une direction particulière, sans recourir à des projectiles. Dans les applications militaires, ces armes utilisent la technologie électromagnétique ou la technologie des particules plutôt que la force cinétique pour neutraliser ou détruire des cibles. Les lasers, les micro-ondes, les ondes millimétriques et les faisceaux de particules en sont quelques exemples. Ils peuvent être utilisés à des fins non létales, comme le brouillage ou l'aveuglement d'êtres humains ou d'appareils et de systèmes électroniques<sup>55</sup>. Lorsqu'elles sont utilisées à des fins militaires, les armes à énergie dirigée peuvent endommager des cibles physiques à plusieurs kilomètres avec une grande précision.

55. Au fur et à mesure des progrès de la technologie des armes à énergie dirigée, les systèmes d'armes deviendront plus puissants, plus répandus et plus intégrés dans les plateformes aériennes, terrestres, maritimes et spatiales. Leur action ultrarapide (à la vitesse de la lumière), leur précision, leur évolutivité, leur efficacité logistique et leur faible coût par tir offrent des avantages dans les applications civiles comme dans les applications militaires<sup>56</sup>.

56. Dans le contexte militaire, les armes à énergie dirigée peuvent toucher les civils. Si des incertitudes subsistent quant à leur caractère opérationnel, les prototypes et les applications utilisés récemment montrent, compte tenu des progrès accomplis, qu'on est au-delà de la phase théorique<sup>57</sup>. Ces armes peuvent provoquer de graves blessures pouvant aller jusqu'à la cécité et des brûlures. Par exemple, les armes lasers à grande énergie peuvent brûler les tissus, tandis que les armes à micro-ondes provoquent d'intenses douleurs en

<sup>54</sup> Muhammad Mudassar Yamin *et al.* (2021), « Weaponized AI for cyber-attacks », *Journal of Information Security and Applications*, n° 57.

<sup>55</sup> Bhaman Zohuri (2016), *Directed Energy Weapons* (Suisse, Springer).

<sup>56</sup> Voir <https://www.nationaldefensemagazine.org/articles/2020/10/13/uptick-in-spending-seen-for-directed-energy-weapons>.

<sup>57</sup> Voir <https://article36.org/wp-content/uploads/2019/06/directed-energy-weapons.pdf> et <https://nualslawjournal.com/2023/07/25/bringing-directed-energy-weapons-within-the-purview-of-the-arms-control-regime>.

chauffant les liquides organiques, ce qui peut causer des blessures graves et durables<sup>58</sup>. Compte tenu de ces effets, ces armes et les incidences de la technologie à énergie directe soulèvent de profondes préoccupations relatives aux droits de l'homme, notamment en ce qui concerne le droit à la santé et à l'intégrité corporelle, voire le droit à la vie et à un environnement sain. Il importe de rappeler que le Protocole additionnel 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 interdit l'utilisation des armes lasers conçues spécialement pour provoquer une cécité permanente.

### **III. Rôle des acteurs étatiques et non étatiques dans la conception, le déploiement, l'utilisation et l'acquisition de technologies nouvelles et émergentes dans le domaine militaire et la formation à ces outils**

#### **A. Obligations des États de prévenir les violations du droit international et de réglementer et surveiller l'utilisation des technologies nouvelles et émergentes dans le domaine militaire**

57. Il faut tenir compte des obligations juridiques internationales lors de la conception, de la mise au point et de l'utilisation des technologies nouvelles et émergentes dans le domaine militaire. Les États sont tenus de veiller à ce que l'application de ces technologies soit pleinement conforme à la législation internationale en matière de droits de l'homme, notamment les droits à la vie, à l'intégrité physique, à la non-discrimination, au respect de la vie privée et à un environnement sain. Les obligations en matière de droit international humanitaire sont particulièrement pertinentes : les États doivent non seulement en respecter les règles – qui imposent des interdictions et des restrictions s'agissant des armes et des moyens et méthodes de guerre –, mais aussi faire respecter ce droit lui-même. Toutefois, cette dernière obligation reste définie de manière imprécise, ce qui fait que certains aspects sont sujets à interprétation. En outre, les États doivent procéder à des examens approfondis de la légalité de leurs armements.

58. L'obligation de faire respecter le droit international exige des États qu'ils veillent à ce que ce droit soit mis en œuvre et appliqué au niveau national, en s'assurant qu'une obligation de diligence raisonnable soit étendue à toutes les mesures prises pour prévenir les violations par les acteurs publics ou privés, notamment les développeurs de technologies nouvelles et émergentes. S'agissant de la diligence raisonnable, la responsabilité d'un État peut être engagée dans les deux cas suivants : a) s'il dispose des moyens d'empêcher ou de réprimer la violation ; b) s'il connaissait ou aurait dû connaître le risque de violation<sup>59</sup>. Cette responsabilité s'étend tout au long du cycle de vie des technologies nouvelles et émergentes, conformément au droit international. En outre, les États doivent en permanence évaluer les risques.

59. Les États sont tenus de prendre des mesures pour prévenir les violations des droits de l'homme relevant de leur juridiction<sup>60</sup>. Le non-respect de cette obligation peut entraîner une responsabilité internationale. Le déploiement de technologies nouvelles et émergentes dans le domaine militaire impose probablement des obligations supplémentaires et des normes de diligence raisonnable renforcées afin de garantir que toutes les précautions possibles sont prises.

60. Un État peut également être tenu responsable des conséquences des agissements d'acteurs privés s'il ne prend pas les mesures nécessaires pour prévenir, surveiller et

<sup>58</sup> Gary M. Vilke et Theodore C. Chan (2007), « Less lethal technology:medical issues », *Policing: An International Journal*, vol. 30, n° 3 et Erdem Eren Demir *et al.* (2022), « The role of non-lethal weapons in public security », *Journal of Criminal Law and Criminology*, vol. 60, n° 3.

<sup>59</sup> Antal Berkes (2018), « The standard of 'Due Diligence' as a result of interchange between the law of armed conflict and general international law », *Journal of Conflict and Security Law*, vol. 23, n° 3.

<sup>60</sup> Voir A/HRC/30/20.

réglementer leurs activités, ou mener des enquêtes à ce sujet et prendre des sanctions<sup>61</sup>. Par conséquent, les États doivent se conformer aux obligations de diligence raisonnable s’agissant de la mise au point, de l’acquisition et de l’utilisation de technologies nouvelles et émergentes dans le domaine militaire par des acteurs non étatiques.

61. Les entreprises privées, en particulier dans le domaine de l’IA, développent des technologies qui peuvent être adaptées à un usage militaire. Leur souhait de commercialiser leurs produits au plus vite les conduit souvent à sous-estimer les risques, notamment l’utilisation abusive de l’IA générative aux fins d’opérations informatiques malveillantes ou de campagnes de désinformation. Une autre préoccupation est la prolifération incontrôlée de ces technologies, qui permet à des acteurs non étatiques d’y accéder. Ces derniers emploient souvent des technologies nouvelles et émergentes dans le domaine militaire, en mettant en œuvre moins de garanties et en ayant des attentes moindres en termes de précision ou de fiabilité par rapport aux acteurs étatiques. Des acteurs non étatiques pourraient également utiliser des technologies nouvelles et émergentes pour perturber ou fausser les systèmes de communication, de façon à compromettre leur précision et leur fiabilité.

62. L’IA et les dispositifs connectés à l’Internet des objets<sup>62</sup>, du fait de leur développement rapide, sont appelés à jouer un rôle clef dans les cyberopérations militaires. L’utilisation de ces technologies pourrait créer ou agraver des vulnérabilités, ce qui permettrait à des acteurs non étatiques de manipuler l’IA, de compromettre les systèmes de l’IoT, de perturber des services essentiels tels que les soins de santé ou de se livrer à la cybercriminalité. De telles attaques peuvent entraîner des violations de données, des défaillances opérationnelles et des dommages physiques et menacer la vie ou l’intégrité des personnes<sup>63</sup>.

63. Compte tenu des nombreux risques liés à l’acquisition ou au développement par des acteurs non étatiques de technologies nouvelles et émergentes dans le domaine militaire, les États ont une obligation juridique internationale essentielle de diligence raisonnable, qui consiste à enquêter sur les violations des droits de l’homme, à mettre en place des voies de recours et à sanctionner les auteurs de violation. Pour cela, ils doivent par exemple mettre en place un cadre réglementaire solide protégeant les droits à la vie, à l’intégrité, à la non-discrimination, à la santé, à un environnement sain et à la vie privée, renforcer leurs activités de surveillance, notamment en matière de cybersécurité, développer la coopération internationale, et fournir aux parties prenantes une formation complète sur les risques potentiels liés à l’utilisation abusive des technologies nouvelles et émergentes dans le domaine militaire. À défaut, ils devraient faire face à des violations des droits à la vie, à l’intégrité, à la vie privée et à la non-discrimination.

## B. Fournisseurs de technologies nouvelles et émergentes dans le domaine militaire et entreprises du secteur

64. Les États sont les premiers utilisateurs de technologies nouvelles et émergentes pour la défense nationale et la sécurité publique. Ils favorisent également leur développement en finançant la recherche et en encourageant les partenariats public-privé. Les entités privées, notamment les entreprises d’armement et les entreprises du secteur informatique, jouent un rôle d’innovateurs et de développeurs en fournissant des services liés à la mise au point de ces technologies, à leur déploiement, à la maintenance et à la formation.

65. Au niveau national, les États ont un rôle de réglementation des technologies nouvelles et émergentes, qui se traduit par la mise en place de cadres juridiques et de normes que les entreprises doivent respecter et qui doivent permettre aux États de satisfaire à leurs obligations au regard du droit international des droits de l’homme. Ce droit impose aux États des obligations contraignantes en matière de respect, de protection et de réalisation des droits

<sup>61</sup> Articles sur la responsabilité de l’État pour fait internationalement illicite.

<sup>62</sup> L’IoT est un réseau de dispositifs interconnectés qui partagent des données en temps réel. Dans le domaine militaire, il relie les capteurs, les véhicules et les équipements afin d’améliorer la surveillance et la logistique et de faciliter la prise de décisions.

<sup>63</sup> Nicholas Tsagourias (2012), « Cyber attacks, self-defence and the problem of attribution », *Journal of Conflict and Security Law*, vol. 17, n° 2.

de l'homme s'agissant des technologies nouvelles et émergentes dans le domaine militaire. En outre, les entreprises concernées doivent se conformer à l'ensemble de la législation et respecter les droits de l'homme, comme le soulignent les Principes directeurs. Cette responsabilité s'applique à toutes les entreprises, notamment les entreprises technologiques, quelle que soit leur taille ou leur structure<sup>64</sup>. Les entreprises doivent prévenir les violations des droits de l'homme et remédier à leurs effets négatifs. En cas de violation, les États ont le devoir d'enquêter et de veiller à ce que les victimes aient accès à des recours effectifs, notamment par des voies judiciaires ou non judiciaires appropriées. Les Principes directeurs et le Groupe de travail sur les entreprises et les droits de l'homme jouent à cet égard un rôle essentiel. Dans ce contexte, le Groupe de travail a constaté que les entreprises d'armement négligeaient souvent de faire preuve de diligence raisonnable en matière de droits de l'homme, en particulier s'agissant de l'évaluation des risques liés à l'utilisation de leurs produits lors d'un conflit<sup>65</sup>. Par ailleurs, dans le cadre de son projet B-Tech, le Haut-Commissariat aux droits de l'homme (HCDH) fournit des orientations de référence et des ressources destinées à faciliter l'application des Principes directeurs dans le domaine technologique et invite les entreprises et les décideurs à adopter une approche fondée sur les droits de l'homme pour relever les défis posés par les nouvelles technologies<sup>66</sup>.

## **IV. Les droits de l'homme dans le cycle de vie des technologies nouvelles et émergentes dans le domaine militaire**

### **A. La perspective du cycle de vie**

66. Les technologies nouvelles et émergentes dans le domaine militaire posent des difficultés inédites s'agissant de la protection de la promotion des droits de l'homme. Nombre de ces technologies sont à double usage, ce qui rend la situation plus complexe en ce qui concerne la répartition des responsabilités entre les États et les acteurs privés. Il est essentiel de mettre en œuvre une approche approfondie du cycle de vie pour pouvoir relever ce défi en veillant à ce que les droits de l'homme soient protégés à toutes les étapes, depuis le développement et la formation jusqu'au déploiement, à l'utilisation opérationnelle et éventuellement à la mise hors service ou au démantèlement.

#### **1. Intégrer les droits de l'homme dans les phases de conception et de développement**

67. La phase de conceptualisation et de conception des technologies nouvelles et émergentes dans le domaine militaire est le moment le plus adéquat pour intégrer les considérations relatives aux droits de l'homme. Au cours de cette période initiale d'idéation, il convient d'évaluer avec rigueur les incidences potentielles en matière de droits de l'homme. Les technologies ne sont pas neutres ; elles orientent par nature l'élaboration des politiques et peuvent restreindre les libertés individuelles<sup>67</sup>. Ainsi, la technologie elle-même et ses créateurs peuvent porter atteinte aux droits de l'homme, car ils incarnent souvent des valeurs et des préjugés précis<sup>68</sup>.

68. Au cours de ces premières phases, il est essentiel de procéder à des évaluations de l'impact des technologies sur les droits de l'homme. Il faut intégrer ces évaluations dans le processus de développement afin de recenser les risques potentiels pour les droits de l'homme et de les atténuer, s'agissant notamment des droits à la vie privée, à la liberté d'expression, à la vie, à l'intégrité, à la santé et à un environnement sain. Si le fait de tenir compte de ces considérations dans la phase de conception peut aider les développeurs à minimiser les effets pervers et les utilisations abusives, il ne peut entièrement résoudre les tensions juridiques inhérentes à certaines technologies. Des questions subsistent quant à savoir si des technologies telles que celles utilisées dans les systèmes d'armes autonomes pourront un jour

<sup>64</sup> Voir <https://www.ohchr.org/sites/default/files/2021-11/tech-2021-response-export-military-software.pdf>.

<sup>65</sup> Voir <https://www.ohchr.org/sites/default/files/2022-08/BHR-Arms-sector-info-note.pdf>.

<sup>66</sup> Voir <https://untoday.org/un-b-tech-project/>.

<sup>67</sup> A/HRC/47/52, par. 4.

<sup>68</sup> Andrew Feenberg (2002), *Transforming Technology* (Oxford, Oxford University Press) et Cathy O'Neil (2016), *Weapons of Math Destruction* (New York, Crown).

être pleinement compatibles avec les normes relatives aux droits de l'homme, en particulier si leur utilisation va à l'encontre de principes tels que la protection de la dignité humaine. Par conséquent, le respect des normes internationales relatives aux droits de l'homme peut, dans certains cas, nécessiter des cadres réglementaires d'ensemble qui couvrent les questions juridiques uniques soulevées par ces technologies.

69. Le développement de technologies nouvelles et émergentes dans le domaine militaire implique souvent l'utilisation de vastes ensembles de données qui peuvent intégrer et perpétuer des préjugés. Pour prévenir la discrimination, il est essentiel, pendant la phase de conception, de mettre en œuvre des algorithmes tenant compte de l'équité et de l'analyse d'une situation fictive. Les développeurs doivent veiller à la diversité de leur personnel et réaliser des audits de la diversité afin de réduire la probabilité que soient utilisés des ensembles de données et des programmes biaisés qui renforcent les préjugés.

70. Les entreprises qui participent au développement des technologies nouvelles et émergentes ont le devoir de veiller à ce que leurs pratiques respectent le droit international des droits de l'homme, en particulier les Principes directeurs. Elles doivent notamment s'assurer que leurs technologies ne contribuent pas à des violations des droits de l'homme, dans des contextes militaires ou civils. Les États ayant un devoir de diligence raisonnable, ils doivent réglementer ces domaines où opèrent des acteurs privés et établir au niveau national des obligations pour les entreprises de respecter les droits de l'homme.

## **2. Gérer les risques pendant les phases de déploiement et d'utilisation opérationnelle**

71. Le risque de violation des droits de l'homme augmente à mesure que les technologies nouvelles et émergentes deviennent opérationnelles. Il est essentiel d'établir des normes juridiques strictes qui garantissent la dignité humaine, la mise en œuvre d'un contrôle humain significatif et le respect des principes de transparence et de responsabilité, en particulier dans les cas où l'automatisation et l'IA peuvent entraîner une perte du contrôle humain significatif, des biais liés à l'automatisation ou une utilisation abusive de la technologie d'une manière contraire au droit international.

72. Afin d'éviter les préjugés, il convient d'associer des groupes diversifiés aux processus de vérification, d'essais et d'évaluation, en tenant compte de facteurs tels que l'âge, la race et le sexe. Cela permet de s'assurer que l'utilisation des technologies nouvelles et émergentes dans le domaine militaire n'accroît pas les effets négatifs des armes sur les droits humains des populations vulnérables et ne perpétue pas les inégalités existantes. Les États devraient adopter un cadre réglementaire fondé sur le risque et appliquer des réglementations strictes ou des interdictions pour les technologies à haut risque qui représentent des menaces importantes pour la vie, la santé, la sécurité personnelle et d'autres droits de l'homme.

73. La transparence est un aspect crucial du déploiement des technologies nouvelles et émergentes, notamment en ce qui concerne les données et les algorithmes utilisés. Il faut prendre des mesures de diligence raisonnable en mettant en œuvre des outils de détection des biais ou en réalisant un audit des algorithmes afin de repérer et de traiter les biais présents dans les produits fournis par les systèmes.

## **3. Garanties lors de la mise hors service ou du démantèlement et prévention de la prolifération**

74. La dernière étape du cycle de vie des technologies nouvelles et émergentes dans le domaine militaire – la mise hors service ou le démantèlement – s'accompagne d'un ensemble de considérations relatives aux droits de l'homme et à la sécurité qui lui sont propres. Il s'agit en particulier du démantèlement physique des outils technologiques, de l'élimination sûre des matières dangereuses et de la protection de toutes les données sensibles recueillies au cours de la phase opérationnelle. Pour lutter contre les risques de prolifération, il est essentiel de mettre en œuvre des garanties visant à empêcher le détournement de matériels et la vente non autorisée d'équipements excédentaires. Pour préserver les droits de l'homme, il faut veiller à ce que ces processus soient menés de manière transparente et responsable et

empêcher qu'ils aient des effets différenciés sur les groupes historiquement marginalisés tels que les populations autochtones et les femmes<sup>69</sup>.

75. Compte tenu de l'évolution rapide des technologies nouvelles et émergentes dans le domaine militaire, il est impératif de prendre des mesures proactives et globales pour faire respecter les droits de l'homme. L'analyse présentée ci-dessus souligne la nécessité d'un cadre juridique international renforcé, d'une responsabilisation accrue des entreprises et d'une intensification de la coopération multilatérale. En établissant des mécanismes de contrôle rigoureux et en promouvant la transparence et la responsabilité juridique, la communauté internationale peut veiller à ce que les processus de développement, de déploiement et de démantèlement des technologies nouvelles et émergentes dans le domaine militaire respectent les principes des droits de l'homme.

## B. Transparence et obligation de rendre compte

76. La prolifération des technologies nouvelles et émergentes pose des défis juridiques et réglementaires sans précédent. L'IA soulève la question de savoir si les cadres existants sont adaptés<sup>70</sup>. Dans les cas où il existe des risques élevés pour les droits de l'homme, de plus en plus de voix s'élèvent pour demander une révision rapide des cadres et la mise en place de nouveaux mécanismes de transparence et de responsabilité<sup>71</sup>.

77. Les technologies nouvelles et émergentes peuvent optimiser la réalisation de tâches complexes en agissant comme des multiplicateurs de force qui améliorent la vitesse, la précision et les capacités humaines<sup>72</sup>. Elles sont de plus en plus utilisées pour la collecte de renseignements, la surveillance, la reconnaissance, la prise de décision militaire et des tâches telles que la vérification et la sélection des cibles<sup>73</sup>. Cependant, ces systèmes sont souvent des boîtes noires dont le fonctionnement est difficile à interpréter, et encore plus à expliquer. Étant donné l'importance du caractère prévisible et compréhensible de l'IA, il est essentiel de veiller à ce que ces systèmes fonctionnent comme prévu et de manière intelligible. Les efforts déployés pour comprendre le fonctionnement interne de ces technologies sont de plus en plus novateurs et permettent d'obtenir des résultats significatifs en matière de transparence. La recherche visant à mieux comprendre l'IA a considérablement progressé et a permis d'améliorer la transparence des systèmes, ce qui pourrait faciliter leur adoption dans des domaines critiques à haut risque<sup>74</sup>. L'intérêt intrinsèque du développement de l'IA explicable est de répondre aux préoccupations concernant le manque de transparence et d'obligation de rendre compte. Toutefois, il ne faut pas sous-estimer les risques associés à la mise en œuvre de l'IA explicable, tels que les atteintes à la vie privée et les vulnérabilités des systèmes dues à une transparence accrue<sup>75</sup>.

78. Le droit international des droits de l'homme exige la transparence. Dans le contexte des technologies nouvelles et émergentes dans le domaine militaire, il s'agit de garantir l'accès à des informations pertinentes sur leur développement, leur déploiement et leurs effets. La transparence joue également un rôle essentiel dans leur utilisation de façon

<sup>69</sup> Voir A/75/290.

<sup>70</sup> Stefan Larsson et Fredrik Heintz (2020), « Transparency in artificial intelligence », *Internet Policy Review*, vol. 9, n° 2 et Jordan Richard Schoenherr *et al.* (2023), « Designing AI using a human-centered approach », *IEEE Transactions on Technology and Society*, vol. 4, n° 1.

<sup>71</sup> Voir A/HRC/48/31.

<sup>72</sup> Jonathan Han Chung Kwik et Tom van Engers (2021), « Algorithmic fog of war », *Journal of Future Robot Life*, vol. 2, n° 1.

<sup>73</sup> Hannah Bryce et Jacob Parakilas (2018), « Conclusions and recommendations », dans *Artificial Intelligence and International Affairs: Disruption Anticipated*, M. L. Cummings *et al.*, dir. publ. (Londres, Chatham House) et CICR (2019), « L'intelligence artificielle et l'apprentissage automatique dans les conflits armés : une approche centrée sur l'humain » (Genève).

<sup>74</sup> Arthur Holland Michel (2020), « The black box, unlocked » (Institut des Nations unies pour la recherche sur le désarmement), et Arun Das et Paul Rad (2020), « Opportunities and challenges in explainable artificial intelligence (XAI) », *arXiv preprint*.

<sup>75</sup> Voir [https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-2023-explainable-artificial-intelligence\\_en](https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-2023-explainable-artificial-intelligence_en).

respectueuse du droit international, de manière à ce que soient protégés les droits à la liberté d'opinion et d'expression, à la vie privée, à la non-discrimination et à l'égalité.

79. Par ailleurs, il convient, face aux risques qui caractérisent l'utilisation de technologies nouvelles et émergentes dans le domaine militaire, de veiller à ce que les capacités de prise de décision intégrées dans les systèmes ne reproduisent pas les préjugés existants et les formes de discrimination répandues dans la société. L'une des principales difficultés consiste à s'assurer que les lacunes des processus de collecte, de traitement et de conservation des données ne perpétuent pas ou n'aggravent pas les violations des droits de l'homme. Pour surmonter ces problèmes, il faut instaurer de la transparence et prendre des mesures énergiques visant à rendre tous les acteurs responsables de l'utilisation éthique et légale des technologies nouvelles et émergentes.

### C. Lacunes des cadres existants des droits de l'homme

80. Il est difficile d'appliquer les cadres existants des droits de l'homme aux technologies nouvelles et émergentes dans le domaine militaire. Il est essentiel de respecter le droit international, mais il existe des lacunes importantes qui doivent être comblées pour garantir la protection des droits de l'homme dans ce contexte. En dépit de l'importance des Principes directeurs et des travaux réalisés dans le cadre du projet B-Tech du HCDH, il n'existe pas de normes internationales en matière de droits de l'homme qui précisent, dans le contexte des technologies nouvelles et émergentes dans le domaine militaire, ce que le droit international exige à la fois des États et des acteurs non étatiques. En outre, au niveau national, l'utilisation des technologies nouvelles et émergentes dans le domaine militaire échappe dans une large mesure à la réglementation, faute de cadres législatifs ou directifs régissant la conception, le développement et l'essai de ces technologies et veillant à la mise en place de protections claires et conformes aux obligations juridiques internationales.

81. Par exemple, il n'existe pas de stratégies d'achat transparentes portant sur l'ensemble des technologies nouvelles et émergentes dans la chaîne d'approvisionnement du secteur militaire et établissant des garanties fondées sur le droit international des droits de l'homme, d'où des risques d'utilisation discriminatoire de certaines technologies. En outre, l'absence de mécanismes internationaux de contrôle du développement, de l'acquisition et de l'utilisation de ces technologies dans le domaine militaire empêche les États de s'acquitter efficacement de leurs obligations juridiques internationales, en particulier lorsqu'ils ne disposent pas d'une réglementation nationale adaptée. Si certains pays ont mis en place des cadres réglementaires, des lacunes importantes subsistent dans les procédures nationales de contrôle et d'audit fondées sur les Principes directeurs des activités des entreprises et fournisseurs de technologies nouvelles et émergentes du secteur privé, ce qui limite la capacité des États à garantir le respect des normes nationales et internationales en matière de droits de l'homme. Il est essentiel de combler ces lacunes réglementaires si l'on veut prévenir les violations des droits de l'homme et les atteintes à ces droits découlant du développement et de l'utilisation de technologies nouvelles et émergentes dans le domaine militaire.

82. Une autre lacune importante du cadre actuel des droits de l'homme concerne l'impact environnemental des technologies nouvelles et émergentes. Les activités de développement, d'entraînement et de déploiement sont très énergivores, ont une empreinte carbone importante et requièrent une utilisation intensive de matières premières telles que le nickel, le cobalt et le graphite, ce qui a des conséquences environnementales à long terme<sup>76</sup>. Cela concerne notamment le refroidissement des centres de données, qui nécessite beaucoup d'eau, et l'élimination des déchets dangereux au moment du démantèlement. Faute de cadres juridiques et de mécanismes d'application au niveau mondial, il est difficile de protéger les droits environnementaux. Pour respecter le droit de l'homme à un environnement sain, il faut communiquer l'information de façon transparente, exercer une surveillance environnementale rigoureuse et mettre en place un dispositif collaboratif d'application du principe de responsabilité.

<sup>76</sup> Wichuta Teeratanabodee (2022), « The environmental impact of military AI », IDSS Paper n° 39 (S. Rajaratnam School of International Studies).

## V. Recommandations

### A. À l'intention des États et de la communauté internationale

83. Les États devraient élaborer d'urgence des stratégies et des politiques nationales et réglementer la conception, la mise au point et l'utilisation responsables des technologies nouvelles et émergentes dans le domaine militaire, conformément aux obligations qui leur incombent en vertu du droit international. Il s'agit de créer des cadres solides d'examen de la légalité des armes pour permettre de faire face aux défis que posent les armes intégrant des technologies nouvelles et émergentes et de mettre en place, aux fins de leur mise au point et du déploiement de telles armes, des mécanismes de prévention et d'établissement des responsabilités. Par ailleurs, il faudrait renforcer les mécanismes institutionnels pour pouvoir anticiper les violations potentielles des droits de l'homme ou y remédier, en mettant particulièrement l'accent sur l'amélioration des capacités de contrôle des entités locales, telles que les institutions nationales des droits de l'homme.

84. Les États et les organisations internationales devraient intégrer les considérations relatives au droit international des droits de l'homme dans toute négociation multilatérale sur les technologies nouvelles et émergentes dans le domaine militaire, en particulier au sein du Groupe de travail II de la Commission du désarmement, dans le cadre de ses recommandations sur les interprétations communes relatives aux technologies émergentes dans le contexte de la sécurité internationale. Tout cadre qui serait élaboré doit tenir compte, au-delà des préoccupations en matière de sécurité, des risques liés aux droits de l'homme, y compris les pratiques discriminatoires. En outre, le cadre juridique international des droits de l'homme doit orienter les discussions sur les systèmes d'armes autonomes, notamment au sein du Groupe d'experts gouvernementaux.

85. Les États devraient établir des partenariats stratégiques pour relever les défis qui se posent en matière de sécurité. Des discussions suivies, des échanges de bonnes pratiques et des cadres inclusifs associant les États, le secteur privé, les milieux universitaires et d'autres parties prenantes contribueront à garantir la stabilité et à atténuer les risques. La priorité devrait également être donnée au partage des analyses des aspects juridiques des technologies nouvelles et émergentes dans le domaine militaire. Par ailleurs, le renforcement de la collaboration entre les communautés scientifiques et techniques, la société civile et les défenseurs et praticiens des droits de l'homme favorisera l'utilisation responsable des technologies nouvelles et émergentes dans le domaine militaire.

86. Les États et les organisations internationales devraient envisager d'adopter des mesures contraignantes ou d'autres mesures permettant de veiller à ce que les technologies nouvelles et émergentes dans le domaine militaire dont la conception, la mise au point ou l'utilisation présentent des risques importants de mauvais usage, de violence ou de dommages irréversibles – en particulier lorsque ces risques peuvent entraîner des violations des droits de l'homme – ne soient pas développées. Il s'agit notamment des technologies de surveillance de masse qui portent atteinte à la vie privée, ainsi que des biotechnologies et des neurotechnologies qui menacent l'intégrité physique et mentale, en particulier dans des contextes de coercition.

87. Les États devraient tout mettre en œuvre pour qu'aucun système d'armes autonome ne soit pas mis au point ou déployé à moins qu'il ne puisse fonctionner sans un contrôle humain significatif. Ils devraient adopter des règles claires et contraignantes pour garantir le respect total des normes juridiques internationales.

88. Les États devraient faire preuve de diligence raisonnable et appliquer le principe de précaution en procédant à des évaluations des risques et des incidences sur les droits de l'homme de tous les types de technologies nouvelles et émergentes utilisées dans le domaine militaire. Des organismes indépendants tels que les institutions nationales des droits de l'homme devraient piloter ces évaluations afin de garantir la participation du public et un contrôle démocratique. Les États devraient utiliser les résultats de ces

évaluations pour adopter des mesures visant à prévenir les dommages, à suspendre l'utilisation des technologies à haut risque et à faire respecter les normes relatives à l'utilisation responsable des technologies nouvelles et émergentes dans le domaine militaire. Ils doivent impérativement collaborer dans le cadre des instruments internationaux existants – tels que la Convention sur les armes chimiques et la Convention sur les armes biologiques, qui interdisent la mise au point, la fabrication, l'acquisition, le stockage, le transfert ou l'utilisation d'armes biologiques, chimiques ou à toxines – pour renforcer la gouvernance des technologies nouvelles et émergentes et l'action à mener face à ces technologies.

89. Les États et les organisations internationales devraient adopter une approche collaborative de la gouvernance des technologies nouvelles et émergentes dans le domaine militaire, en veillant au respect du droit international tout en s'attaquant aux impacts disproportionnés sur les nations dotées de peu de moyens, car les inégalités en matière d'IA et de technologie militaire, en plus d'exacerber les disparités existantes, sont également susceptibles d'engendrer une instabilité à long terme. Les États en mesure de le faire – notamment ceux qui développent de telles technologies – devraient atténuer les dommages en partageant leurs connaissances, en fournissant une assistance technique et en s'attaquant aux effets déstabilisants.

## B. À l'intention des entreprises

90. Les entreprises, en particulier dans les secteurs de la défense et de la sécurité, devraient respecter les droits de l'homme conformément aux Principes directeurs, en établissant des garanties mesurables adaptées à des contextes précis et en éliminant les préjugés et la discrimination grâce à des évaluations de l'impact sur les droits de l'homme. Ces mesures devraient, dans la mesure du possible, tenir compte du secret industriel, notamment dans le cadre des rapports d'activité et des audits indépendants, afin de garantir une participation civique inclusive et diversifiée. Par ailleurs, les entreprises doivent se conformer aux réglementations établies par les États et continuer à élaborer et à appliquer des normes fondées sur les risques en matière de droits de l'homme, s'agissant notamment de l'exigence de transparence, en mettant en place des mécanismes faisant l'objet d'examens réguliers visant à en garantir l'efficacité et le bon alignement sur le droit international des droits de l'homme.

91. Les entreprises doivent disposer d'un processus de diligence raisonnable en matière de droits de l'homme et le mettre en œuvre afin de détecter, prévenir et atténuer les incidences négatives de leur utilisation de technologies nouvelles et émergentes dans le domaine militaire sur les droits de l'homme, conformément aux Principes directeurs. Elles doivent également procéder à une évaluation approfondie de ces technologies et modèles d'IA pour en déceler les risques, notamment en ce qui concerne les droits de l'homme et la sécurité internationale. Dans les cas où les essais relatifs aux risques extrêmes sont limités par les classifications de défense, elles doivent préalablement se coordonner avec les autorités nationales pour garantir la conformité avec le droit international.

## C. À l'intention de l'ensemble des parties prenantes

92. Toutes les parties prenantes, notamment les milieux universitaires, la société civile, les organisations internationales et les États, devraient mettre l'accent sur la recherche concernant les implications sur les droits de l'homme des technologies nouvelles et émergentes dans le domaine militaire, en appuyant les politiques d'évaluation des impacts de ces technologies de rupture tout en soulignant l'interdépendance, l'indivisibilité et l'universalité de tous les droits de l'homme à tous les stades du développement de ces technologies.

93. Toutes les parties prenantes doivent coopérer pour garantir la mise au point et le déploiement responsables des technologies nouvelles et émergentes dans le domaine militaire et pour veiller à ce que la réglementation soit en phase avec les avancées technologiques, en encourageant le dialogue international afin d'élaborer et d'appliquer des cadres juridiques respectueux des droits de l'homme.

---