



# Assemblée générale

Distr. générale  
23 juillet 2024  
Français  
Original : anglais

## Soixante-dix-neuvième session

Point 97 de l'ordre du jour provisoire\*

### Rôle de la science et de la technique dans le contexte de la sécurité internationale et du désarmement

## **Dernières évolutions scientifiques et techniques et leurs incidences éventuelles sur l'action menée en matière de sécurité internationale et de désarmement**

### **Rapport du Secrétaire général**

#### *Résumé*

Le présent rapport donne un aperçu des innovations scientifiques et techniques présentant une utilité pour les armes, les moyens ou les méthodes de guerre et de leurs incidences éventuelles sur l'action menée en matière de sécurité internationale et de désarmement, ainsi que des évolutions dans les instances intergouvernementales compétentes, conformément à la résolution 78/22 de l'Assemblée générale. Il couvre l'intelligence artificielle et l'autonomie, les systèmes sans équipage, les technologies numériques, la biologie et la chimie, les techniques spatiales et aérospatiales, les techniques électromagnétiques et les techniques des matériaux. Il traite également de la convergence des technologies.

\* [A/79/150](#).



## **I. Introduction**

1. Au paragraphe 4 de sa résolution [78/22](#) sur le rôle de la science et de la technique dans le contexte de la sécurité internationale et du désarmement, l'Assemblée générale a prié le Secrétaire général de lui présenter, à sa soixante-dix-neuvième session, un rapport actualisé sur les dernières évolutions scientifiques et techniques et leurs incidences éventuelles sur l'action menée en matière de sécurité internationale et de désarmement.
2. La science et la technique contribuent au développement humain et à la prospérité et sont des catalyseurs essentiels des efforts visant à mettre en œuvre le Programme de développement durable à l'horizon 2030. Comme l'a fait remarquer le Secrétaire général dans sa note d'orientation sur le Nouvel Agenda pour la paix ([A/77/CRP.1/Add.8](#)), il est important de veiller à ce que les mesures prises pour faire face aux dangers de la militarisation des technologies nouvelles et émergentes ne limitent pas l'accès des pays du Sud aux avantages considérables que ces technologies promettent pour la réalisation des objectifs de développement durable.
3. Cela étant, d'aucuns continuent de craindre que les cadres normatifs et les dispositifs de gouvernance n'arrivent plus à suivre le rythme des évolutions de la science et de la technique présentant une utilité pour la sécurité et le désarmement et ne soient donc plus capables de gérer les risques connexes. Les avantages que les technologies nouvelles et émergentes procurent ne sauraient être exploités au détriment de la sécurité mondiale. Des dispositifs de gouvernance devraient être mis en place pour limiter les dommages potentiels et parer aux risques transversaux que font courir les innovations rapides et les technologies convergentes (*ibid.*, action 11).
4. Le présent rapport donne un aperçu des innovations scientifiques et techniques présentant une utilité particulière pour les armes, les moyens ou les méthodes de guerre et de leurs incidences éventuelles sur l'action menée en matière de sécurité internationale et de désarmement, ainsi que des évolutions dans les instances intergouvernementales compétentes.

## **II. Dernières évolutions scientifiques et techniques présentant une utilité pour les armes, les moyens ou les méthodes de guerre**

### **A. Intelligence artificielle et autonomie**

5. Les systèmes d'intelligence artificielle peuvent être intégrés dans différentes applications qui facilitent le processus décisionnel, la planification et la logistique militaires et permettent d'autonomiser les systèmes d'armes, y compris, potentiellement, les fonctions d'emploi de la force létale. La convergence de l'intelligence artificielle avec d'autres domaines de la science et de la technologie peut ouvrir la voie à la prolifération des armes et à de nouveaux moyens et nouvelles méthodes de guerre. L'intelligence artificielle développée à des fins civiles peut être utilisée de manière abusive, notamment à des fins de désinformation politique, de cyberattaque, de terrorisme ou à d'autres fins malveillantes, ce qui présente des risques importants pour les technologies à double usage et la gouvernance internationale.
6. Outre les progrès rapides réalisés dans le domaine de l'intelligence artificielle civile, il apparaît de plus en plus que des États utilisent des systèmes fondés sur l'intelligence artificielle dans le contexte militaire, et l'acquisition de ces technologies par des acteurs non étatiques suscite des inquiétudes grandissantes. Si

les activités de recherche et de développement de l'intelligence artificielle sont actuellement concentrées dans un petit nombre d'États et principalement menées par des acteurs du secteur privé, le caractère immatériel de cette technologie et son évolution rapide rendent difficiles son suivi, sa réglementation et sa gouvernance.

7. Une préoccupation particulière concerne la manière dont on peut mener des contrôles rigoureux qui garantissent la fiabilité, la sûreté, la sécurité et la précision des systèmes d'intelligence artificielle dans le domaine militaire. S'il est généralement admis que l'intelligence artificielle dans le domaine militaire doit être « robuste » (c'est-à-dire techniquement fiable et sûre), les différences probables entre les environnements d'essai et de déploiement soulèvent des questions quant à la manière de garantir cette robustesse, notamment en ce qui concerne les violations potentielles du droit international humanitaire. Par exemple, lorsqu'elles sont employées à des fins telles que la sélection des cibles dans des systèmes d'armes autonomes et des systèmes informatisés d'aide à la décision, les applications d'intelligence artificielle peuvent faire échec au principe de distinction en raison, notamment, de problèmes de fiabilité des données, d'erreurs dans la reconnaissance des formes et d'un manque de compréhension du contexte. Lorsqu'elles sont utilisées à des fins de ciblage à grande échelle ou sans discernement, ces applications peuvent aller à l'encontre des principes de proportionnalité et de précaution.

8. Les progrès rapides de l'intelligence artificielle générative constituent une évolution importante et mettent en relief l'ampleur des données et des ressources informatiques qui définissent l'intelligence artificielle contemporaine. Les grands modèles de langage sont un type de modèle de fondation entraîné à l'aide d'une grande quantité de données. Ils peuvent être adaptés à un large éventail de tâches en aval, et éventuellement utilisés à des fins militaires. L'augmentation rapide de l'utilisation de grands modèles de langage et la publication de modèles libres de droits, qui élargissent l'accès à ces modèles, peuvent présenter des risques pour la paix et la sécurité internationales, allant des utilisations délibérément abusives visant à créer de nouvelles armes, moyens et méthodes de guerre, à une série de risques liés aux applications militaires qui peuvent survenir même lorsque cette technologie est utilisée par des acteurs responsables<sup>1</sup>. Le débat actuel sur les compromis en matière de transparence dans le domaine de l'intelligence artificielle témoigne de la nécessité, d'une part, de maintenir une tradition d'ouverture propre à favoriser l'innovation et le développement et, d'autre part, d'assurer un contrôle.

### **Processus, organismes et instruments intergouvernementaux pertinents**

9. À la Réunion de 2023 des Hautes Parties contractantes 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, il a été décidé que le Groupe d'experts gouvernementaux sur les technologies émergentes dans le domaine des systèmes d'armes létaux autonomes poursuivrait ses travaux. Il a également été décidé que le Groupe devrait poursuivre l'examen et l'élaboration, par consensus, d'un ensemble d'éléments d'un instrument, sans préjuger de la nature de celui-ci, et d'autres mesures possibles pour traiter la question des technologies émergentes dans le domaine des systèmes d'armes létaux autonomes, en prenant en compte l'exemple des Protocoles se rapportant à la Convention, les propositions présentées par les Hautes Parties contractantes et d'autres solutions relatives au cadre normatif et opérationnel ayant trait aux technologies émergentes dans le domaine des systèmes d'armes autonomes létaux, en s'appuyant sur les recommandations et les conclusions qu'il avait déjà

<sup>1</sup> Les bénéfices offerts par les modèles libres de droits au regard du risque d'utilisation à des fins malveillantes font encore l'objet d'un examen.

formulées et en faisant appel à des compétences spécialisées sur les aspects juridiques, militaires et technologiques. Le Groupe a estimé que les systèmes d'armes basés sur des technologies émergentes dans le domaine des systèmes d'armes létaux autonomes s'appuyaient sur des ensembles de données qui pouvaient perpétuer ou amplifier des préjugés sociaux involontaires, notamment les préjugés liés au genre et les préjugés raciaux, et pouvaient donc avoir des incidences sur le respect du droit international.

10. Bien qu'il existe des initiatives externes, il n'y a actuellement aucun processus intergouvernemental sous les auspices de l'Organisation des Nations Unies qui s'intéresse au cycle de vie responsable de l'intelligence artificielle dans le domaine militaire.

## B. Systèmes sans équipage

11. Les systèmes sans équipage sont des systèmes pouvant être pilotés à distance, de manière semi-autonome ou autonome et sont employés dans les secteurs aérien, terrestre et maritime. Il s'agit le plus souvent de systèmes aériens, mais le développement et l'utilisation de dispositifs maritimes et terrestres deviennent de plus en plus courants. Ces systèmes sont notamment utilisés dans les activités de surveillance et de reconnaissance militaires, à des fins d'acquisition de cibles et dans les opérations de frappe.

12. La polyvalence des systèmes sans équipage et les risques moindres qu'ils présentent pour la vie des opérateurs par rapport aux systèmes avec équipage rendent ces dispositifs de plus en plus attrayants pour les acteurs tant étatiques que non étatiques. Les drones aériens, en particulier, sont largement utilisés dans les conflits, car ils sont souvent moins chers et plus rapides à produire que des systèmes comparables avec équipage. Les systèmes sans équipage peuvent être armés ou non armés. À titre d'exemple, on peut citer les munitions rôdeuses, qui sont des systèmes aériens d'attaque à sens unique combinant les caractéristiques des systèmes sans équipage et des missiles, le système lui-même étant utilisé comme arme, évoluant dans les airs jusqu'à ce qu'elle frappe. L'utilisation récente de systèmes sans équipage dans des zones peuplées a soulevé des inquiétudes concernant la protection des civils et le respect du droit international humanitaire, dans la mesure où ils permettent notamment de mener des frappes à grande échelle contre des cibles éloignées de la ligne de front. L'utilisation de systèmes armés présente par ailleurs le risque d'abaisser le seuil de recours à la force, en raison notamment du risque moindre auquel sont exposés les opérateurs humains.

13. Les innovations scientifiques et technologiques visent à améliorer la performance des composants individuels des systèmes sans équipage et des systèmes dans leur ensemble, le but étant d'améliorer leur autonomie de vol, leur fiabilité et leur efficacité<sup>2</sup>. Néanmoins, les systèmes sans équipage sont vulnérables aux interférences, notamment au brouillage ou à l'usurpation des données de surveillance, des systèmes de communication et des systèmes de positionnement. L'intégration de l'intelligence artificielle serait un moyen d'accroître l'autonomie et de réduire la dépendance à l'égard de liens de communication potentiellement vulnérables (voir également sect. II.A et II.F).

<sup>2</sup> Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR), « Uncrewed aerial, ground, and maritime systems: a compendium », avril 2023.

### Processus, organismes et instruments intergouvernementaux pertinents

14. Dans sa résolution [2370 \(2017\)](#), le Conseil de sécurité a condamné fermement la circulation continue d'armes, notamment de drones et de leurs pièces détachées entre les groupes armés illégaux, les terroristes et d'autres utilisateurs non autorisés, ou à destination de ces groupes, et encouragé les États Membres à prévenir et à démanteler les réseaux d'achat de ces armes, systèmes et pièces détachées. La Déclaration de Delhi sur la lutte contre l'utilisation des technologies nouvelles et émergentes à des fins terroristes a été adoptée en 2022<sup>3</sup>. En 2023, les Principes directeurs d'Abou Dhabi sur les systèmes de drones aériens ont été élaborés conformément à cette déclaration (voir [S/2023/1035](#)).

15. En ce qui concerne l'amélioration de la transparence dans le domaine des armements et la promotion des transferts responsables, les systèmes sans équipage sont explicitement inclus dans la catégorie IV (« Avions de combat et véhicules de combat aériens non pilotés ») et la catégorie V (« Hélicoptères d'attaque et véhicules de combat aériens non pilotés à voilure tournante ») du Registre des armes classiques de l'Organisation des Nations Unies. Certains États parties au Traité sur le commerce des armes font figurer les systèmes sans équipage dans les rapports qu'ils présentent en application du Traité.

## C. Technologies numériques

16. La dépendance croissante à l'égard des technologies numériques et les progrès dans ce domaine se poursuivent à un rythme rapide. L'Internet des objets continue de se développer sans aucun signe de fléchissement : on estime à 7 milliards le nombre d'appareils connectés, un chiffre qui devrait passer à 22 milliards d'ici à 2025<sup>4</sup>. Les percées réalisées dans le domaine des technologies numériques, notamment les technologies de l'information et de la communication, les technologies quantiques, l'informatique en nuage, les technologies de la chaîne de blocs, les réseaux 5G et l'intelligence artificielle, continuent d'offrir des possibilités de transformer les industries, les économies et les sociétés.

17. L'utilisation accrue des technologies numériques offre des perspectives sans précédent aux sociétés. Toutefois, l'exploitation de nouvelles vulnérabilités et l'utilisation malveillante de ces technologies pourraient avoir des répercussions sur la paix et la sécurité internationales. Les activités malveillantes pourraient avoir des effets en cascade aux niveaux sous-régional, régional et mondial. Au-delà des répercussions directes qu'elles ont sur la population en raison de leurs effets sur les infrastructures critiques, les activités malveillantes fondées sur les technologies numériques peuvent également saper la confiance dans les processus électoraux et les institutions publiques et compromettre la confidentialité, l'intégrité et la disponibilité des données.

### Informatique et technologies des communications

18. L'utilisation malveillante des technologies de l'information et des communications par des acteurs étatiques et non étatiques est en hausse. En 2023, des incidents graves ont été signalés, notamment ceux ayant des conséquences sur les infrastructures qui servent à fournir des services essentiels au public, tels que les services de santé, les services bancaires et les services de télécommunications civiles.

<sup>3</sup> Voir [https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/outcome\\_document\\_ctc\\_special\\_mtg\\_final\\_f.pdf](https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/outcome_document_ctc_special_mtg_final_f.pdf).

<sup>4</sup> Voir <https://www.oracle.com/fr/internet-of-things/>.

L'exploitation des vulnérabilités des logiciels, y compris par la vente sur Internet d'informations sur ces vulnérabilités, s'est également poursuivie.

19. Au cours de l'année écoulée, certains États ont signalé une augmentation considérable du nombre d'incidents liés à des logiciels rançonneurs et fait état d'une recrudescence de l'activité criminelle à motivation financière<sup>5</sup>. Selon certaines estimations, en 2023, le total des sommes versées à de tels logiciels en guise de rançon s'est élevé à un montant record de 1,1 milliard de dollars<sup>6</sup>. La prolifération de divers types de logiciels malveillants, tels que les logiciels rançonneurs, les virus effaceurs et les chevaux de Troie, associée à une expansion des techniques telles que l'hameçonnage ciblé, l'exploitation de l'informatique en nuage et les attaques par déni de service distribué, a également continué d'être observée dans toutes les régions, avec des niveaux d'impact variables. La prolifération des moyens de cyberintrusion disponibles dans le commerce, notamment de logiciels espions et autres « kits d'exploitation », suscite une inquiétude croissante<sup>7</sup>. Des activités malveillantes visant les chaînes d'approvisionnement d'entreprises telles que les fournisseurs de logiciels auraient également eu des effets perturbateurs<sup>8</sup>.

20. La diversification des acteurs et des techniques rend les menaces toujours plus complexes. Des acteurs non étatiques, notamment des organisations criminelles, des terroristes, des groupes de pirates informatiques et des particuliers, ont utilisé divers outils, techniques, exploits et vecteurs d'attaque pour perturber et détruire des réseaux, des applications et du contenu.

### Technologies quantiques

21. Les États appellent de plus en plus l'attention sur les implications potentielles des nouvelles technologies quantiques pour la paix et la sécurité internationales. L'intégration des propriétés quantiques dans des applications telles que le calcul, la détection et l'imagerie et la cryptographie peut offrir des possibilités considérables en matière d'action et de transformation, notamment pour la paix et la sécurité internationales. Par exemple, les ordinateurs quantiques ont des capacités de calcul sans commune mesure avec celles des machines actuelles et permettront de résoudre des problèmes plus complexes. Quant à la détection et l'imagerie quantiques, celles-ci permettent de capturer des objets avec une résolution supérieure à celle offerte par des capteurs classiques, tandis que la cryptographie post-quantique est considérée comme hautement sécurisée.

22. Malgré les avantages qu'elles peuvent offrir, les technologies quantiques pourraient présenter des risques pour la paix et la sécurité internationales. On s'attend par exemple à ce que l'informatique remette en question les systèmes cryptographiques actuels, rendant les infrastructures numériques, y compris celles qui servent à fournir des services essentiels au public, vulnérables aux activités malveillantes. Il convient également de noter l'augmentation potentielle des attaques de type « harvest now, decrypt later » (récolter maintenant, déchiffrer plus tard), par lesquelles des acteurs malveillants accumulent des données sensibles et chiffrées, sachant que la technologie facilitera plus tard leur déchiffrement.

<sup>5</sup> Voir <https://www.cisa.gov/stopransomware/official-alerts-statements-cisa>.

<sup>6</sup> Alexander Culafi, « Chainalysis: 2023 a 'watershed' year for ransomware », TechTarget, 7 février 2024.

<sup>7</sup> Voir <https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities>.

<sup>8</sup> Karamveer Singh Sidhu, « Top 5 famous software supply chain attacks in 2023 », CloudSEK, 24 novembre 2023.

23. Alors que les technologies quantiques devraient avoir de vastes répercussions, à l'heure actuelle, moins de 20 pays ont investi dans un programme national de recherche et de développement dans ce domaine. Afin d'éviter que le fossé technologique ne se creuse davantage, il importe de faire en sorte que l'enseignement quantique soit ouvert à tous.

### Réseaux 5G

24. L'omniprésence toujours plus marquée de la cinquième génération de technologie mobile, communément appelée 5G, révolutionne les communications en augmentant considérablement la vitesse de téléchargement et en réduisant le délai de communication entre les appareils connectés. Alors que la transition vers la technologie 5G se poursuit, de nouvelles perspectives et vulnérabilités sont apparues. Cette technologie a été saluée dans la mesure où elle offre de nombreux avantages, tels qu'une meilleure connectivité pour les villes intelligentes, la télémédecine et la croissance économique dans son ensemble. Toutefois, des risques ont également été recensés, tels que l'introduction malveillante ou involontaire de vulnérabilités au stade de la conception. Il est également possible que des vulnérabilités soient introduites ou apparaissent dans la chaîne d'approvisionnement et dans l'architecture 5G correspondante.

### Processus, organismes et instruments intergouvernementaux pertinents

25. La question « Progrès de l'informatique et des télécommunications et sécurité internationale » est inscrite à l'ordre du jour de l'Assemblée générale depuis 1998<sup>9</sup>. Les débats tenus dans le cadre des groupes d'experts et des groupes de travail à composition non limitée ont abouti à des recommandations relatives aux normes, règles et principes de comportement responsable des États et aux mesures de confiance et de renforcement des capacités. Des débats ont eu lieu sur la manière dont le droit international s'applique à l'utilisation de ces technologies (voir [A/65/201](#), [A/68/98](#), [A/70/174](#) et [A/76/135](#)). Parallèlement aux travaux du sixième Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, un groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale a été créé par la résolution [73/27](#) de l'Assemblée générale. Le Groupe a adopté un rapport de consensus en mars 2021 ([A/75/816](#)), qui a été approuvé par l'Assemblée générale dans sa décision 75/564.

26. En 2020, l'Assemblée générale a créé un deuxième groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, doté d'un mandat de cinq ans et chargé, entre autres, de poursuivre l'élaboration des règles, normes et principes de comportement responsable des États, de continuer à étudier les menaces existantes et potentielles dans le domaine de la sécurité informatique et la manière dont le droit international s'applique à l'utilisation du numérique par les États, et de proposer des mesures de confiance et de renforcement des capacités. Le groupe de travail a adopté son premier rapport d'activité en juillet 2022 ([A/77/275](#)) et un deuxième en 2023 ([A/78/265](#)). On y trouve un certain nombre de recommandations concernant les prochaines étapes, notamment l'établissement d'un répertoire mondial et intergouvernemental d'interlocuteurs. Dans ces rapports, le groupe a reconnu l'existence d'une « fracture numérique entre genres » a été reconnue

<sup>9</sup> Pour plus d'informations sur les délibérations intergouvernementales concernant les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, voir [www.un.org/disarmament/ict-security](http://www.un.org/disarmament/ict-security).



et réaffirmé qu'il fallait encourager les activités de renforcement des capacités tenant compte des questions de genre.

27. Sous les auspices du groupe de travail à composition non limitée, les États ont continué à examiner les menaces existantes et émergentes qui pèsent sur la sécurité numérique. Les États ont réfléchi de diverses manières aux répercussions des technologies numériques sur la paix et la sécurité internationales, notamment des technologies de l'information et des communications, de l'intelligence artificielle et des technologies quantiques, ainsi qu'aux conséquences de leur convergence.

## D. Biologie et chimie

28. Les normes interdisant l'utilisation de la chimie et de la biologie à des fins hostiles sont consacrées depuis longtemps par le droit international, notamment la Convention sur l'interdiction de la mise au point, de la fabrication et du stockage des armes bactériologiques (biologiques) ou à toxines et sur leur destruction, de 1972, et la Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'emploi des armes chimiques et sur leur destruction, de 1993. Cependant, les emplois récents de produits chimiques comme armes, les allégations de mise au point d'armes biologiques et les avancées de la chimie et de la biologie risquent de fragiliser ces mesures juridiques et normatives.

29. Les avancées réalisées dans la biologie et la chimie s'accroissent et deviennent de plus en plus liées entre elles. D'une manière générale, elles offrent un certain nombre de moyens de relever les défis sociétaux. Elles entraînent néanmoins des risques pour la paix et la sécurité internationales.

30. L'autorisation d'une thérapie de modification du génome fondée sur de courtes répétitions palindromiques groupées et régulièrement espacées (CRISPR) aux fins du traitement de la drépanocytose et de la bêta-thalassémie dépendante des transfusions témoigne du potentiel qu'offre cette technologie pour aider à guérir des maladies jusqu'ici incurables<sup>10</sup>. Toutefois, le pouvoir de modifier le génome s'accompagne également de risques importants. En théorie, les mêmes techniques pourraient être utilisées à des fins abusives pour améliorer les agents utilisés dans les anciens programmes d'armes biologiques ou pour créer de nouvelles formes d'armes biologiques. Il est donc nécessaire d'instaurer une gouvernance solide et une collaboration internationale et de mener des recherches approfondies sur les effets involontaires de la modification du génome, afin de garantir que ces innovations profitent à l'humanité sans poser de risques excessifs.

31. Le début des essais sur l'être humain de la technologie d'interface neuronale nous rapproche de la fusion de la cognition humaine avec les machines. En 2024, le premier implant cérébral posé sur un humain par une entreprise privée a été réalisé. Cette prouesse ouvre des perspectives prometteuses pour le monde de la médecine, dans la mesure où l'on pourrait restaurer des fonctions sensorielles perdues ou traiter des troubles cérébraux. Elle risque toutefois d'avoir des répercussions profondes en matière de sécurité. Cette technologie pourrait être exploitée pour manipuler ou contrôler les comportements humains, ce qui renforce la nécessité d'établir des normes strictes de déontologie et de mettre en place des mesures de protection<sup>11</sup>.

<sup>10</sup> Cormac Sheridan, « The world's first CRISPR therapy is approved: who will receive it? », *Nature Biotechnology*, vol. 42, n° 1 (janvier 2024) ; Willow Shah-Neville, « A gene editing milestone: the FDA approves CASGEVY, the first CRISPR-based therapy », *Labiatech*, 11 décembre 2023.

<sup>11</sup> Miryam Naddaf, « Mind-reading devices are revealing the brain's secrets », *Nature*, vol. 626, n° 8000 (février 2024) ; Rachael Levy, Marisa Taylor et Akriti Sharma, « Elon Musk's Neuralink wins FDA approval for human study of brain implants », *Reuters*, 26 mai 2023.



32. Les drones à voilure fixe ou tournante sont utilisés pour surveiller les cultures et le bétail ainsi que pour répandre des nutriments et des pesticides sur les cultures de manière intelligente et efficace afin de maximiser la production. En ce qui concerne le maintien de l'ordre, des drones semi-autonomes capables de disséminer des agents de lutte antiémeute ont été mis au point pour contrôler les foules. Le risque d'utilisation malveillante des drones agricoles et antiémeutes comme vecteurs d'agents nocifs est une source de préoccupation constante, d'autant plus qu'ils sont de plus en plus abordables et répandus.

33. L'intégration de nouvelles technologies permet également de mettre au point des contre-mesures et traitements innovants contre les menaces biologiques et chimiques, tels que des antidotes aux poisons et de nouvelles contre-mesures en cas d'exposition à des agents neurotoxiques<sup>12</sup>. Il s'agit là d'une évolution essentielle pour renforcer la résilience face aux attaques potentielles, voire les dissuader.

### **Processus, organismes et instruments intergouvernementaux pertinents**

34. La Convention sur les armes biologiques et la Convention sur les armes chimiques prévoient la tenue de conférences d'examen tous les cinq ans pour faire le point sur les évolutions de la science et de la technique. La neuvième Conférence des États parties chargée de l'examen de la Convention sur les armes biologiques s'est tenue en novembre et en décembre 2022, tandis que la cinquième Conférence d'examen des États parties à la Convention sur les armes chimiques a eu lieu en mai 2023.

35. Les deux conventions contiennent des dispositions relatives à la tenue d'examens plus réguliers des évolutions pertinentes de la science et de la technique. Conformément à un mandat confié par la Conférence d'examen des États parties à la Convention sur les armes chimiques, la direction générale de l'Organisation pour l'interdiction des armes chimiques (OIAC) a établi un conseil scientifique consultatif au sein de l'organisation. En 2023, ledit conseil a tenu sa trente-septième session<sup>13</sup>, tandis que son groupe de travail temporaire sur l'analyse des biotoxines a mené à bien ses travaux et publié son rapport de fin de mandat<sup>14</sup>. Il a également publié un rapport scientifique complet sur les progrès de la science et de la technique, à l'appui de la cinquième Conférence d'examen des États parties à la Convention sur les armes chimiques<sup>15</sup>. En outre, l'OIAC a inauguré son Centre pour la chimie et la technologie, qui lui permettra de mener des activités de recherche pour soutenir et renforcer le régime de vérification, ainsi que d'organiser des cours de formation et d'autres activités de renforcement des capacités.

36. À la neuvième Conférence d'examen des États parties à la Convention sur les armes biologiques, qui s'est tenue en 2022, les États parties sont convenus de créer un groupe de travail sur le renforcement de la Convention. Le groupe de travail a pour mandat de mettre en évidence, d'examiner et d'élaborer des mesures spécifiques et efficaces, y compris d'éventuelles mesures juridiquement contraignantes, visant à renforcer l'application de la Convention, ainsi que de formuler des recommandations à ce sujet. Dans le cadre de ce mandat, il examine les innovations scientifiques et

<sup>12</sup> Illia V. Kapitanov *et al.*, « Sustainable ionic liquids-based molecular platforms for designing acetylcholinesterase reactivators », *Chemico-Biological Interactions*, vol. 385 (novembre 2023).

<sup>13</sup> Organisation pour l'interdiction des armes chimiques (OIAC), « Report of the Scientific Advisory Board at its thirty-seventh session », document SAB-37/1.

<sup>14</sup> OIAC, « Analysis of biotoxins: report of the Scientific Advisory Board's temporary working group », document SAB/REP/1/23.

<sup>15</sup> OIAC, « Report by the Director-General: report of the Scientific Advisory Board on developments in science and technology to the Fifth Special Session of the Conference of the States Parties to Review the Operation of the Chemical Weapons Convention », document RC-5/DG.1.

techniques en rapport avec la Convention, étudie les recommandations relatives à la mise en place d'un mécanisme d'examen et d'évaluation de ces innovations et donne des conseils aux États parties. Les débats consacrés à ces questions ont eu lieu à la deuxième session du groupe de travail, en août 2023, et se poursuivront dans le cadre des travaux intersessions et des réunions qui seront organisées avant la dixième Conférence d'examen, qui se tiendra en 2027.

## E. Techniques spatiales et aérospatiales

### Technologies balistiques

37. L'évolution des technologies émergentes permet aux systèmes de missiles, qui sont de plus en plus utilisés comme armes de frappe à longue portée dans les conflits armés, de remplir des fonctions nouvelles et élargies, ce qui a des répercussions sur la paix et la sécurité internationales et sur les efforts visant à assurer le désarmement, une réglementation efficace des armements, la non-prolifération et le respect des principes humanitaires.

#### *Missiles balistiques et roquettes d'artillerie*

38. Un nombre croissant d'États s'intéressent aux diverses innovations technologiques qui ont permis d'améliorer la précision des missiles balistiques et des systèmes de roquettes d'artillerie. Cela a conduit à l'utilisation de missiles balistiques et de roquettes de plus longue portée comme armes de frappe, notamment dans les conflits armés en cours et d'autres attaques très médiatisées. Certains acteurs non étatiques sont également parvenus à acquérir et à utiliser des missiles balistiques et des roquettes.

39. Ces innovations technologiques ont également permis de développer et de mettre à l'essai des systèmes de roquettes d'artillerie de gros calibre qui peuvent brouiller la distinction entre les roquettes d'artillerie et les missiles balistiques capables de transporter une arme nucléaire. Cette tendance continue de nuire au respect des régimes de non-prolifération des missiles balistiques capables d'emporter des charges nucléaires.

40. Cette évolution a également amené les États à développer et à acquérir des moyens de défense antimissiles, dont certains types peuvent exacerber les tensions et accroître l'instabilité, compte tenu des différences de points de vue sur la relation entre les systèmes d'armes offensifs et défensifs.

#### *Planeurs hypersoniques*

41. Certains États continuent également de mettre au point et de déployer des missiles dotés d'ogives capables de planer et de manœuvrer à des vitesses hypersoniques sur de longues distances dans l'atmosphère, en tirant parti de la sustentation aérodynamique. Les planeurs hypersoniques pourraient être capables de se soustraire aux défenses antimissiles à mi-course et d'échapper à la défense terminale, grâce à leur manœuvrabilité, ou du fait qu'ils volent sous l'horizon des radars de défense terminale à des distances plus éloignées de leurs cibles. L'utilisation de ces systèmes n'a pas encore été observée dans les conflits armés, et leurs implications stratégiques ne sont pas entièrement comprises. Néanmoins, le premier déploiement connu, en 2019, d'un planeur hypersonique propulsé sur un missile balistique à portée intercontinentale a suscité des inquiétudes quant à la possible reprise de la course aux armements stratégiques.

### *Véhicules hypersoniques motorisés*

42. Des États et des entreprises privées continuent à tester des statoréacteurs à combustion supersonique destinés, du moins en partie, à propulser des missiles de croisière hypersoniques à même d'échapper aux systèmes de défense aérienne et aux systèmes antimissiles. Ces systèmes, en cours de développement, peuvent être lancés par des propulseurs terrestres, maritimes ou aériens et armés de têtes classiques ou éventuellement nucléaires.

### *Défense antimissile et systèmes antisatellites au sol*

43. De plus en plus d'États mettent au point et acquièrent des systèmes antimissiles, notamment en réponse directe à leur utilisation dans les conflits armés en cours. Les systèmes surface-air conçus pour intercepter leur cible en basse atmosphère sont de plus en plus courants. Le déploiement généralisé de ces systèmes a entraîné une augmentation de l'acquisition et de l'utilisation de drones auto-détonants peu coûteux, notamment dans l'idée d'essayer de surmonter ces défenses.

44. Des États continuent à mettre au point, mettre à l'essai et développer des systèmes antimissiles pour frapper les missiles hors de l'atmosphère dans la phase de vol dite à mi-course. Les systèmes de ce type les plus performants sont capables de frapper des satellites en orbite terrestre basse. Des États continuent également à déployer des missiles terrestres qui auraient été conçus spécifiquement pour frapper des satellites en orbite terrestre basse et géostationnaire.

### *Processus, organismes et instruments intergouvernementaux pertinents*

45. Entre 2001 et 2008, l'Assemblée générale a créé trois groupes d'experts gouvernementaux sur la question des missiles sous tous ses aspects (voir [A/57/229](#), [A/61/168](#) et [A/63/176](#)). Bien que la question des missiles reste inscrite à l'ordre du jour de la Première Commission, aucune résolution à ce sujet n'a été adoptée depuis la résolution [63/55](#).

46. Il existe deux mécanismes intergouvernementaux consistant dans des mesures volontaires relatives à la technologie des missiles. Le Régime de contrôle de la technologie des missiles (RCTM) a été établi en 1987 afin de limiter la prolifération des missiles balistiques et autres vecteurs sans équipage capables d'emporter des armes de destruction massive. Il est composé de 35 membres. Les États signataires du Code de conduite de La Haye contre la prolifération des missiles balistiques, adopté en 2002, ont pris l'engagement politiquement contraignant de faire preuve de la plus grande retenue dans la mise au point, l'essai et le déploiement de missiles balistiques et de respecter les mesures de transparence concernant le lancement de missiles balistiques et d'engins spatiaux civils et les politiques y relatives. Un total de 145 États souscrivent au Code.

47. La question des armes antisatellites au sol a été soulevée dans le cadre des travaux de divers organismes des Nations Unies concernés par la sécurité de l'espace, y compris, tout récemment, le Groupe d'experts gouvernementaux chargé d'étudier de nouvelles mesures concrètes de prévention d'une course aux armements dans l'espace. Dans sa résolution [77/41](#), l'Assemblée générale a demandé à tous les États de prendre l'engagement de ne pas procéder à des essais de missile antisatellite à ascension directe et à visée destructrice.

### **Techniques spatiales**

48. Les forces militaires sont de plus en plus tributaires de techniques spatiales, dont elles ont besoin pour effectuer des tâches relatives aux alertes rapides, à la navigation, à la surveillance, à la sélection de cibles et aux communications. Les

moyens spatiaux, dont les satellites, sont particulièrement vulnérables à diverses techniques de neutralisation spatiale.

*Capacités utilisées dans les opérations de rendez-vous et de proximité*

49. De nombreuses capacités émergentes impliquent des opérations de rendez-vous et de proximité, dans le cadre desquelles des satellites se rapprochent d'un satellite cible afin d'opérer à proximité ou d'établir un contact physique. Au-delà de leurs applications bénéfiques, telles que la maintenance et la réparation des satellites, ces opérations pourraient également servir à commettre des actes non consensuels, risqués, perturbateurs ou hostiles.

50. La mise au point de systèmes capables de fournir d'autres services aux satellites actifs en orbite, notamment des services d'inspection, de réparation, d'expansion et de relocalisation, s'est poursuivie. En 2020, des entreprises privées ont lancé pour la première fois un satellite qui s'est amarré à un autre satellite ayant épuisé sa réserve de carburant afin de prolonger sa durée de vie.

51. Un nombre croissant d'entreprises privées déploient des remorqueurs spatiaux, conçus pour le déploiement de multiples charges utiles sur des orbites précises, à différents plans orbitaux et à différentes altitudes orbitales. Ces systèmes sont conçus pour pouvoir être manœuvrés après leur insertion orbitale et déployer de nombreux petits satellites en différents points de leur trajectoire. On a observé des satellites qui déployaient de petites charges utiles secondaires à des vitesses relativement élevées.

52. Des entreprises privées ont continué à lancer des satellites de démonstration technologique à l'appui du développement des capacités d'élimination active des débris. Elles continuent d'étudier différents moyens, notamment l'utilisation de bras robotiques, de filets, de harpons, d'aimants et d'adhésifs, ainsi que le recours éventuel à des lasers basés dans l'espace, pour détruire des débris spatiaux relativement petits.

53. Un certain nombre d'États ont continué à lancer et à exploiter des satellites destinés à inspecter visuellement les satellites d'autres États, en particulier dans la ceinture géostationnaire. Il s'agit généralement de systèmes exploités par des agences de renseignements militaires ou nationales, qui s'approchent à la fois des satellites commerciaux et d'autres satellites militaires.

*Autres capacités spatiales*

54. Des entreprises privées ont également démontré leur capacité à incorporer un bouclier thermique pour la charge utile de leurs satellites afin de récupérer du matériel fabriqué en orbite. Des acteurs commerciaux ont récemment mis au point et utilisé des systèmes de rentrée pour les engins spatiaux pilotés, une technologie que les États utilisent depuis des décennies.

55. Les États et les entreprises privées ont continué à étudier et à mettre à l'essai l'utilisation des lasers basés dans l'espace comme moyens de communication. Alors que les lasers de faible puissance peuvent éblouir ou aveugler temporairement les capteurs optiques, les lasers de plus forte puissance peuvent endommager certains composants sensibles des satellites ou d'autres systèmes spatiaux.

*Processus, organismes et instruments intergouvernementaux pertinents*

56. Le droit international interdit de mettre des armes nucléaires ou autres armes de destruction massive en orbite, de les installer sur des corps célestes ou de les placer, de toute autre manière, dans l'espace extra-atmosphérique ; l'aménagement de bases et d'installations militaires et de fortifications, les essais d'armes de tous types et l'exécution de manœuvres militaires sur les corps célestes ; et toute explosion

expérimentale d'arme nucléaire, ou toute autre explosion nucléaire, dans l'espace extra-atmosphérique<sup>16</sup>.

57. La prévention d'une course aux armements dans l'espace figure à l'ordre du jour de la Conférence du désarmement depuis 1985.

58. Le Groupe d'experts gouvernementaux sur les mesures de transparence et de confiance relatives aux activités spatiales a adopté un rapport de consensus en 2013 (A/68/189). En 2023, la Commission du désarmement a souscrit à une recommandation sur la mise en œuvre des recommandations figurant dans le rapport du Groupe (voir A/78/42). En 2019, le Comité des utilisations pacifiques de l'espace extra-atmosphérique a adopté 21 lignes directrices aux fins de la viabilité à long terme des activités spatiales et le préambule y relatif (A/AC.105/C.1/L.366) et reconstitué le Groupe de travail sur la viabilité à long terme des activités spatiales du Sous-Comité scientifique et technique, pour une durée de cinq ans à compter de 2021.

59. À la demande de l'Assemblée générale, le Secrétaire général a créé ces dernières années deux groupes d'experts gouvernementaux chargés d'étudier de nouvelles mesures concrètes de prévention d'une course aux armements dans l'espace. Le Groupe créé en application de la résolution 72/250 s'est réuni en 2018 et 2019, mais n'est pas parvenu à adopter un rapport de fond de la question (voir A/74/77). Celui créé en application de la résolution 77/250 a commencé ses travaux en 2023 et fera rapport à l'Assemblée à sa soixante-dix-neuvième session. Dans sa résolution 78/238, l'Assemblée a décidé de constituer un groupe de travail à composition non limitée au titre de cette question, qui se réunirait entre 2024 et 2028.

60. Par sa résolution 76/231, l'Assemblée générale a constitué le groupe de travail à composition non limitée sur la réduction des menaces spatiales au moyen de normes, de règles et de principes de comportement responsable, qui s'est réuni en 2022 et 2023. Le groupe de travail n'est pas parvenu à adopter un rapport ; toutefois, les points de vue des États Membres ont été résumés dans un document de travail soumis par le Président (A/AC.294/2023/WP.22). Dans sa résolution 78/20, l'Assemblée a décidé de constituer un groupe de travail à composition non limitée au titre de cette question, qui se réunirait en 2025 et 2026.

## F. Techniques électromagnétiques

61. Divers types d'armes existantes ou en cours de développement utilisent l'énergie électromagnétique pour produire leurs principaux effets ou propulser un projectile. On peut répartir ces armes dans trois catégories générales : a) les capacités de guerre électronique, qui empêchent, entravent ou éliminent les moyens par lesquels l'adversaire exploite le spectre électromagnétique ; b) les armes à énergie dirigée, qui utilisent l'énergie électromagnétique pour causer des dommages ou détruire ; c) les armes à propulsion électromagnétique, qui utilisent l'énergie électromagnétique pour propulser un projectile solide à une vitesse hypersonique.

62. Les systèmes militaires modernes dépendent fréquemment de capteurs et de systèmes de guidage et de communication qui utilisent des signaux électromagnétiques. Les systèmes de guerre électronique peuvent être utilisés pour attaquer ou protéger du matériel militaire dépendant de ces signaux. On assiste récemment à l'utilisation de systèmes de guerre électronique conçus pour perturber la connexion entre les drones aériens et les stations au sol, ce que l'intégration

<sup>16</sup> Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, art. IV ; Traité interdisant les essais d'armes nucléaires dans l'atmosphère, dans l'espace extra-atmosphérique et sous l'eau, art. I 1) a).

croissante de l'autonomie permet de contrer. Plusieurs États développent des capacités de guerre électronique au sol pour perturber les services faisant appel aux techniques spatiales. De telles capacités ont déjà été utilisées à cette fin, notamment pour nuire aux activités de diffusion dans les médias ou à la fourniture de services de positionnement, de navigation et de synchronisation. L'utilisation des systèmes de guerre électronique, en particulier en temps de paix, peut perturber ou désactiver à grande échelle les connexions numériques, par exemple en brouillant les satellites fournisseurs d'Internet et leurs stations au sol.

63. Les armes à énergie dirigée comprennent les lasers, les micro-ondes de forte puissance, les ondes millimétriques et les faisceaux de particules. Des États ont testé avec succès des armes laser terrestres destinées à être utilisées contre des cibles aériennes, notamment des drones aériens, des roquettes, des missiles et des munitions entrantes. L'un des avantages de ces systèmes serait leur faible « coût par tir ». Des armes laser terrestres auraient également été utilisées par certains États pour « aveugler », « éblouir », voire détruire les capteurs optiques des satellites de surveillance en orbite terrestre basse. Des travaux de recherche sont en cours sur la possibilité d'utiliser des réseaux de lasers à fibre optique de très petite taille, les lasers à électrons libres en tant qu'armes à énergie dirigée et les impulsions électromagnétiques comme armes antisatellites.

64. Les armes à propulsion électromagnétique, comme les canons à rail ou les canons à bobine, pourraient lancer des projectiles à une distance et à une vitesse supérieures à celles atteintes par la propulsion au propergol. Si de prototypes ont été mis à l'essai, des obstacles techniques subsistent, en lien notamment avec la nécessité d'une importante alimentation électrique et de composants suffisamment robustes. Ces armes sont principalement envisagées pour des missions d'interdiction de zone, de déni d'accès et de défense navale.

#### **Processus, organismes et instruments intergouvernementaux pertinents**

65. Les capacités de guerre électronique et les armes à énergie dirigée ont été examinées par le Groupe d'experts gouvernementaux chargé d'étudier de nouvelles mesures concrètes de prévention d'une course aux armements dans l'espace (A/74/77). Les vues actuelles des États Membres figurent dans les récents rapports du Secrétaire général sur les aspects du désarmement relatifs à l'espace extra-atmosphérique, notamment ceux publiés sous les cotes A/76/77 et A/77/80. Le groupe de travail à composition non limitée sur la réduction des menaces spatiales au moyen de normes, de règles et de principes de comportement responsable a examiné diverses questions ayant trait à la guerre électronique dans le cadre de son mandat, comme indiqué dans le résumé du Président (A/AC.294/2023/WP.22).

## **G. Techniques des matériaux**

66. Les progrès réalisés dans le domaine de la science des matériaux jouent un rôle clé sur le plan de l'innovation dans de nombreux domaines liés à la paix et à la sécurité. L'utilisation de nouveaux matériaux a par exemple permis des améliorations significatives en matière de miniaturisation, de réduction du poids, d'efficacité énergétique, de renforcement de la protection et de la résistance physique et d'optimisation des capacités de furtivité. Ces avancées ont contribué de façon déterminante à la mise au point de plateformes classiques modernes ainsi que de systèmes d'armes et de leurs pièces et éléments.

67. L'impression tridimensionnelle continue à révolutionner les processus de fabrication en permettant la production décentralisée d'un nombre croissant de pièces et d'éléments, avec à la clé de nouveaux défis en matière de gouvernance et de suivi

des chaînes d'approvisionnement et de contrôle des exportations. Les améliorations apportées aux imprimantes, tant industrielles que commerciales, la possibilité d'imprimer un nombre croissant de matériaux, y compris à l'aide d'un même appareil, et la richesse des connaissances disponibles en libre accès ont encore abaissé les barrières empêchant les acteurs étatiques et non étatiques de fabriquer des composants complexes pour un large éventail d'applications ayant trait aux systèmes d'armes classiques et non classiques. Ces dernières années, la prolifération transrégionale des armes automatiques de petit calibre produites par fabrication additive et l'accroissement de leur durabilité ont suscité des inquiétudes. Une autre tendance récente concerne l'utilisation de la fabrication additive à des fins de production de munitions, notamment de petit calibre. Bien qu'elles soient actuellement moins efficaces que celles fabriquées de manière classique, ces munitions posent de nouveaux défis en matière de contrôle des armes de petit calibre et des munitions. La fabrication additive a également accru l'importance des transferts immatériels de technologie et de la conception assistée par ordinateur dans le contexte de la maîtrise des armements.

68. Les progrès de la nanotechnologie ont facilité la production, le transport et l'acheminement d'agents chimiques et biologiques, ce qui pourrait entraver les efforts de non-prolifération. Des capteurs faisant appel aux nanotechnologies sont actuellement mis au point et pourraient être utilisés pour détecter de très petites quantités de gaz et de vapeurs. Ces avancées pourraient soutenir les activités de vérification du désarmement. Les risques liés aux nanotechnologies sont notamment liés à la nature toxique de certaines nanoparticules qui sont dangereuses pour l'environnement <sup>17</sup>. Les nanotechnologies pourraient également faciliter le développement de la technologie informatique et de techniques de communication de pointe pour les opérations militaires.

69. Les armes modulaires sont composées de plusieurs composants qui peuvent être reconfigurés. Cette modularité pose des problèmes particuliers en ce qui concerne l'obligation prévue par l'Instrument international visant à permettre aux États de procéder à l'identification et au traçage rapides et fiables des armes légères et de petit calibre illicites d'inclure un marquage distinctif sur un élément essentiel ou structurel d'une arme. En outre, l'utilisation de polymères dans la fabrication d'armes suscite des inquiétudes, car les marquages sur ces matériaux sont plus vulnérables à l'effacement et à l'altération que sur des matériaux plus traditionnels comme l'acier.

### **Processus, organismes et instruments intergouvernementaux pertinents**

70. Dans sa résolution [2325 \(2016\)](#), le Conseil de sécurité a demandé au Comité créé par la résolution [1540 \(2004\)](#) de prendre note dans ses travaux, le cas échéant, de la nature en constante évolution des risques de prolifération, y compris l'utilisation par des acteurs non étatiques des progrès rapides de la science, de la technologie et du commerce international à des fins de prolifération, dans le cadre de la mise en œuvre de la résolution [1540 \(2004\)](#). Il a également engagé les États à contrôler, selon qu'il conviendrait, l'accès aux transferts intangibles de technologie et aux informations susceptibles d'être utilisées à des fins en rapport avec les armes de destruction massive et leurs vecteurs.

71. L'Assemblée générale a encouragé les États à tenir compte de l'évolution récente de la fabrication des armes légères et de petit calibre et de la technologie employée dans leur conception, s'agissant en particulier des armes en polymère et des armes modulaires (voir la résolution [78/46](#) de l'Assemblée). En juin 2024, la

<sup>17</sup> UNIDIR, « Enabling technologies and international security: a compendium – 2023 edition », 6 mars 2024, p. 13 à 15.



quatrième Conférence des Nations Unies chargée d'examiner les progrès accomplis dans l'exécution du Programme d'action en vue de prévenir, combattre et éliminer le commerce illicite des armes légères sous tous ses aspects a décidé de créer un groupe d'experts techniques à composition non limitée, qui se réunirait pendant la semaine des réunions biennales des États en 2026 et 2028, afin d'élaborer des recommandations par consensus permettant d'assurer l'application de l'Instrument international de traçage et du Programme d'action au vu de l'évolution récente de la technologie, de la fabrication et de la conception des armes légères et de petit calibre, s'agissant en particulier des armes en polymère et des armes modulaires ainsi que des armes à feu fabriquées à l'aide de l'impression 3D. Le groupe examinera à la fois les problèmes posés par l'évolution de la technologie et les possibilités qu'elle offre. Par ailleurs, les États sont convenus de faciliter le transfert de technologies aux fins du marquage, de l'enregistrement et du traçage des armes légères et de petit calibre, de mettre en commun leurs pratiques pour lutter contre la fabrication illicite de ces armes au moyen de technologies de fabrication additive, et de dialoguer, le cas échéant, avec le secteur de la fabrication additive (voir [A/CONF.192/2024/RC/3](#)).

### III. Convergence des technologies

72. La convergence de la science avec la technologie consiste en une interaction interdisciplinaire d'un domaine technologique particulier avec des technologies émergentes et établies. Pareille convergence est source à la fois de possibilités et de défis pour la paix et la sécurité internationales. Les interactions interdisciplinaires sont souvent à l'origine d'innovations et de percées scientifiques. D'une part, les progrès rapides de la science et de la technologie peuvent promouvoir le développement humain et servir de catalyseur pour la mise en œuvre du Programme de développement durable à l'horizon 2030. D'autre part, les interactions entre ces technologies peuvent donner lieu à des résultats inattendus pour la paix et la sécurité internationales.

73. Les données constituent le fondement du développement technologique et sous-tendent les interactions croissantes qui interviennent entre plusieurs domaines technologiques. La présente section donne un aperçu des sujets de préoccupation souvent abordés dans les discussions multilatérales.

#### Intelligence artificielle et autonomie

74. L'intelligence artificielle n'est pas une condition préalable au fonctionnement des systèmes d'armes autonomes. Son intégration peut néanmoins accroître l'autonomie de ces systèmes.

75. Parmi les utilisations possibles de l'intelligence artificielle dans les systèmes d'armes autonomes, on peut citer : a) le traitement en temps quasi réel des données provenant de divers capteurs (des radars terrestres aux satellites) et des signaux électroniques aux fins de la reconnaissance, de l'identification et de la classification des cibles ; b) la navigation autonome dans des terrains divers et l'adaptation à ces terrains de manière à pouvoir définir le moment du tir ou de la détonation ; c) l'analyse des menaces en temps réel de sorte à définir un plan d'action ou à proposer des mesures qui pourraient être prises à un opérateur humain chargé de décider de la marche à suivre ; d) l'apprentissage à partir des enseignements tirés des missions passées et des précédentes confrontations de façon à améliorer la performance au fil du temps ; e) le traitement du langage naturel et la vision par ordinateur, l'idée étant de permettre une interaction homme-machine.

76. La notion de « contrôle humain » sur l'emploi de la force est un sujet de préoccupation aussi bien en ce qui concerne l'utilisation de l'intelligence artificielle

dans le domaine militaire que l'autonomie<sup>18</sup>. De nombreux États et experts non gouvernementaux s'interrogent sur les niveaux acceptables d'autonomie des fonctions critiques des systèmes d'armes, notamment les fonctions de sélection des cibles et d'emploi de la force.

77. Au sein du Groupe d'experts gouvernementaux sur les technologies émergentes dans le domaine des systèmes d'armes autonomes létaux, établi sous les auspices de la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques qui peuvent être considérées comme produisant des effets traumatiques excessifs ou comme frappant sans discrimination, de nombreux États ont indiqué que les systèmes d'armes fonctionnant sans aucun « contrôle humain » pourraient ne pas être acceptables d'un point de vue juridique ou déontologique. Des désaccords subsistent quant au niveau de « contrôle humain » requis aux différents stades du « cycle de vie » du système<sup>19</sup>. Les avis divergent également sur la question de savoir si un « contrôle humain » est nécessaire pour garantir le respect du droit international humanitaire.

### **Technologies de l'information et des communications, intelligence artificielle et technologie quantique**

78. Les capacités fondées sur l'intelligence artificielle peuvent présenter à la fois des risques et des possibilités en matière de sécurité informatique.

79. Les États et les sociétés privées ont de plus en plus recours à l'intelligence artificielle pour détecter les menaces dans leurs réseaux informatiques. Par exemple, les systèmes fondés sur l'intelligence artificielle peuvent repérer et bloquer automatiquement les tentatives d'hameçonnage, les logiciels malveillants ou d'autres activités malveillantes moyennant l'analyse de tendances inhabituelles et d'anomalies dans le trafic du réseau.

80. Dans le même temps, l'intelligence artificielle peut également présenter des risques liés à l'informatique. Les applications d'intelligence artificielle, telles que les grands modèles de langage, peuvent être détournées par des attaquants pour générer des codes malveillants, repérer les vulnérabilités au niveau du système, diffuser des informations erronées ou briser les méthodes de chiffrement actuelles. Bien que ces risques ne soient pas propres aux grands modèles de langage ou à l'intelligence artificielle générative, ces technologies peuvent les accroître<sup>20</sup>. L'intelligence artificielle peut servir à créer des hypertrucages, c'est-à-dire des vidéos réalistes mais fabriquées de toutes pièces, notamment de personnalités publiques, afin de diffuser de fausses informations et d'influencer l'opinion publique. En outre, les cybercriminels peuvent créer des hypertrucages qui imitent les voix d'êtres chers<sup>21</sup>.

81. Les modèles d'intelligence artificielle pourraient être détournés pour commettre des actes malveillants dans le domaine informatique. Les auteurs de tels actes peuvent se servir de ces modèles pour accéder aux codes sources ou à des jeux de données, ou pour injecter délibérément des données erronées ou trompeuses dans les jeux de

<sup>18</sup> À l'heure actuelle, il n'existe pas de terminologie convenue entre les États pour désigner le contrôle humain. Parmi les autres termes utilisés, on peut citer le contrôle humain effectif, l'intervention humaine, la surveillance humaine, le jugement humain approprié, la capacité d'action humaine et l'humain dans/hors de la boucle.

<sup>19</sup> Le cycle de vie de l'intelligence artificielle passe par plusieurs étapes, notamment la préconception, la conception, la mise au point, la mise en service, l'utilisation et la mise hors service.

<sup>20</sup> Ioana Puscas, *AI and International Security: Understanding the Risks and Paving the Path for Confidence-building Measures* (Genève, UNIDIR, 2023).

<sup>21</sup> Emily Flitter et Stacy Cowley, « Voice deepfakes are coming for your bank balance », *The New York Times*, 30 août 2023.

données utilisés à des fins d'entraînement. Ce dernier phénomène, connu sous le nom d'attaque par empoisonnement, compromettrait la sûreté et la sécurité des systèmes d'intelligence artificielle.

82. Les technologies quantiques, associées à d'autres applications technologiques telles que les technologies de l'information et des communications et l'intelligence artificielle, peuvent présenter des possibilités et des défis en matière de paix et de sécurité. La technologie de distribution quantique de clés devrait permettre de communiquer de manière sécurisée. Elle pourrait également permettre un meilleur chiffrement et déchiffrement des données, ce qui est essentiel pour assurer la sécurité des outils numériques. Les technologies quantiques devraient également améliorer les protocoles de sécurité informatique fondés sur les principes quantiques. Néanmoins, en raison de leur puissance de calcul avancée, les ordinateurs quantiques ont le potentiel de briser les méthodes de chiffrement couramment utilisées, compromettant ainsi les systèmes de chiffrement actuels. Cela pourrait mettre en lumière de nouvelles vulnérabilités, notamment pour les infrastructures critiques qui servent à fournir des services essentiels au public. L'intégration des technologies quantiques dans l'informatique est susceptible de poser des difficultés supplémentaires aux pays disposant de capacités limitées. Il est donc nécessaire de renforcer les capacités dans ce domaine au moyen de mesures adaptées, par exemple en levant les obstacles qui entravent l'accès aux technologies quantiques à l'échelle mondiale et en faisant en sorte que les travailleurs dans le monde maîtrisent les technologies quantiques.

83. Le groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) donne l'occasion aux États Membres d'échanger leurs vues sur les risques qui se posent ou qui pourraient se poser. Ainsi, de nombreux États Membres ont mis en évidence les risques que posent l'intelligence artificielle et les technologies quantiques, entre autres technologies, et les possibilités qu'elles offrent dans le domaine informatique.

### **Intelligence artificielle et sciences de la vie**

84. Comme l'a fait remarquer le Secrétaire général dans sa note d'orientation sur le Nouvel Agenda pour la paix, de multiples technologies dans le domaine des sciences de la vie progressent et convergent pour générer des avantages potentiels considérables pour la société dans son ensemble. Du fait de la convergence des sciences de la vie avec les applications d'intelligence artificielle, il est possible de collecter et d'analyser de grandes quantités de données afin d'en dégager des modèles qui permettent d'apporter des réponses plus efficaces aux problèmes de santé publique.

85. Toutefois, ces progrès pourraient également réduire le coût des armes biologiques et les obstacles techniques à leur mise au point. Les applications d'intelligence artificielle pourraient être utilisées pour concevoir, synthétiser et diffuser des agents biologiques néfastes ou mettre au point des vecteurs, ce qui donnerait lieu à la création de nouvelles armes biologiques de pointe. La convergence de l'intelligence artificielle avec la biologie pourrait avoir d'autres effets en cascade, dont des pandémies artificielles ou d'autres événements imprévus.

86. L'intégration de l'intelligence artificielle générative dans la conception de protéines et la recherche pharmaceutique transforme rapidement la manière dont on fait face aux défis en matière de santé, dans la mesure où elle aide les scientifiques et les développeurs à accélérer le processus de prévision du fonctionnement des nouvelles protéines et des petites molécules et de leur interaction avec d'autres molécules. Une telle précision pourrait révolutionner le secteur de la recherche et du développement pharmaceutiques, mais elle pose également d'importants problèmes

de double usage<sup>22</sup>. Les progrès réalisés dans la conception de protéines et d'autres molécules peuvent renforcer la virulence ou la résistance d'agents pathogènes, ce qui fait planer la menace de leur emploi en tant qu'armes biologiques. Ce risque d'utilisation abusive montre qu'il est urgent d'instaurer un dialogue et de coopérer au niveau international pour faire en sorte que ces technologies soient employées de manière responsable.

87. L'essor de la synthèse chimique automatisée ou semi-automatisée, dans le cadre de laquelle des plateformes robotisées, alimentées par l'intelligence artificielle générative, aident à effectuer ou effectuent entièrement les opérations de synthèse, promet de rationaliser la production de produits chimiques, en réduisant potentiellement les coûts, les délais et la complexité de ces opérations. Les systèmes entièrement automatisés peuvent même abaisser les barrières à l'utilisation de ce procédé, permettant à des non-spécialistes d'effectuer des transformations chimiques complexes. Si cette pratique peut stimuler l'innovation, elle ouvre également la porte à la production clandestine de substances dangereuses, ce qui constitue une menace grave pour la paix et la sécurité internationales, car cela pourrait faciliter la prolifération des agents chimiques et compliquer la surveillance et le contrôle de ces substances.

### **Sciences de la vie et technologies de l'information et des communications**

88. La convergence de la biologie avec l'informatique a profondément modifié la nature de la recherche dans le domaine des sciences de la vie, créant de nouvelles possibilités de collaboration et d'accélération de la recherche, au moyen notamment d'un meilleur accès aux jeux de données<sup>23</sup>. Elle pourrait néanmoins s'accompagner de risques importants, liés notamment à l'exploitation des vulnérabilités des réseaux dans le secteur de la santé, y compris ceux des centres médicaux et des laboratoires biologiques, et dans la chaîne d'approvisionnement<sup>24</sup>. En outre, le risque de manipulation des données de recherche et d'accès non autorisé à ces données, qui donne lieu à la divulgation de renseignements médicaux privés, suscite des inquiétudes. Cela pourrait saper la confiance du public dans les institutions de santé, compliquer la lutte contre les pandémies mondiales et exacerber les tensions entre les États au sujet des normes de sécurité informatique à appliquer.

### **Armes nucléaires, technologies de l'information et des communications et intelligence artificielle**

89. Les armes nucléaires ont été mises au point pour la première fois alors que les capacités informatiques n'en étaient qu'à leurs balbutiements<sup>25</sup>. De ce fait, peu d'attention avait été accordée aux répercussions que pourraient avoir l'intelligence artificielle et la sécurité informatique, qui présentent aujourd'hui des défis potentiels pour les armes nucléaires et les systèmes de commandement et de contrôle et systèmes de détection lointaine qui y sont associés.

<sup>22</sup> Voir <https://www.nature.com/articles/d41586-024-00699-0>, <https://www.technologyreview.com/2023/02/15/1067904/ai-automation-drug-development/>, <https://communities.springernature.com/posts/cavitomix-drug-solver-a-gpu-accelerated-tool-for-drug-repurposing-and-off-target-analysis-using-cavity-property-point-clouds-on-nvidia-dgx-a71725f0-77f6-46e5-8a3d-9c6d19aae6b6> et <https://www.nvidia.com/en-us/clara/bionemo/>.

<sup>23</sup> Voir [https://documents.unoda.org/wp-content/uploads/2021/04/07\\_31\\_Pauwels\\_Slides\\_MX2.pdf](https://documents.unoda.org/wp-content/uploads/2021/04/07_31_Pauwels_Slides_MX2.pdf).

<sup>24</sup> Lauren C. Richardson *et al.*, « Cyberbiosecurity: a call for cooperation in a new threat landscape », *Frontiers in Bioengineering and Biotechnology*, vol. 7 (juin 2019).

<sup>25</sup> Voir <https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf>.

90. Les activités malveillantes liées à l'informatique qui sont menées en temps de paix sont susceptibles d'accroître les tensions et les risques de conflits armés classiques entre États dotés de l'arme nucléaire, augmentant ainsi le risque d'escalade nucléaire (voir [A/76/182](#)). Lors d'un conflit armé, les actes malveillants qui visent des systèmes d'armes nucléaires ou des systèmes à double usage, tels que les systèmes de détection lointaine, peuvent entraîner des erreurs d'interprétation et d'appréciation et conduire à l'utilisation accidentelle d'une arme nucléaire.

91. Des spécialistes ont recensé les activités, telles que le piratage, l'usurpation d'identité, l'interférence et d'autres actes malveillants, qui visent à exploiter les vulnérabilités informatiques des systèmes d'armes nucléaires. Parmi ces vulnérabilités, on peut citer : a) les communications entre les systèmes de commandement et de contrôle<sup>26</sup> ; b) les communications entre les stations de commandement et les plateformes de missiles (comme les sous-marins) et les missiles ; c) les données de télémétrie des missiles transmises aux installations de commandement et de contrôle au sol et dans l'espace ; d) les centres d'analyse pour la collecte et l'interprétation des données ; e) les technologies numériques dans les moyens de transport ; f) l'utilisation des technologies numériques dans les laboratoires et les installations d'assemblage ; g) les informations de ciblage en temps réel provenant des systèmes spatiaux, y compris les données de positionnement, de navigation et de synchronisation ; h) les données de positionnement des plateformes de lancement ; i) les informations de ciblage en temps réel provenant des stations terrestres ; j) les systèmes autonomes ou fondés sur l'intelligence artificielle intégrés dans les systèmes de commandement, de contrôle ou de communication.

92. Les États parties au Traité sur la non-prolifération des armes nucléaires ont exprimé leur inquiétude individuellement et collectivement au sujet des liens qui existent entre ces technologies et les armes nucléaires, notamment dans divers documents de travail présentés tout au long du cycle d'examen du Traité<sup>27</sup>.

93. L'intégration de l'intelligence artificielle dans les armes nucléaires et les vulnérabilités informatiques des systèmes nucléaires de commandement, de contrôle et de communication pourraient compromettre la stabilité internationale et avoir des répercussions sur les concepts de sécurité, tels que la dissuasion réciproque (ibid.). Des acteurs mal intentionnés pourraient exploiter ces vulnérabilités pour lancer des attaques non cinétiques, par exemple en usurpant ou en piratant des systèmes de détection lointaine, leur but étant de déclencher de fausses alertes ou de créer des perturbations dans les réseaux qui pourraient dégénérer en confrontations nucléaires involontaires. L'intelligence artificielle pourrait accroître la sophistication de ces attaques. Dans les conflits armés, les craintes d'interférence avec les systèmes d'armes nucléaires pourraient créer des situations déstabilisantes dans lesquelles les États se sentiraient obligés de recourir aux armes nucléaires en premier, ce qui provoquerait une escalade rapide et incontrôlée.

94. L'intégration de l'intelligence artificielle dans les systèmes d'armes nucléaires, comme le contrôle autonome ou la délégation d'autorité relative au lancement d'armes nucléaires, pourrait avoir des conséquences catastrophiques. Les problèmes techniques liés à la sécurité de l'intelligence artificielle, tels que les attaques par empoisonnement et la prise de décisions potentiellement imprévisibles (« boîte noire »), suscitent des inquiétudes quant à la crédibilité des informations essentielles à la prise de décisions en matière nucléaire et augmentent les risques d'utilisation

<sup>26</sup> UNIDIR, *Understanding Nuclear Weapon Risks*, John Borrie, Tim Caughley et Wilfred Wan, éd. (Genève, 2017).

<sup>27</sup> Voir, par exemple, [NPT/CONF.2020/WP.6](#), [NPT/CONF.2020/WP.9/Rev.1](#), [NPT/CONF.2020/WP.70](#), [NPT/CONF.2026/PC.I/WP.24](#) et [NPT/CONF.2026/PC.I/WP.30](#).

accidentelle d'armes nucléaires<sup>28</sup>. Le recours à l'intelligence artificielle dans les systèmes nucléaires de commandement, de contrôle et de communication pourrait réduire le temps consacré à la prise de décisions, la vitesse de l'intelligence artificielle pouvant dépasser les capacités humaines, ce qui entraînerait des erreurs d'appréciation et une escalade en cas de crise. Pour éviter qu'une telle situation ne se produise, trois États dotés de l'arme nucléaire ont souligné, dans le document de travail qu'ils ont présenté à la dixième Conférence d'examen des Parties chargée d'examiner le Traité sur la non-prolifération des armes nucléaires (NPT/CONF.2020/WP.70), qu'ils s'engageaient à maintenir « le contrôle humain et l'intervention humaine à toutes les étapes essentielles à la formation de décisions souveraines concernant l'emploi des armes nucléaires et à leur exécution ».

#### IV. Conclusions et recommandations

95. Les entités des Nations Unies continueront de soutenir et de faciliter les processus existants et les nouveaux processus pour faire face aux nouveaux défis avant que ceux-ci ne puissent constituer une menace pour la paix et la sécurité, les droits humains, les normes et principes humanitaires ou d'autres buts et objectifs de l'Organisation. Il est recommandé que les États Membres définissent les instances multilatérales dans le cadre desquelles ils peuvent discuter des synergies entre les technologies examinées dans le présent rapport.

96. La Commission du désarmement a accepté d'examiner le point inscrit à son ordre du jour intitulé « Recommandations visant à promouvoir une communauté de vues sur les questions relatives aux technologies émergentes dans le contexte de la sécurité internationale » au cours de son cycle triennal 2024-2026. Il s'agit d'une occasion importante pour les États Membres de se pencher sur les questions transversales applicables à toutes les technologies émergentes et d'étudier les technologies qui ont des répercussions sur la sécurité internationale mais qui ne font pas encore l'objet d'un examen au sein de l'ONU.

97. Il est recommandé que les organes et entités des Nations Unies continuent d'encourager une participation multipartite, géographiquement équitable et respectueuse de l'équilibre entre les sexes, notamment de la part du monde académique, de l'industrie et d'autres acteurs du secteur privé, en s'appuyant sur des plateformes formelles et informelles.

98. Les États Membres sont encouragés à continuer de rechercher des moyens d'intégrer l'examen des évolutions de la science et de la technique dans les travaux qu'ils mènent au sein de l'ensemble des organes de désarmement des Nations Unies, notamment dans le cadre des processus d'examen de l'application des traités sur le désarmement. Il pourrait s'agir de mettre en place de mécanismes d'examen de la science et de la technologie, le cas échéant, afin d'éclairer les débats intergouvernementaux. Ces mécanismes devraient recenser et examiner les technologies nouvelles et émergentes qui perpétuent ou amplifient les préjugés sociaux, notamment les préjugés sexistes, ainsi que leurs répercussions sur l'application du droit international.

99. Le Sommet de l'avenir, qui se tiendra les 22 et 23 septembre 2024, représente une occasion importante de prendre des mesures visionnaires et concrètes concernant

<sup>28</sup> En informatique, une « boîte noire » est un système dans lequel on connaît les entrées et les sorties mais dont le fonctionnement interne est masqué. On a donc affaire à cette notion lorsque le fonctionnement interne et les processus décisionnels d'un système d'intelligence artificielle sont opaques et ne peuvent être expliqués ou être compris par les humains. Voir <https://undir.org/files/2020-09/BlackBoxUnlocked.pdf>.

les technologies émergentes et leur incidence sur la paix et la sécurité. J'exhorte les États Membres à donner suite aux recommandations formulées à cet égard dans ma note d'orientation intitulée « Un Nouvel Agenda pour la paix ».

100. Il est recommandé que l'Assemblée générale continue de demander que soient soumis chaque année des rapports contenant une actualisation des informations contenues dans le présent rapport, afin de contribuer à continuer de sensibiliser aux évolutions de la science et de la technique et à leurs incidences éventuelles sur l'action menée en matière de sécurité internationale et de désarmement.

---