United Nations A/HRC/60/63

General Assembly

Distr.: General
14 July 2025

Original: English

Human Rights Council
Sixtieth session
8 September–3 October 2025
Agenda items 3 and 5
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Human rights bodies and mechanisms

Human rights implications of new and emerging technologies in the military domain

Report of the Human Rights Council Advisory Committee

GE.25-10692 (E) 110725 110725

I. Introduction

A. Mandate

1. The present report was mandated by the Human Rights Council in its resolution 51/22, in which it requested the Human Rights Council Advisory Committee to prepare a study examining the human rights implications of new and emerging technologies in the military domain.

2. At its twenty-ninth session, the Advisory Committee established a drafting group composed of Buhm-Suk Baek (Chair), Nadia Amal Bernoussi, Milena Costas Trascasas, Alessandra Devulsky, Jewel Major, Javier Palummo (Rapporteur), Vasilka Sancin, Vassilis Tzevelekos, Catherine Van de Heyning, Frans Viljoen and Yue Zhang.

B. Scope of the study

3. In the present study, the Advisory Committee addresses the full life cycle of new and emerging technologies in the military domain. It examines how international human rights law informs decision-making on data collection and management, transparency, accountability, non-discrimination and rights protection. It outlines the applicable international legal frameworks for the design, development, deployment and oversight of such technologies and their potential dual use (military and non-military).

4. The study contains an analysis of how existing international treaties, customary international law and soft law instruments, including the Guiding Principles on Business and Human Rights, may contribute to regulating the development and use of these technologies, and an examination of the importance and complementary roles of international humanitarian law and international human rights law.

5. It also contains an examination of the human rights implications of new and emerging technologies in the military domain, incorporating United Nations discussions, stakeholder contributions, including 22 questionnaire responses,[1] and secondary research to analyse the current state of and emerging human rights concerns related to new and emerging technologies in the military domain. The analysis takes a forward-looking approach, considering potential scenarios arising from new technologies. The study's final section contains recommendations for future actions.

C. Conceptual and normative framework

1. New and emerging technologies, military domain and dual use

6. For the purposes of the present report, "military domain" refers to the operational environment of armed forces and defence-related activities, including security forces. "New and emerging technologies" refer to those technologies that are in the process of development or have recently been introduced, often characterized by their transformative potential. As they are driven by advances in several fields, notably artificial intelligence (AI), neuroscience, biotechnology, nanotechnology and robotics, new and emerging technologies in the military domain may not always be synonymous with "weapons"; while some weapons may involve new and emerging technologies, not all new and emerging technologies in the military domain are weapons. Due to their dual-use nature, it is challenging to find new and emerging technologies in the military domain not affected by innovation, just as technological innovations cannot be confined to a purely military domain.[2] "Dual-use technologies" refer to innovations with both civilian and military applications, with potential

[1] See https://www.ohchr.org/en/hr-bodies/hrc/advisory-committee/human-rights-implications.

[2] See international-conference_-military-technologies-vis-a-vis-human-rights-concerns-_-summary-report.pdf.

uses in the commercial, public and military domains.[3] Consequently, the conceptual framework of the report should be considered porous, as it is challenging to define these categories precisely.

7. While military armaments have always incorporated new technologies, today's digital advancements, particularly AI, represent a significant leap forward. This paradigm shift is occurring in a context of technological divide and power asymmetry, in which military technologies developed in some parts of the world may be deployed in States with limited influence over their development. For instance, States from the global South are often excluded from the development and governance of new and emerging technologies in the military domain although their populations may be disproportionately affected by their use.

8. New and emerging technologies in the military domain pose significant challenges for States and other actors to comply with international human rights law. Fundamentally, the use of such technologies in the military domain presents a risk of dehumanizing the use of force, exacerbating trends that reduce human lives to mere data points through algorithmic labelling and targeting, diminishing or even excluding the moral and ethical considerations inherent to human judgment[4] and enhancing the risk of arbitrary and disproportionate use of force. Such dehumanization is incompatible with human rights principles, including the right to life, personal integrity, non-discrimination and human dignity, a cornerstone of international human rights law and many domestic legal systems. Furthermore, new and emerging technologies in the military domain might have differentiated impacts on the human rights of distinct groups.[5]

9. A key concern regarding new and emerging technologies in the military domain is the extent to which humans maintain meaningful control over technologies, particularly those involving the use of force, including autonomous weapons systems and other armed, uncrewed systems. These technologies rely on automation and autonomous decision-making, raising risks of diminished human oversight and accountability. Autonomous new and emerging technologies in the military domain may lead to serious human rights violations, including threats to the rights to life, freedom of expression, privacy and non-discrimination, as well as violations of the prohibition of ill-treatment. The entire life cycle of these technologies must adhere to a robust human rights protection framework, ensuring that technological advancements do not undermine human rights and that victims have access to accountability mechanisms and redress.

10. An additional challenge is that new and emerging technologies in the military domain – from goods and computer hardware to software – are referred to as "dual-use technologies" and have the potential to be used in commercial, public and military domains. Given potential gaps between legal frameworks and the deployment of new and emerging technologies, emerging human rights concerns must be addressed before they become operational, especially in conflict settings. Risks are further amplified by the private sector's central role in the development of new and emerging technologies. Businesses, therefore, play a crucial role in preventing human rights violations and abuses.

2. International legal frameworks applicable throughout the life cycle of new and emerging technologies in the military domain

11. International law, both treaty-based and customary, applies to the development and use of new and emerging technologies in the military domain, and States must comply with it. Furthermore, States have a positive duty to ensure compliance where such technologies are employed by non-State actors falling under their jurisdiction. The full life cycle of new

[3] Marcello Ienca and Effy Vayena, "Dual use in the 21st century", *Swiss Medical Weekly*, vol. 148, No. 4748 (2018); and Marcus Schulzke, "Drone proliferation and the challenge of regulating dual-use technologies", *International Studies Review*, vol. 21, No. 3 (September 2019).

[4] Christof Heyns, "Autonomous weapons in armed conflict and the right to a dignified life", *South African Journal on Human Rights*, vol. 33, No. 1 (2017).

[5] See International Conference of the Red Cross and Red Crescent, resolution 34IC/24/R2.

and emerging technologies in the military domain is governed by multiple international legal frameworks,[6] which apply in a complementary and mutually reinforcing manner.[7]

12. International human rights law plays a crucial role in governing new and emerging technologies in the military domain and applies both in peacetime and during armed conflict. Certain human rights are non-derogable, even during armed conflict, including the right to life,[8] the prohibition of ill-treatment, slavery and servitude and the principles of legality, non-retroactivity and freedom of thought, conscience and religion.[9]

13. Key instruments relevant to new and emerging technologies in the military domain include the International Bill of Human Rights and other core international human rights instruments. Given the potential of new and emerging technologies to be used for mass surveillance and discriminatory practices, the principles of transparency and accountability are crucial in this context. Rights such as privacy, freedom of expression and non-discrimination, as well as those related to health, culture and work, must be safeguarded in the design, development and deployment of such technologies. The prohibition of ill-treatment also applies to their use. Non-discrimination is especially relevant, as new and emerging technologies can reinforce biases against marginalized and/or vulnerable groups if algorithms are not properly designed and monitored. States must ensure that the development and use of new and emerging technologies in the military domain comply with international human rights law and provide effective remedies for violations. Businesses involved in developing or deploying such technologies must adhere to relevant standards, under the Guiding Principles, avoid human rights infringements and proactively prevent potential human rights risks in their operations.

14. International humanitarian law is also fundamental in regulating new and emerging technologies in the military domain. While certain treaties explicitly regulate or prohibit specific weapons, the Geneva Conventions and the Additional Protocols thereto apply to all forms of warfare and weapons, including those yet to be developed, as affirmed by the International Court of Justice.[10] Article 36 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), obliges Parties to review whether the new weapons, means or methods of warfare that they are studying, developing, acquiring or adopting would be prohibited by the Protocol or other rules of international law. Although the provision formally binds only the Parties to that Protocol, some non-Parties also conduct legal weapons reviews.

15. The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects is aimed at banning and restricting the use of certain types of weapons that are considered to cause unnecessary or unjustifiable suffering to combatants or to affect civilians indiscriminately. The Protocols to the Convention govern the use of specific weapons and the development of weapons technologies by applying three fundamental principles of international humanitarian law: (a) the right of the Parties to an armed conflict to choose methods or means of warfare is not unlimited; (b) the protection of the civilian population against the effects of hostilities; and (c) the prohibition of superfluous injury or unnecessary suffering upon combatants. Moreover, the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems has reaffirmed that international humanitarian law continues to apply fully to the potential development and use of lethal autonomous weapons systems.[11]

16. International humanitarian law remains essential to protect civilians from the effects of armed conflict in the face of rapidly advancing technology, making it incumbent on States

[6] This includes other areas of international law (e.g. environmental and labour law). Groups of States have also adopted related statements, commitments and codes of conduct.

[7] *International Legal Protection of Human Rights in Armed Conflict* (United Nations publication, 2011). See also Human Rights Council resolution 51/22.

[8] See Human Rights Committee, general comment No. 36 (2018).

[9] See Human Rights Committee, general comment No. 29 (2001).

[10] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996*, p. 226, para. 86.

[11] CCW/GGE.1/2023/2, para. 21 (a).

to ensure compliance, regardless of scientific and technological advances.[12] Even if States are not parties to the treaties referenced above, they remain bound by customary international law, of which several norms are of jus cogens nature. States must also comply with their due diligence obligations, meaning that they must make all efforts to prevent a breach of an international obligation, including by adopting regulations and measures, and the duty of vigilance, applicable to public and private actors.[13] Notably, due diligence is an obligation of means and not of result.

17. The duty to ensure that developments of new and emerging technologies in the military domain do not violate international law is a primary obligation of each State.[14] Therefore, States must conduct comprehensive evaluations to determine how specific international legal norms apply to new and emerging technologies in the military domain. In this regard, national human rights institutions must take on a relevant role.[15] The timely review of the domestic laws of each State is crucial to identifying and addressing any inconsistencies with international laws.

18. Despite existing legal frameworks, the rapid advancement of new and emerging technologies in the military domain challenges their implementation. This has spurred debates on applying international law to new and emerging technologies in the military domain, including AI-driven decision-making, autonomous weapons systems, uncrewed systems and military programmes enhancing combatants' physical and cognitive abilities. While AI and new and emerging technologies introduce new terms, stakeholders must ensure alignment with international legal language and standards.[16]

II. Human rights impact

A. Artificial intelligence as an enabling technology in the military domain

19. In the military domain, AI serves as a critical enabling technology, enhancing operational capabilities across various functions. It is important to distinguish between AI-enabled technologies – tools and systems that leverage AI to support human decision-making – and autonomous systems, such as autonomous weapons systems, which can operate with limited or no human intervention. While AI can assist in decision-making, not all AI-enabled systems are autonomous, nor does autonomy inherently involve AI. This section focuses on the role of AI as an enhancement tool under human oversight.

20. Although AI has been in development for decades and could be considered as a long-standing emerging technology, its role in enhancing weapon system autonomy, supporting military decision-making and integrating into military supply chains has recently gained prominence. Recent computing advances have heightened its role in those areas.[17]

21. AI is increasingly integrated into military operations and used to enhance intelligence analysis, scenario planning, logistics and battlefield decision-making. AI systems can operate with varying degrees of autonomy: the trend is that the greater the autonomy, the less human oversight and control. AI can assist in decision-making by, for instance, rapidly processing vast amounts of data and can potentially override human judgment in particular preordained scenarios such as high-pressure situations. However, AI also raises human rights concerns, including regarding freedom of expression, privacy and non-discrimination. For example, it could misidentify a disability assistive device as a weapon, violating non-discrimination

[12] Treaty law is also applicable in this respect (e.g. Protocol I Additional to the Geneva Conventions of 1949).

[13] International Court of Justice, *Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010*, p. 14, para. 197.

[14] International Committee of the Red Cross (ICRC), *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons* (Geneva, 2016).

[15] Digital Rights Alliance submission.

[16] See committees.parliament.uk/writtenevidence/120290/pdf/.

[17] Stefka Schmid, Thea Riebe and Christian Reuter, "Dual-use and trustworthy?", *Science and Engineering Ethics*, vol. 28, No. 2 (March 2022).

principles.[18] Algorithmic bias may also lead to racial or gender discrimination. Upholding human dignity, as required by international human rights law, is essential throughout the life cycle of AI to ensure equal worth for all individuals.[19]

22. AI may limit human oversight and the ability to exercise moral or legal judgment over its outputs. The key challenge is determining whether, and to what extent, international law requires human control in targeting, detention, weapons use and safeguarding human dignity. This includes compliance with legal frameworks such as the Universal Declaration of Human Rights, which states that all humans are "endowed with reason and conscience and should act towards one another in a spirit of brotherhood".

23. Another major issue is the lack of transparency in AI decision-making, with many systems functioning as "black boxes", challenging human rights principles of transparency and effective remedy. Existing responsibility frameworks, based on human action, may be disrupted by AI integration, especially with machine learning. Ensuring clear lines of responsibility is essential but challenging when AI operates with significant autonomy or when its reasoning is opaque. Accountability includes both preventive measures and ex-post evaluations of potential violations of international law. Key international accountability mechanisms apply to both individual criminal responsibility and State responsibility.

24. It is also a human rights concern that new and emerging technologies in the military domain, particularly those using AI, consume large amounts of energy, generate significant carbon emissions and rely heavily on raw materials including nickel, cobalt and graphite, posing long-term risks, including to the right to a clean, healthy and sustainable environment. As these technologies evolve, addressing their environmental and human rights impacts is essential.

B. Autonomous weapons systems and their implications for human agency and accountability

25. Autonomous weapons systems can make independent decisions with limited or no human intervention. Lethal autonomous weapons systems, a subset of autonomous weapons systems, stand out due to their capacity to independently execute decisions potentially involving lethal force. A legal challenge is defining autonomous weapons systems, due to the varied levels of possible human intervention and control. Lack of consensus among States on such a legal definition further complicates their regulation.[20]

26. Unlike automated decision-making systems that operate based on predefined commands and criteria, autonomous weapons systems are designed to operate with higher levels of autonomy, raising thereby complex legal questions regarding their compliance with international law. These systems introduce, for example, unique challenges concerning human dignity, as well as human control and transparency with implications for the rights to life, to an adequate remedy and to privacy.[21] In the field of international humanitarian law, the main challenges relate to the principles of distinction, proportionality, precaution in attack and the requirement to undertake weapons reviews.

27. Proponents of a ban on autonomous weapons systems argue that they could violate the Martens clause of the Convention for the Pacific Settlement of International Disputes, according to which weapons must comply with the "principles of humanity and the dictates of the public conscience".[22] However, they often see this clause as a basis for regulation rather

[18] A/HRC/49/52, para. 54.

[19] United Nations Educational, Scientific and Cultural Organization, Recommendation on the Ethics of Artificial Intelligence.

[20] See 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.

[21] Privacy International submission.

[22] Rupert Ticehurst, "The Martens clause and the laws of armed conflict", *International Review of the Red Cross*, No. 317, April 1997.

than a ban.[23] Conversely, opponents of a ban may even question the legal value of this clause.[24]

28. Despite consensus on the need to maintain human control over autonomous weapons systems, specific international regulations and standards to ensure meaningful human control over the use of force are lacking.[25] Various proposals have identified practical elements of human control, including restrictions on the parameters of their use, and the operational environment. Measures such as target restrictions, mandatory human oversight and accountability mechanisms have been suggested to address the inherent unpredictability and risks posed by the development, deployment and use of these systems.[26] Within the Group of Governmental Experts, whose work encompasses both autonomous and AI technologies, there has been ongoing debate on what constitutes "meaningful human control". However, consensus has yet to be reached. Nonetheless, there is broad agreement on the need to retain some level of human involvement. Furthermore, human rights remain largely absent from the discussions of the Group of Governmental Experts.[27]

29. Integrating AI and autonomous technologies into these new systems presents unique international legal challenges. Under the current legal regime, AI deployment may complicate the determination of responsibility and accountability for violations of international law. Reduced transparency in AI-driven targeting may create gaps, making it harder to attribute individual criminal responsibility for war crimes or State responsibility for violations of international law. While individual criminal responsibility has been widely debated in legal doctrine and the United Nations, discussions on challenges posed by autonomous weapons systems to State responsibility remain nascent.[28] In addressing accountability, it is necessary to delineate the specific responsibilities of technology developers, operators and military commanders and the State's obligations under international law, including under the Guiding Principles. Further legal clarity on these aspects remains crucial, as each new and emerging technology presents unique challenges across different levels of responsibility.

30. Furthermore, attributing conduct for the purposes of establishing State responsibility under international law in the context of autonomous weapons systems raises critical legal questions that warrant in-depth examination. While States in the Group of Governmental Experts agreed by consensus that every internationally wrongful act of a State, including those potentially involving lethal autonomous weapons systems, entails international responsibility, they did not provide further clarity on the attribution of State responsibility for violations of international law.[29] It was noted in the Chair's first draft proposal that the conduct of a State's organs – such as its agents and all persons forming part of its armed forces – is attributable to that State, including acts and omissions involving the use of such systems.[30]

[23] See https://blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons/.

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

[25] See https://www.ejiltalk.org/what-level-of-human-control-over-autonomous-weapon-systems-is-required-by-international-law/.

[26] Ibid.; Vincent Boulanin and others, *Limits on Autonomy in Weapon Systems* (Stockholm, Stockholm International Peace Research Institute and ICRC, 2020); and CCW/GGE.1/2023/WP.6.

[27] See CCW/GGE.1/2020/WP.6, CCW/GGE.1/2023/WP.2/Rev.1 and CCW/GGE.1/2024/WP.10.

[28] Robin Geiß, "State control over the use of autonomous weapon systems", in *Military Operations and the Notion of Control Under International Law*, Rogier Bartels and others., eds. (The Hague, Asser Press, 2021); and Lutiana Valadares Fernandes Barbosa, *Autonomous Weapons Systems and the Responsibility of States: Challenges and Possibilities* ((Boca Raton, Florida, United States of America, and Abingdon, United Kingdom of Great Britain and Northern Ireland, CRC Press, 2024).

[29] CCW/GGE.1/2022/2, para. 19.

[30] See https://documents.unoda.org/wp-content/uploads/2022/07/CCW-GGE.1-2022-CRP.1.docx. See also CCW/GGE.1/2022/WP.2; and Alisha Anand Ioana Puscas, "Proposals related to emerging technologies in lethal autonomous weapons systems" (United Nations Institute for Disarmament Research, 2022).

31. A key consideration is whether, and under what circumstances, the conduct of autonomous weapons systems can or should be attributed to the State and whether the current regime on the international responsibility of States, which is based on a human action paradigm, suffices to attribute responsibility in the context of such systems.[31] While States have positive human rights obligations to ensure that these technologies comply with international law and take preventive measures to minimize risks, the framework of positive obligations alone may not suffice to establish State responsibility in cases where autonomous weapons systems operate with significant autonomy and beyond the foreseeability of the human in charge. The challenge lies in determining under what circumstances the actions in the context of such systems should be equated to the conduct of the deploying State, thereby engaging State responsibility for such actions under international law. Addressing these questions is essential to ensure accountability and compliance with international law.

32. Integrating autonomous capabilities into weapon systems encompassing AI technology introduces unique challenges in legal reviews. Autonomous weapons systems interact with their environment, necessitating testing across multiple scenarios. As human reliance on AI grows, greater attention must be given to these systems' compatibility with legal standards. While the selection and revision of algorithmic data are essential components, a comprehensive legal review of autonomous weapons systems incorporating AI systems should take into account States' obligations under international human rights law, including the rights to life, integrity, non-discrimination and privacy, as well as the principles of transparency and accountability and the potential risks of unintended consequences.[32] Due diligence obligations should be specified to eliminate unintended biases and discrimination, especially where these could violate rights protected under international law. Legal reviewers must be involved in the design phases to address these issues proactively and implement safeguards against potential human rights violations. Nevertheless, questions persist about the compatibility of machine-based decision-making with human rights principles,[33] and it is important to note that there is considerable debate over whether autonomous weapons systems can be produced and used in a manner that fully complies with all requirements of international law.

33. The advent of new and emerging technologies in the military domain, such as the technology used in autonomous weapons systems, challenges existing international law, highlighting the need for new rules to regulate and, where necessary, possibly prohibit such technologies if they cannot meet international legal standards. The Group of Governmental Experts is exploring a two-tier approach: prohibiting weapons incompatible with international humanitarian law and regulating others. This aligns with calls from the Secretary-General and the President of the International Committee of the Red Cross for new international rules to safeguard humanity.[34] In his report prepared pursuant to General Assembly resolution 78/241, the first Assembly resolution on lethal autonomous weapons systems, the Secretary-General urged States to conclude, by 2026, a legally binding instrument to prohibit such systems that function without human control or oversight and that cannot be used in compliance with international humanitarian law, and to regulate all other types of autonomous weapons systems.[35] However, States remain divided on whether these regulations should be legally binding or voluntary in nature.[36] Furthermore, discussion on international human rights law and autonomous weapons systems is necessary.

[31] Articles on responsibility of States for internationally wrongful acts (*Yearbook of the International Law Commission 2001*, vol. II (Part Two) (A/CN.4/SER.A/2001/Add.1 (Part 2), p. 26); Rebecca Crootof, "War torts", *University of Pennsylvania Law Review*, vol. 164, No. 6 (May 2016); and Valadares Fernandes Barbosa, *Autonomous Weapons Systems and the Responsibility of States*.

[32] Tobias Vestner Altea Rossi, "Legal reviews of war algorithms", *International Law Studies*, vol. 97 (2021).

[33] See A/HRC/23/47.

[34] See https://www.icrc.org/en/document/joint-call-un-and-icrc-establish-prohibitions-and-restrictions-autonomous-weapons-systems.

[35] A/79/88, para. 90.

[36] Ibid., paras. 63–86.

C. Technologies for human enhancement in the military domain

34. Despite their potential for non-lethal strategies and stress reduction in conflict, the development of physical and cognitive enhancement technologies presents significant ethical, legal, societal and operational challenges. Concerns include impacts on military values, operational dilemmas, military law application and informed consent. Moreover, different enhancement types – genetic, biological or cybernetic – pose distinct human rights and ethical risks. Similar civilian advancements, as in employment settings, underscore the broader implications and dual-use nature of such technologies.[37]

35. Advances in AI further expand the potential of human enhancement technologies, playing a crucial role in medical treatments and rehabilitation for physical and cognitive impairments in non-military settings.[38] Historically, efforts to enhance human performance have prioritized mission success, sometimes at the expense of individual well-being. This tension may limit soldiers' and military physicians' autonomy in administering neurotechnologies (e.g. pills, neural implants or neuroprostheses). Ensuring transparency and respect for human dignity and the right to health is essential, including decision-making autonomy and the post-service conditions of enhanced combatants.[39]

36. The adoption of technologies such as brain-computer interfaces in the military domain is said to enhance cognitive capabilities by merging human and machine intelligence. While the development of robotics and neurotechnologies such as brain-computer interfaces clearly present significant promise in the healthcare domain, their use in the military context raises specific challenges, particularly with respect to the application of laws governing accountability and human control over military operations and decision-making. Brain-computer interfaces and other advanced neurotechnologies could also potentially be misused for coercive interrogation techniques in an adversarial context. The use of such methods could violate human rights as they might inflict psychological harm or constitute torture, even absent physical violence.[40]

37. Introducing novel human enhancement technologies into military activities raises significant concerns regarding the legal implications and potential human rights abuses as they pose risks, particularly concerning the right to privacy, the necessity of obtaining free and informed consent, and potential violations of the physical and mental integrity of combatants over the long term. States and businesses have a duty to address these risks in accordance with the applicable provisions of international law.[41]

38. Furthermore, the power asymmetries inherent in the military domain, coupled with the longer-term implications of data collection, processing and retention practices of personal data, may result in downstream privacy violations that manifest much later. For instance, the coercive use of these technologies could severely undermine the dignity and autonomy of soldiers, whereas non-coercive applications raise serious ethical questions regarding consent and long-term health effects. Such considerations should lead to specific prohibitions in cases of coercive use, as well as moratoriums or limitations for non-coercive uses to prevent the potential abuse of these technologies.[42]

---

[37] Timo Istace and Milena Costas Trascasas, "Between science-fact and science-fiction", Research Brief (Geneva, Geneva Academy of International Humanitarian Law and Human Rights, 2024).

[38] Yuval Shany and Tal Mimran, "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 and Russal Buchan, eds. (Talinn, NATO CCDCOE Publications, 2022); and Margaret Kosal and Joy Putney, "Neurotechnology and international security", *Politics and the Life Sciences*, vol. 42, No. 1 (spring 2023).

[39] Sebastian Sattler and others, "Neuroenhancements in the military" *Neuroethics*, vol. 15, No. 1 (February 2022).

[40] Charles N. Munyon, "Neuroethics of non-primary brain computer interface", *Frontiers in Neuroscience* (October 2018).

[41] See A/HRC/57/61.

[42] Ibid., para. 80 (b).

D. Law enforcement and border control

39. Technologies such as AI-driven surveillance, predictive modelling and biometrics are increasingly used by border control and law enforcement authorities. While these tools are often promoted for their potential to enhance public safety, by optimizing emergency responses, enabling secure and seamless crossings and assisting in crime prevention, they also pose serious risks to human rights in law enforcement and border control settings.[43]

40. Biometric applications in this field include identity verification for access control and identification during capture or detention. While these systems can fail, little attention has been given to the potential human rights impacts of their use in the military domain, particularly on vulnerable groups, including persons with disabilities, older persons, children, people of African descent, migrants and others affected by historical and structural discrimination. There is concern that their application reinforces inequality through biases and discriminatory profiling, often stemming from prejudices embedded in historical data collection, processing and retention practices. In migration management, the diversity in biometric data influenced by cultural differences can exacerbate these biases. For example, biometric technologies such as facial recognition could violate the right to non-discrimination, as they are prone to misidentifying Indigenous Peoples and people of African descent, particularly women. They may also infringe on the right to privacy if Governments and businesses share biometric data without an individual's consent. Given the emphasis in international human rights law on the explicit right to privacy, equality and non-discrimination, it is essential to conduct human rights impact assessments and address how those technologies may reinforce existing inequalities.[44]

41. Optical surveillance systems, including aerial surveillance, now have unprecedented capabilities to remotely monitor, record and track individuals in public spaces, including borders, using technologies such as drones and facial recognition. These advancements pose serious risks to human rights, including the freedoms of movement, association, assembly, privacy and non-discrimination.

42. In recent years, there has been growing attention on autonomous weapons systems. While much of the discourse has been focused on their use in armed conflict, it is increasingly evident that they are also being considered for border management and domestic law enforcement. This shift raises significant human rights concerns, particularly regarding rights to life, bodily integrity and dignity. Unlike armed conflict, where force is mainly governed by international humanitarian law, law enforcement personnel may use force only when unavoidable, strictly necessary and proportionate to their duties.[45]

E. Cognitive warfare

43. Cognitive warfare is aimed at controlling an adversary's thoughts and perceptions to influence decisions and actions.[46] Rooted in military disinformation, it represents a new strategic frontier due to the transformative impact of AI. Advanced technologies enable large-scale psychological influence, targeting cognition without awareness and enhancing precision. By altering perceptions and exploiting decision-making vulnerabilities, it secures strategic advantages.

44. While cognitive warfare alone may not be sufficient to win wars, combined with physical and informational operations – as such AI-driven disinformation – it can lead to dominance over an adversary. Non-combatants, including civilians, are increasingly exposed to the strategies of cognitive warfare, which raises serious concerns about the protection of human rights in this domain. Such tactics could jeopardize human rights, including the right to privacy through data collection and profiling, the right to freedom of opinion and

[43] Matias Leese and others, "Data matters", *Geopolitics*, vol. 27, No. 1 (2022).
[44] See A/HRC/51/17.
[45] Code of Conduct for Law Enforcement Officials.
[46] Jean-Marc Rickli, Federico Mantellassi and Gwyn Glasser, "Peace of mind", Policy Brief No. 9 (Geneva, Geneva Centre for Security Policy, 2023).

expression due to manipulation and disinformation, the right to access truthful information and the right to psychological integrity. Furthermore, targeted cognitive operations risk exacerbating discrimination based on ethnicity, religion, gender or political affiliation, potentially infringing on the right to non-discrimination.

45. The rapid development of AI is profoundly changing information dissemination and making human cognition a key field of military confrontation. Moreover, high-stress virtual-reality simulations are used for combat training, with collected data aiding future preparedness. This highlights the high stakes of cognitive domain competition.[47]

F. Potential convergence of artificial intelligence and biological technologies, including biological weapons

46. AI has become integral to life sciences, enabling breakthroughs in biotechnology that help tackle global issues such as food security and clean water. However, merging AI and biotechnology may pose serious human rights risks, especially through AI-enhanced biological weapons. The development, production, acquisition, transfer, stockpiling and use of biological weapons is prohibited by the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction. This prohibition is comprehensive, regardless of the technologies used, meaning that AI-enhanced biological weapons are also prohibited.

47. The integration of AI with synthetic biology, which involves redesigning organisms for specific purposes, could facilitate creating entirely new organisms with tailored characteristics. This poses the risk of unforeseen and hazardous biological agent development, potentially leading to new forms of biological threats.[48] Furthermore, while AI can facilitate access to information and knowledge dissemination, it can also spread biosecurity risks by allowing for the sharing of sensitive knowledge with misguided or malicious actors.[49]

48. AI-enhanced bioweapons present challenges to the rights to life, integrity, health and a clean, healthy and sustainable environment. Furthermore, they could potentially present biosecurity and biosafety challenges in terms of detection and attribution where they are purposefully designed to evade existing detection systems, making it difficult to identify and respond to an attack by an adversary. In addition, bioweapons might be designed to mimic naturally occurring outbreaks, complicating attribution and efforts to specify their source, thereby inhibiting an appropriate response and potentially also hindering the right to an effective remedy.[50]

49. Addressing these risks requires a multifaceted, human rights-based approach, including enforcing international human rights law, embedding international frameworks such as the Biological Weapons Convention, multilateral cooperation, biosecurity investment and research into defensive technologies.

G. Artificial intelligence and nuclear command and control systems

50. While nuclear-capable States acknowledge, to some extent, the risks of integrating AI into nuclear command and control systems for situational awareness and threat detection, the pursuit of strategic advantage in an evolving nuclear landscape – combined with concerns about falling behind in AI innovation – could lead to the accelerated and premature adoption

[47] See https://www.act.nato.int/activities/cognitive-warfare/.

[48] Anshula Sharma and others, “Next generation agents (synthetic agents)”, in *Handbook on Biological Warfare Preparedness*, S.J.S Flora and Vidhu Pachaur, eds. (London, Elsevier, 2020).

[49] Zhaohui Su and others, “Addressing biodisaster X threats with artificial intelligence and 6G technologies”, *Journal of Medical Internet Research*, vol. 23, No. 5 (May 2021); and Renan Chaves de Lima and others, “Artificial intelligence challenges in the face of biological threats”, *Frontiers in Artificial Intelligence* (May 2024).

[50] Connor O’Brien, Kathleen Varty and Anna Ignaszak, “The electrochemical detection of bioterrorism agents”, *Microsystems and Nanoengineering*, vol. 7, No. 1 (2021).

of these technologies.[51] It is important to distinguish between the use of AI systems for situational awareness and threat detection and its potential use in decision-making processes regarding nuclear weapons. Currently, the use of AI in nuclear command, control and communications systems appears to be primarily focused on early threat detection, intelligence collection and decision-support functions. While there is reportedly an automatic system designed for use in the event of a decapitating strike, this system predates contemporary AI developments. The reliability and implications of AI in these systems are concerning, particularly if future advancements push towards deeper reliance on AI-driven decision-making.[52]

51. Integrating advanced deep learning-based AI presents broader challenges than existing rule-based models. Key concerns include trustworthiness, transparency, vulnerability to adversarial attacks and the misalignment of large-scale models in critical functions, such as nuclear weapons decision-making.[53] Deep learning models are inherently opaque, making their decision-making processes difficult to interpret, which can lead to unpredictable outcomes and undermine human oversight. Moreover, rapid decision cycles allow AI to operate at speeds beyond human capabilities, potentially reducing the time available for nuclear response decisions to a level where effective human control becomes difficult. This raises serious concerns regarding human dignity and human rights, including the right to life, integrity, non-discrimination, health and the right to a healthy environment.

52. Moreover, the risk that AI systems misinterpret benign activities or false alarms as threats could lead to unintended escalation. A further concern is automation bias, where human operators may over-rely on decisions made by AI systems, even where human intuition, training-based awareness or other intelligence otherwise counsels an alternate course of action, leading to potential misjudgments with high-risk outcomes. Malicious information and communications technology (ICT) activity targeting AI-based systems could enable adversaries to infiltrate, disable, manipulate or spoof responses, leading to uncertainty and potential miscalculations or unintended actions.[54] In addition, AI systems necessarily rely on large datasets for training. Adversaries could corrupt these data, leading to flawed decision-making processes, possibly leading to breaches of the human right to non-discrimination.

53. Integrating AI into nuclear command and control systems presents significant risks that must be cautiously managed through a coalescence of risk assessments, technical safeguards, ethical considerations and robust legal frameworks. The momentum of AI development requires initiative and a proactive approach to expedite mechanisms that can ensure that these capabilities are deployed responsibly, safely and in accordance with international human rights law.

H. Directed energy weapons

54. Directed energy weapons encompass systems that emit concentrated energy in a specific direction without using projectiles. In military applications, such weapons rely on electromagnetic or particle technology, rather than kinetic force, to neutralize or destroy targets. These weapons include lasers, microwaves, millimetre waves and particle beams. They can be used for non-lethal purposes such as jamming or dazzling humans or devices and electronic systems.[55] When used for military purposes, directed energy weapons have the capability to damage physical targets over several kilometres with high precision and accuracy.

[51] See https://warontherocks.com/2024/12/beyond-human-in-the-loop-managing-ai-risks-in-nuclear-command-and-control/.

[52] Alice Saltini, “AI and nuclear command, control and communications” (London, European Leadership Network, 2023).

[53] Ibid.

[54] Muhammad Mudassar Yamin and others, “Weaponized AI for cyber-attacks”, *Journal of Information Security and Applications*, No. 57 (March 2021).

[55] Bhaman Zohuri, *Directed Energy Weapons* (Switzerland, Springer, 2016).

55. As directed energy weapon technology advances, weaponized systems are becoming more powerful, widespread and integrated across air, land, sea and space platforms. Their speed-of-light action, precision, scalability, logistical efficiency and low cost per shot offer advantages in both civilian and military applications.[56]

56. In the military context, directed energy weapons can affect civilians. Although there are uncertainties about their complete deployment, recent prototypes and applications indicate progress beyond theoretical stages.[57] Such weapons can cause severe injuries, including blindness and burns. For example, high-energy lasers can burn tissue, while microwave weapons cause severe pain by heating body fluids, potentially resulting in serious, lasting injuries.[58] Given these effects, such weapons and the impact of direct energy deployment raise serious human rights concerns, including to the right to health and bodily integrity and even the right to life and a healthy environment. Significantly, the Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may Be deemed to Be Excessively Injurious or to have Indiscriminate Effects (Protocol IV, entitled Protocol on Blinding Laser Weapons) prohibits the use of laser weapons specifically designed to cause permanent blindness.

III. Role of State and non-State actors in the design, training, deployment, use and acquisition of new and emerging technologies in the military domain

A. State obligations to prevent violations of international law and to regulate and monitor new and emerging technologies in the military domain

57. International legal obligations must be integrated into the design, development and use of new and emerging technologies in the military domain. States are required to ensure that the application of such technologies fully complies with international human rights law, including the rights to life, physical integrity, non-discrimination, privacy and a healthy environment. International humanitarian law obligations are particularly relevant: States must not only "respect" the rules – imposing prohibitions and restrictions on weapons, means and methods of warfare – but also "ensure respect" for international humanitarian law. However, this latter duty remains imprecisely defined, leaving certain aspects subject to interpretation. Furthermore, States must conduct thorough weapons reviews.

58. The duty to "ensure respect" requires States to ensure that international law is implemented and applied at the national level, with due diligence obligations extending to all measures necessary to prevent violations by public and private actors, including developers of new and emerging technologies. The two conditions for responsibility to ensue in the case of due diligence are: (a) had the means to prevent or to repress the breach; and (b) knew or should have known about the risk of violation.[59] This responsibility covers the entire life cycle of new and emerging technologies, ensuring compliance with international law. Furthermore, this assessment must be continuous.

[56] See https://www.nationaldefensemagazine.org/articles/2020/10/13/uptick-in-spending-seen-for-directed-energy-weapons.

[57] See https://article36.org/wp-content/uploads/2019/06/directed-energy-weapons.pdf; and https://nualslawjournal.com/2023/07/25/bringing-directed-energy-weapons-within-the-purview-of-the-arms-control-regime.

[58] Gary M. Vilke and Theodore C. Chan, "Less lethal technology", Policing: An International Journal, vol. 30, No. 3 (2007); and Erdem Eren Demir and others, "The role of non-lethal weapons in public security", *Journal of Criminal Law and Criminology*, vol. 60, No. 3 (July–December 2022).

[59] Antal Berkes, "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, No. 3 (winter 2018).

59. States are obliged to take measures to prevent human rights violations under their jurisdiction.[60] Failure to do so may incur international responsibility. The deployment of new and emerging technologies in the military domain likely imposes additional obligations and higher standards of due diligence to ensure that all feasible precautions are taken.

60. A State can also be responsible for the consequences of private actors' conduct if it fails to take measures necessary to prevent, monitor, regulate, investigate or sanction those outcomes.[61] Therefore, States must comply with obligations of due diligence in the development, acquisition and use of new and emerging technologies in the military domain by non-State actors.

61. The private sector, particularly in AI, may develop technologies adaptable for military use. The urgency to commercialize often leads to underestimating risks, including the misuse of generative AI in malicious ICT operations or disinformation campaigns. Another concern is the uncontrolled proliferation of these technologies, which allows non-State actors to access them. These actors often employ new and emerging technologies in the military domain with fewer safeguards and lower expectations of accuracy or reliability compared with State actors. Non-State actors could also use new and emerging technologies to disrupt or distort communication systems, compromising their accuracy and reliability.

62. The rapid expansion of AI and devices connected to the Internet of things[62] is set to play a key role in future military cyber operations. Exploiting these technologies could introduce or exacerbate vulnerabilities, enabling non-State actors to manipulate AI, compromise Internet of things systems, disrupt essential services such as healthcare, or engage in cybercrime. Such attacks may lead to data breaches, operational failures, physical damage and threats to life and integrity.[63]

63. Given the multifaceted risks of non-State actors acquiring or developing new and emerging technologies in the military domain, States have a critical international legal due diligence obligation to effectively investigate and establish effective remedies for violations of human rights, and sanction actors who violate them. This requires measures such as a robust regulatory framework protecting the rights to life, integrity, non-discrimination, health, a healthy environment and privacy; enhanced monitoring, including strengthened cybersecurity; international cooperation; and comprehensive training for stakeholders on the potential risks and misuse of new and emerging technologies in the military domain. Failure to address these risks could lead to violations of the rights to life, integrity, privacy and non-discrimination.

B. Providers and business of new and emerging technologies in the military domain

64. States are the primary users of new and emerging technologies in national defence and public security. They also promote the development of such technologies by financing research and fostering public-private partnerships. Private entities, including defence contractors and ICT businesses, serve as innovators and developers, providing services such as development, deployment, maintenance and training.

65. At the national level, States act as regulators of new and emerging technologies by establishing legal frameworks and standards for businesses, which must comply with States' obligations under international human rights law. That law imposes binding duties on States to respect, protect and fulfil human rights in relation to new and emerging technologies in the military domain. Moreover, relevant businesses must comply with all legislation and respect human rights, as outlined in the Guiding Principles. This responsibility applies to all

[60] See A/HRC/30/20.

[61] Articles on responsibility of States for internationally wrongful acts.

[62] The Internet of things is a network of interconnected devices sharing real-time data. In the military, it links sensors, vehicles and equipment to enhance surveillance, logistics and decision-making.

[63] Nicholas Tsagourias, "Cyber attacks, self-defence and the problem of attribution", *Journal of Conflict and Security Law*, vol. 17, No. 2 (2012).

businesses, including technology companies, regardless of size or structure.[64] Business enterprises must prevent human rights violations and address any negative impacts. If violations occur, States have a duty to investigate and must ensure that victims have access to effective remedies, including through appropriate judicial or non-judicial means. The Guiding Principles and the Working Group on the issue of human rights and transnational corporations and other business enterprises are key to preventing and mitigating violations. In this sense, the Working Group has noted that arms companies often neglect adequate human rights due diligence, particularly in assessing the risks of their devices used in conflicts.[65] In addition, the B-Tech Project of the Office of the United Nations High Commissioner for Human Rights provides authoritative guidance and resources for implementing the Guiding Principles in the technology space and calls for business enterprises and policymakers to take a human rights-based approach to tackling the challenges of new technologies.[66]

IV. Human rights in the life cycle of new and emerging technologies in the military domain

A. Life cycle perspective

66. New and emerging technologies in the military domain present unique challenges for the protection and promotion of human rights. Many such technologies have a dual-use nature, rendering the situation more complex regarding the allocation of responsibilities between States and private actors. A robust life cycle approach is essential to address these challenges effectively, ensuring human rights are safeguarded from development and training to deployment, operational use and eventual disposal or decommissioning.

1. Embedding human rights in the design and development phases

67. The conceptualization and design phase of new and emerging technologies in the military domain is crucial for embedding human rights considerations from the outset. It involves the initial ideation and development of technology, where the potential human rights impacts should be rigorously evaluated. Technologies are not neutral; they inherently influence policymaking and can restrict individual liberties.[67] As such, both technology itself and its creators can affect human rights, as they often embody specific values and biases.[68]

68. Conducting human rights impact assessments in these early phases is crucial. Assessments should be integrated into the development process to identify and mitigate potential risks to human rights, including the rights to privacy, freedom of expression, life, integrity, health and a healthy environment. While embedding these considerations in the design phase can help developers minimize unintended consequences and misuse, it may not fully resolve the inherent legal tensions posed by certain technologies. Questions remain as to whether technologies such as those used in autonomous weapons systems can ever be fully compatible with human rights standards, especially if their use challenges principles such as the protection of human dignity. Therefore, ensuring compliance with international human rights standards may, in some cases, require broader regulatory frameworks that address the unique legal issues that these technologies raise.

69. The development of new and emerging technologies in the military domain often involves the use of large datasets, which can embed and perpetuate biases. To prevent discrimination, it is essential to implement human rights-based fairness-aware algorithms and counterfactual analysis during the design phase. Developers should consider diversity within

[64] See https://www.ohchr.org/sites/default/files/2021-11/tech-2021-response-export-military-software.pdf.
[65] See https://www.ohchr.org/sites/default/files/2022-08/BHR-Arms-sector-info-note.pdf.
[66] See https://untoday.org/un-b-tech-project/.
[67] A/HRC/47/52, para. 4.
[68] Andrew Feenberg, *Transforming Technology* (Oxford, Oxford University Press, 2002); and Cathy O'Neil, *Weapons of Math Destruction* (New York, Crown, 2016).

their developing teams and conduct diversity audits to reduce the likelihood of biased datasets and programming that exacerbate prejudices.

70. Business enterprises involved in the development of new and emerging technologies have a duty to align their practices with international human rights law, particularly the Guiding Principles. This includes due diligence to ensure that their technologies do not contribute to human rights abuses, in military or civilian contexts. As States have a duty of due diligence, they must regulate these spheres where private actors operate and establish obligations for businesses domestically to comply with human rights.

2. Managing risks during the deployment and operational use phases

71. As new and emerging technologies move into operational use, the potential for human rights violations intensifies. It is vital to establish stringent legal standards that ensure human dignity, meaningful human control, transparency and accountability at all stages of deployment and use, especially in scenarios where automation and AI may lead to a loss of meaningful human control, automation bias or the misuse of technology in ways that violate international law.

72. Verification, testing and evaluation processes should involve diverse groups to address potential biases, considering factors such as age, race and gender. This helps to ensure that new and emerging technologies in the military domain do not further exacerbate negative human rights impacts on vulnerable populations or perpetuate existing inequalities. States should adopt a risk-based regulatory framework, implementing stricter regulations or prohibitions on high-risk technologies that pose significant threats to life, health, personal security and other human rights.

73. Transparency is crucial in the deployment of new and emerging technologies, particularly regarding the data and algorithms used. Due diligence techniques such as bias detection tools or algorithm audits should be employed to identify and address biases in system outputs.

3. Safeguards during disposal, decommissioning and proliferation prevention

74. The final stage in the life cycle of new and emerging technologies in the military domain – disposal or decommissioning – carries its own set of human rights and security considerations. It involves the physical dismantling of technologies, the safe disposal of hazardous materials and the protection of any sensitive data collected during the operational phase. Implementing safeguards to prevent the diversion of materials from stockpiles and the unauthorized sale of surplus equipment is essential to combat proliferation risks. Ensuring that these processes are conducted with transparency and accountability and preventing differentiated impacts on historically marginalized populations, such as Indigenous Peoples and women, is crucial for safeguarding human rights.[69]

75. Considering the rapidly evolving landscape of new and emerging technologies in the military domain, it is imperative to take proactive and comprehensive measures to safeguard human rights. The analysis above underscores the need for a strengthened international legal framework, heightened corporate accountability and robust multilateral cooperation. By establishing rigorous monitoring mechanisms and promoting transparency and legal responsibility, the international community can ensure that the development, deployment and decommissioning of new and emerging technologies in the military domain uphold human rights principles.

[69] See A/75/290.

B. Transparency and accountability

76. The proliferation of new and emerging technologies presents unprecedented legal and regulatory challenges. AI raises concerns about whether existing frameworks are sufficient.[70] Where high human rights risks exist, pressure is mounting to expedite framework revisions and establish new mechanisms for transparency and accountability.[71]

77. New and emerging technologies may enhance performance in complex tasks, acting as force multipliers that improve speed, accuracy and human capabilities.[72] They are increasingly used in intelligence-gathering, surveillance, reconnaissance, military decision-making and tasks such as verification and target selection.[73] However, these systems are often "black boxes", difficult to interpret and even harder to explain. Given the importance of predictability and understandability in AI, ensuring that these systems perform as expected and in an intelligible manner is crucial. Efforts to elucidate the technologies' inner workings are proving increasingly innovative, yielding significant results in advancing transparency. Research to advance explainable AI has grown considerably, achieving successes in making AI more transparent, potentially facilitating its adoption in critical high-risk domains.[74] The intrinsic value of developing explainable AI is to address concerns over insufficient transparency and accountability. However, the risks associated with the implementation of explainable AI, such as privacy breaches and system vulnerabilities due to increased transparency, should not be underestimated.[75]

78. International human rights law requires transparency. In the context of new and emerging technologies in the military domain, this means ensuring access to relevant information on their development, deployment and impacts. Transparency is also essential for aligning their use with international law, safeguarding the rights to freedom of opinion and expression, privacy, non-discrimination and equality.

79. Moreover, a relevant issue in addressing the risks of new and emerging technologies in the military domain is how decision-making capabilities integrated into systems may mirror existing biases and forms of discrimination prevalent in society. One of the main challenges is ensuring that representation gaps in data collection, processing and retention do not perpetuate or exacerbate human rights violations. Addressing these issues requires transparency and strong accountability measures that hold all actors responsible for the ethical and lawful use of new and emerging technologies.

C. Gaps in the current human rights framework

80. New and emerging technologies in the military domain pose challenges to enforcing existing human rights frameworks. While compliance with international law is essential, critical gaps must be addressed to ensure human rights protection in this context. Despite the importance of the Guiding Principles and the work of the OHCHR B-Tech project, there is an absence of international human rights standards that specify in the context of new and emerging technologies in the military domain what existing international human rights law requires from both States and non-State actors. Furthermore, at the national level, new and

[70] Stefan Larsson and Fredrik Heintz, "Transparency in artificial intelligence", *Internet Policy Review*, vol. 9, No. 2 (2020); and Jordan Richard Schoenherr and others, "Designing AI using a human-centered approach", *IEEE Transactions on Technology and Society*, vol. 4, No. 1 (March 2023).

[71] See A/HRC/48/31.

[72] Jonathan Han Chung Kwik and Tom van Engers, "Algorithmic fog of war", *Journal of Future Robot Life*, vol. 2, No. 1 (2021).

[73] Hannah Bryce and Jacob Parakilas, "Conclusions and recommendations", in *Artificial Intelligence and International Affairs: Disruption Anticipated*, M.L. Cummings and others, eds. (London, Chatham House, 2018); and ICRC, "Artificial intelligence and machine learning in armed conflict: a human-centred approach" (Geneva, 2019).

[74] Arthur Holland Michel, "The black box, unlocked" (United Nations Institute for Disarmament Research, 2020); and Arun Das and Paul Rad, "Opportunities and challenges in explainable artificial intelligence (XAI)", *arXiv preprint* (2020).

[75] See https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16-techdispatch-22023-explainable-artificial-intelligence_en.

emerging technologies in the military domain remain largely unregulated, lacking legislative or policy frameworks to guide the industry and developers in the design, development and testing of new and emerging technologies in the military domain, ensuring that clear protective barriers, consistent with international legal obligations, are established.

81. For instance, transparent procurement strategies covering the entire new and emerging technologies in the military domain supply chain and establishing safeguards based on international human rights law are lacking, creating risks of discriminatory uses of certain technologies. Moreover, the absence of international oversight mechanisms for the development, procurement and use of such technologies in the military domain hinders the effective enforcement of international legal obligations, particularly where national regulations are insufficient. While some countries have implemented regulatory frameworks, significant deficiencies remain in national oversight and verification procedures based on the Guiding Principles for private-sector new and emerging technology business enterprises and providers, limiting the ability to ensure compliance with national and international human rights law standards. Addressing these regulatory gaps is crucial to prevent human rights violations and abuses arising from the development and use of new and emerging technologies in the military domain.

82. Another critical gap in the current human rights framework concerns the environmental impact of new and emerging technologies. Their development, training and deployment involve high energy consumption, a significant carbon footprint and intensive use of raw materials such as nickel, cobalt and graphite, leading to long-term environmental consequences.[76] These include water-intensive cooling of data centres and disposal of hazardous waste during decommissioning. Protecting environmental rights remains challenging due to the lack of global legal frameworks and enforcement mechanisms. Transparent information disclosure, robust environmental monitoring and a collaborative accountability framework are essential to safeguarding the human right to a healthy environment.

V. Recommendations

A. States and the international community

83. **States should urgently develop national strategies and policies and regulate the responsible design, development and use of new and emerging technologies in the military domain in accordance with their obligations under international law. This entails creating robust weapon review frameworks that address the unique challenges posed by new and emerging technology-based weapons and establishing effective preventive and accountability mechanisms for their development and deployment. Moreover, institutional mechanisms should be strengthened to anticipate and address potential human rights violations, with a particular focus on enhancing the oversight capacities of local entities, such as national human rights institutions.**

84. **States and international organizations should integrate international human rights law considerations into any multilateral negotiations on new and emerging technologies in the military domain, particularly in Working Group II of the Disarmament Commission, on its recommendations on common understandings related to emerging technologies in international security. Any frameworks developed must address human rights risks, including discriminatory practices, alongside security concerns. Moreover, the international human rights law framework must be included in discussions on autonomous weapons systems, including within the Group of Governmental Experts.**

85. **States should pursue strategic partnerships to address relevant security challenges. Ongoing discussions, best practice exchanges and inclusive frameworks involving States, the private sector, academia and other stakeholders will help ensure**

[76] Wichuta Teeratanabodee, “The environmental impact of military AI”, IDSS Paper No. 039 (S. Rajaratnam School of International Studies, 2022).

stability and mitigate risks. Priority should also be given to sharing legal reviews of new and emerging technologies in the military domain. Moreover, enhancing collaboration between scientific and technical communities, civil society and human rights advocates and practitioners will promote the responsible use of new and emerging technologies in the military domain.

86. **States and international organizations should consider adopting binding or other effective measures to ensure that new and emerging technologies in the military domain whose design, development or use pose significant risks of misuse, abuse or irreversible harm – particularly where such risks may result in human rights violations – are not developed, deployed or used. This includes mass surveillance technologies that infringe on privacy, as well as biotechnologies and neurotechnologies that threaten physical and mental integrity, especially in coercive contexts**

87. **States should categorically ensure that autonomous weapons systems are not developed or deployed unless they operate under meaningful human control. Clear and binding regulations must be adopted to ensure full compliance with international legal standards.**

88. **States should apply due diligence and the precautionary principle by conducting risk assessments and human rights impact assessments across all types of new and emerging technologies in the military domain. Independent bodies, such as national human rights institutions, should lead these assessments to ensure public participation and democratic oversight. The outcomes of these assessments should guide States in adopting measures to prevent harm, suspend high-risk technologies and enforce norms for the responsible military use of new and emerging technologies in the military domain. Collaboration with existing international frameworks – such as those under the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction and the Biological Weapons Convention, which prohibit the development, production, acquisition, stockpiling, transfer or use of biological, toxin and chemical weapons – is essential to strengthen governance and the global response to new and emerging technologies.**

89. **States and international organizations should adopt a collaborative approach to the governance of new and emerging technologies in the military domain, ensuring compliance with international law while addressing disproportionate impacts on less-resourced nations, as inequalities in AI and military technology not only exacerbate existing disparities but also have the potential to drive long-term instability. States in a position to do so – such as developer States – should mitigate harm by sharing knowledge, providing technical assistance and addressing destabilizing effects.**

B. Business enterprises

90. **Business enterprises, especially in the defence and security sectors, should respect human rights under the Guiding Principles by establishing measurable safeguards tailored to specific contexts, eliminating bias and discrimination through human rights impact assessments. These measures should, as far as possible, consider industry secrecy, including business reporting and independent verification, to ensure inclusive and diverse civic participation. Moreover, companies must comply with State-established regulations and further develop and engage human rights risk-based standards, which include transparency requirements, with mechanisms regularly reviewed to ensure effectiveness and alignment with international human rights law.**

91. **Business enterprises must have and implement a human rights due diligence process to identify, prevent, mitigate and account for how new and emerging technologies in the military domain affect human rights, as stated in the Guiding Principles. They must also proactively evaluate such technologies and AI models for risks, including impacts on human rights and international security. If extreme risk testing is restricted by defence classifications, coordination with national authorities before release is essential to ensure compliance with international law.**

C. All stakeholders

92. **All stakeholders, including academia, business, civil society, international organizations and States, should place emphasis on research regarding the human rights implications of new and emerging technologies in the military domain, supporting policies that assess the impacts of disruptive technologies while emphasizing the interdependency, indivisibility and universality of all human rights throughout all development stages.**

93. **All stakeholders must cooperate to ensure the responsible development and deployment of new and emerging technologies in the military domain and to keep the regulation of such technologies aligned with technological advances, fostering international dialogue to develop and enforce legal frameworks that safeguard human rights.**