Λ				
\boldsymbol{H}	/HR	C/56/	CR	P 5

16 April 2024

English only

Human Rights Council Fifty-sixth session

Autonomous weapons systems

Special Rapporteur on extrajudicial, summary or arbitrary executions, Morris Tidball-Binz

Autonomous weapons systems¹

- 1. Following the adoption of the Resolution A/C1/78/L56 by the First Committee of the General Assembly, on "Lethal autonomous weapons systems," and the call to the Secretary General to seek and invite the views from relevant stakeholders, the Special Rapporteur would like to share his contribution elaborating on the key challenges posed by autonomous weapons systems to international human rights law and building on the findings of his predecessors, Phillip Alston and Christof Heyns.
- 2. Among the previously identified challenges are:
 - Threats posed to the right to life² and to human dignity;³
 - Increased difficulty of attributing killing and holding individuals accountable for violations of international law committed with an Autonomous Weapons' System (AWS);⁴
 - Human rights threats associated with AWS proliferation,⁵ including uses of AWS outside of armed conflict, such as policing.⁶
- 3. On this basis, both Special Rapporteurs called, *inter alia*, for the "convening of an expert group to consider robotic technology and compliance with international human rights and humanitarian law." In addition, the call of former Special Rapporteur Heyns, in 2013, for national moratoria on the development and use of AWS "to prevent steps from being taken that may be difficult to reverse later..." was unsuccessful. Instead, States addressed AWS within disarmament fora. In this respect, the Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE on LAWS) has made progress by identifying key issues of dispute, finding positional commonalities, and building greater state understanding of the topic. However, key and serious challenges identified by previous Special Rapporteurs have not been fully addressed and remain unresolved. In the interim, development of AWS technologies accelerated, with some states reportedly seeking to produce AWS at scale in the near future. There are reports of AWS deployment. The international community is crossing a threshold which may be difficult, if not impossible, to reverse later.

¹ The academic assistance of Bernard Duhaime and Leif Monnett in writing this report is acknowledged with gratitude. Background research assistance was also provided by Vincent Roffi, Riddhi Sen Majumder, and Tianxin Zhang of the Graduate Institute of International and Development Studies, and Marjorie Côté-Barton and Fanny Dagenais-Dion of L'Université du Québec à Montréal.

² A/65/321, A/HRC/23/47

https://doi.org/10.1017/CBO9781316597873.001., https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Informal_Meeting_of_Experts_(2016)/heyns%2BCCW%2B2016%2Btalking%2Bpoints.pdf

⁴ A/65/321, paragraphs 33-36.

⁵ A/65/321, paragraphs 43-44.

⁶ https://www.jstor.org/stable/24738054, 362

⁷ A/HRC/23/47, para. 35., A/65/321, para 47

⁸ A/HRC/23/47, para. 111.

⁹ https://www.tandfonline.com/doi/abs/10.1080/09662839.2021.2007476

https://crsreports.congress.gov/product/pdf/IF/IF11294

¹¹ S/2021/229

- 4. In the last two years, there has been a wave of substantive activity by the international community outside the GGE on LAWS. ¹², ¹³, ¹⁴, ¹⁵, ¹⁶, ¹⁷, ¹⁸, ¹⁹ The Special Rapporteur welcomes these initiatives, notably the GA Resolution (A/C1/78/L56), and looks forward to the forthcoming reports by the Secretary General²⁰ and the Human Rights Council Advisory Committee. ²¹ The Special Rapporteur hopes these reports will address the key challenges to international law posed by AWS, including risks to the right to life, human dignity, and accountability, as well as risks to human rights associated with the proliferation of AWS and their potential use outside of war-fighting. He appreciates and fully supports the recommendations on AWS put forth by the International Committee of the Red Cross. ²² It is imperative that the international community build on these recent encouraging and substantive actions with "a sense of urgency": ²³ the window of opportunity to effectively control, and to mitigate adverse effects of, AWS is rapidly closing.
- 5. AWS have been identified as militarily attractive to at least some nations, and may become a "must-have" technology. A Some countries have suggested that AWS may enhance compliance with international law. Mether this outcome is likely has been a topic of contention for some time. It least to far potential benefits, the development, transfer, and increasing use of AWS by multiple actors will lead to two unresolved challenges that are particularly concerning to this mandate: threats to human rights from proliferation, in particular the right to life, and challenges to attribution and accountability.
- 6. This report briefly reiterates human rights concerns associated with AWS raised by Alston and Heyns, discusses challenges posed by proliferation of AWS to human rights, and recommends specific actions that should be taken to mitigate risks to human rights from AWS.

Human Rights

7. Two previous Special Rapporteurs²⁷ described that AWS potentially threatened the right to life,²⁸ "the supreme right,"²⁹ without which no other rights can be enjoyed. In 2013, Special Rapporteur Heyns notably highlighted the severe threats which autonomous killing posed to human dignity, emphasizing that "each use of force…requires that a human being should decide afresh whether to cross that threshold,"³⁰ and that failing to do so reduced

¹² A/HRC/51/L.25

https://estatements.unmeetings.org/estatements/11.0010/20221021/ A1jJ8bNfWGlL/KLw9WYcSnnAm_en.pdf.

¹⁴ https://www.government.nl/latest/news/2023/02/16/reaim-2023-call-to-action.

https://conferenciaawscostarica2023.com/wp-content/uploads/2023/02/EN-Communique-of-La-Ribera-de-Belen-Costa-Rica-February-23-24-2023..pdf.

http://gouvernement.lu/en/actualites/toutes_actualites/communiques/2023/02-fevrier/02-bausch-law-conference.html.

¹⁷ https://www.caricom-aws2023.com/_files/ugd/b69acc_4d08748208734b3ba849a4cb257ae189.pdf.

https://www.icrc.org/en/document/joint-call-un-and-icrc-establish-prohibitions-and-restrictionsautonomous-weapons-systems.

¹⁹ A/C.1/78/L.

²⁰ A/C.1/78/L.56

²¹ A/HRC/51/L.25

²² ICRC, Submission On Autonomous Weapon Systems To The United Nations Secretary-General, link

²³ Secretary-General's remarks to the Security Council on Artificial Intelligence, 18 July 2023, link.

https://direct.mit.edu/isec/article/46/3/7/109668/Prediction-and-Judgment-Why-Artificial

United States, UN Geneva, Digital Recordings of the CCW GGE of LAWS 2022, 2nd session (25-29 July 2022), https://conf.unog.ch/digitalrecordings/,

²⁶ "A further question is whether LARs will be capable of complying with the requirements of IHL..." See A/HRC/23/47, para. 63.

²⁷ A/65/321, pg. 19, para 37, A/HRC/23/47, pg. 6, para 30.

https://www.ohchr.org/en/calls-for-input/general-comment-no-36-article-6-right-life.

²⁹ Ibid

Christof Heyns, "Presentation Made at the Informal Expert Meeting Organized by the State Parties to the Convention on Certain Conventional Weapons," 2014, 9.

humans to objects:³¹ and was therefore a fundamental affront to human dignity. These challenges have received inadequate attention in state discourse: due, at least in part, to the limitations of the GGE on LAWS. While there has been considerable discussion of AWS as "weapons of war,' IHL would never be the sole, and in many instances, it would not be the primary legal frame of reference to assess the legality of their use."³²

8. AWS have also been identified as posing threats to other human rights.³³ For example, the Special Rapporteur on the rights of persons with disabilities identified that AWS may threaten the rights of bodily integrity³⁴ of persons with disabilities. The potential use of AWS for extrajudicial killings of persons in situations of vulnerability³⁵ may threaten a wide range of civil and political rights.³⁶,³⁷,³⁸. These threats may be particularly acute if AWS technologies proliferate, and if AWS are used in non-armed conflict settings.

Proliferation Risks

9. For at least a decade,³⁹ there has been compelling evidence that certain kinds of AWS are at risk of proliferating. Many AWS are composed of dual-use hardware and software technologies: many of which are readily available to non-state actors and states alike.⁴⁰ Compounding this challenge, "many systems originally intended for civilian purposes could easily be modified to serve military functions."⁴¹ It appears increasingly possible to produce AWS which would be efficient at killing, yet which would struggle to comply with international human rights and humanitarian law. Certain widely available dual-use technologies may heighten this concern. Facial recognition technology, which uses widely available "software to identify or verify an individual based on unique facial patterns,"⁴² would facilitate the targeting of specific individuals, and may be of particular concern in enabling AWS use in extrajudicial killings against vulnerable populations. Facial recognition technologies are also inherently prone to error, including bias.⁴³

Switzerland: Meeting of High Contracting Parties to the Convention on Certain Conventional Weapons, 2016)., 2; https://www.jstor.org/stable/24738054, 270

³² https://ssrn.com/abstract=2972071 or http://dx.doi.org/10.2139/ssrn.2972071.

³³ A/HRC/49/52, § 54.

[&]quot;[T]he rights to bodily integrity...include the right to life; the right to security; and the right against cruel, inhuman, or degrading treatment," https://www.jstor.org/stable/24738054

³⁵ "Persons in situations of vulnerability" are those "whose lives have been placed at particular risk because of specific threats or pre-existing patterns of violence." CCPR/C/GC/36, para. 23

³⁶ https://digitallibrary.un.org/record/573104., 7. Alston documented and discussed killings in Sri Lanka.

³⁷ https://www.hrw.org/report/2023/10/10/join-us-or-die/rwandas-extraterritorial-repression., 9

³⁸ https://doi.org/10.2139/ssrn.2972071., 70

³⁹ https://unoda-documents-

library.s3.amazonaws.com/Convention_on_Certain_Conventional_Weapons_-_Informal_Meeting_of_Experts_(2016)/Recommendations_LAWS_2016_AdvancedVersion%2B%284%2Bparas%29%2B.pdf, para. 70

⁴⁰ https://unoda-documents-

 $library.s3.amazonaws.com/Convention_on_Certain_Conventional_Weapons_-\\ Linformal_Meeting_of_Experts_(2016)/ReportLAWS_2016_AdvancedVersion.pdf., 12$

⁴¹ https://unoda-documents-

library.s3.amazonaws.com/Convention_on_Certain_Conventional_Weapons_-_Informal_Meeting_of_Experts_(2016)/ReportLAWS_2016_AdvancedVersion.pdf., 12

⁴² http://ai.stanford.edu/users/sahami/ethicscasestudies/FacialRecognition.pdf.

⁴³ https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf

10. Concerns regarding AWS proliferation have also been evident for at least a decade. 44,45,46,47,48 These concerns include, inter alia, impacts on jus ad bellum and a reduced threshold of engaging in war;49 concerns regarding AWS use in policing and potential violations of a wide range of human rights thereof;50 and fears that AWS might fall into the hands of non-state actors, and their subsequent potential use against "State or other non-State actors, including civilians."51 Threats to human rights posed by the acquisition and use of AWS by "governments and their agents in times of peace as well as armed conflict"52 to conduct extrajudicial killings against a wide range of potential targets should be thoroughly explored and considered.

Attribution and Accountability

- 11. Accountability is a "fundamental" element of international law:⁵³ "international human rights and humanitarian law frameworks are predicated on the fundamental premise that they bind States and individuals, and seek to hold them to account."⁵⁴ States are obligated to investigate and prosecute alleged violations of international law.⁵⁵ Accountability serves both a retributive purpose and to deter violations from reoccurring.⁵⁶ The ability to investigate and hold violators accountable is critical to this Special Rapporteur mandate.
- 12. Challenges to accountability were identified as "[o]ne of the most important issues"⁵⁷ raised by increased autonomy in weapons systems. A predecessor Special Rapporteur concluded that: "If the nature of a weapon renders responsibility for its consequences impossible, its use should be considered unethical and unlawful as an abhorrent weapon."⁵⁸ What human(s) should be held accountable for violations of international law perpetrated by an AWS—has often been identified as an "accountability gap."⁵⁹ In its 2019 Guiding Principles, the GGE on LAWS stated that "Human responsibility for decisions on the use of weapons systems must be retained since accountability cannot be transferred to machines,"⁶⁰ and that AWS should be operated "within a responsible chain of human command and control"⁶¹ to ensure human accountability for their actions. However, there is considerable

⁴⁴ https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014

https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Informal_Meeting_of_Experts_(2016)/2016_LAWS%2BMX_presentations_security_dhanapalanote s.pdf.

⁴⁶ https://unoda-documents-

library.s3.amazonaws.com/Convention_on_Certain_Conventional_Weapons_-_Informal_Meeting_of_Experts_(2016)/2016_LAWS%2BMX_Towardaworkingdefinition_Statement

s_United%2BKindgom.pdf 47 https://unoda-documents-

library.s3.amazonaws.com/Convention_on_Certain_Conventional_Weapons_-

_Informal_Meeting_of_Experts_(2016)/Recommendations_LAWS_2016_AdvancedVersion%2B%284%2Bparas%29%2B.pdf, para. 70

⁴⁸ https://www.ccdcoe.org/uploads/2020/02/UN-191213_CCW-MSP-Final-report-Annex-III_Guiding-Principles-affirmed-by-GGE.pdf.

⁴⁹ https://doi.org/10.4324/9781003172987, 163.

⁵⁰ https://www.jstor.org/stable/.

⁵¹ A/HRC/23/47, para. 98

⁵² A/65/321.

⁵³ A/65/321.

⁵⁴ A/65/321.

⁵⁵ A/RES/60/147, pg. 4

 $^{^{56}\} https://www.hrw.org/report/2014/05/12/shaking-foundations/human-rights-implications-killer-robots.$

⁵⁷ A/65/321, 2010, pg. 17, para. 33

⁵⁸ A/HRC/23/47, 2013, pg. 15, para. 80

⁵⁹ https://doi.org/10.4337/9781802207675.00009, 178.

⁶⁰ https://documents.unoda.org/wp-content/uploads/2020/09/CCW_GGE.1_2019_3_E.pdf

⁶¹ Ibid.

divisiveness in the international community on what form of human involvement in AWS is required. 62

13. Accountability must not only be possible in law, but in practice. AWS proliferation may challenge functional processes of investigating and attributing killings to the responsible party. Investigators must be able to determine if a violation occurred due to human intent, or AWS malfunction.⁶³ The increased spatio-temporal separation from killing which AWS may afford,⁶⁴ the ability to attack targets in communication denied areas, opaque decision-making algorithms,⁶⁵ or AWS which do not retain vital information for reasons of operational security—present serious challenges to the determination of accountability for violations of international law. In 2010, Special Rapporteur Alston wrote "that unmanned systems…leave open the possibility of soldiers pointing to the machine, declaring, '1'm not responsible — the machine is'."⁶⁶ This Special Rapporteur noted that violating states may choose to cloak violations behind a veil of military secrecy regarding AWS use and/or characteristics, hindering attribution and accountability.⁶⁷ Attributing use of AWS may be particularly challenging for states lacking robust digital investigative capabilities and other key stakeholders.

Recommendations

14. The Special Rapporteur welcomes and encourages the GGE on LAWS to continue its valuable work, and urges it to intensify its efforts, including addressing outstanding issues identified in this report. The Special Rapporteur recognizes and supports the involvement of academia and NGOs in development of international policy on the control of AWS. The Special Rapporteur acknowledges, encourages, and supports the important work of the ICRC in this domain. The Special Rapporteur encourages the UN, State authorities, and other relevant entities to implement the following recommendations to address and mitigate risks posed to human rights by the development and deployment of AWS.

(1) The Human Rights Council should:

- (a) Remain fully engaged on the issue of the human rights implications of AWS;
- (b) Urge states to ensure that human rights implications of AWS, with particular emphasis given to the right to life and human dignity, are considered in all international efforts related to control of such weapons, including in upcoming negotiations on control of AWS;
- (c) Facilitate full evaluation and consideration of human rights implications of AWS in international discussions on AWS regulation;
- (d) Evaluate human rights implications of AWS proliferation to both state and non-state actors;
- (e) Ensure that their findings on these topics are readily available to states and other entities to inform negotiations on AWS regulation;
- (f) Provide adequate guidance and instructions to States, so that they comply with their international obligations on the matter;
- (g) Establish a Special Procedure with a mandate to: monitor and report on the development and use of AWS and related military technologies; to evaluate and report on human rights impacts of these technologies; and to recommend actions to mitigate related human rights impacts.

⁶² https://www.sipri.org/sites/default/files/SIPRIYB21c13sII.pdf.

⁶³ https://doi.org/10.1017/9781009090001., 254

⁶⁴ https://doi.org/10.1162/DAED_a_00409.

⁶⁵ https://unidir.org/sites/default/files/2020-09/BlackBoxUnlocked.pdf.

⁶⁶ A/65/321, pg. 18

⁶⁷ See, for example, A/61/311 or A/HRC/14/24/Add.6.

- (2) The international community should identify technical and legal measures to ensure that attribution of, and accountability for, all uses of AWS is possible, and to facilitate the investigation of violations of international law.
- (3) **Monitor AWS Use.** To enable the international community to understand the patterns and severity of use of AWS, systems to detect, report and evaluate the use of AWS should be developed and implemented. To the extent possible, any specific procedures needed to do so AWS use should be integrated into existing monitoring systems. Information that would enable such monitoring needs to be developed. Thus, the international community should:
 - (a) Convene a working group to assess the feasibility of, and technical information needed for, detecting the use by governmental and non-governmental actors of AWS. If detection is feasible, the working group should create and implement a framework for monitoring, evaluation, and reporting of the use of AWS by governmental and non-governmental actors.

(4) Implement specific prohibitions on types of AWS posing particular risks to human rights:

- (a) States and other developers of AWS should commit to a voluntary pledge to refrain from developing, producing, otherwise acquiring, stockpiling or retaining, or transferring, directly or indirectly to anyone, or to use any autonomous weapons system which includes facial recognition technologies.
- (b) To mitigate the potentially severe threats posed by AWS with facial recognition capabilities to "persons in situations of vulnerability whose lives have been placed at particular risk because of specific threats or pre-existing patterns of violence," the Human Rights Council, and parties involved in negotiation of the legally binding instrument to regulate AWS called for by the UN Secretary-General and the President of the ICRC and by the UN Secretary-General's "A New Agenda for Peace," should ensure that the instrument provides that it prohibits in all circumstances the development, production, other acquisition, stockpiling or retention, or transfer, directly or indirectly to anyone, or the use of any autonomous weapon system, that includes facial recognition capabilities.
- (c) In light of the particular challenges which anti-personnel AWS pose to compliance with international law,⁶⁹ consider inclusion of a prohibition on the development, production, acquisition, stockpiling or retention, or transfer, directly or indirectly to anyone, the use, or sale of anti-personnel AWS⁷⁰ in the legally binding instrument to regulate AWS called for by the UN Secretary-General and the President of the ICRC⁷¹ and by the UN Secretary-General's "A New Agenda for Peace."⁷²
- (d) States and other developers of AWS should commit to a voluntary pledge to refrain from developing, producing, otherwise acquiring, stockpiling or retaining, or transferring, directly or indirectly to anyone, or to use any autonomous weapons systems intended for anti-personnel use.
- (5) **Refrain from domestic use of autonomous weapons systems.** Domestic use of AWS by states poses risks to a variety of human rights of the affected populations. It poses challenges to investigation, attribution, and accountability for violations of law, thus

⁶⁸ CCPR/C/GC/36

⁶⁹ ICRC, Submission On Autonomous Weapon Systems To The United Nations Secretary-General, link, 86

⁷⁰ The term "anti-personnel AWS" refers to the definition provided by the ICRC. Ibid., §6

⁷¹ https://www.icrc.org/en/document/joint-call-un-and-icrc-establish-prohibitions-and-restrictions-autonomous-weapons-systems.

https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf., 26. This UN policy document calls for the conclusion, "by 2026, [of] a legally binding instrument to prohibit lethal autonomous weapon systems that function without human control or oversight, and which cannot be used in compliance with international humanitarian law, and to regulate all other types of autonomous weapons systems."

undermining the rule of law at both national and international levels. To uphold the rule of law and to protect and promote human rights:

- (a) States should commit to a voluntary pledge to refrain from the domestic use of AWS, including by both military and non-military state actors.
- (b) The UN Human Rights Council should draft and pass a resolution calling on member states to make such a pledge.
- (6) Take proactive steps to protect vulnerable groups who may become future targets. The Human Rights Council should take proactive steps to protect vulnerable groups from attack by AWS. Such steps should include:
- (a) Convening a working group to identify practical methods⁷³ that can be taken to reduce the threat to vulnerable groups from AWS.
- (b) Developing and disseminating protocols to inform vulnerable groups of AWS use in their region and/or by hostile actors. Specific measures could be added to existing protection protocols.

https://www.state.gov/wp-content/uploads/2024/03/HRD-Guidance_Joint_Updated-_-Accessible-3.12.24.pdf, 6, "Recommendation 7. Provide Safety Tools and Security Education to HRD"