Humanitarian, legal, security, technological, and ethical considerations for autonomous weapons systems

Submitted by Virtual Planet Africa, Women’s International League for Peace and Freedom (WILPF) Zimbabwe, Cultural Youth Movement Education Foundation...

1. This paper contributes to the request for views by Member States set out in Resolution 78/241 adopted by the General Assembly 22 December 2023 that “requests the Secretary-General to seek the views of Member States and observer States on lethal autonomous weapons systems, inter alia, on ways to address the related challenges and concerns they raise from humanitarian, legal, security, technological and ethical perspectives and on the role of humans in the use of force, and to submit a substantive report reflecting the full range of views received with an annex containing these views, to the General Assembly at its seventy-ninth session for further discussion by Member States, and also requests the Secretary-General to invite the views of international and regional organisations, the International Committee of the Red Cross, civil society, the scientific community and industry to include these views in the original language received in the annex of the aforementioned report.”

2. Autonomous weapons systems present risks and concerns to the security of states and communities, particularly in the Global South, including the risks of proliferation, access by non-state actors, algorithmic bias, risks to civilians, unpredictability of systems, lack of traceability, lack of explainability, lowering the threshold of war, breach of sovereignty of vulnerable states by highly militarised developer states, lack of responsibility attribution, human rights challenges, and many others.

3. In light of this, we support the development of a legally-binding instrument (LBI), clearly setting out the widely accepted ‘two-tier approach’ showing which autonomous weapons systems (AWS) are to be prohibited and which are to be regulated.

4. A legally-binding instrument should consider (a) meaningful human control as an integral and intrinsic concept, (b) risk assessment and mitigation, (c) clarification of international humanitarian law (IHL) requirements for AWS, (d) transparency and confidence building measures (TCBM), (e) prohibitions and regulations, (f) regulations on
autonomous arms trade, and (g) consideration of AWS challenges in other international law frameworks.

A. Definition

5. Autonomous weapons systems (AWS) are systems that are capable of, once activated by a human, operating using sensor data to identify, track, select, and engage a target without further human intervention.

We believe that the lack of a single definition should not hamper the development of a legally-binding instrument, given that most proposed definitions agree that the characteristics of autonomy in weapons include minimal or no human input in a system’s decision-making regarding selection, targeting, tracking, and engagement of targets, and that these critical functions are enabled by sensors, artificial intelligence (AI), machine learning (ML), and other emerging technologies.

B. Meaningful Human Control

6. Meaningful human control of systems refers to the making of critical decisions by humans, contextualisation, and rationalisation by a human(s) operator in the application of force. Meaningful human control is an intrinsic value in itself, ensuring that war does not become unpredictable and inhuman. All systems that can make critical decisions on the use of force should be banned.

Meaningful human control entails:

- The making of command decisions by human leaders,
- The making of decisions on targeting, selecting, tracking, and engaging of (human) targets by human decision-makers,
- The ability of humans to change, redirect, and call off attacks by a system,
- A clear framework for the attribution of accountability and responsibility for an attack by an AWS.

C. Risks and Mitigation Measures

7. AWS pose several risks, challenges, and concerns. In line with the provisions of the Convention on Certain Conventional Weapons, AWS that can result in excessive or superfluous injury to civilians and civilian objects should not be developed, distributed, or used. Targeting civilian objects like hospitals, schools, inter alia using AWS should be prohibited.

8. AWS have a high risk of being accessed and used by armed non-state actors. This problem is more defined in the majority of developing states where state institutions may not be robust enough and are susceptible to insurgencies, armed non-state actors, and terrorist activity. A legally-binding instrument on AWS should consider ways of safeguarding developing states, and would ensure that armed non-state
actors do not easily access AWS. This would be done through building a robust framework for the regulation and restriction on the development and trade in AWS.

9. Algorithmic bias is also a major concern for AWS especially for people in the Global South. AWS are only as good as the data used to train them. Given that the development of such systems has so far been predominantly done in the Global North, the risks of cultural, social, and identity bias presented by AWS can have adverse effects. As such, the proposed legally-binding instrument should include clear and strong measures to ensure that algorithmic bias relating to gender, sex, race, ethnicity, age, class, language, location, and other identity categories can be eliminated before a system is deployed. Proper protocols should be put in place for the prosecution and punishment for developers and users of AWS with algorithmic bias and that make mistakes based on algorithmic bias.

10. System failure and possible manipulation by malicious actors is another key concern. Our approach values the control of systems by human operators at all levels in a system’s cycle and machine failure, hacking, or reprogramming by malicious actors can lead to loss of control.

D. International Humanitarian Law

11. The International Court of Justice Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons opined that all types of weapons, whether from the past or in the future, are governed by IHL. Guiding Principle (a) of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems affirmed that IHL “continues to apply fully to all weapons systems, including the potential development and use of lethal autonomous weapons systems.” Although IHL is just a bare minimum requirement, the development, distribution, and use of AWS should ensure that AWS fulfil the ‘cardinal principles’ of IHL;

12. Distinction: AWS should not target civilians and civilian objects. We suggest the expansion of the interpretation of this principle in the context of AWS to prohibit the targeting of human targets by AWS. Only military objects should be targeted and engaged using sensor data.

13. Proportionality: AWS must not cause excessive, superfluous, and unnecessary injury in relation to anticipated military advantage anticipated. To avoid the killing of those deemed as hors de combat by AWS, we suggest that AWS should not be used to target or against humans.

14. Precaution: proper precautions must be made before deployment of AWS to ensure that they do not attack civilians and civilian objects,

---

1 The ICJ advisory opinion on the ‘Legality of the Threat or Use of Nuclear Weapons’ (8 July 1998).
they do not contain algorithmic bias, they will not cause unnecessary damage/injury, and that they will not disregard humanitarian needs in the use of force.

E. Transparency and Confidence Building Measures (TCBM)

15. Transparency and Confidence Building Measures (TCBM) should be put in place to ensure that AWS do not lead to an arms race, unintended conflicts, and misconceptions about AWS. These should include Article 36 reviews of weapons, transparent risk assessments at all levels, information sharing and exchange, internationally agreed review processes and procedures, national obligations for safety and risk mitigation, national and regional ethical standards, periodic reports on military expenditure on AWS for all states, and the creation of an oversight body.

F. Prohibitions and Regulations

16. In line with the ‘two-tier’ approach, the following AWS should be prohibited:
   - Systems that operate without meaningful human control,
   - Systems with unpredictable or unexplainable actions and outcomes,
   - Those that cannot distinguish between civilians, civilian objects, and military objects/targets,
   - Systems that cause unnecessary or superfluous injuries,
   - Any system that cannot fulfil the requirements of international law, especially IHL,
   - Systems that cannot be terminated by a human user once deployed,
   - Systems that contain algorithmic bias and other harmful identity-based risks,
   - Systems that can learn and change decisions or goals after deployment, and
   - Systems that target humans directly without the input of a human operator.

17. The following positive obligations and limits to the development, testing, distribution, and use of AWS should be put in place through regulations:
   - Limits should be put in place on the geographical and mission-based operation of AWS,
   - The types and nature of targets shall be limited,
   - Human supervision must be ensured at all stages of the weapon’s lifecycle,
   - Mandatory obligations for training of personnel shall be put in place before a system is used,
● The duration and scale of AWS operations must not be unlimited,
● Clear chains of command and responsibility shall be outlined,
● Frameworks for the prosecution and punishment of individuals, entities, or states who misuse or develop prohibited systems must be established before systems are deployed,
● Human users must be able to always trace the whereabouts and actions of an AWS, and
● Human users must be able to terminate AWS at any and all times.

G. AWS Trade and Distribution

18. The trade and distribution of AWS must be strictly regulated. In addition to the provisions of the Arms Trade Treaty, clear regulations must be put in place to ensure that AWS do not fall into the wrong hands. With consideration to Africa and the Global South, the distribution of AWS to irresponsible entities, individuals, and state parties poses the greatest threat to peace and security.

19. States and companies that develop AWS should not be allowed to test them in active combat zones in fragile communities. Security assistance for fragile states and states with high levels of insecurity should only be done with AWS whose effects, effectiveness, and efficacy has already been tested elsewhere. States should not use security assistance as an excuse to test AWS. This should be put in place to ensure the safety and dignity of vulnerable communities.

20. Industry developers of AWS must have clear guidelines on the development and distribution obligations they have, including the obligation to vet the state parties they sell to. AWS should be sold only to state parties and reputable registered companies. Rules to prosecute developers who sell to armed non-state actors and terrorist groups shall be put in place.

21. AWS shall be sold only to, and used only in, states with existing national ethical guidelines and standards to govern the development, testing, trade, and use of AWS. These ethical guidelines and standards must be in line with the proposed international legally binding instrument.

H. Other International Law Provisions

22. *International Human Rights Law*: Because AWS can be used in civilian sectors like policing, border control, security, and other sectors that involve the use of force, the development, testing, distribution, and use of AWS must be interpreted and clarified using the provisions of IHRL. Instruments shall be developed to emphasize and mitigate the
possible risks of human rights violations by AWS. Work on this should be guided by the foundation provided by Resolution A/HRC/51/L.25 of the Human Rights Council on the ‘Human rights implications of new and emerging technologies in the military domain’ (2022) and the ongoing work by the UN Human Rights Council.

23. **International Criminal Law:** A robust framework and regime for the prosecution of individuals and developers who violate human rights through AWS should be put in place. The framework should clearly show who is responsible at each stage of an AWS’s cycle and who is responsible when an AWS violates specific rules.

24. **Other Codes of Conduct:** The proposals to develop further codes of conduct and ethical guidelines should be encouraged. These guidelines should be in line with the proposed legally binding instrument.

I. Conclusion

25. Considering the wide-ranging risks and challenges associated with AWS, we welcome the efforts by various actors and states to discuss issues relating to AWS in different forums. This has the potential to result in a robust and effective international law system that governs AWS, leading to lasting customary international law. We are committed to contributing to the further development of the discussions on AWS in the different forums and with the diversity of stakeholders active in this issue.