apils ASIA-PACIFIC INSTITUTE FOR LAW AND SECURITY

Good Practices in the Legal Review of Autonomous Weapon Systems

VERSION 0.4 | 7 AUGUST 2024

Introduction

Purpose

This document contains a set of good practices that may assist States in carrying out legal reviews of autonomous weapon systems ('AWS') in a manner that accounts for their unique characteristics. Adoption of these practices can enhance the efficacy of legal reviews as a mechanism for implementing international legal obligations relevant to AWS. Considering that legal reviews are undertaken at the national level and that States have significant discretion in terms of the conduct of the reviews, some or all of these practices could be independently adopted by States, or agreed as representing good practice with other States.

These good practices do not aim to offer an interpretation of existing legal obligations. Indeed, the obligations of States differ when it comes to legal reviews: in particular, not all States are party to Additional Protocol I to the Geneva Conventions ('AP I'), Article 36 of which creates a binding obligation to conduct a legal review of weapon systems, including AWS. The practices included in this document could be relevant to all States reviewing AWS, irrespective of whether they have an obligation under international law to do so, and what the scope of that obligation might be. That said, some States may view some of these good practices as flowing from their international legal obligations.

The articulation of these good practices is without prejudice to efforts aimed at clarifying or further developing the current normative framework with respect to the development and use of AWS. This document seeks to support States in operationalising the Guiding Principles developed and affirmed by the Group of Governmental Experts on Lethal Autonomous Weapon Systems ('GGE')[1] and en-

[1] *Report of the 2018 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems* (23 October 2018) CCW/GGE.1/2018/3, para 21; *Report of the 2019 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems* (25 September 2019) CCW/GGE.1/2019/3, Annex IV.

dorsed by the Meeting of the High Contracting Parties to the Convention on Certain Conventional Weapons.[2] These good practices relate specifically to Guiding Principle (e), which stipulates that '[i]n accordance with States' obligations under international law, in the study, development, acquisition, or adoption of a new weapon, means or method of warfare, determination must be made whether its employment would, in some or all circumstances, be prohibited by international law'.[3] These good practices are also in line with the most recent report of the GGE, which reaffirmed Guiding Principle (e) in its conclusions and encouraged the voluntary exchange of relevant best practices between States.[4]

Genesis and current status

Work on these good practices began with a comprehensive review of submissions by States and other participants in the GGE. This exercise resulted in a report that collated these statements– first published in March 2023[5] and reissued with updates in May 2023.[6] This report extrapolated from the statements an initial list of propositions about legal reviews of AWS.

This list of propositions was presented and discussed during an Expert Meeting on the Legal Review of AWS in Sydney in March 2023. Following this meeting, a working group composed of Netta Goussac, Natalia Jevglevskaja, Rain Liivoja and Lauren Sanders – with additional input from Damian Copeland – revised the list into a structured set of Elements of Possible Good Practices in the Legal Review of Autonomous Weapon Systems. These elements were, after a round of written feedback from participants of the 2023 Sydney Meeting, refined further and annexed to the report of the meeting.[7]

Subsequently, the working group, having been joined by Renato Wolf, made minor textual changes to some elements and proposed two further elements (1bis and 7bis). This revised set of good practices was presented and discussed during the Second Expert Meeting on the Legal Review of AWS in Sydney in April 2024.

This document remains a draft and is subject to further revision. Suggestions and comments are welcome, and may be sent to **info@apils.org**.

Terminology

There is no internationally agreed definition of the term 'autonomous weapon system'. In these good practices, the term refers broadly to any weapon system that, once activated, can select and engage targets without further intervention by an operator. Thus, for the purposes of these good practices, AWS include systems with varying degrees of autonomy. These practices are not intended to be limited to 'lethal autonomous weapon systems' ('LAWS'), a concept used by the GGE.

All AWS, whether capable of lethal effects or not, can create challenges for legal review. In addition, the lack of a lethal effect does not absolve States of their obligations to use capabilities consistently with international law, or of any legal

[2] *Final Report of the 2019 Meeting of the High Contracting Parties 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* (13 December 2019) CCW/MSP/2019/9, para 31 and Annex III.

[3] *2018 GGE Report* (n 1) para 21(d); *2019 GGE Report* (n 1) Annex IV, para (e); *2019 MHCP Report* (n 2) Annex III, para (e).

[4] *Report of the 2023 Session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems* (24 May 2023) UN Doc CCW/GGE.1/2023/2, para 23.

[5] Rosie Cavdarski, Lauren Sanders, and Rain Liivoja, *Weapons Reviews of Autonomous Weapon Systems: Report on Submissions to the GGE on LAWS* (Version 1.0, University of Queensland, 2023) doi: 10.14264/6670709.

[6] Rosie Cavdarski, Lauren Sanders, and Rain Liivoja, *Legal Reviews of Autonomous Weapon Systems: Report on Submissions to the GGE on LAWS* (Version 2.0, University of Queensland, 2023) doi: 10.14264/1c0275b.

[7] Netta Goussac, Natalia Jevglevskaja, Rain Liivoja and Lauren Sanders, *Enhancing the Legal Review of Autonomous Weapon Systems: Report of an Expert Meeting* (University of Queensland, 2023) doi: 10.14264/2bbfd31.

obligation to conduct a pre-emptively review. Thus, lethality is a characteristic not separately addressed in these good practices.

The reference to 'weapon systems' indicates that the focus is broader than just the weapon itself (such as a munition). The 'system' includes other hardware (eg, sensors and platforms) and software necessary for the operation of the weapon. Importantly, autonomous targeting capability may be enabled at a system-of-systems level rather than through the interaction of subsystems of single weapon systems or platforms. There is no consensus as to what equipment might be captured by the term 'system' or the related international law term 'means of warfare'.

These good practices refer to the pre-emptive assessment of weapons, means and methods of warfare for compliance with international law as 'legal review'. This term is preferred over the notion of 'Article 36 review' because it covers review processes undertaken without any obligation under AP I. Also, 'legal review' is preferable to 'weapons review' as the purpose of the review is to assess legal compliance; where non-legal considerations are included in the review, they play a secondary role.

Good Practices

Scope of the legal review

1. A State could conduct a legal review, including the review of an AWS, as a result of the State's:

a. specific obligation under international law to undertake the review;
b. interpretation of its general obligations to implement international humanitarian law ('IHL'); and/or
c. national law or policy.

1bis. A State should codify its process for legal reviews of AWS in an appropriate document. The review process should be assessed periodically in light of legal and technological changes, and updated as required.

2. The legal review should identify and assess issues of international law compliance specific to AWS.

3. The legal review should assess whether the AWS can be used in compliance with the reviewing State's applicable international legal obligations. In addition to IHL, these legal obligations may arise from, for example, arms control and disarmament law, international human rights law, international environmental law, law of the sea, space law and jus contra bellum.

4. The legal review of an AWS could assess the ability of the AWS to be used in compliance with rules relating to the conduct of hostilities. This may require considering each anticipated method of use of the AWS.

5. States could articulate criteria for determining which capabilities and systems, including those with autonomous functions, amount to weapons, means or methods of warfare and therefore should be the subject of a legal review.

Conducting a legal review

Relevant considerations

6. A legal review of an AWS could assess the human-machine interaction to determine whether humans will be able to fulfil their obligations under international law in the use of AWS.

7. A legal review of an AWS could assess if, where and how its use would transfer responsibility for acts necessary for complying with international law from one human to another human, and whether such a transfer would be consistent with international law.

7bis. A legal review of an AWS should assess whether physical and cybersecurity controls of the system are adequate to ensure the integrity of the system.

8. A legal review of an AWS could include a reflection upon additional considerations that the State deems relevant to its use, such as:

a. policy constraints;
b. domestic law;
c. security and proliferation risk;
d. ethical and societal implications;
e. possible future development of the law.

9. Where a legal review addresses issues not based on an international law obligation, the review could make that explicit.

10. A legal review could conclude that the capability's normal or anticipated use is:

a. lawful; or
b. lawful under certain circumstances or subject to certain conditions; or
c. unlawful.

11. With respect to the study, development, acquisition and use of AWS, the conditions imposed as a result of the legal review could relate to, for example:

a. the characteristics of a system under development;
b. the operating environment;
c. the approved use case(s) (such as use in a certain type of armed conflict, a particular domain of warfare, or against particular types of targets);
d. the approved methods of use;
e. degree and type of human–machine interaction;
f. the system(s) within which the capability may be integrated.

Modifications

12. States could articulate what kind of changes would cause the legal review to become inadequate, so as to require a reconsideration of the existing legal review, including:

a. changes to the applicable law;
b. modifications to a capability or its normal or expected use, following its introduction to service.

13. With respect to AWS, such modifications could include changes to:

a. the nature and extent of human–machine interaction;
b. system algorithms and datasets;
c. intended mission sets;
d. intended operational environments;
e. intended target sets;
f. expected adversarial countermeasures.

14. States could identify parameters, limits, appropriate safeguards or risk-mitigation measures with respect to the use of technological processes (such as artificial intelligence techniques) that result in modifications.

Legal review process

Timing

15. States could commence legal reviews of AWS as early as feasible in the study, development and acquisition processes. States could reconsider legal reviews as often as necessary.

Relationship to other national practices

16. States could articulate how legal reviews are integrated into their broader weapons design and development processes.

17. States could communicate the outcomes of legal reviews to those involved in the review process, as well as operational legal advisers and commanders. This could be facilitated by establishing an appropriately controlled national repository to ensure previous legal reviews can easily be found and accessed.

18. States could articulate how legal reviews interact with other policy, administrative and technical frameworks, including control and risk-mitigation measures, in the broader weapons acquisition and use processes.

Participants

19. States could determine the required qualifications of legal reviewers.

20. States could articulate how and by whom legal reviews, including reviews of an AWS or modifications of an AWS, are authorised.

21. States could specify the national authorities for approving modifications of AWS and the legal advice required.

22. States could articulate ways to ensure that the legal review takes a multidisciplinary approach capable of properly assessing functions of the AWS that may affect the user's ability to comply with IHL.

Testing, evaluation, verification and validation

23. States could articulate the requirements for reliable and independent testing, evaluation, verification and validation ('TEVV') of AWS to inform the legal review. States could identify and require the use of:

a. specific TEVV procedures, methods, environments and protocols;
b. specific standards or models of performance, including in relation to reliability and predictability.

24. States could independently evaluate:

a. algorithms and training data sets;
b. context or use-cases for an AWS.

25. States could articulate what information they require to undertake such evaluations.

26. States could specify the extent to which TEVV of an AWS may be automated.

Sharing information about legal reviews

27. An exchange of information pertaining to legal review processes could occur as a result of States':

a. obligations under international law to communicate to each other information about laws and regulations giving effect to IHL;
b. decision to engage, on a voluntary basis, in a broader exchange of information and good practices.

28. An exchange of information pertaining to legal review processes could improve their effectiveness. In relation to AWS, such an exchange could include information about:

a. if and how the legal review of an AWS differs from a legal review process of a capability that is not an AWS;
b. what challenges have arisen in conducting legal reviews of AWS;

c. what novel legal issues have required consideration during the legal review of an AWS.

29. States could establish, and contribute to, a repository for information about processes and practices of legal reviews.

30. Having due regard to national security requirements and the protection of proprietary information, States could also add to the repository select information relating to specific legal reviews of particular AWS. This could include outlining the general type of AWS capabilities, functionality or use contexts that a State considers to be consistent or inconsistent with its obligations under international law.