# AIDP Resolutions
# Opatija, Croatia, 7-8 December 2023

# International Perspectives on AI: Challenges for Judicial Cooperation and International Humanitarian/Criminal Law" (Section IV)

**Preamble**

*Considering* that the artificial intelligence (AI) is an integral part of the Autonomous Weapons Systems (AWS) decision-making process, and such weapons have already reached a significant level of development in this third decade of the 21st century and that they are already widely used by many states and non-state actors.

*Considering* that multiple surveillance and targeting decisions traditionally adopted or informed by humans are beginning to be automated through the use of AWS, causing significant legal, moral, and ethical considerations;

*Highlighting* the growing concern about the harmfulness of malicious or negligent uses of AWS;

*Acknowledging* the need to analyze whether the legal response of states and the international community to the challenges of AI is sufficient or whether it needs to be reformed and adapted, either through specific modifications or through the creation of new forms of criminalization;

*Acknowledging* the need for AWS to be designed and developed in compliance with the international law.

**********

*Noting* that AWS can be defined as "[a]ny weapon system with autonomy in its critical functions—that is, a weapon system that can select (search for, detect, identify, track or select) and attack (use force against, neutralize, damage or destroy) targets without human intervention;"[1]

*Noting* however that this definition of AWS is not universally accepted, and that different international, regional and national regimes may choose to adopt different understandings of the definition of AWS and of meaningful human control in their use ("human on the loop");

[1] ICRC, *Views of the ICRC on autonomous weapon systems*, paper submitted to the Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), 11 April 2016, https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system

**********

*Noting* that different international, regional and national regimes may also choose to distinguish between AWS and Lethal Autonomous Weapons Systems, and also between AWS and Automated Weapons Systems;

*Considering* that the use of AWSs may cause significant harm to humans and societies, and that such use raises legal and ethical implications related to both *ius ad bellum* and *ius in bello*, serious human rights violations, *ius cogens* violations and core international crimes;

*Considering* that the use of AWSs can influence public opinion and policy in favor of the use of force, because of the perception that the use of AWSs minimizes risks of destruction, death or bodily injury to soldiers and other individuals involved;

*Considering* that the use of AWSs can negatively affect the respect of fundamental principles of *ius in bello*, such as the principles of distinction, proportionality and precaution(s);

*Considering* that by removing or reducing the human element in the decision making, the use of AWSs can contribute to the increase in the number of deaths because of the absence of human feelings, such as fear and compassion, which may play a role in reducing the number of deaths;

*Considering* that the use of AWSs may cause significant destruction and collateral damage;

*Considering* that core international crimes can be committed through the use of AWSs and that such use of AWSs may raises serious and new issues related to the attribution of criminal responsibility questions, including, but not limited to issues related to command responsibility.

**********

*Considering* that the use of AWSs can raise jurisdictional issues, because AWSs use may be trans-territorial;

*Finding* that an international regulatory approach to AWSs is necessary and should include a legally binding norm prohibiting the design, development, production and use of fully AWSs (without meaningful human control);

*Encouraging* all states to open official negotiations within the United Nations (under the auspices of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons and/or within other appropriate United Nations conventions, bodies, agencies, and institutions) with the goal of developing regulations or other guidelines which will apply to the design, development, production and use of AWS.

*Finding* that this also enhances the need toward a global approach to AWSs.

**********

**Aware of**:

United Nations, *Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS);*[2]

United Nations, 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 as amended on 21 December 2001;[3]

European Parliament Resolution of 12 September 2018 on autonomous weapon systems;[4]

Latin American and the Caribbean Conference of Social and Humanitarian Impact of Autonomous Weapons, Communique of the Latin American and The Caribbean Conference of Social and Humanitarian Impact of Autonomous Weapons, 23 and 24 February, 2023;

International Committee of the Red Cross Report, *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, Geneva, September 2016;[5]

International Committee of the Red Cross, *Statement to the Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS),* 13-17 April 2015, Geneva;[6]

XXth AIDP Congress, Criminal Justice and Corporate Business, Rome, 13-16 November 2019.[7]

## Resolutions

1) In order to prevent and reduce AWS-related harms, it is necessary for international, regional, national legislators and other competent authorities to fully define AWS, as well as to develop regulations governing design, development, production and use of AWS.

2) Use of AWS must be regulated in advance by a law or a norm of equivalent binding force.[8]

---

[2] https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-_Informal_Meeting_of_Experts_(2016)/ReportLAWS_2016_AdvancedVersion.pdf.
[3] https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/#:~:text=It%20was%20adopted%20on%2010,or%20to%20affect%20civilians%20indiscriminately.
[4] https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html.
[5] ICRC, *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons*, ICRC, Geneva, September 2016, https://www.icrc.org/en/publication/4283-autonomous-weapons-systems
[6] ICRC (2015) *Statement to the Convention on Certain Conventional Weapons (CCW) Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), 13-17 April 2015, Geneva*, https://www.icrc.org/en/document/lethal-autonomous-weapons-systems- LAWS
[7] https://www.penal.org/fr/aidp-xx-international-congress-penal-law-%E2%80%9Ccriminal-justice-and-corporate-business%E2%80%9D-rome-13-16-0.
[8] Article 36 of Additional Protocol I to the Geneva Conventions already requires member states to continue to assess whether the development or use of any new weapons would be prohibited by the Additional Protocol or by any other rule of international law. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Article 36,

3) States are urged to be more transparent about their use of AWS.

4) States must ensure that decisions taken by authorities to use AWS are based on transparent criteria that are subject to public scrutiny. States that use AWS must choose systems the functioning of which is fully transparent, explainable and traceable (white box AI).

5) Law or other equivalent norms related to the use of AWS must require that such systems have a high degree of technological reliability. A sufficiently precise regulation requiring appropriate evaluations and validations, independent of the AWS developer, must limit to the greatest possible extent the risk of bias or any form of discrimination in machine learning, coding errors, and other technological malfunction.

6) Laws or equivalent norms must require that before an AWS based on self-learning algorithms may be used in surveillance, selection of targets or any other purpose, the algorithms must be developed, trained, tested and used under human supervision (human-in-the-loop principle). These laws and equivalent norms must require a human evaluation before any action is taken to use an AWS.

7) States and law enforcement authorities must ensure that their personnel who operate AWS receive appropriate training in the proper use of the relevant AWS, as well as training with respect to the risk of error and bias. They must ensure that such personnel have a thorough knowledge of the dangers that AWS may pose to human rights.

8) Laws or equivalent norms must explicitly provide that where there is a human rights violation occurring as a result of any malfunction of an AWS, the company that designed or manufactured the system will incur criminal liability for fault or negligence[9] without excluding civil liability for defective products. Such laws or equivalent norms must also provide that investigations must be carried out to determine the cause of the violation.

9) Every state choosing to use AWS must have adequate penal laws in place, which must provide that individuals who use AWS in a manner inconsistent with relevant international and national legal standards will incur individual criminal responsibility before competent penal jurisdictions.[10]

10) States and regional and international human rights bodies must ensure that the use of AWS does not lead to serious human rights violations, ius cogens violations or other violations of relevant international law and international humanitarian law norms.

---

https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and.

[9] AIDP XXI Congress: Artificial Intelligence and Criminal Justice, Section I: Traditional Criminal Law Categories and AI, Resolutions, approved by the Colloquium of Siracusa, 15-17 September 2022; AIDP XXI Congress: Artificial Intelligence and Criminal Justice, Section II: Penal Law and Criminalization in the Face of the Challenges of AI, Resolutions, approved by the Colloquium of Bucharest, 16-16 June 2023.

[10] AIDP XXI Congress: Artificial Intelligence and Criminal Justice, Section I: Traditional Criminal Law Categories and AI, Resolutions, approved by the Colloquium of Siracusa, 15-17 September 2022.

11) States must ensure that they have fully implemented their international law-based legal obligations into their respective national legal orders, through laws, regulations, executive orders, military codes, or other types of binding domestic legal norms. Such domestic legislation must provide for different modes of liability, including, but not limited to, command responsibility.

12) States should establish independent research bodies to study, on a continuous basis, whether the use of AWS is being conducted in a manner consistent with all applicable international and national law norms and regulations.

13) It is necessary to identify and define specific modes for attributing criminal responsibility to the persons (both natural and legal persons) who are responsible for the development of AWS.[11] Such responsibility should not exclude persons, either natural or legal, who contribute to the causal chain of harm: from the designer, programmer, producer, seller, distributor to the end -users of the systems themselves.

14) States should strive to foster cooperation between policy and academic experts on the subject of international law and members of the military, law enforcement or intelligence forces who are tasked with developing and/or deploying AWS. Such cooperation should be conducted with the goal of ensuring that the use of AWS is always consistent with relevant international law norms, as well as with applicable domestic laws and regulations.

15) States must provide for extraterritorial application of their domestic laws in instances where AWSs are deployed or otherwise utilized abroad by states or by entities under state control.

16) States must develop appropriate conflict of law and conflict of jurisdictions laws which allow for the application of domestic law in instances where AWS are deployed or otherwise utilized abroad. Such laws may be developed at the domestic, regional and/or international level. Such laws must allow for the imposition of criminal responsibility (as well as civil liability) against those natural or legal persons within the relevant states control who are responsible for the misuse or malfunctioning of the AWS located outside the territory of the relevant state.

17) States must develop models of judicial cooperation in criminal matters, especially in order to collect evidence related to AWS-caused offenses. Such models of judicial cooperation may be particularly necessary for states which have not already concluded appropriate bilateral, regional, or international agreements on this subject.

18) States must ensure that they have extradition mechanisms in place in order to effectively prosecute and punish those responsible for AWS-caused offences.

[11] AIDP XXI Congress: Artificial Intelligence and Criminal Justice, Section I: Traditional Criminal Law Categories and AI, Resolutions, approved by the Colloquium of Siracusa, 15-17 September 2022.