

Photo: Mike Marreen, Unsplash

FREQUENTLY ASKED QUESTIONS

AUTONOMOUS WEAPON SYSTEMS AND HUMAN RIGHTS

WHAT ARE AUTONOMOUS WEAPON SYSTEMS?

There is no internationally agreed definition of Autonomous Weapon Systems (AWS). However, some actors, including the ICRC, define them as weapon systems that, once activated, can identify, select and engage targets without further human intervention. This characterization is technology-neutral, focusing on the absence of human judgement and control during the critical functions of target selection and force application.

WHAT ARE ANTI-PERSONNEL AUTONOMOUS WEAPON SYSTEMS?

A subset of AWS are anti-personnel autonomous weapon systems. These are:

- Triggered by the presence, proximity, or contact of a person; or
- Programmed to engage targets that are human beings, without the user knowing either who or where those individuals are and when they will be targeted.

WHAT IS THE LINK BETWEEN AI AND AWS?

While AI is not strictly required for AWS, AI often increases the autonomy of such weapon systems. AI enhanced systems can process quantities of data and generate recommendations, compressing decision-making by increasing its speed and scale.

This can significantly reduce the time available for the assessment of the legality of the use of force, verification, contextual judgement and the exercise of precautions. Even when weapons systems are less than fully autonomous, the integration or reliance on AI in weapon systems raises serious legal concerns, including under international human rights law (IHRL), which have not yet been adequately addressed in intergovernmental discussions.

WHY IS INTERNATIONAL HUMAN RIGHTS LAW RELEVANT TO AWS?

> ***Having a machine deciding whether you live or die is the ultimate indignity.***
>
> Christof Heyns, former Special Rapporteur for Extrajudicial, Summary or Arbitrary Executions

The use of AWS raises fundamental questions regarding human dignity. The use of AWS has direct implications for the rights to life, the right to security of persons, the prohibition of torture and other forms of cruel, inhuman or degrading treatment, dignity, non-discrimination and accountability, among other human rights and principles.

International human rights law applies at all times, including during armed conflict, and is the key international legal framework governing law enforcement, as well as other areas. IHRL is therefore central to assessing the legality of AWS in general and in specific contexts, particularly when the weapon or technology could be used in policing, border control, counter-terrorism, or assembly management.

Weapons developed for the military must only be developed, acquired and deployed where they are capable of being used in accordance with applicable international law, including international humanitarian law (IHL) and IHRL. In law enforcement contexts, the use of AWS that are capable of deploying lethal or less-lethal force, such as through the release of tear gas, rubber bullets, electric shocks, small explosives, or live ammunition against people, raises serious human rights concerns.

WHAT ARE STATES' OBLIGATIONS UNDER IHRL IN RELATION TO AWS?

Under international human rights law, States have obligations to respect, protect and fulfil human rights, including by exercising due diligence to prevent or mitigate foreseeable human rights violations where they know or ought to have known of a real risk of human rights harm.

- The **obligation to respect** requires States, when developing, procuring, selling, regulating or deploying AWS, to refrain from conduct that directly infringes human rights and proactively assess and address risks associated with the use of such systems.

- The **obligation to protect** requires States to regulate and oversee private actors involved in the design, development, sale and deployment of AWS where such activities pose foreseeable risks to human rights. Where preventive or mitigating measures are insufficient to address serious or irreversible harms, due diligence may require States to prohibit particular uses or types of weapons altogether.

- The **obligation to fulfill** requires States to adopt positive measures to ensure effective oversight, contestability and human review of automated decision-making.

HOW DOES INTERNATIONAL HUMAN RIGHTS LAW APPLY TO THE USE OF AWS IN LAW ENFORCEMENT SITUATIONS?

The use of force in law enforcement must conform to the strict requirements of:

Legality	Must have a lawful basis.
Necessity	Must be strictly required to achieve a legitimate purpose.
Proportionality	The force must be appropriate and not excessive.
Precaution	Measures must be taken to minimize harm.

AWS lack the capacity to make the real-time, context-specific assessments required to comply with the principles of legality, necessity, proportionality and precaution under IHRL. The lawful use of force demands continuous assessment of the situation, evaluation of intent and mental health of the person subject to the use of force, consideration of non-violent alternatives, and a graduated, proportionate response. These decisions require human judgement, especially in complex, dynamic environments, that AWS cannot replicate. Accordingly, the deployment of AWS against people risks rendering the use of force unlawful under IHRL as it fundamentally contradicts the principle that force must be used only as a last resort and in a situationally adaptive manner, a determination that requires human judgement.

The use of AWS against people therefore raises **serious concerns about arbitrary deprivation of life**.

HOW DO AWS IMPEDE THE RIGHT TO PEACEFUL ASSEMBLY?

The use of AWS in assemblies, including in the form of less-lethal weapons, where environments are fluid and rapidly evolving, can pose a direct threat to the right to freedom of peaceful assembly. States have positive obligations to facilitate peaceful assemblies by promoting an enabling environment and establishing a legal and institutional framework that ensures the right can be exercised effectively and without discrimination.

Real-time human judgment is critical for lawful policing during protests or gatherings, and law enforcement officials must exhaust non-violent means and apply force only as a last resort. The mere threat of use of AWS in peaceful assemblies may have a chilling effect on the exercise by people of this right.

WHAT RISKS DO AWS POSE TO EQUALITY AND THE RIGHT TO NON-DISCRIMINATION?

The reliance by AWS on broad data sets that incorporate bias and include personal data, such as data related to racial or ethnic origins, political opinions, gender, or religious beliefs, raises concerns that are common across AI systems and exposes individuals to serious risks of discrimination, particularly in surveillance and law enforcement contexts. Use of AI within AWS can replicate and amplify societal biases. Facial recognition and target profiling may lead to racial profiling, over-policing of marginalized groups, misidentification, or disproportionate targeting based on ethnicity, gender, or disability, with potentially severe consequences when such outputs inform decisions regarding the use of force.

WHAT RISKS DO AWS RAISE FOR ENSURING ACCOUNTABILITY FOR HUMAN RIGHTS VIOLATIONS AND OTHER HARMS?

Accountability is a cornerstone of international human rights law and international humanitarian law, requiring States to investigate alleged violations and ensure effective remedies for victims. The use of AWS complicates attribution of responsibility for human rights violations, as the temporal and spatial distance between human actors and the effects of AWS can obscure who is responsible for a specific act.

The involvement of multiple actors, such as developers, manufacturers, and operators, further complicates the process of attributing responsibility, in particular in assigning individual criminal responsibility for violations related to the development, deployment and use of AWS. Ensuring human control and judgement over weapons systems is therefore essential to ensure accountability for the weapons' use.

DO BUSINESS ENTERPRISES HAVE HUMAN RIGHTS RESPONSIBILITIES IN RELATION TO AWS?

Yes, they certainly do. Business enterprises are designing and developing AWS. The UN Guiding Principles on Business and Human Rights (UNGPs) provide the international legal framework for responsible business conduct by States and companies, including in relation to the development and use of AWS.

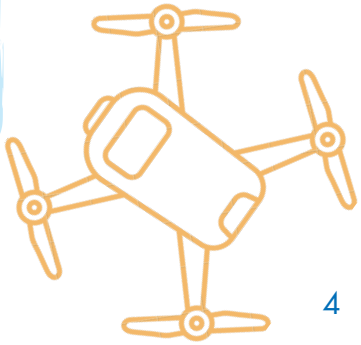
In line with the UNGPs, business enterprises should conduct human rights due diligence throughout the lifecycle of their development of AWS. This includes identifying, preventing, and mitigating adverse human rights impacts. Particular attention is needed where AWS may be exported, deployed in conflict-affected areas, or used by private security actors, given the heightened risk of serious harm and the potential for accountability gaps.

WHY ARE THESE RISKS SO PRESSING?

There is a substantial risk that use of AWS will grow in the coming months and years, before these risks to human rights are addressed.

The relatively low cost, scalability, and accessibility of some AWS increases the likelihood of widespread development and use, not only in the conduct of hostilities but also in law enforcement settings. The threats to human rights are significant in both scenarios.

In addition, the question is not if, but when, non-state armed groups or criminal actors will acquire and deploy low-cost, small-scale AWS, exacerbating risks of harm to human rights and increasing the challenges of ensuring that decisions involving the use of force remain subject to human judgement.



RECOMMENDATIONS ON AWS TO STATES AND THE PRIVATE SECTOR

Prohibitions

- **Prohibit the development, acquisition, transfer and use of AWS** whose functioning or effects cannot be understood, predicted, explained by human users and controlled and limited to ensure compliance with international law.
- **Prohibit the use of AWS against humans** as well as the development of AWS specifically designed to target humans.

Restrictions and safeguards

- **In the conduct of hostilities**, any AWS not otherwise prohibited should be subject to strict operational limits to ensure compliance with international law, including IHL and IHRL. This includes clear limits on the types of targets, the time and area of operation, the scale of possible engagements and the circumstances in which the system may be used, while preserving context-specific human assessment and judgement and the ability to suspend or stop the system in time to prevent harm.
- **In law enforcement contexts, including border control**, any AWS not otherwise prohibited, capable of deploying force, lethal or less-lethal, must not be used. Such systems are unlikely to meet the IHRL standards on the use of force, which require real-time, context-specific human assessment and judgement.

Accountability and non-discrimination

- **Ensure** that the responsibility for decisions related to AWS are clearly and coherently assigned and that a person can be held accountable for any violations, including through individual criminal liability.

In cases in which States nevertheless use AWS, they should strictly ensure that they:

- **Refrain** from any use of AWS based on data that could lead to discrimination.
- **Refrain** from the use of AWS relying on facial recognition technologies, which are prone to error and bias.

Human rights due diligence and impact assessment

- **Conduct** legal reviews, including where applicable under Article 36 of Additional Protocol I, of any new or modified weapons, including autonomous weapon systems or systems that acquire similar autonomous capabilities, to determine whether their use should be prohibited under international law in some or all circumstances.
- **Undertake** robust and forward-looking risk identification and human rights impact assessments in the design, development and sale of AWS, including by the private sector.
- **Prevent** the sale, transfer, export, acquisition or procurement of AWS without adequate IHRL safeguards, licensing arrangements and end-use controls.

International regulations

- **Clarify and strengthen existing law** by negotiating a legally binding instrument that sets clear prohibitions and restrictions on AWS, building upon and reinforcing existing obligations under international human rights law, in particular the prohibition of arbitrary deprivation of life and rules on the use of force.
- **Consider agreeing upon and imposing** a global moratorium on AWS until such norms are in place.



Palais des Nations,
CH-1211 Geneva 10, Switzerland
www.ohchr.org