AWS in the Hands of Crime:

A Nearby Threat in Latin America with Gendered Implications[1]

Gisela Luján Andrade

The growing interest of organized crime in the military use of emerging technologies, including autonomous technology and artificial intelligence (AI), raises alarms about the tangible perils of their application and development in Latin America, making us realize that we are no longer dealing with a scenario far removed from our reality.

The primary purpose of this article is to contribute to discussions in the region regarding the risks associated with the proliferation of 'low-end' autonomous weapons systems (AWS) to non-state armed actors, particularly organized crime, which constitute one of the main threats to human security in the region. Additionally, this analysis adopts a human rights and gender approach, emphasizing how the likely use of these systems by organized crime exacerbates the structural discrimination and violence already faced by women and other marginalized groups. Finally, this article calls for urgent action toward the regulation of AWS as a matter of global justice and equity.

The proliferation risk of AWS and organized crime

As the ICRC defines it, autonomous weapons systems are systems that can select and apply force to targets without human intervention. Such systems may initiate, or otherwise trigger, a strike based on information received from the environment through sensors and on the basis of a generalized "target profile".[2] In this way, the application of force is based on data processed from sensor inputs rather than an immediate human order.

For this reason, autonomous weapons —especially those lacking meaningful human control or used to target individuals— raise serious moral, legal, and ethical concerns, including digital dehumanization, the undermining of accountability for the use of force, and threats to international peace, security, and stability.

These considerations become even more concerning when such technologies are made available to actors outside the law such as criminal organizations, especially since they

---

[1] This article presents reflections, research, and analysis based on two presentations I delivered at international conferences: "El crimen organizado en América Latina desde un enfoque feminista," organized by Amassuru and held in Buenos Aires in November 2024 (The full version in Spanish can be found here: https://sehlac.org/f/armas-aut%C3%B3nomas-ia-militarizada-y-g%C3%A9nero), and "Harms and Risks of AI in the Military," organized by MILA PhD researchers and held in Montreal in December 2024 (The full presentation in English can be found here: https://www.youtube.com/watch?v=CNwc09cvIV4&list=PLXJ0UJfeO6DME5iPXWirP-Z8f7jLjfM25&index=1&t=153s&ab_channel=HarmsandRisksofAIintheMilitary).

[2] International Committee of the Red Cross (ICRC). (2018). *ICRC position on autonomous weapon systems: ICRC position and background paper. International Review of the Red Cross.* Retrieved January 14, 2025, from https://international-review.icrc.org/articles/icrc-position-on-autonomous-weapon-systems-icrc-position-and-background-paper-915

may gain even greater benefits from emerging technologies like AI[3] and autonomous technology.

To better understand these risks, I would like to consider the categorization of AWS proposed by a recently published research brief from the Geneva Academy[4]. The brief identifies two types of AWS based on their technological complexity: High-end systems, which "are likely to remain technologically complex and expensive" and may require sophisticated technologies, including complex sensor systems, radiation-absorbing material, and high-performance jet turbines, among others. And, low-end systems, which are simpler and cheaper, and rely on dual-use civilian technologies, such as autonomous drones.

These latter systems, with capabilities to navigate, identify targets, and attack, are much more accessible and represent an increased risk of proliferation toward organized crime. One key reason is that many of the hardware components required by autonomous weapons systems are widely available and numerous existing weapons can be easily retrofitted to operate in a fully autonomous mode.

For example, commercially manufactured drones for civilian or recreational purposes can easily be adapted for military uses, such as to carry explosives or for surveillance. That is the case of Colombian dissident groups from the former FARC[5], that have deployed drones loaded with improvised explosives or fireworks to attack enemies and terrorize rural populations.[6] Also, Mexican cartels have used them for surveillance, smuggling, and reportedly dropping explosives that have, on several occasions, killed Mexican soldiers.[7] Similarly, in Ecuador, criminals have used drones with explosives to target prisons as part of attempts to disable their physical infrastructure.[8]

Herein lies a clear example of hardware — in this case, unmanned drones — capable of being fitted for autonomous or semi-autonomous missions and thus inherently more likely to proliferate.

On the other hand, these systems' proliferation is further accelerated by their growing autonomy. Although the technologies involved in AWS development are advanced and

---

[3] Although not all AWS rely on artificial intelligence, AI greatly increases their capabilities and complicates their operation. This escalation is seriously raising concerns about the predictability and transparency of such systems. Large amounts of data can be processed at incredible speed using AI, resulting in force being applied to the target with minimal human involvement.

[4] Geneva Academy. (n.d.). Sending up a flare: Autonomous weapons systems proliferation risks. Geneva Academy. Retrieved January 14, 2025, from https://www.geneva-academy.ch/joomlatools-files/docman-files/Sending%20Up%20a%20Flare%20Autonomous%20Weapons%20Systems%20Proliferation%20Risks.pdf

[5] FARC (Fuerzas Armadas Revolucionarias de Colombia - Revolutionary Armed Forces of Colombia).

[6] *Semana*. (2023). *Así utilizan las disidencias de las FARC drones con explosivos para atacar al Ejército en Cauca*. Retrieved from https://www.semana.com/nacion/articulo/asi-utilizan-las-disidencias-de-las-farc-drones-con-explosivos-para-atacar-al-ejercito-en-cauca/202326/; *Infobae*. (2025, January 5). *Disidencias de las Farc en Tolima estarían reclutando y adoctrinando menores para operar drones bomba*. Retrieved from https://www.infobae.com/colombia/2025/01/05/disidencias-de-las-farc-en-tolima-estarian-reclutando-y-adoctrinando-menores-para-operar-drones-bomba/.

[7] Fox News. (2024, November 23). *Drug cartels using bomb-dropping drones killed Mexican army soldiers: Report*. Retrieved from https://www.foxnews.com/world/drug-cartels-using-bomb-dropping-drones-killed-mexican-army-soldiers-report; El País. (2022, February 1).

[8] AP News. (2024, January 8). *Ecuador: un ataque con dron con explosivos en cárcel de máxima seguridad es frustrado por la policía.* AP News. Retrieved from https://apnews.com/world-news/general-news-d7588e2ff10c07e3a764d0d7f861ebe8;

require the integration of powerful processing chips, sophisticated sensors, and advanced digital software, lower-quality sensors, chips, and software already exist commercially and are being integrated by criminal organizations in this region. This is the case, for example, with software allowing systems to surveil, deliver explosives, or target people without direct human intervention.

Additionally, access to open-source software and subscription-based platforms on the "dark web" makes such advanced technology available to criminal groups. This widens the spectrum for such practices in the region. An example is in Mexico, where drug cartels resort to open-source drone technology for surveillance and drug delivery. These drones are often modified with software obtained from dark web forums to enhance their performance.[9]

Finally, there is significant concern about the implications of low-end AWS for extrajudicial purposes, as such systems would enable targeted killings with a very low risk of attribution, making them a convenient tool for transnational assassinations or for the elimination of political dissidents, journalists, and human rights defenders in countries where the rule of law is virtually nonexistent.

Gendered impacts of AWS used by organized crime

Keeping these risks in mind, we now discuss how autonomous weapons change the security landscape and have differentiated effects on different segments of the population.

Technology is never neutral; in fact, it's often sexist. In the case of AI, for instance, the algorithms underlying these systems echo and amplify existing gender biases already entrenched in our societies, which are deepened by the biased data used in training them and by the limited frameworks shaping the approaches of their developers. Through data and structures steeped in systemic inequalities, AI exacerbates flaws in the system, entrenches discrimination, intensifies patriarchal dynamics, and heightens gender-based violence in our societies.

This reality is particularly alarming in contexts where organized crime exacerbates levels of violence rooted in gender inequality and may exploit these systems for monitoring, control, and tracking of individuals.

Considering the misrepresentation of technology concerning racialized women, as well as individuals from marginalized sectors — such as Afro-descendant people, Indigenous peoples, LGBTQ+ individuals, children, and people with disabilities — the climate of violence and intimidation would have fertile ground, worsening and amplifying the diverse forms of oppression and harm that these groups already suffer.

And this impact wouldn't be uniform. For instance, in areas controlled by criminal groups, Indigenous and Afro-descendant women, already marginalized historically, are particularly prone to being the most affected. Likewise, a diverse cohort of women experiencing or living in poverty and extreme poverty, who are also affected by trafficking and exploitation, may find these risks exacerbated through the application of AI technologies.

---

[9] *Infobae*. (2024, June 15). *Drones, the latest weapon of Mexico's cartels*. Retrieved from https://english.elpais.com/usa/2022-02-01/drones-the-latest-weapon-of-mexicos-cartels.html

Furthermore, autonomous weapons can also engage in targeted operations based on data collected or automated profiles. As such, they can be leveraged as lethal means by criminal organizations to intimidate, subjugate, or kill human rights defenders, activists, or victims of trafficking who are attempting to flee exploitation networks.

The use of autonomous weapons in organized crime may also contribute to a culture of impunity by enabling the commission of crimes from a distance and imposing additional barriers to justice, making accountability more difficult and responsibility more complex.

In other words, autonomous weapons systems don't just pose a security threat; they can also reinforce existing systems that oppress women and other marginalized people. Unregulated, their proliferation could intensify the inequality and violence that so many societies already experience.

Final thoughts

The increasing incorporation of emerging technologies by organized crime demonstrates that the risk of AWS proliferation in our region could begin to manifest using low-end systems that cannot only target and engage individuals but also become instruments of control and impunity.

This possibility would have a significant impact on communities and territories permanently under the control of criminal groups, particularly affecting women and women in their diversity, human rights defenders, and marginalized communities.

To highlight this threat and bring this underexplored issue to the forefront of national and international forums where AWS regulation is being discussed, it is crucial to ensure that these groups are adequately represented and take an active role in demonstrating that the urgency of starting negotiations of a legally binding instrument on autonomous weapons is not just a technical problem, but a global justice, equity, and human rights issue, especially for women and people from marginalized groups living under the weight of organized crime.

That said, civil society needs not only to engage in advocacy for regulating AWS but also to contribute to a broader debate about the human costs of these technologies, particularly in terms of the global inequalities in play. By uplifting the perspectives of women as members of marginalized communities from the Global Majority, civil society helps ensure that the discourse surrounding disarmament and regulation represents the diverse realities of communities most impacted by conflict, violence, and instability. It is not only about preventing these abuses but about advancing a more just and inclusive international security system that prioritizes human dignity and human rights.

This article was published as part of the Forum on the Arms Trade's "Looking Ahead 2025" blog series. Inclusion on the Forum on the Arms Trade expert list and the publication of this post does not indicate agreement with or endorsement of the opinions of others. The opinions expressed are the views of the author. See https://www.forumarmstrade.org/lookingahead2025.html.