Reframing Security in the Age of Militarized AI: Patriarchal, Decolonial, and Intersectional Perspectives

Submission to: AI for Peace Workshop - ICLR 2026

Elaborated by: Gisela Luján Andrade

Abstract

The integration of artificial intelligence into military infrastructures - specifically through autonomous weapons systems (AWS) and AI-enabled decision-support systems (AI-DSS) - is increasingly framed through legal and technical safeguards that leave unexamined the security paradigms shaping these technologies. Drawing on feminist and decolonial perspectives, this paper argues that such approaches are insufficient without a structural analysis of these paradigms and develops an integrated analytical framework structured around three interrelated dimensions: patriarchal, decolonial, and intersectional. These dimensions are applied to assess how militarized AI reorganizes decision-making processes, redistributes vulnerability, and consolidates pre-existing inequalities into operational parameters. Insights from Latin American contexts marked by militarized governance illustrate the layered effects of AI-enabled security infrastructures in settings of structural asymmetry. This paper engages critically with the AI for Peace agenda, arguing that technical risk mitigation is insufficient without confronting the security paradigms that militarized AI reflects and reinforces.

1. Introduction

The rapid integration of artificial intelligence (AI) into military infrastructures has largely been addressed through legal and technical safeguards focused on control, reliability, and compliance. While necessary, such approaches often leave unexamined the security paradigms that legitimize automated force and overlook the extent to which military AI is embedded in long-standing architectures of militarized power structured around the hierarchization of lives, where some are deemed worthy of defense while others remain expendable. Documented patterns of disproportionate harm in surveillance technologies, predictive analytics, and automated targeting systems demonstrate that these dynamics are not hypothetical risks but already materialized forms of structural inequality (O'Neil, 2016; Loewenstein, 2023).

This paper argues, from feminist and decolonial perspectives, that military AI consolidates and deepens patriarchal and colonial structures that have historically organized violence and protection (Lugones, 2008; Enloe, 2014; Mejías & Couldry, 2019; Gasztold, 2017). By translating classification, prioritization, and targeting criteria into operational parameters, these systems integrate structural hierarchies within decision-making processes, stabilizing and accelerating them under the rhetoric of efficiency and precision. To examine these dynamics, the paper develops an integrated analytical framework structured around three interrelated dimensions - patriarchal, decolonial, and intersectional - to examine how these systems restructure security and redistribute vulnerability. With particular attention to contexts of militarized governance in the Global South, particularly in Latin America, it argues that AI for Peace requires not only technical safeguards but a transformation of the paradigms that define what security is for and whom it protects.

This paper focuses on two categories of military AI that intervene in profiling and use of force: autonomous weapons systems (AWS), which can select and apply force without further human intervention once activated, and AI-enabled decision-support systems (AI-DSS), which generate targeting recommendations that human operators validate. Additionally, throughout this paper, I use

the term “militarized AI” as an analytical category that moves beyond purely technical understandings, emphasizing instead the political and strategic processes by which investments, doctrines, and institutional logics redirect technologies toward military ends.

2. Three Analytical Dimensions

2.1 The Patriarchal Dimension: Security as Dominance

Traditional security paradigms have historically been constructed around masculinist values: power understood as control, defense as domination, and force as the capacity to exercise violence. Such frameworks prioritize state sovereignty, territorial integrity, and national interests, understood primarily in military terms. This conception rests on an artificial division between the public and the private that elevates militarized, state-centered threats as the “real” security concerns, while relegating everyday insecurities - gender-based violence, poverty, forced displacement, food insecurity, or lack of access to healthcare - to a secondary plane. (Tickner, 1992).

Within this logic, protection becomes oriented toward preserving sovereign authority rather than sustaining concrete human lives. Militarized AI is embedded within this paradigm. Developed inside military-technological complexes, it reproduces associations between efficiency, rationality, and technical authority that appear neutral but rest upon long-standing masculinized conceptions of security.

One visible manifestation of this patriarchal hierarchy lies in the modeling and calculation of so-called “collateral damage.” Historically calibrated around the adult male combatant, such models have systematically underestimated differential impacts on women, children, and other marginalized bodies (Blanchard & Bruun, 2024). Automation does not correct this hierarchy; it risks reinforcing and accelerating it by transforming ethical deliberation into technical validation. The question shifts from “Is this just?” to “Does this fall within acceptable operational parameters?” Yet those parameters are never neutral: they encode prior judgments about which harms are tolerable and which lives are fully protectable.

2.2 The Decolonial Dimension: Data Extractivism and Experimental Territories

From a decolonial perspective, AI can be understood as an extractive logic that prolongs colonial patterns in the digital domain. Just as historical colonialism extracted material resources, data colonialism extracts human experience - biometrics, mobility patterns, communications, and behavioral traces - as raw material for systems designed, controlled, and monetized elsewhere. (Mejías & Couldry, 2019). Gaza represents one of the most extreme expressions of this dynamic: as Antony Loewenstein documents in *The Palestine Laboratory*, decades of occupation have transformed Palestinian life into a continuous data stream feeding surveillance, profiling, and targeting systems, which are subsequently exported globally as "combat-tested" security solutions.

Militarized AI operates within global hierarchies that transform certain territories into sites of experimentation and technological testing. Populations become observable, quantifiable, and governable through infrastructures of surveillance and profiling. Technologies refined in contexts of occupation or intense militarization are subsequently exported as “combat-proven” solutions, reinforcing transnational infrastructures of automated control. This dynamic reproduces asymmetries between AI-producing states and regions dependent on imported security technologies, embedding colonial power relations into algorithmic architectures and reorganizing global security practices accordingly.

2.3 The Intersectional Dimension: When Bias Becomes Operational

Intersectionality provides the third analytical lens, examining how multiple axes of power - racism, sexism, classism, ableism, and coloniality - operate simultaneously to produce differentiated exposures to automated error and violence. Applied to militarized AI, this lens reveals how historical inequalities are translated into datasets, design choices, proxies, and probabilistic profiles.

Algorithmic bias often originates in training data that reflect preexisting patterns of surveillance, criminalization, and territorial control. Even when technically accurate, such data may encode structural discrimination. Once integrated into predictive or targeting systems, these asymmetries become recurring statistical patterns. Territory may function as a proxy for racialization; youth, poverty, or geographic location may become indirect indicators of threat. (Blanchard & Bruun, 2024).

When these factors converge, entire communities may become constructed as “targetable” not because of verified conduct but due to intersectional configurations encoded as risk. Exposure to error and automated violence is therefore unevenly distributed. Intersectionality shows that algorithmic discrimination is not a technical malfunction but the crystallization of overlapping structural inequalities.

3. Insights from Latin America: Militarized Governance and Structural Vulnerability

Latin American contexts offer a situated lens through which to observe how these intersecting dynamics materialize. While the region lacks the institutional and technological capacity to develop AWS or AI-DSS in the military sense defined above, the underlying logic of these systems - profiling, automated threat classification, the redistribution of vulnerability - operates through dual-use technologies deployed in public security contexts. Their deployment, however, is never context-free.

In several countries, national security strategies increasingly rely on technological control mechanisms within environments already structured by racialized policing, territorial stigmatization, and gendered violence. In these contexts, dual-use AI technologies intersect with entrenched inequalities. Communities historically subjected to surveillance and militarization - Afro-descendant populations, Indigenous communities, residents of impoverished urban peripheries, among others - face heightened exposure to both human and algorithmic targeting. The introduction of AI-enabled systems into these contexts amplifies preexisting asymmetries in how threat is defined and how vulnerability is distributed.

Brazil offers a concrete illustration. According to the Rede de Observatórios da Segurança, over 90% of arrests made based on facial recognition involve Black individuals, a pattern connected to significantly higher error rates for darker-skinned faces (Buolamwini & Gebru, 2018; Da Hora, in Conectas, 2025). Young Black people and residents of peripheral urban areas face heightened exposure to false positives, arbitrary arrests, and police lethality, illustrating how AI-enabled security infrastructures enter contexts already structured by racialized policing and territorial stigmatization, amplifying preexisting asymmetries in how threat is defined and who bears the costs of automated error. Instead of addressing structural drivers of violence, this reliance on technological solutions risks reinforcing cycles of exclusion, criminalization, and differential exposure to harm.

4. Reframing Security and Peace

Feminist and decolonial perspectives offer not only critique of these dynamics but normative reorientation. Rather than defining security as the capacity to neutralize threats through calculation and force, these approaches reframe security as the sustainability of life.

Security, from this standpoint, is relational: its evaluation cannot be separated from its effects across communities and territories. Vulnerability and interdependence are not deficiencies to be eliminated but shared human conditions that generate mutual responsibility. The legitimacy of militarized AI, therefore, cannot be assessed solely through improvements in precision, efficiency, or compliance with operational standards.

An AI for Peace agenda grounded in this integrated framework would require intersectional impact assessments prior to deployment, meaningful participation of affected communities in governance processes, and transnational accountability mechanisms capable of addressing asymmetries in technological production and export. It would shift evaluative criteria from the optimization of force toward the prevention of structural harm and the equitable distribution of protection.

5. Conclusion

The debate on militarized AI is ultimately a debate about the differential value assigned to human lives and about the ethical limits of force. No technological architecture is neutral. Every decision to automate classification, targeting, or risk assessment is simultaneously a political decision about whose vulnerability becomes normalized and whose lives are rendered conditionally protectable.

If security continues to be defined exclusively as the capacity to neutralize threats through calculation and domination, militarized AI will appear as an inevitable technical advancement. If, instead, security is understood as the equitable protection of human dignity and the sustainability of life, the central question shifts: no longer only how to regulate these systems, but whether their underlying logic is compatible with that horizon. By integrating patriarchal, decolonial, and intersectional dimensions, this paper offers a structured analytical framework to confront that question. In doing so, it enables AI for Peace to move beyond technical containment toward a deeper transformation of how security and peace themselves are conceptualized.

References

- Blanchard, A., & Bruun, L. (2024, December). *Bias in military artificial intelligence* (SIPRI Background Paper). Stockholm International Peace Research Institute.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81.*
- Da Hora, N. (2025, October 13). Lack of regulation and inequality exacerbate flaws in facial recognition in Brazil. *Conectas Direitos Humanos.*
- Enloe, C. (2014). *Bananas, beaches and bases: Making feminist sense of international politics* (Updated ed.). University of California Press.
- Mejías, U.A & Couldry, N. (2019). Colonialismo de datos: repensando la relación de los datos masivos con el sujeto contemporáneo. *Virtualis, 10* (18), pp. 78-97.
- Gasztold, A. (2017). A feminist approach to security studies. *Przegląd Politologiczny*, *22*(3), 179–189.
- Loewenstein, A. (2023). *The Palestine laboratory: How Israel exports the technology of occupation around the world*. Verso, pp. 272.
- Lugones, M. (2008). Colonialidad y género. *Tabula Rasa*, (9), 73-101
- Tickner, J. A. (1992). *Gender in international relations: Feminist perspectives on achieving global security*. Columbia University Press.

LLM usage disclosure: The conceptual framework, arguments, and content were developed by the author in previous work drafted in Spanish and English and have been incorporated into this paper. LLMs (Claude, ChatGPT) were used as assistive tools for the translation of original Spanish-language lecture materials into English, English proofreading, extraction and structural organization of pre-existing arguments, and grammar editing. All AI-assisted revisions were critically reviewed and edited by the author.