

13 July 2026

IW PERSPECTIVES



The Hollowing Arsenal: How Artificial Intelligence Erodes the Foundations of Irregular Warfare

By Harrison Santiago

Harrison Santiago is a Washington D.C.-based analyst supporting the Department of War. He is broadly interested in emerging technologies related to artificial intelligence and human cognition, and the impacts on the future.

For centuries, irregular warfare has derived its power from a simple truth: populations matter. Whether a state seeks to coerce an adversary, support a resistance movement, or undermine the legitimacy of a rival government, every strategy ultimately depends on the human beings who staff armies, run factories, cultivate loyalty, and choose whom to obey. This dependency on influence has been the foundation of irregular warfare, codified across a dozen distinct activities from Civil Affairs Operations to unconventional warfare (UW). It

The views expressed in these articles are those solely of the authors and do not reflect the policy or views of the Irregular Warfare Center, Department of War, or the U.S. Government.

is also, increasingly, a vulnerability that artificial intelligence threatens to render obsolete.

This essay argues that as adversarial states integrate AI into their security apparatuses, the effectiveness of some irregular warfare activities will correspondingly diminish, not because these methods will become tactically impossible, but because their strategic logic will collapse. The power of irregular warfare offers leverage over human decision-making. Automation severs that leverage.

I. The Human Substrate of Irregular Warfare

Irregular warfare, as defined by [U.S. joint doctrine](#), is a contest of influence, a campaign to assure or coerce states and groups through indirect, non-attributable, or asymmetric means. Beneath the terminology of its twelve constituent activities lies a unified assumption: that a state's capacity to project force depends on the willing or coerced participation of human beings throughout its security apparatus and supporting society.

This assumption is not merely theoretical. History demonstrates it repeatedly. Counterinsurgency campaigns succeed or fail based on whether local populations can be persuaded to withhold support from insurgents. Foreign Internal Defense programs function only insofar as host-nation soldiers choose to fight. Psychological Operations (PSYOP) work by shifting the beliefs and behaviors of foreign individuals and organizations. Unconventional warfare, perhaps most directly, exploits the willingness of underground networks and auxiliary forces to act against their own government.

In each case, the human element is the mechanism. An insurgency is not a military problem solved by firepower; it is a political problem solved by changing what people are willing to do. A resistance movement does not succeed by outgunning occupiers; it succeeds when enough individuals decide the cost of compliance exceeds the cost of resistance. This is why irregular warfare's most potent instruments are fundamentally tools of human persuasion and leverage, not tools of physical destruction.

The coupling between a state's security apparatus and its broader population has historically created multiple points of leverage for an irregular campaign. A conscript army can be demoralized. An industrial workforce can be convinced to slow production or share intelligence. Security forces can exercise discretion; declining orders they find illegitimate. Commanders can be turned. Logistics networks can be subverted. These vulnerabilities exist because human beings bring values, fears, loyalties, and judgments to their work, and those qualities can be influenced.

II. The Incentive Structure Driving AI Adoption

Understanding the threat that AI poses to irregular warfare requires first understanding why states are compelled to adopt it. The pressures are structural and arise from competitive dynamics that no state can afford to ignore. The most immediate driver is scalability. Human expertise is slow to develop, impossible to copy, and costly to sustain. An AI system, once developed, can be replicated at the cost of hardware and updated near-instantaneously. A military that deploys ten AI systems for surveillance and targeting analysis effectively fields what would have required hundreds of trained analysts. States that hesitate to automate face adversaries who do not.

Closely related is sustainability. AI systems do not fatigue, require no rotation schedules, and operate without the geographic and logistical constraints that attend human deployment. A system conducting signals intelligence analysis works the same at hour seventy-two of a crisis as at hour one. This durability compounds over time: an AI-assisted security apparatus maintains operational tempo under conditions that would exhaust any human organization.

Decision-making speed represents perhaps the most strategically significant advantage. AI systems process information at speeds orders of magnitude greater than any human analyst. As competition intensifies and operational timescales compress, the ability to act within an adversary's decision cycle will increasingly depend on automated systems. A state that routes all intelligence assessments through human analysts will simply

be too slow to compete against one that automates the same function.

Finally, and most consequentially for the long term, there is anticipatory disinvestment. As tasks become candidates for future automation, rational actors (i.e. states, companies, and individuals) face diminishing incentives to invest in developing human capabilities in those areas. This creates a self-reinforcing cycle: the expectation of AI capability reduces investment in human alternatives, which accelerates the shift toward AI even before full automation is realized. The decision to automate, once made by leading powers, tends to become compulsory for everyone else.

The result of these pressures is predictable: over time, states will delegate increasing proportions of their security apparatus functions to AI systems. This delegation will not be uniform or instantaneous, but the directional pressure is clear and strong.

III. Decoupling: How AI Severs the Leverage of Irregular Warfare

The strategic logic of irregular warfare rests on a “coupling problem” because a state’s security apparatus requires human participation at multiple levels, it remains vulnerable to campaigns that influence those humans. AI adoption systematically attacks this coupling, replacing human nodes in the security apparatus with automated systems that cannot be persuaded, demoralized, or turned.

Consider the following examples of functions currently performed by humans within a security apparatus: intelligence processing and analysis, administrative coordination, logistics management, industrial base supervision, and industrial base participation. Each of these functions, as it migrates from human to AI execution, represents a point of leverage removed from an irregular warfare campaign’s reach.

The most direct impact falls on the three IW activities that most explicitly target human agency: Civil-Military Operations (CMO), Psychological Operations (PSYOP), and unconventional warfare. Civil-Military Operations function by shaping the relationship between military forces and civil-

ian populations, namely establishing legitimacy, managing grievances, and creating conditions in which the population supports rather than undermines the security apparatus. This works because human soldiers and commanders are embedded in communities, because their behavior matters to local populations, and because local populations in turn affect the security environment. AI adoption fundamentally reshapes how CMO functions are delivered.

Automated logistics and resource allocation can accelerate humanitarian assistance, getting aid to affected populations faster than traditional coordination chains allow. AI-driven data fusion can help commanders identify where civil needs are most acute. NGO coordination, historically plagued by duplicative efforts and communication gaps, can be streamlined through shared AI-enabled common operating pictures. Yet these efficiencies carry risk. When the interface between military and civilian becomes algorithmic, the relational foundation of CMO erodes. The population may receive the service but lose the human connection that converts service delivery into lasting legitimacy and stability.

Unconventional warfare is even more threatened. UW operates through underground networks, auxiliary forces, and guerrilla units that coerce, disrupt, or overthrow governments by exploiting the willingness of individuals to resist. It works because occupying powers and adversarial governments depend on human cooperation at every level. An AI-managed border surveillance system cannot be bribed. An automated administrative process cannot be intimidated into looking the other way. An automated factory will not sabotage materiel. As the human nodes through which UW operates are replaced by automated systems, the entire tradecraft of unconventional warfare loses its purchase.

PSYOP face the most profound challenges. PSYOP targets foreign audiences to influence their emotions, motives, and behavior. Its effectiveness depends on the assumption that human decision-makers can be reached and moved by PSYOP, that propaganda works, that morale matters, and that soldiers and citizens can be made to doubt, defect, or delay. As AI systems assume greater authority over operational decisions,

PSYOP campaigns directed at human operators become strategically marginal. You cannot demoralize a targeting algorithm. You cannot convince an automated logistics system that the cause is unjust. The audience that PSYOP requires simply ceases to be the decision-making audience.

IV. The Diminishing Returns of Influence Operations

One might object that irregular warfare retains its relevance as long as human beings inhabit the adversary's society, that even if the security apparatus automates, the broader population remains influenceable. This objection is valid but increasingly bound.

The effectiveness of influencing a population depends on whether that population's choices actually affect the security environment. During the Cold War, winning hearts and minds in contested societies mattered because local populations could actively support or undermine guerrilla forces, sabotage infrastructure, provide intelligence, or withhold cooperation from occupying forces in ways that materially affected military outcomes. The chain of causation between popular sentiment and security outcomes was short and direct.

AI adoption lengthens and weakens that chain. A security apparatus that automates its domestic intelligence gathering does not rely on human informants. One that uses AI-driven logistics management does not depend on a compliant civilian workforce to sustain supply chains. As each of these dependencies dissolves, the strategic value of influencing the underlying population diminishes—not to zero, but substantially.

The more complete the automation, the more the adversary's security apparatus resembles a closed system: one that derives its capability from hardware, software, and energy rather than from human labor and loyalty.

V. Implications and Adaptations

None of this implies that irregular warfare will vanish or argues that it will become useless. How-

ever, several implications follow from the analysis above.

First, the relative effectiveness of different IW activities will diverge sharply. Activities that target infrastructure, technical systems, or decision-making processes (e.g. Countering Threat Networks or Counter Threat Finance) may retain or even gain relevance, because they attack the material substrates of AI-enabled security rather than the human agents within it.

Second, the timeline of AI adoption will determine the window of IW effectiveness. States and non-state actors conducting irregular campaigns against adversaries who are early in the automation process will have far more leverage than those confronting mature AI-integrated security apparatuses. This creates a strategic premium on early action and on slowing adversary adoption where possible.

Third, the doctrine and resourcing of IW must evolve to account for this shift. Continued investment in human-influence-based activities against adversaries who are systematically removing human decision points from their security architecture represents a diminishing return on resources. New concepts are needed: approaches that contest AI systems directly, through means such as adversarial inputs, supply chain influence over AI development, and exploitation of automation dependencies.

Fourth, and perhaps most importantly, the analysis highlights an asymmetry. The United States and allied democracies face significant domestic constraints on the degree to which they can automate their own security apparatuses, there are political, legal, and ethical constraints on autonomous weapons, mass surveillance, and AI-driven decision-making. Adversaries operating under fewer such constraints may automate faster and more completely, gaining the very immunity from irregular influence that this essay describes. Managing this asymmetry, maintaining the capacity to wage irregular warfare while confronting adversaries who are increasingly immune to it, is among the most consequential strategic challenges of the coming decades.