LEVELING THE BATTLEFIELD: AI-ENABLED TECHNOLOGY IN THE HANDS OF NON-STATE ACTORS

BY LAM TRAN

***Lam Tran** is an MS Candidate studying Science and Technology Policy at Georgetown University. She has been a Young Leader with the Pacific Forum since 2021. Contact: via X: @lamxtran or LinkedIn.*

Drones will be an essential tool for multiple industries. Source: Creative Commons

Advancements in artificial intelligence (AI) technology are reshaping modern warfare, impacting conduct on the battlefield and the decision-making chain in command centers alike. The open-source, low-cost, and dual-use characteristics of AI technology make weaponizing these AI-enabled capabilities for malicious purposes more accessible to non-state actors. This development disrupts the traditional power balance between states and non-state entities and complicates deterrence strategies that have long underpinned international security frameworks.

Drawing on discussions in a workshop titled Techno-Optimism, Geopolitics, and the Future of AI hosted by the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory, this commentary analyzes how non-state actors are deploying AI-based tools in conflict and its implications for arms control regime.

How Does AI Lower the Cost of Entry for Non-State Actors?

Artificial intelligence is a branch of computer science focused on creating systems or machines that can perform tasks typically requiring human intelligence. These tasks include identifying patterns from large data sets, making predictions, and solving problems. Through algorithms, computing power, and large-scale data processing, AI enables machines to analyze inputs, improve over time, and undertake complex operations with minimal human supervision.

Unlike conventional military capabilities such as fighter aircraft or nuclear weapons, which require significant financial and scientific investment that only wealthy governments can afford, AI-based technology presents a much lower barrier to entry for non-state actors. Many AI algorithms are open-source and developed by private companies, allowing non-state actors to acquire commercially available capabilities and overcome their resource and expertise disadvantages. Furthermore, the dual-use nature of many AI technologies, serving both civilian and military purposes, makes it easier for non-state actors, who do not have to abide by international rules and norms on the ethical use of these technologies, to abuse AI-based tools.

Non-state actors, including international criminal organizations, paramilitary or terrorist groups, state-backed non-state actors, and individuals, acquire AI capabilities through various sophisticated channels. Some groups exploit off-the-shelf technology and publicly available resources, while others benefit from state sponsorship and technology transfer. The rise of cryptocurrency, mobile payments, and virtual assets has further facilitated illicit procurement by allowing groups to bypass existing financial controls and sanctions.

How Do Non-State Actors Deploy AI in Physical and Digital Battlefields?

In kinetic warfare, drones, including air, ground, surface, and underwater platforms, and uncrewed aerial vehicles (UAVs), are transforming combat dynamics as they provide non-state actors with inexpensive tools to conduct surveillance, gather intelligence, and execute precision strikes. Between 2016 and 2020, researchers documented 440 cases of non-state actors using weaponized UAVs. Groups like the Houthis and Hezbollah have demonstrated sophisticated drone attack capabilities against state actors. In a more high-profile example, in 2022, Houthi drone attacks targeted Emirati oil tankers and airport infrastructure, exemplifying how non-state armed groups with fewer resources can pose serious threats to a country's critical infrastructure.

Criminal organizations, such as drug cartels, have also adopted AI-enabled drones. A $5,000 drone, capable of carrying around 35 pounds of payload, allows these organizations to move drugs and weapons across borders more efficiently. The Department of Homeland Security has flagged these "narcodrones" as a significant emerging threat, noting their capacity to bypass current law enforcement efforts. The use of semi or fully autonomous AI-powered systems could allow "narcodrones" to identify and target customs and border patrol agents, increasing the lethal threats of these technologies.

In the cyber realm, non-state actors increasingly leverage AI to enhance their cyber operations with AI-assisted cyberattacks and disinformation campaigns. Machine learning algorithms allow cyber operators to sift through massive data sets to identify vulnerabilities, enhance phishing attacks, and automate the targeting of people based on individualized profiles. In information warfare, generative AI technology, a type of AI system that can create new content, such as text, images, videos, and music, has been extensively employed to flood social media with disinformation and sow public confusion and distrust. For example, following Hamas' October 2023 attacks against Israel, Iranian-back groups used AI-generated content in an extensive propaganda effort, deploying fabricated footage and images to influence public opinion.

What are the Implications for Military Planning and Arms Control Efforts?

The proliferation of AI capabilities to non-state actors has forced a fundamental reassessment of Western governments' military strategy and planning. As low-cost, AI-enabled systems undermine battlefield advantages that have been long held by state actors, military planners should revise their strategy while accounting for sophisticated uses of emerging technologies by non-state actors. Defense planners in Washington have responded to these developments by doubling down on asymmetrical capabilities and aiming to field "multiple thousands" autonomous, unmanned systems within the next two years. U.S. allies and adversaries also have programs to build fleets of stealthy drone fighters that operate alongside crewed aircraft.

The rise of AI-enabled non-state actors highlights the limitations of current deterrence and arms control frameworks in addressing emerging technological threats. Several key challenges fuel this issue. First, the dual-use nature of AI technology complicates regulation, as many civilian applications can easily be adapted for military use. The lower entry barriers for AI, compared to conventional weapons, enable a wider range of actors to access and deploy these capabilities, with non-state entities often existing outside existing regulatory regimes. Furthermore, the speed of technological advancement outpaces existing frameworks, and the decentralized development of AI complicates attribution and accountability.

Broadening multilateral engagement platforms to include a variety of stakeholders beyond just states is imperative to address these challenges. Forums like the United Nations' Groups of Governmental Experts (GGEs) and specialized working groups on ICT, machine learning, autonomous weapons, biotechnology, and space technology provide venues to clarify the responsible use of AI and emerging technologies. These platforms can facilitate discussions on adapting international law and political norms to include state and non-state uses of such technologies, enabling agile responses to identify when new global norms or rules—whether binding or non-binding—are necessary. Furthermore, public-private partnerships could engage companies and other stakeholders in advocating for legally binding AI regulations, contributing to a cohesive international framework that balances technological advancement with security imperatives.

Disclaimer: All opinions in this article are solely those of the author and do not represent any organization.