

October 2025

## Confronting Asymmetric Innovation: The Policy Challenge of Drone Warfare

Dr. Dorian B. Kantor and Felipe SantoFimio Nevares

### Executive Summary

In August, Colombian Senator Nicolás Echeverry, a member of the Congressional Commission on national security, [underscored](#): “The use of drones for offensive purposes marks an unprecedented escalation in the Colombian conflict. ... The recent tragedy in Amalfi, Antioquia, where a police helicopter was brought down by an explosive drone ... is painful proof that our warnings were not rhetorical.” This paper argues that while drones did not revolutionize the battlefield in the so-called Global War on Terror, they now allow weaker actors in Latin America and Ukraine to reshape combat dynamics. Unlike earlier state-led advances in warfare, this revolution is driven by the private sector, rapidly adopted by violent non-state actors, and has diffused faster than international regulatory regimes and norms can adapt. This paper calls for export controls, stronger regional coordination, and national investments in counter-drone technology, training, and legal frameworks to secure supply chains, prevent diversion, harmonize standards, and adapt doctrine and force structures to drone-enabled warfare.

### 1. Background: War as a Historic Driver of Innovation and Constraint

Although uncrewed aerial systems date back to World War I, they only gained prominence in the Global War on Terror, when armed drones became central to U.S. counterterrorism. By the 2000s, remote-controlled warfare had come to define a “[revolution in military affairs](#)” (RMA), marking a shift from industrial-age mass warfare to an information-age model built on speed, agility, and precision.

Much like earlier military innovations, the United States’ drone program was state-driven, with research by the Defense Advanced Research Projects Agency, Pentagon contracts, Air Force procurement, and CIA incentives laying the groundwork and defense contractors like General Atomics executing contracts under state direction. Under Defense Secretary Rumsfeld, the Bush administration leveraged the RMA to drastically reduce “[boots on the ground](#)” in both high-intensity wars and low-intensity counterterrorism campaigns. Large, weaponized Predator and Reaper drones (brand names of the MQ-1 and MQ-9) came to sustain a [nonstop, low-level conflict](#) in the borderless war on terror.

These drones, however, did not revolutionize the battlefield. They merely reinforced the war’s asymmetry, as

adversaries lack effective countermeasures. Their legal impact, however, was substantial: for over 20 years, drone operations have unfolded in an exceptionally [permissive legal environment](#), often unmoored from law-of-armed-conflict constraints and geographical limits.

By 2022, drone innovation was evolving in reverse. Ukraine, the militarily weaker side in the conflict with Russia, turned small, cheap, off-the-shelf unmanned aerial vehicles (UAVs) into a means of survival, adapting commercial and first-person-view (FPV) drones for intelligence-surveillance-reconnaissance and strike missions. Drones are now so central to the country's defense that every battalion fields a UAV unit and the armed forces have established a [branch](#) dedicated to unmanned warfare.

Initially, Ukraine relied on large foreign-made platforms like the [Turkish Bayraktar TB2](#). But Russian air defenses and electronic warfare quickly blunted their utility. The focus then shifted to small commercial UAVs. First imported from Chinese companies such as DJI and Autel, later mass-produced by a cottage industry of volunteers and startups. Fueled by “[dronations](#),” this bottom-up model allows developers to mass-produce [FPV attack drones](#) tailored to battlefield needs. To scale this momentum, the Ukrainian government launched [Brave1](#) in 2023, channeling millions of dollars to arms producers and registering thousands of defense-tech innovations. Today, Ukraine is recognized as a major military innovator with a cutting-edge defense industry that produces millions of drones annually thanks to domestic and [foreign investment](#).

While Ukraine's drone defenses initially caught the invaders off guard, Russia has [adapted](#), deploying thousands of Iranian Shahed-136 variants and producing an estimated two million FPV drones in 2025. Unlike Ukraine's bottom-up model, Russia's UAV industry is [state-managed](#), with private firms supplementing but not driving innovation.

Dronification has reshaped the battlefield by widening the kill zone, reviving trench warfare, and making electronic warfare ubiquitous. With drones accounting for [70 percent](#) of casualties, counter-UAV systems – from FPV detectors and low-altitude radars to jammers – have become indispensable for force protection, and drone defenses are now [standard in military-industrial design](#).

## 2. Contagion effect: Drones in the Colombian Internal Armed Conflict and Beyond

Ukraine's example has set a new trend for insurgent groups, which operate like startups in their rapid adoption of new tactics and high risk-tolerance. Today, over [65 violent non-state actors](#) worldwide field drones, a capability made possible by private sector innovation and mass production by firms like DJI. Commercial UAVs – along with advanced components like GPS, open-source sensors, and digital command and control systems – have become global commodities. Newer models endure [harsh conditions](#), fly longer, and integrate military grade [cameras and thermal imaging](#). Meanwhile, [DJI's removal of hard no-fly zones](#) has lowered the barrier for violent

non-state groups to use drone against state authority.

The contagion effect is evident in Latin America. [Mexican cartels](#) were first to integrate drones into their operations for narcotics transport, surveillance, and attacks. [Colombian insurgents](#) soon followed suit, mimicking Ukrainian tactics by modifying commercial drones to extend their reach, increase lethality, and reinforce psychological intimidation. This has reignited armed confrontation, driving a spike in violence and introducing [previously unseen forms of attack](#).

For groups like the National Liberation Army (ELN) and dissident factions of the largely demilitarized Revolutionary Armed Forces of Colombia (FARC), drones mark an evolutionary leap in guerrilla warfare by providing an aerial force multiplier that enhances their intelligence, mobility, and surprise attacks capabilities and help sustain campaigns at low cost and with minimal manpower. The rapid integration of drones – from [crude bomb-droppers](#) to [sophisticated FPVs](#) – has emboldened Colombia’s armed groups to adopt a more offensive posture, striking civilian and military targets at increasing frequency and intensity. Innovation is taking place on multiple fronts: Colombian authorities recently intercepted an autonomous “[narco-submarine](#)” equipped with Starlink satellite internet, reportedly used for long-range smuggling operations – further evidence that insurgent and criminal networks are embracing advanced, commercially available technologies to expand their operational reach.

### 3. Policy Context: Gaps in Battlefield and Export Regulations

The spread of drones underscores a familiar problem: new technologies evolve faster than regulatory frameworks or strategic doctrines. The current regulations are a fragmented patchwork of national policies on use and trade, and militaries have devised ad hoc responses to weaponized commercial UAVs. A coherent international legal regime is absent, as the Hague and Geneva Conventions – drafted long before robotics and remote warfare – leave major gaps. [Norm evolution theory](#) explains this well: great powers rarely constrain weapons that serve their strategic interests, sustaining instead an “[unrestricted](#)” posture that normalizes permissive practices.

Because unmanned platforms facilitate the use of lethal force, responsible proliferation is a key challenge. The United States previously led efforts to prevent the spread of large systems under the [Missile Technology Control Regime](#), which presumed export denial. The Trump administration, however, [reclassified](#) these platforms as “aircraft” rather than “missile system” to ease export restrictions and to improve competitiveness with less selective proliferators. Major exporters like Turkey and Israel have interpreted regulations loosely to sell their systems [widely](#).

China not only exports its Wing Loong large combat UAS widely but also dominates the commercial market with DJI controlling [70% of global sales](#). While Beijing introduced a series of export controls on commercial drones beginning in 2023, those restrictions are primarily aimed at Europe

and North America. In contrast, under its “no-limits” partnership with Moscow, China continues to [supply](#) around 80% of the critical electronics used in Russian drones and has even set up a [joint production facility](#).

Without a comprehensive regime governing the proliferation of dual-use UAVs and their supporting technology, fragile states risk becoming proving grounds for criminal groups to refine drone tactics to destabilize governments and export violence abroad.

#### 4. Policy Recommendations

The proliferation of dual-use drone technology demands a coordinated, rules-based response across international, regional, and national levels.

On the international level, the United States and its allies should secure supply chains and prevent diversion to illicit actors. Forums such as the US–EU Trade and Technology Council, NATO, the G7, the G20, and the WTO can be used to set a common regulatory framework for commercial UAVs. NATO’s [Defense Innovation Accelerator](#) can complement these efforts by linking governments, industry, and academia to foster innovation with embedding safeguards against misuse. Export controls regarding dual-use technology should also be strengthened and harmonized. Building on the 2016 [Joint Declaration](#) for the Export and Subsequent use of Armed or Strike-Enabled Unmanned Aerial Vehicles, and modeled after the [Missile Technology Control Regime](#), states should extend restrictions to critical components, with regular reviews to match technological change. Arms-control–style

mechanisms emphasizing transparency, oversight, and restraint are also viable models to adopt.

At the regional level in the Americas, policies should strengthen coordination and oversight. The Organization of American States (OAS), though lacking enforcement power, can facilitate consultation and coordination through the Permanent Council. Under the [Rio Treaty framework](#), Latin American states could seek a collective response to the destabilizing threat of drone proliferation, including common export controls, intelligence-sharing, and collective counter-drone measures. The [Inter-American Defense Board](#) (IADB) should be empowered to coordinate counter-drone monitoring and training, pooling resources across states. However, recent frictions – exemplified by Washington’s [decision](#) to add Bogotá to its list of countries “failing” in the fight against drugs – highlight the fragility of regional trust and the political sensitivities that may complicate collective security efforts. Colombia, already confronting insurgent drone attacks, could nevertheless play a leading role in advancing cooperative mechanisms, particularly through best-practice sharing.

At the national level, governments should invest in counter-drone research and development and integrate these systems into military and police forces. Building [domestic manufacturing](#) is crucial to reduce reliance on external suppliers, as highlighted by [Ukraine’s challenges](#) following China’s introduction of export restrictions. Legal frameworks should treat drones as complete systems – operators and supporting

electronics – rather than as objects alone. Building on [India](#)'s end-to-end model, regulatory oversight should cover the entire lifecycle of drones – from purchase to operation – with mandatory permits, standardized training, and centralized registration across all weight categories. Effective regulation should also cover dual-use components to close loopholes that allow illicit actors to exploit gaps by importing parts separately or weaponizing commercial platforms. The recent [Chinese export control model](#) illustrates how states can tighten oversight and curb diversion. Finally, national forces should adapt their doctrine and training to the realities of drone warfare by updating counterinsurgency concepts, deploying fixed and mobile counter-UAV systems, and implementing force structure hardening. Colombia is both a warning and an example: while its armed forces are updating strategy and tactics, political will, and resources lag, leaving doctrine to outpace capabilities.

## **Author**

**Dorian B. Kantor, Ph.D.**, founder of Kantor Consulting, is an international security analyst specializing on military technology, international law, and global governance. He has advised military and public institutions and taught at leading universities in Europe and Latin America.

**Felipe Santofimio Nevares** is researcher and analyst at Kantor Consulting and a graduate student in defense policy and international security at Universidad Externado de Colombia.

## **Disclaimer**

This publication is part of the Jack D. Gordon Institute for Public Policy at FIU's Policy Innovation Series edited by Dr. Inga Trauthig. The views expressed in this publication are solely those of the author/s and do not necessarily reflect the official policies or positions of the Florida International University, the Jack D. Gordon Institute for Public Policy, or any affiliated institutions.