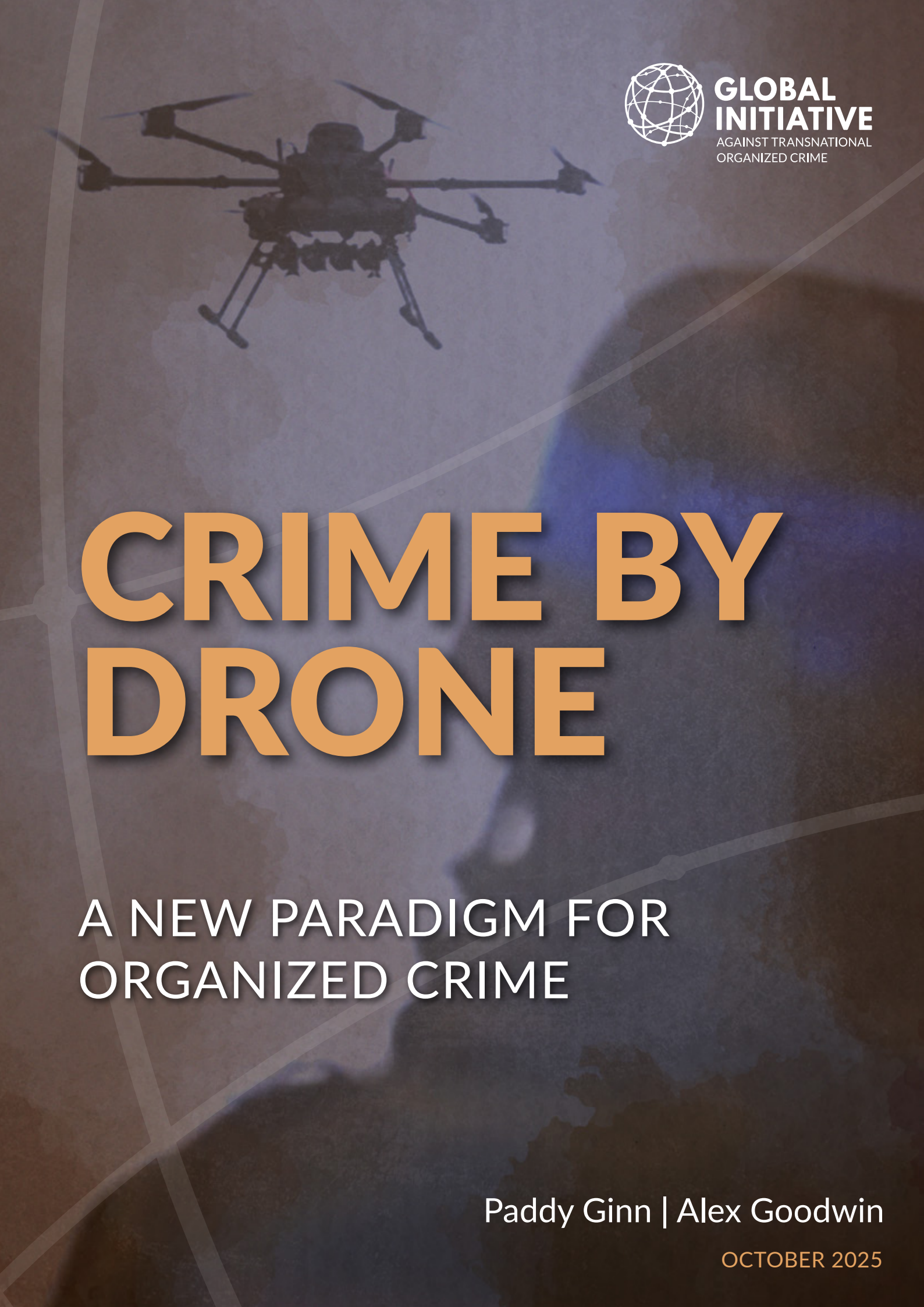

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

CRIME BY DRONE

A NEW PARADIGM FOR ORGANIZED CRIME

Paddy Ginn | Alex Goodwin

OCTOBER 2025

ACKNOWLEDGEMENTS

This report relied on the expertise and knowledge of our drone-operator colleagues from Ukraine; we would like to thank them for their insights and recognize their skill in this highly advanced field.

ABOUT THE AUTHORS

Paddy Ginn is a senior expert at the Global Initiative Against Transnational Organized Crime (GI-TOC). A former senior military officer, he recently served as the military adviser to the United Nations Assistance Mission in Afghanistan, advising on security, counterproliferation, counterterrorism and sanctions. Previously, he led a British Army brigade modernization project and commanded 20th Armoured Infantry Brigade, deploying forces across Europe. He has served in Afghanistan, Iraq and Northern Ireland. A decorated infantry officer, he holds a BSc in Psychology, graduated from the US Joint Advanced Warfighting School and the UK Higher Command and Staff College, and is a Fellow of the Forward Institute. He was awarded CBE in 2020 for leadership.

Alex Goodwin is an analyst at the GI-TOC, focusing on the impact of the Russo-Ukrainian war on illicit economies in Ukraine and the broader region. Previously, he worked as an editor at the International Institute for Strategic Studies and in the publishing sector.

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS

EXECUTIVE SUMMARY

The Russo-Ukrainian war is a striking case study of how a technology, in this case drones, can reshape a war. In the civilian realm, organized crime has already been quick to adopt drones, mainly for surveillance and smuggling, but the innovations of the war – both tactical and technological – may well bring about a paradigm shift in how organized crime operates in the future. Indeed, reports emerged in October 2025 of a Mexican cartel member who had been sent to Ukraine to learn how to pilot drones as part of the International Legion – skills he planned to transfer to his criminal career afterwards. Fibre-optic drones – a relatively recent battlefield innovation – have also found their way into Mexican criminal hands.[1] Risk has already become reality.

The question of drone use is immediately relevant. Poland recently responded to Russian drone incursions into its airspace, a test of NATO's reactions.[2] Drones have shut down airports in Norway, Denmark and Belgium.[3] Politicians are talking of a 'drone wall' along Europe's eastern borders.[4] Terrorists were arrested in Belgium for planning to use drones in a 'jihadist-inspired terrorist attack' against Belgium Prime Minister Bart De Wever.[5]

In the public discourse, drones are a weapon of states and terrorists; this policy brief takes a different angle and considers how drone technology forged in the crucible of war has been co-opted by organized crime and repurposed to achieve criminal goals. At the heart of the research is an exercise conducted with Ukrainian drone pilots, which aimed to understand the potential crossover of drone technology into organized crime within the land, air and sea domains. Various criminal scenarios were assessed, as were the requirements necessary to execute them, to illustrate this complex problem.

In response to the suggestion that this may be doing the criminals' homework for them, this paper argues that it is only by thinking through the concrete applications of drone technology that responses can be accurately formulated. Using these scenarios and insights from drone operators, we demonstrate that the use of drones requires a suite of skills and considerations that could represent points of disruption for law enforcement and policymakers. The risk should not be underestimated. Drones are being adopted for criminal purposes: smuggling, reconnaissance, intelligence gathering and worse. The trend is towards criminal gangs using them with greater scale and sophistication.

In order to conceptualize how organized crime may use drones, this report adopts a framework based on military doctrine concerning the organization and application of forces, and applies it to create 'criminal functions'. It thus considers drones to be part of an integrated criminal ecosystem, a combination of elements that create the conditions for criminals to shape the environment in their favour, sustain their activities and execute the decisive criminal act, be it smuggling, piracy, violence or coercion.

Examining organized crime through this functional framework reveals how illicit activity operates across multiple domains. In the air, for example, drones enable surveillance, delivery and targeted violence. On land, they facilitate the movement of goods and reconnaissance. The sea domain offers opportunities for large-scale smuggling and transnational logistics, with drones and digital networks increasingly being layered onto maritime trafficking.

Mapping criminal drone operations over air, land and sea activities makes it clear that organized crime's use of drones is now multi-domain. Crucially, the success of criminal operations hinges not only on the platforms themselves, but also on the supporting networks of engineers, logistics hubs and cross-border facilitators. The integration of drones and humans, and the convergence of physical and digital methods, produces a flexible and resilient criminal system that is increasingly difficult to counter with conventional law enforcement tools.

Constrained uses

Ultimately, drones have dramatically reduced financial and operational risks for criminals, while increasing the tactical options available in each domain. However, this is not without constraints. As our research makes clear, the utility of drones for criminal tasks must be viewed in the light of factors such as their range, payload, cost and detectability.

Aerial platforms have been used for high-profit smuggling and assassinations. However, precision strikes demand detailed reconnaissance, skilled pilots and/or AI-enabled targeting. Consequently, criminal gangs still employ hitmen, but drone assassinations could be used for hard-to-reach targets (such as politicians, as evidenced by the attempt on Nicolás Maduro's life in 2018) or where a display of reach and power is desired.[6]

Although land drones can carry heavy payloads in smuggling operations, they have a limited range and are unable to navigate rough terrain. As they use line-of-sight signal communications, they also require a chain of repeaters at regular intervals, which complicates their use for criminal activities. However, an armed land drone could provide a powerful element of terror in urban environments, an alarming prospect for public security worth illustrating.

Maritime drones are a long-range, high-capacity option well suited to the trafficking of drugs or even arms, and may also have potential as offensive weapons in maritime piracy. Although they have more limited distance capabilities, they are more robust and technologically advanced than the narco-submarines previously employed for these activities. However, due to their high cost and the challenges of operating at sea, they are likely to be accessible only to the most sophisticated criminal groups operating in lucrative illicit markets, such as the cocaine trade.

Ultimately, it seems probable that drones will primarily be used by criminals for smuggling and surveillance rather than for weaponization. A 2023 study of drone use in Africa's illicit economies showed that drones were first employed for intelligence, surveillance and reconnaissance, and propaganda purposes, only later progressing to payload delivery.[7] Drones have a clear advantage in these areas for organized crime, in terms of cost versus profit and ease of use. However, if the expertise and experience gained during the Russo-Ukrainian war filters down to the criminal underworld, there is a significant risk that sophisticated and lethal drone operations will become much more feasible; the current trends are already pointing in this direction.

Maritime drones could offer short-range, uncrewed alternatives to narco-submarines, such as this one seized by the Colombian authorities, which had a range of 13 000 kilometres and a payload of 7.3 tonnes of cocaine. *© Juan Manuel Barrero Bueno/Miami Herald/Tribune News Service via Getty Images*

Future responses to the criminal use of drones will need to combine 'soft' and 'hard' approaches within an integrated ecosystem of technology, regulation and forensics. On the soft side, electronic warfare tools such as jamming, signal seizure and directed-energy weapons can be used to suppress hostile unmanned aerial vehicles (UAVs), supported by next-generation detection technologies such as AI-enhanced radar, as well as acoustic, optical and radio-frequency monitoring systems. Hard countermeasures focus on physically destroying drones using anti-aircraft weapons, interceptor drones, lasers and microwave systems. Passive protection measures like geofencing, nets, false walls and specialized hangars could provide an additional defensive layer for critical sites. Alongside this, regulatory frameworks such as flight restrictions, identification schemes and interagency coordination mechanisms will help to shape the threat landscape, with concepts like 'urban anti-drone domes' offering metropolitan-scale protection. Forensics plays a vital accountability role by enabling investigators to trace captured or destroyed drones back to their operators through serial numbers, GPS data, communication packets or firmware. However, this process is often hindered by damage, encryption or deliberate erasure. Together, these soft and hard measures represent a multi-layered response that balances suppression and destruction with regulation and attribution.

The effectiveness of drones in warfare makes them an attractive potential tactical solution for kinetic strikes against criminal gangs. This paper briefly considers the legal, moral and practical implications of this approach, ultimately recommending against it, citing Haiti as the clearest example of where drones are causing more problems than they solve.

For responses to be effective, they will require legal clarity, the targeting of technical enablers, transnational intelligence cooperation and proportionate surveillance. Combining interdiction with disruption and demand reduction can raise the operational costs of drone smuggling, rendering it less viable. Conversely, piecemeal or poorly coordinated measures will rapidly be outpaced by criminal innovation.

Key findings

- Organized crime is using drones extensively, but in different ways in different places. A one-size-fits-all approach to responses is not appropriate.
- The Russo-Ukrainian war has led to technological advances in drone capabilities, which organized crime groups are adopting. We may be witnessing the prodromal signs of an underworld paradigm shift.
- Drones have criminal applications in the spheres of smuggling, reconnaissance and assassination, but each domain – land, air and sea – has its own specific challenges and constraints.
- Evaluating the use of drones by criminals through the framework of the functions in crime allows for a more thorough analysis of where law enforcement can truly make an impact and where they will offer only minor gains.
- Consultations with drone operators in Ukraine reveal that human expertise remains at the heart of the capability and a vital point of intervention. Engineers, workshop operators, parts suppliers and firmware modifiers are all vital for scaling up the use of drones. Unmanned systems also rely on skilled technical networks, particularly pilots. Couriers, spotters and coordinators play a critical role in marking drop zones and retrieving payloads.
- The widespread availability of commodified components, such as batteries, motors and autopilots, on online marketplaces significantly reduces the barriers to entry for aspiring operators.
- Responses must be multi-layered and cross-domain, adopting an integrated approach. Simply improving soft and hard defences around critical infrastructure is not sufficient. Other tools that should be employed include regulating critical drone components and commercial sales, enhancing forensics to improve tracing and reviewing the legal status of criminal drone use.

Legal and regulatory frameworks – European Union

There is no single criminal offence in the European Union (EU) that covers the misuse of drones. Instead, the EU has created a harmonized framework for the safe manufacture and operation of drones, leaving the criminalization of misuse largely to member states. Key EU instruments include the Commission Implementing Regulation 2019/947, which sets out the rules and procedures for operating unmanned aircraft, and the Commission Delegated Regulation 2019/945, which establishes product requirements and covers third-country operators. These regulations, overseen by the European Union Aviation Safety Agency (EASA), establish categories of drone operation (open, specific and certified); set requirements for registration, remote identification and geofencing; and specify the competence levels required of remote pilots. Breaches of these rules can result in administrative penalties and can be used as evidence in criminal investigations under national law.[8]

When drones are used to commit crimes, prosecutions are based on existing national criminal codes, rather than dedicated EU-level legislation. Offences include smuggling, endangering civil aviation, unlawful surveillance, weapons violations and breaches of privacy or data protection. Europol has noted the growing involvement of drones in organized crime, such as the smuggling of contraband into prisons or across borders, and law enforcement responses are coordinated at both the national and EU levels.[9]

In light of these threats, the European Commission published a policy document on countering malicious drone use in 2023, setting out a roadmap for EU-wide coordination. The communication emphasizes the need for member states to develop clear frameworks for detection technologies and on the lawful use of counter-unmanned aircraft systems, including measures such as jamming or neutralization, to prevent potential interference with aviation safety and telecommunications. It also calls for closer cooperation between the EASA, Europol and national authorities to ensure proportionate and safe responses to drone incidents.[10]

In practice, only authorized state services, such as the police or military, are permitted to use active counter-drone measures, with private actors generally being prohibited from doing so. The EU's role is therefore to harmonize aviation safety rules and support cross-border coordination, while the criminalization of drone misuse remains the responsibility of national law, supplemented by EU instruments in the context of terrorism and organized crime. ■

INTRODUCTION: WAR THE INNOVATOR, CRIME THE BENEFICIARY

Wars act as crucibles of innovation, compressing years of technological, organizational and scientific development into mere months. In conditions of existential urgency, governments and militaries throw vast resources into experimentation, while necessity drives creativity and risk-taking at a scale not seen in peacetime. The resulting breakthroughs rarely remain confined to the battlefield; once the conflict ends, these innovations diffuse into wider society, reshaping economies, daily life and even cultural expectations. From Florence Nightingale to the internet, the methods and technologies developed in war have continually redefined our civilian experience.[11]

But each transfer of technology also carries with it unintended consequences. The same GPS that revolutionized navigation has enabled smugglers to plot illicit trafficking routes through deserts and jungles.[12] Night-vision devices, once the preserve of elite military units, are now in the hands of poachers and organized crime groups, who exploit them to evade rangers in wildlife reserves.[13] Facial recognition software, refined in counterinsurgency, is now being used by authoritarian regimes and organized crime for surveillance, tracking and scams.[14]

Since Russia's full-scale invasion of Ukraine in February 2022, the world has entered into another evolutionary cycle. This time, the focus of innovation has been on a form of technology that came of age during the Afghanistan and Iraq conflicts, and which was already commercially available: drones. Unlike traditional weapons development, which can take months or even years, the 'off-the-shelf' nature of drones meant they were a quick and inexpensive tool for the Ukrainian military in the early days of the invasion, when it was seeking to compensate for its materiel and manpower disadvantages.[15]

Since then, drones have undergone staggering levels of innovation in use and design. Commercial quadcopters have been adapted into precision strike platforms; fibre-optic guidance systems have transformed battlefields into webs of crisscrossing fibres; electronic warfare tactics are evolving in real time; and swarming experiments are pushing the boundaries of what unmanned systems can achieve alongside AI. First-person view (FPV) drones now account for 60–80% of frontline strikes, drastically reducing reliance on artillery. Notably, Ukrainian forces have carried out the first fully unmanned assaults, using a combination of ground-based kamikaze platforms and aerial drones to seize enemy positions without incurring infantry casualties.

There have also been significant advances in long-range strike capabilities. Aerial drones can operate over distances exceeding 1 200 kilometres and deliver warheads weighing up to 120 kilograms. Laser-equipped UAVs provide precise target designation for artillery and aviation munitions. Drone boats and other unmanned naval systems have been used in attacks on high-value targets, including Russian flagship vessels and radar installations. Robust mesh network technologies and resilient communication systems allow the continuous coordination of drone swarms and ground robots, even under electronic warfare disruption, facilitating large-scale, multi-platform operations with enhanced redundancy and situational awareness. [16]

At the same time, criminal gangs have moved quickly to exploit the accessibility and adaptability of drone technology (see Figure 1). These developments have enabled them to reduce personnel risk, innovate across domains (air, land and sea) and bypass traditional patrol and surveillance regimes. Their methods range from small quadcopters carrying heroin or methamphetamine to adapted industrial UAVs and autonomous underwater vehicles designed for the bulk transport of drugs.

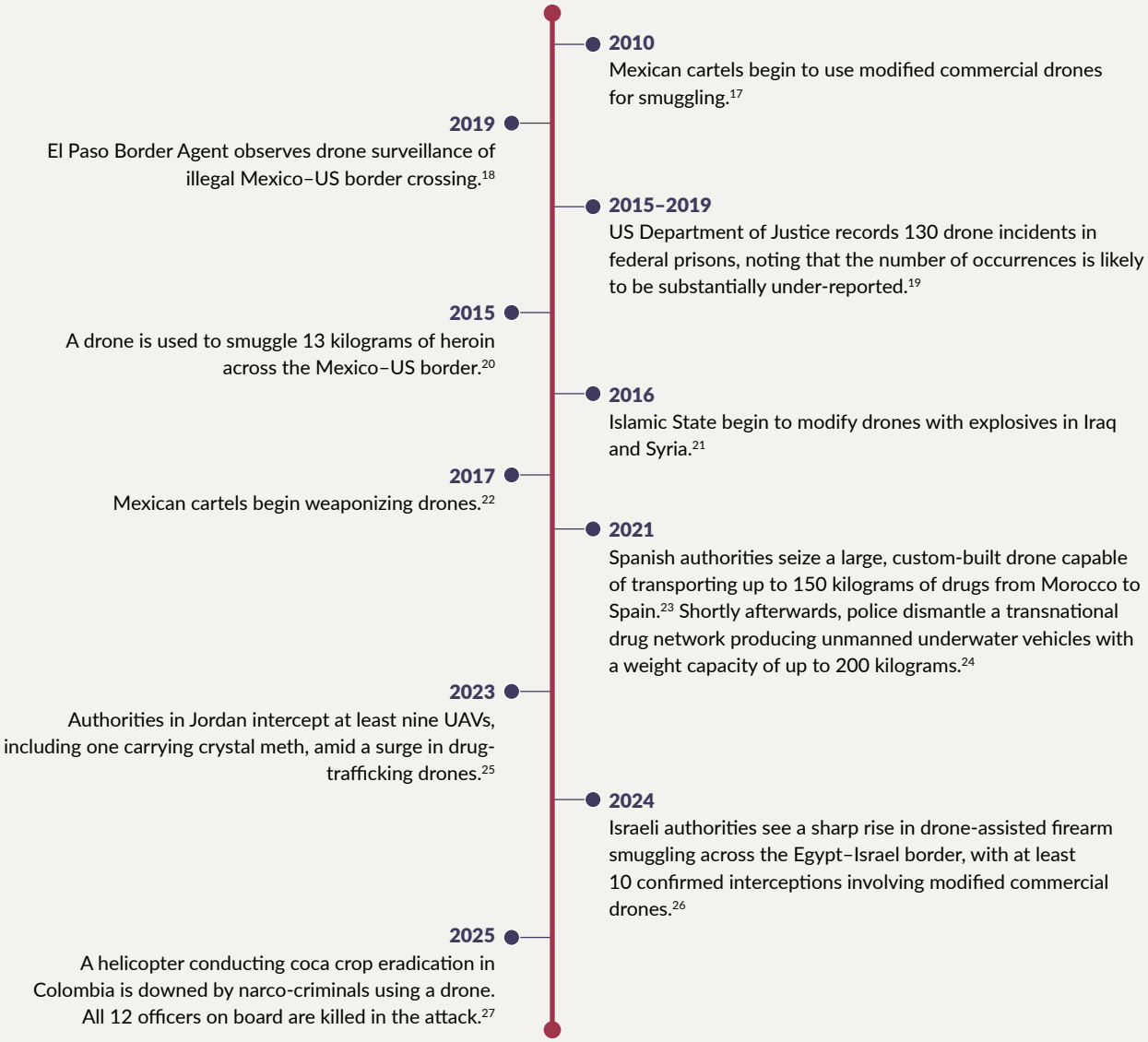

FIGURE 1 Notable cases of drone deployment by organized crime.

It seems likely that criminals will learn from the Russo-Ukrainian war to enhance and develop their own use of drones. But how? And what can be done to mitigate these risks? This report aims to map these two spheres – criminal and military – onto one another, in an attempt to answer the question: How will transnational organized crime gangs utilize the skills, experience, techniques, tactics and technological advances relating to drones that result from the Russo-Ukrainian war?

The GI-TOC engaged with serving drone pilots and operational practitioners in Ukraine to gather their insights into the potential use of drone technology by organized crime. In a systematic approach, the participants were presented with illustrative scenarios: the smuggling of 30 RGD-5 grenades, the delivery of a cargo of AK-47 rifles and the targeted elimination of competitors or protected individuals. These examples were chosen because they reflect current criminal actions and allowed law enforcement and policymakers to assess the feasibility, trade-offs and vulnerabilities of interventions without providing operational instructions.

Building on these scenarios, a structured set of questions were designed to draw out practitioners' judgements about enablers, constraints and adaptation pathways. Further questions explored the maritime and ground domains, illuminating the use of marine drones for sabotage, piracy or magnetic cargo attachment, as well as the operational limits of ground drones in different terrains and with varying payloads. Short-term technological trajectories were also probed, including likely innovations in automated assembly and the reliability of drones under hostile electronic or environmental conditions.

The final section of questions focused on countermeasures and forensics, including the future of interception technologies, the effectiveness of jamming against larger drones and whether drones could be traced back to their manufacturing sources through components or additive processes. In each case, the focus was on practitioner assessments of plausibility, likelihood and points of intervention, rather than operational detail, ensuring that the insights gathered could inform risk assessments and policy discussions without compromising security.

The following section reveals the answers to these questions. It is important to note that these comments come from operators involved in the Russo-Ukrainian war, and that further research is required to determine how their knowledge of tactics, techniques and procedures can be mapped onto other geographical contexts.

FROM BATTLEFIELD TO CRIME: TRANSLATING DRONE EXPERTISE

Air domain

Smuggling RGD-5 grenades and AK-47s across a state border

The first two scenarios involved cross-border arms trafficking. The initial illustrative task was to smuggle 30 RGDs, a Soviet-era grenade now being mass produced domestically by Ukraine.[28] As a criminal commodity, these weapons are commonly trafficked already because they represent a good option for profit. While prices are a complicated metric, grenades are generally cheap to buy (US$10–US$30, depending on the region) and easy to acquire in Ukraine, and can be sold for much more in the underworlds of Western and Northern Europe, particularly in Sweden, where they sell for SEK1 500–SEK5 000 (€135–€450).[29] They are also easier to disguise than firearms, being lighter and less bulky.

The weight of the cargo determines the type of drone for the task. Our interviewees advised that with each grenade weighing 310 grams, the craft would require a payload capacity of at least 10 kilograms. Law enforcement at the border should note that the launching station would need to be at least 20 kilometres from the border on both sides, giving a range of at least 40 kilometres, although up to 100 kilometres would be likely, and the operation would be conducted at night. Taking these considerations into account, efforts should focus on interdicting a twin-engine aircraft-type UAV with a flight time of 4.5 hours. This type of drone has the added benefit of a lower noise signature than multi-rotor drones due to its electric motors. These specific UAVs can be obtained commercially or through illicit channels, but criminals could buy some components and 3D print the rest, before hiring an engineer to assemble them.[30]

In terms of personnel, three or four people would be sufficient: two ‘senders’ and one or two ‘receivers’, who could communicate through an encrypted messaging service such as Signal to share information such as timings and drop-off coordinates. To maximize anonymity, an experienced drone pilot would pre-programme the UAV for autonomous flight, and either drop the load using a small parachute before returning or treat it as a one-way mission and land it at the drop-off point for probable immediate destruction.

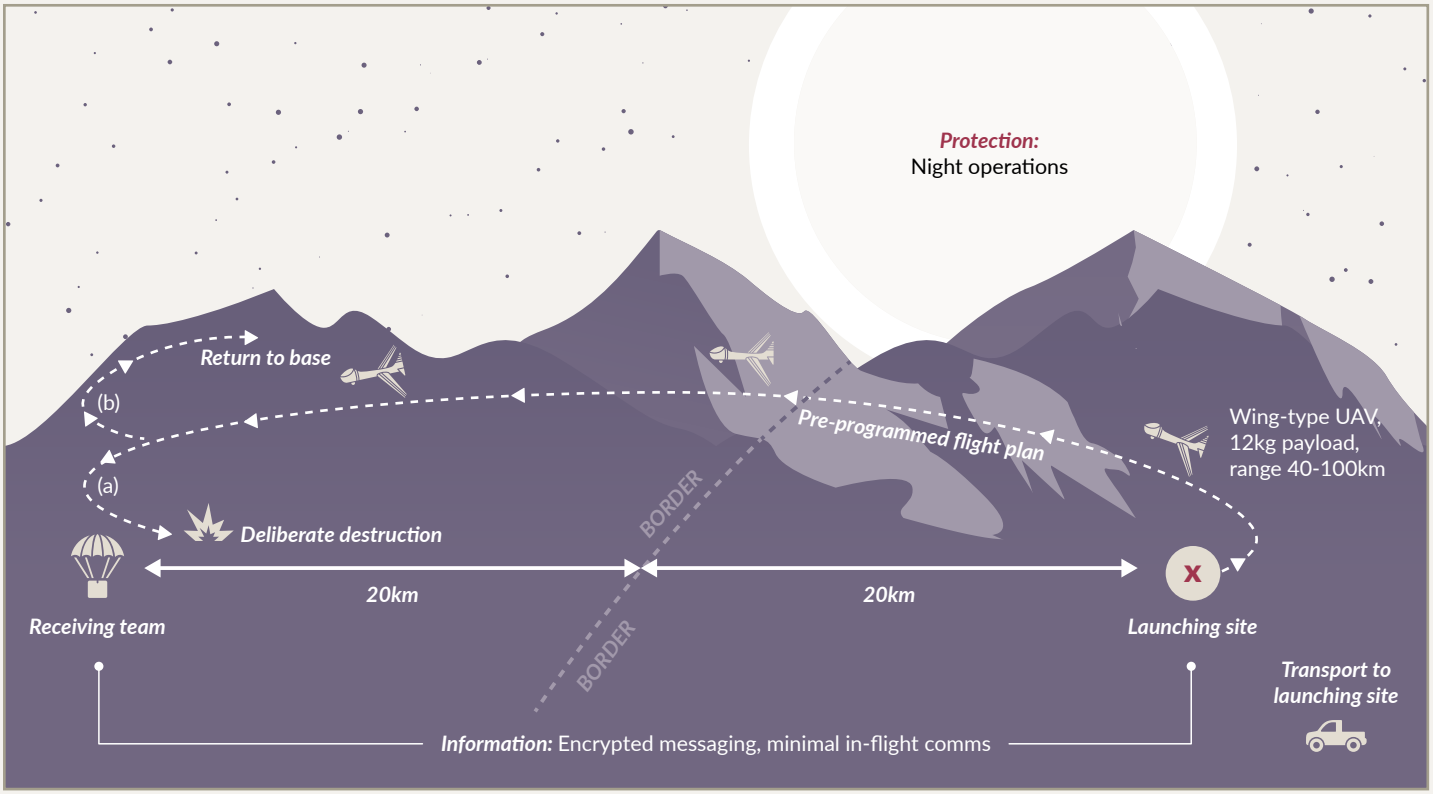

FIGURE 2 Example of a cross-border drone smuggling operation.

Operational costs would vary from approximately US$5 000 to US$10 000, depending on the type of drone used, transport to the launch site and other logistics.[31] This means that, although the experts deemed the operation entirely feasible, it would not be financially viable for criminals, particularly if the drone were destroyed after making the delivery. Smuggling tobacco, by contrast, would be more profitable, as cigarette cartons are lighter, bribes could be avoided and the risks would be far lower.[32] Drug smuggling would also have a more favourable profit margin.

The second scenario involved transporting 10 AK-47 rifles. These are a common commodity on the black market, and command a higher price than grenades. However, this drone operation would be far more complex to undertake due to weight constraints, with each rifle and full magazine weighing approximately 6.5 kilograms. While a single launch is theoretically possible with the right type of craft, such as a multi-copter or hexacopter, these are very noisy and noticeable, which would increase the ease of detection in Ukraine's border regions.[33]

Criminals could use the same wing-type UAV used in the first scenario here. However, as each craft could only carry only one or two rifles with magazines, at least three launches would be required, each with a different take-off site and drop point. This, in turn, would necessitate dispersed planning, a larger logistical footprint and a more extensive reconnaissance phase involving mapping multiple routes, assessing drop zones and coordinating separate pick-up teams. The total operation would therefore require multiple UAVs, launch crews and recovery teams, each moving stealthily to avoid observation. In the views of our consultants, this method was extremely unlikely, given the risk of

AI-assisted hunter drones, such as this version operated by a drone unit with Ukraine's 13 Khartiia Brigade, offer possibilities for targeted assassination. *© Oleksandr Ratushniak/Reuters via Gallo Images*

capture.[34] It is interesting to note that this view, from a Ukrainian perspective, contrasts with the ongoing weapon smuggling by drone across the Egypt–Israel border, where the motivations to supply weapons into militant hands, and differing terrain, presumably outweigh the risks. Some reporting on this corridor has even stated that the profit margins on certain types of weapons makes it a financially lucrative activity.[35]

Targeted assassination using drones

In the third scenario, our interviewees considered how criminal actors would target a protected individual or competitor in an urban environment using FPV or AI-enabled drones. This undertaking would require far more operational planning than the smuggling of criminal commodities. Reconnaissance, possibly over several days, would be essential to identify the target's routines, offices and vehicles. This could be carried out either using a drone or by a human surveillance team, which would need to be highly trained to avoid detection by the target's security detail. Our research indicated there would likely be both: two to operate the drone and six to conduct round-the-clock surveillance, resulting in much higher costs for the criminals and more opportunities for disruption.

Once the reconnaissance phase is complete, the team and equipment would need to be moved into position at nearby premises, potentially at more than one location if the drone is to be controlled remotely. It would be possible to control the drone from another city using Starlink. Communications would be encrypted and distributed through Starlink or other resilient channels.

As seen in Mexico, a strike quadcopter would be loaded with a thermobaric, anti-tank or fragmentation charge. If the target's environment had electronic warfare systems in operation, a fibre optic model would be possible, but highly challenging to pilot in a crowded urban area.

During the strike phase of the operation, the drone could be piloted by a human operator working with the surveillance team, or it could be used in AI-assisted 'hunter mode' to track licence plates and people autonomously, or even to strike a pre-identified target, such as an office door or window, at up to 20 kilometre range. The human-piloted option offers advantages for law enforcement, as the drone would transmit a detectable signal, although frequency-hopping or use of fibre-optic guidance could affect this. The AI-assisted 'hunter mode', a novel technology, would disadvantage the criminal due to higher cost, difficulty accessing the software and unreliability, although each are becoming less of an impediment. Due to the variables and complexities of a strike operation, especially with regard to personnel, overall costs varied significantly. In theory, hiring a hitman or using a different mechanical method, such as a remote-controlled explosion, could be cheaper. Nevertheless, the messaging impact of a drone assassination would be significant, and the operation would be a real display of criminal reach and power. It may also be the only way to access highly protected targets, such as prominent political figures and businesspeople.

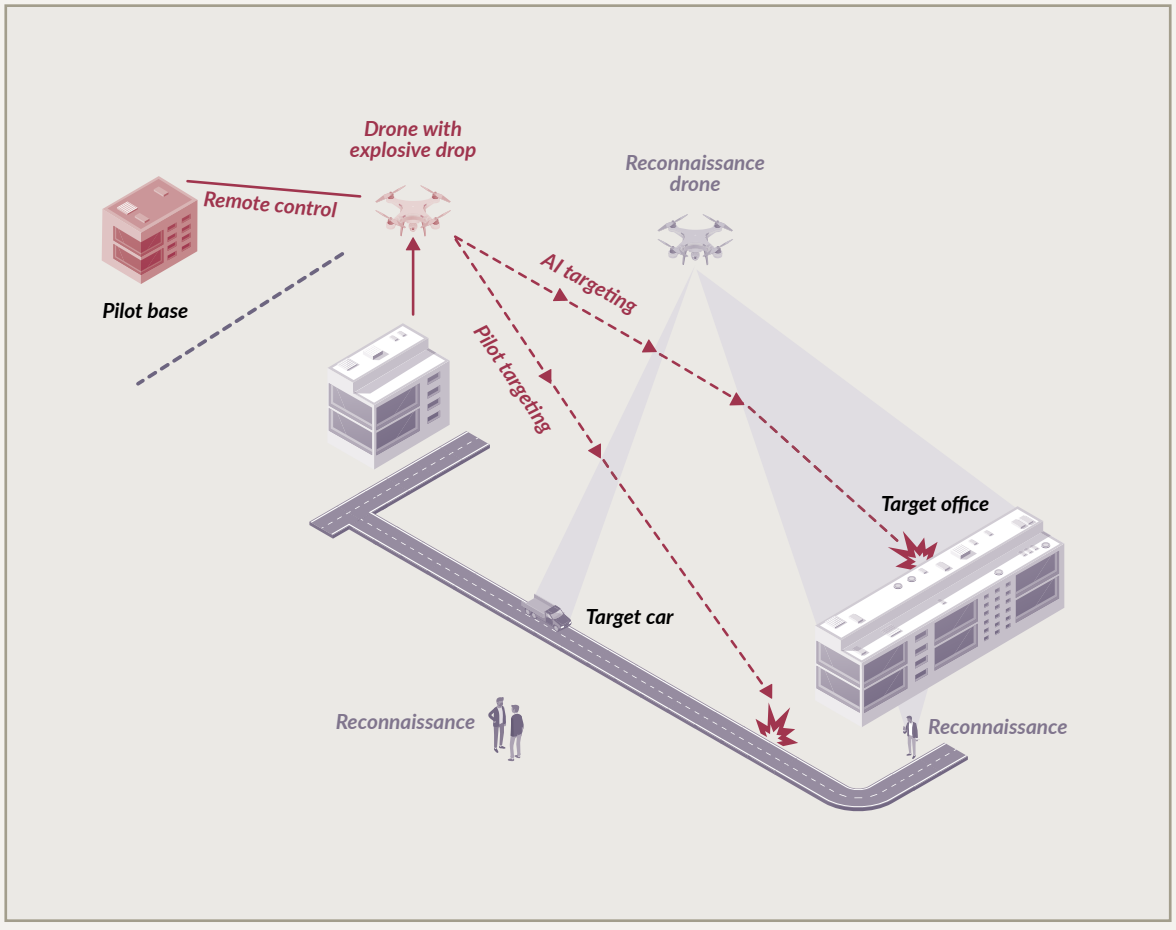

FIGURE 3 Example of a drone assassination operation.

Land domain

Unmanned ground vehicles (UGVs) are among the oldest forms of drone technology, with a notable example being successfully tested in 1941.[36] However, their development has accelerated dramatically in Ukraine, where they have become increasingly important for resupply, rescue, reconnaissance and even strike operations. Small land drones are used as kamikaze vehicles to deliver explosives, while weaponized versions can be equipped with machine guns, grenade launchers and rocket-propelled grenades (RPGs), and can even carry integrated FPV drones.

Ukraine's Lyut (Fury) tactical unmanned ground vehicle attacking Russian soldiers, July 2025. For organized crime, drones like this could provide extraordinary lethal capacity with minimal risk. *Photo: Main Directorate of Intelligence of the Ministry of Defence of Ukraine, Telegram, 14 July 2025, https://t.me/DIUkraine/6429*

In civilian life, land drones are used for purposes such as food delivery, disaster relief and law enforcement operations. For criminals, they represent a novel way to smuggle contraband or place objects such as drugs, explosives and weapons, or to attack competitors or law enforcement without endangering their own personnel. They have the capacity to cover large payloads: currently, small drones can carry 10–20 kilograms, medium drones up to 200 kilograms, and large drones over 200 kilograms. Caterpillar-tracked drones are less likely to get stuck on rough terrain than wheeled drones.

Armed land drones could effectively act as foot soldiers for organized crime groups, pushing out competitors and claiming territory in street battles. They may be especially effective in this role because of their size: it would, for instance, be possible to conceal some variants in the back of a van. In 2024, the Chinese army mounted an automatic rifle on a robotic dog – a quadrupedal UGV that can handle more diverse terrain and is even smaller than wheeled variants.[37]

Land drones also come with constraints. Most can only operate effectively on firm terrain with minor irregularities, at speeds of 15–30 kilometres per hour, within 10 kilometres of a control point, and with an overall travel envelope of approximately 20 kilometres, depending on payload and conditions.[38] Reliable communication across irregular terrain is also a challenge. Unlike aerial platforms, which benefit from a relatively unobstructed earth–sky signal path, ground drones face persistent breaks in line of sight caused by depressions and surface variations. For criminal networks, exercising command through remote operators would therefore depend heavily on securing robust communication links, whether by line of sight, repeater systems or tethered fibre optics. These links would be central to the operation, and the command nodes of the operators, relays and control software would be key points of intervention for law enforcement. However, land drones are less sensitive to communication cut-outs than aerial platforms. While an aerial drone may crash if it loses communication with the pilot for even a few seconds, many land drones have protocols to deal with a temporary loss of signal.

Land drones, like this dog reconnaissance drone, can be delivered by aerial platforms to desired locations. Conversely, land drones can also deliver aerial drones. *© Bay Ismoyo/AFP via Getty Images*

ADVANTAGES	DISADVANTAGES
Can operate day or night	Difficulty in maintaining signal; Starlink an option[39]
Can operate in any weather	Limited range
Can tolerate temporary lost communication without system failure (as with air drones)[40]	Requires relatively level ground
Heavy payload	Wheeled variants liable to get stuck
Possible to 'daisy chain' drones – land drones deliver air drones, air drones deliver land drones	Slow and easy to intercept

FIGURE 4 Advantages and disadvantages of land drones.

Sea domain

Maritime drones have been at the forefront of Ukraine's efforts to roll back Russia's naval presence in the Black Sea. Due to their size and capabilities, they also present significant opportunities for smuggling. They can operate at distances of between 800 and 1 100 kilometres and transport payloads from 300 to 650 kilograms. To avoid detection, most sea drones are relatively small, with a maximum length of 8–9 metres, whether operating under or above water. While long-distance routes such as the Latin America–West Africa–Europe cocaine corridor are out of range, drones could execute 'small hops' in the Caribbean, the Mediterranean and littoral regions. They could also conceivably be launched from motherships at sea to complete the final leg of a journey to shore.

Ukraine's Magura sea drones, which have been used to attack and destroy Russian ships in the Black Sea, offer various possibilities for smuggling, although their high cost is a prohibitive factor. *© Danylo Antoniuk/Anadolu via Getty Images*

Law enforcement must also consider that such platforms could also be used for maritime piracy. In Ukraine, unmanned boats have been fitted with remotely operated weapons, including large-calibre machine guns and anti-tank guided missiles, as well as automatic grenade launchers, with a calibre of up to 50 mm, and small air-to-air missiles.[41] This, however, would not be sufficient to threaten bulk carriers, container ships and oil tankers, which are common targets for pirates, particularly in the waters off the coast of Somalia, the Singapore Strait, Indonesia and the Gulf of Guinea.[42] Instead, criminals may resort to the threat of suicide drones, which could deliver an explosive payload of up to 500 kilograms. The analysts also emphasized various technical limitations: platform stability, weapon weight and target size all reduce the likelihood of small unmanned systems realistically capturing or decisively disabling a large tanker or container vessel in open water. Marshalling multiple boats to strike targets in the high seas would require considerable operational planning, and would be difficult to execute without being detected.

Experts deemed the prospect of using underwater drones to attach magnetic cargo to the hulls of ships while they are at anchor – a technique known as 'parasite smuggling', which is already carried out by human divers for criminal purposes[43] – unfeasible. Such operations would require expensive, high-tech equipment and would be extremely complex to carry out. The drones themselves are also very expensive: the Magura-class drone, for example, which Ukraine has used to attack and destroy Russian ships, costs around US$250 000–US$300 000, while the Sea Baby costs around US$220 000.[44] Nevertheless, this is still cheaper than many long-range missiles. A similar logic may apply to activities such as cocaine smuggling: 500 kilograms of cocaine smuggled by maritime drone would be worth approximately £12.5 million (US$16.8 million) wholesale in the UK.[45] The method would also allow for far greater control than container shipping, where drugs have to leave criminal hands, albeit with the payoff of very low interdiction rates.

The prospect of criminal control may also make sea drones an attractive option for arms trafficking, particularly if the craft could ferry illicit commodities back on the return journey. With a payload of 650 kilograms, a drone could carry 100 AK-47s with magazines or the same number of 72 mm RPG-32s – a serious proposition, and one that may be appealing to some of organized crime's customers, such as terrorists and non-state actors.

ADVANTAGES	DISADVANTAGES
Large payload	Complex operations
Long range	Attack potential limited against maritime targets
Difficult to detect	Expensive

FIGURE 5 Advantages and disadvantages of sea drones.

AI, swarms, automation – Drones of the future

The example of the assassin drone in 'hunter mode' above illustrates the growing significance of AI in UAV technology. Ukrainian forces have deployed drones equipped with machine vision and AI to enhance autonomy, target acquisition and resilience against electronic warfare. A notable example of this trend is the TFL-1 guidance module from The Fourth Law, a Ukrainian drone autonomy startup, which enables drones to identify and engage targets independently. This reduces the number required per mission, dramatically improving operational efficiency. Simultaneously, the integration of traditional weapons, such as 60 mm mortar rounds, into FPV drones has produced rapid-deployment strike systems capable of coordinated aerial and ground missions. The operational impact of Ukraine's drone developments is profound. Machine learning algorithms are also being applied to battlefield imagery, signals intelligence and logistics optimization.

Tools developed for analyzing drone footage or coordinating artillery fire are rapidly finding their way into civilian life, from medical diagnostics to self-driving vehicles. Automated drone swarms are already being used in civilian and combat contexts alike. Although challenges remain, the technology has proven reliable in a variety of applications, ranging from advertising to complex coordinated operations. However, these technologies bring with them immense potential for criminal exploitation. ■

ANALYSIS BY FUNCTION: OPPORTUNITIES FOR COUNTERMEASURES

Our grassroots research with Ukrainian drone pilots yielded two crucial findings. While this report discusses drones as a proliferating technology, its focus is ultimately on people. It is humans who provide the expertise, experience and knowledge to pilot the machinery. The criminal use of drones must be examined from the perspective of the human operator adapting the technology to their use, as well as the human victim, be that a border guard unaware of the smuggling drone flying overhead or the unsuspecting target of an assassination sitting in the back seat of what they think is a protected car.

The other key point raised by the consultants was the importance of organization. To harness the full potential of drones, you not only need the right people, but also an operational framework to form and execute your plans.

In order to conceptualize how organized crime may use drone technology, this paper therefore draws on a military operational framework. As warfare became increasingly complex, combining artillery, infantry, cavalry, engineers and logistics, militaries have long faced the problem of how to organize, arrange, sequence and coordinate activities and actions for maximum effect.[46] Napoleon innovated by creating corps,[47] self-contained 'mini armies' that coordinated each of the components for battlefield success. They operated under a doctrinal framework that has evolved over time into a model of tactical functions that guide the planning and execution of operations. These functions are:

- **Command**, which orchestrates forces and ensures cohesion;
- **Intelligence**, which collects, analyzes and applies information to anticipate threats and opportunities;
- **Movement and manoeuvre**, which positions forces to gain advantage;
- **Protection**, which safeguards personnel and resources;
- **Fires**, which project physical or psychological coercion;
- **Logistics and sustainment**, which secure and deliver the necessary resources; and
- **Information**, which integrates communications, influence and situational awareness across the battlefield.

Together, these tactical functions allow military forces to act flexibly and decisively, even in conditions of uncertainty and friction.[48] When adapted for the study of organized crime, they can be reframed as 'functions in crime'. In this context, 'command' governs illicit operations and the coordination of criminal networks; 'intelligence' identifies vulnerabilities in targets, competitors and state enforcement; 'movement and manoeuvre' enable the transport of goods, people and capital across borders and jurisdictions; 'protection' safeguards both personnel and illicit assets; 'fires' represent strike, coercion or disruption, whether physical, digital or psychological; 'logistics and sustainment' ensure continuous access to materials, technology and operational infrastructure; and 'information' functions as both connective tissue and a tool for deception, control and influence.

This recast framework offers a systematic understanding of how organized crime organizes itself to maximize effectiveness. In addition, it facilitates an analysis of how drone technology is changing the way illicit networks operate.

MILITARY TACTICAL FUNCTION	MILITARY MEANING (SHORT)	EQUIVALENT FUNCTION IN ORGANIZED CRIME	CRIME MEANING (SHORT)	KEY DIFFERENCES/ CONCRETE EXAMPLES/ INDICATORS
Command	Orchestrates forces, issues orders, ensures cohesion and unity of effort	Command/ leadership	Governs illicit operations, sets strategy, manages networks and alliances	Crime leaders operate more through networks, proxies, bribery and secrecy than formal chains of command. **Examples:** crime bosses, cartel councils, gang leaders. **Indicators:** coordination of concurrent actions, sudden reorganization after arrests.
Intelligence	Collects, analyzes, applies information to anticipate threats and exploit opportunities	Intelligence/ reconnaissance	Identifies vulnerabilities in targets, law enforcement activities, competitors, supply chains	Emphasis on clandestine collection (informants, hacked data, surveillance) and tradecraft. **Examples:** insider access to ports, corrupt officials, open-source monitoring. **Indicators:** targeted timing of operations, use of stolen documentation.
Movement and manoeuvre	Positions forces to gain advantage; deploys units across terrain	Movement and logistics of people/ goods/capital	Transport of drugs, weapons, people, money across jurisdictions and through controls	Focus on concealment, legal cover (front companies), routing to exploit jurisdictional gaps. **Examples:** smuggling routes, money-laundering circuits, human trafficking corridors. **Indicators:** use of shell companies, trans-shipment hubs, false manifests.

Protection	Safeguards personnel, critical assets, maintains survivability	Protection/ security	Protects people, property and revenue streams (physical security, legal/ financial shields)	Includes corruption, intimidation, violence, legal obfuscation and cyber protections. **Examples:** armed guards, safe houses, payoffs to officials, encrypted communications. **Indicators:** repeated successful evasion of prosecutions, encrypted communications platforms.
Fires	Projects physical or psychological coercion to neutralize or deter	Coercion/ disruption (physical, digital, reputational)	Use of violence, threats, sabotage, cyber-attack or smear campaigns to control or eliminate obstacles	May be political, commercial or interpersonal. Unlike military fires, they are often targeted at civilians, witnesses or rivals. **Examples:** assassinations, arson, DDoS, doxxing. **Indicators:** spikes in violent incidents linked to disputes or enforcement actions.
Logistics and sustainment	Secures and delivers supplies, ammunition, fuel, maintenance to sustain operations	Logistics and sustainment (criminal supply chains)	Ensures continuous access to goods, cash flow, equipment, safe houses and technical services	Highly decentralized, reliant on illicit markets, front businesses and corrupt supply nodes. **Examples:** precursor chemical procurement, arms sourcing, cash couriers, money-laundering networks. **Indicators:** complex supplier webs, recurring shipments just below inspection thresholds.
Information	Integrates communications, influence, situational awareness across battlefield	Information and influence	Communications, propaganda, deception, market/ partner management, controlling narratives to enable operations	Uses both classic influence (bribes, media manipulation) and modern tools (social media, encrypted channels). Often blends misinformation with operational security. **Examples:** rumours to intimidate witnesses, fake documents, social media campaigns. **Indicators:** coordinated messaging around events, rapid spread of smears or false claims.

FIGURE 6 Tactical functions mapped to functions in crime.

The interviews conducted during this research sketched an outline of how criminal groups might exploit unmanned systems in the future. When fed through the 'functions in crime' framework, however, they form a coherent and worrying picture. At the heart of the findings is the simple prediction that drone use by criminals will become more widespread. Better communications and cheaper, more accessible production methods are already reshaping command, information and logistics, while movement, protection and the application of force adapt around these changes.

A more detailed assessment of these functions reveals nuances about how criminal organizations may evolve their operations thanks to drones, as well as highlighting their potential vulnerabilities to law enforcement responses.

Command, for instance, is becoming untethered from geography. While commanders once needed to be close to their assets, modern communications architectures, such as chains of relay control stations, covert forward nodes and direct satellite links, make it feasible for an operator to task a drone from a location thousands of kilometres away.[49] A single operator sitting behind a consumer device can now receive high-quality video streams and send precise commands, and commercial mobile phones with the right software are explicitly described as viable control terminals.[50] This resilience is attractive to criminal networks: placing redundant control nodes or using a mix of cellular and satellite backchannels preserves continuity of operations even if one node is disrupted.[51] It also lowers the barriers to entry. However, relay stations must be placed in territory that the group can access, a hard constraint that necessitates risky clandestine emplacement or reliance on permissive environments. Furthermore, the use of commercial services leaves observable footprints in the form of device activations, SIM usage patterns and persistent data flows.[52]

Intelligence also undergoes a step-change thanks to drone technology. High-quality telemetry and video links enhance situational awareness, providing criminal actors with a continuous intelligence-gathering capability in both urban and rural environments. In Skopje, North Macedonia, even minor criminal groups, such as those organizing illegal street races, have adopted drones for the surveillance of traffic police. By monitoring from above, they can identify safe windows in which to conduct races and place bets.[53] On land, dog drones demonstrate how quadrupedal platforms can navigate complex terrain. These vehicles, along with tracked or wheeled ground drones, can also be used to scout targets, assess law enforcement presence and identify vulnerabilities. However, constraints such as topography, noise and signature make ground reconnaissance by UGVs less plausible.

Movement and manoeuvre are being reframed, as the range, weight, reliability and security (for the criminal) have all improved. Drones that once required line of sight can now be pushed beyond visual range through chained control stations, and satellite-enabled FPV craft can be piloted from almost anywhere.[54] While maritime unmanned systems are generally smaller to reduce detectability, they can still cover hundreds of miles and carry substantial payloads. However, movement is not limitless. Relay approaches require forward nodes, and systems must contend with terrain, sea state, currents and the detectability of approach. These vulnerabilities constrain what is tactically feasible,[55] and the environmental and geographic constraints create predictable windows of opportunity for defenders. Moored vessels, constricted coastal approaches and the physical locations where relay hardware must be installed all concentrate risk in time and space, offering options for investigation and disruption.[56]

Protection for illicit operations is increasingly reliant on plausible deniability, forensic awareness and dispersal.[57] Criminal groups exploit everyday commercial technologies and unregulated sales platforms, such as consumer phones, cash purchases of 3D printers and online marketplaces selling second-hand drone equipment.[58] While these practices reduce straightforward traceability, they do not erase patterns. Large-scale or repetitive purchases, unusual cash transactions tied to specialist sellers and the emergence of workshops or adverts

seeking skilled technicians betray underlying sustainment networks. Moreover, the demand for skilled engineers, airframe designers, radio frequency (RF) systems and control software creates human intelligence vulnerabilities. Expertise is a force multiplier, but it is also a point of leverage for investigators.[59]

The fires function, the application of coercive force, is already being improved by unmanned systems, although with one important caveat. Aerial FPV drones and surface/underwater craft can deliver explosive payloads or mount small, remotely controlled weapons. This gives criminal actors a means of inflicting harm while keeping personnel at a remove.[60] However, current systems are largely semi-automated and rely on human operators to designate targets, meaning the most advanced threat vectors still require manual intervention. Perhaps most importantly, fully autonomous swarming and self-targeting capabilities remain immature.[61]

Logistics and sustainment form the practical backbone of these capabilities and reveal where disruption can be most effective. The consultations indicate that plastic frames and small components can be cheaply and locally produced using consumer 3D printers and commonly available parts. In contrast, metal additive manufacturing remains prohibitively expensive for most actors.[62] Turnaround times of weeks to a month for new components and systems, and the wage structures of production crews, suggest that creating and maintaining an effective strike capability is not an immediate process; it requires a supply chain, workspace and skilled technicians.[63] These dependencies generate multiple intervention points, such as supply-chain monitoring, partnerships with sellers and marketplaces, and targeted action against specialist procurement flows, all of which raise the cost and friction of sustained operations. Ground drones can form part of a wider logistical chain in illicit operations, particularly in difficult or contested environments where human couriers are at risk. However, the limited endurance of most current platforms creates a dependency on battery management and charging infrastructure, which is itself a logistical vulnerability for organized crime groups.

Finally, information – the glue that binds everything together. High-bandwidth video feeds, telemetry and command channels provide operators with rich situational awareness and enable agile, adaptive operations.[64] However, these same information flows traverse commercial networks, satellite providers and public infrastructure, creating opportunities for detection and disruption. Persistent uplinks, satellite terminal activations at unusual times or in unusual locations, and clusters of encrypted, low-latency traffic that map onto known drone activity can all serve as early warnings. By focusing efforts at the intersection of information flows and logistics – the moment a satellite terminal is installed, for example, or a series of SIM cards used to support continuous uplink – law enforcement can gain disproportionate leverage.

The emphasis on telemetry, video and communication reliability highlights the importance of information for command, intelligence and fires alike. Developments such as fibre optic tethers aim to preserve data integrity and minimize the risk of electronic interception, while repeaters extend the information network across terrain. Criminal groups that master these information flows will gain the ability to coordinate the more complex, multi-functional uses of ground drones.

Taken together, the consultations presented a threat-scape that is plausible and concerning, but not unconstrained. Criminal groups may adopt more resilient remote command systems, manufacture airframes locally more easily and maritime unmanned systems tactically to threaten vessels, especially when moored. However, geography, physics, cost and the continuing immaturity of fully autonomous targeting systems impose hard limits. Those responsible for defending against these developing threats should focus on the highest-value levers where communications, procurement and physical vulnerability overlap. This includes monitoring unusual satellite and cellular activations, tracking specialist component flows through marketplaces, strengthening the security of ships and ports during predictable vulnerability windows, and building cross-sector intelligence partnerships that fuse telecoms, maritime and law enforcement data. In short, the future described by the consultants is neither unstoppable nor invisible; it is a landscape of new capabilities that create fresh detection opportunities for those looking for the right signals in the right places.

SCENARIO	UAV TYPE/ PAYLOAD	FUNCTIONS IN CRIME (WITH DESCRIPTION)	LAW ENFORCEMENT COUNTERMEASURES
Smuggling RGD-5 grenades	Wing-type UAV, 12 kg payload, parachute drop	**Command:** small team coordinates launch, drop and fallback **Intelligence:** reconnaissance of terrain, drop sites and border patterns **Movement and manoeuvre:** autonomous flight and precise parachute delivery **Protection:** dispersed personnel, night operations, drone self-destruction **Fires:** grenades as potential coercive payload **Logistics and sustainment:** UAV assembly, battery management, transportation **Information:** encrypted messaging, minimal in-flight communication	Multi-sensor detection, UAV regulation, predictive monitoring of smuggling routes
Smuggling AK-47s	Wing-type UAV or multi-copter, multiple sorties	**Command:** coordinates multiple UAV launches and recovery teams **Intelligence:** evaluates law enforcement presence and safe drop points **Movement and manoeuvre:** sequential flights to deliver multiple rifles safely **Protection:** operational dispersion to reduce exposure **Fires:** AK-47s as coercive payload **Logistics and sustainment:** repeated UAV prep, battery and transport management Information: pre-flight coordination, encrypted communication	Multi-sensor UAV detection, monitor repeated launches, restrict access to heavy-duty drones
Targeted assassination	FPV/AI-assisted UAV, lethal payload	**Command:** pilot and surveillance team coordinated for strike execution **Intelligence:** target mapping, route analysis, vulnerability assessment **Movement and manoeuvre:** autonomous navigation through urban/rural terrain **Protection:** operator distance, minimized exposure through automation **Fires:** lethal payload delivered to target **Logistics and sustainment:** drone assembly, programming, payload prep **Information:** AI-assisted tracking, encrypted channels, situational deception	Professional counter-drone units, UAV regulation, multi-layered urban airspace monitoring (optical, RF, thermal, AI)

FIGURE 7 Functions in crime mapped to criminal drone use.

RESPONSES TO CRIMINAL USE OF DRONES

The future response to the criminal use of drones must incorporate a variety of detection technologies, countermeasure systems, legal frameworks and forensic capabilities. Threat mitigation will require a combination of soft and hard approaches, incorporating electronic suppression and physical destruction.

On the detection side, advances are being made in next-generation radar, acoustic sensors for sound recognition, optical and infrared systems, and radio frequency monitoring to capture control signals. These systems are increasingly incorporating AI, enabling faster and more precise classification of aerial threats. Together, these innovations form the basis of a dual-track response: the suppression of hostile drones through electronic warfare and their physical elimination through kinetic means.

Electronic warfare offers a soft line of defence. Systems that can jam unmanned system control signals, including satellite-based links, or interfere directly with internal circuits to seize control of enemy drones are being developed. This approach is particularly effective against large drones that lack advanced protection measures. However, more sophisticated drones require additional tools, leading to the refinement of hard destruction systems in parallel. These include traditional anti-aircraft weapons, dedicated interceptor drones and laser systems, which are already being tested on the front line. AI is being trialled not only for detection, but also for directing interceptors and laser weapons, enabling the autonomous pursuit and neutralization of criminal drones.

Alongside these, several more specialized countermeasures are emerging. While conventional machine guns, missiles and grenades remain effective, they are often prohibitively expensive. As a result, anti-drone missiles designed for this purpose are being introduced; India's Bhargavastra system is a prime example. Autonomous interceptors, such as the MARSS Interceptors, promise a rapid response time of under three seconds. Directed-energy solutions, including microwave weapons like Thor, Leonidas and the British Radio Frequency Directed Energy Weapon, can neutralize swarms of drones by emitting concentrated electronic pulses. Quantum radar, which generates entangled photons to penetrate stealth technology, is expected to be viably operational by 2025–2026.

Physical protection has also gained attention in the form of passive defence measures. Facilities vulnerable to attack by unmanned systems are experimenting with protective nets, false walls, double ceilings and specialized hangars, which are typically constructed at least two metres away from critical assets.

Beyond technology, the threat landscape will be shaped significantly by governance and regulation. Legislative measures such as flight restrictions, no-fly zones and identification schemes for civil drones are likely to become more widespread. Meanwhile, machine learning applications are being developed to analyze the behavioural patterns of drones, enabling authorities to predict hostile intent by studying previous incidents.

Institutional coordination is another cornerstone of the strategy for combating future threats. The establishment of interagency response centres linking military units, the police, civil aviation authorities and private security companies is gaining traction. This is reflected in the concept of urban anti-drone domes, which involves deploying integrated detection and interdiction systems across metropolitan areas to protect airports, power plants, government facilities and other critical infrastructure.

A complementary aspect of the threat response will lie in forensics. Even if a drone is damaged, investigators may be able to trace it back to its origin using various indicators. For example, serial numbers and component identifiers embedded in microchips, controllers or cameras often provide direct links to manufacturers and models, as is the case with commercial drone platforms such as DJI or Parrot. Flight logs and GPS data can typically be recovered after an incident, enabling the reconstruction of routes, launch and landing points, and even the associated photo or video metadata. Communication data, including MAC addresses, Wi-Fi SSIDs, MAVLink packets or SIM card information, could further aid identification.

Forensic analysis could also extend to cross-referencing manufacturer or importer databases, comparing recovered component serial numbers with production records and reviewing operator data synchronized with mobile applications or cloud services. The drone's own flash memory and firmware can yield valuable information, including launch locations. However, these processes are complicated by several limitations. For instance, severe damage may scatter or destroy key components, onboard memory may become corrupted or encrypted, and GPS functions may be disabled. Furthermore, cloud data can be altered, erased or rendered inaccessible by security protocols, and skilled operators may intentionally erase traces. The effectiveness of forensic attribution therefore hinges on the availability of data, the extent of physical damage, the levels of protection or erasure and the sophistication of investigative tools.

Taken together, these trends point towards a future in which threats are met with an integrated ecosystem of detection, suppression, destruction, regulation and forensic attribution. The interplay between emerging technologies, institutional coordination and investigative science will not only define the effectiveness of defence, but also the accountability mechanisms that underpin security in the drone age.

Fighting organized gangs with drones: a cautionary tale

In Port-au-Prince, Haiti, weaponized drones were touted as a quick fix, offering a cheap and precise way to attack gang leaders in their strongholds, which police and peacekeepers could not access. But the first months of strikes in 2025 told a different story. Reports from the city documented improvised munitions slung from modified commercial drones, scant transparency regarding targeting, and injuries to women and children, with authorities refusing to say who exactly was holding the controls.[65] From day one, analysts warned that turning a crowded capital into a drone battlespace would add 'fuel to a combustible conflict' and risk civilian lives; GI-TOC analysts described it as 'a very, very dangerous escalation'.[66] The fear was not theoretical. What appeared to be technological precision in video footage often concealed legal ambiguity and collateral effects on the ground.

These fears were realized on 23 September 2025, when explosions tore through a birthday gathering in Cité Soleil. At least 13 people were killed, eight of them children, according to witnesses and human rights groups. After 48 hours without any official explanation, expert observers were asking who, ultimately, would assume responsibility for the

attack: the prime minister? The Transitional Presidential Council? Private security companies? The leadership of Haiti national police?[67] In a city where gangs already mine mistrust, such opacity handed them a ready narrative: the state kills indiscriminately while hiding the chain of command. The strategic effect of this is perverse and unintended; every unclaimed strike that harmed civilians strengthened the criminal governance the drones are meant to erode.

Private military contractors exacerbate the problem. In March, Haiti hired Vectus Global, led by the American private security executive Erik Prince, to help coordinate drone strikes against the gangs controlling most of the capital. Media reports have detailed Prince's role and the controversies that shadow it.[68] Critics warned that outsourcing sovereign force to profit-seeking firms demands transparency regarding the rules of engagement and the legal authority to use lethal force, a level of openness that has not been achieved. The GI-TOC's own analysis states that, without clear oversight, private military contractors blur accountability, complicate cooperation with national police and international missions, and risk fuelling collusive, extractive practices rather than dismantling them.[69] Their use of drones will not reverse the lack of manpower, funding and governance on the ground.[70]

Legally, morally and practically, Haiti's use of drones to combat organized crime is a cautionary tale.[71] International human rights law requires necessity, distinction and proportionality in armed combat, but improvised airborne explosives over densely populated neighbourhoods invert this logic. Morally, families mourn their dead while officials issue no ownership of strikes, deepening the legitimacy crisis that gangs exploit. In practice, drones are not a strategy: without courts, custody and credible policing, kinetic effects are short-lived and encourage imitation, with gang leaders openly vowing to buy what the state buys. The arms race simply moves to the skies. Each headline-grabbing blast risks trading temporary tactical shock for long-term strategic loss.[72]

Forensic traceability and privacy in drone regulation

Blockchain: a solution to falsified logs?

A growing body of research is emerging on how blockchain technology could strengthen efforts to reduce the illegal use of drones by creating tamper-proof logs of flight data. These immutable records would provide regulators and law enforcement agencies with reliable evidence trails, lowering the risk of manipulation during criminal or hostile drone operations. Such systems could ensure compliance with no-fly zones, track cargo movements and maintain usage accountability. However, significant challenges remain regarding their scalability, overheads and real-time responsiveness.[73]

Experts have therefore proposed a general blockchain-based logging framework applicable across all types of drones, on the basis that trusted, decentralized records could prevent attackers from erasing or altering key forensic data.[74] At the same time, however, studies of existing industry practices demonstrate the potential for law enforcement. Researchers have reverse-engineered DJI's DroneID system, revealing critical vulnerabilities. DroneID transmits the unencrypted location data of drones and pilots, thereby exposing operators to tracking, spoofing and privacy risks. The experts identified 16 firmware vulnerabilities that could be exploited for remote code execution, denial of service or disabling safety features.[75] These findings highlight the fact that even dominant commercial platforms contain weaknesses that can be exploited.

This analysis reveals the tension between traceability and privacy in drone regulation. While current industry practices (such as DroneID) expose operators and infrastructure, blockchain logging could create stable, decentralized accountability. Both are beneficial for law enforcement. However, increased industry regulation could result in the backdoors in DroneID being closed, thereby closing off this particular forensic route. ■

Key lessons – what matters most

Several overarching lessons emerge. No single technology can solve the problem entirely. Detection, identification, tracking and lawful mitigation must be integrated into layered systems, as smugglers adapt quickly. Criminal networks scale primarily by resolving both engineering and supply chain challenges, suggesting that targeting fabrication hubs, engineers and component flows could cause disproportionate disruption. Legal and regulatory frameworks critically shape what countermeasures are feasible. Many effective mitigations require clear authorization and protocols. Intelligence gathering and regional cooperation are more effective than isolated solutions, particularly for transnational trafficking. Finally, robust evidence collection and prosecution can create a deterrent effect by linking recovered flight logs, payload traces and operators to meaningful legal outcomes.

Recommendations

The following recommendations are not just aimed at law enfocement officers and border security. They apply equally to those considering physical security of critical infrastructure and prisons, forensic investigators, judiciary teams and inter-agency task forces. Policymakers and public servants are encouraged to consider the cross-cutting points regarding public awareness, communications and the importance of harnessing the scientific community to improve responses to criminal use of drones.

Immediate

- Conduct threat triage and hotspot mapping to produce a geotagged risk map identifying high-frequency corridors such as prison yard blind spots, border strips and coastal chokepoints, using local incident data and open reports.
- Implement low-cost detection and hardening measures, including human observation, raised vantage points, visual/night cameras, nets and physical barriers around high-value drop zones.
- Standardize incident reporting and forensic collection protocols for downed drones, ensuring rapid evidence capture and consistent documentation.

Short-term

- Pilot layered sensor deployments combining acoustic, RF and electro-optical detection at vulnerable sites, assessing fidelity, false alarm rates and operational burden.
- Establish a clear legal roadmap with aviation authorities, communications regulators and prosecutors to enable rapid, lawful active mitigation.
- Target enablers through intelligence operations to identify drone fabricators, component suppliers and local coordinators, prioritizing disruption of workshops and logistics hubs over low-level couriers.
- Form cross-agency task forces integrating border guards, the military, drugs, customs and prosecutorial resources for rapid interdiction and evidence handling.

Medium-term

- Enhance regional cooperation and collaborative interdiction efforts, sharing telemetry, imagery and forensics, and establish joint investigative teams for known transnational routes.
- Regulate critical drone components and commercial sales through licensing, export controls or audits, particularly for high-payload motors, long-range autopilots and unmanned underwater vehicle (UUV) components.
- Develop a technology roadmap and procurement strategy focusing on scalable, upgradeable counter-unmanned aircraft systems sensors and integrated data fusion platforms rather than single-purpose devices.

Cross-cutting

- Mobilize communities as drone observers through awareness-raising projects to ensure citizens observe and report illicit drone use.
- Communicate publicly about interdictions and prosecutions to raise perceived risk among traffickers and reassure affected communities.
- Support research and development in resilient, tamper-resistant forensics; secure DroneID systems and detection across multiple domains, including UUVs.

NOTES

1 Colin Freeman and Verity Bowman, Mexican and Colombian drug cartels infiltrate Ukrainian military, *The Telegraph*, 15 October 2025, https://www.telegraph.co.uk/world-news/2025/10/14/drug-cartels-learn-modern-warfare-ukrainian-front-lines/.

2 Shaun Walker, Russian drone incursion into Poland 'was Kremlin test on Nato', *The Guardian*, 15 September 2025, https://www.theguardian.com/world/2025/sep/14/russian-drone-incursion-poland-nato-ukraine-europe.

3 Tabby Wilson, Copenhagen and Oslo airports forced to close temporarily due to drone sightings, BBC, 23 September 2025, https://www.bbc.co.uk/news/articles/cn4lj1yvgvgo; Elena Giordano, Belgium launches probe after reports that 15 drones buzzed military base, *Politico*, 3 October 2025, https://www.politico.eu/article/15-suspicious-drones-spotted-above-belgium-military-base/.

4 Miranda Bryant and Jennifer Rankin, Talks on European 'drone wall' after Danish airport incursions, *The Guardian*, 25 September 2025, https://www.theguardian.com/world/2025/sep/25/drones-aalborg-airport-denmark-closed-days-after-copenhagen-oslo.

5 Elena Giordano and Pieter Haeck, 3 arrested in suspected terror plot targeting Belgian PM Bart De Wever, *Politico*, 9 October 2025, https://www.politico.eu/article/belgium-terror-plot-prime-minister-bart-de-wever-crime/.

6 Associated Press, Venezuela's Maduro: 'Shield of love' thwarted drone attack, VOA, 5 August 2018, https://www.voanews.com/a/venezuela-s-maduro-object-of-attack-but-is-fine-official-says/4513955.html.

7 Bárbara Morais Figueiredo, The use of uncrewed aerial systems by non-state armed groups: Exploring trends in Africa, UNIDIR, 30 January 2024, https://unidir.org/publication/the-use-of-uncrewed-aerial-systems-by-non-state-armed-groups-exploring-trends-in-africa/.

8 European Union EUR-Lex, Consolidated text: Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, 12 March 2019, https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj; European Union EUR-Lex, Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft (Text with EEA relevance), 24 May 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019R0947-20250501.

9 Europol, EU serious and organised crime threat assessment (EU-SOCTA), 27 May 2025, https://www.europol.europa.eu/publications-events/main-reports/socta-report.

10 European Union EUR-Lex, Communication from the Commission to the Council and the European Parliament on countering potential threats posed by drones, 18 October 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023DC0659.

11 Frank G Hoffman, *Mars Adapting: Military Change During War*, Annapolis: Naval Institute Press, 2021; Alfred D Chandler, *The Visible Hand: The Managerial Revolution in American Business*, Cambridge: Harvard University Press, 1977; Florence Nightingale, *Notes on Hospitals*, London: Longman, Green, Longman, Roberts and Green, 1863.

12 National Research Council, *The Global Positioning System: A Shared National Asset*, Washington, DC: National Academies Press, 1995.

13 Annette M Hübschle, The social economy of rhino poaching: Of economic freedom fighters, professional hunters and marginalized local people, *Current Sociology*, 65, 3 (2016), 427–447.

14 Steven Feldstein, *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*, New York: Oxford University Press, 2021; Alcides Eduardo dos Reis Peron et al, Beyond digital repression: Techno-authoritarianism in radical right governments, *Cogent Social Sciences*, 11, 1 (2025), https://doi.org/10.1080/23311886.2025.2528457.

15 Samuel Bendett and Leonid Nersisyan, The drone war over Ukraine, in Dag Henriksen and Justin Bronk (eds), *The Air War in Ukraine*, London: Routledge, 2024.

16 Olena Kryzhanivska, Arms trends in Ukraine: 8 September–14 September, 2025, Ukraine's Arms Monitor, 15 September 2025, https://ukrainesarmsmonitor.substack.com/p/arms-trends-in-ukraine-8-september.

17 Robert J Bunker and John P Sullivan, Mexican cartels are embracing aerial drones and they're spreading, War on the Rocks, 11 November 2021, https://warontherocks.com/2021/11/mexican-cartels-are-embracing-aerial-drones-and-theyre-spreading/; Juan Camilo Jaramillo, Drones fuel criminal arms race in Latin America, InSight Crime, 6 March 2025, https://insightcrime.org/news/drones-fuel-criminal-arms-race-latin-america.

18 US Customs and Border Protection, El Paso Sector Border Patrol encounters new tactic as smugglers keep sending in families and felons, 17 April 2019, https://www.cbp.gov/newsroom/local-media-release/el-paso-sector-border-patrol-encounters-new-tactics-smugglers-keep.

19 National Institute of Justice, Addressing contraband: As threat of drone deliveries grows, 2 June 2023, https://nij.ojp.gov/topics/articles/addressing-contraband-prisons-and-jails-threat-drone-deliveries-grows.

20 United States Department of Justice, International smuggling drones nets 28 pounds of heroin, 12 August 2015, https://www.justice.gov/usao-sdca/pr/international-smuggling-drones-nets-28-pounds-heroin.

21 Joby Warrick, Use of weaponized drones by ISIS spurs terrorism fears, *The Washington Post*, 21 February 2017, https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html; Don Rassler et al, On the horizon: The Ukraine war and the evolving threat of drone terrorism, *CTC Sentinel*, 18, 3 (2025), https://ctc.westpoint.edu/on-the-horizon-the-ukraine-war-and-the-evolving-threat-of-drone-terrorism/.

22 Robert J Bunker and John P Sullivan, Mexican cartels are embracing aerial drones and they're spreading, War on the Rocks, 11 November 2021, https://warontherocks.com/2021/11/mexican-cartels-are-embracing-aerial-drones-and-theyre-spreading/.

23 Nacho Sánchez, Spanish police seize large drone used to carry drugs from Morocco, *El País*, 15 July 2021, https://english.elpais.com/spain/2021-07-15/spanish-police-seize-large-drone-used-to-carry-drugs-from-morocco.html.

24 Sam Jones, Spanish police seize underwater drones designed to carry drugs, *The Guardian*, 4 July 2022, https://www.theguardian.com/world/2022/jul/04/spanish-police-seize-underwater-drones-designed-to-carry-drugs.

25 Jordan shoots down crystal-meth-laden drone from Syria, Al Jazeera, 14 August 2023, https://www.aljazeera.com/news/2023/8/14/jordan-shoots-down-crystla-meth-laden-drone-from-syria.

26 Yannick Veilleux-Lepage, Guns by drone: The rise of drone-assisted firearm smuggling on Israel's southern border, Global Network on Extremism & Technology, 5 June 2025, https://gnet-research.org/2025/06/05/guns-by-drone-the-rise-of-drone-assisted-firearm-smuggling-on-israels-southern-border.

27 James Crisp, Police helicopter targeting cocaine crops downed by drone, *The Telegraph*, 22 August 2025, https://www.telegraph.co.uk/world-news/2025/08/22/colombia-drone-police-helicopter-drugs-operation.

28 Ukraine launches domestic production of F-1, RGD-5 hand grenades, the ordnance's already in use with the army, Defense Express, 9 September 2024, https://en.defence-ua.com/industries/ukraine_launches_domestic_production_of_f_1_rgd_5_hand_grenades_the_ordnances_already_in_use_in_with_the_army-11797.html.

29 Nordic Noir: The rise of Swedish organized crime, at home and abroad, GI-TOC, 2025 (forthcoming).

30 GI-TOC interviews with Ukrainian drone operators, May–July 2025.

31 Ibid.

32 Smuggling inc.: Illicit trade between Ukraine's Transcarpathia and the EU, GI-TOC, April 2025, https://globalinitiative.net/analysis/illicit-trade-between-ukraines-transcarpathia-and-the-eu/.

33 Commercial DJI drones, mainly the Matrice 300 RTK, FlyCart 30 and Agras T30, have been modified with custom cargo mounts, stripped sensors, dual battery packs and improvised fasteners. The FlyCart 30 has transported 9 to 10 M16-type rifles and magazines per flight, totalling 31.5–35 kilograms, beyond typical commercial capacities. Weapons carried also include AKs, pistols and ammunition, highlighting advanced planning and operational maturity. Analysts suggest this shift represents a 'substitution effect', as drone smuggling adapts to the Israeli destruction of Gaza smuggling tunnels post-October 2023. Beyond Israel, such cases illustrate how off-the-shelf drones allow non-state actors to replicate military logistics, signalling the potential for global replication in other conflict zones. See Yannick Veilleux-Lepage, Guns by drone: The rise of drone-assisted firearm smuggling on Israel's southern border, Global Network on Extremism & Technology, 5 June 2025, https://gnet-research.org/2025/06/05/guns-by-drone-the-rise-of-drone-assisted-firearm-smuggling-on-israels-southern-border. DJI has recently unveiled a new quadcopter commercial drone that has an 80-kilogram maximum payload capacity and is equipped with intelligent cargo handling capabilities. See DJI launches FlyCart 100 delivery drone, Heliguy, 2 July 2025, https://www.heliguy.com/blogs/posts/dji-launches-flycart-100-delivery-drone.

34 GI-TOC interviews with Ukrainian drone operators, May–July 2025.

35 Hodaya Busheri, Drone threat on the Egyptian border has Israel on edge, Israel Hayom, 20 October 2025, https://www.israelhayom.com/2025/10/20/drone-threat-on-the-egyptian-border-has-israel-on-edge/.

36 Mechanical robot, land torpedo or explosive tankette 'Jeffrey the robot': Corporal Harold Edward Jeffery, RAAF, Australian War Memorial, https://www.awm.gov.au/collection/C138021.

37 Alex Hern, Meet the Chinese army's latest weapon: the gun-toting dog, *The Guardian*, 30 May 2024, https://www.theguardian.com/science/article/2024/may/30/chinese-armys-latest-weapon-gun-toting-dog.
38 GI-TOC interviews with Ukrainian drone operators, May–July 2025.
39 Kyiv Independent, Ground drones are changing Ukraine's fight against Russia, YouTube, 20 August 2025, https://www.youtube.com/watch?v=k9x-v5dL3k4.
40 Radio Free Europe/Radio Liberty, How ground drones in Ukraine are changing the future of war, YouTube, 17 March 2025, https://www.youtube.com/watch?v=skPRtSIJI7Y.
41 Olena Kryzhanivska, Drone warfare in Ukraine: Long-range strikes and naval drone export, Ukraine's Arms Monitor, 25 September 2025, https://ukrainesarmsmonitor.substack.com/p/drone-warfare-in-ukraine-long-range.
42 Maritime piracy dropped in 2024 but crew safety remains at risk, ICC Commercial Crime Services, 2024, https://icc-ccs.org/maritime-piracy-dropped-in-2024-but-crew-safety-remains-at-risk.
43 Max Daly, The deadly rise of underwater parasite cocaine smuggling, Vice, 27 July 2023, https://www.vice.com/en/article/the-deadly-rise-of-underwater-parasite-cocaine-smuggling.
44 David Kirichenko, Ukraine's cheap robot drones extract heavy price from Russia, The Interpreter, 5 June 2025, https://www.lowyinstitute.org/the-interpreter/ukraine-s-cheap-robot-drones-extract-heavy-price-russia.
45 European drug trends monitor, Issue 2, GI-TOC, March 2025, https://globalinitiative.net/analysis/european-drug-trends-monitor-1/.
46 Hoffman's work on military adaptation provides an analytical lens that helps make sense of this dynamic. His central argument, grounded in 'organizational learning theory', highlights how military organizations change most effectively through the interplay of leadership, culture, structured learning processes and effective dissemination of knowledge. See Frank G Hoffman, *Mars Adapting: Military Change During War*, Annapolis: Naval Institute Press, 2021.
47 Napoleon's corps system revolutionized the coordination of large armies, but its legacy went far beyond the battlefield. By dividing forces into semi-autonomous units capable of independent manoeuvre, he demonstrated the value of decentralized yet coordinated structures. This organizational principle was later adapted by modern businesses in the form of divisional management and flexible corporate hierarchies – another military innovation bequeathed to civilian life. See Alfred D Chandler, *The Visible Hand: The Managerial Revolution in American Business*, Cambridge: Harvard University Press, 1977.
48 Land operations, Land Warfare Development Centre, Army Doctrine Publication: AC 71940, 2016, https://assets.publishing.service.gov.uk/media/677fe2d4d721a08c0066560c/Army_Doctrine_Publication_land_operations__withdrawn_25_May_2022_.pdf.
49 GI-TOC interviews with Ukrainian drone operators, May–July 2025.
50 Ibid.
51 Ibid.
52 Ibid.
53 GI-TOC interview with Macedonian police officer, Skopje, 10 September 2025.
54 GI-TOC interviews with Ukrainian drone operators, May–July 2025.
55 Ibid.
56 Ibid.
57 Ibid.
58 Ibid.
59 Ibid.
60 Ibid.
61 Ibid.
62 Ibid.
63 Ibid.
64 Ibid.
65 Amanda Coletta et al, Haiti turns to weaponized drones in fight against gangs, *Washington Post*, 10 April 2025, https://img.washingtonpost.com/world/2025/04/10/haiti-government-drones-gangs/.
66 Ibid.
67 Haiti: at least eight children among 13 killed in drone attack on birthday party, *The Guardian*, 23 September 2025 https://www.theguardian.com/world/2025/sep/23/haiti-drone-attack-eight-children-killed.
68 David C Adams et al, A desperate Haiti turns to Erik Prince, Trump ally, in fight against gangs, *New York Times*, 28 May 2025, https://www.nytimes.com/2025/05/28/us/haiti-erik-prince-blackwater-gangs.html.
69 Walter Kemp and Romain Le-Cour-Grandmaison, Guns for hire: Should private military companies take on organized crime?, GI-TOC, 8 September 2025, https://globalinitiative.net/analysis/haiti-military-companies-organized-crime-gangs/.
70 Daniel Blanco Paz, Haiti 2025 threat assessment: Gangs and drones, Grey Dynamics, 9 June 2025, https://greydynamics.com/haiti-2025-threat-assessment-gangs-and-drones/,
71 Henry Shuldiner, Drone strikes shake Haiti's gangs but leave legal and strategic questions, InSight Crime, 24 June 2025, https://insightcrime.org/news/drone-strikes-shake-haiti-gangs-leave-legal-strategic-questions/.
72 UN approves militarized force to take on Haiti's gangs, *Washington Post*, 30 September 2025, https://www.washingtonpost.com/world/2025/09/30/haiti-gang-suppression-force-un-security-council/; see also Reuters and PBS coverage on mission limits and resourcing: Sarah Morland and Daphne Psaledakis, US funding for Haiti mission in doubt if UN resolution rejected, official says, Reuters, 24 September 2025; UN Security Council approves larger international force to combat gangs in Haiti, PBS,

1 October 2025, https://www.pbs.org/newshour/world/un-security-council-approves-larger-international-force-to-combat-gangs-in-haiti.

73 Asma Almusayli, Tanveer Zia and Emad-ul-Haq Qazi, Drone forensics: An innovative approach to the forensic investigation of drone accidents based on digital twin technology, *Technologies*, 12(1), 11 (2024), https://doi.org/10.3390/technologies12010011.

74 Thomas H Austin and Fabio Di Troia, A blockchain-based tamper-resistant logging framework, in Luis Bathen, Gokay Saldamli, Xiaoyan Sun, Thomas H Austin, and Alex J Nelson (eds), *Silicon Valley Cybersecurity Conference*, Communications in Computer and Information Science, vol 1683. Springer, Cham (2022), https://doi.org/10.1007/978-3-031-24049-2_6.

75 Nico Schiller et al, Drone security and the mysterious case of DJI's DroneID. Proceedings of the Network and Distributed System Security Symposium 2023, San Diego, CA, 27 February – 3 March 2023. Ruhr University Bochum; CISPA Helmholtz Center for Information Security, https://dx.doi.org/10.14722/ndss.2023.24217.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 700 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net