Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Research Article

DEATH FROM ABOVE: USE OF ATTACK DRONES BY TERRORIST ORGANISATIONS

English translation with AI assistance (DeepL)

Diego de Lorenzo de Guindos
Second Lieutenant of Guardia Civil
Degree in Security Engineering
delorenzodeguindos@gmail.com

Received 07/09/2025
Accepted 19/11/2025
Published 30/01/2026

doi: https://doi.org/10.64217/logosguardiacivil.v4i1.8472

Recommended citation: de Lorenzo, D. (2026). Death from above: use of attack drones by terrorist organisations. *Revista Logos Guardia Civil*, 4 (1), 53-82. https://doi.org/10.64217/logosguardiacivil.v4i1.8472

License: This article is published under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0) license.
Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

doi: https://doi.org/10.64217/logosguardiacivil.v4i1.8472

DEATH FROM ABOVE: THE USE OF ATTACK DRONES BY TERRORIST ORGANISATIONS

Abstract: Small drones have become increasingly present in conflict scenarios. Their versatility, wide availability, and low cost explain this trend. This article examines the possibility that such devices may be incorporated into attempted terrorist attacks, first analyzing their use in armed conflicts, with particular attention to rear-area operations, whose characteristics could inspire the planning of attacks. To assess the operational utility of drones for actors with more limited logistical, economic, and operational capabilities than states, the article also explores their use by criminal organizations in South America. The findings are then related to the vulnerabilities historically exploited by terrorist groups to evade state action and carry out their operations. The article concludes that drones constitute highly attractive tools for these groups and that their proliferation entails the emergence of new vulnerabilities that must be identified and addressed to prevent potential attacks against the state or its citizens.

Resumen: Los drones de pequeñas dimensiones se han convertido en sistemas cada vez más presentes en los escenarios de conflicto. Su versatilidad, amplia disponibilidad y bajo coste explican esta expansión. Este artículo analiza la posibilidad de que estos dispositivos puedan incorporarse a tentativas de atentados terroristas, examinando previamente los usos que han recibido en conflictos bélicos, con especial atención a las acciones en la retaguardia, cuya naturaleza podría resultar inspiradora para la planificación de ataques. Con el fin de valorar la utilidad operativa de los drones para actores con capacidades logísticas, económicas y operativas inferiores a las de los Estados, se estudiará también su empleo por parte de organizaciones criminales en Sudamérica. Las conclusiones obtenidas se pondrán en relación con las vulnerabilidades históricamente explotadas por grupos terroristas para evadir la acción del Estado y materializar sus operaciones. El artículo concluye que los drones constituyen herramientas especialmente atractivas para estos grupos, y que su proliferación implica la aparición de nuevas vulnerabilidades que deberán ser identificadas y corregidas para prevenir atentados contra el Estado o sus ciudadanos.

Keywords: Drones, Artificial Intelligence, Terrorism, Ukraine, Attacks.

Palabras clave: Drones, Inteligencia Artificial, Terrorismo, Ucrania, Atentados.

doi: https://doi.org/10.64217/logosguardiacivil.v4i1.8472

ABBREVIATIONS

9/11: 9/11 Attacks

CDS - Sinaloa Cartel

CIA: Central Intelligence Agency

CJNG: Jalisco Cartel - Cartel de Jalisco Nueva Generación (Jalisco Cartel - New Generation)

DEA: U.S. Drug Enforcement Administration

ISIL/ISIS: Islamic State in Iraq and the Levant

USA: UNITED STATES USA: United States

FARC: Fuerzas Armadas Revolucionarias de Colombia (Revolutionary Armed Forces of Colombia)

FBI: Federal Bureau of Investigation

FPV: First Person View

GPS: Global Positioning System

AI: Artificial Intelligence

TCOs: Transnational Criminal Organisations

RPAS: Remotely Piloted Aircraft System

SBU: Security Service of Ukraine

UAS: Unmanned Aerial Systems

UAV: Unmanned Aerial Vehicles

INTRODUCTION

Humankind has always made use of advances in science to enhance its military capabilities. In some cases, they have adapted existing discoveries to military purposes; in others, it has been precisely the need to obtain more powerful and effective means of destruction than those of their adversaries that has driven real technological revolutions.

One such stage of conflict triggered an unprecedented scientific explosion in all branches: the Second World War. Of all the projects, great ideas and discoveries, we would like to focus on two in particular to analyse their long-term consequences: the German projects that led to the use of the V1 and V2 ballistic missiles, as well as "Project Pigeon".

First, the German projects that led to the use of the V1 and V2 ballistic missiles. They could be launched from the territory of occupied France and reach cities in England, where they wreaked havoc (Reuter, 2000).

Second, a more obscure but no less revolutionary project was American psychologist B.F. Skinner's "Project Pigeon" to develop guided anti-ship missiles using AI technology (although in this case, AI would stand for "animal intelligence"). Based on the findings of Pavlov's Dog, Skinner concluded that pigeons could be trained to continuously peck at a point they saw on a screen. That point would at some point have been an actual enemy ship, and the points at which the pigeon pecked would send signals to the missile's controls to modify its trajectory. The project was discontinued in 1953 because of the advance of electronic guidance measures (Skinner, 1960).

Although these two projects bear little direct relation to the development of drones, they were the first to implement ideas that are now a reality. The first proposed being able to attack enemy targets from a great distance with missiles that did not put any pilot's life at risk, and the second was the first step towards weapon systems that could think for themselves and make their own decisions, without the need for human intervention and without emitting electromagnetic radiation to detect targets, as pigeons did by interpreting images. These experiments laid the conceptual foundations for the automation of weapons, an idea that would evolve decades later into today's combat drones.

Today, as of September 2025, we do not have pigeons guiding gliding projectiles launched from aircraft. Instead, we have small explosive-laden flying devices with the ability to understand where they are, where they need to go, what their mission is and to recognise potential targets and decide which one is the most suitable and crash into it, detonating the explosives in the process.

This phenomenon has come to be seen as a regular part of the contemporary warfare landscape, but perhaps with an overconfident spatial delimitation: it is a phenomenon of the front lines of warfare. However, the continuous Ukrainian and Russian rearguard actions with drones hundreds of kilometres from the front lines, and the news coming from South America regarding their use by organised crime groups , make us suspicious of the possible uses that terrorist groups might make of these devices.

The aim of this article is to analyse, firstly, the potential of unmanned aerial vehicles to be used in targeted attacks against military targets, as well as recent historical

examples of their use. It will then proceed to explore the transposition of these systems to organisations operating outside the state that has occurred in South American countries, principally Mexico, Colombia and Brazil. It will then look at past terrorist attacks to highlight the mistakes that made them possible. All of the above sections will support the final thesis, which is that drones are a particularly attractive system for those seeking to carry out attacks against large masses of people, as well as specific targets.

For the purposes of this article, the definition of terrorism will be that contained in a US Department of Defense directive: "calculated use of violence or threat of violence against individuals or property, to instil fear, with the intent to coerce or intimidate government or society to achieve political, ideological or religious objectives" *(Department of Defense,* 2000). However, actions that manifest themselves through the same external conduct, even if they do not pursue a political, ideological or religious purpose, will be considered analogously.

In order to limit the scope of this article, the use of large drones will be omitted. This is in consideration of their limited availability and greater ease of detection. Drones used by the United States Air Force, those belonging to the Ukrainian and Russian forces, as well as any other drone of identical consideration, are therefore excluded from this study.

The object of study is therefore defined as the use of small drones by groups pursuing violent actions against groups of people, high-ranking personalities, important properties for society, and the rest of those that fall within the definition of an attack.

2. ATTACK DRONES IN CONVENTIONAL WARS

2.1. SYRIAN CIVIL WAR

The role of small drones in conflicts has seen a progressive increase towards what we know today. The first significant uses could be detected during the Syrian civil war, where more specifically, the Islamic State in Iraq and the Levant (ISIL/IS) explored the offensive possibilities of Unmanned Aerial Vehicles (UAVs) (Hambling, 2016).

In this context, the first recorded use of drones as attack tools were the drone-car bomb combinations with which ISIS attacked its enemies in the battle for Mosul. The drones were used for target reconnaissance and subsequent guidance of the VBIEDs through the streets of the city (Balkan, 2017).

The use of drones as a weapon of war evolved when explosive charges were added to UAVs and released on enemy positions. This model was exported to the ISIL fighting in Deir ez-Zor and offensives against the Kurds in Syria.

Incidents of First Person View (FPV) kamikaze drone strikes were residual at first, although their frequency would increase over time (Lyle, 2019).

2.2. WAR IN UKRAINE

Another notable scenario was the conflict in the Donbas, which began in 2014. The initial role of UAVs was to reconnoitre targets that artillery would later harass. These drones,

sometimes equipped with night vision, became known to the military on both sides because of their night-time buzzes, which were often immediately accompanied by barrages from enemy pieces.

However, the evolution of small drones as weapons of war would enter a spiral of innovation after the start of the foiled Russian attack on Ukraine on 24 February 2022, and the ensuing war, which, in November 2025, seems to have no end in sight.

As seen in Syria, drones were quickly modified with homemade remedies to carry explosives, such as grenades or mortar shells, and drop them on enemy defensive positions. The first difference that emerged in this theatre of operations was the rapid emergence of First Person View (FPV) drone strikes. These were quadcopters carrying an explosive payload with attached impact fuses (Naber, 2025).

This paradigm shift offered both sides the possibility of executing precise actions against specific targets, facilitating successful operations, albeit with the loss of at least one aircraft per action.

The use of drones increased exponentially during the early phases of the war, reaching the current situation where both armies have specialised Unmanned Aerial Systems (UAS) attack units integrated at a very low level. For example, the Ukrainian Army's 12th Special Forces Brigade "Azov" has a drone company in each combat battalion, as well as an additional UAS battalion to support the brigade. Something similar can be observed in other units of both armies (12th Special Forces Brigade "Azov", n.d.).

Both Ukraine and Russia began a technological struggle at that time, trying to find remedies against drones while improving them. For example, anti-drone networks began to be deployed in defensive positions and main logistical routes, which was immediately followed by tandem tactics: a first drone would break the network, and the second would go in for the targets (Méheut, 2025).

In order to protect each side's most important assets, jammers were widely used to thwart attempts to destroy them. This led to a long *stalemate* on the front lines. Drone teams began to have a decreasing rate of effectiveness, as jammers became more widely distributed. Both nations tried to find solutions to this defensive system which, while not foolproof, greatly reduced the operational capability of UAS (Loh, 2025).

During the summer of 2024, the first considerable efforts with drones linked to the controlling terminal by thin fibre-optic cables began to be recorded during the Ukrainian invasion of the Kursk Oblast. The main advantage of the cable connection is its immunity to jammers. It should also be noted that they are undetectable by systems based on the interception of electromagnetic waves, as well as ensuring a better connection with the control terminal, returning higher quality images and facilitating their effectiveness, since as long as the cable length remains, the connection will not be lost (Hambling, 2025).

At present, technological developments seem to be moving towards the increasingly common use of autonomous drones guided by Artificial Intelligence. Ukraine's defence industry is working on large-scale production of drone models that recognise tactical situations on their own, analyse them properly, and make optimal decisions for Ukrainian interests. The Russian military industrial complex is acting in the

same way. By the end of August 2025, there were at least 100 such incidents (MacDonald, 2025; Boffey, 2025; Khomenko, 2024).

In addition to frontline actions, since the start of the Ukrainian war there has been a succession of increasingly complex enemy rearguard actions in which UAS from both sides play a crucial role in achieving objectives.

Lessons learned in Ukraine have inspired operations elsewhere in the world. For example, during the 7 October 2023 massacre in southern Israel, the Hamas group attacked IDF border positions with small UAVs (Page, 2025).

3. OPERATION SPIDER WEB

3.1. THE ATTACK ON 1 JUNE 2025

On 1 June 2025, the Russian air bases at Olenya, Ivanovo Severny, Dyagilevo, Ukrainka and Belaya came under attack by Ukrainian special forces. These were not ballistic missiles or long-range drones, as Ukraine had frequently used until then. Swarms of small First Person Vision (FPV) drones attacked Russian air force positions.

The target of the attack was the strategic bomber fleet that Russia had been systematically employing in its campaign of attrition against Ukrainian civilian infrastructure. The end result was the destruction or incapacitation of 34% of the targeted fleet. Moreover, these aircraft models had been out of production since 1993, making it difficult to rebuild strategic long-range capability. Economically, Ukraine claims that the damage incurred would amount to around $7 billion (Gibson et al. 2025).

It should be noted that small FPV drones would have directly attacked enemy air bases extremely far from the front line, such as the Ukrainka base, which is more than 5,800 km from Ukraine's internationally recognised border, and more than 6,000 km from the front line. To put these figures in context, this is more than the distance from the centre of Madrid to Herat (Afghanistan), and about the same distance from Madrid to Baltimore in the United States (US).

The Security Service of Ukraine (SBU) managed to attack military bases more than 6,000 kilometres away using drone models that usually perform tactical missions very close to the front line, and whose main weakness is their difficulty in linking to the control terminal. This was possible because the drones used in this operation took off close to each of the air bases. In the case of the attack on Belaya air base (the largest attack of the operation, with 3 Tu-95 bombers and 4 Tu-22M3 bombers destroyed), the FPV drones took off from a position about 8 kilometres southeast of the base (Dempsey, 2025).

3.2. THE OPERATION

The Ukrainian Security Service (SBU) "Operation Spider's Web" had a planning and preparation phase of more than 18 months, according to Ukrainian President *Volodymyr Zelenskyy (Zelenskyy*, 2025*)*. First Person Vision (FPV) quadcopters "Osa" from the Ukrainian company *First Contact* (First Contact, 2025) were used.

The Osa model drones are distinguished by the location of their electronic components under a particularly thick outer casing and by having the power port in a fixed position, whereas most FPV drone models regularly used by the Ukrainian Armed Forces tend to have a "skeleton" body, in which the electronics and wiring are usually uncovered. After considering the complexity of the mission, the distance between the operation preparation site and the targets, and the varying weather conditions in which the infiltration would take place, the SBU opted for the most robust model.

During the 18 months of preparation, the SBU managed to get 117 Osa drones into the Russian Federation. Once inside enemy territory, a front construction company was set up to build wooden modular housing units to conceal the movements. These housing modules were fitted with a retractable false roof, in which 9 rows of 4 drones each were concealed, for a theoretical total capacity of 36 drones per module. In parallel, drones were also hidden in cargo containers (Bondar, 2025).

A remote control system was also installed in each module, which would act as an intermediary between the 117 drones carrying out the attack and the 117 pilots controlling them from Ukraine. The link between the remote control systems and the positions of the operators could be made via satellite.

Once the "Trojan horses" were assembled, the SBU contacted Russian freight forwarding companies. They took the Osa drones to the cargo "delivery points" , which were eventually the locations arranged by the SBU for the subsequent take-off of the drones.

In the early hours of 1 June 2025, the covers of the already infiltrated "Trojan horses" were lifted, allowing the drones to take off and head for their targets. Numerous videos were released of Russian civilians in these modules and containers with drones flying out of them into the black clouds caused by the explosions of those that preceded them.

Taking the overall balance of the operation, some 117 Osa drones, worth between $600 and $1,000 per unit, caused losses to Russian aviation, and thus to the country's entire armed wing, of $7 billion.

This attack is an unmitigated defeat for Russia, which not only suffered such irreplaceable losses, but did so in a way that exposed the serious shortcomings of both the country's air defence and counter-intelligence efforts. In terms of humiliation, it may be greater than the twin drone strike on the Kremlin on 3 May 2023 (Barnes et al., 2023).

It should be noted that all Ukrainians involved were exfiltrated from Russian territory well in advance of the attack. Thus, not only was the operation carried out without a single Ukrainian casualty, but Ukraine now has personnel with the experience to carry out such actions. If this operation had an 18-month planning and preparation phase, it would not be unreasonable to think that the next large-scale attack against the Russian rearguard could be in the making as we speak.

3.3. DIFFERENCES WITH OTHER SIMILAR OPERATIONS

Operation Spiderweb is by no means the first small-scale drone strike against infrastructure critical to a state's national defence. Insurgents in Iraq have been attacking the positions of the Iraqi Army and the international coalition armies against the Islamic State with UAVs for years. Syrian rebels also carried out drone strikes against the Russian airbase at Hmeimim in the region loyal to Bashar Al-Assad's government in Latakia. However, what is most remarkable about this action is the depth of the attack inside enemy territory, the technical sophistication of its execution, and the fact that it targeted bases with critical and scarce materiel of the world's second largest army, in a context of warfare in which rearguard attacks were a constant dynamic of the conflict.

Ben Connable argues that the Ukrainian operation, while successful, must be interpreted in its proper context. He notes that previous experience in Syria (Hmeimim), Iraq, Yemen, and elsewhere reveals that airfields can be effectively protected against such attacks by layered air defence. Therefore, we should not be tempted to label as a revolution in warfare what may be no more than a case of isolated security failure (Connable, 2025).

It is possible that it is a failure of Russian air defence planning, as Ben Connable suggests. However, the examples the author mentions must also be put in context.

The case with the most readily available information will be analysed: the multiple drone strikes against the Hmeimim Air Base in Latakia (Syria). The facility was built in 2015 to be used as a strategic hub for the Russian intervention in Syria. This base has suffered a long list of UAV attacks from 2018 until the most recent one in January 2025.

The first of these attacks occurred on 6 January 2018, when 13 fixed-wing UAVs were intercepted by electronic warfare assets present at the base and subsequently captured, although some did have to be shot down by air defence. Remarkable is both the difference in numbers and the means employed by the rebels compared to Operation Spider's Web (BBC, 2018).

From that moment on, the air base began to be attacked continuously until 2021, when the attacks ceased, except for some sporadic cases. The official Russian media, possibly seeking the greatest propaganda gain, tended to give data for long periods of time, and not so much for specific attacks. During August 2018, the base was attacked by 47 Unmanned Aerial Vehicles (UAVs), and between September and October 2018, the base's military personnel shot down 50 UAVs.

Thus, the scale of the attacks by Syrian rebel groups would have been far beyond Russia's defence capabilities. Moreover, it can be understood that, in order to protect the strategic centre of its military intervention in Syria, Russia has significantly increased its air defence assets at the base. Moreover, the Hmeimim base is less than 100 kilometres from Idlib, the Syrian region with the greatest rebel presence and control throughout the civil war.

The experiences in Hmeimim would therefore not be comparable to what happened at the bases attacked by Ukraine on 1 June 2025, given the differences in the geographical context, level of prior alert and complexity of the action.

The effort required for Russia to have adequately protected all air, naval, and land bases on its territory, as well as any critical infrastructure susceptible to military targeting, would be immense. This difficulty is compounded for a country at war with its neighbour to the west, with obvious implications for determining the deployment of units with air defence capabilities.

3.4. IMPLICATIONS

As is theoretically the case in naval warfare, drone strikes are more focused on swarm tactics than on ensuring the impact of individual drones. This is evident both in Ukraine and in Iran's strikes against Israel. We must therefore conclude that drone strikes against targets protected by anti-drone means base their success on the swarm (Price, 2025; Tangredi, 2023).

It is relevant to consider the decisive role that Artificial Intelligence played in the execution of the operation. Although the drones were officially piloted by Ukrainian operators, they could have used autonomous navigation means to anticipate possible link losses. Thus, even if the pilots had lost connection with the drones, they would have continued on their way to the airbases without human control or GPS signal. They would also have distinguished the targets from a distance (De Troullioud, 2025).

During the preparation phase of Operation Spider's Web, the drones were programmed to recognise the air assets they were going to attack, and thus highlight them to the pilot so that he could crash the drone into the most sensitive places for the structural integrity of the aircraft, e.g. fuel tanks. These capabilities would later have been put into practice with decommissioned bomber aircraft that Ukraine had in its depots (Bondar, 2025).

Thus, despite Ukraine's use of human pilots to execute this operation, it is clear that the level of AI involvement in the success of this operation is undeniable. It also begs the question of whether the execution could have been carried out entirely by autonomous UAVs. On this occasion, it could not be used, but given the progress made, it can be concluded that it could be used in the near future. It is even possible that experimentation in this direction is already underway. The immediate benefits would be decisive for the success of future operations: enabling the use of gigantic swarms, several times larger than those that can be seen today, and greatly increasing the security of the operation, avoiding the signals sent from the control centre to the drones.

Operation Spider's Web could be considered one of the most successful infiltration operations of the 21st century. It is an action that has been recognised by the Western community, even if it is now not fully aware of its future implications. The Russian government was quick to condemn the action as a terrorist attack, despite the fact that legitimate military targets were attacked in the context of an armed conflict recognised by both states. Nevertheless, and on the occasion of the images broadcast that day, it is worth reflecting: how would a terrorist attack on Spanish air bases differ visually from what happened inside the territory of the Russian Federation?

4. ATTACK DRONES ARRIVE IN SOUTH AMERICA

As José Nemesio García Naranjo said: "poor Mexico, so far from God and so close to the United States". This statement could well be extended to several American nations south of the Rio Grande, particularly those where there is a large presence of organised crime groups. Poor economic conditions, coupled with the incessant demand for illicit substances in external markets such as the US or Europe, have for decades led the American continent into confrontation, civil war and social instability. At times, extremes have been reached such as in El Salvador, where 1.7% of the country's total population is incarcerated, mostly for alleged involvement in substance trafficking and membership in organised crime groups (Human Rights Watch, 2024).

The US government calls some of these groups Transnational Criminal Organisations (TCOs) because of their power and influence. Some have arsenals, personnel and capabilities on par with some national armies, such as the Jalisco Cartel - New Generation (CJNG), led by Nemesio Oseguera Cervantes "el Mencho". Other organisations have an operational presence in the criminal markets of more than 40 countries, such as the Sinaloa Cartel (CDS) (Drug Enforcement Administration [DEA], 2025). The case of the latter group is paradigmatic of the control they exert over their territory, as a conflict over the cartel's leadership that began in 2024 has led to the state of Sinaloa being declared a war zone at various times by international journalists, causing at least 1,900 deaths and 2,000 disappearances in one year exclusively because of this conflict (Villegas, October 2025).

These criminal organisations have taken advantage of the technological advances of recent decades for their operations. In line with this, they have joined the drone revolution, using them primarily to perform three tasks: surveillance and security, trafficking of goods, and direct attack.

As has been seen in Ukraine, Latin America has experienced exponential growth in the use of drones, particularly since 2022. Organised crime groups have analysed the experiences in Eastern Europe almost as closely as professional armies, if not more so. The two South American countries with the largest drone presence in the context of organised crime are Mexico and Colombia.

4.1. MEXICO

To analyse the use of drones by organised crime groups in Mexico, we have to go back to the early 2010s. It was in these years that commercial drones began to be discovered and used for surveillance purposes. From then on, the possibility of transporting illicit substances loaded on them began to be explored.

In January 2015, a drone loaded with 2.5 kilograms of methamphetamine crashed in the city of Tijuana, Mexico, on its way to cross the US border. Until then, US border control authorities had not recorded any smuggling attempts using drones (Valencia, 2015).

It was not until 2017 that the first indications emerged that Transnational Criminal Organisations (TCOs) might be experimenting with the concept of explosive drones. Four men travelling in a vehicle that had been reported stolen were arrested by police in

Guanajuato State, in an area that was "hot" (disputed by more than one organised crime group). The Sinaloa, Jalisco Nueva Generación and Zetas cartels had a significant presence in Guanajuato, and were in conflict for control. Upon inspection of the vehicle, they found a drone with a "large quantity" (not describing the exact amount) of explosives attached to the body, and equipped with a radio frequency-activated initiator (AFP, 2017).

The first record of attempted drone attacks occurred on 9 July 2018, when an Unmanned Aerial Vehicle (UAV) struck the home of Gerardo Manuel Sosa, Baja California's Secretary of State for Public Security, in the town of Tecate. This drone was carrying two fragmentation grenades that ultimately failed to detonate. Moreover, the secretary of state was not at home at the time of the attack (CNN Español, 2018).

The use of drones began to gradually increase across the country, albeit without any concrete organisation and through small actions, clearly carried out with *ad hoc* materials, equipment and procedures.

Everything changed in 2021, with the leader of the 'Los Deltas' group, Armando Gómez Núñez, alias 'Delta 1'. The Deltas are an armed wing of the Jalisco Cartel - New Generation that operated in the border area between the states of Jalisco and Michoacán. Armando Gómez created the first specialised attack drone unit, commanded by "El Flaco Drones", and a mysterious member nicknamed "Lady Drones", who was arrested on 13 August 2025 (Secretaría de Defensa Nacional, 2024; Mendoza, 2025).

This new drone unit, along with others in various criminal groups, began to operate in a more technical and sophisticated way. Operators of medium Unmanned Aerial Systems (UAS) began to be called "droneros", and various patches of "drone" units have been seized (Maza, 2025).

The Jalisco Cartel - New Generation (CJNG) drone effort on the Jalisco-Michoacán border responded to a conflict against the "Familia Michoacana", which was quick to respond to the Jalisco group by establishing its own drone operator units.

Today, the use of UAS attack units has spread throughout Mexico, although incidents are concentrated in the states of Michoacán and Guerrero. As far as operators are concerned, the CJNG and the Familia Michoacana are the two most advanced organisations in the use of drones. After these two comes the Sinaloa Cartel, and then the rest of the criminal groups in various stages of evolution in this field (Jaramillo, 2025).

The most common type of drone attack in conflicts in Mexico are *droppers*, i.e., those that release explosive charges on a target, being rare to find actions carried out with drones with First Person Vision (FPV), although they are increasingly common. These *droppers* are also used for surveillance, and even for smuggling or transporting small objects (Villegas, September 2025).

At first, drone attacks were generally directed at other criminal organisations, with some specific cases of attacks against police or Mexican Armed Forces personnel being reported. In 2021, 10 fatalities were recorded, of which seven were members of criminal groups. Casualties decreased in 2022 to 8 (Ziemer, 2025).

doi: https://doi.org/10.64217/logosguardiacivil.v4i1.8472

Drone attacks increased considerably in 2023. That year, the number rose to 35, almost five times more than the previous year. However, it was not the increase that was most frightening, but the distribution of victims. Of the 35, 27 were civilians. A new era of drones had begun in Mexico. Criminal groups were now using drones, no longer just to attack direct enemies, but to spread panic among the population in the "hot" territories. In this period, there were direct attacks on villages in the states of Michoacán and Guerrero, in one of which villagers captured a Familia Michoacana hitman (Grillo, 2024).

This hitman, Fernando, made a statement to journalists in which he implied that UAS are not only here to stay in Mexico, but that their use will increase from now on: "they have *drone operators*. They have people specialised *in drone operations* (...). They have a lot of (many) drones, so even if a mule (a person dedicated to the trafficking of hidden objects and merchandise) loses one, they don't care (...). As this is just starting' (Grillo, 2024).

The technical capacity of TCOs in the field of UAS has reached such a level that the first signs of a real effort on the part of criminal organisations to invest in anti-drone measures and units are already beginning to be seen. Proof of this is that, in 2024 and in the context of the Sinaloa civil war, a member of one of the factions fighting for control of the Sinaloa Cartel, "los Mayitos" (the faction led by the sons of Ismael "el Mayo" Zambada, arrested in 2024), was photographed carrying a *Skyfend* anti UAS jamming system, valued at $100,000 (Jiménez, 2025).

While a single air defence system is insufficient to counter the destructive potential of attack drones, it does reveal an effort to enter the arms race that can be seen in other scenarios such as the Ukrainian one.

In terms of combating the illicit use of drones, the Mexican government has reacted by issuing provisions to make access to UAVs more difficult. In 2019, NOM-107-SCT3-2019, which regulates Remotely Piloted Aircraft Systems (RPAS), was drafted. In it, any device weighing more than 250 grams must be registered. It is prohibited to modify RPAS to enable the transport of dangerous goods or to drop objects. This measure, in a country where there are entire regions where the de facto government is in the hands of TCOs, has had little impact on addressing the problem of criminal use of drones.

On the humanitarian front, threats against the civilian population have led to a number of refugee displacements. In 2023, around 600 residents of Nuevo Caracol, Guerrero State, were forced to flee their homes because of ongoing drone attacks on the population (Ortiz, 2023).

4.2. COLOMBIA

One Latin American scenario in which the use of drones by organisations in confrontation with the national government is becoming increasingly relevant is Colombia. Colombia recorded its first death attributable to attack drones in July 2024, when a 10-year-old boy was killed and 12 other people were injured when a Unmanned Aerial Vehicle (UAV) attacked a football field in El Platerado with a fragmentation grenade (Torres, 2024).

The main perpetrator of drone use in Colombia is the National Liberation Army, particularly since it launched its offensive over Catatumbo in early 2025. Drone attacks are partly responsible for the displacement crisis in this region, with more than 52,000 people forced to flee their homes (UNHCR, 2025).

One of the dissident factions of the Revolutionary Armed Forces of Colombia People's Army (FARC-EP), the FARC-EP has also carried out drone attacks, such as the attacks in November 2024 and in July and August 2025 on three Colombian Navy Heavy River Support Patrol Boats (Patrulleras de Apoyo Fluvial Pesado), in the San Juan del Micay river, Department of Cauca, or the downing of an anti-narcotics helicopter in Antioquia in August 2025, with the death of the 13 policemen inside (Saumeth, 2025; Torrado, 2025).

On 10 June 2025, the FARC-EP's self-proclaimed Secretariat of the Central General Staff issued a communiqué with 10 recommendations for the civilian population, the press and humanitarian organisations, with the aim of avoiding incidents of attacks on civilians. These include maintaining a minimum distance of 500 metres from military or police convoys, and requiring the armed forces to abandon installations adjacent to residential buildings (W Radio Colombia, 2025).

The number of casualties from drone attacks in Colombia continues to be lower than in Mexico, although Colombia is beginning to see much larger attacks, such as the aforementioned attacks on ships and helicopters, from mid-2025.

Governments facing enemies with Unmanned Aerial Systems UAS in South America have been overwhelmed for the time being. Several countries, including Colombia, Peru and Mexico, have begun to equip their armed forces and security forces with drone defence systems to at least protect their bases and critical infrastructure.

Meanwhile, governments in the Americas are opting to combat organised crime groups with drones. In Haiti, a government drone operation on 1 March 2025 resulted in 80 casualties that day, although it has not been confirmed that all were members of criminal organisations. One of Port-au-Prince's gang leaders, Jimmy Cherizier, condemned the attack, threatening to respond with drones of his own, potentially killing "anyone in the country" (Vyas, 2025).

4.3. PROPOSED SOLUTIONS

The problem facing Latin American states is extremely serious, and three recommendations have been compiled from a variety of perspectives that should form the guiding principles of the anti-UAS policy that these nations develop: attack the supply lines, learn from the experts, and invest in training and tactics (Ziemer, 2025).

It is necessary to recognise that the fight against the supply lines of illegal organisations is inseparable and intrinsic to the fight against the groups themselves. Nonetheless, victory for states, at least in terms of drones, will necessarily come from the approach of attacking supply lines.

There is therefore an opportunity to perhaps take inspiration from Operation *Grim Beeper*, carried out by Israel's intelligence services, which infiltrated Hezbollah's supply chain of "fighters" with the end result we are all familiar with (Doran, 2024).

For their part, learning from experts and investing in research and tactics means making the most of the information that the countries most involved in this development - Ukraine, Russia and Israel - can offer.

5. APPLYING LESSONS

Many lessons can be drawn from an analysis of the experiences of Syria, Ukraine, Israel, Mexico and Colombia. The ones that we consider most salient are:

A. UAS are particularly effective when compared to their price and destructive capability.
B. The fibre-optic link makes it possible to avoid the incapacitation of drones by radio frequency jamming devices.
C. The strength of a UAV action generally relies on late detection and swarm tactics for its success.
D. Advances in artificial intelligence are leading to the emergence of autonomous drones with the ability to recognise their environment and designate their targets.
E. The use of drones makes it possible to remove the maximum number of personnel from the operation before it begins, reducing own casualties to virtually zero.

These lessons will have to be duly taken into account when dealing with the possible use of UAS as terrorist tools.

Similarly, it should always be borne in mind that groups that have the capability to use drones will use them. This technology and techniques are easy to adapt to different modes of operation and environments, as demonstrated by their recent incorporation into the organised crime scene in Brazil. On 28 October 2025, as part of an operation against the *Red Command* structure in Rio de Janeiro, the Red Command used combat drones against security force agents. The *Red Command* is the largest organised crime organisation in Brazil, and has already incorporated Unmanned Aerial Systems (UAS) into its operations (Braun, 2025).

5.1. LESSONS LEARNED FROM PREVIOUS ATTACKS

5.1.1. 9/11 Attacks

In the report issued by the 9/11 Commission of Inquiry on 22 July 2004 (*National Commission on Terrorist Attacks*, 2004), the eleventh chapter: "Foresight and Hindsight" makes a critical judgement detailing the four main weaknesses in the US counterintelligence and counterterrorism system that made possible the commission of the largest attack by number of casualties in history: lack of imagination, inadequate policy towards Al-Qaeda, misuse of federal government capabilities, and serious errors in the operational management of the attack as such. Inadequate policy and misuse of

capabilities are more a matter of dealing with an emerging enemy, so we understand that they are beyond the scope of this article.

Of the two that we are going to analyse, the most critical is the lack of imagination, as the other stems directly or indirectly from this. The first of the errors was the US intelligence community's classification of risk. The head of the counter-terrorism office, Richard A. Clarke, argued in a 4 September 2001 memo that some of the counter-terrorism agencies regarded the attacks as "a nuisance that kills a number of Americans every 18-24 months". Even those who did see the risk as real, such as Clarke, wrote hypothetical scenarios in which "hundreds" of Americans fell victim to terrorism. Virtually no one imagined a possible scenario such as the one that eventually occurred.

The report also mentions that the intelligence community almost completely ignored the possibility of a plane being used as a suicide vehicle, even though suicide attacks had been becoming the most common in the Middle East. If an exercise had been conducted by putting oneself in the shoes of a terrorist who wanted to use a hijacked plane, the security lapses that would become evident in the aftermath of 9/11 might have been detected. Indeed, the issue was even raised on occasion by bodies outside the intelligence community and in all cases dismissed by the intelligence community as extremely unlikely. This was set out in the report of the 9/11 Commission of Inquiry, pages 345-348 (*National Commission on Terrorist Attacks*, 2004).

No less serious were the mistakes made in the operational handling of the actions that made the attack possible. Of particular note was the lack of coordination between federal agencies, mainly the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI). All the preparatory actions were detected by a US institution (the previous meeting in Kuala Lumpur, the entry of the suspects into US territory, the training of the suspects as pilots, and a long etcetera), but there was no good communication of this information, which meant that the FBI did not consider including the presence of the suspects they had located in the report on the risk of imminent attacks.

5.1.2. Barcelona and Cambrils attacks

Something similar may have happened in the attacks that unfortunately shook Spain in 2017 in Barcelona and Cambrils. The competent authorities reportedly decided not to act on the official notice issued by the then Commissioner General of Citizen Security of the National Police, Florentino Villabona Madera, which called for the installation of "large planters or bollards at the entrances (to places with a high number of people)" (Redacción Barcelona La Vanguardia, 2017). In this case, the imagination of the Security Forces and Corps did not fail, although that of those in charge of putting their recommendations into practice did. The same shortcomings were seen in terms of police coordination, and an alleged warning sent by the CIA on 25 May 2017 warning of ISIL's intention to attack La Rambla in Barcelona may have been ignored (El Periódico Barcelona, 2017).

5.1.3. Summary of lessons learned

The lack of imagination and coordination of institutions are two of the cardinal sins in the fight against terrorism. The new age of technology forces us to rethink how potential terrorists will act in the future, with the likely use of drones, artificial intelligence, or the

lethal combination of both in the next attempted terrorist attacks, as well as other tools still under development.

5.2. POSSIBILITIES FOR TERRORIST ATTACKS USING DRONES

5.2.1. Attacks against crowds of people

In terms of attacks against large crowds of people, the Las Vegas mass shooting of 1 October 2017 is noteworthy, in which a subject seized an arsenal valued at $95,000 and opened fire from a suite in the Mandalay Bay hotel at an open-air festival adjacent to the hotel, resulting in 60 fatalities and 867 injuries. This incident demonstrated how ineffective facility access control measures can be if the risk comes from above (Las Vegas Metropolitan Police Department, 2018).

It does not require a great stretch of the imagination to think how destructive this same attack could have been, but using Unmanned Aerial Vehicles (UAVs) dropping explosive charges of several kilos on the crowd, especially considering that the attack took place at night, which in reality already had tragic consequences, as a climate of total chaos was imposed on those present.

5.2.2. Attacks on individuals

The possibility of attacks on high-ranking state authorities should not be ruled out either. Venezuelan President Nicolás Maduro suffered an attack with explosive drones during a military parade on 4 August 2018 (El Mundo, 2018). Thus, not only are such attacks possible, but they have already been attempted.

We know that, while difficult, it is not impossible to get dangerously close to high authorities, as the assassination attempt on then US presidential candidate Donald Trump on 13 July 2024 demonstrated. Thomas Crooks managed to get within 150 metres of Trump armed with an AR-15 rifle, and even managed to fire eight rounds before being shot down by Secret Service agents (*Task Force on the Attempted Assassination of Donald J. Trump*, 2024).

A hypothetical drone strike would not have had to get as close as a shooter, and could more easily camouflage itself in the surrounding area before launching a fibre-optic guided drone or a swarm of drones equipped with AI-guided software targeting Donald Trump.

5.2.3. Attacks against aviation and other sectors

The aviation sector can also be the target of this type of attack. Similar to Operation Spiderweb, drones could in the future recognise the engines, fuel tanks or cockpit window of an aircraft and collide with them during take-off or landing. Considering that a Boeing 737-800 or an Airbus A320 (the two most common commercial aviation models) can carry more than 180 passengers, an effective impact against a single aircraft would immediately become the second largest attack in Spain's history.

The options are countless: trains stopped by a first drone and then started to be attacked with secondaries, attacks combining known methods of terrorism and using drones to attack people fleeing through bottlenecks, to name a few examples.

5.3. ATTACKING THE SUPPLY LINE

The advantages for terrorists are also innumerable: they do not have as a *conditio sine qua non* the death of the executor, preparatory actions are not carried out at the site of the attack, making early detection difficult (no one can find a backpack bomb that is not there) and they are widely sold in civilian markets, so they do not arouse as much suspicion as other methods.

Perhaps part of a correct perspective on combating drone attacks is to recognise that stopping them once they are underway is going to be an increasingly complex, if not sometimes impossible, task; just as Russia cannot have large air defence units on every square metre of its territory, neither can we. Drones should not be dealt with when they are already flying towards their target, but when they are in a box being transported from one place to another.

5.4. SENSITIVE STAGES IN THE PROCESS OF PREPARING A UAS ATTACK

We have been able to detect at least 4 delicate processes in the preparation of a terrorist action with drones: the procurement of the drones, the training of the pilots, the programming of the drones and the procurement of the explosives.

Procuring large numbers of Unmanned Aerial Systems (UAS) in the European Union, and more specifically in Spain, would not be the most sensitive part of the operation. Although it is mandatory to be registered and licensed to fly drones weighing more than 250g, these restrictions do not apply to the simple act of buying one. This brings to light a deficiency. Excessive and illogical stockpiling of these products should always be monitored, which is deeply undermined by this freedom to purchase. All the more so when they can be made in any establishment in the European Union, or even in other nations, while no customs permit is required for the import of UAS for personal use. Drones resulting from the work of 3D printers should also be considered.

The training of pilots could provide a good opportunity to disrupt the commission of the attack, particularly if they try to obtain it through legal channels. American intelligence services may have already come close to thwarting 9/11, at least in the way the terrorists had organised it, when the FBI issued a report in July 2001 on the interest suspected jihadists were taking in flight training entitled "Islamic Extremist Learns to Fly" (National Commission on Terrorist Attacks, 2004).

Particular attention will need to be paid to what happens when hostilities in Ukraine end, and Ukrainian and Russian attack drone pilots try to reintegrate into society. So far, studies on the psychological effects of operating attack drones have focused almost exclusively on US unmanned bomber pilots, who by the nature of their actions are subjected to considerably less stress than Ukrainian and Russian operators.

Programming the devices to follow specific instructions using Artificial Intelligence (AI) requires advanced knowledge in several technical areas, such as Python

doi: https://doi.org/10.64217/logosguardiacivil.v4i1.8472

and C++ programming, AI training, robotics and electronics. It is not particularly time-consuming, but a sudden interest of a suspicious subject in these areas of knowledge should be an immediate red flag.

As with the previous point, the possibility that veterans of the Ukrainian war, or others similar in terms of massive drone use, might be involved in the preparation of these operations, or even actively participate, should be raised. The drone teams of these conflicts have a technical knowledge of adapting package drones to specific missions that far exceeds that of virtually any other individual.

Finally, the acquisition of explosives is, logically, the most fragile process of the whole *iter criminis*. This is accentuated when we take into consideration that Unmanned Aerial Systems (UAS), due to their technical characteristics, cannot carry excessively heavy charges, forcing potential terrorists to resort to explosive substances with greater detonation potential, which could reduce the search for these attempts to a certain extent.

6. CONCLUSIONS

A. Drones are here to stay. There is no doubt that their use will increase enormously. The experiences of countries that have been involved in conflicts with drones should be added to their own procedures.

B. Operation Cobweb conducted by the Ukrainian Security Service (SBU) against the Russian strategic long-range fleet demonstrated the versatility of drone actions against targets thousands of kilometres behind the front line. These assets have demonstrated their ability to be infiltrated, distributed and operated over long distances. Extrapolating from this experience, one can deduce the destructive capability of a group determined to eliminate infrastructure in a civilian area, given the necessary resources.

C. The use of Artificial Intelligence (AI) in this operation, coupled with the already documented instances of the use of these tools, dramatically changes the future threat scenario. Attack drones will end up as AI-guided explosive devices with the tools required to differentiate allies from enemies and eliminate them.

D. Transnational Criminal Organisations in Latin America have moved steadily into the technological battle for dominance of the skies. Their established networks for trafficking all kinds of materials and substances have allowed them to accumulate large numbers of Unmanned Aerial Systems (UAS), which are performing surveillance, transport and attack tasks. They have had their own specialised units since 2021 and are currently beginning to invest in anti-drone material.

Attacks, although timid and small at first, are becoming increasingly ambitious, even targeting enemy convoys on the move. The civilian population has also suffered as a result of the introduction of these technologies in conflicts between criminal groups, with direct and indiscriminate attacks on populations increasingly frequent in Mexico and Colombia.

In the latter country, the armed forces and security forces are the target of considerable attacks, which could be a precursor to other actions on a scale not yet seen on this continent.

E. Experience in all theatres has shown that the success of a drone action against a defended target lies in the swarm.

F. Attack drones have been shown in Ukraine to be extremely useful assets in the context of war, and in South America they can be used to spread terror among populations and state security units, especially if their operations serve the interests of large organisations with a logistical and military capacity greater than that of some sovereign states.

It seems a reality that sooner or later these forms of violent action will reach the West, as well as Spain. We must be prepared, and remember the mistakes made in the past so as not to repeat them in the future.

G. Imagination and the ability to manage these scenarios are two fundamental requirements for dealing with new threats. Several terrorist attacks in the past have been

doi: https://doi.org/10.64217/logosguardiacivil.v4i1.8472

made possible by incorrect risk analysis. The emergence of AI-enabled drones opens the door for terrorists to find opportunities where previously it would have been unthinkable, both for them and for security forces.

Perhaps the most effective way to deal with them might be to intercept attempts during their preparation phase. The stockpiling of drones, training of pilots, programming of UAS and procurement of explosives would all seem to be ideal times to thwart attempted attacks on civilians.

Security should not be neglected either. Small attacks would be more difficult to detect, although, unlike complex attacks, they could be stopped during their execution.

Finally, we must stress the urgent need to take advantage of the experience being acquired in this sector by countries currently involved in conflicts where the presence and use of drones is commonplace. Such information could be decisive in future investigations against terrorist cells determined to perpetrate an attack against our territory.

7. BIBLIOGRAPHICAL REFERENCES

12th Special Forces Brigade "Azov" (n.d.). *About Azov*. Retrieved 3 September 2025 from https://azov.org.ua/en/about-azov/.

UNHCR (2025). *Urgent Need to Strengthen Response to Unprecedented Mass Displacement in Catatumbo, Colombia.* https://www.acnur.org/noticias/comunicados-de-prensa/acnur-urge-fortalecer-la-respuesta-frente-al-desplazamiento-masivo-sin-precedentes-en-el-catatumbo-colombia

AFP (2017). An explosive drone, the latest organised crime device in Mexico. *El País.* https://elpais.com/internacional/2017/10/24/mexico/1508802891_139491.html

BBC (2018). Syria war: Russia thwarts drone attack on Hmeimim airbase. *BBC.* https://www.bbc.com/news/world-europe-42595184

Barnes, J. E., Entous, A., Schmitt, E., Troianovski, A. (2023). Ukrainians Were Likely Behind Kremlin Drone Attack, U.S. Officials Say. *The New York Times.* https://www.nytimes.com/2023/05/24/us/politics/ukraine-kremlin-drone-attack.html

Balkan, S. (2017). DAESH's Drone Strategy. Technology and the Rise of Innovative Terrorism. *Foundation for Political, Economic and Social Research (SETA).* https://media.setav.org/en/file/2017/08/daeshs-drone-strategy-technology-and-the-rise-of-innovative-terrorism.pdf

Boffey, D. (2025). Killing Machines: how Russia and Ukraine's race to perfect deadly pilotless drones could harm us all. *The Guardian.* https://www.theguardian.com/world/2025/jun/25/ukraine-russia-autonomous-drones-ai

Bondar, K. (2025). How Ukraine's Operation Spider's Web" Redefines Asymmetric Warfare. *Center for Strategic & International Studies.* https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

Braun, J. and Toledo, L. F. (2025). Comando Vermelho: how imported drones and rifles are ending up in the hands of organised crime in Brazil and transforming urban conflict. *BBC.* https://www.bbc.com/mundo/articles/c4g32d0rzr5o

Connable, B. (2025). Putting Operation Spider's Web in Context. *Irregular Warfare.* http://irregularwarfare.org/articles/putting-operation-spiders-web-in-context/

De Troullioud de Lanversin, J. (2025). Ukrainian attack on Russian bombers show how cheap drones could upset global security. *Bulletin of the Atomic Scientists.* https://thebulletin.org/2025/06/ukrainian-attack-on-russian-bombers-shows-how-cheap-drones-could-upset-global-security/#:~:text=The%20drones%20were%20likely%20%E2%80%9COsa,for%20Strategic%20and%20International%20Studies

Dempsey, J. (2025). Operation Spiderweb: an assessment on Russian Aerospace Force losses. *International Institute for Strategic Studies.* https://www.iiss.org/online-analysis/military-balance/2025/062/operation-spiderweb-an-assessment-of-russian-aerospace-forces-losses/

Department of Defense (2000). DOD Directive 12/2000.

Doran, M. (2024). The Brilliance of "Operation Grim Beeper". *Hudson Institute.* https://www.hudson.org/technology/brilliance-operation-grim-beeper-lebanon-pager-explosion-israel-iran-michael-doran

Drug Enforcement Administration (2025). *2025 National Drug Threat Assessment.* https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf

El Mundo (2018). Maduro denounces "an assassination attempt" with explosive drones and blames President Santos. *El Mundo.* https://www.elmundo.es/internacional/2018/08/05/5b662beeca4741d0498b4648.html

El Periódico Barcelona (2017). Full text of the CIA's Barcelona attack alert to the Mossos. *El Periódico.* https://www.elperiodico.com/es/politica/20170831/texto-integro-alerta-cia-mossos-atentado-barcelona-rambla-6255316

First Contact (2025). *High-Acrobatic UAV Osa*. Retrieved 4 September 2025 from https://firstcontact.biz/en/projects/high-acrobatic-uav-osa/

Gibson, O., Harvey, A., Novikov, D., Harvard, C. and Stepanenko, K. (2025). Russian Offensive Campaign Assessment, June 1, 2025. *Institute for the Study of War.* https://understandingwar.org/research/russia/russian-offensive-campaign-assessment-june-1-2025/

Grillo, I. (2024). Drone Warfare in Guerrero. *CrashOut by Ioan Grillo.* https://www.crashoutmedia.com/p/la-guerra-de-drones-entre-carteles

Hambling, D. (2025). New Drone Tactics Sealed Russian Victory in Kursk. *Forbes.* https://www.forbes.com/sites/davidhambling/2025/03/17/new-drone-tactics-sealed-russian-victory-in-kursk/

Hambling, D. (2016). How Islamic State is using consumer drones. *BBC.* https://www.bbc.com/future/article/20161208-how-is-is-using-consumer-drones

Human Rights Watch (2024). *Report for the Universal Periodic Review of El Salvador (United Nations 48th session; 4th cycle).* https://www.hrw.org/es/news/2024/07/30/informe-para-el-examen-periodico-universal-de-el-salvador

Jaramillo, J. C. (2025). Drones Fuel Criminal Arms Race in Latin America. *Insight Crime.* https://insightcrime.org/news/drones-fuel-criminal-arms-race-latin-america/

Jiménez, X. (2025). La Mayiza' puts armed forces in check in Sinaloa with elite anti-drone equipment. *Milenio.* https://www.milenio.com/policia/mayiza-combate-fuerzas-armadas-equipo-anti-dron-elite

Khomenko, I. (2024). How Ukraine is Using AI Drones to Outsmart Russia on the Battlefield. *United24 Media.* https://united24media.com/latest-news/how-ukraine-is-using-ai-drones-to-outsmart-russia-on-the-battlefield-3833

Las Vegas Metropolitan Police Department (2018). *LVMPD Criminal Investigative Report of the 1 October Mass Casualty Shooting.* https://www.lvmpd.com/home/showpublisheddocument/134/638298568313170000

Loh, M. (2025). Ukraine's drone jammers are proving decisive amid a new push on Russian soil, pro-Kremlin milbloggers say. *Business Insider.* https://www.businessinsider.com/ukraine-drone-jammers-killing-it-new-kursk-push-russian-bloggers-2025-1

Lyle, P. (2019). Air Power Proliferation: How Commercial-off-the-Shelf Drones are Being Used by Violent Extremist Organizations to Influence the Future of Warfare in the Air. *Air and Space Power Review, 22*(3). https://www.raf.mod.uk/what-we-do/centre-for-air-and-space-power-studies/aspr/aspr-vol22-iss3-6-pdf/

MacDonald, A. (2025). AI-Powered Drone Swarms Have Now Entered the Battlefield. *The Wall Street Journal.* https://www.wsj.com/world/ai-powered-drone-swarms-have-now-entered-the-battlefield-2cab0f05

Maza, J. (2025). Drones and Technological Lethality of Mexican Cartels. *Mexican Council on International Affairs.* https://www.consejomexicano.org/mediateca/articulo/7275

Méheut, C. (2025). Ukraine Turns to Fishing Nets to Catch Russian Drones. *The New York Times.* https://www.nytimes.com/2025/07/07/world/europe/ukraine-russia-drones-nets.html

Mendoza López, D. (2025). Golpean al CJNG en Campeche: caen "El 80", "Lady Drones" y tres sicarios tras operativo en Champotón. *Infobae.* https://www.infobae.com/mexico/2025/08/14/golpean-al-cjng-en-campeche-caen-el-80lady-drones-y-tres-sicarios-tras-operativo-en-champoton/

National Commission on Terrorist Attacks (2004). *The 9/11 Commission Report.* https://www.9-11commission.gov/report/911Report.pdf

Naber, I. (2025). Why Ukraine Remains the World's Most Innovative War Machine. *Politico.* https://www.politico.com/news/magazine/2025/08/27/ukraine-drones-war-russia-00514712

Ortiz, J. (2023). El Caracol: el pueblo guerrerense asediado por narcodrones. *La Silla Rota.* https://lasillarota.com/estados/2023/9/4/el-caracol-el-pueblo-guerrerense-asediado-por-narcodrones-445996.html

Page, J. M. (2025). Drones and the Hamas-led Attack of 7 October 2023: Innovation and Implications. *Perspectives on Terrorism.* https://www.jstor.org/stable/27372135

Price, R. E. (2025). Defining Swarm: A Critical Step Toward Harnessing the Power of Autonomous Systems. *Military Review Online Exclusive.* https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2025/Defining-Swarm/Defining-Swarms-UA.pdf

Redacción Barcelona La Vanguardia (2017). The document with which the police recommended placing bollards at entrances to crowded places. *La Vanguardia.* https://www.lavanguardia.com/politica/20170819/43665066008/documento-policia-recomendo-instalar-bolardos-accesos-lugares-concurridos.html

Reuter, C. (2000). *The V2, and the Russian and American Rocket Program*. S.R. Research & Publishing.

Salinas, A. (2018). Drone with grenades falls on Baja California Public Security Secretary's house. *Excelsior.* https://www.excelsior.com.mx/nacional/dron-con-granadas-cae-en-casa-del-secretario-de-seguridad-publica-de-baja-california

Saumeth, E. (2025). FARC attacks a third Colombian Navy river patrol boat with drones. *Infodefensa.* https://www.infodefensa.com/texto-diario/mostrar/5404281/125-colombia

Secretariat of National Defence (SEDENA) (2024). *Mexican Army and National Guard detained Armando "N" alias "Delta 1", alleged leader of the Jalisco Cartel - New Generation in Michoacán and Jalisco.* https://www.gob.mx/defensa/prensa/ejercito-mexicano-y-guardia-nacional-detuvieron-a-armando-n-alias-delta-1-presunto-lider-del?tab=

Skinner, B. F. (1960). Pigeons in a pelican. *American Psychologist*. American Psychological Association. https://www.appstate.edu/~steelekm/classes/psy3214/Documents/Skinner1960.pdf

Tangredi, S. J. (January 2023). Bigger Fleets Win. *Proceedings.* https://www.usni.org/magazines/proceedings/2023/january/bigger-fleets-win

Task Force on the Attempted Assassination of Donald J. Trump (2025). *Final Report Findings and Recommendations.* https://taskforce.house.gov/sites/evo-subsites/july13taskforce.house.gov/files/evo-media-document/12-5-2024-Final-Report-Redacted.pdf

Torrado, S. (2025). Dissidents multiply drone attacks and set off alarm bells in Colombia. *El País.* https://elpais.com/america-colombia/2025-08-30/las-disidencias-multiplican-los-ataques-con-drones-y-encienden-las-alarmas-en-colombia.html

Torres, M. (2024). A child dies after a drone attack by FARC dissidents in Cauca. *CNN Español.* https://cnnespanol.cnn.com/2024/07/24/nino-muere-ataque-drones-disidencias-farc-cauca-colombia-orix

Valencia, N. (2015). Drone carrying drugs crashes south of U.S. border. *CNN.* https://edition.cnn.com/2015/01/22/world/drug-drone-crashes-us-mexico-border

Villegas, P. (October 2025). Amid cartel war, funeral workers carry Sinaloa's grief. *The New York Times.* https://www.nytimes.com/es/2025/10/24/espanol/america-latina/sinaloa-muertes-trabajadores-funerarios.html

Villegas, P. (September 2025). Drones and improvised explosives: Mexico's cartels adopt weapons of modern warfare. *The New York Times.* https://www.nytimes.com/es/2025/09/01/espanol/america-latina/mexico-carteles-armas.html

Vyas, K. (2025). Haiti's Beleaguered Government Launches Drones Against Gangs. *The Wall Street Journal.* https://www.wsj.com/world/americas/haiti-drones-gangs-fight-27e8341f?gaa_at=eafs&gaa_n=ASWzDAh20VgfmnFWwEE7OjowH1KxYc34z1aFI1uRw1vF-bKPi6aj4r7cWJlndm9cN1U%3D&gaa_ts=6841c7eb&gaa_sig=rJSPFiTqfMVMvHpXOVl9jsTqFd52rHCtmsgOdyDTpuRUVJ13ks5cvK5_LMvUMG6mn7gI_qSmKfkG5KLkeR4UAg%3D%3D

W Radio Colombia [@WRadioColombia] (10 June 2025). *#After the chain of attacks in Cauca and Valle del Cauca, the FARC's Central General Staff issued* [Recommendations to the civilian population]. X. https://x.com/WRadioColombia/status/1932474602267021560

Zelenskyy, V (1 June 2025). Speech to the Nation on the Operation Spiderweb Drone Strike [Transcript]. American Rhetoric. https://www.americanrhetoric.com/speeches/volodymyrzelenskyoperationspiderweb.htm

Ziemer, H. (2025). Illicit Innovation: Latin America Is Not Prepared to Fight Criminal Drones. *Center for Strategic & International Studies.* https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones

8. LEGISLATION

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and third country operators of unmanned aircraft systems. 11 June 2019. OJEU No 152.

Royal Decree 517/2024 of 4 June developing the legal regime for the civil use of unmanned aircraft systems (UAS), and amending various regulations on import control of certain products with respect to the applicable product safety standards; civil air demonstrations; firefighting and search and rescue and airworthiness requirements and licensing requirements for other aeronautical activities; registration of civil aircraft; electromagnetic compatibility of electrical and electronic equipment; air regulations and licensing requirements for other aeronautical activities; firefighting and search and rescue and airworthiness and licensing requirements for other aeronautical activities; civil aircraft registration; electromagnetic compatibility of electrical and electronic equipment; air regulations and common operating rules for air navigation services and procedures; and civil aviation occurrence reporting. 5 June 2024. BOE No. 136.

NORMA Oficial Mexicana NOM-107-SCT3-2019, Que establece los requerimientos para operar un sistema de aeronave pilotada a distancia (RPAS) en el espacio aéreo mexicano (Mexican Official Mexican Standard NOM-107-SCT3-2019, Establishing the requirements for operating a remotely piloted aircraft system (RPAS) in Mexican airspace. 14 November 2019.

doi: https://doi.org/10.64217/logosguardiacivil.v4i1.8472