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

**Article de recherche**

# LA MORT D'EN HAUT : UTILISATION DE DRONES D'ATTAQUE PAR DES ORGANISATIONS TERRORISTES

*Traduction en français à l'aide de l'IA (DeepL)*

**Diego de Lorenzo de Guindos**
**Sous-lieutenant de la Guardia Civil**
**Étudiant en licence d'ingénierie de la sécurité**
**delorenzodeguindos@gmail.com**

Reçu le 07/09/2025
Accepté le 19/11/2025
Publié le 30/01/2026

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

Citation recommandée : d' e Lorenzo, D. (2026). La mort venue d'en haut : utilisation de drones d'attaque par des organisations terroristes. *Revista Logos Guardia Civil*, 4 (1), 53–82. https://doi.org/10.64217/logosguardiacivil.v4i1.8472


Dépôt légal : M-3619-2023
NIPO en ligne : 126-23-019-8
ISSN en ligne : 2952-394X

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

# LA MORT VUE D'EN HAUT : UTILISATION DE DRONES D'ATTAQUE PAR DES ORGANISATIONS TERRORISTES



**Résumé :** Les drones de petite taille sont de plus en plus présents dans les zones de conflit. Leur polyvalence, leur grande disponibilité et leur faible coût expliquent cette expansion. Cet article analyse la possibilité que ces appareils puissent être utilisés dans le cadre d'attentats terroristes, en examinant au préalable les utilisations qui en ont été faites dans les conflits armés, avec une attention particulière pour les actions à l'arrière, dont la nature pourrait inspirer la planification d'attaques. Afin d'évaluer l'utilité opérationnelle des drones pour des acteurs dont les capacités logistiques, économiques et opérationnelles sont inférieures à celles des États, leur utilisation par des organisations criminelles en Amérique du Sud sera également étudiée. Les conclusions obtenues seront mises en relation avec les vulnérabilités historiquement exploitées par les groupes terroristes pour échapper à l'action de l'État et mener à bien leurs opérations. L'article conclut que les drones constituent des outils particulièrement attrayants pour ces groupes et que leur prolifération implique l'apparition de nouvelles vulnérabilités qui devront être identifiées et corrigées afin de prévenir les attentats contre l'État ou ses citoyens.

**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.

**Mots clés :** Drones, intelligence artificielle, terrorisme, Ukraine, attentats.

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

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

## ABRÉVIATIONS

11-S : Attentats du 11 septembre

CDS : Cartel de Sinaloa

CIA : Agence centrale de renseignement

CJNG : Cartel de Jalisco Nueva Generación

DEA : Administration américaine de contrôle des drogues

EIIL/EI : État islamique en Irak et au Levant

États-Unis : États-Unis d'Amérique

FARC : Forces armées révolutionnaires de Colombie

FBI : Bureau fédéral d'enquête

FPV : First Person View (vue à la première personne)

GPS : Système de positionnement global

IA : Intelligence artificielle

OCT : Organisations criminelles transnationales

RPAS : Système d'aéronefs pilotés à distance

SBU : Service de sécurité ukrainien

UAS : Systèmes aériens sans pilote

UAV : Véhicules aériens sans pilote

## 1. INTRODUCTION

L'être humain a toujours utilisé les progrès scientifiques pour accroître sa capacité militaire. Dans certains cas, il a adapté les découvertes existantes à des fins militaires ; dans d'autres, c'est précisément la nécessité d'obtenir des moyens de destruction plus puissants et plus efficaces que ceux de ses adversaires qui a été à l'origine de véritables révolutions technologiques.

L'une de ces périodes de conflit a déclenché une explosion scientifique sans précédent dans tous les domaines : la Seconde Guerre mondiale. Parmi tous les projets, les grandes idées et les découvertes, nous aimerions nous attarder particulièrement sur deux d'entre eux afin d'analyser leurs conséquences à long terme : les projets allemands qui ont conduit à l'utilisation des missiles balistiques V1 et V2, ainsi que le « projet Paloma ».

Tout d'abord, les projets allemands qui ont conduit à l'utilisation des missiles balistiques V1 et V2. Ils pouvaient être lancés depuis le territoire de la France occupée et atteindre des villes en Angleterre, où ils ont causé de véritables ravages (Reuter, 2000).

Deuxièmement, un projet moins connu, mais non moins révolutionnaire, était le « projet Paloma » du psychologue américain B.F. Skinner visant à développer des missiles antinavires guidés par la technologie IA (bien que dans ce cas, IA signifierait « intelligence animale »). S'appuyant sur les conclusions du chien de Pavlov, Skinner a conclu que les pigeons pouvaient être entraînés à picorer continuellement un point qu'ils voyaient sur un écran. Ce point aurait à un moment donné été un véritable navire ennemi, et les points où le pigeon picorait envoyaient des signaux aux commandes du missile pour modifier sa trajectoire. Le projet a été suspendu en 1953 en raison des progrès réalisés dans le domaine des mesures de guidage électronique (Skinner, 1960).

Bien que ces deux projets aient peu de rapport direct avec le développement des drones, ils ont été les premiers à mettre en œuvre des idées qui sont aujourd'hui une réalité. Le premier proposait de pouvoir attaquer des cibles ennemies à grande distance avec des missiles qui ne mettaient en danger la vie d'aucun pilote, et le second était le premier pas vers des systèmes d'armes capables de penser par eux-mêmes et de prendre leurs propres décisions, sans intervention humaine et sans émettre de rayonnement électromagnétique pour détecter les cibles, car les pigeons le faisaient en interprétant des images. Ces expériences ont jeté les bases conceptuelles de l'automatisation des armes, une idée qui, des décennies plus tard, allait évoluer vers les drones de combat actuels.

À l'heure actuelle, en septembre 2025, nous n'avons pas de pigeons pour guider les projectiles planants lancés depuis des avions. À la place, nous avons de petits appareils volants chargés d'explosifs, capables de comprendre où ils se trouvent, où ils doivent aller, quelle est leur mission, et de reconnaître les cibles potentielles afin de décider laquelle est la plus appropriée et de s'écraser dessus, faisant exploser les explosifs au passage.

Ce phénomène est désormais considéré comme faisant partie intégrante du paysage militaire contemporain, mais peut-être avec une délimitation spatiale trop confiante : il s'agit d'un phénomène propre aux lignes de front des guerres. Cependant, les actions continues menées par l'Ukraine et la Russie à l'arrière avec des drones à des centaines de kilomètres du front, et les informations qui nous parviennent d'Amérique du

Sud concernant leur utilisation par des groupes d' u de criminalité organisée nous font soupçonner les utilisations possibles que des groupes terroristes pourraient faire de ces appareils.

L'objectif du présent article est d'analyser, en premier lieu, le potentiel des moyens aériens sans pilote pour être utilisés dans des attaques dirigées contre des cibles militaires, ainsi que des exemples historiques récents de cette utilisation. Ensuite, nous explorerons la transposition de ces systèmes à des organisations opérant en marge de l'État qui s'est produite dans des pays d'Amérique du Sud, principalement au Mexique, en Colombie et au Brésil. Enfin, nous nous appuierons sur des attentats terroristes passés pour mettre en évidence les erreurs commises qui ont permis leur perpétration. Toutes les sections précédentes viendront étayer la thèse finale, selon laquelle les drones constituent un système particulièrement attractif pour ceux qui cherchent à mener des attaques contre de grandes masses de personnes, ainsi que contre des cibles spécifiques.

Dans le cadre du présent article, la définition du terrorisme retenue est celle qui figure dans une directive du ministère américain de la Défense : « recours calculé à la violence ou à la menace de violence contre des personnes ou des biens, dans le but d'instiller la peur, afin de contraindre ou d'intimider le gouvernement ou les sociétés pour atteindre des objectifs politiques, idéologiques ou religieux » *(ministère américain de la Défense,* 2000). Toutefois, les actions qui se manifestent par les mêmes comportements externes, même si elles ne poursuivent pas un objectif politique, idéologique ou religieux, seront considérées de manière analogue.

Afin de délimiter le champ d'application de cet article, l'utilisation de drones de grande taille sera ignorée. Cela tient compte de leur faible disponibilité et de leur plus grande facilité de détection. Sont donc exclus de cette étude les drones utilisés par l'armée de l'air américaine, ceux appartenant aux forces ukrainiennes et russes, ainsi que tout autre drone de même nature.

L'objet de cette étude est donc défini comme étant l'utilisation de drones de petite taille par des groupes poursuivant des actions violentes contre des groupes de personnes, des personnalités importantes, des biens importants pour la société et tout autre élément entrant dans la définition d'un attentat.

## 2. DRONES D'ATTAQUE DANS LES GUERRES CONVENTIONNELLES

### 2.1. GUERRE CIVILE SYRIENNE

Le rôle des drones de petite taille dans les conflits a connu une augmentation progressive jusqu'à ce que nous connaissons aujourd'hui. Les premières utilisations d'importance ont pu être détectées pendant la guerre civile syrienne, où plus précisément, l'État islamique en Irak et au Levant (EIIL/EI) a exploré les possibilités offensives des véhicules aériens sans pilote (UAV) (Hambling, 2016).

Dans ce contexte, la première utilisation enregistrée de drones comme outils d'attaque a été la combinaison de drones et de voitures piégées avec lesquelles l'EI a attaqué ses ennemis lors de la bataille de Mossoul. Les drones ont effectué des missions de reconnaissance des cibles, puis ont guidé les véhicules explosifs dans les rues de la ville (Balkan, 2017).

L'utilisation des drones comme arme de guerre a évolué lorsque des charges explosives ont été ajoutées aux UAV, qui ont ensuite été larguées sur les positions ennemies. Ce modèle a été exporté vers les combats de l'EIIL à Deir ez-Zor et les offensives contre les Kurdes en Syrie.

Les incidents d'attaques par des drones kamikazes à vision à la première personne (FPV) étaient rares au début, mais leur fréquence allait augmenter avec le temps (Lyle, 2019).

## 2.2. GUERRE EN UKRAINE

Un autre scénario notable a été le conflit dans le Donbass, qui a débuté en 2014. Le rôle initial des drones était de repérer des cibles qui seraient ensuite prises pour cible par l'artillerie. Ces drones, parfois équipés de moyens de vision nocturne, ont commencé à être connus des militaires des deux camps en raison de leurs bourdonnements nocturnes, qui étaient généralement immédiatement suivis de salves tirées par les pièces ennemies.

Cependant, l'évolution des petits drones en tant qu'armes de guerre allait entrer dans une spirale d'innovation après le début de l'attaque russe contre l'Ukraine le 24 février 2022, qui s'est soldée par un échec, et la guerre qui s'en est suivie et qui, en novembre 2025, ne semble pas près de prendre fin.

Comme on a pu le voir en Syrie, les drones ont été rapidement modifiés à l'aide de moyens artisanaux afin de pouvoir transporter des explosifs, tels que des grenades ou des obus de mortier, et les larguer sur les positions défensives ennemies. La première différence qui est apparue sur ce théâtre d'opérations a été l'émergence rapide des attaques par drones à vision à la première personne (FPV). Il s'agissait de quadricoptères équipés d'une charge explosive avec des détonateurs à impact (Naber, 2025).

Ce changement de paradigme a offert aux deux camps la possibilité d'exécuter des actions précises contre des cibles spécifiques, facilitant ainsi le succès des opérations, mais entraînant la perte d'au moins un appareil par action.

L'utilisation des drones a augmenté de manière exponentielle pendant les premières phases de la guerre, jusqu'à atteindre la situation actuelle, où les deux armées disposent d'unités spécialisées dans les attaques avec des systèmes aériens sans pilote (UAS) intégrées à un très bas niveau. Par exemple, la 12e brigade des forces spéciales « Azov » de l'armée ukrainienne dispose d'une compagnie de drones dans chaque bataillon de combat, ainsi que d'un bataillon supplémentaire d'UAS pour soutenir la brigade. On observe une situation similaire dans d'autres unités des deux armées (12e brigade des forces spéciales « Azov », s.f.).

À ce moment-là, l'Ukraine et la Russie se sont lancées dans une course technologique, cherchant à trouver des remèdes contre les drones, tout en les améliorant. Par exemple, des réseaux anti-drones ont commencé à être déployés dans des positions défensives et sur les principales voies logistiques, ce qui a été immédiatement suivi par des tactiques en tandem : un premier drone brisait le réseau, puis un second entrait en action pour atteindre les cibles (Méheut, 2025).

Afin de protéger les moyens les plus importants de chaque camp, l'utilisation d'inhibiteurs s'est généralisée pour contrecarrer les tentatives de destruction. Cela a provoqué une longue *impasse* sur les fronts. Les équipes de drones ont commencé à voir leur taux d'efficacité diminuer, à mesure que les inhibiteurs étaient distribués plus fréquemment. Les deux nations ont tenté de trouver des solutions à ce système défensif qui, bien que non infaillible, réduisait considérablement la capacité opérationnelle des UAS (Loh, 2025).

Au cours de l'été 2024, lors de l'invasion ukrainienne de l'oblast de Koursk, les premières initiatives importantes ont été enregistrées avec des drones reliés au terminal qui les contrôlait à l'aide de fins câbles à fibre optique. Le principal avantage de la connexion par câble est son immunité aux inhibiteurs. Il convient également de souligner qu'ils sont indétectables par les systèmes basés sur l'interception des ondes électromagnétiques et qu'ils assurent une meilleure connexion avec le terminal de contrôle, renvoyant des images de meilleure qualité et facilitant leur efficacité, car tant que la longueur du câble est suffisante, la connexion ne sera pas perdue (Hambling, 2025).

À l'heure actuelle, les progrès technologiques semblent s'orienter vers l'utilisation de plus en plus courante de drones autonomes guidés par l'intelligence artificielle. L'industrie de la défense ukrainienne travaille à la fabrication à grande échelle de modèles de drones capables de reconnaître eux-mêmes les situations tactiques, de les analyser correctement et de prendre les décisions optimales pour les intérêts ukrainiens. Le complexe militaro-industriel russe agit de la même manière. À la fin du mois d'août 2025, au moins 100 incidents de cette nature ont été recensés (MacDonald, 2025 ; Boffey, 2025 ; Khomenko, 2024).

Outre les actions menées en première ligne, depuis le début de la guerre en Ukraine, des actions de plus en plus complexes ont été menées dans les arrières-gardes ennemies, dans lesquelles les UAS des deux acteurs jouent un rôle crucial pour la réalisation des objectifs.

Les leçons tirées en Ukraine ont inspiré les opérations qui se sont déroulées ailleurs dans le monde. À titre d'exemple, lors du massacre du 7 octobre 2023 dans le sud d'Israël, le groupe Hamas a attaqué les positions frontalières des Forces de défense israéliennes avec des drones de petite taille (Page, 2025).

## 3. L'OPÉRATION TELARAÑA

### 3.1. L'ATTAQUE DU 1ER JUIN 2025

Le 1er juin 2025, les bases aériennes russes d'Olenya, Ivanovo Severny, Dyagilevo, Ukrainka et Belaya ont été attaquées à l'aube par les forces spéciales ukrainiennes. Il ne s'agissait pas de missiles balistiques ni de drones à longue portée, comme ceux que l'Ukraine avait fréquemment utilisés jusqu'alors. Des essaims de petits drones à vision à la première personne (FPV) ont attaqué les positions de l'armée de l'air russe.

L'attaque visait la flotte de bombardiers stratégiques que la Russie avait systématiquement utilisée dans sa campagne d'usure contre les infrastructures civiles ukrainiennes. Au final, 34 % de la flotte attaquée a été détruite ou mise hors d'état de nuire. De plus, ces modèles d'avions n'étaient plus produits depuis 1993, ce qui rendait

difficile la reconstruction de la capacité stratégique à longue portée. Sur le plan économique, l'Ukraine estime que les dommages causés s'élèveraient à environ 7 milliards de dollars (Gibson et al. 2025).

Il convient de souligner le fait que de petits drones FPV aient attaqué directement des bases aériennes ennemies extrêmement éloignées de la ligne de front, comme la base d'Ukrainka, située à plus de 5 800 km de la frontière internationalement reconnue de l'Ukraine et à plus de 6 000 km de la ligne de front. Pour mettre ces chiffres en perspective, cette distance est supérieure à celle qui sépare le centre de Madrid de Herat (Afghanistan), et pratiquement identique à celle qui sépare Madrid de Baltimore, aux États-Unis (USA).

Le Service de sécurité ukrainien (SBU) a réussi à attaquer des bases militaires situées à plus de 6 000 kilomètres en utilisant des modèles de drones qui effectuent généralement des missions tactiques très proches du front et dont la principale faiblesse est leur difficulté à se connecter au terminal de contrôle. Cela a été possible parce que les drones utilisés dans cette opération ont décollé à proximité de chacune des bases aériennes. Dans le cas de l'attaque contre la base aérienne de Belaya (la plus grande attaque de l'opération, avec 3 bombardiers Tu-95 et 4 bombardiers Tu-22M3 détruits), les drones FPV ont décollé d'une position située au sud-est de la base, à environ 8 kilomètres (Dempsey, 2025).

## 3.2. L'OPÉRATION

L'opération « Telaraña » du Service de sécurité ukrainien (SBU) a nécessité une phase de planification et de préparation de plus de 18 mois, selon le président ukrainien *Volodymyr Zelenskyy (Zelenskyy*, 2025*).* Des quadricoptères à vision à la première personne (FPV) « Osa » de la société ukrainienne *First Contact* (First Contact, 2025) ont été utilisés.

Les drones du modèle Osa se distinguent par l'emplacement de leurs composants électroniques sous un revêtement extérieur particulièrement épais et par la position fixe de leur port d'alimentation, alors que la plupart des modèles de drones FPV régulièrement utilisés par les forces armées ukrainiennes ont généralement un corps « squelettique », dans lequel les composants électroniques et le câblage sont souvent exposés. Après avoir pris en compte la complexité de la mission, la distance entre le lieu de préparation de l'opération et les cibles, ainsi que les conditions climatiques variées dans lesquelles l'infiltration devait se dérouler, le SBU a opté pour le modèle le plus robuste.

Au cours des 18 mois de préparation, le SBU a réussi à introduire 117 drones Osa en Fédération de Russie. Une fois à l'intérieur du territoire ennemi, une société écran de construction dédiée à la construction de maisons modulaires en bois a été créée pour dissimuler les mouvements. Ces modules d'habitation étaient équipés d'un faux plafond rétractable, dans lequel étaient dissimulées 9 rangées de 4 drones chacune, pour une capacité théorique totale de 36 drones par module. Parallèlement, des drones ont également été dissimulés dans des conteneurs de marchandises (Bondar, 2025).

Chaque module était également équipé d'un système de commande à distance, qui servait d'intermédiaire entre les 117 drones effectuant l'attaque et les 117 pilotes qui les contrôlaient depuis l'Ukraine. La liaison entre les systèmes de commande à distance et les positions des opérateurs a pu être établie par satellite.

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

Une fois les « chevaux de Troie » assemblés, le SBU a contacté des entreprises russes de transport de marchandises. Celles-ci ont acheminé les drones Osa vers les « points de livraison » des cargaisons, qui étaient en fait les emplacements prévus par le SBU pour le décollage ultérieur des drones.

Tôt le matin du 1er juin 2025, les couvercles des « chevaux de Troie » déjà infiltrés ont été soulevés, permettant aux drones de décoller et de se diriger vers leurs cibles. De nombreuses vidéos de civils russes ont été diffusées, montrant ces modules et conteneurs d'où sortaient des drones se dirigeant vers les nuages noirs causés par les explosions de ceux qui les avaient précédés.

Au bilan global de l'opération, quelque 117 drones Osa, dont la valeur oscillerait entre 600 et 1 000 dollars l'unité, ont causé des pertes à l'aviation russe, et donc à l'ensemble du bras armé du pays, de 7 milliards de dollars.

Cette attaque représente une défaite sans appel pour la Russie, qui a non seulement subi ces pertes impossibles à remplacer, mais l'a fait d'une manière qui a mis en évidence les graves lacunes tant de la défense aérienne du pays que des efforts de contre-espionnage. En termes d'humiliation, elle pourrait être plus importante que l'attaque à deux drones contre le Kremlin le 3 mai 2023 (Barnes et al., 2023).

Il convient de noter que toutes les personnes ukrainiennes impliquées ont été exfiltrées du territoire russe suffisamment tôt avant l'attaque. Ainsi, non seulement l'opération a été menée sans subir la moindre perte, mais l'Ukraine dispose désormais de personnel expérimenté dans la réalisation de ce type d'actions. Si cette opération a nécessité une phase de planification et de préparation de 18 mois, il ne serait pas déraisonnable de penser qu'à l'heure actuelle, la prochaine attaque à grande échelle contre l'arrière-garde russe pourrait être en cours de préparation.

### 3.3. DIFFÉRENCES AVEC D'AUTRES OPÉRATIONS SIMILAIRES

L'opération Telaraña n'est en aucun cas la première attaque à l'aide de petits drones contre des infrastructures critiques pour la défense nationale d'un État. Les insurgés en Irak ont attaqué pendant des années les positions de l'armée irakienne et des armées de la coalition internationale contre l'État islamique à l'aide de drones. Les rebelles syriens ont également mené des attaques à l'aide de drones contre la base aérienne russe de Hmeimim, dans la région de Lattaquié, fidèle au gouvernement de Bachar Al-Assad. Cependant, ce qui est le plus remarquable dans cette action, c'est la profondeur de l'attaque à l'intérieur du territoire ennemi, la sophistication technique de son exécution et le fait qu'elle ait été menée contre des bases contenant du matériel critique et rare de la deuxième plus grande armée de la planète, dans un contexte de conflit armé où les attaques à l'arrière constituaient une dynamique constante du conflit.

Ben Connable soutient que l'opération ukrainienne, bien que couronnée de succès, doit être interprétée dans son contexte approprié. Il souligne que les expériences précédentes en Syrie (Hmeimim), en Irak, au Yémen et ailleurs révèlent que les aérodromes peuvent être efficacement protégés contre ces attaques grâce à une défense aérienne disposée en couches. Nous ne devrions donc pas céder à la tentation de qualifier de révolution militaire ce qui pourrait n'être qu'un cas isolé de défaillance de la sécurité (Connable, 2025).

Il est possible qu'il s'agisse d'une défaillance dans la planification de la défense aérienne russe, comme le suggère Ben Connable. Cependant, il faut également replacer dans leur contexte les exemples mentionnés par l'auteur.

Nous analyserons le cas pour lequel nous disposons du plus d'informations : les multiples attaques de drones contre la base aérienne de Hmeimim, à Lattaquié (Syrie). Cette installation a été construite en 2015 pour servir de centre stratégique à l'intervention russe en Syrie. Cette base a subi une longue série d'attaques par des drones depuis 2018 jusqu'à la plus récente en janvier 2025.

La première de ces attaques a eu lieu le 6 janvier 2018, lorsque 13 drones à voilure fixe ont été interceptés par les moyens de guerre électronique présents sur la base, puis capturés, même si certains ont dû être abattus par la défense antiaérienne. Il convient de souligner la différence tant en termes de nombre que de moyens utilisés par les rebelles par rapport à l'opération Telaraña (BBC, 2018).

À partir de ce moment, la base aérienne a commencé à être attaquée de manière continue jusqu'en 2021, année où les attaques ont cessé, à l'exception de quelques cas sporadiques. Les médias officiels russes, cherchant probablement à tirer le meilleur parti de la propagande, avaient l'habitude de donner des informations sur de longues périodes, plutôt que sur des attaques spécifiques. En août 2018, la base a été attaquée par 47 véhicules aériens sans pilote (UAV) et, entre septembre et octobre 2018, le personnel militaire de la base a abattu 50 UAV.

Ainsi, les attaques des groupes rebelles syriens auraient été d'une ampleur bien supérieure aux capacités de défense russes. De plus, on peut supposer que, dans le but de protéger le centre stratégique de son intervention militaire en Syrie, la Russie aurait considérablement renforcé les moyens de défense aérienne présents sur la base. De plus, la base de Hmeimim est située à moins de 100 kilomètres d'Idlib, la région syrienne où la présence et le contrôle des rebelles ont été les plus importants tout au long de la guerre civile.

Les expériences de Hmeimim ne seraient donc pas comparables à ce qui s'est passé dans les bases attaquées par l'Ukraine le 1er juin 2025, compte tenu des différences de contexte géographique, de niveau d'alerte préalable et de complexité de l'action.

L'effort requis par la Fédération de Russie pour protéger de manière adéquate toutes les bases aériennes, navales et terrestres de son territoire, ainsi que toute infrastructure critique susceptible d'être une cible militaire, serait immense. Cette difficulté est accrue pour un pays en guerre contre son voisin occidental, avec les implications évidentes que cela comporte lorsqu'il s'agit de déterminer le déploiement des unités dotées de capacités de défense antiaérienne.

### 3.4. CONSÉQUENCES

Comme c'est théoriquement le cas dans la guerre navale, les attaques de drones sont davantage axées sur des tactiques d'essaimage que sur l'impact de chaque drone individuel. C'est ce qui ressort des événements en Ukraine et des attaques menées par l'Iran contre Israël. Nous devons donc conclure que le succès des attaques de drones

contre des cibles protégées par des moyens anti-drones repose sur l'essaim (Price, 2025 ; Tangredi, 2023).

Il est important de prendre en compte le rôle déterminant joué par l'intelligence artificielle dans l'exécution de l'opération. Bien que les drones aient été officiellement pilotés par des opérateurs ukrainiens, ceux-ci auraient pu utiliser des moyens de navigation autonomes afin de parer à d'éventuelles pertes de liaison. Ainsi, même si les pilotes avaient perdu la connexion avec les appareils, ceux-ci auraient poursuivi leur route vers les bases aériennes sans contrôle humain ni signal GPS. Ils auraient également distingué les cibles à distance (De Troullioud, 2025).

Au cours de la phase de préparation de l'opération Telaraña, les drones ont été programmés pour reconnaître les moyens aériens qu'ils allaient attaquer, et ainsi les signaler au pilote afin qu'il fasse s'écraser le drone sur les endroits les plus sensibles pour l'intégrité structurelle des aéronefs, par exemple les réservoirs de carburant. Ces capacités auraient ensuite été mises en pratique avec des bombardiers hors service que l'Ukraine avait dans ses dépôts (Bondar, 2025).

Ainsi, même si l'Ukraine a fait appel à des pilotes humains pour mener à bien cette opération, il est évident que le niveau d'implication de l'IA dans son succès est indéniable. Cela soulève également la question de savoir si l'opération aurait pu être menée entièrement par des drones autonomes. Cela n'a pas été possible cette fois-ci, mais au vu des progrès réalisés, on peut conclure que cela sera possible dans un avenir proche. Il est même possible que des expériences soient déjà en cours dans ce sens. Les avantages immédiats seraient déterminants pour le succès des opérations futures : ils permettraient l'utilisation d'essaims gigantesques, plusieurs fois plus grands que ceux que l'on peut voir actuellement, et augmenteraient considérablement la sécurité de l'opération, en évitant les signaux envoyés du centre de contrôle aux drones.

L'opération Spiderweb pourrait être considérée comme l'une des opérations d'infiltration les plus réussies du XXIe siècle. Elle a été saluée par la communauté occidentale, même si celle-ci n'est pas encore tout à fait consciente de ses implications futures. Le gouvernement russe s'est empressé de condamner cette action comme un attentat terroriste, bien que des cibles militaires légitimes aient été attaquées dans un contexte de conflit armé reconnu par les deux États. Néanmoins, à la vue des images diffusées ce jour-là, il convient de s'interroger : en quoi une attaque terroriste contre des bases aériennes espagnoles serait-elle visuellement différente de ce qui s'est passé à l'intérieur du territoire de la Fédération de Russie ?

## 4. LES DRONES D'ATTAQUE ARRIVENT EN AMÉRIQUE DU SUD

Comme l'a dit José Nemesio García Naranjo : « Pauvre Mexique, si loin de Dieu et si près des États-Unis ». Cette affirmation pourrait très bien s'étendre à plusieurs nations américaines situées au sud du Rio Grande, en particulier celles où les groupes criminels organisés sont très présents. Les mauvaises conditions économiques, associées à la demande incessante de substances illicites sur les marchés extérieurs tels que les États-Unis ou l'Europe, ont conduit pendant des décennies le continent américain à des affrontements, des guerres civiles et une instabilité sociale. Dans certains cas, la situation a atteint des extrêmes, comme au Salvador, où 1,7 % de la population totale du pays est

incarcérée, principalement pour participation présumée au trafic de substances et appartenance à des groupes criminels organisés (Human Rights Watch, 2024).

Le gouvernement des États-Unis qualifie certains de ces groupes d'organisations criminelles transnationales (OCT) en raison de leur pouvoir et de leur influence. Certains disposent d'un arsenal, d'effectifs et de capacités comparables à ceux de certaines armées nationales, comme le Cartel de Jalisco Nueva Generación (CJNG), dirigé par Nemesio Oseguera Cervantes « el Mencho ». D'autres organisations sont présentes sur les marchés criminels de plus de 40 pays, comme le Cartel de Sinaloa (CDS) (Drug Enforcement Administration [DEA], 2025). Le cas de ce dernier groupe est emblématique du contrôle qu'il exerce sur son territoire, car un conflit pour la direction du cartel qui a débuté en 2024 a conduit l'État de Sinaloa à être déclaré à plusieurs reprises zone de guerre par des journalistes internationaux, causant au moins 1 900 morts et 2 000 disparitions en un an uniquement à cause de ce conflit (Villegas, octobre 2025).

Ces organisations criminelles ont tiré parti des progrès technologiques des dernières décennies pour mener leurs opérations. Dans cette optique, elles ont rejoint la révolution des drones, qu'elles utilisent principalement pour accomplir trois tâches : la surveillance et la sécurité, le trafic de marchandises et les attaques directes.

À l'instar de ce qui s'est passé en Ukraine, l'Amérique hispanique a connu une croissance exponentielle de l'utilisation de ces moyens, en particulier depuis 2022. Les groupes criminels organisés ont analysé les expériences en Europe de l'Est presque aussi minutieusement que les armées professionnelles, voire davantage. Les deux pays d'Amérique du Sud où les drones sont les plus présents dans le contexte de la criminalité organisée sont le Mexique et la Colombie.

## 4.1. MEXIQUE

Pour analyser l'utilisation des drones par les groupes criminels organisés au Mexique, il faut remonter au début des années 2010. C'est à cette époque que l'on a commencé à découvrir des drones commerciaux utilisés à des fins de surveillance. À partir de là, on a commencé à explorer la possibilité de transporter des substances illicites à bord de ces appareils.

En janvier 2015, un drone transportant 2,5 kg de méthamphétamine s'est écrasé dans la ville de Tijuana, au Mexique, alors qu'il s'apprêtait à franchir la frontière avec les États-Unis. Jusqu'alors, les autorités américaines chargées du contrôle des frontières n'avaient enregistré aucune tentative de contrebande à l'aide de drones (Valencia, 2015).

Il a fallu attendre 2017 pour voir apparaître les premiers signes indiquant que les organisations criminelles transnationales (OCT) pourraient être en train d'expérimenter le concept des drones explosifs. Quatre hommes voyageant dans un véhicule qui avait été signalé comme volé ont été arrêtés par la police dans l'État de Guanajuato, dans une zone « chaude » (disputée par plusieurs groupes criminels organisés). Les cartels de Sinaloa, Jalisco Nueva Generación et Los Zetas étaient très présents à Guanajuato et se disputaient le contrôle de la région. En inspectant le véhicule, ils ont trouvé un drone avec une « grande quantité » (sans préciser la quantité exacte) d'explosifs fixés à la carrosserie et équipé d'un détonateur activé par radiofréquence (AFP, 2017).

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

La première tentative d'attaque à l'aide d'un drone a eu lieu le 9 juillet 2018, lorsqu'un véhicule aérien sans pilote (UAV) a percuté la maison de Gerardo Manuel Sosa, secrétaire d'État à la sécurité publique de Basse-Californie, dans la ville de Tecate. Ce drone transportait deux grenades à fragmentation qui n'ont finalement pas explosé. De plus, le secrétaire d'État n'était pas chez lui au moment de l'attentat (CNN Español, 2018).

L'utilisation de drones a commencé à se développer progressivement dans tout le pays, mais sans organisation particulière et à travers de petites actions, manifestement menées avec du matériel, des équipements et des procédures *ad hoc*.

Tout a changé en 2021, avec le leader du groupe « Los Deltas », Armando Gómez Núñez, alias « Delta 1 ». Los Deltas est une branche armée du cartel Jalisco Nueva Generación qui opérait dans la zone frontalière entre les États de Jalisco et Michoacán. Armando Gómez a créé la première unité de drones d'attaque spécialisés, commandée par « El Flaco Drones » et une mystérieuse membre surnommée « Lady Drones », qui a été arrêtée le 13 août 2025 (Secrétariat à la Défense nationale, 2024 ; Mendoza, 2025).

Cette nouvelle unité de drones, ainsi que d'autres appartenant à divers groupes criminels, ont commencé à opérer de manière plus technique et sophistiquée. Les opérateurs de systèmes aériens sans pilote (UAS) ont commencé à être appelés « droneros », et divers écussons d'unités « droneras » ont été saisis (Maza, 2025).

Les efforts déployés par le Cartel de Jalisco Nueva Generación (CJNG) dans le domaine des drones à la frontière entre Jalisco et Michoacán répondaient à un conflit avec la « Familia Michoacana », qui n'a pas tardé à riposter en créant ses propres unités d'opérateurs de drones.

Actuellement, l'utilisation d'unités d'attaque équipées de moyens UAS s'est étendue à tout le Mexique, même si les incidents se concentrent dans les États de Michoacán et Guerrero. En ce qui concerne les opérateurs, le CJNG et la Familia Michoacana sont les deux organisations les plus avancées dans l'utilisation des drones. Derrière ces deux organisations viennent le Cartel de Sinaloa, puis le reste des groupes criminels à différents stades d'évolution dans ce domaine (Jaramillo, 2025).

Le type d'attaque par drone le plus courant dans les conflits au Mexique est celui *des droppers*, c'est-à-dire ceux qui larguent des charges explosives sur une cible. Il est rare de voir des actions menées avec des drones à vision à la première personne (FPV), bien qu'ils soient de plus en plus courants. Ces *droppers* sont également utilisés pour des missions de surveillance, voire de contrebande ou de transport d'objets de petite taille (Villegas, septembre 2025).

Au départ, les attaques de drones visaient généralement d'autres organisations criminelles, mais certains cas concrets d'attaques contre des membres de la police ou des forces armées mexicaines ont été signalés. En 2021, 10 décès ont été enregistrés, dont 7 étaient des membres de groupes criminels. Le nombre de victimes a diminué en 2022 pour atteindre 8 (Ziemer, 2025).

Les attaques de drones ont considérablement augmenté en 2023. Cette année-là, leur nombre est passé à 35, soit près de cinq fois plus que l'année précédente. Cependant, le plus effrayant n'était pas cette augmentation, mais la répartition des victimes. Sur les

35 victimes, 27 étaient des civils. Une nouvelle ère des drones avait commencé au Mexique. Les groupes criminels utilisaient désormais les drones non seulement pour attaquer leurs ennemis directs, mais aussi pour semer la panique parmi la population des territoires « chauds ». Au cours de cette période, des attaques directes ont été menées contre des villages dans les États de Michoacán et de Guerrero, au cours de l'une desquelles des villageois ont capturé un tueur à gages de la Familia Michoacana (Grillo, 2024).

Ce tueur à gages, Fernando, a fait une déclaration aux journalistes dans laquelle il a laissé entendre que non seulement les UAS sont arrivés au Mexique pour y rester, mais que leur utilisation va augmenter à partir de maintenant : « Ils ont *des pilotes de drones*. Ils ont des personnes spécialisées dans *les drones* (...). Ils ont beaucoup de drones, donc même si un passeur (une personne qui se consacre au trafic d'objets et de marchandises cachées) en perd un, cela ne les dérange pas (...). Comme cela ne fait que commencer » (Grillo, 2024).

La capacité technique des OCT dans le domaine des UAS a atteint un tel niveau que l'on commence à voir les premiers signes d'un réel effort de la part des organisations criminelles pour investir dans des mesures et des unités anti-drones. La preuve en est qu'en 2024, dans le contexte de la guerre civile à Sinaloa, un membre de l'une des factions qui se disputent le contrôle du cartel de Sinaloa, « los Mayitos » (la faction dirigée par les fils d'Ismael « el Mayo » Zambada, arrêté en 2024), a été photographié avec un système de brouillage anti-UAS *Skyfend*, d'une valeur de 100 000 dollars (Jiménez, 2025).

Bien qu'un seul système de défense antiaérienne soit insuffisant pour contrer le potentiel destructeur des drones d'attaque, il révèle néanmoins une volonté de se lancer dans la course à l'armement, comme on peut le voir dans d'autres contextes, notamment en Ukraine.

Dans le cadre de la lutte contre l'utilisation illicite des drones, le gouvernement mexicain a réagi en adoptant des dispositions visant à rendre plus difficile l'accès aux UAV. En 2019, la norme NOM-107-SCT3-2019, qui réglemente les systèmes d'aéronefs pilotés à distance (RPAS), a été rédigée. Selon cette norme, tout appareil de plus de 250 grammes doit être enregistré. Il est interdit de modifier les RPAS pour permettre le transport de marchandises dangereuses ou le largage d'objets. Cette mesure, dans un pays où des régions entières sont gouvernées de facto par des OCT, a eu peu d'impact sur la résolution du problème de l'utilisation des drones à des fins criminelles.

Sur le plan humanitaire, les menaces proférées contre la population civile ont entraîné plusieurs déplacements de réfugiés. En 2023, environ 600 habitants de Nuevo Caracol, dans l'État de Guerrero, ont dû quitter leurs maisons en raison des attaques incessantes de drones sur la population (Ortiz, 2023).

### 4.2. COLOMBIE

La Colombie est un pays d'Amérique latine où l'utilisation de drones par des organisations en conflit avec le gouvernement national prend de plus en plus d'importance. Ce pays a enregistré son premier décès attribuable à des drones d'attaque en juillet 2024, lorsqu'un enfant de 10 ans a été tué et 12 autres personnes blessées lorsqu'un drone de combat ( ) a

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

attaqué avec une grenade à fragmentation un terrain de football à El Platerado (Torres, 2024).

Le principal responsable de l'utilisation des drones en Colombie est l'Armée de libération nationale, en particulier depuis qu'elle a lancé son offensive sur le Catatumbo au début de l'année 2025. Les attaques de drones sont en partie responsables de la crise des déplacés qui a frappé cette région, où plus de 52 000 personnes ont été contraintes de quitter leur foyer (HCR, 2025).

L'une des factions dissidentes des Forces armées révolutionnaires de Colombie - Armée du peuple (FARC-EP), les FARC-EP ont également mené des attaques à l'aide de drones, comme celles perpétrées en novembre 2024 et en juillet et août 2025 contre trois patrouilleurs fluviaux lourds de la marine colombienne sur le fleuve San Juan del Micay, dans le département du Cauca, ou la destruction d'un hélicoptère anti-drogue à Antioquia en août 2025, qui a causé la mort des 13 policiers qui se trouvaient à son bord (Saumeth, 2025 ; Torrado, 2025).

Le 10 juin 2025, le Secrétariat général autoproclamé des FARC-EP a publié un communiqué contenant 10 recommandations à l'intention de la population civile, de la presse et des organisations humanitaires, dans le but d'éviter les incidents d'attaques contre des civils. Parmi celles-ci, il convient de souligner le maintien d'une distance minimale de 500 mètres avec les convois militaires ou policiers, et l'exigence faite aux forces armées d'abandonner les installations adjacentes aux bâtiments à usage résidentiel (W Radio Colombia, 2025).

Le nombre de victimes d'attaques de drones en Colombie reste inférieur à celui du Mexique, bien que depuis le milieu de l'année 2025, on commence à observer en Colombie des attaques de beaucoup plus grande envergure, comme celles déjà mentionnées contre des navires et des hélicoptères.

Les gouvernements confrontés à des ennemis équipés de systèmes aériens sans pilote (UAS) en Amérique du Sud se sont pour l'instant retrouvés dépassés. Plusieurs pays, dont la Colombie, le Pérou et le Mexique, ont commencé à doter leurs forces armées et de sécurité de systèmes de défense anti-drones, afin de pouvoir au moins protéger leurs bases et leurs infrastructures critiques.

De leur côté, certains gouvernements du continent américain ont choisi de lutter contre les groupes criminels organisés à l'aide de drones. En Haïti, une opération menée par le gouvernement à l'aide de drones le 1er mars 2025 a fait 80 morts ce jour-là, même s'il n'a pas été possible de confirmer que tous étaient membres d'organisations criminelles. L'un des chefs des gangs de Port-au-Prince, Jimmy Cherizier, a condamné l'attaque, menaçant de riposter avec ses propres drones, ce qui pourrait causer la mort de « n'importe qui dans le pays » (Vyas, 2025).

### 4.3. SOLUTIONS PROPOSÉES

Le problème auquel sont confrontés les États hispano-américains est extrêmement grave, et trois recommandations ont été formulées à partir de différents points de vue, qui devraient constituer les principes directeurs de la politique anti-UAS développée par ces

nations : attaquer les lignes d'approvisionnement, apprendre des experts et investir dans la formation et les tactiques (Ziemer, 2025).

Il faut reconnaître que la lutte contre les chaînes d'approvisionnement des organisations illégales est indissociable et intrinsèque à la lutte contre les groupes eux-mêmes. Malgré cela, la victoire des États, du moins en ce qui concerne les drones, devra nécessairement passer par une approche axée sur l'attaque des chaînes d'approvisionnement.

Il est donc peut-être possible de s'inspirer de l'opération *Grim Beeper*, menée par les services de renseignement israéliens, qui ont infiltré la chaîne d'approvisionnement en « buskas » du Hezbollah, avec le résultat final que nous connaissons tous (Doran, 2024).

Pour sa part, apprendre des experts et investir dans la recherche et les tactiques signifie tirer le meilleur parti possible des informations que peuvent fournir les pays les plus impliqués dans ce développement : l'Ukraine, la Russie et Israël.

## 5. APPLICATION DES LEÇONS

De nombreuses leçons peuvent être tirées d'une analyse des expériences de la Syrie, de l'Ukraine, d'Israël, du Mexique et de la Colombie. Celles qui nous semblent les plus importantes sont les suivantes :

A. Les UAS sont particulièrement efficaces si l'on compare leur prix et leur capacité destructrice.

B. La liaison par fibre optique permet d'éviter la neutralisation des drones par des dispositifs inhibiteurs de radiofréquences.

C. La force d'une action menée par des UAV repose généralement sur la détection tardive et la tactique d'essaimage.

D. Les progrès de l'intelligence artificielle favorisent l'apparition de drones autonomes capables de reconnaître leur environnement et de désigner leurs cibles.

E. L'utilisation de drones permet de retirer le maximum de membres de l'opération avant qu'elle ne commence, réduisant ainsi les pertes propres à pratiquement zéro.

Ces enseignements devront être dûment pris en compte lorsqu'il s'agira d'affronter d'éventuelles utilisations des UAS comme instruments terroristes.

De même, il faut toujours tenir compte du fait que les groupes qui ont la capacité d'utiliser des drones vont les utiliser. Cette technologie et ces techniques sont faciles à adapter à différents modes d'opération et environnements, comme l'a démontré leur récente incorporation dans la lutte contre le crime organisé au Brésil. Le 28 octobre 2025, dans le cadre d'une opération contre la structure du *Comando Vermelho* à Rio de Janeiro, celui-ci a utilisé des drones de combat contre les agents des forces de sécurité. Le *Comando Vermelho* est la plus grande organisation criminelle organisée du Brésil, et a déjà intégré les systèmes aériens sans pilote (UAS) à ses opérations (Braun, 2025).

## 5.1. LEÇONS TIRÉES DES ATTENTATS PRÉCÉDENTS

### 5.1.1. Attentats du 11 septembre

Dans le rapport publié le 22 juillet 2004 par la Commission d'enquête sur les attentats du 11 septembre (11-S) (*National Commission on Terrorist Attacks*, 2004), le onzième chapitre, intitulé « Prévision et rétrospective », porte un jugement critique en détaillant les quatre principales faiblesses du système de contre-espionnage et de lutte antiterroriste des États-Unis qui ont permis la perpétration de l'attentat le plus meurtrier de l'histoire : manque d'imagination, politique inadéquate face à Al-Qaïda, mauvaise utilisation des capacités du gouvernement fédéral et graves erreurs dans la gestion opérationnelle de l'attaque elle-même. La politique inadéquate et la mauvaise utilisation des capacités relèvent davantage de la manière de faire face à un ennemi émergent, ce qui, selon nous, dépasse le cadre du présent article.

Parmi les deux que nous allons analyser, la plus critique est le manque d'imagination, car l'autre découle directement ou indirectement de celle-ci. La première erreur a été la classification du risque effectuée par la communauté du renseignement américaine. Le responsable du bureau antiterroriste, Richard A. Clarke, a fait valoir dans une note du 4 septembre 2001 qu'une partie des agences antiterroristes considéraient les attentats comme « un désagrément qui tue un certain nombre d'Américains tous les 18 à 24 mois ». Même ceux qui, comme Clarke, considéraient le risque comme réel, rédigeaient des scénarios hypothétiques dans lesquels « des centaines » d'Américains étaient victimes du terrorisme. Pratiquement personne n'imaginait un scénario possible tel que celui qui s'est finalement produit.

Le rapport mentionne également que les services de renseignement ont presque totalement ignoré la possibilité qu'un avion soit utilisé comme véhicule suicide, alors que les attentats-suicides étaient devenus monnaie courante au Moyen-Orient. Si l'on s'était mis à la place d'un terroriste souhaitant utiliser un avion détourné, on aurait peut-être détecté les failles de sécurité qui sont apparues au grand jour après le 11 septembre. De plus, la question a parfois été soulevée par des organismes extérieurs à la communauté du renseignement, mais elle a toujours été rejetée par celle-ci comme étant extrêmement improbable. Ceci a été exposé dans le rapport de la Commission d'enquête sur les attentats du 11 septembre, aux pages 345 à 348 (*National Commission on Terrorist Attacks*, 2004).

Les erreurs commises dans la gestion opérationnelle des actions qui ont rendu possible la commission de l'attentat n'étaient pas moins graves. Il convient de souligner le manque de coordination entre les agences fédérales, principalement la Central Intelligence Agency (CIA) et le Federal Bureau of Investigation (FBI). Toutes les actions préparatoires ont été détectées par une institution américaine (la réunion préalable à Kuala Lumpur, l'entrée des suspects sur le territoire américain, la formation des suspects comme pilotes, et bien d'autres encore), mais ces informations n'ont pas été bien communiquées, ce qui a conduit le FBI à ne pas inclure la présence des suspects qu'il avait localisés dans le rapport sur les risques d'attaques imminentes.

### 5.1.2. Attentats de Barcelone et Cambrils

Une situation similaire a pu se produire lors des attentats qui ont malheureusement secoué l'Espagne en 2017 à Barcelone et Cambrils. Les autorités compétentes auraient décidé de

ne pas donner suite à la note de service du commissaire général de la sécurité citoyenne de la police nationale de l'époque, Florentino Villabona Madera, qui recommandait d'installer « de grands bacs à fleurs ou des bornes aux accès (des lieux très fréquentés) » (Rédaction Barcelona La Vanguardia, 2017). Dans ce cas, l'imagination des forces et corps de sécurité n'a pas fait défaut, contrairement à celle des responsables chargés de mettre en œuvre leurs recommandations. Les mêmes lacunes ont été constatées en matière de coordination policière, puisqu'un avertissement présumé envoyé par la CIA le 25 mai 2017, alertant sur la volonté de l'EIIL de commettre un attentat sur la Rambla de Barcelone, aurait pu être ignoré (El Periódico Barcelona, 2017).

### 5.1.3. Résumé des enseignements tirés

Le manque d'imagination et de coordination des institutions sont deux des péchés capitaux dans la lutte contre le terrorisme. La nouvelle ère technologique nous oblige à repenser la manière dont les terroristes potentiels agiront à l'avenir, avec l'utilisation probable de drones, d'intelligence artificielle ou de la combinaison mortelle des deux dans les prochaines tentatives d'attentats terroristes, en plus d'autres outils encore en cours de développement.

## 5.2. POSSIBILITÉS D'ATTENTATS TERRORISTES AVEC DES DRONES

### 5.2.1. Attaques contre des foules

En ce qui concerne les attentats contre les foules, nous considérons comme remarquable la fusillade massive de Las Vegas du 1er octobre 2017, au cours de laquelle un individu s'est procuré un arsenal d'une valeur de 95 000 dollars et a ouvert le feu depuis une suite de l'hôtel Mandalay Bay sur un festival en plein air à proximité de l'hôtel, faisant 60 morts et 867 blessés. Cet incident a démontré à quel point les mesures de contrôle d'accès à une installation peuvent être inefficaces si le risque vient d'en haut (Las Vegas Metropolitan Police Department, 2018).

Il n'est pas nécessaire de faire un effort d'imagination considérable pour penser à quel point cette même attaque aurait pu être destructrice si elle avait été menée à l'aide de véhicules aériens sans pilote (UAV) larguant des charges explosives de plusieurs kilos sur la foule, d'autant plus que l'attentat a eu lieu de nuit, ce qui a déjà eu des conséquences tragiques dans la réalité, car un climat de chaos total s'est installé parmi les personnes présentes.

### 5.2.2. Attaques contre des individus

La possibilité d'attentats contre de hautes autorités de l'État ne doit pas non plus être écartée. Le président du Venezuela, Nicolás Maduro, a été victime d'un attentat à l'aide de drones explosifs lors d'un défilé militaire le 4 août 2018 (El Mundo, 2018). Ainsi, non seulement ces attaques sont possibles, mais elles ont déjà été tentées.

Nous savons que, même si cela est difficile, il n'est pas impossible de s'approcher dangereusement des hautes autorités, comme l'a démontré la tentative d'assassinat contre le candidat à la présidence des États-Unis, Donald Trump, le 13 juillet 2024. Thomas Crooks a réussi à s'approcher à moins de 150 mètres de Trump, armé d'un fusil AR-15, et

a même réussi à tirer huit cartouches avant d'être abattu par des agents des services secrets (*Task Force on the Attempted Assassination of Donald J. Trump*, 2024).

Une attaque hypothétique à l'aide d'un drone n'aurait pas nécessité de s'approcher autant qu'un tireur, car il aurait été plus facile de se camoufler dans les environs avant de lancer un drone guidé par fibre optique ou un essaim de drones équipés d'un logiciel de guidage par intelligence artificielle visant Donald Trump.

### 5.2.3. Attaques contre l'aviation et d'autres secteurs

Le secteur aérien peut également être la cible de ce type d'attaque. À l'instar de l'opération Telaraña, les drones pourraient à l'avenir repérer les moteurs, les réservoirs de carburant ou la fenêtre de la cabine d'un appareil et les percuter au moment du décollage ou de l'atterrissage. Étant donné qu'un Boeing 737-800 ou un Airbus A320 (les deux modèles les plus courants dans l'aviation commerciale) peuvent transporter plus de 180 passagers, un impact effectif contre un seul avion deviendrait immédiatement le deuxième plus grand attentat de l'histoire de l'Espagne.

Les options sont innombrables : des trains arrêtés par un premier drone, puis attaqués par d'autres drones, des attaques combinant des méthodes terroristes déjà connues et utilisant des drones pour attaquer les personnes qui fuient par des goulets d'étranglement, pour ne citer que quelques exemples.

## 5.3. ATTAQUER LA CHAÎNE D'APPROVISIONNEMENT

Les avantages pour les terroristes sont également innombrables : la mort de l'exécutant n'est pas *une condition sine qua non*, les actions préparatoires ne sont pas menées sur le lieu même de l'attaque, ce qui rend leur détection précoce difficile (personne ne peut trouver un sac à dos piégé qui n'est pas là) et ce sont des objets largement vendus sur les marchés civils, ils ne suscitent donc pas autant de soupçons que d'autres méthodes.

Une partie de la bonne approche pour lutter contre les attentats à l'aide de drones consiste peut-être à reconnaître qu'il sera de plus en plus difficile, voire parfois impossible, de les arrêter une fois qu'ils ont été lancés. Tout comme la Russie ne peut pas disposer de grandes unités de défense antiaérienne sur chaque mètre carré de son territoire, nous ne le pouvons pas non plus. Il ne faudrait pas affronter les drones lorsqu'ils volent déjà vers leur cible, mais lorsqu'ils sont dans une boîte, transportés d'un endroit à un autre.

## 5.4. PHASES DÉLICATES DU PROCESSUS DE PRÉPARATION D'UN ATTENTAT AVEC DES UAS

Nous avons pu détecter au moins quatre processus délicats dans la préparation d'une action terroriste avec des drones : l'obtention des drones, la formation des pilotes, la programmation des drones et l'obtention des explosifs.

L'obtention de grandes quantités de systèmes aériens sans pilote (UAS) dans l'Union européenne, et plus particulièrement en Espagne, ne serait pas la partie la plus délicate de l'opération. Bien qu'il soit obligatoire d'être enregistré et d'avoir une licence pour piloter des drones de plus de 250 g, ces restrictions ne s'appliquent pas au simple fait

de les acheter. Cela met en évidence une lacune. L'accumulation excessive et illogique de ces produits devrait toujours être surveillée, ce qui est profondément compromis par cette liberté d'achat. D'autant plus qu'ils peuvent être achetés dans n'importe quel établissement de l'Union européenne, voire dans d'autres pays, dans la mesure où aucune autorisation douanière n'est requise pour l'importation d'UAS à usage personnel. Il faut également tenir compte des drones issus de l'impression 3D.

La formation des pilotes pourrait constituer une bonne occasion d'empêcher la commission de l'attentat, en particulier s'ils tentent de se les procurer par des voies légales. Les services de renseignement américains auraient déjà pu être sur le point de déjouer les attentats du 11 septembre, du moins tels que les terroristes les avaient organisés, lorsque le FBI a publié en juillet 2001 un rapport sur l'intérêt que portaient des suspects djihadistes à la formation au pilotage, intitulé « Un extrémiste islamique apprend à piloter » (Commission nationale sur les attentats terroristes, 2004).

Il faudra être particulièrement attentif à ce qui se passera lorsque les hostilités prendront fin en Ukraine et que les pilotes de drones d'attaque ukrainiens et russes tenteront de se réinsérer dans la société. Jusqu'à présent, les études menées sur les effets psychologiques de l'utilisation de drones d'attaque se sont presque exclusivement concentrées sur les pilotes de bombardiers sans pilote américains qui, de par la nature de leurs actions, sont soumis à un niveau de stress considérablement inférieur à celui des opérateurs ukrainiens et russes.

La programmation des appareils pour qu'ils suivent des instructions spécifiques, à l'aide de l'intelligence artificielle (IA), nécessite des connaissances avancées dans plusieurs domaines techniques, tels que la programmation en Python et C++, la formation en IA, la robotique et l'électronique. Ces connaissances ne sont pas particulièrement coûteuses en termes de temps, mais un intérêt soudain d'un sujet suspect pour ces domaines doit être considéré comme un signal d'alarme immédiat.

Comme dans le point précédent, il faudra envisager la possibilité que des vétérans de la guerre en Ukraine, ou d'autres guerres similaires en termes d'utilisation massive de drones, collaborent à la préparation de ces opérations, voire y participent activement. Les équipes de drones de ces conflits armés ont des connaissances techniques sur l'adaptation des drones de colis à l'accomplissement de missions spécifiques qui dépassent de loin celles dont peut disposer pratiquement tout autre individu.

Enfin, l'acquisition d'explosifs constituerait, comme on peut s'y attendre, *l'étape* la plus fragile de tout le *processus criminel*. Cela est d'autant plus vrai si l'on tient compte du fait que les systèmes aériens sans pilote (UAS), en raison de leurs caractéristiques techniques, ne peuvent pas transporter de charges trop lourdes, ce qui oblige les terroristes potentiels à recourir à des substances explosives ayant un plus grand potentiel de détonation, ce qui peut réduire dans une certaine mesure la recherche de ces tentatives.

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

## 6. CONCLUSIONS

A. Les drones sont là pour rester. Il ne fait aucun doute que leur utilisation va considérablement augmenter. Les expériences des pays qui ont été impliqués dans des conflits avec des drones devront être ajoutées aux procédures propres.

B. L'opération « Telaraña » menée par les services de sécurité ukrainiens (SBU) contre la flotte stratégique russe à longue portée a démontré la polyvalence des actions menées à l'aide de drones contre des cibles situées à des milliers de kilomètres derrière la ligne de front. Ces moyens ont prouvé leur capacité à être infiltrés, distribués et utilisés à grande distance. En extrapolant cette expérience, on peut déduire la capacité destructrice d'un groupe déterminé à éliminer une infrastructure dans une zone civile, compte tenu des ressources nécessaires.

C. L'utilisation de l'intelligence artificielle (IA) dans cette opération, accompagnée des cas déjà documentés d'utilisation de ces outils, modifie radicalement le scénario des menaces futures. Les drones d'attaque finiront par être des dispositifs explosifs guidés par l'IA, dotés des outils nécessaires pour différencier les alliés des ennemis et éliminer ces derniers.

D. Les organisations criminelles transnationales d'Amérique latine se sont lancées avec détermination dans la bataille technologique pour la domination des cieux. Leurs réseaux bien établis de trafic de toutes sortes de matériaux et de substances leur ont permis d'accumuler de grandes quantités de systèmes aériens sans pilote (UAS), qui sont utilisés à des fins de surveillance, de transport et d'attaque. Depuis 2021, elles disposent de leurs propres unités spécialisées et commencent actuellement à investir dans du matériel anti-drones.

Les attaques, bien que timides et limitées au départ, prennent une dimension de plus en plus ambitieuse, allant jusqu'à attaquer des convois ennemis en mouvement. La population civile a également souffert de l'introduction de ces technologies dans les conflits entre groupes criminels, avec des attaques directes et aveugles contre les populations de plus en plus fréquentes au Mexique et en Colombie.

Dans ce dernier pays, les forces armées et les forces de sécurité font l'objet d'attaques considérables, qui pourraient être les prémices d'autres actions d'une ampleur encore jamais vue sur ce continent.

E. L'expérience acquise sur tous les théâtres d'opérations a montré que le succès d'une action menée à l'aide de drones contre une cible défendue réside dans l'essaim.

F. En Ukraine, il a été démontré que les drones d'attaque sont des ressources extrêmement utiles dans le contexte d'une guerre, et en Amérique du Sud, qu'ils peuvent servir à semer la terreur parmi les populations et les unités de sécurité des États, d'autant plus si leurs opérations répondent aux intérêts de grandes organisations dotées d'une capacité logistique et militaire supérieure à celle de certains États souverains.

Il semble évident que tôt ou tard, ces formes d'actions violentes arriveront en Occident, ainsi qu'en Espagne. Nous devons nous préparer et nous souvenir des erreurs commises par le passé afin de ne pas les répéter à l'avenir.

G. L'imagination et la capacité à gérer ces scénarios sont deux conditions fondamentales pour faire face aux nouvelles menaces. Plusieurs attentats terroristes passés ont pu être menés à bien en raison d'analyses de risques incorrectes. L'apparition des drones dotés d'une intelligence artificielle ouvre la porte à des opportunités que les terroristes n'auraient jamais pu imaginer auparavant, tout comme les forces de sécurité.

La manière la plus efficace de les affronter pourrait être d'intercepter leurs tentatives pendant leur phase de préparation. Le stockage des drones, la formation des pilotes, la programmation des UAS et l'obtention d'explosifs semblent être des moments propices pour déjouer les tentatives d'attaques contre la population civile.

La sécurité ne doit pas non plus être négligée. Les attaques de petite envergure seraient plus difficiles à détecter, mais contrairement aux attaques complexes, elles pourraient être stoppées pendant leur exécution.

Enfin, nous devons souligner l'urgence de tirer parti de l'expérience acquise dans ce domaine par les pays actuellement en conflit, où la présence et l'utilisation de drones sont courantes. Ces informations pourraient s'avérer décisives dans les futures enquêtes contre des cellules terroristes déterminées à perpétrer une attaque sur notre territoire.

## 7. RÉFÉRENCES BIBLIOGRAPHIQUES

12e brigade des forces spéciales « Azov » (s.d.). *À propos d'Azov*. Consulté le 3 septembre 2025 sur https://azov.org.ua/en/about-azov/

HCR (2025). *Il est urgent de renforcer la réponse face au déplacement massif sans précédent dans le Catatumbo, en Colombie*. 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). Un drone explosif, le dernier gadget du crime organisé au Mexique. *El País*. https://elpais.com/internacional/2017/10/24/mexico/1508802891_139491.html

BBC (2018). Guerre en Syrie : la Russie déjoue une attaque de drone contre la base aérienne de Hmeimim. *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). Comment l'opération « Spider's Web » de l'Ukraine redéfinit la guerre asymétrique. *Center for Strategic & International Studies*. https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

Braun, J. et Toledo, L. F. (2025). Comando Vermelho : comment des drones et des fusils importés se retrouvent entre les mains du crime organisé au Brésil et transforment le conflit urbain. *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). L'attaque ukrainienne contre les bombardiers russes montre comment des drones bon marché pourraient perturber la sécurité mondiale. *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). Opération Spiderweb : une évaluation des pertes de la Force aérospatiale russe. *Institut international d'études stratégiques*. https://www.iiss.org/online-analysis/military-balance/2025/062/operation-spiderweb-an-assessment-of-russian-aerospace-forces-losses/

Département de la Défense (2000). Directive DOD 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). *Évaluation nationale de la menace liée à la drogue 2025*. https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf

El Mundo (2018). Maduro dénonce « une tentative d'assassinat » à l'aide de drones explosifs et accuse le président Santos. *El Mundo*. https://www.elmundo.es/internacional/2018/08/05/5b662beeca4741d0498b4648.html

El Periódico Barcelona (2017). Texte intégral de l'alerte à l'attentat à Barcelone transmise par la CIA aux 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*. Consulté le 4 septembre 2025 sur https://firstcontact.biz/en/projects/high-acrobatic-uav-osa/

Gibson, O., Harvey, A., Novikov, D., Harvard, C. et Stepanenko, K. (2025). Évaluation de la campagne offensive russe, 1er juin 2025. *Institut d'étude de la guerre*. https://understandingwar.org/research/russia/russian-offensive-campaign-assessment-june-1-2025/

Grillo, I. (2024). La Guerra de Drones en Guerrero. *CrashOut par 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). Comment l'État islamique utilise les drones grand public. *BBC*. https://www.bbc.com/future/article/20161208-how-is-is-using-consumer-drones

Human Rights Watch (2024). *Rapport pour l'Examen périodique universel du Salvador (48e session des Nations Unies ; 4e cycle)*. https://www.hrw.org/es/news/2024/07/30/informe-para-el-examen-periodico-universal-de-el-salvador

Jaramillo, J. C. (2025). Les drones alimentent la course aux armements criminels en Amérique latine. *Insight Crime*. https://insightcrime.org/news/drones-fuel-criminal-arms-race-latin-america/

Jiménez, X. (2025). « La Mayiza » met en échec les forces armées de Sinaloa grâce à un équipement anti-drone d'élite. *Milenio*. https://www.milenio.com/policia/mayiza-combate-fuerzas-armadas-equipo-anti-dron-elite

Khomenko, I. (2024). Comment l'Ukraine utilise des drones dotés d'intelligence artificielle pour déjouer la Russie sur le champ de bataille. *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). *Rapport d'enquête criminelle du LVMPD sur la fusillade meurtrière du 1er octobre*. https://www.lvmpd.com/home/showpublisheddocument/134/638298568313170000

Loh, M. (2025). Les brouilleurs de drones ukrainiens s'avèrent décisifs dans le cadre d'une nouvelle offensive sur le sol russe, selon des blogueurs militaires pro-Kremlin. *Business Insider*. https://www.businessinsider.com/ukraine-drone-jammers-killing-it-new-kursk-push-russian-bloggers-2025-1

Lyle, P. (2019). Prolifération de la puissance aérienne : comment les drones commerciaux sont utilisés par les organisations extrémistes violentes pour influencer l'avenir de la guerre aérienne. *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). Les essaims de drones alimentés par l'IA ont désormais fait leur apparition sur le champ de bataille. *The Wall Street Journal*. https://www.wsj.com/world/ai-powered-drone-swarms-have-now-entered-the-battlefield-2cab0f05

Maza, J. (2025). Drones et létalité technologique des cartels mexicains. *Conseil mexicain des affaires internationales*. https://www.consejomexicano.org/mediateca/articulo/7275

Méheut, C. (2025). L'Ukraine se tourne vers les filets de pêche pour attraper les drones russes. *The New York Times*. https://www.nytimes.com/2025/07/07/world/europe/ukraine-russia-drones-nets.html

Mendoza López, D. (2025). Coup dur pour le CJNG à Campeche : « El 80 », « Lady Drones » et trois tueurs à gages arrêtés après une opération à 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/

Commission nationale sur les attaques terroristes (2004). *Rapport de la Commission sur le 11 septembre*. https://www.9-11commission.gov/report/911Report.pdf

Naber, I. (2025). Pourquoi l'Ukraine reste la machine de guerre la plus innovante au monde. *Politico*. https://www.politico.com/news/magazine/2025/08/27/ukraine-drones-war-russia-00514712

Ortiz, J. (2023). El Caracol : le village guerrerense assiégé par les 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). Les drones et l'attaque menée par le Hamas le 7 octobre 2023 : innovation et implications. *Perspectives sur le terrorisme*. https://www.jstor.org/stable/27372135

Price, R. E. (2025). Définir le terme « essaim » : une étape cruciale pour exploiter la puissance des systèmes autonomes. *Military Review Online Exclusive*. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2025/Defining-Swarm/Defining-Swarms-UA.pdf

Rédaction Barcelone La Vanguardia (2017). Le document dans lequel la police recommandait d'installer des bornes aux accès des lieux très fréquentés. *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). Un drone équipé de grenades s'écrase sur la maison du secrétaire à la Sécurité publique de Basse-Californie. *Excelsior*. https://www.excelsior.com.mx/nacional/dron-con-granadas-cae-en-casa-del-secretario-de-seguridad-publica-de-baja-california

Saumeth, E. (2025). Les FARC attaquent avec des drones un troisième patrouilleur fluvial de la marine colombienne. *Infodefensa*. https://www.infodefensa.com/texto-diario/mostrar/5404281/125-colombia

Secrétariat à la Défense nationale (SEDENA) (2024). *L'armée mexicaine et la Garde nationale ont arrêté Armando « N », alias « Delta 1 », présumé chef du cartel Jalisco Nueva Generación dans les États de Michoacán et 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. (janvier 2023). Bigger Fleets Win. *Proceedings*. https://www.usni.org/magazines/proceedings/2023/january/bigger-fleets-win

Task Force sur la tentative d'assassinat de Donald J. Trump (2025). *Conclusions et recommandations du rapport final*. https://taskforce.house.gov/sites/evo-subsites/july13taskforce.house.gov/files/evo-media-document/12-5-2024-Final-Report-Redacted.pdf

Torrado, S. (2025). Les dissidents multiplient les attaques de drones et déclenchent l'alerte en Colombie. *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). Un enfant meurt après une attaque au drone menée par les dissidents des FARC dans le Cauca. *CNN Español*. https://cnnespanol.cnn.com/2024/07/24/nino-muere-ataque-drones-disidencias-farc-cauca-colombia-orix

Valencia, N. (2015). Un drone transportant de la drogue s'écrase au sud de la frontière américaine. *CNN*. https://edition.cnn.com/2015/01/22/world/drug-drone-crashes-us-mexico-border

Villegas, P. (octobre 2025). En pleine guerre des cartels, les pompes funèbres portent le deuil de Sinaloa. *The New York Times*. https://www.nytimes.com/es/2025/10/24/espanol/america-latina/sinaloa-muertes-trabajadores-funerarios.html

Villegas, P. (septembre 2025). Drones et explosifs improvisés : les cartels mexicains adoptent les armes de guerre modernes. *The New York Times*. https://www.nytimes.com/es/2025/09/01/espanol/america-latina/mexico-carteles-armas.html

Vyas, K. (2025). Le gouvernement haïtien en difficulté lance des drones contre les 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 juin 2025). *#NoticiaW | À la suite de la série d'attentats dans le Cauca et la vallée du Cauca, l'état-major central des FARC a publié* [des recommandations à la population civile]. X. https://x.com/WRadioColombia/status/1932474602267021560

Zelenskyy, V (1er juin 2025). Discours à la nation sur l'attaque par drones de l'opération Telaraña [Transcription]. 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. RÉGLEMENTATION

Règlement délégué (UE) 2019/945 de la Commission du 12 mars 2019 relatif aux systèmes d'aéronefs sans pilote et aux exploitants de systèmes d'aéronefs sans pilote de pays tiers. 11 juin 2019. JOUE n° 152.

Décret royal 517/2024 du 4 juin, qui développe le régime juridique pour l'utilisation civile des systèmes d'aéronefs sans pilote (UAS) et modifie diverses réglementations en matière de contrôle à l'importation de certains produits par rapport aux normes applicables en matière de sécurité des produits ; démonstrations aériennes civiles ; lutte contre les incendies et recherche et sauvetage, et exigences en matière de navigabilité et de licences pour d'autres activités aéronautiques ; immatriculation des aéronefs civils ; compatibilité électromagnétique des équipements électriques et électroniques ; réglementation aérienne et dispositions opérationnelles communes pour les services et procédures de navigation aérienne ; et notification des événements dans l'aviation civile. 5 juin 2024. BOE n° 136.

NORME officielle mexicaine NOM-107-SCT3-2019, qui établit les exigences pour exploiter un système d'aéronef télépiloté (RPAS) dans l'espace aérien mexicain. 14 novembre 2019.

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