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

Artigo de Investigação

A MORTE VINDA DE CIMA: UTILIZAÇÃO DE DRONES DE ATAQUE POR ORGANIZAÇÕES TERRORISTAS

Tradução para o português com ajuda de IA (DeepL)

Diego de Lorenzo de Guindos
Alferes da Guardia Civil
Licenciando em Engenharia de Segurança
delorenzodeguindos@gmail.com

Recebido em 07/09/2025
Aceite em 19/11/2025
Publicado em 30/01/2026

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

Citação recomendada: de Lorenzo, D. (2026). A morte vista de cima: uso de drones de ataque por organizações terroristas. *Revista Logos Guardia Civil*, 4 (1), 53–82. https://doi.org/10.64217/logosguardiacivil.v4i1.8472

Depósito Legal: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

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

A MORTE VINDA DE CIMA: UTILIZAÇÃO DE DRONES DE ATAQUE POR ORGANIZAÇÕES TERRORISTAS

Resumo: Os drones de pequenas dimensões tornaram-se sistemas cada vez mais presentes em cenários de conflito. A sua versatilidade, ampla disponibilidade e baixo custo explicam esta expansão. Este artigo analisa a possibilidade de esses dispositivos serem incorporados a tentativas de atentados terroristas, examinando previamente os usos que receberam em conflitos bélicos, com especial atenção às ações na retaguarda, cuja natureza poderia servir de inspiração para o planejamento de ataques. A fim de avaliar a utilidade operacional dos drones para atores com capacidades logísticas, económicas e operacionais inferiores às dos Estados, será também estudada a sua utilização por organizações criminosas na América do Sul. As conclusões obtidas serão relacionadas com as vulnerabilidades historicamente exploradas por grupos terroristas para evadir a ação do Estado e concretizar as suas operações. O artigo conclui que os drones são ferramentas especialmente atraentes para esses grupos e que a sua proliferação implica o surgimento de novas vulnerabilidades que devem ser identificadas e corrigidas para prevenir ataques contra o Estado ou os seus cidadãos.

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.

Palavras-chave: Drones, Inteligência Artificial, Terrorismo, Ucrânia, Ataques.

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

ABREVIATURAS

11-S: Ataques de 11 de setembro

CDS: Cartel de Sinaloa

CIA: Agência Central de Inteligência

CJNG: Cartel de Jalisco Nova Geração

DEA: Administração de Controle de Drogas dos EUA

EIIL/EI: Estado Islâmico no Iraque e no Levante

EUA: Estados Unidos

FARC: Forças Armadas Revolucionárias da Colômbia

FBI: Departamento Federal de Investigação

FPV: Visão em primeira pessoa

GPS: Sistema de Posicionamento Global

IA: Inteligência Artificial

OCT: Organizações Criminosas Transnacionais

RPAS: Sistema de Aeronaves Pilotadas Remotamente

SBU: Serviço de Segurança da Ucrânia

UAS: Sistemas Aéreos Não Tripulados

UAV: Veículos Aéreos Não Tripulados

1. INTRODUÇÃO

O ser humano sempre fez uso dos avanços da ciência para aumentar a sua capacidade militar. Em alguns casos, adaptou as descobertas existentes para fins bélicos; noutros, foi precisamente a necessidade de obter meios de destruição mais potentes e eficazes do que os dos seus adversários que impulsionou verdadeiras revoluções tecnológicas.

Numa dessas fases de conflito, desencadeou-se uma explosão científica sem precedentes em todos os ramos: a Segunda Guerra Mundial. De todos os projetos, grandes ideias e descobertas, gostaríamos de nos deter particularmente em dois deles para analisar as suas consequências a longo prazo: os projetos alemães que levaram ao uso dos mísseis balísticos V1 e V2, bem como o «Projeto Paloma».

Em primeiro lugar, os projetos alemães que levaram ao uso dos mísseis balísticos V1 e V2. Eles podiam ser lançados a partir do território da França ocupada e atingir cidades na Inglaterra, onde causaram verdadeiros estragos (Reuter, 2000).

Em segundo lugar, um projeto menos conhecido, mas não menos revolucionário, foi o «Projeto Paloma» do psicólogo americano B.F. Skinner para desenvolver mísseis antinavio guiados por tecnologia IA (embora, neste caso, IA significasse «inteligência animal»). Com base nas conclusões do cão de Pavlov, Skinner concluiu que as pombas poderiam ser treinadas para picar continuamente num ponto que vissem num ecrã. Esse ponto teria sido, em algum momento, um navio inimigo real, e os pontos em que a pomba picava enviariam sinais aos controlos do míssil para modificar a sua trajetória. O projeto foi suspenso em 1953 devido ao avanço das medidas de orientação eletrónica (Skinner, 1960).

Embora esses dois projetos tenham pouca relação direta com o desenvolvimento dos drones, eles foram os primeiros a implementar ideias que hoje são uma realidade. O primeiro propôs atacar alvos inimigos a grande distância com mísseis que não colocassem em risco a vida de nenhum piloto, e o segundo foi o primeiro passo em direção a sistemas de armas que pensassem por si mesmos e tomassem suas próprias decisões, sem a necessidade de intervenção humana e sem emitir radiação eletromagnética para detectar os alvos, pois as pombas faziam isso com uma interpretação de imagens. Essas experiências estabeleceram as bases conceituais para a automação de armas, uma ideia que, décadas depois, evoluiria para os atuais drones de combate.

Atualmente, em setembro de 2025, não temos pombas para guiar projéteis planadores lançados de aviões. Em vez disso, temos pequenos aparelhos voadores carregados de explosivos com a capacidade de entender onde estão, para onde devem ir, qual é a sua missão e reconhecer os alvos potenciais para decidir qual é o mais adequado e colidir com ele, detonando os explosivos no processo.

Este fenómeno passou a ser considerado parte habitual do panorama bélico contemporâneo, mas talvez com uma delimitação espacial excessivamente confiante: é um fenómeno próprio das linhas da frente das guerras. No entanto, as contínuas ações ucranianas e russas na retaguarda com drones a centenas de quilómetros da frente, e as notícias que nos chegam da América do Sul sobre a sua utilização por grupos de s do crime organizado fazem-nos suspeitar das possíveis utilizações que os grupos terroristas poderiam dar a estes aparelhos.

O objetivo do presente artigo é analisar, em primeiro lugar, o potencial dos meios aéreos não tripulados para serem utilizados em ataques dirigidos contra alvos militares, bem como exemplos históricos recentes dessa utilização. Posteriormente, proceder-se-á à exploração da transposição desses sistemas para organizações que operam à margem do Estado, o que tem ocorrido em países da América do Sul, principalmente México, Colômbia e Brasil. Em seguida, serão analisados atentados terroristas passados para destacar os erros cometidos que possibilitaram a sua ocorrência. Todas as secções anteriores sustentarão a tese final, que é a de que os drones são um sistema especialmente atraente para aqueles que tentam realizar ataques contra grandes massas de pessoas, bem como contra alvos específicos.

Para efeitos deste artigo, adotar-se-á como definição de terrorismo a contida numa diretiva do Departamento de Defesa dos EUA: «uso calculado da violência ou da ameaça de violência contra indivíduos ou propriedades, para incutir medo, com a intenção de coagir ou intimidar o governo ou as sociedades para alcançar objetivos políticos, ideológicos ou religiosos» *(Departamento de Defesa,* 2000). No entanto, serão consideradas de forma análoga as ações que se manifestem através dos mesmos comportamentos externos, mesmo que não tenham uma finalidade política, ideológica ou religiosa.

Com o objetivo de delimitar o âmbito deste artigo, será omitida a utilização de drones de grandes dimensões. Isto devido à sua escassa disponibilidade e maior facilidade de deteção. Ficam, portanto, excluídos deste estudo os drones utilizados pela Força Aérea dos Estados Unidos, os pertencentes às forças ucranianas e russas, bem como quaisquer outros de idêntica consideração.

Considera-se, portanto, como objeto de estudo o uso de drones de pequenas dimensões por grupos que realizam ações violentas contra grupos de pessoas, personalidades importantes, propriedades importantes para a sociedade e todos os demais que se enquadram na definição de atentado.

2. DRONES DE ATAQUE EM GUERRAS CONVENCIONAIS

2.1. GUERRA CIVIL NA SÍRIA

O papel dos drones de pequenas dimensões em conflitos tem vindo a aumentar progressivamente até ao que conhecemos hoje. As primeiras utilizações de considerável importância puderam ser detetadas durante a guerra civil síria, onde, mais concretamente, o Estado Islâmico no Iraque e no Levante (EIIL/EI) explorou as possibilidades ofensivas dos Veículos Aéreos Não Tripulados (UAV) (Hambling, 2016).

Neste contexto, a primeira utilização registada de drones como ferramentas de ataque foi a combinação de drones com carros-bomba, com os quais o EI atacou os seus inimigos na batalha de Mossul. Os drones realizaram tarefas de reconhecimento de alvos e posterior orientação dos veículos explosivos pelas ruas da cidade (Balkan, 2017).

A utilização de drones como arma de guerra sofreu uma evolução quando foram adicionadas cargas explosivas aos UAV, sendo estas lançadas sobre posições inimigas. Este modelo foi exportado para os combates do EIIL em Deir ez-Zor e para as ofensivas contra os curdos na Síria.

Os incidentes de ataques com drones kamikazes com Visão em Primeira Pessoa (FPV) foram residuais no início, embora a sua frequência aumentasse com o tempo (Lyle, 2019).

2.2. GUERRA DA UCRÂNIA

Outro cenário digno de nota foi o conflito no Donbass, iniciado em 2014. O papel inicial dos UAV era reconhecer alvos que, posteriormente, seriam atacados pela artilharia. Estes drones, por vezes equipados com meios de visão noturna, começaram a ser conhecidos pelos militares de ambos os lados devido aos zumbidos noturnos, que costumavam ser imediatamente acompanhados por rajadas de tiros inimigos.

No entanto, a evolução dos pequenos drones como armas de guerra entraria numa espiral de inovação após o início do frustrado ataque russo contra a Ucrânia em 24 de fevereiro de 2022 e a guerra subsequente que, em novembro de 2025, não parece ter um fim próximo à vista.

Tal como se pôde observar na Síria, os drones foram rapidamente modificados com recursos artesanais para transportar explosivos, como granadas ou projéteis de morteiro, e lançá-los sobre as posições defensivas inimigas. A primeira diferença que surgiu neste teatro de operações foi o rápido surgimento de ataques com drones com Visão em Primeira Pessoa (FPV). Eram quadricópteros com uma carga explosiva com espoletas de impacto acopladas (Naber, 2025).

Esta mudança de paradigma ofereceu a ambos os lados a possibilidade de executar ações precisas contra alvos específicos, facilitando o sucesso das operações, embora implicando a perda de pelo menos um aparelho por ação.

O uso de drones aumentou exponencialmente durante as primeiras fases da guerra, até chegar à situação atual, em que ambos os exércitos contam com unidades especializadas em ataques com Sistemas Aéreos Não Tripulados (UAS) integrados em nível muito baixo. Por exemplo, a 12.ª Brigada de Forças Especiais «Azov» do Exército Ucraniano conta com uma companhia de drones em cada batalhão de combate, bem como um batalhão adicional de UAS para dar apoio à brigada. Algo semelhante pode ser observado noutras unidades de ambos os exércitos (12.ª Brigada de Forças Especiais «Azov», s.f.).

Tanto a Ucrânia como a Rússia iniciaram nessa altura uma disputa tecnológica, tentando encontrar soluções contra os drones, ao mesmo tempo que os melhoravam. Por exemplo, começaram a ser implantadas redes antidrones em posições defensivas e principais vias logísticas, o que foi imediatamente seguido por táticas em tandem: um primeiro drone romperia a rede e o segundo entraria para atingir os alvos (Méheut, 2025).

A fim de proteger os meios mais importantes de cada lado, o uso de inibidores se espalhou para frustrar as tentativas de destruí-los. Isso provocou um longo *impasse* nas frentes. As equipas de drones começaram a ter uma taxa de eficácia cada vez menor, à medida que os inibidores eram distribuídos com maior assiduidade. Ambas as nações tentaram encontrar soluções para este sistema defensivo que, embora não fosse infalível, reduzia em grande medida a capacidade operacional dos UAS (Loh, 2025).

Durante o verão de 2024, começaram a ser registados, durante a invasão ucraniana do óblast de Kursk, os primeiros esforços consideráveis com drones ligados ao terminal que os controlava através de finos cabos de fibra ótica. A principal vantagem da ligação por cabo é a sua imunidade aos inibidores. Da mesma forma, deve-se destacar que eles são indetetáveis por sistemas baseados na interceção de ondas eletromagnéticas, além de garantirem uma melhor conexão com o terminal de controlo, retornando imagens de maior qualidade e facilitando sua eficácia, pois enquanto houver comprimento de cabo, a conexão não será perdida (Hambling, 2025).

Atualmente, os avanços tecnológicos parecem estar a caminhar para o uso cada vez mais comum de drones autónomos guiados por Inteligência Artificial. A indústria de defesa da Ucrânia está a trabalhar na fabricação em grande escala de modelos de drones que reconheçam as situações táticas por si mesmos, as analisem adequadamente e tomem as decisões ótimas para os interesses ucranianos. O complexo industrial militar russo está a agir da mesma forma. No final de agosto de 2025, ocorreram pelo menos 100 incidentes dessa natureza (MacDonald, 2025; Boffey, 2025; Khomenko, 2024).

À margem das ações na linha de frente do combate, desde o início da guerra na Ucrânia, têm ocorrido ações cada vez mais complexas na retaguarda inimiga, nas quais os UAS de ambos os atores desempenham um papel crucial para a consecução dos objetivos.

As lições aprendidas na Ucrânia inspiraram operações que ocorreram em outros lugares do planeta. Para citar um exemplo, durante o massacre de 7 de outubro de 2023 no sul de Israel, o grupo Hamas atacou posições fronteiriças das Forças de Defesa de Israel com UAVs de pequenas dimensões (Page, 2025).

3. A OPERAÇÃO TELARAÑA

3.1. O ATAQUE DE 1 DE JUNHO DE 2025

Em 1 de junho de 2025, as bases aéreas russas de Olenya, Ivanovo Severny, Dyagilevo, Ukrainka e Belaya amanheceram sob um ataque das forças especiais ucranianas. Não se tratava de mísseis balísticos nem de drones de longo alcance, como os que a Ucrânia tinha utilizado frequentemente até então. Enxames de pequenos drones de visão em primeira pessoa (FPV) atacaram as posições da Força Aérea Russa.

O objetivo do ataque era a frota de bombardeiros estratégicos que a Rússia vinha empregando sistematicamente na sua campanha de desgaste contra a infraestrutura civil ucraniana. O resultado final foi a destruição ou incapacitação de 34% da frota atacada. Além disso, esses modelos de aeronaves estavam fora de produção desde 1993, dificultando a reconstrução da capacidade estratégica de longo alcance. No plano económico, a Ucrânia assegura que os danos causados ascenderam a cerca de 7 mil milhões de dólares (Gibson et al. 2025).

Deve-se destacar o facto de pequenos drones FPV terem atacado diretamente bases aéreas inimigas extremamente distantes da linha de frente, como a base de Ukrainka, que fica a mais de 5.800 km da fronteira internacionalmente reconhecida da Ucrânia e a mais de 6.000 km da linha de frente. Para contextualizar estes números, trata-se de uma

distância superior à que existe entre o centro de Madrid e Herat (Afeganistão) e praticamente igual à que existe entre Madrid e Baltimore, nos Estados Unidos (EUA).

O Serviço de Segurança da Ucrânia (SBU) conseguiu atacar bases militares a mais de 6.000 quilómetros utilizando modelos de drones que normalmente cumprem missões táticas muito próximas da linha da frente e cuja maior fraqueza é a dificuldade em estabelecer ligação com o terminal de controlo. Isso foi possível porque os drones utilizados nesta operação descolaram perto de cada uma das bases aéreas. No caso do ataque à base aérea de Belaya (o maior ataque da operação, com 3 bombardeiros Tu-95 e 4 bombardeiros Tu-22M3 destruídos), os drones FPV descolaram de uma posição a sudeste da base, a cerca de 8 quilómetros (Dempsey, 2025).

3.2. A OPERAÇÃO

A "Operação Teia de Aranha" do Serviço de Segurança da Ucrânia (SBU) teve uma fase de planeamento e preparação de mais de 18 meses, de acordo com o presidente ucraniano *Volodymyr Zelenskyy (Zelenskyy*, 2025*).* Foram utilizados quadricópteros com visão em primeira pessoa (FPV) «Osa», da empresa ucraniana *First Contact* (First Contact, 2025).

Os drones do modelo Osa distinguem-se pela localização dos seus componentes eletrónicos sob uma cobertura exterior particularmente espessa e por terem a porta de alimentação numa posição fixa, enquanto a maioria dos modelos de drones FPV regularmente utilizados pelas Forças Armadas ucranianas têm normalmente um corpo «esquelético», no qual os componentes eletrónicos e a cablagem ficam normalmente expostos. Depois de considerar a complexidade da missão, a distância entre o local de preparação da operação e os alvos, e as diversas condições climáticas em que a infiltração se desenvolveria, a SBU optou pelo modelo mais robusto.

Durante os 18 meses de preparação, a SBU conseguiu introduzir 117 drones Osa na Federação Russa. Uma vez dentro do território inimigo, foi criada uma empresa de construção de fachada dedicada à construção de casas modulares de madeira para ocultar os movimentos. Esses módulos habitacionais contavam com um teto falso retrátil, no qual foram escondidas 9 fileiras de 4 drones cada, para uma capacidade total teórica de 36 drones por módulo. Paralelamente, também foram escondidos drones em contentores de mercadorias (Bondar, 2025).

Em cada módulo também foi instalado um sistema de controlo remoto, que atuaria como intermediário entre os 117 drones que realizavam o ataque e os 117 pilotos que os controlavam a partir da Ucrânia. A ligação entre os sistemas de controlo remoto e as posições dos operadores foi possível através de satélite.

Depois de montados os «cavalos de Tróia», a SBU contactou empresas russas de transporte de mercadorias. Estas levaram os drones Osa para os «pontos de entrega» das cargas, que acabaram por ser os locais determinados pela SBU para a posterior descolagem dos drones.

Na madrugada de 1 de junho de 2025, as coberturas dos "cavalos de Tróia" já infiltrados foram levantadas, permitindo que os drones decolassem e se dirigissem aos seus alvos. Foram divulgados vários vídeos de civis russos desses módulos e contentores

com drones saindo deles em direção às nuvens negras causadas pelas explosões dos que os precederam.

Fazendo um balanço global da operação, cerca de 117 drones Osa, cujo valor oscilaria entre 600 e 1.000 dólares por unidade, causaram perdas à aviação russa, e portanto a todo o braço armado do país, de 7.000 milhões de dólares.

Este ataque representa uma derrota sem paliativos para a Rússia, que não só sofreu estas perdas impossíveis de substituir, como o fez de uma forma que revelou as graves deficiências tanto da defesa aérea do país como dos esforços de contra-espionagem. Em termos de humilhação, pode ser maior do que o ataque com dois drones ao Kremlin em 3 de maio de 2023 (Barnes et al., 2023).

É importante notar que todos os ucranianos envolvidos foram retirados do território russo com antecedência suficiente antes do ataque. Assim, não só a operação foi realizada sem sofrer uma única baixa própria, como a Ucrânia conta agora com pessoal com experiência na execução deste tipo de ações. Se esta operação teve uma fase de planeamento e preparação de 18 meses, não seria descabido pensar que, neste preciso momento, poderia estar a ser preparado o próximo ataque em grande escala contra a retaguarda russa.

3.3. DIFERENÇAS EM RELAÇÃO A OUTRAS OPERAÇÕES SEMELHANTES

A Operação Telaraña não constitui, de forma alguma, o primeiro ataque com drones de pequenas dimensões contra infraestruturas críticas para a defesa nacional de um Estado. Os insurgentes no Iraque atacaram durante anos as posições do Exército iraquiano e dos exércitos da coligação internacional contra o Estado Islâmico com UAV. Também os rebeldes sírios realizaram ataques com drones contra a base aérea russa de Hmeimim, na região leal ao governo de Bashar Al-Asad, em Latakia. No entanto, o mais notável nesta ação é a profundidade do ataque dentro do território inimigo, a sofisticação técnica da sua execução e o facto de ter sido contra bases com material crítico e escasso do segundo maior exército do planeta, num contexto de conflito bélico em que os ataques à retaguarda constituíam uma dinâmica constante do conflito.

Ben Connable defende que a operação ucraniana, embora bem-sucedida, deve ser interpretada dentro do seu contexto adequado. Ele destaca que experiências anteriores na Síria (Hmeimim), Iraque, Iémen e outros locais revelam que os aeródromos podem ser eficazmente protegidos contra esses ataques por meio de uma defesa aérea disposta em camadas. Portanto, não devemos cair na tentação de classificar como revolução bélica o que pode ser apenas um caso isolado de falha de segurança (Connable, 2025).

É possível que se trate de uma falha no planeamento da defesa aérea russa, como sugere Ben Connable. No entanto, é necessário contextualizar os exemplos mencionados pelo autor.

Analisaremos o caso com maior disponibilidade de informação: os múltiplos ataques com drones contra a Base Aérea de Hmeimim, em Latakia (Síria). A instalação foi construída em 2015 para ser utilizada como centro estratégico da intervenção russa na Síria. Esta base sofreu uma longa lista de ataques com meios UAV desde 2018 até ao mais recente em janeiro de 2025.

O primeiro desses ataques ocorreu em 6 de janeiro de 2018, quando 13 aeronaves não tripuladas de asa fixa foram interceptadas pelos meios de guerra eletrónica presentes na base e posteriormente capturadas, embora algumas tenham sido abatidas por meio de defesa antiaérea. É notável tanto a diferença de números como dos meios utilizados pelos rebeldes em relação à Operação Telaraña (BBC, 2018).

A partir desse momento, a base aérea começou a ser atacada continuamente até 2021, ano em que os ataques cessaram, exceto em alguns casos esporádicos. Os meios oficiais russos, possivelmente buscando o maior retorno propagandístico, costumavam fornecer dados de longos períodos de tempo, e não tanto de ataques específicos. Durante agosto de 2018, a base foi atacada por 47 veículos aéreos não tripulados (UAV), e entre setembro e outubro de 2018, o pessoal militar da base abateu 50 UAV.

Assim, os ataques dos grupos rebeldes sírios teriam sido de uma escala que está longe de ser superior à capacidade de defesa russa. Além disso, é de se entender que, na busca por proteger o centro estratégico da sua intervenção militar na Síria, a Rússia teria aumentado de forma muito significativa os meios de defesa aérea presentes na base. Além disso, a Base de Hmeimim fica a menos de 100 quilómetros de Idlib, a região síria com maior presença e controlo rebelde ao longo de toda a guerra civil.

As experiências de Hmeimim não seriam, portanto, comparáveis ao que aconteceu nas bases atacadas pela Ucrânia em 1 de junho de 2025, dadas as diferenças no contexto geográfico, nível de alerta prévio e complexidade da ação.

O esforço necessário para que a Federação Russa protegesse adequadamente todas as bases aéreas, navais e terrestres do seu território, bem como qualquer infraestrutura crítica suscetível de ser um alvo militar, seria imenso. Esta dificuldade é ainda maior para um país em guerra com o seu vizinho a oeste, com as implicações óbvias que isso tem na hora de determinar o destacamento de unidades com capacidades de defesa antiaérea.

3.4. CONSEQUÊNCIAS

Tal como acontece teoricamente na guerra naval, os ataques com drones estão mais centrados em táticas de enxame do que em garantir o impacto de cada drone individual. Isto resulta do que aconteceu tanto na Ucrânia como nos ataques que o Irão realizou contra Israel. Devemos, portanto, concluir que os ataques com drones contra alvos protegidos por meios antirrobôs baseiam o seu sucesso no enxame (Price, 2025; Tangredi, 2023).

É importante considerar o papel determinante que a Inteligência Artificial teve na execução da operação. Embora oficialmente os drones tenham sido pilotados por operadores ucranianos, estes poderiam ter utilizado meios de navegação autónoma como precaução contra possíveis perdas de ligação. Desta forma, mesmo que os pilotos tivessem perdido a ligação com os aparelhos, estes teriam continuado o seu caminho em direção às bases aéreas sem controlo humano nem sinal de GPS. Também teriam distinguido os alvos à distância (De Troullioud, 2025).

Durante a fase de preparação da Operação Telaraña, os drones foram programados para reconhecer os meios aéreos que iriam atacar e, assim, destacá-los ao piloto para que colidisse o drone contra os locais mais sensíveis para a integridade estrutural das aeronaves, por exemplo, os depósitos de combustível. Estas capacidades teriam sido

posteriormente postas em prática com aviões bombardeiros fora de serviço que a Ucrânia tinha nos seus depósitos (Bondar, 2025).

Assim, apesar de a Ucrânia ter utilizado pilotos humanos para executar esta operação, é evidente que o nível de envolvimento da IA no sucesso da mesma é inegável. Isso também leva à questão de se a execução poderia ter sido realizada inteiramente por meios UAV autónomos. Nesta ocasião, isso não pôde ser utilizado, embora, atendendo aos avanços ocorridos, se possa concluir que, num futuro próximo, será possível utilizá-lo. É até possível que já estejam a ser feitos testes nesse sentido. Os benefícios imediatos seriam determinantes para o sucesso de futuras operações: possibilitar o uso de enxames gigantescos, várias vezes maiores do que os que podem ser vistos atualmente, e aumentar enormemente a segurança da operação, evitando os sinais enviados do centro de controlo para os drones.

A Operação Telaraña pode ser considerada uma das operações de infiltração mais bem-sucedidas do século XXI. É uma ação que recebeu reconhecimento da comunidade ocidental, embora agora não esteja totalmente consciente das implicações futuras da mesma. O governo russo condenou rapidamente a ação como um ataque terrorista, apesar de terem sido atacados alvos militares legítimos num contexto de conflito armado reconhecido por ambos os Estados. No entanto, e com base nas imagens divulgadas nesse dia, vale a pena refletir: em que se diferenciaria visualmente um ataque terrorista contra bases aéreas espanholas do que aconteceu no interior do território da Federação Russa?

4. OS DRONES DE ATAQUE CHEGAM À AMÉRICA DO SUL

Como disse José Nemesio García Naranjo: «Pobre México, tão longe de Deus e tão perto dos Estados Unidos». Esta afirmação poderia muito bem ser estendida a várias nações americanas situadas ao sul do Rio Grande, em particular aquelas onde há uma grande presença de grupos de crime organizado. As más condições económicas, aliadas à procura incessante de substâncias ilícitas em mercados externos como os EUA ou a Europa, têm levado há décadas o continente americano a confrontos, guerras civis e instabilidade social. Por vezes, chegou-se a extremos como o de El Salvador, onde 1,7% da população total do país está presa, na sua maioria por alegada participação no tráfico de substâncias e pertença a grupos de crime organizado (Human Rights Watch, 2024).

O governo dos Estados Unidos denomina alguns desses grupos como Organizações Criminosas Transnacionais (OCT) devido ao seu poder e influência. Alguns deles possuem arsenal, pessoal e capacidades comparáveis a alguns exércitos nacionais, como o Cartel de Jalisco Nueva Generación (CJNG), liderado por Nemesio Oseguera Cervantes, conhecido como «el Mencho». Outras organizações têm uma taxa de implantação operacional nos mercados criminosos de mais de 40 países, como o Cartel de Sinaloa (CDS) (Drug Enforcement Administration [DEA], 2025). O caso deste último grupo é paradigmático do controlo que exercem sobre o seu território, pois um conflito pela liderança do cartel iniciado em 2024 levou o estado de Sinaloa a ser declarado em vários momentos como zona de guerra por jornalistas internacionais, causando pelo menos 1.900 mortes e 2.000 desaparecimentos em um ano exclusivamente por esse conflito (Villegas, outubro de 2025).

Estas organizações criminosas têm aproveitado os avanços tecnológicos das últimas décadas para as suas operações. Em consonância com isso, aderiram à revolução

dos drones, aplicando-os fundamentalmente para o desempenho de três tarefas: vigilância e segurança, tráfico de mercadorias e ataque direto.

Assim como se pôde observar na Ucrânia, a América Latina experimentou um crescimento exponencial no uso desses meios, particularmente desde 2022. Os grupos de crime organizado analisaram as experiências no leste europeu quase com tanto cuidado quanto os exércitos profissionais, se não mais. Os dois países sul-americanos com maior presença de drones no contexto do crime organizado são o México e a Colômbia.

4.1. MÉXICO

Para analisar o uso de drones por grupos de crime organizado no México, temos que voltar ao início da década de 2010. Foi nessa época que começaram a ser descobertos drones comerciais que eram usados para vigilância. A partir daí, começou-se a explorar a possibilidade de transportar substâncias ilícitas carregadas neles.

Em janeiro de 2015, um drone carregado com 2,5 kg de metanfetamina caiu na cidade de Tijuana, no México, quando se preparava para cruzar a fronteira com os EUA. Até então, as autoridades de controlo fronteiriço dos EUA não tinham registado nenhuma tentativa de contrabando utilizando drones (Valencia, 2015).

Foi preciso esperar até 2017 para que surgissem os primeiros indícios de que as Organizações Criminosas Transnacionais (OCT) poderiam estar a experimentar o conceito de drones explosivos. Quatro homens que viajavam num veículo que tinha sido dado como roubado foram detidos pela polícia no estado de Guanajuato, numa zona que se encontrava «quente» (disputada por mais do que um grupo de criminalidade organizada). Os cartéis de Sinaloa, Jalisco Nueva Generación e Los Zetas tinham uma presença importante em Guanajuato e estavam em conflito pelo controlo. Ao inspecionar o veículo, encontraram um drone com uma «grande quantidade» (sem descrever exatamente a quantidade) de explosivos acoplados ao corpo e equipado com um iniciador ativado por radiofrequência (AFP, 2017).

A primeira evidência de tentativas de ataques com drones ocorreu em 9 de julho de 2018, quando um Veículo Aéreo Não Tripulado (UAV) colidiu com a casa de Gerardo Manuel Sosa, secretário de Estado de Segurança Pública da Baixa Califórnia, na localidade de Tecate. Este drone transportava duas granadas de fragmentação que acabaram por não detonar. Além disso, o secretário de Estado não se encontrava em sua residência no momento do atentado (CNN Español, 2018).

O uso de drones começou a aumentar gradualmente em todo o país, embora sem nenhuma organização concreta e por meio de pequenas ações, claramente realizadas com materiais, equipamentos e procedimentos *ad hoc*.

Tudo mudou em 2021, com o líder do grupo «los Deltas», Armando Gómez Núñez, também conhecido como «Delta 1». Os Deltas são um braço armado do Cartel de Jalisco Nueva Generación que operava na zona fronteiriça entre os estados de Jalisco e Michoacán. Armando Gómez criou a primeira unidade especializada em drones de ataque, comandada por "el Flaco Drones" e uma misteriosa integrante apelidada de "Lady Drones", que foi detida em 13 de agosto de 2025 (Secretaria de Defesa Nacional, 2024; Mendoza, 2025).

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

Esta nova unidade de drones, juntamente com outras em vários grupos criminosos, começou a operar de forma mais técnica e sofisticada. Os operadores de sistemas aéreos não tripulados (UAS) passaram a ser chamados de «droneros», e vários emblemas de unidades «droneras» foram apreendidos (Maza, 2025).

O esforço em drones do Cartel de Jalisco Nueva Generación (CJNG) na fronteira entre Jalisco e Michoacán foi uma resposta a um conflito contra a «Familia Michoacana», que não demorou a responder ao grupo de Jalisco, estabelecendo as suas próprias unidades de operadores de drones.

Atualmente, o uso de unidades de ataque com meios UAS se espalhou por todo o México, embora os incidentes se concentrem nos estados de Michoacán e Guerrero. No que diz respeito aos operadores, o CJNG e a Família Michoacana são as duas organizações mais avançadas no uso de drones. Atrás destas duas viria o Cartel de Sinaloa e, depois, o resto dos grupos criminosos em diversas fases de evolução neste domínio (Jaramillo, 2025).

O tipo de ataque com drones mais comum nos conflitos no México são os *droppers*, ou seja, aqueles que lançam cargas explosivas sobre um alvo, sendo raro encontrar ações realizadas com drones com visão em primeira pessoa (FPV), embora sejam cada vez mais comuns. Esses *droppers* também são usados em tarefas de vigilância e até mesmo contrabando ou transporte de objetos de pequenas dimensões (Villegas, setembro de 2025).

Inicialmente, os ataques com drones eram geralmente dirigidos a outras organizações criminosas, com alguns casos concretos de ataques contra pessoal da polícia ou das Forças Armadas Mexicanas. Em 2021, foram registados 10 mortos, dos quais 7 eram membros de grupos criminosos. As vítimas diminuíram em 2022 para 8 (Ziemer, 2025).

Os ataques com drones sofreram um aumento considerável em 2023. Nesse ano, o número subiu para 35, quase cinco vezes mais do que no ano anterior. No entanto, o mais assustador não foi o aumento, mas a distribuição das vítimas. Das 35, 27 eram civis. Uma nova era dos drones havia começado no México. Os grupos criminosos agora usavam os drones não apenas para atacar inimigos diretos, mas também para semear o pânico na população dos territórios "quentes". Nesse período, houve ataques diretos contra vilas nos estados de Michoacán e Guerrero, em um dos quais os moradores capturaram um assassino da Família Michoacana (Grillo, 2024).

Este assassino, Fernando, fez uma declaração aos jornalistas na qual deu a entender que não só os UAS chegaram ao México para ficar, mas que o seu uso vai aumentar daqui para a frente: «eles têm *operadores de drones*. Eles têm pessoas especializadas em *drones* (...). Eles têm muitos drones, então, mesmo que um traficante (pessoa dedicada ao tráfico de objetos e mercadorias ocultas) perca algum, eles não se importam (...). Como isso está apenas a começar" (Grillo, 2024).

A capacidade técnica das OCT no âmbito dos UAS atingiu tal nível que já se começam a ver os primeiros indícios de um esforço real por parte das organizações criminosas para investir em medidas e unidades antidrones. Prova disso é que, em 2024 e no contexto da guerra civil em Sinaloa, um membro de uma das facções que disputa o

controlo do Cartel de Sinaloa, "los Mayitos" (a facção liderada pelos filhos de Ismael "el Mayo" Zambada, detido em 2024), foi fotografado carregando um sistema de inibição anti-UAS *Skyfend*, avaliado em 100.000 dólares (Jiménez, 2025).

Embora um único sistema de defesa antiaérea seja insuficiente para contrariar o potencial destrutivo dos drones de ataque, ele revela um esforço para entrar na corrida armamentista que pode ser vista em outros cenários, como o ucraniano.

No plano da luta contra o uso ilícito de drones, o governo mexicano reagiu promulgando disposições para dificultar o acesso aos UAV. Em 2019, foi redigida a NOM-107-SCT3-2019, que regula os Sistemas de Aeronaves Pilotadas Remotamente (RPAS). Nela, todos os aparelhos com mais de 250 gramas devem ser registrados. É proibido modificar os RPAS para possibilitar o transporte de mercadorias perigosas ou para lançar objetos. Essa medida, em um país onde há regiões inteiras onde o governo de facto está nas mãos de OCT, teve pouco impacto na resolução do problema do uso de drones para fins criminosos.

No plano humanitário, as ameaças proferidas contra a população civil levaram a vários deslocamentos de refugiados. Em 2023, cerca de 600 residentes de Nuevo Caracol, no estado de Guerrero, tiveram que abandonar suas casas devido aos contínuos ataques com drones sobre a população (Ortiz, 2023).

4.2. COLÔMBIA

Um cenário hispano-americano em que o uso de drones por organizações em confronto com o governo nacional está a se tornar cada vez mais relevante é a Colômbia. Este país registou a sua primeira morte atribuível a drones de ataque em julho de 2024, em que uma criança de 10 anos morreu e outras 12 pessoas ficaram feridas quando um Veículo Aéreo Não Tripulado (, UAV) atacou com uma granada de fragmentação um campo de futebol em El Platerado (Torres, 2024).

O principal responsável pelo uso de drones na Colômbia é o Exército de Libertação Nacional, particularmente desde que lançou a sua ofensiva sobre Catatumbo no início de 2025. Os ataques com drones são parcialmente responsáveis pela crise de deslocados que se viveu nesta região, com mais de 52 000 pessoas forçadas a abandonar as suas casas (ACNUR, 2025).

Uma das facções dissidentes das Forças Armadas Revolucionárias da Colômbia Exército do Povo (FARC-EP), as FARC-EP também protagonizaram ataques com drones, como os ataques em novembro de 2024 e em julho e agosto de 2025 a três Patrulheiras de Apoio Fluvial Pesado da Marinha Colombiana, no rio San Juan del Micay, no departamento de Cauca, ou a queda de um helicóptero antinarcóticos em Antioquia, em agosto de 2025, com a morte dos 13 policiais que estavam a bordo (Saumeth, 2025; Torrado, 2025).

Em 10 de junho de 2025, o autoproclamado Secretariado do Estado-Maior Central das FARC-EP emitiu um comunicado com 10 recomendações para a população civil, imprensa e organismos humanitários, com o objetivo de evitar incidentes de ataques a civis. Entre elas, destacam-se manter uma distância mínima de 500 metros de comboios

militares ou policiais e exigir que as Forças Armadas abandonem instalações adjacentes a edifícios residenciais (W Radio Colombia, 2025).

O número de vítimas de ataques com drones na Colômbia continua sendo menor do que no México, embora na Colômbia estejam começando a ser observados, desde meados de 2025, ataques de magnitude muito maior, como os já mencionados ataques a navios e helicópteros.

Os governos que enfrentam inimigos com Sistemas Aéreos Não Tripulados (UAS) na América do Sul têm-se visto sobrecarregados até ao momento. Vários países, entre os quais a Colômbia, o Peru e o México, começaram a dotar as suas forças armadas e de segurança com sistemas de defesa antirrobôs, para poderem pelo menos proteger as suas bases e infraestruturas críticas.

Por outro lado, há governos no continente americano que estão optando por combater os grupos do crime organizado com drones. No Haiti, uma operação com drones do governo em 1º de março de 2025 resultou em 80 mortes naquele dia, embora não tenha sido possível confirmar que todos fossem membros de organizações criminosas. Um dos líderes das gangues de Porto Príncipe, Jimmy Cherizier, condenou o ataque, ameaçando responder com seus próprios drones, o que poderia causar a morte de "qualquer pessoa do país" (Vyas, 2025).

4.3. SOLUÇÕES PROPOSTAS

O problema enfrentado pelos Estados hispano-americanos é extremamente grave e, a partir de diversas perspetivas, foram compiladas três recomendações que devem constituir os princípios orientadores da política anti-UAS a ser desenvolvida por essas nações: atacar as linhas de abastecimento, aprender com os especialistas e investir em treinamento e táticas (Ziemer, 2025).

É necessário reconhecer que a luta contra as linhas de abastecimento das organizações ilegais é inseparável e intrínseca à luta contra os próprios grupos. Apesar disso, a vitória dos Estados, pelo menos no que diz respeito aos drones, terá necessariamente de vir da abordagem do ataque às linhas de abastecimento.

Abre-se, portanto, uma oportunidade para, talvez, inspirar-se na Operação *Grim Beeper*, realizada pelos serviços de inteligência de Israel, através da qual se infiltraram na cadeia de abastecimento de «buscas» do Hezbollah, com o resultado final que todos conhecemos (Doran, 2024).

Por sua vez, aprender com os especialistas e investir em investigação e táticas significa extrair o máximo rendimento possível das informações que podem oferecer os países mais envolvidos neste desenvolvimento: Ucrânia, Rússia e Israel.

5. APLICAÇÃO DAS LIÇÕES

Muitas lições podem ser extraídas de uma análise das experiências da Síria, Ucrânia, Israel, México e Colômbia. As que consideramos mais importantes são:

A. Os UAS são especialmente eficazes se compararmos o seu preço e capacidade destrutiva.

B. A ligação por fibra ótica permite evitar a incapacitação dos drones por dispositivos inibidores de radiofrequências.

C. A força de uma ação realizada por UAV geralmente baseia o seu sucesso na deteção tardia e na tática de enxame.

D. O avanço da inteligência artificial favorece o surgimento de drones autónomos com capacidade de reconhecer o seu ambiente e designar os seus objetivos.

E. O uso de drones permite retirar o máximo de membros da operação antes de ela começar, reduzindo as baixas próprias a praticamente zero.

Estas lições terão de ser devidamente tidas em conta ao enfrentar possíveis utilizações dos UAS como instrumentos terroristas.

Da mesma forma, deve-se sempre levar em consideração que os grupos que têm capacidade para empregar drones irão utilizá-los. Essa tecnologia e técnicas são fáceis de adaptar a diferentes modos de operação e ambientes, como ficou demonstrado com sua recente incorporação ao cenário da luta contra o crime organizado no Brasil. Em 28 de outubro de 2025, no âmbito de uma operação contra a estrutura do *Comando Vermelho* no Rio de Janeiro, este utilizou drones de combate contra os agentes das forças de segurança. O *Comando Vermelho* é a maior organização de crime organizado do Brasil e já incorporou os Sistemas Aéreos Não Tripulados (UAS) às suas operações (Braun, 2025).

5.1. LIÇÕES APRENDIDAS EM ATAQUES ANTERIORES

5.1.1. Ataques de 11 de setembro

No relatório emitido pela Comissão de Investigação dos atentados de 11 de setembro (11-S) de 22 de julho de 2004 (*National Commission on Terrorist Attacks*, 2004), o décimo primeiro capítulo: «Previsão e Retrospectiva» faz uma análise crítica detalhando as quatro principais fraquezas no sistema de contra-espionagem e luta antiterrorista dos EUA que possibilitaram a prática do maior atentado em número de vítimas da história: falta de imaginação, política inadequada em relação à Al-Qaeda, mau uso das capacidades do governo federal e erros graves na gestão operacional do ataque como tal. A política inadequada e o mau uso das capacidades respondem mais à forma de lidar com um inimigo emergente, pelo que entendemos que escapam ao objetivo deste artigo.

Das duas que vamos analisar, a mais crítica é a falta de imaginação, pois a outra decorre direta ou indiretamente desta. O primeiro erro foi a classificação do risco feita pela comunidade de inteligência dos EUA. O chefe do gabinete antiterrorista, Richard A. Clarke, argumentou numa nota de 4 de setembro de 2001 que parte das agências antiterroristas consideravam os atentados como «um incómodo que mata um número de americanos a cada 18-24 meses». Mesmo aqueles que consideravam o risco real, como

Clarke, redigiam hipóteses em que «centenas» de americanos eram vítimas do terrorismo. Praticamente ninguém imaginava um cenário possível como o que acabou por acontecer.

O relatório também menciona que a comunidade de inteligência ignorou quase completamente a possibilidade de um avião ser usado como veículo suicida, apesar de os ataques suicidas terem se tornado os mais comuns no Oriente Médio. Se tivesse sido realizado um exercício colocando-se no lugar de um terrorista que quisesse usar um avião sequestrado, possivelmente teriam sido detectadas as falhas de segurança que se tornariam evidentes como consequência do 11 de setembro. Além disso, a questão chegou a ser levantada em algumas ocasiões por órgãos externos à comunidade de inteligência, sendo em todos os casos descartada por esta como extremamente improvável. Isto foi exposto no relatório da Comissão de Investigação dos Ataques de 11 de setembro, nas páginas 345 a 348 (*National Commission on Terrorist Attacks*, 2004).

Não menos graves foram os erros cometidos na gestão operacional das ações que possibilitaram a prática do atentado. Destaca-se a falta de coordenação entre agências federais, principalmente a Agência Central de Inteligência (CIA) e o FBI. Todas as ações preparatórias foram detectadas por alguma instituição norte-americana (a reunião prévia em Kuala Lumpur, as entradas dos suspeitos no território norte-americano, a formação como pilotos dos suspeitos e uma longa lista de outras), mas não houve uma boa comunicação dessas informações, o que facilitou que o FBI não considerasse incluir a presença dos suspeitos que tinham localizado no relatório de risco de ataques iminentes.

5.1.2. Ataques de Barcelona e Cambrils

Algo semelhante pode ter acontecido nos atentados que infelizmente abalaram a Espanha em 2017, em Barcelona e Cambrils. As autoridades competentes teriam decidido não agir com base no ofício do então Comissário Geral de Segurança Cidadã da Polícia Nacional, Florentino Villabona Madera, no qual se instava a instalar «grandes vasos de plantas ou postes de amarração nos acessos (a locais com grande afluência de pessoas)» (Redação Barcelona La Vanguardia, 2017). Neste caso, a imaginação das Forças e Corpos de Segurança não falhou, mas sim a dos responsáveis por pôr em prática as suas recomendações. As mesmas lacunas foram observadas no que diz respeito à coordenação policial, podendo ter sido ignorado um suposto aviso enviado pela CIA em 25 de maio de 2017, alertando para a intenção do EIIL de atacar a Rambla de Barcelona (El Periódico Barcelona, 2017).

5.1.3. Resumo das lições aprendidas

A falta de imaginação e coordenação das instituições são dois dos pecados capitais na luta contra o terrorismo. A nova era da tecnologia obriga-nos a repensar a forma de agir dos potenciais terroristas daqui em diante, com o provável uso de drones, inteligência artificial ou a combinação letal de ambos nas próximas tentativas de ataques terroristas, além de outras ferramentas ainda em desenvolvimento.

5.2. POSSIBILIDADES DE ATAQUES TERRORISTAS COM DRONES

5.2.1. Ataques contra aglomerações de pessoas

No que diz respeito aos ataques contra grandes aglomerações de pessoas, consideramos digno de nota o tiroteio em massa em Las Vegas, em 1 de outubro de 2017, no qual um indivíduo se apoderou de um arsenal avaliado em 95 000 dólares e abriu fogo a partir de uma suíte do hotel Mandalay Bay contra um festival ao ar livre nas proximidades do hotel, resultando em 60 mortos e 867 feridos. Este incidente demonstrou o quão ineficazes podem ser as medidas de controlo de acesso a uma instalação, se o risco vier de cima (Las Vegas Metropolitan Police Department, 2018).

Não é preciso muito esforço de imaginação para pensar em como esse mesmo ataque poderia ter sido destrutivo, mas usando Veículos Aéreos Não Tripulados (UAV) que lançassem cargas explosivas de vários quilos sobre a multidão, ainda mais considerando que o ataque aconteceu à noite, o que na realidade já teve consequências trágicas, pois um clima de caos total se instalou entre os presentes.

5.2.2. Ataques contra indivíduos

A possibilidade de atentados contra altas autoridades do Estado também não deve ser descartada. O presidente da Venezuela, Nicolás Maduro, sofreu um atentado com drones explosivos durante um desfile militar em 4 de agosto de 2018 (El Mundo, 2018). Assim, não só esses ataques são possíveis, como já foram tentados.

Sabemos que, embora difícil, não é impossível aproximar-se perigosamente de altas autoridades, como demonstrou a tentativa de assassinato do então candidato à presidência dos EUA, Donald Trump, em 13 de julho de 2024. Thomas Crooks conseguiu aproximar-se armado com uma espingarda AR-15 a menos de 150 metros de Trump e chegou mesmo a disparar oito cartuchos antes de ser abatido por agentes dos Serviços Secretos (*Task Force on the Attempted Assassination of Donald J. Trump*, 2024).

Um hipotético ataque com drones não teria precisado se aproximar tanto quanto um atirador, podendo se camuflar mais facilmente nos arredores antes de lançar um drone guiado por fibra óptica ou um enxame de drones equipados com software de orientação por Inteligência Artificial com o objetivo de atingir Donald Trump.

5.2.3. Ataques contra a aviação e outros setores

O setor aéreo também pode ser alvo deste tipo de ataque. De forma semelhante à Operação Telaraña, no futuro, os drones poderiam reconhecer os motores, depósitos de combustível ou a janela da cabine de um aparelho e colidir contra eles no momento da descolagem ou aterragem. Considerando que um Boeing 737-800 ou um Airbus A320 (os dois modelos mais comuns da aviação comercial) podem transportar mais de 180 passageiros, um impacto efetivo contra um único avião se tornaria imediatamente o segundo maior atentado da história da Espanha.

As opções são inúmeras: comboios detidos por um primeiro drone e que posteriormente começam a ser atacados por outros secundários, ataques combinando

métodos já conhecidos de terrorismo e utilizando drones para atacar pessoas que fogem por pontos de estrangulamento, para citar alguns exemplos.

5.3. ATACAR A LINHA DE ABASTECIMENTO

As vantagens para os terroristas também são inúmeras: não têm como *condição sine qua non* a morte do executor, as ações preparatórias não são realizadas no mesmo local do ataque, dificultando a sua deteção precoce (ninguém pode encontrar uma mochila-bomba que não está lá) e são objetos amplamente vendidos nos mercados civis, pelo que não levantam tantas suspeitas como outros métodos.

Talvez parte de uma perspectiva correta na hora de combater os ataques com drones seja reconhecer que detê-los uma vez iniciada a execução será uma tarefa cada vez mais complexa, se não diretamente impossível em algumas ocasiões; assim como a Rússia não pode ter grandes unidades de defesa antiaérea em cada metro quadrado do seu território, nós também não. Não se deve enfrentar os drones quando já estão a voar em direção ao seu objetivo, mas quando estão dentro de uma caixa a ser transportados de um lugar para outro.

5.4. FASES DELICADAS DO PROCESSO DE PREPARAÇÃO DE UM ATAQUE COM UAS

Conseguimos detetar pelo menos quatro processos delicados na preparação de uma ação terrorista com drones: a obtenção dos drones, o treino dos pilotos, a programação dos drones e a obtenção dos explosivos.

A obtenção de grandes quantidades de Sistemas Aéreos Não Tripulados (UAS) na União Europeia, e mais concretamente em Espanha, não seria a parte mais delicada da operação. Apesar de ser obrigatório estar registado e ter licença para pilotar drones com peso superior a 250 g, estas restrições não se aplicam ao simples ato de comprá-los. Isto revela uma deficiência. O armazenamento excessivo e ilógico desses produtos deve ser sempre vigiado, o que é profundamente prejudicado por essa liberdade de compra. Ainda mais quando isso pode ser feito em qualquer estabelecimento da União Europeia, ou mesmo em outros países, uma vez que não é exigida autorização alfandegária para a importação de UAS para uso pessoal. Também devem ser considerados os drones resultantes do trabalho de impressoras 3D.

O treino dos pilotos poderia ser uma boa oportunidade para impedir a prática do atentado, particularmente se eles tentarem obtê-los por meios legais. Os serviços de inteligência americanos já poderiam ter estado perto de frustrar o 11 de setembro, pelo menos da forma como os terroristas o haviam organizado, quando o FBI emitiu um relatório em julho de 2001 sobre o interesse que suspeitos de serem jihadistas estavam adquirindo pelo treinamento de voo, intitulado: “Extremista islâmico aprende a voar” (Comissão Nacional sobre Ataques Terroristas, 2004).

Será necessário estar especialmente atento ao que acontecerá quando as hostilidades na Ucrânia terminarem e os pilotos de drones de ataque ucranianos e russos tentarem reinserir-se na sociedade. Até agora, os estudos realizados sobre os efeitos psicológicos da operação de drones de ataque têm-se centrado quase exclusivamente nos pilotos de bombardeiros não tripulados americanos, que, pela natureza das suas ações,

estão sujeitos a um nível de stress consideravelmente inferior ao dos operadores ucranianos e russos.

A programação dos aparelhos para seguirem instruções específicas, através do uso de Inteligência Artificial (IA), requer conhecimentos avançados em várias áreas técnicas, como programação em Python e C++, formação em IA, robótica e eletrónica. Não é um conhecimento particularmente dispendioso em termos de tempo, mas um interesse repentino de um sujeito suspeito nessas áreas do conhecimento deve ser um sinal de alerta imediato.

Tal como no ponto anterior, será necessário considerar a possibilidade de que veteranos da guerra da Ucrânia, ou de outras guerras semelhantes no que diz respeito ao uso massivo de drones, colaborem ou mesmo participem ativamente na preparação destas operações. As equipas de drones destes conflitos bélicos têm conhecimentos técnicos sobre a adaptação de drones de pacote para o cumprimento de missões específicas que excedem em muito os conhecimentos que praticamente qualquer outro indivíduo pode ter.

Por último, a aquisição de explosivos constituiria, como é lógico, o processo mais frágil de todo o *iter criminis*. Isto é ainda mais evidente quando se considera que os Sistemas Aéreos Não Tripulados (UAS), devido às suas características técnicas, não podem transportar cargas excessivamente pesadas, obrigando os potenciais terroristas a recorrer a substâncias explosivas com maior potencial de detonação, o que pode, de certa forma, reduzir a procura por essas tentativas.

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

6. CONCLUSÕES

A. Os drones vieram para ficar. Não há dúvida de que o seu uso aumentará enormemente. As experiências dos países que se viram envolvidos em conflitos com drones devem ser adicionadas aos procedimentos próprios.

B. A Operação Telaraña, levada a cabo pelo Serviço de Segurança da Ucrânia (SBU) contra a frota estratégica de longo alcance russa, demonstrou a versatilidade das ações com drones contra alvos situados a milhares de quilómetros atrás da linha da frente. Estes meios demonstraram a sua capacidade de serem infiltrados, distribuídos e operados a grande distância. Extrapolando esta experiência, deduz-se a capacidade destrutiva de um grupo determinado a eliminar uma infraestrutura numa zona civil, dados os recursos necessários.

C. O uso da Inteligência Artificial (IA) nesta operação, acompanhado dos casos já documentados do uso dessas ferramentas, modifica drasticamente o cenário das ameaças futuras. Os drones de ataque acabarão por ser dispositivos explosivos guiados por IA com as ferramentas necessárias para diferenciar aliados de inimigos e eliminar estes últimos.

D. As Organizações Criminosas Transnacionais da América Latina entraram com passo decidido na batalha tecnológica pelo domínio dos céus. As suas redes estabelecidas de tráfico de todos os tipos de materiais e substâncias permitiram-lhes acumular grandes quantidades de Sistemas Aéreos Não Tripulados (UAS), que estão a desempenhar tarefas de vigilância, transporte e ataque. Desde 2021, elas contam com unidades próprias especializadas e atualmente estão começando a investir em material antidrones.

Os ataques, embora tímidos e reduzidos no início, estão a adquirir uma dimensão cada vez mais ambiciosa, atacando até mesmo comboios inimigos em movimento. A população civil também tem sofrido as consequências da introdução dessas tecnologias nos conflitos entre grupos criminosos, com ataques diretos e indiscriminados contra populações cada vez mais frequentes no México e na Colômbia.

Neste último país, as forças armadas e as forças e corpos de segurança estão a ser alvo de ataques consideráveis, que podem ser os primeiros passos para outras ações de uma magnitude ainda nunca vista neste continente.

E. A experiência em todos os teatros de operações demonstrou que o sucesso de uma ação com drones contra um alvo defendido reside no enxame.

F. Na Ucrânia, ficou demonstrado que os drones de ataque são recursos extremamente úteis no contexto de uma guerra e, na América do Sul, que podem servir para semear o terror nas populações e nas unidades de segurança dos Estados, ainda mais se as suas operações responderem aos interesses de grandes organizações com uma capacidade logística e militar superior à de alguns Estados soberanos.

Parece ser uma realidade que, mais cedo ou mais tarde, estas formas de cometer ações violentas chegarão ao Ocidente, bem como a Espanha. Devemos estar preparados e recordar os erros cometidos anteriormente para não os repetir no futuro.

G. A imaginação e a capacidade de gerir estes cenários são dois requisitos fundamentais para enfrentar as novas ameaças. Vários atentados terroristas no passado puderam ser consumados devido a análises de risco incorretas. O aparecimento de drones com IA abre a porta para que os terroristas possam encontrar oportunidades onde antes seria impensável, tanto para eles como para as forças de segurança.

Talvez a forma mais eficaz de os enfrentar seja interceptar as tentativas durante a sua fase de preparação. Tanto a aquisição de drones, como a formação dos pilotos, a programação dos UAS e a obtenção de explosivos parecem ser momentos ideais para frustrar as tentativas de ataques contra a população civil.

A segurança também não deve ser menosprezada. Ataques de pequena dimensão seriam mais difíceis de detetar, mas, ao contrário dos complexos, poderiam ser detidos durante a sua execução.

Por último, devemos salientar a necessidade urgente de aproveitar a experiência que estão a adquirir neste setor os países que se encontram atualmente em conflitos onde a presença e o uso de drones são habituais. Essa informação poderia ser decisiva em futuras investigações contra células terroristas decididas a perpetrar um ataque contra o nosso território.

7. REFERÊNCIAS BIBLIOGRÁFICAS

12ª Brigada de Forças Especiais «Azov» (s.f.). *About Azov*. Recuperado em 3 de setembro de 2025 de https://azov.org.ua/en/about-azov/

ACNUR (2025). *É urgente fortalecer a resposta diante do deslocamento maciço sem precedentes em Catatumbo, Colômbia*. 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). Um drone explosivo, o mais recente artefacto do crime organizado no México. *El País*. https://elpais.com/internacional/2017/10/24/mexico/1508802891_139491.html

BBC (2018). Guerra na Síria: Rússia frustra ataque com drone à base aérea de Hmeimim. *BBC*. https://www.bbc.com/news/world-europe-42595184

Barnes, J. E., Entous, A., Schmitt, E., Troianovski, A. (2023). Ucranianos provavelmente estiveram por trás do ataque com drones ao Kremlin, afirmam autoridades norte-americanas. *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. *Fundação para a Investigação Política, Económica e Social (SETA)*. https://media.setav.org/en/file/2017/08/daeshs-drone-strategy-technology-and-the-rise-of-innovative-terrorism.pdf

Boffey, D. (2025). Máquinas assassinas: como a corrida da Rússia e da Ucrânia para aperfeiçoar drones mortíferos sem piloto pode prejudicar a todos nós. *The Guardian*. https://www.theguardian.com/world/2025/jun/25/ukraine-russia-autonomous-drones-ai

Bondar, K. (2025). Como a Operação Teia de Aranha da Ucrânia redefine a guerra assimétrica. *Centro de Estudos Estratégicos e Internacionais*. https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

Braun, J. e Toledo, L. F. (2025). Comando Vermelho: como drones e armas importadas acabam nas mãos do crime organizado no Brasil e estão a transformar o conflito urbano. *BBC*. https://www.bbc.com/mundo/articles/c4g32d0rzr5o

Connable, B. (2025). Colocando a Operação Teia de Aranha em Contexto. *Guerra Irregular*. http://irregularwarfare.org/articles/putting-operation-spiders-web-in-context/

De Troullioud de Lanversin, J. (2025). O ataque ucraniano aos bombardeiros russos mostra como drones baratos podem perturbar a segurança global. *Boletim dos Cientistas Atómicos*. 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). Operação Spiderweb: uma avaliação das perdas da Força Aeroespacial Russa. *Instituto Internacional de Estudos Estratégicos*. https://www.iiss.org/online-analysis/military-balance/2025/062/operation-spiderweb-an-assessment-of-russian-aerospace-forces-losses/

Departamento de Defesa (2000). Diretiva DOD 12/2000.

Doran, M. (2024). O brilhantismo da «Operação Grim Beeper». *Instituto Hudson*. https://www.hudson.org/technology/brilliance-operation-grim-beeper-lebanon-pager-explosion-israel-iran-michael-doran

Administração de Combate às Drogas (2025). *Avaliação Nacional da Ameaça das Drogas 2025*. https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf

El Mundo (2018). Maduro denuncia «uma tentativa de assassinato» com drones explosivos e culpa o presidente Santos. *El Mundo*. https://www.elmundo.es/internacional/2018/08/05/5b662beeca4741d0498b4648.html

El Periódico Barcelona (2017). Texto integral do alerta de atentado em Barcelona da CIA aos Mossos. *El Periódico*. https://www.elperiodico.com/es/politica/20170831/texto-integro-alerta-cia-mossos-atentado-barcelona-rambla-6255316

First Contact (2025). *UAV Osa de alta acrobacia*. Recuperado em 4 de setembro de 2025 de https://firstcontact.biz/en/projects/high-acrobatic-uav-osa/

Gibson, O., Harvey, A., Novikov, D., Harvard, C. e Stepanenko, K. (2025). Avaliação da Campanha Ofensiva Russa, 1 de junho de 2025. *Instituto para o Estudo da Guerra*. https://understandingwar.org/research/russia/russian-offensive-campaign-assessment-june-1-2025/

Grillo, I. (2024). A Guerra dos Drones em Guerrero. *CrashOut por Ioan Grillo*. https://www.crashoutmedia.com/p/la-guerra-de-drones-entre-carteles

Hambling, D. (2025). Novas táticas com drones garantiram a vitória russa em Kursk. *Forbes*. https://www.forbes.com/sites/davidhambling/2025/03/17/new-drone-tactics-sealed-russian-victory-in-kursk/

Hambling, D. (2016). Como o Estado Islâmico está a usar drones comerciais. *BBC*. https://www.bbc.com/future/article/20161208-how-is-is-using-consumer-drones

Human Rights Watch (2024). *Relatório para a Revisão Periódica Universal de El Salvador (48.ª sessão das Nações Unidas; 4.º ciclo)*. https://www.hrw.org/es/news/2024/07/30/informe-para-el-examen-periodico-universal-de-el-salvador

Jaramillo, J. C. (2025). Drones alimentam corrida armamentista criminosa na América Latina. *Insight Crime*. https://insightcrime.org/news/drones-fuel-criminal-arms-race-latin-america/

Jiménez, X. (2025). 'La Mayiza' põe em xeque as forças armadas em Sinaloa com equipamento anti-drones de elite. *Milenio*. https://www.milenio.com/policia/mayiza-combate-fuerzas-armadas-equipo-anti-dron-elite

Khomenko, I. (2024). Como a Ucrânia está a usar drones com IA para superar a Rússia no campo de batalha. *United24 Media*. https://united24media.com/latest-news/how-ukraine-is-using-ai-drones-to-outsmart-russia-on-the-battlefield-3833

Departamento de Polícia Metropolitana de Las Vegas (2018). *Relatório de Investigação Criminal do LVMPD sobre o Tiroteio com Várias Vítimas de 1 de outubro*. https://www.lvmpd.com/home/showpublisheddocument/134/638298568313170000

Loh, M. (2025). Os bloqueadores de drones da Ucrânia estão a revelar-se decisivos no meio de uma nova ofensiva em solo russo, afirmam blogueiros militares pró-Kremlin. *Business Insider*. https://www.businessinsider.com/ukraine-drone-jammers-killing-it-new-kursk-push-russian-bloggers-2025-1

Lyle, P. (2019). Proliferação do poder aéreo: como os drones comerciais estão a ser usados por organizações extremistas violentas para influenciar o futuro da guerra aérea. *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). Enxames de drones com inteligência artificial entraram agora no campo de batalha. *The Wall Street Journal*. https://www.wsj.com/world/ai-powered-drone-swarms-have-now-entered-the-battlefield-2cab0f05

Maza, J. (2025). Drones e letalidade tecnológica dos cartéis mexicanos. *Conselho Mexicano de Assuntos Internacionais*. https://www.consejomexicano.org/mediateca/articulo/7275

Méheut, C. (2025). Ucrânia recorre a redes de pesca para capturar drones russos. *The New York Times*. https://www.nytimes.com/2025/07/07/world/europe/ukraine-russia-drones-nets.html

Mendoza López, D. (2025). Golpe ao CJNG em Campeche: "El 80", "Lady Drones" e três sicários são presos após operação em 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/

Comissão Nacional sobre Ataques Terroristas (2004). *Relatório da Comissão sobre o 11 de setembro*. https://www.9-11commission.gov/report/911Report.pdf

Naber, I. (2025). Por que a Ucrânia continua sendo a máquina de guerra mais inovadora do mundo. *Politico*. https://www.politico.com/news/magazine/2025/08/27/ukraine-drones-war-russia-00514712

Ortiz, J. (2023). El Caracol: o povo de Guerrero sitiado 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). Os drones e o ataque liderado pelo Hamas em 7 de outubro de 2023: inovação e implicações. *Perspectivas sobre o terrorismo*. https://www.jstor.org/stable/27372135

Price, R. E. (2025). Definindo enxame: um passo crítico para aproveitar o poder dos sistemas autónomos. *Military Review Online Exclusive*. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Online-Exclusive/2025/Defining-Swarm/Defining-Swarms-UA.pdf

Redação Barcelona La Vanguardia (2017). O documento com o qual a Polícia recomendou a colocação de postes de amarração nos acessos a locais movimentados. *La Vanguardia*. https://www.lavanguardia.com/politica/20170819/43665066008/documento-policia-recomendo-instalar-bolardos-accesos-lugares-concurridos.html

Reuter, C. (2000). *O V2 e os programas espaciais russo e americano*. S.R. Research & Publishing.

Salinas, A. (2018). Drone com granadas cai na casa do secretário de Segurança Pública da Baixa Califórnia. *Excelsior*. https://www.excelsior.com.mx/nacional/dron-con-granadas-cae-en-casa-del-secretario-de-seguridad-publica-de-baja-california

Saumeth, E. (2025). As FARC atacam com drones uma terceira patrulha fluvial da Marinha da Colômbia. *Infodefensa*. https://www.infodefensa.com/texto-diario/mostrar/5404281/125-colombia

Secretaria de Defesa Nacional (SEDENA) (2024). *Exército Mexicano e Guarda Nacional detiveram Armando "N", conhecido como "Delta 1", suposto líder do Cartel Jalisco Nueva Generación em Michoacán e 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. (janeiro de 2023). Bigger Fleets Win. *Proceedings*. https://www.usni.org/magazines/proceedings/2023/january/bigger-fleets-win

Força-Tarefa sobre a Tentativa de Assassinato de Donald J. Trump (2025). *Conclusões e Recomendações do Relatório 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). Dissidências multiplicam ataques com drones e acendem alarmes na Colômbia. *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). Criança morre após ataque com drones de dissidentes das FARC em Cauca. *CNN Español*. https://cnnespanol.cnn.com/2024/07/24/nino-muere-ataque-drones-disidencias-farc-cauca-colombia-orix

Valencia, N. (2015). Drone transportando drogas cai ao sul da fronteira dos EUA. *CNN*. https://edition.cnn.com/2015/01/22/world/drug-drone-crashes-us-mexico-border

Villegas, P. (outubro de 2025). Em meio à guerra do cartel, os funerários carregam a dor de Sinaloa. *The New York Times*. https://www.nytimes.com/es/2025/10/24/espanol/america-latina/sinaloa-muertes-trabajadores-funerarios.html

Villegas, P. (setembro de 2025). Drones e explosivos improvisados: os cartéis do México adotam armas de guerra modernas. *The New York Times*. https://www.nytimes.com/es/2025/09/01/espanol/america-latina/mexico-carteles-armas.html

Vyas, K. (2025). Governo do Haiti, em dificuldades, lança drones contra gangues. *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 de junho de 2025). *#NoticiaW | Após a série de atentados em Cauca e Valle del Cauca, o Estado-Maior Central das FARC emitiu* [Recomendações à população civil]. X. https://x.com/WRadioColombia/status/1932474602267021560

Zelenskyy, V (1 de junho de 2025). Discurso à nação sobre o ataque com drones da Operação Telaraña [Transcrição]. American Rhetoric. https://www.americanrhetoric.com/speeches/volodymyrzelenskyoperationspiderweb.htm

Ziemer, H. (2025). Inovação ilícita: a América Latina não está preparada para combater drones criminosos. *Centro de Estudos Estratégicos e Internacionais*. https://www.csis.org/analysis/illicit-innovation-latin-america-not-prepared-fight-criminal-drones

8. NORMATIVA

Regulamento Delegado (UE) 2019/945 da Comissão, de 12 de março de 2019, relativo aos sistemas de aeronaves não tripuladas e aos operadores de sistemas de aeronaves não tripuladas de países terceiros. 11 de junho de 2019. DOUE n.º 152.

Real Decreto 517/2024, de 4 de junho, que desenvolve o regime jurídico para a utilização civil de sistemas de aeronaves não tripuladas (UAS) e altera diversas normas regulamentares em matéria de controlo da importação de determinados produtos no que diz respeito às normas aplicáveis em matéria de segurança dos produtos; demonstrações aéreas civis; combate a incêndios e busca e salvamento e requisitos em matéria de aeronavegabilidade e licenças para outras atividades aeronáuticas; matrícula de aeronaves civis; compatibilidade eletromagnética de equipamentos elétricos e eletrónicos; Regulamento aéreo e disposições operacionais comuns para os serviços e procedimentos de navegação aérea; e notificação de ocorrências na aviação civil. 5 de junho de 2024. BOE n.º 136.

NORMA Oficial Mexicana NOM-107-SCT3-2019, que estabelece os requisitos para operar um sistema de aeronaves pilotadas remotamente (RPAS) no espaço aéreo mexicano. 14 de novembro de 2019.

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