TECNOLOGIAS PARA A DETECÇÃO DE ATAQUES CIBERNÉTICOS POR DRONES EM AEROPORTOS

Matheus Gondim Peixoto[1]
Mauro Caetano[2]
Cristian da Silveira Smidt[3]
Bruno Avelino[4]

RESUMO

Nesse estudo são identificados métodos de detecção de drones em espaço aéreo controlado, mais especificamente para utilização no contexto aeroportuário. A aplicação dos métodos foi direcionada para detecção de drones de pequeno porte, por conta da crescente popularização desses dispositivos, que vem se tornando cada vez mais acessíveis. O estudo identifica três tipos de ataques possíveis feitos por agentes mal-intencionados, que podem afetar as operações aeroportuárias e a segurança de voos. Com a intenção de propor soluções para essas ameaças, foram identificadas técnicas e instrumentos relevantes identificados na literatura e também disponíveis no mercado. A análise comparativa entre as tecnologias de detecção permitiu uma compreensão aprofundada para a proposição de soluções direcionadas aos ataques de drones propostos. Os resultados indicam que a integração de diversos métodos é a melhor resposta para ataques de drones aos aeroportos, promovendo um espaço aéreo mais seguro. Recomenda-se a personalização de cada solução de acordo com as características específicas do aeroporto em questão, para assegurar a eficácia da solução proposta e manter a integridade do espaço aéreo brasileiro.

Palavras-chaves: Infraestrutura aeroportuária; Transporte aéreo; Segurança operacional.

[1]Engenheiro Civil-Aeronáutico formado pelo ITA. 1º Tenente da Força Aérea Brasileira, concluiu o curso de preparação de oficiais da Reserva (CPOR). Instituto Tecnológico de Aeronáutica (ITA). E-mail: matheus.peixoto@ga.ita.br

[2]Professor e Pesquisador em Inovações no Transporte Aéreo no Instituto Tecnológico de Aeronáutica (ITA). Realizou seu pós-doutoramento em Engenharia de Infraestrutura Aeronáutica pelo ITA, Doutorado em Engenharia de Produção pela Universidade de São Paulo (USP), com período sanduíche na Technische Universität Berlin (TUBerlin), Alemanha, foi pesquisador visitante no Institute of Transport and Logistics Studies (ITLS) / The University of Sydney, Austrália, e no International Project Laboratory / The University of Tokyo, Japão. Coordena o MTOW – Grupo de Pesquisas Inovações em Transporte Aéreo e o Laboratório de Transporte Aéreo (LABTAR/ITA) e é Piloto Aerodesportista. ORCID: https://orcid.org/0000-0002-5978-1054
E-mail: caetano@ita.br

[3]Chefe da Subdivisão de Gestão da Inovação do Instituto de Controle do Espaço Aéreo (ICEA). Possui graduação em Tecnologia em Gerenciamento de Tráfego Aéreo pelo Centro de Instrução e Adaptação da Aeronáutica (2010) e Pós-Graduação "Lato Sensu" em Liderança com Ênfase em Gestão no Comando da Aeronáutica pela Universidade da Força Aérea e em Gestão de Projetos, pelo Centro Universitário do Sul de Minas. Tem experiência na área de Defesa, com ênfase em Gerenciamento de Tráfego Aéreo, com foco em planejamento de espaço aéreo, procedimentos de navegação aérea e processos de fomentos e inovação. ORCID: https://orcid.org/0000-0001-9576-5572 E-mail: cristiancss3@fab.mil.br

[4] Pesquisador e Mestrando em Otimização no Instituto Tecnológico de Aeronáutica (ITA) / Exército Brasileiro (EB. Realizou sua graduação em Engenharia da Computação no Instituto Militar de Engenharia (IME) e em Ciências Militares na Academia Militar das Agulhas Negras (AMAN). Integrante do MTOW – Grupo de Pesquisas Inovações em Transporte Aéreo e do Laboratório de Transporte Aéreo (LABTAR/ITA). Trabalhou como Engenheiro de Simulação de Aeronaves de Asa Rotativa e como Analista de Cybersegurança. Mantém expertise em cybersegurança, pesquisa operacional, desenvolvimento de software, inteligência computacional, engenharia de sistemas e inovação. ORCID: https://orcid.org/0000-0003-3256-679X. E-mail: avel.bruno@gmail.com

TECHNOLOGIES FOR THE DETECTION OF CYBER ATTACKS BY DRONES AT AIRPORTS.

ABSTRACT

This study identifies methods for detecting drones in controlled airspace, specifically focusing on their application in the airport context. The use of these methods is directed towards detecting small drones, given the increasing popularity and accessibility of these devices. The study identifies three possible attacks by malicious agents that can impact airport operations and flight safety. To propose solutions to these threats, relevant techniques and tools identified in the literature and available in the market were identified. Comparative analysis of detection technologies allowed for a comprehensive understanding to propose solutions targeted at the proposed drone attacks. The results indicate that the integration of various methods is the best response to drone attacks at

airports, promoting safer airspace. It is recommended to customize each solution according to the specific characteristics of the airport in question to ensure the effectiveness of the proposed solution and maintain the integrity of the Brazilian airspace.

***Keywords**: Airport infrastructure; Air transportation; Operational safety.*

1 INTRODUÇÃO

O uso de drones tem se popularizado na sociedade contemporânea, abrangendo atividades que variam desde aplicações militares, como monitoramento de áreas de risco e observação ampla do espaço aéreo em sistemas e vigilância, entrega de equipamentos e insumos em regiões de difícil acesso, especialmente em situações de desastres naturais (SOUZA; HENKES, 2023), monitoramento de canteiros de obras, fotografia aérea e levantamentos topográficos (MOSLY, 2017), além da agricultura de precisão na coleta de dados em propriedades rurais (JÚNIOR; NUÑEZ, 2023), entre outras.

Com o desenvolvimento dessas aeronaves pilotadas remotamente, surge a necessidade de se desenvolver métodos eficientes de detecção e monitoramento de drones de diversos modelos e tamanhos distintos, principalmente em áreas de uso restrito do espaço aéreo, como o entorno de aeroportos devido às operações de aeronaves e a suscetibilidade de possíveis ataques cibernéticos ocasionados por esses objetos voadores.

Nesse estudo, são identificadas diferentes tecnologias capazes de detectar diferentes objetos voadores que possam apresentar ameaças cibernéticas à segurança das operações aeroportuárias, sendo apresentadas soluções disponíveis na literatura e no mercado, bem como a análise das suas possíveis utilizações em situações de ataques cibernéticos em aeroportos.

1.1 AERONAVES PILOTADAS REMOTAMENTE – DRONES

As aeronaves não tripuladas são denominadas por VANTs (Veículos Aéreos

Não Tripulados), já quando estas são controladas remotamente possuem a classificação de Drones. Outra classificação ocorre no caso em que aeronaves são controladas não recreativamente à distância por um operador, onde passam a ser identificadas como RPAs, acrônimo da sigla em Inglês para *Remotely Piloted Aircraft System* (DECEA, 2018).

O surgimento dos drones ocorreu durante a segunda guerra mundial, com a introdução de bombas lançadas remotamente pelos alemães. Desde então, as aeronaves remotamente controladas tem sido cada vez mais desenvolvidas, aproximando dos padrões mais recentes apenas com os trabalhos do engenheiro aeroespacial Abraham E. Karem (WHITTLE, 2013). Com isso, os drones deixaram de ser utilizados exclusivamente em contextos militares e passaram a integrar setores comerciais da sociedade.

Os tipos mais comuns de drones são: drones de asa fixa, drones de asas rotativas, dirigíveis e ornitópteros (DECEA, 2023). A Figura 1 ilustra um VANT de asas rotativas, já a Figura 2 ilustra um VANT de asas fixas.

Figura 1 - VANT de asas rotativas

Fonte: Eisenbeiss (2004).

Figura 2 - VANT de asas fixas

Fonte: Mototolea e Stolk (2018).

A popularidade dos drones tem aumentado devido as suas versatilidades, facilidades de operação e ampla gama de aplicações em diversos setores (ZMYSLOWSKI *et al.,* 2023). Estas tecnologias quando utilizam sensores, câmeras e GPS, possuem uma variedade de usos como entregas, cartografia, monitoramento ambiental, gravações aéreas, entre outras.

No Brasil, os drones foram se tornar populares apenas após o ano de

2017, quando a primeira aeronave remotamente pilotada recebeu a aprovação do Ministério da Defesa. Após esse acontecimento, eles passaram a ser utilizados em áreas como agricultura de precisão, monitoramento ambiental, controle de fronteiras e também de forma recreativa (BRUM, 2019). Os drones se tornaram cada vez mais acessíveis e completos para a execução de diversas atividades, o que tem demandado o desenvolvimento de soluções eficazes para a sua identificação e monitoramento, principalmente durante o seu voo em áreas restritas, como aeroportos e instalações militares, o que pode apresentar riscos às operações aéreas.

Os perigos relacionados aos drones foram evidenciados em ataques como o ocorrido em Abu Dhabi em janeiro de 2022, quando caminhões de combustível foram atacados por drones e acabaram explodindo. O acidente resultou na morte de 3 pessoas (CNN Brasil, 2023). Já em agosto de 2018 ocorreu um grave atentado contra o presidente Nicolas Maduro em Caracas, Venezuela, em que drones carregados com explosivos foram usados para provocarem explosões que causaram pânico e feriram cerca de sete pessoas (BBC NEWS, 2018). Também em dezembro de 2018 o aeroporto de Gatwick, segundo maior do Reino Unido, teve de ser paralisado, durante 30 horas, devido a ocorrência de 129 reportes policiais diferentes sobre a atividade de drones nas imediações do aeroporto (BBC, 2019).

Outra situação semelhante ocorreu em maio de 2019 no aeroporto de Frankfurt, na Alemanha, quando 143 decolagens e aterrisagens foram canceladas no aeroporto após a identificação de um drone de 1,5 metro de diâmetro na parte sul da área do aeroporto (THE LOCAL, 2019). Tais riscos e ataques remontam a necessidade do monitoramento aéreo para que seja garantida a segurança das operações e a prevenção de possíveis acidentes ou incidentes.

O aumento no uso de RPAs também faz com que se torne necessária a criação de regulamentos e órgãos capazes de fiscalizar este tipo de tecnologia. Tal situação motivou a Agencia Nacional de Aviação Civil (ANAC) a tornar obrigatório o cadastro dos drones com peso variando entre 250 gramas e 25 quilos. Para equipamentos com massa superior a 25 quilos, exige-se também o

registro de habilitação por parte dos pilotos, já os drones com pesos inferiores a 250 gramas não apresentam nenhum tipo de restrição (ANAC, 2017), sendo esses os possíveis elementos críticos na gestão do tráfego aéreo.

A ascensão dos drones tem levantado preocupações em escala global, com diversos países identificando simultaneamente os seus potenciais e as ameaças que representam. Como consequência disso, tem-se dado uma ênfase crescente às pesquisas e ao desenvolvimentos de sensores e sistemas anti-drones (ZMYS-lOWSKI et al., 2023). Essa necessidade tem se intensificada devido ao crescente número de incidentes, invasões de áreas restritas e ataques cibernéticos direcionados através destes dispositivos, o que demanda a inovação em equipamentos de detecção cada vez mais avançados (ZMYS-lOWSKI *et al.,* 2023).

O desenvolvimento de sistemas de segurança para a detecção de drones levou tem orientado a adoção de sistemas híbridos, baseados na fusão de tecnologias de sensores e controle de hardware, predominantes em instalações aeroportuárias, presídios e em grandes eventos (PARK *et al.,* 2021). No entanto, apesar dos avanços em sistemas de detecção, muitos desses mecanismos ainda carecem de integração plena com etapas de identificação e neutralização das ameaças.

Zmys-lowski *et al.,* (2023) determinam que para analisar a eficiência de um sistema anti-drone, o critério fundamental reside na capacidade de proteção que ele proporciona a uma instalação específica. Essa eficiência deve ser medida considerando-se as características únicas da instalação, como localização, dimensão, processos tecnológicos em uso, funções desempenhadas e demais atividades. Além disso, Gopal (2020) entende que um sistema eficaz precisa ter um alcance de detecção de, pelo menos, três quilômetros. O sistema deve detectar e também deve ser capaz de rastrear um drone a uma distância mínima de um quilometro, especialmente quando há sinais de que o dispositivo possa transportar uma carga potencialmente destrutiva.

Drones geralmente emitem sinais de calor, som e radiofrequência (RF) para se comunicarem com seus controladores. Existem sistemas que usam esses sinais para identificar se tem drones por perto e suas localizações. Deve-se combinar os radares com outras tecnologias, como câmeras e scanners de radiofrequência,

para que se obtenha um panorama de detecção eficaz (PARK et al., 2021). Contudo, os sistemas de radar emitem sinais potentes de RF, exigindo permissões nacionais para uso de determinadas frequências e locais de instalação. Em áreas de alta segurança, é fundamental o uso de métodos de detecção variados, especialmente para identificar drones que não emitem sinais de RF, como os usados em atos terroristas, que podem se utilizar de tecnologias específicas de ocultamento.

2 IDENTIFICAÇÃO DE DRONES EM VOO

Os aumentos da popularidade e da tecnologia dos drones trouxeram vários benefícios para atividades comerciais, militares e até missões de busca e vigilância. Entretanto, a proliferação destes dispositivos acabou por levantar problemas relacionados à segurança e possíveis riscos às operações de tráfego aéreo. Diante deste cenário, tornou-se necessário identificar e rastrear drones em voo para garantir a segurança aérea e neutralizar possíveis ameaças. Para abordar essas questões, diferentes métodos de identificação e rastreamento em voo foram desenvolvidos pela sociedade acadêmica. Entre eles, destacam-se a tecnologia ADS-B, o pulso-chirp, o uso de aprendizado profundo com câmeras, a assinatura Micro-Doppler com FSR, uso de scanners de RF e uso de câmeras de infravermelho.

a. ADS-B

O ADS-B (*Automatic Dependent Surveillance-Broadcast*) é uma tecnologia utilizada fundamentalmente para o rastreamento e monitoramento de aeronaves no espaço aéreo controlado. Essa Tecnologia facilita a troca de informações precisas entre aeronaves, com uso de informações confiáveis provenientes principalmente do Sistema de Posicionamento Global GPS (*Global Positioning System*) e faz uso da comunicação por radiofrequência. As trocas de informações sobre as posições e velocidades atualizadas das

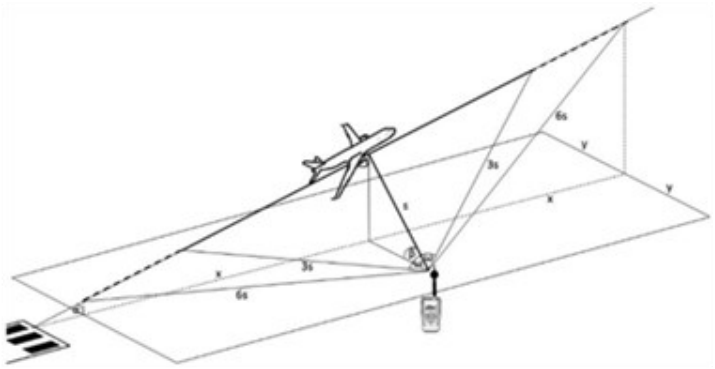
aeronaves ocorrem com o uso de transponders instalados nestas (RODRIGUES, 2010).

O rastreamento de drones pode ser beneficiado desse método amplamente utilizado com aeronaves, em que é possível obter informações em tempo real sobre localização e velocidade deles. O monitoramento desse tipo de atividade aérea possibilita evitar colisões entre drones e aviões. Aeronaves equipadas com sensores do tipo ADS-B usam receptores para enviarem suas posições e combinarem dados como seus rumos, velocidades e altitudes. Segundo Rodrigues (2010), as informações são transmitidas para outras aeronaves que tenham o sistema equipado (ADS-B IN) e para estações com antenas receptoras no solo ou no mar (ADS-B OUT). As estações repassam em tempo real as informações para os centros de controle de tráfego aéreo.

No estudo realizado por Giladi (2020), a frequência de velocidade utilizada para a transmissão das mensagens ADS-B é de 1090 MHz, uma frequência designada para comunicações de vigilância em diversos países (OACI, 2012). Através desta frequência, as aeronaves emitem sinais contendo informações cruciais para o monitoramento do tráfego aéreo e para o conhecimento mútuo entre as aeronaves em espaço aéreo compartilhado. Essas mensagens são transmitidas em intervalos de aproximadamente 0,5 segundos, proporcionando uma atualização frequente das informações.

Neste estudo qualquer aeronave voando acima da área de interesse e abaixo de 1,2 km acima do nível do solo (AGL) pode ser detectada pelo sistema de medição. Quando uma mensagem ADS-B é recebida de uma aeronave que está voando dentro da área de monitoramento intensivo definida, o sistema de medição realiza as etapas finais, recebendo, registrando e analisando simultaneamente os dados da aeronave e o ruído medido. De tal forma, são registradas todas as mensagens ADS-B da aeronave específica que ativou a gravação, juntamente com o nível de ruído medido, a partir de um nível de ruído acima de um limite pré-definido. A representação geométrica da situação pode ser explicitada com a Figura 3.

Figura 3 - Distâncias para monitoramento de ruídos



Fonte: Giladi (2020).

O ADS-B apresenta-se bastante eficaz para identificar eventos sonoros e outras informações de aeronaves por meio do uso essa tecnologia, mesmo quando os ambientes possuem diversos obstáculos e ruídos de fundo. Constatou-se que em função do uso dessa tecnologia depender de satélites GPS confiáveis, este método se destaca frente ao uso de outros radares tradicionais que dependem de outras fontes externas. Apesar disso, o método proposto por Giladi (2020) pode apresentar falhas de detecção dos ruídos durante a propagação, isto devido a dissipação do som de aeronaves que se encontram distante dos microfones instalados ou por interferências de outros ruídos durante a propagação.

Os transponders ADS-B usualmente utilizados são excessivamente grandes para o modelo de drone abordado por este estudo, sendo mais adequados para drones com maiores dimensões. Uma possibilidade para drones de pequeno porte seria a tecnologia ADS-B pertencente à família Ping2020 da uAvionix (2023), um produto pronto para uso ADS-B em nível de drone, que pode ser conectado ao controlador de voo do drone e transmitir informações de voo através do canal RF (faixa de frequência dentro do espectro de radiofrequência utilizada para a transmissão de sinais) (PARK *et al.,* 2021). O referido transponder possui alto valor de obtenção, sendo previamente necessário que houvesse opções de baixo custo de produção em todo o país para que o método de identificação fosse economicamente viável.

b. Radar de pulso-chirp

O radar de pulso pode ser usado na identificação e localização de drones no espaço aéreo, isso pois o radar emite um pulso curto e com alta intensidade de energia eletromagnética que sofre aliterações quando ocorre reflexão do pulso pelo drone. Os pulsos são emitidos em intervalos padrões, que são registrados os intervalos decorridos entre os momentos de emissão e os momentos em que ocorrem detecção dos ecos refletido pelo objeto (CURRIE, 2005).

O uso deste método consiste em direcionar o pulso em uma dada direção e analisar a mudança de frequência ocorrida após o fenômeno da reflexão, essa análise é capaz de fornecer informações sobre o objeto em que ocorre a colisão. Para Misaridis et al. (2000) as vantagens do uso do radar pulso-chirp em comparação com os radares convencionais estão relacionadas com uma maior capacidade de resolução em distância, melhor discriminação de alvos em ambientes com muitos objetos refletores e melhor velocidade de análise.

O radar em questão é capaz de emitir pulsos com frequências variáveis e também pode fornecer as análises dos sinais refletidos, identificando se há presença ou não de drones no espaço monitorado. Os sinais refletidos são analisados quanto as flutuações de amplitude e fase que ocorrem neste fenômeno da reflexão. As flutuações são consideradas como características distintivas dos drones em comparação com outros objetos, de tal modo que dados dessas variações são utilizados para construírem os modelos de flutuação do alvo. Esses modelos representam as características específicas das flutuações que são esperadas quando um drone está presente.

Com o objetivo de identificar drones pelo modelo de flutuação do alvo, Kim *et al.,* (2018) propõem um algoritmo capaz de reconhecer características dos sinais de radar e fazer comparações com modelos de flutuação que já compõem a sua base de dados. São utilizadas técnicas de processamento de sinal e análise estatística durante as comparações, então após a verificação

da similaridade dos sinais observados e os modelos de flutuação dos alvos, pode-se dizer se o alvo é um drone ou não. Neste método, a equação do radar é empregada para determinar o RCS (*Radar Cross Section*) máximo detectável. O RCS é uma medida da quantidade de energia refletida por um objeto quando iluminado por um radar. A partir da Equação básica do radar é possível relacionar a potência do sinal recebido pelo radar com a potência do sinal transmitido e o RCS do objeto. A Equação 1 apresenta como pode ser obtido o RCS máximo detectável de drones.

$$P_r = \frac{P_t . G_t . G_r . \lambda^2 . RCS . A}{4 . \pi . R^4} \quad (1)$$

onde *Pr* é a potência do sinal recebido pelo radar, *Pt* a potência do sinal transmitido pelo radar, *Gt* o ganho da antena transmissora, *Gr* o ganho da antena receptora, λ o comprimento de onda do sinal transmitido, *RCS* a seção transversal de radar do objeto, *A* a área efetiva do alvo, e *R* a distância entre o radar e o objeto.

No contexto do estudo proposto por Kim et al. (2018), a Equação 1 é utilizada para determinar o RCS máximo detectável de diferentes drones utilizando um radar de pulso chirp. O RCS máximo detectável é um parâmetro necessário para definir a capacidade do radar em detectar e rastrear drones com eficiência. Os resultados obtidos comprovam a qualidade do método frente a identificação de drones com sucesso, conseguindo distinguir de outros objetos como pássaros ou aeronaves. Entretanto, o uso de radar de pulso-chirp possui limitações quanto à existência de interferências externas que afetam o radar, podendo apresentar falhas se houver sinais de outros dispositivos eletrônicos e existirem obstáculos físicos que alterem as propriedades do sinal.

A efetividade da identificação pode ser comprometida dependendo da localização da área protegida. Drones tem a capacidade de voar em altitudes extremamente baixas e essa habilidade de sobrevoar terrenos irregulares é um dos fatores que pode tornar sua detecção por radar mais complexa

(LUKASIEWICZ; TWARDOWSKA, 2022). Outra limitação do método é a dependência de características específicas dos drones, de forma que não reconheça drones com características de flutuações atípicas. Uma diferente abordagem de monitoramento de drones consiste na abordagem que envolve obtenção de imagens e estratégias computacionais, apresentadas em seguida.

c. Aprendizado profundo na detecção e rastreamento de drones por imagens

A detecção e o rastreamento de drones podem ser realizados por meio do uso da tecnologia de aprendizado profundo (*Deep Learning*) em conjunto com diversas câmeras coordenadas. A tecnologia de aprendizado profundo é explorada de forma a permitir que o sistema aprenda e se adapte com base nos dados disponíveis, fazendo com que os resultados obtidos sejam cada vez mais precisos.

Uma maneira de potencializar os resultados obtidos com o uso do aprendizado profundo e com a integração de redes neurais convolucionais para que sejam extraídas características importantes das imagens obtidas com as filmagens (CUNHA, 2020). O diferencial das redes convolucionais reside na qualidade com que extraem características dentro da própria rede, possibilitando obterem informações sobre formatos, tamanhos, cores e movimentos do drone para identificarem suas posições e trajetórias. Os algoritmos mais relevantes utilizados são os classificadores do tipo YOLO (*You Only Look Once*) que dividem as imagens em grades regulares de células capazes de identificar os limites dos objetos com o uso de caixas delimitadoras (*bounding boxes*) e prever por meio de probabilidades as classes dos objetos contidos dentro delas. A Figura 4 ilustra a comparação de detecções produzidas por diferentes arquiteturas de algoritmos.

Figura 4 - detecções produzidas por diferentes arquiteturas

Fonte: Unlu *et al.,* (2019).

As detecções pela arquitetura YOLO são representadas pela coloração verde e as de- mais pelas colorações azul e vermelha. A arquitetura YOLO é a que melhor identificou a presença de 2 pássaros e 1 drone se aproximando em voo na imagem. O treinamento dessa arquitetura de algoritmos com grandes conjuntos de dados que contenham exemplos de diferentes drones é efetivo para garantir que o método identifique possíveis ameaças e colabore para a criação de um sistema confiável de monitoramento. Unlu et al. (2019) propõem um sistema que emprega uma câmera esta ‘tica de amplo ângulo e uma câmera inferior montada em uma torre giratória para detecção e rastreamento de drones com o intuito de otimizar o uso de memória e o tempo de processamento. Este estudo sugere uma abordagem de aprendizado profundo que combina múltiplos quadros. O quadro capturado pela câmera com zoom na torre é sobreposto ao quadro de amplo ângulo da câmera estática, resultando em um fluxo de processamento eficiente. Assim, a detecção inicial de pequenas incursões aéreas é realizada simultaneamente tanto no plano da imagem principal quanto no plano da imagem ampliada.

O método desenvolvido é capaz de fornecer vistas panorâmicas e tridimensionais durante o monitoramento dos ambientes desejados, o que acaba permitindo que a detecção e o rastreamento dos drones sejam efetuados de maneira mais precisa. Com a obtenção e combinação de

imagens por diferentes câmeras em tempo real, o acompanhamento permite respostas rápidas em caso de identificação de drones ou outras ameaças aéreas. No entanto, o método precisa ser adaptado para que consiga superar as limitações encontradas como variações de luminosidade dos ambientes e ruídos visuais que interferem nos resultados encontrados.

Equipamentos de detecção de drones que utilizam câmeras ópticas são mais acessíveis financeiramente e sofrem menos restrições regulamentares em comparação com as outras técnicas apresentadas (PARK et al., 2021). Isso permite que sejam aplicados sistemas densos de câmeras que se complementam no monitoramento. Apesar disso, possuem limitações como alcance limitado. Essas limitações evidenciam a necessidade de integrá-los a outros sistemas de detecção. Os sistemas militares eletro-ópticos e infravermelhos (EO/IR), costumam ser empregados em grandes escalas e utilizam câmeras ópticas com sensores infravermelhos para a identificação de drones (PARK; AHN; BAEK, 2012).

d. Assinatura Micro-Doppler para detecção de drones usando FSR

A assinatura Micro-Doppler é uma técnica utilizada para detecção e classificação de objetos em movimento, como drones, baseando-se no fenômeno Doppler (MUSA *et al.,* 2019). Ela consiste na análise dos padrões de modulação dos sinais de Micro-Doppler refletidos pela interação entre as hélices do drone e o ambiente ao seu redor. Ocorre também um formato de modulação adicional de frequência devido a partes específicas do corpo do drone que estão em micro movimento. Esses movimentos como foi analisado por Chen (2011) podem ser causados por vibrações ou pequenas regiões do objeto que refletem os sinais e causam variações nas frequências dos sinais refletidos (CAMMENGA *et al.,* 2014). O uso da assinatura permite identificar características e padrões distintos no sinal refletido pelo drone, possibilitando a detecção e classificação precisa do objeto em movimento.

No processo de recebimento das ondas geradas por esses movimentos

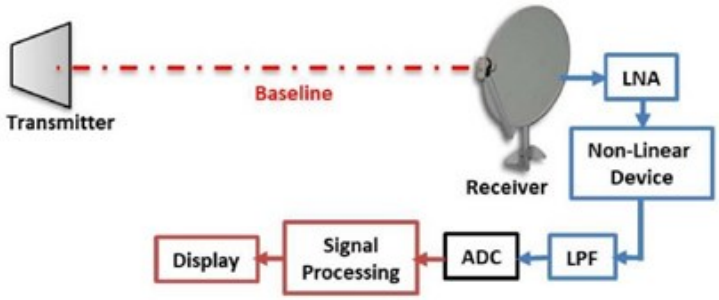
descritos, a geometria de radar de dispersão direta *Forward Scatter Radar* (FSR) é escolhida para o recebimento dos sinais refletidos e as antenas do radar são dispostas em uma linha reta ou em uma matriz bidimensional (MUSA *et al.,* 2019). Essa disposição linear ou planar permite que o radar adquira múltiplas amostras do sinal refletido pelo alvo a partir de diferentes posições. Isto, devido a sua vantagem para a detecção de alcance altamente precisa com base na diferença de fase entre os sinais de transmissão e recepção obtidos separadamente em mais de duas frequências operacionais (PARK *et al.,* 2019).

A configuração FSR é capaz de medir a variação da frequência do sinal refletido pelo drone, permitindo a análise da assinatura de micro-Doppler, que contém informações sobre os padrões de movimentação do drone. Além disso, este radar apresenta alta sensibilidade e resolução, o que possibilita a detecção de pequenos objetos em movimento, como os drones, em diferentes condições ambientais.

Já Musa *et al.,* (2019) propõem a utilização da FSR a partir de uma antena de prato parabólico como receptor. O objetivo é realizar a detecção e análise de drones por meio da análise do sinal espalhado. Para isso, o sinal recebido pelo radar é combinado com um sinal de referência, que desempenha um papel crucial na formação do sinal espalhado. O sinal de referência atua como uma referência comparativa para o sinal ecoado, permitindo a identificação de diferenças entre eles (MALANOWSKI, 2011).

Estas diferenças contém informações relevantes sobre a presença e características do drone em análise. A combinação do sinal de referência com o sinal ecoado possibilita a separação e extração de componentes específicos do sinal espalhado, facilitando a detecção e análise precisa do drone (MALANOWSKI, 2011). O modelo proposto com uso de antena é apresentado na Figura 5.

Figura 5 - Geometria de radar de dispersão direta



Fonte: Musa *et al.,* (2019).

No sistema proposto de detecção de drones, a antena parabólica é utilizada para direcionar e concentrar o sinal refletido pelo drone. O sinal recebido é amplificado pelo amplificador de baixo ruído (LNA) antes de ser processado e um dispositivo não linear realiza uma operação de potência no sinal. Essa operação é descrita matematicamente por uma Equação que estabelece a relação não linear entre o sinal de entrada e de saída. A saída desse dispositivo não linear contém informações relevantes sobre a assinatura Micro-Doppler gerada pela rotação das lâminas do drone. Após a passagem pelo dispositivo não linear o sinal tem sua faixa de frequência limitada em um filtro do tipo passa-baixa (LPF), em seguida sofre conversão em forma digital pelo conversor analógico-digital (ADC) e tem as informações que caracterizam sua assinatura Micro-Doppler identificadas com o processamento de sinal pelo uso de algoritmos. Os resultados obtidos no processo são fornecidos em um Display que representa o dispositivo de saída, tais como um computador ou monitor. A Equação 2 representa a modulação de fase gerada como resultado de um micro- movimento circunferencial de cada lamina.

$$\phi_{md}(t) = -\frac{2\pi}{\lambda}\frac{Lb}{2}cos\left(\frac{\beta}{2}\right)cos\,(\delta)\,cos(\,\Omega.\,t + \Theta) \qquad (2)$$

onde λ é o comprimento de onda, Lb o comprimento da lâmina, β o ângulo bistáico, δ o ângulo de incidência, Ω a velocidade angular das lâminas, t o instante de tempo, e ϑ o ângulo inicial.

O ângulo bistáico β é um parâmetro que descreve a geometria de um

sistema de radar, especificamente a configuração angular entre o transmissor, o alvo e o receptor. Para um rotor com *N* lâminas, serão geradores *N* dispersores rotativos com ângulos iniciais diferentes, que são dados pela Equação 3 (MARTIN; MULGREW, 1990).

$$\theta_n = \theta_0 + \frac{2\pi.n}{N} \tag{3}$$

onde *n* varia de 0 a *N-1*. O sinal total recebido para N lâminas é dado pela Equação 4.

$$S_{rx}(tot) = \sum_{k=0}^{N-1} A_{rx}\,(n).Sin(2\pi.f.dt + \varphi_{md}.n(t)) \tag{4}$$

onde *f* é a frequência da onda gerada pela interação entre as hélices do drone e o ambiente ao seu redor, *dt* é o diferencial de tempo, $A_{rx}(n)$ a amplitude do sinal recebido para cada lâmina, e *φmd* é valor numérico que representa a modulação de fase.

A Equação 5 quantifica a amplitude da composição entre os sinais refletidos e o de referência.

$$A_{rx}(n) = A_{ref}\,.A_{surv}(n) \tag{5}$$

onde A_{ref} e A_{surv} são, respectivamente, os sinais de referência e refletido correspondentes para a onda gerada pela enésima lâmina e a relação entre as variáveis.

Os experimentos foram conduzidos utilizando uma antena parabólica como receptor e um drone DJI Phantom-3 quadcopter como alvo. As assinaturas Micro-Doppler são geradas e podem ser então comparadas com os dados teóricos para que se comprove a validade do método. Os resultados obtidos por Musa et al. (2019) indicam que a técnica é eficiente na detecção e análise de drones, isso pois o método possuí a capacidade de resolução adequada para maioria dos casos de detecção por conta da alta sensibilidade do radar para identificar aliterações nas

frequências. Entretanto, o método tem limitações nas situações em que enfrenta condições climáticas adversas, não conseguindo identificar com precisão os drones em situações de chuvas intensa ou nevoeiros.

e. Identificação com uso de scanners de rádio frequência

Os drones operados por controladores tendem a trocar mensagens específicas com uso de sinais radiofrequência (RF), contendo informações como comandos de voo e leituras de sensores (PARK *et al.,* 2021). Em relação a isso, Al-Sa'd *et al.,* (2019) desenvolveram um sistema que utiliza redes neurais profundas com várias camadas ocultas para analisar e categorizar sinais de RF. Esse sistema é capaz de identificar diferentes tipos de drones e seus respectivos modos de voo. Os scanners RF captam os sinais eletromagnéticos emitidos pelos drones, enquanto localizadores de direção indicam de onde o drone está transmitindo (ZMYS-lOWSKI *et al.,* 2023). Dessa forma, esse sistema em conjunto possibilita a identificação e localização de drones de forma que os operadores aeroportuários possam agir rapidamente e conter possíveis riscos.

A detecção baseada em RF é limitada por sua incapacidade de identificar drones que não emitem sinais de RF constantemente, como é o caso dos que operam com navegação autônoma. Existe a limitação também devido aos scanners RF identificarem drones analisando seus sinais, o que pode ser desafiador quando os drones utilizam protocolos de controle desconhecidos (PARK et al., 2021).

Os scanners de RF são bastante eficientes em detectar a presença de um drone e em identificar sua categoria ao compará-los com bandas conhecidas. Apesar disso, esses scanners enfrentam limitações na localização precisa de um drone no espaço, a não ser que sejam usados em uma configuração de triangulação que é definida pelo uso de vários receptores para determinar a localização exata dos drones (MOTOTOLEA; STOLK, 2018).

f. Identificação com uso de câmeras de infravermelho

A detecção de drones em voo pode tornar-se muito difícil em circunstâncias noturnas ou em ambientes urbanos. Uma alternativa para este cenário é o uso de Câmeras termográficas infravermelhas que são capazes de detectarem pequenas variações de calor no nível de dezenas de mK (ANDRAS˘I *et al.,* 2017). Estas câmeras possuem a capacidade de identificar objetos que emitem calor, o que permite que operem com eficiência em períodos noturnos. Isso ocorre porque são capazes de captar a emissão térmica na faixa do infravermelho proveniente da geração de calor pelos componentes eletrônicos dos drones. Assim, as assinaturas térmicas destes equipamentos podem ser facilmente reconhecidas (STURDIVANT; CHONG, 2017).

O estudo de Andra˘si *et al.,* (2017) com drones destacou que ao contrário das expectativas, os motores não são as principais fontes de calor detectáveis no espectro térmico, devido ao eficiente resfriamento pela circulação de ar. As baterias, contidas no corpo principal do drone e que acabam por receber circulação de ar limitada, são facilmente visíveis em imagens térmicas, principalmente nos drones com corpo totalmente fechado em que a temperatura permanece maior. Observa-se também a qualidade do método para identificar até mesmo drones de pequeno porte que passariam despercebidos por outros tipos de radares.

A Tabela 1 apresenta um resumo das principais características dos métodos apresentados identificados na literatura. Deve-se destacar do estudo de Gopal (2020) que a quantidade de calor produzida pelo drone varia conforme o tipo de propulsão utilizada, sendo mais difícil detectar drones com propulsão elétrica que é mais discreta frente ao método. Para os drones civis, o alcance deste método de detecção é atualmente de apenas cerca de 100 m.

Tabela 1 - Principais técnicas de detecção e rastreamento de drones na literatura

Técnicas	Autor	Parâmetros	Limitações	Vantagens
ADS-B	Giladi (2020)	Frequência ADS-B; pacotes ADS-B; alcance máximo de detecção.	Não universalidade; alto custo; complexidade; interferências.	Precisão elevada; ampla utilização na aviação tradicional; grande amplitude de cobertura.
Radar de pulso-chirp	Kim et al. (2018)	Frequência de operação; alcance máximo do radar; sensibilidade do radar.	Obstáculos físicos; interferências; menor precisão.	Alcance longo; eficácia em condições climáticas adversas.
Aprendizado profundo	Dupouy et al. (2019)	Resolução das câmeras; número de câmeras; algoritmos empregados; taxa de amostragem das imagens.	Dependência de boas condições de iluminação; alcance limitado.	Detecção precisa; maior capacidade adaptativa.
Micro-Doppler	Musa et al. (2019)	Banda de frequência; duração da assinatura.	Limitações das condições atmosféricas; problemas na presença de ruídos.	Alta sensibilidade e precisão.
Scanner RF	Al-Sa'd et al. (2019)	Frequência de sinais RF; troca de mensagens específicas; localizadores de direção.	Não identifica drones com navegação autônoma; problemas com protocolos de controle desconhecidos.	Eficiente em detectar e identificar drones; capaz de trabalhar em configuração de triangulação; longo alcance.
Câmeras de infravermelho	Andrašsi et al. (2017)	Diferenciação térmica em mK; emissão infravermelha.	Dificuldade em diferenciar drones de pássaros; não eficaz para longas distâncias.	Eficiente em ambientes noturnos; capaz de identificar drones de pequeno porte.

As desvantagens notadas são a probabilidade significativa do objeto identificado ser considerado um pássaro e a detecção não ser efetiva para longas distâncias.

g. **Soluções de detecção disponíveis no mercado**

A necessidade de monitorar e controlar o tráfego de drones no espaço aéreo tornou-se uma oportunidade para inovações nesse mercado. Diferentes soluções são identificadas para diferentes cenários e necessidades, podendo atuar de maneiras reativas ou preventivas buscando a integração otimizada das tecnologias de detecção disponíveis.

i. Dedrone

A empresa Dedrone tem inovado na linha DedroneTactical de defesa anti-drone com sua plataforma autônoma C2 (controle e coordenação de operações) orientada por IA. Indo além da simples correlação de sensores, a plataforma integra algoritmos avançados e técnicas de aprendizado de máquina, como filtros de modelos de comportamento e redes neurais, processando mais de 18 milhões de imagens baseadas em IA (DEDRONE, 2023). A sua capacidade de processamento de dados procura eliminar os falsos positivos, proporcionando a detecção de drones com alta precisão e confiabilidade.

A empresa oferece o Kit de resposta ágil CsUAS que proporciona flexibilidade modular na fusão de sensores e mitigação em campo, cobrindo detecção de RF e fazendo uso de câmeras (DEDRONE, 2023). O sistema é equipado com um laptop resistente, sensores de RF robustos e acessórios relacionados. O modelo também pode ser expandido para integrar pontos remotos e outros sensores táticos via rede mesh, rede na qual os dispositivos ou nós estão conectados diretamente, de forma dinâmica e não hierárquica. O sistema oferecido pela Dedrone se integra a vários outros sistemas de segurança e pode ser considerado uma solução completa de segurança do espaço aéreo (ZMYSLOWSKI et al., 2023). A Figura 6 apresenta o Kit Base de resposta ágil CsUAS fornecido pela empresa Dedrone.

Figura 6 - Kit Base fornecido pela Dedrone

Fonte: Dedrone (2023).

O Kit Base permite detectar e anular o sinal RF em um mastro e possui cobertura espacial de 360 graus. Até agora, a Dedrone comercializou mais de 100 kits DedroneTactical para governos nos EUA e internacionalmente (NETTLEFOLD, 2023).

ii. MyDefence

iii.

No contexto de encontrar soluções robustas e eficazes para o desafio de detecção de drones, a MyDefence surge como uma empresa inovadora que oferece tecnologias avançadas. A MyDefence desenvolveu soluções baseadas em variadas tecnologias, cada uma focando em necessidades específicas. Uma de suas soluções propostas é a C-UAS de instalação fixa, elaborada especialmente para infraestruturas críticas como prisões, acampamentos militares e aeroportos. Esta solução é permanentemente ancorada no local, capaz de entregar um panorama situacional contínuo, colaborar na identificação da localização do piloto do drone e possui uma sinergia eficaz com as autoridades externas (MYDEFENCE, 2023).

Adicionalmente, todos os alertas de RF são meticulosamente registrados, permitindo análises pós-incidentes detalhadas (MYDEFENCE, 2023). Com foco no segmento governa- mental e corporativo, o portfólio é composto pelas tecnologias Watchdog 202 e o Wolfpack 210, o primeiro atua como um sensor RF de instalação

fixa, especializado na detecção de drones, enquanto o segundo é um detector RF com cobertura de 360°. O diferencial da solução diz respeito a escalabilidade do sistema C-UAS, podendo ser adaptado às características do local a ser protegido mesmo após a instalação inicial (MYDEFENCE, 2023). As atualizações e melhorias também podem ser implementadas sem a necessidade de substituição completa do sistema. As Figuras 7 e 8 apresentam os componentes da solução de instalação fixa proposta.

Figura 7 - Detector de RF WATCHDOG 202 para proteção de perímetro

Fonte: Mydefence (2023).

Figura 8 - Detector de RF WOLFPACK 210 para proteção de perímetro

Fonte: Mydefence (2023).

O sistema C-UAV de instalação fixa pode ser fixado em paredes, postes ou tripés e integra-se facilmente com radar e câmera. Este foi desenvolvido para ser discreto, resistente e eficiente. Outro ponto forte é a economia de energia e a facilidade com que permite atualizações sem a necessidade de substituição completa, adaptando-se crescentes necessidades de segurança.

iv. Hensoldt

O XPeller é uma tecnologia capaz de detectar drones desenvolvida pela empresa alemã Hensoldt. Ele é indicado para a defesa de aéreas sensíveis como aeroportos, estádios e prisões. Uma de suas principais vantagens é sua adaptabilidade, podendo ser configurado de diversas maneiras, o que o torna eficaz para defesas fixas, como em antenas de transmissão e pistas de aeroportos. O XPeller também pode ser anexado `a veículos ou transportado manualmente (HENSOLDT, 2023).

Ele é equipado com radares, câmeras eletro-ópticas e infravermelhas, interferidores de radiofrequência direcionais, IFF (*Identification Friend or Foe*), detectores e localizadores de RF e sensores acústicos. O XPeller destaca-se também por sua abordagem não destrutiva. As informações são coletadas, processadas e fundidas em um software C2 de fácil utilização (HENSOLDT, 2023). Seu sistema de interferência não danifica os drones, mas os obriga a retornar `a base ou a pousar. A Figura 9 apresenta os sensores e radares que compõem a tecnologia XPeller.

Figura 9 - Radar de vigilância para veículos não tripulados e proteção de ativos críticos

Fonte: Hensoldt (2023).

Outro ponto relevante é sua capacidade de rastrear o operador do drone e funcionar tanto de dia quanto de noite, em qualquer condição climática (SPELTA,

2019).

Os radares SPEXER 2000 e SPEXER 600 fornecem dados de detecção precisos e com classificação de alvo que permitem a detecção de alvos pequenos mesmo em condições climáticas adversas. Os sensores ópticos Z:NightOwl ZM / ZM-ER e Z:NightOwl M são capazes de fornecer visão de longo alcance em alta definição e um alcance de observação de 360º, já o sistema MRD7 utiliza as mais recentes tecnologias de RF e síntese de sinal para interferências de curto e médio alcance. Por fim o GMJ9000 é um sistema de vigilância ultracompacto e independente para oferecer monitoramento de banda larga em uma solução compacta e robusta.

v. Geofencing

Geofencing é um recurso tecnológico que estabelece limites virtuais para evitar que drones entrem em espaço aéreo proibido, como os aeroportos, tornando-se essencial para a segurança do espaço aéreo (STEVENS; ATKINS, 2018). Há sistemas de geofencing adaptados a drones de pequeno porte e também modelos de sistemas de piloto automático modernos que já incorporam as barreiras virtuais como uma medida de contenção em regiões de alta sensibilidade (HAYHURST et al., 2015). Ao ser integrado ao software de um drone, o geofencing se mostra uma barreira de segurança altamente eficaz, especialmente quando os drones possuem sistemas de GPS ou GNSS, prevenindo-os de adentrar aéreas não autorizadas (AISC, 2015).

Os fabricantes de drones frequentemente atualizam os sistemas de geofencing para realizar modificações em zonas restritas, incluindo novas áreas ou aliterações temporárias. Alguns fabricantes desenvolveram geocercas tridimensionais ao redor de aeroportos, aumentando a segurança nas rotas de aproximação e partida das aeronaves, minimizando o risco de interferências perigosas durante decolagens e aterrissagens (DJI, 2019). Apesar dessas medidas de precaução, deve ser pontuado que os geofences podem apresentar falhas, principalmente se os operadores de drones desativarem os recursos de

segurança intencionalmente.

3 MÉTODO

Nesse estudo são identificadas e comparadas diferentes tecnologias capazes de detectarem drones em espaço aéreo controlado, especialmente nas proximidades de aéreas sensíveis de aeroportos. Foram definidos como objetos de estudo as tecnologias para detecção de drones de pequeno porte (carga útil inferior a 250g), e suas potenciais implicações em cenários de ataques cibernéticos em aeroportos.

a. Drone de referência

Foi utilizado o drone DJI mini 2 como objeto de análise, visto que possui imensa popularidade devido à combinação de um design moderno com preços atrativos e confiança associada à marca DJI, líder global na área de drones possuindo aproximadamente 70% deste mercado (INSIDER, 2020). O modelo em questão apresenta o maior número de registros junto à ANAC (2022), correspondendo a 9,43% dos registros e, além disso, destaca-se como o drone predominantemente comercializado no Brasil em 2023. A relevância deste drone é potencializada por sua portabilidade e facilidade de uso, tornando-o adequado para aplicações em distintos contextos. A Figura 10 apresenta o modelo de drone escolhido.

Figura 10 - Modelo de drone DJI Mini 2

Fonte: DJI (2023).

As principais especificações do drone de referência são:

- Peso de decolagem: 242g;
- Dimensões: Dobrado (sem hélices): 138×81×58 mm (L×W×H), Desdobrado (sem hélices): 159×203×56 mm (L×W×H), Desdobrado (com hélices): 245×289×56 mm (L×W×H);
- Velocidade horizontal máxima: 16m/s;
- Tempo máximo de voo: 31 minutos;
- Distância máxima de voo: 16 km;
- Sistema Global de Navegação por Satélite: GPS + GLONASS + Galileu;
- Giro 360º;
- Possui 4 motores;
- Com conexão Wi-Fi;
- Funcao retorno automático.

Destaca-se que devido ao peso inferior a 250 g, o DJI Mini 2 cumpre com os regulamentos de voo estabelecidos para maioria dos países e é reconhecido como exemplo de sucesso na miniaturização e eficiência de drones, pois possui especificações e funcionalidades comparáveis a modelos maiores e mais caros. Com preço de venda próximo a R$ 3 mil, inclui câmera de alta resolução e apresenta tempo de voo diferenciado para esta faixa de custo.

Outro ponto a ser observado é a operabilidade do modelo, uma vez que apresenta sistemas intuitivos e modos assistidos de voo que são úteis para uma ampla gama de aplicações. Destaca-se que o drone estudado trata-se de um quadricóptero por possuir 4 asas rotativas.

A detecção eficiente de drones é uma questão de crescente relevância e ainda possuí diversas limitações que são exploradas neste estudo. E´ verificada a necessidade de identificar a presença de drones, especialmente quando podem representar ameaças à segurança, à privacidade ou à integridade de espaços aéreos restritos. Ao definir as qualidades e defeitos dos diferentes métodos de detecção, como radares ativos, scanners de RF, sistemas visuais e sensores, o estudo colabora para uma compreensão detalhada de como cada tecnologia responde a desafios como iluminação variável, interferências sonoras e

obstáculos físicos. Destaca-se que atualmente não ha´ sistema proposto isoladamente que garanta segurança completa contra drones, diferentes técnicas devem ser implantadas simultaneamente no mesmo sistema.

b. Áreas de segurança em um aeroporto

Este estudo considera a estruturação básica de possíveis alvos para ataques em um aeroporto, sendo composta pelas seguintes aéreas vitais de funcionamento operacional: terminais de passageiros, pistas de pousos, decolagens e taxiways, pátio de aeronave, área de chegada, movimentação, estacionamento, manutenção, carregamento, embarque, desembarque e saídas de aeronaves, torre de controle e estações prestadoras de serviços de telecomunicações e de tráfego aéreo, e conexões externas, como pontos que ligam o aeroporto a outros meios de transporte externos ao terminal - carros, metros, ônibus, etc. (SAC/MINFRA; ITA, 2021), Tais pontos são críticos para o aeroporto e podem sofrer ataques por drones.

4 RESULTADOS E DISCUSSÕES

Os métodos de detecção de drones identificados foram selecionados com foco nas características específicas do modelo de drone estudado. Embora a tecnologia ADS-B seja promissora na integração futura de diversos tipos de drones, acredita-se que ela ainda possa levar um tempo para estar presente nas categorias de drones de pequeno porte, dadas as limitações associadas ao seu custo de implantação e inserção em um complexo sistema de controle de tráfego aéreo.

Portanto, a análise se concentra nos demais métodos, que podem ser utilizados eficazmente no corrente cenário. A Tabela 2 apresenta alguns dos principais benefícios e limitações das tecnologias identificadas.

Tabela 2 - Comparação entre tecnologias de detecção de drones

Método	Benefícios	Limitações
Radar	Detecções longas; rastreia diversos tipos de drones; distingue drones de aves; independe das condições climáticas.	Alcance depende do RCS; altos custos de aquisição e operação; requer licença para transmissão.
Scanner RF	Grande acurácia de detecção; detecção passiva, sem necessidade de licença; menor custo em relação aos radares.	Não identifica drones com navegação autônoma; não consegue identificar múltiplos drones simultaneamente.
Visual	Identifica drones sem emissão de sinais RF; registra ocorrências para investigação.	Alcance limitado; depende de condições de iluminação.
Câmeras de Infravermelho	Eficiente em ambientes noturnos; grande acurácia.	Dificuldade em diferenciar drones de pequenas aves; não eficaz para longas distâncias.

A classificação dos métodos de detecção varia de acordo com fatores ambientais e funcionais, devendo ser levada em consideração suas funcionalidades em relação a tais aspectos para entender a eficácia de cada tecnologia em diferentes condições operacionais. Os métodos de Radar, scanners RF, câmeras visuais (VIS) e câmeras infravermelho (IR) são comparados em termos de desempenho sobre a habilidade de operar em condições meteorológicas adversas.

Além disso, aspectos técnicos, como a capacidade de identificação e detecção múltipla, são também analisados. Outros fatores cruciais incluem o custo do sistema, a eficácia na detecção e a precisão na localização dos drones. Esta classificação permite aos usuários e desenvolvedores de sistemas de segurança aeroportuária escolherem a tecnologia mais adequada para integrar em suas soluções de detecção. A Tabela 3 apresenta um resumo dos principais parâmetros associados a tais tecnologias.

Tabela 3 - Diferentes parâmetros associados às tecnologias

Fator	VIS	IR	Radar	Scanners RF
Custo	$	$$	$$$	$$
Aves	✓		✓	✓
Condições Meteorológicas Adversas		✓	✓	✓
Localização do controlador				✓
Detecção de Múltiplos Drones	✓	✓	✓	
Identificação de Drones	✓	Limitado		✓
Ruído		✓	✓	✓
Detecção de Longo Alcance		Limitada	✓	✓
Luz	✓	✓	✓	✓
Escuridão		✓	✓	✓

a. Possíveis ataques por drones em aeroportos

Neste estudo foram identificados 3 cenários de possíveis ataques por drones de pequeno porte em aeroportos, sendo considerado principalmente a ameaça os sistemas indiretos e de suporte, bem como possíveis colisões diretas com aeronaves. Os ataques identificados representam ameaças emergentes e muitas vezes subestimadas. A análise desses cenários pode ser utilizada para antecipar e preparar respostas eficazes contra essas novas formas de ameaças

i Ataque aos sistemas de gestão do tráfego aéreo

O uso de transponder ADS-B para transmissão de informações entre aeronaves e estações terrestres de vigilância pode ser explorado tanto por operadores de drones maliciosos, que visam obter informações com espionagem, quanto por usuários que pretendam disferir ataques diretos contra o sistema aeroportuário. Segundo Manesh e Kabouch (2017), o sistema de comunicação

ADS-B já demonstrou falhas de segurança, muitas relacionadas com a falta de criptografia utilizada no método. Diante dessa fraqueza, muitas informações podem ser obtidas ou até mesmo adulteradas com a intenção de causar ataques diretos ao sistema.

O ataque pode ocorrer com um invasor posicionado nas proximidades do aeroporto com um rádio definido por software fazendo uso de um sistema transmissor/receptor ADS-B capaz de coletar dados das aeronaves em trânsito.

Com a obtenção de informações sobre as coordenadas espaciais e identificação das aeronaves, ele poderia lançar no espaço aéreo drones equipados com transponders ADS-B e capazes de falsificarem suas identidades com os dados anteriormente obtidos. Esses drones podem ser utilizados para a emissão de sinais ADS-B adulterados que imitam as emissões das aeronaves comerciais e podem gerar caos no sistema de vigilância do aeroporto. No pior dos casos, o controlador dos drones utilizaria as informações das aeronaves para criar riscos de colisões ao lançar drones contra as trajetórias mais prováveis das aeronaves em situações mais complexas como decolagens e aterrisagens.

ii Ataque aos sistemas remotos de apoio à gestão do tráfego aéreo

Drones podem ser utilizados para se obterem informações sobre os sistemas de telecomunicações aeronáuticas utilizados pelo aeroporto, identificando vulnerabilidades para serem exploradas em futuros ataques.

Usando o canal FPV (*First Person View*), o operador pode controlar o drone e obter informações à distância. Os drones equipados com câmeras são capazes de capturar dados e imagens em tempo real, o que pode auxiliar na identificação de falhas na segurança do aeroporto. Além disso, drones com transceptores de rádio podem interceptar transmissões de rádio ou causar interferências (LYKOU *et al.,* 2019). Eles também tem potencial para atacar infraestruturas críticas com cargas explosivas, como já ocorrido em aeroportos na Arábia Saudita (NEWS ANI, 2019).

Os sistemas de comunicação, vigilância e navegação são vitais para a operação de aeroportos e frequentemente se encontram em locais remotos,

distantes das estruturas centrais aeroportuárias. Esses sistemas, que incluem telecomunicações aeronáuticas, auxílios à navegação e radares de vigilância, são responsáveis por orientar, localizar e direcionar aeronaves, mantendo o fluxo seguro e eficiente do tráfego aéreo. (ICAO, 2020).

Este ataque dos drones pode ter 2 direcionamentos: primeiro, coletar dados confidenciais das transmissões de instalações remotas ao aeroporto que contribuem na gestão do tráfego aéreo e segundo interromper a funcionalidade desses sistemas ao interferir nos sinais de telecomunicação emitidos dessas infraestruturas remotas para a torre de controle ou danificar fisicamente os equipamentos de suporte à navegação e vigilância, como radares e estações de energia. Estes sistemas podem ser vulneráveis a ataques aéreos pois, em geral, possuem localizações distantes do centro do aeroporto. Um ataque destes pode resultar em impactos adversos no tráfego aéreo, atrasos ou cancelamentos de voos. A Figura 11 ilustra a interceptação de sinais RF emitidos por sistemas remotos de suporte à gestão do tráfego aéreo.

Figura 11 - Drone interceptando e gerando interferência na transmissão de dados para o aeroporto

iii Ataque aos sistemas de comunicação e informação dos aeroportos.

Outra forma de ataque seria direcionado às redes sem fio e às infraestruturas de TI de um aeroporto. Sinais enviados pelo ar podem ser captados por receptores sintonizados na frequência correta. Conforme Lupu (2009) e Wilkinson (2014), os dados transmitidos podem ser obtidos por drones equipados com antenas sem fio com softwares embarcados.

Os drones, para Guri *et al.,* (2017), são capazes também de interceptar e coletar informações de computadores que se mantenham isolados de qualquer outra rede, e Nassi et al. (2019) demonstra que eles podem captar conversas à distância com uso de dispositivos de espionagem. Drones equipados com tecnologia de captura de sinal podem explorar comunicações internas ao aeroporto, infiltrando-se nas redes sem fio para interceptar e capturar dados dos usuários da rede.

Uma das técnicas utilizadas nesse ataque diz respeito ao uso de etiquetas RFID (*Radio-Frequency Identification*), como pequenos dispositivos que armazenam informações e que podem ser rastreados por meio de ondas de rádio. Os drones com leitores RFID podem detectar informações contidas nas etiquetas, podendo obter informações até mesmo a centenas de metros de distância (KLEINER *et al.,* 2006). Um agente infiltrado poderia aproveitar a entrada na cobertura do edifício ou nas instalações e infraestruturas próximas, sem ser notado pelos controles de segurança. O infiltrado seria capaz de distribuir etiquetas RFID para marcar locais como: roteadores sem fio, salas de servidores de aeroportos e redes de câmeras de segurança. O drone pode navegar com seu sistema de navegação GPS desligado, evitando que seja identificado facilmente e seguir a rota identificada pelas etiquetas RFID distribuídas para orientar o seu ataque.

Com este ataque o sistema aeroportuário pode ser prejudicado, com interrupções dos serviços e possíveis fugas de dados das operações realizadas. Informações sigilosas dos aeroportos e de seus usuários correm o risco de serem acessadas por indivíduos mal-intencionados. O aeroporto pode ter que interromper as operações por questões de segurança e arcar com o prejuízo financeiro gerado em tal situação.

b. Soluções propostas para os ataques definidos

Os aeroportos são caracterizados por diferentes tamanhos, fluxo de tráfego, arquitetura, quantidade de pistas, entre outras. Essas estruturas devem

dispor de forma peculiar seus sensores e mecanismos de defesa para que consiga obter a maior segurança para seus funcionários e clientes, bem como para a e eficiência das operações desenvolvidas. As ameaças geradas por drones de pequeno porte podem ser minimizadas com processos de detecção integrados que garantam proteção contra os ataques direcionados aos sistemas de gestão de tráfego aéreo, ataques aos sistemas remotos que apoiam a gestão de tráfego aéreo e ataques aos sistemas de comunicação e informação dos aeroportos.

Embora o geofencing seja uma ferramenta valiosa na proteção contra drones não autorizados, sua eficácia pode ser complementada por outros métodos de detecção e interdição. Neste contexto, são sugeridas medidas específicas para aumentar a segurança dos aeroportos contra operações mal intencionadas de drones.

i Soluções para o ataque aos sistemas de gestão do tráfego aéreo.

A integração de drones no espaço aéreo traz desafios para a segurança dos aeroportos devido `a vulnerabilidade do sistema ADS-B, utilizado para comunicação entre aeronaves e estações terrestres. Conforme indicado por Manesh e Kabouch (2017), a ausência de criptografia adequada no ADS-B permite que invasores, com equipamentos apropriados, capturem dados das aeronaves e lancem drones emitindo sinais falsificados, perturbando o monitoramento aeroportuário e aumentando o risco de colisões durante decolagens e pousos.

Soluções como o Kit Base da Dedrone podem ser utilizadas como forma de resposta ao ataque proposto, sendo disposto em aéreas elevadas como torres de controle. A solução oferece cobertura ampla do espaço aéreo e permite a detecção eficaz de transmissões ADS-B suspeitas. Isto, devido a capacidade de seu sistema de processamento para analisar os dados de comunicação. O XPeller pode ser usado em conjunto por conta de sua versatilidade, sendo ideal para instalação em aéreas periféricas do aeroporto, onde seus detectores de RF e sensores acústicos trabalham conjuntamente para identificar e rastrear operadores de drones mal-intencionados, assegurando a proteção do perímetro

do aeroporto.

O XPeller pode identificar drones mal-intencionados e utilizar seus interferidores de radiofrequência direcionais para neutralizá-los antes que se aproximem de áreas sensíveis. Esta tecnologia também pode ser utilizada para identificar um agente mal-intencionado ainda nas proximidades de um aeroporto, sendo essencial para o combate deste tipo de ataque extremamente letal que demanda pouco tempo de resposta do sistema de detecção. Em complemento, a solução da Dedrone, ao detectar sinais potencialmente perigosos, rapidamente é capaz de acionar um protocolo de alerta, informando a torre de controle e garantindo uma reação imediata. Esta tecnologia diferencia sinais legítimos e adulterados, minimizando interrupções indevidas nas operações aeroportuárias.

Acredita-se que, para este tipo de situação, os radares seriam a opção primária de detecção de drones, dado o seu longo alcance e capacidade de rastrear drones (diferenciando de aves). Eles seriam alocados ao redor do perímetro do aeroporto para maximizar a cobertura do espaço aéreo. O uso de scanners RF agregaria por ser uma detecção passiva de sinais RF, sem prejudicar os sinais da operação. Por terem menor custo frente aos radares, seriam utiliza-dos como uma camada adicional de segurança posicionada próxima às pistas de decolagem e aterrisagem para identificar tentativas de interferência nos sinais ADS-B. Câmeras vi- suais e câmeras infravermelho poderiam ser utilizadas como forma de complementar a identificação e diferenciar alvos com protocolos desconhecidos.

ii Soluções para o ataque aos sistemas remotos de apoio à gestão do tráfego aéreo

Agentes mal-intencionados podem explorar falhas e coletar informações confidenciais utilizando drones de pequeno porte com uso do canal FPV. Este ataque pode expor falhas de segurança e até mesmo conduzir danos diretos a infraestruturas críticas remotas. Os sistemas de comunicação, vigilância e navegação do aeroporto podem estar ameaçados e sofrerem danos fatais.

Nesse padrão de ataque, a defesa deve ser estruturada inicialmente com a

implementação de radares de ampla cobertura ou detectores de RF visando identificar alvos a longas distâncias. Deve-se integrar também o uso de sensores como câmeras eletro-ópticas ou câmeras Infravermelho para ampliar a capacidade de distinguir os drones conforme eles vão se aproximando e tornando possível identificar suas possíveis cargas. Esses mecanismos de defesa podem ser estrategicamente posicionados em aéreas críticas, como nas proximidades dos sistemas remotos, na torre de comando ou em pontos elevados na estrutura aeroportuária. A integração desses sistemas com o centro de operações do aeroporto é suficiente para uma resposta rápida a este tipo de ataque.

Iii Soluções para o ataque aos sistemas de comunicação e informação dos aeroportos

As infraestruturas aeroportuárias precisam ser ágeis no rastreio de drones, especial- mente quando estes realizam movimentos lentos ou permanecem estacionários sobre aéreas críticas. A complementação de scanners de RF com câmeras eletro-ópticas ou infravermelhas, permite ao sistema de detecção monitorar voos não autorizados e ainda coletar informações adicionais sobre possíveis cargas transportadas pelo drone.

A estratégia de posicionamento destes sensores requer uma distribuição cuidadosa ao redor do perímetro aeroportuário, priorizando regiões de acesso público e sendo fundamentada em avaliações de risco realizadas por especialistas. Porém, destaca-se a missão de identificar e neutralizar o operador do drone, em vez de focar exclusivamente no dispositivo aéreo em si.

As equipes de segurança devem ser devidamente capacitadas com a utilização de scanners RF portáteis e intervirem proativamente contra atividades suspeitas. A tecnologia desenvolvida pela Dedrone mostrou-se adequada para o cenário proposto, pelo oferecimento de uma abordagem integrada dos nós de uma forma dinâmica, onde sistemas de radares e sensores eletro-ópticos se comunicam para garantir que os pontos críticos no sistema de comunicação dos aeroportos não sejam atacados. O software avançado da Dedrone também possibilita a distribuição e monitoramento estratégico dos sensores ao redor do

perímetro aeroportuário, otimizando a cobertura de aéreas de alto risco e de acesso público.

5 CONSIDERAÇÕES FINAIS

O presente estudo discutiu sobre a adoção de métodos e tecnologias para detecção de drones em espaço aéreo controlado, mais especificamente focando na detecção de drones de pequeno porte que se aproximam de aeroportos. O estudo abordou as classificações das aeronaves não tripuladas e o fenômeno da popularização dos drones e notou-se que a regulamentação e a supervisão desses equipamentos ainda se encontram em estado de desenvolvimento, principalmente devido aos riscos da utilização desses equipamentos para fins criminosos.

Mesmo havendo diversas soluções tecnológicas para detecção de drones, ainda preocupa a falta de normas e manuais internacionais que orientem a integração, a concepção e a aplicação destes sistemas em aeroportos e infraestruturas críticas. Assim, devem-se avaliar os riscos de interferências nas comunicações que possam ser causadas pelos radares e sensores empregados, que podem afetar outras formas legítimas de comunicação.

A interferência em sinais emitidos por radares de aproximação e comunicações via rádio é um exemplo crítico que pode causar danos catastróficos. É fundamental que os operadores de aeródromos respeitem os limites legais ao implantarem sistemas Anti-Drones e que todos os riscos sejam mapeados e avaliados. A tomada de ações deve ser orientada com dados confiáveis obtidos com os sistemas escolhidos para esta proteção aérea e torna-se fundamental o desenvolvimento de planos de contingência que definam medidas de segurança claras.

A utilização de drones pode atrair agentes com más intenções, uma vez que existem modelos de drones relativamente acessíveis e que fornecem meios para realizar ataques com baixo risco ao usuário. As infraestruturas críticas de aeroportos precisam ser protegidas contra esses ataques aéreos através de uma avaliação eficaz das ameaças e de ações de resistência.

Embora os ambientes aeroportuários sejam complicados, com uma variedade de tamanhos e características, eles tem requisitos de segurança semelhantes para proteger as suas instalações, detectar e identificar drones utilizados indevidamente. Fazendo-se uso de uma extensa pesquisa bibliográfica sobre tecnologias de detecção de drones, foram desenvolvi- das três categorias de cenários de ataque em instalações aeroportuárias e foi proposto um ou mais planos de proteção para cada caso.

Três cenários de ataques por drones de pequeno porte destacam-se pelo potencial de danos: o comprometimento dos sistemas de gestão de tráfego aéreo através da exploração de falhas na criptografia do sistema ADS-B, ataques a sistemas auxiliares remotos que podem afetar a eficiência do gerenciamento do espaço aéreo, e ataques contra infraestruturas críticas de comunicação e informação, que podem desencadear falhas de segurança e roubo de dados.

Os métodos de detecção adotados incluíram a integração de radares e sensores, pois esta combinação é considerada pela literatura como a forma mais efetiva em cobrir diversos tipos de ameaças e configurações de ataques. Para garantir uma vigilância primária completa nos aeroportos, sugere-se o uso de vários radares com diferentes faixas de detecção. Recomenda-se também a combinação de sensores de detecção visual (câmeras eletro-ópticas e infravermelhas) e scanners RF para identificação dos drones e suas cargas.

A detecção de drones em aeroportos para prevenir atividades indesejadas é um dilema amplo e profundo. Por mais que exista uma variedade de soluções tecnológicas disponíveis, os operadores de aeródromos devem permanecer dentro da lei quando utilizam tecnologias disruptivas e os riscos para a comunidade devem ser totalmente avaliados e compreendidos. Os aeroportos devem fundamentalmente desenvolver planos de ação de contingência detalhando as respostas adequadas que ocorrem antes, durante e depois de qualquer incidente com drones. Adicionalmente, a indústria de sistemas Anti-Drones ainda carece de padrões unificados, o que resulta em uma ampla variação na eficácia e confiabilidade dos sistemas disponíveis.

AGRADECIMENTOS

Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

REFERÊNCIAS

AISC. What Is Geofencing? 2015. Disponível em: <https://www.aisc.aero/what-is-geofencing/>. Acesso em: 3 nov. 2023.

AL-SA'D, M. F.; AL-ALI, A.; MOHAMED, A.; KHATTAB, T.; ERBAD, A. Rf-based

drone detection and identification using deep learning approaches: An initiative towards a large open source drone database. Future Gener. Comput. Syst., Elsevier Science Publishers B. V., v. 100, p. 86–97, 2019.

ANAC. Regulamento Brasileiro de Aviação Civil Especial (RBAC-E) 94: Requisitos gerais para aeronaves não tripuladas de uso civil. Bras´ılia, 2017.

ANAC. Drones. 2022. Disponível em: <https://www.anac.gov.br/acesso-a-informacao/dados-abertos/areas-de-atuacao/aeronaves/drones-cadastrados/painel-de-drones-cadastrados>. Acesso em: 23 maio. 2023.

ANDRAS˘I, P.; RADIS˘IC´, T.; MUS˘TRA, M.; IVOS˘EVIC´, J. Night-time detection of UAVs using thermal infrared câmera. Transportation Research Procedia, v. 28, p. 183–190, 2017.

BBC. Gatwick Airport Drone Attack: Police Have No Lines Inquiry. 2019. Disponível em: <https://www.bbc.com/news/uk-england-sussex-49846450>. Acesso em: 27 set. 2023.

BBC NEWS. Venezuela President Maduro survives 'drone assassination attempt'. 2018. Disponível em: <https://www.bbc.com/news/world-latin-america-45073385>. Acesso em: 12 out. 2023.

BIRCH, G. C.; GRIFFIN, J. C.; ERDMAN, M. K. UAS Detection, Classification, and Neutralization: Market Survey 2015. Albuquerque, New Mexico and Livermore, California, 2015.

BRUM, C. B. D. Uso dos drones nos procedimentos civis e criminais no brasil: Considerações sob a ótica dos direitos fundamentais. DRONES E CIÊNCIA, p. 28, 2019.

CAMMENGA, Z. A.; BAKER, C. J.; SMITH, G. E.; EWING, R. Micro-doppler target scattering. In: 2014 IEEE Radar Conference. Cincinnati, Ohio: IEEE, 2014.

CHEN, V. The Micro-Doppler Effect in Radar. 3. ed. London, England: Artech House Radar Library, 2011.

CNN Brasil. Por que ataque a Abu Dhabi pode ser um perigoso ponto de virada no oriente médio. CNN Brasil, v.20, n. 43, p. 64–83, 2023.

CUNHA, L. C. D. Redes neurais convolucionais e segmentac¸˜ao de imagens: uma revisão bibliográfica. 2020. Trabalho de Conclusão de Curso (Especialização) - Escola de Minas, Universidade Federal de Ouro Preto, Ouro Preto.

CURRIE, G. Introduction to radar systems. IEEE Aerospace and Electronic Systems Magazine, v. 20, n. 1, p. 3–36, 2005.

DECEA. AIC no 24, de 11 de junho de 2018. Aeronaves remotamente pilotadas para uso exclusivo em operações dos ´org˜aos de Seguran¸ca Pu´blica, da Defesa Civil e de Fiscaliza¸c˜ao da Receita Federal. Rio de Janeiro: DECEA, 2018.

DECEA. ICA nº 100-40, de 6 de junho de 2023. Sistema de aeronaves remotamente pilotadas e o acesso ao espaço aéreo brasileiro. 2023.

DECEA. Espaço Aéreo Brasileiro. 2023. Disponível em: <https://www.decea.mil.br/?i=quem-somosp=espaco-aereo-brasileiro>. Acesso em: 6 jun. 2023.

DEDRONE. Dedrone Tactical. 2023. Disponível em: <https://www.dedrone.com/solutions/dedrone-tactical>. Acesso em: 22 out. 2023.

DJI. DJI Enhances Geofencing Technology to Protect Airports. 2019. Disponível em: <https://www.dji.com/ae/newsroom/news/dji-improves-geofencing-to-enhance- protection-of-european-airports-and-facilities>. Acesso em: 3 nov. 2023.

DJI. Comparação de Drones de Consumo. 2023. Disponível em:

<https://www.dji.com/br/products/comparison-consumer-drones>. Acesso em: 10 agosto. 2023.

EISENBEISS, H. A mini unmanned aerial vehicle (uav): System overview and image acquisition. International Workshop on PROCESSING AND VISUALIZATION USING HIGH-RESOLUTION IMAGERY, Pitsanulok, Tailaˆndia, 2004.

GILADI, R. Real-time identification of aircraft sound events. Transportation Research Part D: Transport and Environment, v. 87, p. 102527, 2020.

GOPAL, V. Developing an effective anti-drone system for Índia Armed Forces. Observer Research Foundation, n. 370, jun 2020.

GURI, M.; ZADOV, B.; ELOVICI, Y. Led-it-go: Leaking (a lot of) data from air-gapped computers via the (small) hard drive led. In: International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment.

Berlin/Heidelberg, Germany: Springer, 2017. p. 161–184.

HAYHURST, K. J.; MADDALON, J. M.; NEOGI, N. A.; VERSTYNEN, H. A. Case

Study for Assured Containment. Anais da International Conference on Unmanned Aircraft Systems (ICUAS). 2015.

HENSOLDT. XPELLER - Modular Counter-UAS System. 2023. Disponível em:

<https://www.hensoldt.net/solutions/xpeller/>. Acesso em: 23 out. 2023.

ICAO. Annex 10, Aeronautical Telecommunications. 2020. Disponível em: <https://www.business-standard.com/article/news-ani/houthi-says-it-targe ted-saudi-arabia-s-abha-airport-with-drone-attack-119072900175_1.html>. Acesso em: 25 out. 2023.

INSIDER, B. Drone manufacturers and companies to invest in. 2020. Disponível em: https://www.businessinsider.com/drone-manufacturers-companies-invest-stocks.

JÚNIOR, J. C. A.; NUN˜EZ, D. N. C. The use of drones in agriculture 4.0. Brazilian Journal of Science, v. 3, n. 1, p. 1–13, 2023.

KIM, B.; PARK, J.; PARK, S.-J.; KIM, T.-W.; JUNG, D.-H.; KIM, D.-H.; KIM, T.;

PARK, S.-O. Drone detection with chirp-pulse radar based on target fluctuation models. ETRI Journal, v. 40, n. 2, 2018.

KLEINER, A.; PREDIGER, J.; NEBEL, B. Rfid technology-based exploration and slam for search and rescue. In: 2006 IEEE/RSJ International Conference on Intelligent Robots and Systems. Beijing, China: IEEE, 2006.

LUPU, T. Main types of attacks in wireless sensor networks. Recent Advances in Computer Engineering, Vasile Parvan 2, 300223, Timisoara, ROMANIA, n. 9, 2009.

LYKOU, G.; ANAGNOSTOPOULOU, A.; GRITZALIS, D. Smart airport cybersecurity: Threat mitigation and cyber resilience controls. Sensors, v. 19, n. 1, p. 19, 2019. ISSN 1424-8220.

MALANOWSKI, M. Signal Processing for Passive Bistatic Radar. 3. ed. London, England: Artech House Radar Library, 2011.

MANESH, M. R.; KABOUCH, N. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the automatic dependent surveillance-broadcast (ADS-B) system. International Journal of Critical Infrastructure Protection, v. 19, p. 16–31, 2017.

MARTIN, J. L.; MULGREW, B. Analysis of the theoretical radar return signal form aircraft propeller blades. IEEE International Conference on Radar, p. 569–572, 1990.

MISARIDIS, T. X.; GAMMELMARK, K. L.; JØRGENSEN, C. H.; LINDBERG, N.;

THOMSEN, A. H.; PEDERSEN, M. H.; JENSEN, J. A. Potential of coded excitation in medical ultrasound imaging. Ultrasonics, v. 38, n. 1, p. 183–189, 2000.

MOSLY, I. Applications and issues of unmanned aerial systems in the construction industry. International Journal of Construction Engineering and Management, p. 235–239, jun 2017.

MOTOTOLEA, D.; STOLK, C. Detection and localization of small drones using commercial off-the-shelf fpga based software defined radio systems. 2018

International Conference on Communications (COMM), p. 465–470, 2018.

MUSA, S.; ABDULLAH, R. S. A. R.; SALI, A.; ISMAIL, A.; RASHID, N. E.

Micro-doppler signature for drone detection using fsr: a theoretical and experimental validation. The Journal of Engineering, v. 21, p. 7918–7923, 2019.

MYDEFENCE. Fixed Installation. 2023. Disponível em: <https://mydefence.dk/fixed-installation/>. Acesso em: 22 out. 2023.

NASSI, B.; BITTON, R.; MASUOKA, R.; SHABTAI, A.; ELOVICI, Y. Sok: Security

and privacy in the age of commercial drones. Software and Information Systems Engineering, Ben-Gurion University of the Negev, 2019.

NETTLEFOLD, J. C-UAS Systems: A Year in Perspective. 2023. Disponível em:

<https://battle-updates.com/c-uas-systems-a-year-in-perspective-by-julian-nettlefold/>. Acesso em: 29 out. 2023.

NEWS ANI. Houthi says it targeted Saudi Arabia's Abha airport with drone attack. 2019. Disponível em: https://www.business-standard.com/article/news-ani/houthi-says-it-targete d-saudi-arabia-s-abha-airport-with-drone-attack-119072900175_1.html. Acesso em: 25 out. 2023.

OACI. Avaliac¸˜ao do ADS-B e Multilaterac¸˜ao para Apoio aos Servi¸cos de Tráfego Aéreo e Diretrizes para Implementac¸˜ao (Cir 326). Montréal, 2012.

OXFORD, V. S. Director, US Defense Threat Reduction Agency. Mar¸co 2019.

PARK, J.; AHN, J.; BAEK, W. Development of servo actuator for eo/ir photography system. In: Proc. Korean Soc. Precis. Eng. Conf. Seoul, South Korea: Korean Society for Precision Engineering, 2012.

PARK, J.-H.; JEONG, Y.-J.; LEE, G.-E.; OH, J.-T.; YANG, J.-R. 915-mhz continuous-wave doppler radar sensor for detection of vital signs. Electronics, v. 8, n. 5, 2019.

PARK, S.; KIM, H. T.; LEE, S.; JOO, H.; KIM, H. Survey on anti-drone systems: Components, designs, and challenges. IEEE Access, v. 9, p. 42635–42659, 2021.

RODRIGUES, C. V. C. ADS-B- automatic dependent surveillance broadcast: estudo do impacto em Portugal. 2010. 83f. Dissertac˜ao (Mestrado em Engenharia Aeron´autica) - Universidade da Beira Interior, Covilha.

SAC/MINFRA; ITA. Manual de Projetos Aeroportu´arios. Bras´ılia, 2021. v. 1.

SOUZA, M.; HENKES, J. A. O uso de drones pela pol´ıcia militar de santa catarina: Uma abordagem sobre as vantagens para a institui¸c˜ao e as limita¸c˜oes dentro do espaço aéreo próximo a aeroportos. Revista Brasileira De Aviação Civil & Ciências Aeronáuticas, v. 1, n. 3, p. 245–286, 2023.

SPELTA, B. V.-B. Possibilidades de detecção e neutraliza¸c˜ao de drones pela artilharia antiaérea do Exército Brasileiro: uma proposta de emprego em ambiente urbano.2019. Trabalho de Conclusão de Curso (Especialidade em Operações Militares de Defesa Antiaérea e Defesa do Litoral) - Escola de Artilharia de Costa e Antiaérea.

STEVENS, M.; ATKINS, E. Geofencing in Immediate Reaches Airspace for

Unmanned Aircraft System Traffic Management. Anais da AIAA Information Systems-AIAA Infotech Aerospace. 2018.

STURDIVANT, R. L.; CHONG, E. K. P. Systems engineering baseline concept of a multispectral drone detection solution for airports. IEEE Access, v. 5, p. 7123–7138, 2017.

THE LOCAL. 143 Flights Cancelled at Frankfurt Airport Due to Drone Sighting. 2019. Disponível em: <https://www.thelocal.de/20190509/disruption-after-frankfurt-airport- halts-flights-due-to-drone-sighting>. Acesso em: 15 out. 2023.

UAVIONIX. Ping2020. 2023. Disponível em: <https://uavionix.com/products/ping2020/>. Acesso em: 20 out. 2023.

UNLU, E.; ZENOU, E.; RIVIERE, N.; DUPOUY, P.-E. Deep learning-based strategies for the detection and tracking of drones using several câmeras. IPSJ Transactions on Computer Vision and Applications, v. 11, n. 7, 2019.

VISMARI, L. F. Vigilˆancia dependente autom´atica no controle de tráfego aéreo: Avaliac¸˜ao de risco baseada e modelagem em redes de petri fluidas e estoc´asticas. 2007. 272f. Disserta¸cao (Mestrado em Engenharia) - Escola Politécnica da Universidade de Sa˜o Paulo, Sa˜o Paulo.

WHITTLE. The Man Who Invented the Predator. 2013. Disponível em:

<https://www.airspacemag.com/flight-today/the-man-who-invented-the-predator- 3970502/>. Acesso em: 10 jul. 2023.

WILKINSON, G. Digital terrestrial tracking: The future of surveillance. 2014.

ZMYS-lOWSKI, D.; SKOKOWSKI, P.; KELNER, J. Anti-drone sensors, effectors, and systems – a concise overview. TransNav the International Journal on Marine Navigation and Safety of Sea Transportation, v. 17, p. 455–461, 2023.

LUKASIEWICZ, J.; TWARDOWSKA, A. K. Proposed method for building an

anti-drone system for the protection of facilities important for state security. Security and Defence Quarterly, v. 39, n. 3, p. 88–107, 2022.