INSTITUTO TECNOLÓGICO DE AERONÁUTICA

Matheus Gondim Peixoto

PROSPECÇÃO DE TECNOLOGIAS DE IDENTIFICAÇÃO E MONITORAMENTO DE DRONES EM ESPAÇO AÉREO CONTROLADO

Trabalho de Graduação
2023

Curso de Engenharia Civil Aeronáutica

CDU 629.7.072

Matheus Gondim Peixoto

PROSPECÇÃO DE TECNOLOGIAS DE IDENTIFICAÇÃO E MONITORAMENTO DE DRONES EM ESPAÇO AÉREO CONTROLADO

Orientador

Prof. Dr. Mauro Caetano de Souza (ITA)

Coorientador

Maj. Esp. CTA. Cristian da Silveira Smidt (ICEA)

ENGENHARIA CIVIL AERONÁUTICA

São José dos Campos
Instituto Tecnológico de Aeronáutica

2023

Dados Internacionais de Catalogação-na-Publicação (CIP)
Divisão de Informação e Documentação

Peixoto, Matheus Gondim
Prospecção de tecnologias de identificação e monitoramento de drones em espaço aéreo controlado / Matheus Gondim Peixoto.
São José dos Campos, 2023.
60f.

Trabalho de Graduação – Curso de Engenharia Civil Aeronáutica– Instituto Tecnológico de Aeronáutica, 2023. Orientador: Prof. Dr. Mauro Caetano de Souza. Coorientador: Maj. Esp. CTA. Cristian da Silveira Smidt.

1. Aeronaves não-tripulada. 2. Aeroportos. 3. Segurança de aeronaves. 4. Espaço aéreo. 5. Segurança de voo. 6. Monitoramento. 7. Aeronaves teleguiadas. 8. Engenharia aeronáutica. I. Instituto Tecnológico de Aeronáutica. II. Título.

REFERÊNCIA BIBLIOGRÁFICA

PEIXOTO, Matheus Gondim. **Prospecção de tecnologias de identificação e monitoramento de drones em espaço aéreo controlado**. 2023. 60f. Trabalho de Conclusão de Curso (Graduação) – Instituto Tecnológico de Aeronáutica, São José dos Campos.

CESSÃO DE DIREITOS

NOME DO AUTOR: Matheus Gondim Peixoto
TITULO DO TRABALHO: Prospecção de tecnologias de identificação e monitoramento de drones em espaço aéreo controlado.
TIPO DO TRABALHO/ANO: Trabalho de Conclusão de Curso (Graduação) / 2023

Matheus Gondim Peixoto

Matheus Gondim Peixoto
Rua H8B, Ap. 212
12.228-461 – São José dos Campos–SP

PROSPECÇÃO DE TECNOLOGIAS DE IDENTIFICAÇÃO E MONITORAMENTO DE DRONES EM ESPAÇO AÉREO CONTROLADO

Essa publicação foi aceita como Relatório Final de Trabalho de Graduação

Matheus Gondim Peixoto

Matheus Gondim Peixoto

Autor

Mauro Caetano de Souza

Prof. Dr. Mauro Caetano de Souza (ITA)

Orientador

Maj. Esp. CTA. Cristian da Silveira Smidt (ICEA)

Coorientador

Evandro José da Silva

Prof. Dr. Evandro José da Silva
Coordenador do Curso de Engenharia Civil Aeronáutica

São José dos Campos, 6 de Novembro de 2023.

Dedico este trabalho à minha mãe, Maria do Rosário, por ter sempre acreditado em mim e me dado os melhores exemplos.

Agradecimentos

Inicialmente agradeço à minha mãe, Maria do Rosário, ao meu pai, Hélio, e à minha irmã, Isadora, por todo suporte e por todo sacrifício que realizaram para que um dia este sonho fosse real. Agradeço em especial à minha mãe que sempre me trouxe para perto do mundo acadêmico, que nunca mediu esforços para que eu pudesse ter uma educação de qualidade, acreditou em mim e comprou meu sonho de fazer ITA quando eu mesmo tinha dúvidas.

Sou grato ao meu pai, Hélio, pelos incentivos e pelo acompanhamento durante toda a minha jornada acadêmica, agradeço à minha irmã, Isadora, por ter me auxiliado com conselhos, mensagens e com todo suporte possível; e à minha vó, Francisca, que cuidou de mim durante parte da minha infância e sempre me agraciou com seu amor e carinho.

Agradeço aos professores que tive em minha formação, em especial ao professor Frederico Torres, do Colégio Millenium Classe, que colocou muita confiança em mim e me fez acreditar que o impossível era um pouco mais possível. Agradeço ao meu conselheiro, Samuel, que além de um excelente professor se tornou um amigo com quem eu pude contar nos momentos mais desafiadores. Agradeço fortemente ao meu orientador, Professor Mauro Caetano, por todo o direcionamento e disponibilidade oferecidos durante a realização deste trabalho. Sou grato ao Maj. Esp. CTA Cristian da Silveira Smidt por coorientar este trabalho e por todo suporte fornecido.

Por fim, agradeço aos meus amigos e às pessoas que conheci durante esta jornada longa, vocês tornaram meus dias mais felizes e contribuíram tanto na minha formação quanto na minha vida.

Resumo

Este trabalho de Conclusão de curso é direcionado para análise de 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, o trabalho realiza uma revisão bibliográfica sobre métodos de detecção de drones, apresentando e comparando técnicas relevantes encontradas na literatura recente. Em paralelo é feito o estudo de soluções anti-drones disponíveis no mercado, reunindo as principais características dessas tecnologias. São apresentadas definições sobre os veículos aéreos não tripulados, características e limitações do espaço aéreo brasileiro e realizou-se o levantamento das regulamentações relevantes para voos de drones de pequeno porte. A comparação entre os métodos 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 do modelo proposto e manter a integridade do espaço aéreo brasileiro.

Abstract

This Project is directed towards the analysis of drone detection methods in controlled airspace, more specifically for use in the airport context. The application of the methods was targeted at the detection of small drones, due to the growing popularization of these devices that are becoming increasingly accessible. The study identifies three types of possible attacks carried out by malicious agents, which can affect airport operations and the safety of flights.

With the intention of proposing solutions to these threats, the work carries out a bibliographic review of drone detection methods, presenting and comparing relevant techniques found in recent literature. In parallel, a study of some anti-drone solutions available on the market is carried out, gathering the main characteristics of these technologies. Definitions of unmanned aerial vehicles, characteristics and limitations of Brazilian airspace are presented, and a survey of relevant regulations for flights of small drones was conducted. The comparison between detection methods allowed for a deep understanding for the proposition of solutions aimed at the proposed drone attacks.

The results indicate that the integration of various methods is the best response to drone attacks on airports, promoting a safer airspace. It is recommended that each solution be customized according to the specific characteristics of the airport in question, to ensure the effectiveness of the proposed model and to maintain the integrity of Brazilian airspace.

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

1.1 Objetivo

Este trabalho de graduação tem o objetivo de prospectar tecnologias para identificação e monitoramento de drones em espaço aéreo controlado no contexto militar do DECEA (Departamento de controle do Espaço Aéreo). Neste estudo foram caracterizados e analisados trabalhos científicos realizados sobre tecnologias para a identificação e monitoramento de drones em espaço aéreo controlado, sem ignorar as especificidades e necessidades militares do ambiente. Os modelos propostos na literatura (sistemas de radar, sensor ótico, sistema de monitoramento por satélite, sensor térmico e scanner RF) para identificação e rastreamento dos drones foram comparados e operacionalmente avaliados em relação a suas possíveis eficiências na identificação de aeronaves remotamente controladas, os drones. Foram destacadas as vantagens, limitações, possíveis aplicações das tecnologias disponíveis e potenciais contribuições para a gestão segura de drones em espaço aéreo controlado.

1.2 Motivação

Com o desenvolvimento das tecnologias pilotadas remotamente, surgem preocupações a respeito da necessidade de se desenvolverem métodos eficientes de detecção e monitoramento aéreo que identifiquem aeronaves de diversos modelos e tamanhos distintos. 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 com mais eficiência e economia, até a entrega de equipamentos e insumos em regiões de difícil acesso, especialmente em situações de desastres naturais (SOUZA; HENKES, 2023).

Essas tecnologias têm aplicações que ultrapassam o âmbito militar. São empregadas em diversas áreas, como monitoramento de canteiros de obras, fotografia aérea e levantamentos topográficos (MOSLY, 2017). Na agricultura de precisão, por exemplo, são usadas para coletar dados e monitorar a saúde das plantas em propriedades rurais (JÚNIOR;

NUÑEZ, 2023).

O presente trabalho visa esclarecer e contextualizar o uso deste tipo de tecnologia durante o passado, como também objetiva apresentar conceitos fundamentais associados a esse tipo de dispositivo. Além disso, pretende-se detalhar as regulamentações aeronáuticas que regem a utilização destes equipamentos e o uso do Espaço Aéreo Brasileiro. Espera-se que o trabalho em questão consiga contribuir na otimização do controle do espaço aéreo a partir da identificação desses tipos de aeronaves. Deseja-se que este texto consiga motivar o estudo e a elaboração de projetos envolvendo o desenvolvimento de novas práticas e tecnologias que permeiam as operações com aeronaves remotamente pilotadas.

1.3 Contexto Histórico

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 foram cada vez mais desenvolvidas e passaram a fazer parte de projetos militares como o projeto Aquila desenvolvido pela Força Aérea Americana. Apesar disso, apenas com o engenheiro aeroespacial Abraham E. Karem que estas tecnologias se aproximaram do padrão conhecido atualmente (WHITTLE, 2013). Os drones deixaram de ser utilizados exclusivamente em contextos militares e passaram a integrar setores comerciais da sociedade.

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. Com esse fenômeno em alta cada vez mais, demanda-se por soluções eficazes para a identificação e monitoramento dos drones quando estão em voo. A presença destes em áreas restritas, como aeroportos e instalações militares traz riscos operacionais e de segurança que precisam ser abordados.

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 Nicolás Maduro em Caracas, Venezuela. Drones carregados com explosivos foram usados para provocarem explosões que causaram pânico e feriram cerca de sete pessoas (BBC NEWS, 2018).

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 metros de diâmetro na parte sul da área do aeroporto (THE LOCAL, 2019).

Esses riscos e ataques remontam a necessidade do monitoramento aéreo para que seja garantida a segurança das operações e previnam-se incidentes. O monitoramento depende então da prospecção de tecnologias que identifiquem drones em espaços aéreos controlados. Este trabalho tem como objetivo explorar e analisar as tecnologias disponíveis, como também suas limitações e potencialidades.

1.4 Drone escolhido como referência do estudo

Neste estudo, focado na análise do espaço aéreo brasileiro, é essencial que o drone selecionado para referência possua características específicas. Ressalta-se que este trabalho priorizou a escolha de um equipamento que possua viabilidade econômica e facilidade de operação. O modelo escolhido foi DJI Mini 2, este incorpora avançadas inovações tecnológicas a um design compacto e economicamente viável, portanto é adotado por uma variedade de usuários, desde entusiastas a profissionais especializados.

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. Estas técnicas serão detalhadas na sequência deste capítulo.

2.1 Identificação com uso de tecnologia 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. É importante que o monitoramento desse tipo de atividade aérea evite 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 1.

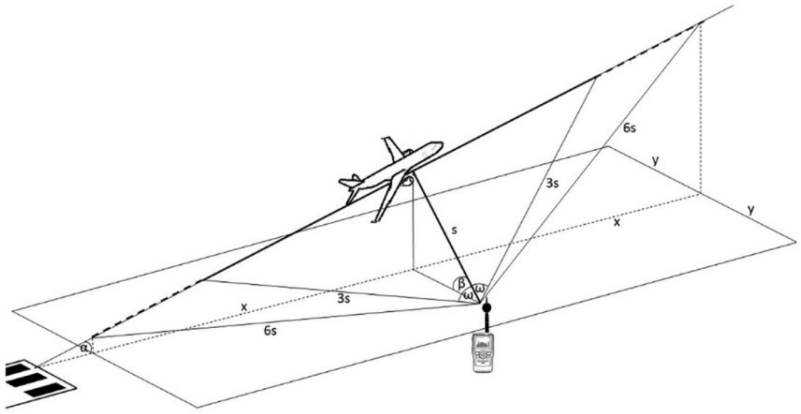

FIGURA 1 – Distâncias para monitoramento de ruídos.
Fonte: (GILADI, 2020)

As conclusões sobre o método foram de que é bastante eficaz para identificar eventos sonoros e outras informações de aeronaves por meio do uso da tecnologia ADS-B, mesmo quando os ambientes possuem diversos obstáculos e ruídos de fundo. Constatou-se que por o 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 propagração, 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.

A seguir é apresentado outro método de detecção que envolve o uso de radar.

2.2 Identificação com uso de 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 alterações 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 - Seção Transversal de Radar) 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.

$$P_r = \frac{P_t * G_t * G_r * \lambda^2 * RCS * A}{4 * \pi * R^4} \tag{1}$$

Onde: P_r é a potência do sinal recebido pelo radar, P_t é a potência do sinal transmitido pelo radar, G_t é o ganho da antena transmissora, G_r é o ganho da antena receptora, λ é o comprimento de onda do sinal transmitido, RCS é a seção transversal de radar do objeto, A é a área efetiva do alvo e R é a distância entre o radar e o objeto. No contexto do artigo desenvolvido por Kim *et al.* (2018), essa equação é utilizada para determinar o RCS máximo detectável de drones utilizando um radar de pulso chirp. O RCS máximo detectável é um parâmetro importante para definir a capacidade do radar em detectar e rastrear drones com eficiência. Com o uso da Equação 1 podem-se realizar cálculos que determinam o RCS máximo detectável para diferentes modelos de drones, isso com base nas particularidades do radar utilizado e nas propriedades dos drones em relação à reflexão do sinal de radar pulso-chirp. 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 possuí limitações quanto a 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 têm 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 (ŁUKASIEWICZ; 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.

2.3 Estratégias baseadas em aprendizado profundo para a detecção e rastreamento de drones utilizando câmeras

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 é 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 2 ilustra a comparação de detecções produzidas por diferentes arquiteturas de algoritmos.

FIGURA 2 – Detecções produzidas por diferentes arquiteturas.
Fonte: (UNLU *et al.*, 2019)

As detecções pela arquitetura YOLO são representadas pela coloração verde e as demais 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).

Unlu *et al.* (2019) propõem um sistema que emprega uma câmera estática 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, J.; AHN, J.; BAEK, W., 2012).

2.4 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 à 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 com a utilização 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). Essas diferenças contêm 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 3.

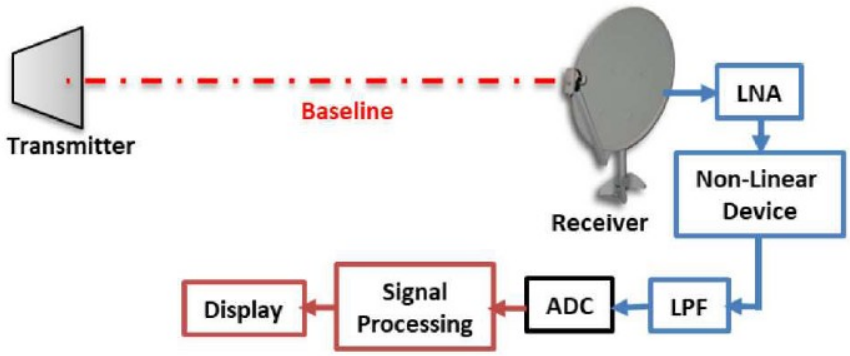

FIGURA 3 – Geometria de radar de dispersão direta
Fonte: (MUSA *et al.*, 2019)

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 mo-

nitor.

A Equação 2 representa a modulação de fase gerada como resultado de um micro-movimento circunferencial de cada lâmina.

$$\phi_{md}(t) = -\frac{2\pi}{\lambda}\frac{Lb}{2}cos(\frac{\beta}{2})cos(\delta)cos(\Omega * t + \theta) \tag{2}$$

onde λ é o comprimento de onda, Lb é o comprimento da lâmina, β é o ângulo bistático, δ é o ângulo de incidência, Ω é a velocidade angular das lâminas, t representa o intante de tempo e θ é o ângulo inicial. O ângulo bistático 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 4 (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

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

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 e $A_{rx(n)}$ representa a amplitude do sinal recebido para cada lâmina e φ_{md} 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.

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

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 é exposta na equação 5. 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 metodo possuí a capacidade de resolução adequada para maioria dos casos de detecção por conta da alta sensibilidade do radar para identificar alterações 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.

2.5 Identificação com uso de scanners de RF

Os drones operados por controladores tendem a trocar mensagens específicas com uso de sinais RF de Radiofrequência, 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 (ZMYSŁOWSKI *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).

2.6 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 (ANDRAŠI *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 Andraši *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.

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

2.7 Resumo dos principais estudos identificados

A Tabela 1 apresenta o resumo das principais características dos métodos apresentados.

ADS-B	**Autor:** Giladi (2020)
	Parâmetros: Frequência ADS-B; Pacotes ADS-B; Alcance máximo de detecção
	Limitações: Não universalidade; Custo; Complexidade; Interferências
	Vantagens: Precisão elevada; Ampla utilização na aviação tradicional; Grande amplitude de cobertura
Radar de pulso-chirp	**Autor:** Kim et al. (2018)
	Parâmetros: Frequência de operação; Alcance máximo do radar; Sensibilidade do radar
	Limitações: Obstáculos físicos; Interferências; Menor precisão
	Vantagens: Alcance longo; Eficácia em condições climáticas adversas
Aprendizado profundo	**Autor:** Dupouy et al. (2019)
	Parâmetros: Resolução das câmeras; Número de câmeras; Algoritmos empregados; Taxa de amostragem das imagens
	Limitações: Dependência de boas condições de iluminação; Alcance limitado
	Vantagens: Detecção precisa; Maior capacidade adaptativa
Micro-Doppler	**Autor:** Musa et al. (2019)
	Parâmetros: Banda de Frequência; Duração da assinatura
	Limitações: Limitações das condições atmosféricas; Problemas na presença de ruídos.
	Vantagens: Alta sensibilidade e Precisão
Scanner RF	**Autor:** Al-Sa'd et al. (2019)
	Parâmetros: Frequência de sinais RF; Troca de mensagens específicas; Localizadores de direção
	Limitações: Não identifica drones com navegação autônoma; Problemas com protocolos de controle desconhecidos
	Vantagens: Eficiente em detectar e identificar drones; Capaz de trabalhar em configuração de triangulação; Alcance longo
Câmeras de infravermelho	**Autor:** Andraši et al. (2017)
	Parâmetros: Diferenciação térmica em mK; Emissão infravermelha
	Limitações: Dificuldade em diferenciar drones de pássaros; Não eficaz para longas distâncias
	Vantagens: Eficiente em ambientes noturnos; Capaz de identificar drones de pequeno porte

TABELA 1 – Técnicas de detecção e rastreamento de drones.
Fonte: (autoria própria, 2023)

3 Aeronaves não tripuladas

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, sigla de Remotely Piloted Aircraft System (DECEA, 2018). O seguinte trabalho é destinado ao estudo dos drones, sendo assim serão apresentadas caraterísticas usuais dessa tecnologia. Os tipos mais comuns de drones são: drones de asa fixa, drones de asas rotativas, dirigíveis e or-nitópteros (DECEA, 2023). A Figura 4 ilustra um VANT de asas rotativas e a Figura 5 ilustra um VANT de asas fixas.

FIGURA 4 – VANT de asas rotativas.
Fonte: (EISENBEISS, 2004)

FIGURA 5 – VANT de asas fixas.
Fonte: (MOTOTOLEA; STOLK, 2018)

A popularidade dos drones tem aumentado devido às suas versatilidades, facilidades de operação e ampla gama de aplicações em diversos setores (ZMYSŁOWSKI *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. As inovações permitem que cada vez mais estes sejam equipados com equipamentos que fornecem informações úteis e colaboram para as funções de vigilância e monitoramento.

O aumento no uso de RPAs faz com que se torne necessária a criação de regulamentos e órgãos capazes de fiscalizar este tipo de tecnologia, esta situação acabou por motivar a Agência 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 sofrem nenhum tipo de restrição (ANAC, 2017).

A falta de restrições na compra e venda de drones ou outras aeronaves de aeromodelismo é um tema polêmico que promove discussões e debates sobre quais devem ser os limites nas potências e nos tamanhos dos drones que são comercializados. O DECEA, por meio do documento Circular de Informação Aeronáutica - AIC nº17, determina orientações de uso dos drones exclusivos para fins recreativos. A ANAC Através da Portaria nº 207/DAC (1999), estabelece as diretrizes operacionais para os aeromodelos, com as seguintes regras: a utilização dos aeromodelos deve ocorrer em locais distantes de áreas densamente povoadas; é proibido operar em áreas de aproximação e pouso de aeronaves em aeródromos; é necessário evitar a utilização próxima a locais sensíveis ao ruído, como hospitais e escolas e a operação desses equipamentos acima de 400 pés acima do solo só é permitida com autorização da autoridade aeronáutica.

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 (ZMYSłOWSKI *et al.*, 2023). Algumas pessoas com cargos estratégicos se pronunciaram, como o Oxford (2019), Diretor da Agência de Redução de Ameaças de Defesa dos EUA, que destacou o desafio relacionado aos drones como contínuo e adaptativo, alterando-se a cada trimestre ou semestre. Ele salientou que a capacidade dos drones de se adaptarem e serem utilizados de diversas maneiras torna impossível confiar em uma única técnica para contrariá-los. Nesse contexto, observa-se a necessidade do desenvolvimento de sistemas anti-drones. Essa necessidade é intensificada pelo crescente número de incidentes, invasões de áreas restritas e ataques direcionados através destes dispositivos, o que incentiva a inovação em equipamentos de detecção cada vez mais avançados (ZMYSłOWSKI *et al.*, 2023).

A crescente necessidade de sistemas de segurança para detectar drones levou a maioria dos fornecedores a adotar sistemas híbridos (PARK *et al.*, 2021). Estes sistemas, baseados na fusão de tecnologias de sensores e controle de hardware, têm sido predominantes nas instalações de aeroportos, prisões e em eventos temporários (PARK *et al.*, 2021). No entanto, apesar do avanço em sistemas de detecção, muitos desses mecanismos ainda carecem de integração plena com etapas de identificação e neutralização de ameaças.

Zmysłowski *et al.* (2023) determina 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 eficácia 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 quilômetro, 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 ter métodos de detecção variados, especialmente para identificar drones que não emitem sinais de RF, como os usados em atos terroristas, que podem usar tecnologias para se ocultarem.

4 Espaço aéreo controlado

O espaço aéreo controlado entende-se como uma área de grande interesse comercial e militar, sendo um frequente cenário de invasões territoriais, transporte de pessoas, tráficos e usos comerciais. Trata-se de uma área no céu que além de supervisionada e controlada está sujeita a regulamentações impostas por órgãos aeronáuticos. Esse espaço tem relações com tráfego aéreo e consequentemente é organizado por meio de restrições e monitoramentos.

Já os elementos que compõem o espaço aéreo são identificados pela integração de aeroportos, áreas de tráfego de aeronaves e rotas aéreas. O autor Vismari (2007) destaca que a capacidade do sistema de tráfego aéreo mundial encontra-se limitada devido à dificuldade em reduzir a separação entre aeronaves sem comprometer os padrões de segurança estabelecidos. Quando esta separação é diminuída, resulta em aeronaves voando mais próximas, tanto em termos horizontais quanto verticais, o que intensificam os desafios para manter a segurança do tráfego aéreo.

Devido à capacidade de atualização em tempo real do posicionamento das aeronaves em relação aos radares convencionais, os controladores de tráfego aéreo podem reduzir com mais segurança o espaçamento entre as aeronaves. O controlador pode elaborar um mapa situacional do espaço aéreo controlado e atuar com antecedência sobre as aeronaves de forma a mantê-las separadas com distâncias seguras e aderindo às trajetórias planejadas (VISMARI, 2007). Essa otimização dos espaços ocupados pelas aeronaves possibilita um maior número de operações simultâneas que colaboram para um uso eficiente do espaço aéreo no qual se evitam atrasos e promovem reduções nos tempos de voo.

Neste panorama, Rodrigues (2010) enfatiza que, diante do crescente volume de tráfego aéreo, surgiu uma necessidade imperativa de prevenir colisões. A conformidade com os padrões de separação estabelecidos pelas autoridades aeronáuticas garante que as aeronaves mantenham uma distância segura tanto em relação ao solo quanto a outras aeronaves.

O Brasil detém a soberania sobre o espaço aéreo que está localizado acima de seu território e também sobre o espaço aéreo localizado sobre o seu mar territorial, segundo o Código Brasileiro de Aeronáutica (CBA) essa extensão é definida pelos limites do mar territorial brasileiro até o meridiano 10°W. A soberania mencionada traz a responsabilidade

de se fornecerem serviços de Tráfego aéreo em toda extensão do espaço aéreo Brasileiro, sendo necessário oferecer serviços de comunicação, vigilância e controle para que as operações realizadas sejam seguras e eficientes. A Figura 6 ilustra a extensão do espaço aéreo do Brasil.

FIGURA 6 – Espaço Aéreo Brasileiro.
Fonte: (DECEA, 2023)

5 Soluções de detecção disponíveis no mercado

Como levantado anteriormente, a necessidade de monitorar e controlar o tráfego de drones no espaço aéreo tornou-se uma demanda de urgência e pode-se observar o mercado avançando no sentido de diminuírem os desafios quanto ao desenvolvimento de soluções para detecção de drones. As soluções propostas se adaptam a diferentes cenários e necessidades e podem atuar de maneiras reativas ou preventivas buscando a integração otimizada das tecnologias de detecção disponíveis.

5.1 Dedrone

A empresa Dedrone está inovando 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 Dedrone 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 (ZMYSŁOWSKI *et al.*, 2023). A Figura 7 apresenta o Kit Base de resposta ágil CsUAS fornecido pela empresa Dedrone.

FIGURA 7 – 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).

5.2 MyDefence

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-incidente detalhadas (MYDEFENCE, 2023). Com foco no segmento governamental 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 8 e 9 apresentam os componentes da solução de instalação fixa proposta.

FIGURA 8 – Detector de RF WATCHDOG 202 para proteção de perímetro.
Fonte: (MYDEFENCE, 2023)

FIGURA 9 – 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 às crescentes necessidades de segurança.

5.3 Hensoldt

O XPeller é uma tecnologia capaz de detectar drones desenvolvida pela empresa alemã Hensoldt. Ele é indicado para a defesa de áreas 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 à 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 à base ou a pousar. 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).

A Figura 10 apresenta os sensores e radares que compõem a tecnologia XPeller.

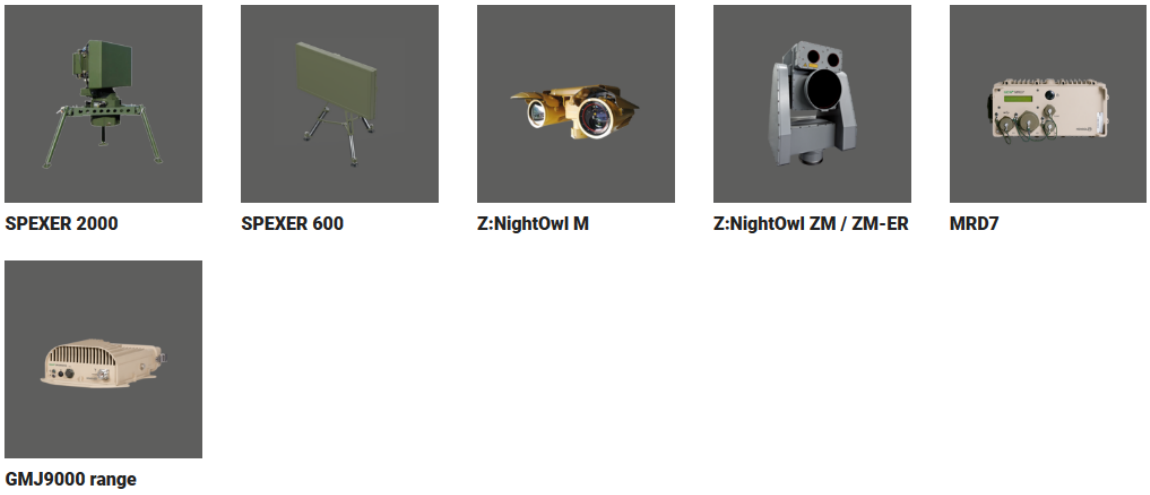

FIGURA 10 – Radar de Vigilância para veículos não tripulados e proteção de ativos críticos.
Fonte: (HENSOLDT, 2023)

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.

5.4 Geofencing

Geofencing é um recurso tecnológico que estabelece limites virtuais para evitar que drones entrem em espaços proibidos, como os aeroportos, tornando-se essencial para a segurança do espaço aéreo (STEVENS; ATKINS, 2018). Existem 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 áreas não autorizadas (AISC, 2015).

Os fabricantes de drones frequentemente atualizam os sistemas de geofencing para realizar modificações em zonas restritas, incluindo novas áreas ou alterações 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.

5.5 Comparação entre as soluções de detecção de drones disponíveis no mercado

Diversas empresas têm se destacado na proposta de oferecer tecnologias para enfrentar a questão de detecção de drones em aeroportos. Ao analisar as soluções disponíveis no mercado, é possível traçar um panorama de como a indústria está respondendo a essa necessidade e identificar as principais características e benefícios de cada proposta. Neste contexto, a Tabela 2 apresenta uma comparação entre as principais tecnologias oferecidas para detecção de drones em aeroportos.

Empresa	**Diferenciais**	**Aplicação no Aeroporto**
Dedrone	Alta precisão, eliminação de falsos positivos, líder de mercado e experiência com operações em aeroportos americanos.	Pistas, Torres de controle, Terminais
MyDefence	Maior resistência à intemperes, economia de tamanho, pouco peso, menor consumo de energia, discreto e orçamento maleável.	Carga/descarga, Pátio
Hensoldt	Adaptabilidade móvel e fixa, fácil integração, escalável, baixa taxa de falsos positivos e abordagem não destrutiva.	Pistas, Hangares, Periferia do aeropórto

TABELA 2 – Comparação entre sistemas anti-drones e suas aplicações em aeroportos.
Fonte: (autoria própria, 2023)

6 Metodologia

6.1 Tema

O tema alvo do presente trabalho foi delimitado ao estudo e a comparação das tecnologias capazes de detectarem drones em espaço aéreo controlado, especialmente nas proximidades de áreas sensíveis de aeroportos. O escopo priorizou o estudo de tecnologias para detecção de drones de pequeno porte (carga útil inferior a 250g) em potenciais cenários de ataques apresentados nas seções seguintes.

6.2 Formulação do Problema

Com o crescimento do uso de drones, principalmente os de pequeno porte que se tornam cada vez mais acessíveis, modificam-se as maneiras de garantir a segurança de áreas sensíveis como aeroportos. Este tipo de drone, por conta do seu tamanho e características pode gerar desafios para os sistemas tradicionais de detecção utilizados nos aeroportos. Quais são as tecnologias mais eficazes na detecção de drones de pequeno porte em espaços aéreos controlados, especialmente nas proximidades de áreas sensíveis de aeroportos, e como elas se comparam entre si em diferentes cenários de ameaça?

6.3 Natureza do trabalho

A metodologia deste estudo sobre tecnologias de detecção de drones em espaços aéreos controlados é caracterizada como uma pesquisa bibliográfica. Esta leitura foi feita por meio de uma busca analítica em fontes primárias e secundárias, onde buscou-se definir, entender e explicar o problema em questão e possíveis soluções. Foram utilizados conhecimentos extraídos de teorias publicadas em livros, artigos, manuais, jornais eletrônicos, relatórios e outros.

6.4 Drone referência para estudo de caso

Este estudo utiliza o drone DJI mini 2 como objeto de análise, visto que possui imensa popularidade devido a 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, conforme indicado pelo Mercado Livre (2023), 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 11 apresenta o modelo de drone escolhido.

FIGURA 11 – Modelo de drone DJI Mini 2.
Fonte: (DJI, 2023)

As principais especificações do drone de referência seguem abaixo:

- 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
- Função 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 casa dos 3 mil reais 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.

6.5 Legislação Restritiva

Este trabalho se fundamenta com a análise da legislação pertinente ao uso de drones, com enfoque em modelos com Peso Máximo de Decolagem (PMD) inferiores à 250 g. Essa legislação estabelece critérios para a segurança e a responsabilização na utilização desses equipamentos no espaço aéreo, exercendo influência sobre as estratégias e procedimentos a serem discutidos.

Embora o Brasil possua uma legislação aeronáutica bem estabelecida, somente após 2017 é que se criou legislação específica para regular o uso dos Veículos Aéreos Não Tripulados (VANTs) no espaço aéreo nacional. Segundo a ICA 100-40 de 2023, a responsabilidade por legislar sobre os procedimentos de acesso ao Espaço Aéreo Brasileiro está atribuída ao Departamento de Controle do Espaço Aéreo (DECEA), o órgão central do Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB), enquanto os outros órgãos reguladores devem tratar das questões pertinentes às suas respectivas esferas de atuação.

A ICA 100-40 estabelece condições operacionais específicas para a operação de Veículos Aéreos Não Tripulados (VANTs), detalhadas a seguir:

> a) Para operações com Altura de Voo Solicitada de até 100 ft (aproximadamente 30 metros) e velocidade máxima de 30 Kt (aproximadamente 60 km/h):

- Deve-se manter uma distância mínima de 3550 metros das cabeceiras das pistas de aeródromos cadastrados, quando operando na Zona de Entorno de Aeródromo (ZAD);
- Deve-se manter uma distância mínima de 1740 metros de aeródromos cadastrados, quando operando no entorno destes;
- Deve-se manter uma distância mínima de 1740 metros de helipontos cadastrados.

b) Para operações com Altura de Voo Solicitada entre 100 ft e 200 ft (aproximadamente 30 a 60 metros) e velocidade máxima de 60 Kt (aproximadamente 120 km/h):

- Deve-se manter uma distância mínima de 4480 metros das cabeceiras das pistas de aeródromos cadastrados, quando operando na ZAD;
- Deve-se manter uma distância mínima de 2350 metros de aeródromos cadastrados, quando operando no entorno destes;
- Deve-se manter uma distância mínima de 2350 metros de helipontos cadastrados.

c) Para operações com Altura de Voo Solicitada entre 200 ft e 300 ft (aproximadamente 60 a 90 metros) e velocidade máxima de 60 Kt (aproximadamente 120 km/h):

- Deve-se manter uma distância mínima de 5400 metros das cabeceiras das pistas de aeródromos cadastrados, quando operando na ZAD;
- Deve-se manter uma distância mínima de 2960 metros de aeródromos cadastrados, quando operando no entorno destes;
- Deve-se manter uma distância mínima de 2960 metros de helipontos cadastrados.

d) Para operações com Altura de Voo Solicitada entre 300 ft e 400 ft (aproximadamente 90 a 120 metros) e velocidade máxima de 60 Kt (aproximadamente 120 km/h):

- Deve-se manter uma distância mínima de 6320 metros das cabeceiras das pistas de aeródromos cadastrados, quando operando na ZAD;
- Deve-se manter uma distância mínima de 3570 metros de aeródromos cadastrados, quando operando no entorno destes;
- Deve-se manter uma distância mínima de 3570 metros de helipontos cadastrados.

Essas diretrizes são cruciais para garantir a segurança no espaço aéreo, evitando interferências com o tráfego de aeronaves tripuladas e a operação de instalações aeroportuárias. Para operações que ocorram em condições meteorológicas visuais com Aeronaves Não Tripuladas que tenham um Peso Máximo de Decolagem de até 250 gramas e que sejam

realizadas abaixo de 200 pés de altura e fora de Zonas de Restrição de Voo (FRZ), não é necessário realizar solicitação de autorização através do Sistema de Solicitação de Acesso de Aeronaves Remotamente Pilotadas (SARPAS). No entanto, essas operações devem aderir às normas e procedimentos descritos nesta instrução regulamentar e também devem atender aos requisitos impostos por outras agências ou entidades reguladoras aplicáveis à atividade.

Adicionalmente, a ICA 100-40 destaca que, mesmo quando uma operação de aeronave não tripulada é autorizada, ela deve ser prontamente interrompida se houver qualquer indicação de aproximação de aeronaves tripuladas ou operações de Unidades Aéreas dos Órgãos de Segurança Pública, visando a segurança de todos os usuários do espaço aéreo.

6.6 Estudo dos métodos propostos para detecção de drones

A detecção eficiente de drones é uma questão de crescente relevância e ainda possuí diversas limitações que são exploradas neste estudo. É 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 há sistema proposto isoladamente que garanta segurança completa contra drones, diferentes técnicas devem ser implantadas simultaneamente no mesmo sistema. A Figura 12 expõe a popularidade das técnicas e abordagens utilizadas para detecção dos drones até o ano de 2015.

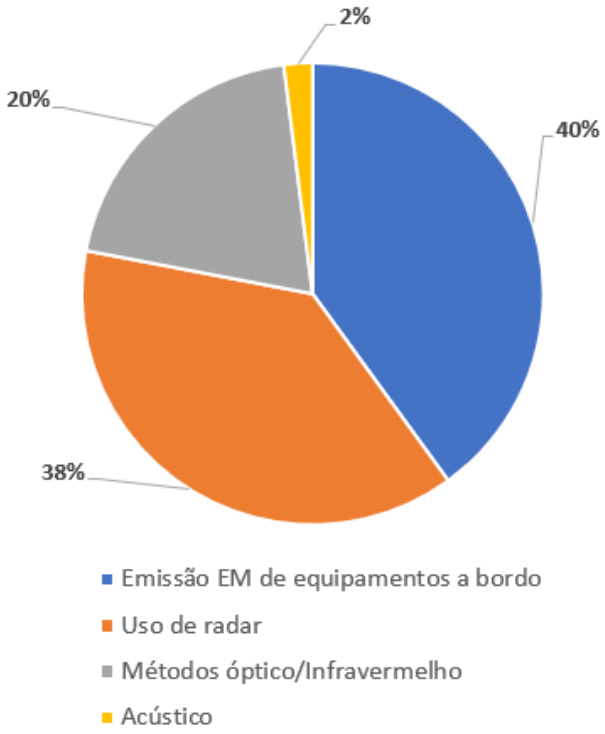

FIGURA 12 – Popularidade das técnicas e abordagens utilizadas para detecção e rastreamento de drones. Adaptado de: (BIRCH *et al.*, 2015)

A maior parte desta distribuição (40%) corresponde à detecção por emissões eletromagnéticas, que captam sinais emitidos pelos próprios drones. Em seguida, com (38%), vem o uso de radares que emitem ondas de rádio e interpretam os ecos retornados. Os métodos óptico e infravermelho, que juntos somam (20%), utilizam câmeras e sensores para detectar drones através de imagens ou calor. Por fim, com apenas (2%), a detecção acústica é a menos comum, identificando drones pelos sons que produzem.

6.7 Estudo das soluções de drones disponíveis no mercado

A popularização do uso de drones acelerou significativamente o desenvolvimento de tecnologias anti-drones. Devido à proliferação desses dispositivos e aos riscos associados, surgiu um vasto leque de soluções projetadas para garantir a segurança em locais críticos como aeroportos, estádios e outros pontos sensíveis. A dualidade dos drones como ferramentas de grandes utilidades e potenciais vetores de ameaças, exige uma abordagem que contemple tanto os benefícios quanto as vulnerabilidades que eles representam. Diante deste panorama, a metodologia empregada neste trabalho centra-se na avaliação comparativa de tecnologias anti-drones proeminentes do mercado, considerando sua eficácia em condições diversas e capacidade de resposta às ameaças. Priorizou-se uma análise múltipla, que levou em conta aspectos técnicos específicos, tais como precisão e a funcio-

nalidade diante de condições adversas. Ao integrar estes aspectos com o reconhecimento das necessidades de segurança aeroportuária, objetivou-se oferecer um panorama das opções disponíveis, fornecendo um guia para a seleção das tecnologias mais adequadas para cada cenário.

7 Resultados e discussões

7.1 Comparação entre os métodos de detecção de drones de pequeno porte

Os métodos de detecção de drones apresentados a seguir foram selecionados com foco nas características específicas do modelo de drones estudado. Atualmente, a tecnologia ADS-B, apesar de promissora para integração futura de diversos tipos de drones, ainda pode demorar para estar presente nas categorias de drones de pequeno porte. Portanto, a análise se concentra nos outros métodos que podem ser utilizados eficazmente no contexto atual. A tabela 3 ilustra os desempenhos dos métodos sobre estes fatores.

Método	**Benefícios**	**Limitações**
Radar	Detecções longas; Rastreia diversos tipos de drones; Distingue drones de aves; Independe das condições climáticas	Alcance depende do RCS; Custos altos 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

TABELA 3 – Comparação entre métodos de detecção de drones.
Fonte: (autoria própria, 2023)

A classificação dos métodos de detecção varia de acordo com fatores ambientais e funcionais, deve-se entender a funcionabilidade deles quanto a esses aspectos para entender a eficácia de cada tecnologia em variadas 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.

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

TABELA 4 – Efetividade dos sensores em diferentes condições.
Fonte: (autoria própria, 2023)

7.2 Caracterização das áreas de defesa em um aeroporto

Este estudo considera a estruturação básica de alvos possíveis para um aeroporto, sendo composta pelas seguintes áreas vitais de funcionamento operacional:

- Terminais de Passageiros: Área parte do aeroporto fora da área de pouso de aeronaves e importante interface entre os transportes terrestre e aéreo. Área de conforto e de atividades de triagem, espera e preparação de embarque e desembarque (SAC/MINFRA; ITA, 2021).
- Pistas do aeroporto: Elementos cruciais para decolagens e aterrissagens.
- Pátio de Aeronaves: Área destinada a facilitar a chegada, movimentação, estacionamento, manutenção, carregamento, embarque, desembarque e saídas de aeronaves (SAC/MINFRA; ITA, 2021).

- Torre de controle e Estações Prestadoras de Serviços de Telecomunicações e de Tráfego Aéreo (EPTA): Responsáveis pelo apoio a gestão do tráfego aéreo.
- Conexões externas: Pontos que ligam o aeroporto a outros meios de transporte (carros, metros, ônibus e outros).

Estes pontos são críticos para o aeroporto e podem sofrer ataques por drones, este estudo considera ataques ocasionados por drones pequenos (peso total menor que 250g). Os drones pequenos são mais difíceis de serem identificados por radares e sistemas de câmeras de modo geral e são capazes de realizarem as seguintes categorias de ataques:

- Ataque de drones aos sistemas de gestão de tráfego aéreo, ameaçando voos tripulados.
- Ataque de drones aos sistemas remotos que apoiam a gestão de tráfego aéreo.
- Ataque de drones aos sistemas de comunicação e informação dos aeroportos.

7.3 Caracterização dos ataques abordados no estudo

Neste estudo foram identificados 3 cenários de ataques possíveis por drones de pequeno porte em aeroportos, esses se concentram principalmente como ameaças à sistemas indiretos e de suporte e não colisões diretas com aeronaves. Esses ataques são mais representativos ao considerar que drones de pequeno porte não geram riscos em colisões contra aeronaves comerciais. Os ataques identificados representam ameaças emergentes e muitas vezes subestimadas, assim não há muita informação disponível de como podem ser neutralizados e seus potências danos. Portanto, a análise desses cenários indiretos pode ser utilizada para antecipar e preparar respostas eficazes contra essas novas formas de ameaças.

7.3.1 Ataque de drones aos sistemas de gestão tráfego aéreo, ameaçando voos tripulados.

O uso de transponder ADS-B para transmissão de informações de aeronaves para outras aeronaves e estações terrestres de vigilância pode ser explorado tanto por controladores 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.

7.3.2 Ataque de drones aos sistemas remotos que apoiam a gestão de 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 a 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 têm 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 a 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 13 ilustra a interceptação de sinais RF emitidos por sistemas remotos de suporte à gestão de tráfego aéreo.

FIGURA 13 – Drone interceptando e gerando interferência na transmissão de dados para aeroporto fictício.
Fonte: (autoria própria, 2023)

7.3.3 Ataque de drones aos sistemas de comunicação e informação dos aeroportos.

Outra forma de ataque possível para o modelo de drone analisado neste estudo seria um ataque direcionado à 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 e softwares embutidos.

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) mostra que 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, se infiltrando nas redes sem fio para interceptar e capturar dados.

Uma das técnicas utilizadas nesse ataque diz respeito ao uso de etiquetas RFID, ”Radio-Frequency Identification” (Identificação por Rádio Frequência), 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 à 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 seu ataque.

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

7.4 Soluções propostas para os ataques definidos

Os Aeroportos são caracterizados pelas distinções de características principais quanto ao tamanho, fluxo de tráfego, arquitetura, quantidade de pistas e outras. Cada um dos aeroportos deve dispor de forma peculiar seus sensores e mecanismos de defesa para que consiga obter a maior segurança e eficiência para as atividades desenvolvidas e para seus funcionários e clientes. 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. É importante destacar que, 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 a seguir medidas específicas para aumentar a segurança dos aeroportos contra drones mal-intencionados.

7.4.1 Ataque de drones aos sistemas de gestão de tráfego aéreo, ameaçando voos tripulados.

A integração de drones no espaço aéreo traz desafios para a segurança dos aeroportos devido à 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.

7.4.1.1 Solução com base no mercado de sistemas anti-drones.

O Kit Base da Dedrone, pode ser utilizado como forma de resposta ao ataque proposto, sendo disposto em áreas 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 áreas 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.

7.4.1.2 Solução com base nos métodos apresentados.

Para este tipo de situação, os radares seriam a opção primária de detecção de drones, por conta do alcance longo e capacidade de rastrear drones (diferenciando de aves). 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 utilizados como uma camada adicional de segurança posicionada próxima às pistas de decolagem e aterrisagem para identificar tentativas de interferência nos sinais ADS-B. Câmeras visuais e câmeras infravermelho poderiam ser utilizadas como forma de complementar a identificação e diferenciar alvos com protocolos desconhecidos.

7.4.2 Ataque de drones aos sistemas remotos que apoiam a gestão de tráfego aéreo.

Como foi apresentado anteriormente, a crescente integração de drones no espaço aéreo é acompanhada de ameaças específicas contra os sistemas de telecomunicações utilizados em aeroportos. 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 à 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 áreas 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.

7.4.3 Ataque de drones aos sistemas de comunicação e informação dos aeroportos.

As infraestruturas aeroportuárias precisam ser ágeis no rastreio de drones, especialmente quando estes realizam movimentos lentos ou permanecem estacionários sobre áreas 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 áreas de alto risco e de acesso público.

7.5 Discussões

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.

8 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. Foram apresentados métodos descritos em artigos científicos no capítulo 2 e soluções disponíveis no mercado no capítulo 5. Ao final desses capítulos compararam-se benefícios, limitações e particularidades de todos os métodos e tecnologias estudados.

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.

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 têm 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 desenvolvidas 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 diver-

sos 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. É fundamental que estes desenvolvam um plano 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.

Este estudo tem a proposta de contribuir para o campo acadêmico, especialmente no direcionamento da pesquisa relacionada à detecção de drones leves, acessíveis e com muitas funcionalidades. Inicialmente, pela análise dos métodos de detecção de drones presentes na literatura acadêmica e pela compilação da legislação aplicável a este tipo de drone. Esta última fornece uma contribuição normativa atualizada e relevante, indicando caminhos para estudos futuros que possam abordar os aspectos regulatórios de forma mais profunda. Para os pesquisadores, este estudo oferece uma base de métodos de detecção e soluções existentes, instigando e incentivando o desenvolvimento de novas tecnologias e estratégias de defesa para resolverem as limitações apresentadas.

Espera-se que o estudo contribua com o mapeamento de três possíveis ataques empregando o modelo de drone abordado e forneça uma perspectiva prática que poderá ser utilizada para aprimorar as estratégias de segurança e as operações de controle do tráfego aéreo. Essa identificação de ameaças pode ajudar na elaboração de respostas direcionais e efetivas. As propostas apresentadas, direcionadas aos drones de menor porte, buscam evidenciar a necessidade de adaptação às novas realidades do espaço aéreo, marcadas pelo aumento da acessibilidade destes dispositivos. Este enfoque pode ser útil para gestores de segurança que buscam atualizar suas políticas de segurança aérea.

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. Brasília, 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.

ANDRAŠI, P.; RADIŠIĆ, T.; MUŠTRA, M.; IVOŠEVIĆ, J. Night-time detection of UAVs using thermal infrared camera. **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.

BRASIL. Comando da Aeronáutica. Departamento do controle Aéreo. AIC nº 24, de 11 de junho de 2018. **Aeronaves remotamente pilotadas para uso exclusivo em operações dos órgãos de Segurança Pública, da Defesa Civil e de Fiscalização da Receita Federal**. Rio de Janeiro, RJ: DECEA, COMAER, 2017.

BRASIL. Comando da Aeronáutica. Departamento do controle Aéreo. ICA nº 100-40, de 6 de junho de 2023. **Sistema de aeronaves remotamente pilotadas e o acesso ao espaço aéreo brasileiro**. Brasília, DF: DECEA, COMAER, 2023.

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.

CUNHA, L. C. D. **Redes neurais convolucionais e segmentação 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.

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

DJI. DJI improves geofencing to enhance protection of European airports and facilities. 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, Tailândia, 2004.

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

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 india's 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-targeted-saudi-arabia-s-abha-airport-with-drone-attack-119072900175_1.html>. Acesso em: 25 out. 2023.

INSIDER, B. . Here are the worlrd´s largest drone companies and manufacturers to watch. . 2020. Disponível em: https://www.businessinsider.com/drone-manufacturers-companies-invest-stocks.

JÚNIOR, J. C. A.; NUÑEZ, 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.-G. Main types of attacks in wireless sensor networks. *In*: **Proceedings of the 9th WSEAS International Conference on Signal, Speech and Image Processing, and 9th WSEAS International Conference on Multimedia, Internet & Video Technologies**. Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS), 2009. p. 180–185.

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.

MANUAL de Projetos Aeroportuários. Brasília, DF: Secretaria Nacional de Aviação Civil, 2021.

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

MERCADO LIVRE. Mini drone DJI Mavic Mini 2 DRDJI017 Single com câmera 4K light gray 1 bateria. 2023. Disponível em: <https://www.mercadolivre.com.br>. Acesso em: 10 ago. 2023.

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-targeted-saudi-arabia-s-abha-airport-with-drone-attack-119072900175_1.html`. Acesso em: 25 out. 2023.

OACI. **Avaliação do ADS-B e Multilateração para Apoio aos Serviços de Tráfego Aéreo e Diretrizes para Implementação (Cir 326)**. Montréal, 2012.

OXFORD, V. S. **Director, US Defense Threat Reduction Agency**. Março 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.

QIBLAWI, T. Por que ataque a Abu Dhabi pode ser um perigoso ponto de virada no oriente médio. **CNN Brasil**, São Paulo, jan. 2022.

RODRIGUES, C. V. C. **ADS-B- automatic dependent surveillance broadcast: estudo do impacto em Portugal**. 2010. 83f. Dissertação (Mestrado em Engenharia Aeronáutica) - Universidade da Beira Interior, Covilhã.

SOUZA, M.; HENKES, J. A. O uso de drones pela polícia militar de santa catarina: Uma abordagem sobre as vantagens para a instituição e as limitações 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 neutralização 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 cameras. **IPSJ Transactions on Computer Vision and Applications**, v. 11, n. 7, 2019.

VISMARI, L. F. **Vigilância dependente automática no controle de tráfego aéreo: Avaliação de risco baseada e modelagem em redes de petri fluidas e estocásticas**. 2007. 272f. Dissertação (Mestrado em Engenharia) - Escola Politécnica da Universidade de São Paulo, São 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.

ZMYSŁOWSKI, 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.

ŁUKASIEWICZ, 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.

FOLHA DE REGISTRO DO DOCUMENTO

1. CLASSIFICAÇÃO/TIPO	2. DATA	3. DOCUMENTO Nº	4. Nº DE PÁGINAS
TC	08 de Novembro de 2023	DCTA/ITA/TC-074/2023	60

5. TÍTULO E SUBTÍTULO:

Prospecção de tecnologias de identificação e monitoramento de drones em espaço aéreo controlado

6. AUTOR(ES):

Matheus Gondim Peixoto

7. INSTITUIÇÃO(ÕES)/ÓRGÃO(S) INTERNO(S)/DIVISÃO(ÕES):

Instituto Tecnológico de Aeronáutica – ITA

8. PALAVRAS-CHAVE SUGERIDAS PELO AUTOR:

Drones leves, Sistemas anti-drones, Segurança em Aeroportos

9. PALAVRAS-CHAVE RESULTANTES DE INDEXAÇÃO:

Aeronaves não-tripulada; Aeroportos; Segurança de aeronaves; Espaço aéreo; Segurança de voo; Monitoramento; Aeronaves teleguiadas; Engenharia aeronáutica.

10. APRESENTAÇÃO: (**X**) **Nacional** ( ) **Internacional**

ITA, São José dos Campos. Curso de Graduação em Engenharia Civil-Aeronáutica. Orientador: Prof. Dr. Mauro Caetano de Souza; coorientador: Maj. Esp. CTA. Cristian da Silveira Smidt. Publicado em 2023.

11. RESUMO:

Este trabalho de Conclusão de curso é direcionado para análise de 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, o trabalho realiza uma revisão bibliográfica sobre métodos de detecção de drones, apresentando e comparando técnicas relevantes encontradas na literatura recente. Em paralelo é feito o estudo de soluções anti-drones disponíveis no mercado, reunindo as principais características dessas tecnologias. São apresentadas definições sobre os veículos aéreos não tripulados, características e limitações do espaço aéreo brasileiro e realizou-se o levantamento das regulamentações relevantes para voos de drones de pequeno porte. A comparação entre os métodos 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 do modelo proposto e manter a integridade do espaço aéreo brasileiro.

12. GRAU DE SIGILO:

(**X**) **OSTENSIVO** ( ) **RESERVADO** ( ) **SECRETO**