DISSERTAÇÃO DE MESTRADO PROFISSIONAL

# ESTUDO SOBRE EMPREGO DE DRONES EM OPERAÇÕES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

**JEFERSON NASCIMENTO AQUILAR PEY**

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

# ESTUDO SOBRE O EMPREGO DE DRONES EM OPERAÇÕES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

# STUDY ON THE USE OF DRONES IN PUBLIC SAFETY INTELLIGENCE OPERATIONS

**Jeferson Nascimento Aquilar Pey**

**Orientador: Prof. Dr. Georges Daniel Amvame Nze, FT/UnB**

**Co-orientador: Prof. Dr. Robson de Oliveira Albuquerque, FT/UnB**

PUBLICAÇÃO: PPEE.MP.032

BRASÍLIA-DF

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

# ESTUDO SOBRE EMPREGO DE DRONES EM OPERAÇÕES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA

**JEFERSON NASCIMENTO AQUILAR PEY**

*Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica*

Banca Examinadora

Prof. Georges Daniel Amvame Nze, Ph.D, FT/UnB _____
*Orientador*

Prof. Robson de Oliveira Albuquerque, Ph. D, FT/UnB _____
*Examinador suplente e Co-orientador*

Prof. Christiano Cruz Ambros, Ph.D, UFRGS _____
*Examinador externo*

Prof. Fábio Lúcio Lopes de Mendonça, Ph.D, FT/UnB _____
*Examinador Interno*

**FICHA CATALOGRÁFICA**

PEY, JEFERSON
ESTUDO SOBRE EMPREGO DE DRONES EM OPERAÇÕES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA [Distrito Federal] 2022.
xvi, 76 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

| | |
|---|---|
| 1. Drone RPA | 2. Inteligência |
| 3. Segurança Pública | 4. UAV UAS |
| I. ENE/FT/UnB | II. Título (série) |

**REFERÊNCIA BIBLIOGRÁFICA**

PEY, J. (2022). *ESTUDO SOBRE EMPREGO DE DRONES EM OPERAÇÕES DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 76 p.



JEFERSON NASCIMENTO AQUILAR PEY
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

## DEDICATÓRIA

Aos meus pais Francisco (*in memoriam*) e Amélia (*in memoriam*) que, mesmo na simplicidade de analfabetos, me ensinaram tanto.

## AGRADECIMENTOS

Agradeço inicialmente a Deus pelo dom da vida, pela saúde e pela motivação que me permitiram ultrapassar todos os obstáculos encontrados ao longo da realização deste trabalho.

A minha família pelo apoio incondicional, pelo companheirismo e pela compreensão nas minhas ausências necessárias para se dedicar ao mestrado.

Aos professores Georges Daniel Amvame Nze (orientador) e Robson de Oliveira Albuquerque (co orientador) pelas correções e orientações transmitidas que foram fundamentais para eu chegar até aqui.

Aos professores do PPEE/UnB que ministraram as disciplinas do curso do mestrado. Os ensinamentos transmitidos certamente contribuíram muito para o amadurecimento e surgimento de novas ideias ao longo do processo de construção de conhecimentos.

Aos colegas do mestrado profissional PPEE/UnB pelas conversas, pelos trabalhos em conjunto e pelas amizades formadas ao longo deste período. Que o vínculo formado seja a base para novas conquistas.

A ABIN e a UnB, instituições promotoras deste mestrado, que esta parceria possa continuar a produzir frutos em benefício da transformação dos assuntos de Inteligência em algo mais acadêmico e difundido dentro da sociedade brasileira.

## RESUMO

O emprego de Aeronaves Remotamente Pilotadas (RPA), *Unmanned Aerial Vehicle* (UAV), *Unmanned Aircraft Systems* (UAS) ou mais conhecidos como “drones” tem crescido nos últimos anos e isso se deve à sua versatilidade de uso. Esses veículos aéreos possuem uma variedade de tecnologias embarcadas que fazem com que sejam atrativos e de fácil utilização. Este trabalho, em particular, almejou contribuir com a análise de RPA em apoio à atividade de Inteligência de Segurança Pública, agregando achados acerca de requisitos técnicos, vulnerabilidades cibernéticas e melhores práticas empregadas por equipes operacionais de Segurança Pública. Por fim, esta dissertação apresenta contribuições aderentes à legislação brasileira para o emprego de drones em proveito das Instituições que trabalham com a temática de Inteligência de Segurança Pública e aponta alguns direcionamentos futuros de estudos sobre o emprego dessas aeronaves. Os resultados da pesquisa, conduzida com base no método de investigação hipotético dedutivo, demonstram que as RPA são ferramentas capazes de contribuir com a otimização dos trabalhos de segurança pública, conferindo celeridade e segurança nas ações operacionais, além de proporcionar maior grau de eficiência quanto aos resultados almejados. Em conclusão, este estudo demonstra que o emprego sistematizado de RPA para realizar atividades de ISP é uma forma inovadora de transformação das atividades nas instituições de segurança pública.

## ABSTRACT

Use of Remotely Piloted Aircraft (RPA), Unmanned Aerial Vehicle (UAV), Unmanned Aircraft Systems (UAS) or better known as “drones” has been increasing in recent years and this is due to their versatility of use. These aerial vehicles have a variety of embedded technologies that make them exciting and user-friendly. This work, in particular, has always contributed with RPA analysis in support of Public Security Intelligence (ISP) activity, adding findings on technical requirements, cybernetic vulnerabilities and best practices employed by Public Security operational teams. Finally, this dissertation presents contributions that adheres to Brazilian legislation for the use of drones for the benefit of Institutions that work with the theme of ISP and points out some future directions for studies on the use of these aircraft. The results of this research, conducted based on the method deductive hypothetical investigation, demonstrating that RPA tools are capable of contributing to the optimization of public safety work, providing speed and security in operational actions, in addition to providing a greater degree of efficiency in terms of the desired results. In conclusion, this study demonstrates that the systematic use of RPA to carry out ISP activities is an innovative way of transforming the activities of public security institutions.

# SUMÁRIO

# LISTA DE FIGURAS

# LISTA DE TABELAS

# 1 INTRODUÇÃO

## 1.1 CONTEXTUALIZAÇÃO

O século XXI é caracterizado por grandes transformações ocorrendo rapidamente em todos os setores da sociedade. Enquanto no século anterior as grandes mudanças ocorreram nos meios de produção, com o aumento da força de trabalho por meio do uso da tecnologia, neste século constata-se uma sociedade baseada no conhecimento em que a aprendizagem organizada deve se tornar um processo ao longo da vida profissional. Nesta sociedade é seguro afirmar que qualquer pessoa deve adquirir novos conhecimentos a cada 4 ou 5 anos, do contrário, se torna obsoleta [31].

Levando-se em conta a premissa do parágrafo anterior, pode-se afirmar que os drones vieram para ficar, ou melhor, os drones vieram para revolucionar. A utilização e desenvolvimento dessas aeronaves já existe há muito tempo, embora a curva exponencial de crescimento de comercialização tenha sido observada apenas nas últimas décadas, tornando-se implemento protagonista em diversas áreas da atividade humana.

O emprego de drones tem se popularizado em diversas áreas: indústria de energia, construção civil, *hobby*, turismo, agropecuária, mineração, defesa, segurança pública, dentre outras. Esses veículos aéreos possuem uma grande variedade de tecnologias embarcadas, que fazem com que sejam muito atrativos de serem utilizados. Além disso, sob o ponto de vista econômico, devido ao aumento da economia de escala na produção de drones, a relação custo-benefício torna-se cada vez mais vantajosa em favor da aquisição dessas aeronaves.

O ponto de partida para se estudar essas aeronaves é entender a sua definição, sob pena de não delimitar exatamente o assunto a ser tratado. A terminologia empregada para conceituar drones apresenta variações a depender do país em que é empregado, do contexto e do arcabouço jurídico a ele vinculado.

Cumpre ressaltar que o termo “drone” não é o mais adequado do ponto de vista técnico, mas tornou-se um jargão mundial para referir-se a aeronaves remotamente pilotadas. O vocábulo “drone” tem origem no idioma inglês e significa zangão, denominação comum ao animal macho das espécies de abelhas. Provavelmente este termo foi escolhido devido à versatilidade do voo desses animais e ao barulho característico emitido pelas aeronaves e que se assemelha ao som emitido pelo voo dos zangões.

Os drones são veículos aéreos não tripulados conhecidos como VANTs (Veiculo Aéreo Não Tripulado), *Unmanned Aircraft* (UA), *Remotely Operated Aircraft* (ROA), *Remotely Piloted Vehicle* (RPV), *Unmanned Aerial Vehicle* (UAV) e *Remotely Piloted Aircraft* (RPA) [32] e [33].

A legislação brasileira designou inicialmente estes artefatos como ‘Veículos Aéreos Não Tripulados’ (VANT), termo que, de acordo com Bispo et al. [34], origina-se da expressão inglesa *Unmanned Aerial Vehicle* (UAV). Apesar disso, esta terminologia não definia claramente se havia, ou não, a intervenção humana em relação ao voo da aeronave, o que provocava confusão com as aeronaves autônomas. Em um aeromodelo ou drone o sistema de pilotagem está centrado no controle do operador, enquanto que no VANT, todo o sistema está na própria aeronave. A pilotagem remota limita-se a repassar ao subsistema de

voo da aeronave um ponto alvo ou uma proa, além dos parâmetros de voo [35].

Além disso, de acordo com a Instrução do Comando da Aeronáutica, ICA 100-40 [36], emitida pelo Departamento de Controle do Espaço Aéreo (DECEA), o termo VANT não é mais usado pela comunidade internacional de aviação, posto que o vocábulo 'veículo' não abrange outros tipos de vetores aéreos que não são classificados como aeronaves.

A Organização da Aviação Civil Internacional (ICAO) definiu que toda aeronave sem piloto humano a bordo e que seja controlada a partir de um operador em solo, seja definida como um *Remotely Piloted Aircraft* (RPA), e seu sistema de *Remotely Piloted Aircraft Systems* (RPAS), a exemplo do conjunto da aeronave e o piloto em solo. Esse sistema define todos os recursos operacionais que fazem a aeronave voar, sejam eles a estação de pilotagem remota, *link* ou estação de comando que possibilita um controle da aeronave, seus equipamentos de apoio e a própria aeronave.

Os Estados Unidos, segundo a *Federal Aviation Administration* (FAA) [37], mantêm a nomenclatura de *Unmanned Aircraft* (UA) e *Unmanned Aircraft Systems* (UAS). Já a Agência Europeia de Segurança de Aviação (EASA) considera válidas ambas as nomenclaturas de RPA, RPAS, UA e UAS, segundo consta em suas diretivas mais recentes as resoluções 2019/945 e 2019/947, tendo sido acrescentadas alterações pela resolução 2022/425 [38].

No Brasil, o termo oficial empregado pela legislação do Departamento de Controle do Espaço Aéreo (DECEA) e pela Agência Nacional de Aviação Civil (ANAC) é Aeronave Remotamente Pilotada (RPA), conforme os documentos ICA 100- 40 [36] e o Regulamento Brasileiro de Aviação Civil Especial nº 94 (RBAC-E nº 94) [29].

## 1.2 DEFINIÇÃO DO PROBLEMA

O problema de pesquisa delineado para esta dissertação foi o seguinte: dado que a utilização de drones apresenta inúmeras possibilidades, como utilizar os RPAs em proveito da Inteligência de Segurança Pública (ISP) de forma mais eficiente e segura? Existem muitos estudos recentes relativos aos drones, sobretudo em língua inglesa, mas no tema específico de emprego para segurança pública a literatura acadêmica em língua portuguesa ainda é rarefeita e pouco densa, conforme será exposto nos estudos relacionados.

O assunto é importante porque a proliferação de UAS traz uma série de preocupações relativas à segurança da sociedade e do Estado, seja por causa dos riscos a aviação, seja por causa do uso malicioso: crimes comuns, tráfico de drogas e armas ou terrorismo, dentre outros. Além disso, é preciso discutir os ataques cibernéticos sobre drones a fim de aprimorar a gestão de riscos.

A hipótese básica busca constatar a viabilidade da utilização de drones para atividade de ISP a fim de se aprimorar a qualidade dos serviços prestados pelos Órgãos de Segurança Pública, levando à adoção de medidas e decisões menos subjetivas e mais científicas, porporcionando melhores resultados operacionais.

Como hipótese secundária pode-se verificar se o uso de RPA na atividade de ISP pode colaborar na análise de risco de uma operação de OSP, que é uma função clássica da inteligência no assessoramento da autoridade decisora.

## 1.3 OBJETIVOS E ESTRUTURAÇÃO

O objetivo deste estudo é apresentar contribuições no emprego de RPA para ISP e, para isso, alguns objetivos intermediários serão delineados:

1. Realizar revisão de literatura a fim de verificar o estado da arte na seara de UAV.

2. Analisar alguns tipos de ataques cibernéticos - *jamming* e *spoofing* - no uso de RPAs.

3. Descrever aspectos legais e doutrinários sobre o emprego de drones no contexto da realidade brasileira.

4. Estudar casos concretos de emprego de RPAs no tocante a segurança pública a fim de reunir ensinamentos para embasamento teórico das contribuições propostas.

Para fins metodológicos, a pesquisa será classificada da seguinte forma: quanto à natureza, será pesquisa aplicada porque gera conhecimentos a fim de aplicações práticas na resolução de um problema específico, em consonância ao que se propõe a realização de uma dissertação de Mestrado Profissional. Quanto à abordagem do problema, será qualitativa e quantitativa, uma vez que se valerá de dados obtidos de forma objetiva e a vertente qualitativa será demonstrada nas impressões obtidas em revisão de literatura.

Quanto aos objetivos, a pesquisa será exploratória, visando aprofundar conhecimentos sobre determinado problema formulado e, finalmente, quanto aos procedimentos técnicos serão realizadas pesquisas bibliográficas e documentais, levantamentos e estudos de caso. Como contribuição, a dissertação descreve experiências que podem ser aproveitadas pelas autoridades públicas, auxiliando especialmente as instituições vinculadas à segurança pública no direcionamento de ações gerenciais e operacionais para a condução de projetos desta natureza.

A dissertação está estruturada, na sequência à introdução, no capítulo 2, pela contextualização de desenvolvimento dos drones até o seu estado da arte. Em seguida, o capítulo 3 com os estudos relacionados, onde são abordados sistemas de aeronaves remotamente pilotadas, ataques cibernéticos e considerações em relação ao 5G e 6G. Na sequência, o capítulo 4 explora conceitos legais, tópicos doutrinários e os sistemas de controle de drones no Brasil. A seguir, o capítulo 5 apresenta discussão de vantagens e desvantagens do uso de RPA em ISP, escolha de drones e análise de casos reais de emprego de RPAs em algumas instituições brasileiras, apresentando oportunidades de melhoria que foram utilizadas para a elaboração deste estudo. As propostas de contribuições são apresentadas no capítulo 6, com a discussão da problemática, a escolha de drones e explanação do modelo de uma Unidade de Emprego de Drones. Os trabalhos futuros e considerações finais são apresentados no capítulo 7, destacando oportunidades de aprofundamento para trabalhos futuros e exposição das considerações finais.

O desenvolvimento tecnológico impõe a necessidade de atualização permanente de meios e métodos para realizar atividades de Inteligência, mas, fazer surgir e consolidar inovações na área de Segurança Pública, além de ser uma necessidade, é um grande desafio. Este estudo contribui com o necessário movimento de transformação imposto por este cenário ao avaliar os reais impactos da aplicação de Aeronaves Remotamente Pilotadas (RPA) em estudos de Inteligência de Segurança Pública (ISP) [24]. Daí a importância desta dissertação, que visa apresentar metodologia eficiente para o emprego de drones e que possam ser analisadas pelas instituições que lidam com a temática de ISP no Brasil.

# 2 DESENVOLVIMENTO DE DRONES

## 2.1 DESENVOLVIMENTO DE DRONES NO MUNDO

Buscando-se a origem histórica do surgimento dessas aeronaves, observa-se que a concepção inicial para emprego de drones foi na área militar, devido as evidentes vantagens do ponto de vista de análise de risco de vidas humanas e de economia de recursos [20]. Os primeiros projetos de RPA utilizadas no contexto militar datam do fim da 1ª Guerra Mundial, em 1918. Na prática, eram mísseis de cruzeiro construídos para se destruírem juntamente com o alvo, como o *Kattering Aerial Torpedo*. Em 1935, Reginald Denny projetou e testou o RP-1 ou *Remotely Piloted Vehicle* (RPV), como eram denominadas as RPA à época, que foi a primeira aeronave não tripulada rádio-controlada [24]. Após isso, foram aperfeiçoados novos protótipos denominados RP-2 e o RP-3, com diversos ensaios de voo. Em novembro de 1939, o protótipo RP-4 foi concluído e o *US Army* adquiriu 53 unidades, dando-lhe a designação de OQ-1, conforme figura 2.1.

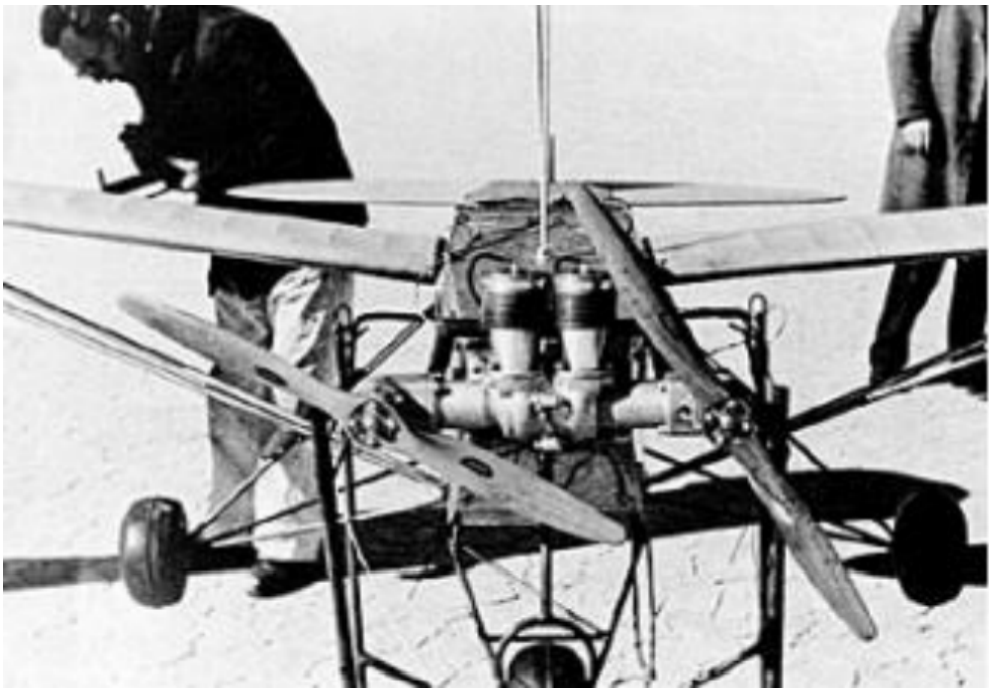

Figura 2.1: Aeronave OQ1 - Hardgrave (2005) apud [1]

Com o advento da Guerra Fria, após a 2ª Guerra Mundial (1945), surgiu a necessidade do emprego de RPA para o uso da espionagem. Já na Guerra do Vietnã (1955-1975), os UAS passaram a ser utilizados para o reconhecimento de alvos inimigos. A *US Air Force* criou um RPA – o *Firebee* – com câmeras, passando a espionar posições norte-vietnamitas e chinesas durante o conflito. Pouco tempo depois, estes UAS eram consideradas os melhores produtos disponíveis no mercado para missões de reconhecimento, o que despertou o interesse de Israel [1]. Israel usou os *Firebee* em combate durante a Guerra do *Yom-Kippur* (1973), voando sobre a Síria e o Egito. Seu objetivo era localizar as defesas antiaéreas inimigas. Outro marco histórico na utilização das RPA foi durante a Guerra do Líbano (1982), no Vale do *Bekaa*, quando

Israel conseguiu destruir 16 das 17 baterias antiaéreas sírias após fazer o reconhecimento do local com UAV.

O crescimento do emprego militar deste tipo de aeronave atingiu auge após os atentados de 11 de setembro de 2001, quando os Estados Unidos mais do quaduplicaram o orçamento destinado aos projetos de aeronaves não tripuladas. Em 2002, tornou-se notória a RPA estadunidense *'Predator'*, utilizada durante a Guerra do Afeganistão. Esse foi considerado o primeiro emprego real de um veículo não tripulado com o lançamento de míssil. Também se destaca no cenário mundial a RPA *Global Hawk*, modelo RQ-4A. A *Global Hawk* é operada pela *US Air Force* e pela *US Navy* e é utilizada como plataforma de grande altitude para missões de *Intelligence, Surveillance and Reconnaissance* - ISR (Inteligência, Vigilância e Reconhecimento). Recentemente, observou-se a eficácia e efetividade do emprego de RPA em conflitos armados, tais como observados na guerra entre Rússia e Ucrânia.

### 2.1.1 Drones na guerra da Ucrânia - Rússia 2022

A guerra entre a Rússia e a Ucrânia (2022) tem se mostrado uma experiência real para o desenvolvimento e emprego de drones em conflitos armados. No que tange ao emprego de missões de reconhecimento e aquisição de alvos para a artilharia, destaca-se o uso do *Orlan 10*, mostrado na figura 2.2. Além disso, equipamentos de inteligência eletrônica também podem ser instalados a bordo do drone, capazes de determinar com precisão as coordenadas de qualquer fonte de ondas eletromagnéticas. Na prática, isso significa que um alvo, que tente usar comunicações de rádio ou via telefone celular, pode ser imediatamente detectado e atingido por fogos de artilharia. A principal carga útil (*payload)* do *Orlan 10* é uma estação optoeletrônica com canais diurnos, noturnos e telêmetro. Além disso, o referido UAV pode ser equipado com um sistema de guerra eletrônica do tipo *Leer-3* e ser operado a partir de uma estação de inteligência rádio.

Figura 2.2: Drone *Orlan 10* [2]

Já os drones *Lancet 1* e *Lancet 3*, exibido na figura 2.3, são muito parecidos, diferindo apenas no que

concerne a autonomia de voo, tamanho e massa da ogiva. São utilizados para bombardeios de alvos pré selecionados. O *ZALA Lancet* é um drone *kamikaze* desenvolvido pela empresa russa *ZALA Aero Group* para as Forças Armadas Russas. No modo de combate, pode ser armado com ogivas de alto explosivo (HE) ou de fragmentação. Possui orientação óptico-eletrônica e unidade de orientação por TV, que permite o controle da munição no estágio terminal do voo. Além disso, tem equipamentos de inteligência (dispositivo de escuta, de verificação de origem e tráfego de comunicações), além de módulos de navegação e de comunicação.


Figura 2.3: Drone *Lancet 3* [3]

Desde setembro de 2022, ataques sistemáticos à infraestrutura militar e energética da Ucrânia têm sido realizados por meio do uso de um novo drone *kamikaze* intitulado *Geranium-2*, que é uma versão do drone *kamikaze* iraniano *Shahed-136*, ilustrado na figura 2.4. Neste RPA, o controle de voo se dá pelo uso de sistemas de navegação e lançamentos realizados a partir de uma plataforma terrestre especial, que pode ser rebocada e deslocada por viaturas. Após o lançamento, o *Geranium-2* é acelerado por um motor de foguete e, em seguida, usa uma hélice alimentada por um motor a gasolina ou diesel. O drone é descartável, a ogiva está localizada na proa e serve para o direcionamento direto de alvos inimigos.

Devido ao seu tamanho reduzido, o *Geranium-2* é de difícil detecção por sistemas de radar moderno, principalmente se realizar aproximação do alvo a uma altitude abaixo de 60 metros. Além disso, devido a utilização de motor de fraca potência (50 HP), esse UAV tem uma baixa assinatura térmica, dificultando ainda mais sua detecção por sistemas de defesa aérea da OTAN, empregados pela Ucrânia [26].

Segundo especialistas internacionais, a guerra Rússia/Ucrânia demonstrou que o combate contemporâneo é diferente daqueles observados até o início do século XXI. O emprego de forças terrestres é importante para atacar, ocupar e manter o terreno. No entanto, atualmente, os sistemas de Comando e Controle (C2) e de Inteligência, Vigilância e Reconhecimento (ISR), que fornecem consciência situacional aos comandantes, têm aumentado de relevância no campo de batalha. Exemplo disso, são os diversos tipos de drones que transmitem informações em tempo real, permitindo a rápida tomada de decisão em relação as operações em curso.

Tanto para as forças russas, quanto para as forças ucranianas, o comando e controle das operações no Teatro de Operações mudou. Grupos de combate são acompanhados por vários drones. As forças terrestres russas empregam usualmente três drones em batalhas urbanas: um monitora as possíveis posições


Figura 2.4: Drone *Geranium 2/ Shahed 136* [4]

da artilharia inimiga, o segundo reconhece itinerários em busca de emboscadas e fortificações, ao passo que o terceiro exerce a vigilância, acompanhando a operação em tempo real e fornecendo dados para o sistema C2 coordenar as ações.

Tabela 2.1: Drones russos na guerra da Ucrânia adaptado de [26]

| **Características** | **Orlan 10** | **Lancet 1** | **Lancet 3** | **Geranium 2/ Shahed 136** |
|---|---|---|---|---|
| Envergadura | 3.1m | - | - | 2.5m |
| Comprimento | 1.8m | - | - | 3.5m |
| Autonomia voo | 10h | 30min | 40min | 10-12h |
| Altitude voo | 3000m | - | - | 60 - 4.000m |
| Velocidade voo | 100-150km/h | 80 - 110km/h | 80 - 110km/h | 150 - 185km/h |
| Peso Máximo Decolagem | 18kg | 5 kg | 12kg | 250kg |
| Payload | 5.5kg | 1 kg | 3kg | 50kg |
| Alcance | 1000km | - | 40 km | 1500 - 2500 km |
| Missão | Reconhecimento | Bombardeio | Bombardeio | Bombardeio |

Pelo lado da Ucrânia, há que se destacar o uso dos drones de origem turca *Bayraktars*, ilustrado na figura 2.5. Fabricados na Turquia pela *Baykar Technology*, os drones são capazes de destruir tanques de guerra. O modelo *Bayraktar TB2* utiliza bombas e mísseis ar-terra a laser, projetados para serem lançados por uma aeronave militar contra objetivos de superfície com maior precisão. Ele foi desenvolvido a pedido do exército turco, após a experiência positiva com o *Bayraktar TB1*, e o primeiro voo ocorreu em 2014 [5].

Os *Bayraktar TB2* podem ser equipados com metralhadoras e usados em operações de ISR. Eles têm

envergadura de 12 metros, 6,2 metros de comprimento e peso máximo de decolagem (PMD) de 700 Kg. Podem operar até a 30 mil pés de altitude e têm autonomia de 27 horas, sendo operados de forma remota a partir de uma estação de controle em solo.

Figura 2.5: Drone *Bayraktar TB2* [5]

Além disso, a *Baykar Technology* uniu forças com a Ucrânia para o desenvolvimento de um drone de combate com tecnologia furtiva (*stealth*). Em setembro de 2022 foi anunciada a conclusão bem sucedida de testes de integração do *Bayraktar Kizilelma* com um motor ucraniano, mostrado na figura 2.6. O projeto foi iniciado em 2021 e ganhou impulso devido à necessidade ucraniana na guerra com a Rússia em 2022.

A nova aeronave não tripulada utiliza um motor AI-25 TLT produzido na Ucrânia, pela companhia *Motor Sich*. Ele terá a potência suficiente para levar o *Kizilelma* a *Mach* 0.9, com velocidade de cruzeiro de *Mach* 0.6. Os voos poderão ocorrer a até 14 km de altura e duração de uma hora. A carga útil será de uma tonelada.

O planejamento é de que o *Bayraktar Kizilelma* possa destruir alvos no ar, conquistar a superioridade aérea e, na função ar-solo, destruir sistemas antiaéreos. Há a perspectiva de que o drone possa operar em combate no início de 2023 e que, futuramente, seja empregado como ala de caças tripulados.

O uso de drones para múltiplas funções no Teatro de Operações da Guerra da Ucrânia por ambas forças beligerantes consolida a mudança de paradigma na interoperabilidade de sistemas de armas, os quais dependem cada vez mais de uma eficiente e ampla rede de vigilância, reconhecimento e designação de alvos por RPAs, cujo custo mais baixo e alta eficácia operacional permite uso sistemático em campo de batalha, diferentemente de ativos mais complexos e caros para finalidades semelhantes, tais como: blindados, aviões e helicópteros.

Dessa forma, pode-se conjecturar que a doutrina e a estrutura organizacional das tropas em combate estão sendo influenciadas pelo uso, cada vez mais intenso, de drones nos Teatros de Operações militares.

Figura 2.6: Drone *Kizilelma* [6]

## 2.2 DESENVOLVIMENTO DE DRONES NO BRASIL

Para o Brasil, o uso de aeronaves iniciou-se em 23 de outubro de 1906, quando o inventor Alberto Santos Dumont realizou o primeiro voo de um artefato mais pesado que o ar, no campo de *Bagatelle* em Paris. Mas, foi com o advento da 1ª Guerra Mundial (1914-1918) que a utilização das aeronaves teve grande impulso para a realização de uma série de missões, desde o reconhecimento aéreo, essencial para verificar antecipadamente a posição e o movimento do inimigo, até o ataque direto às posições adversárias, por meio de caças e bombardeiros, razão pela qual a superioridade aérea tem sido cada vez mais importante nos conflitos modernos.

### 2.2.1 Emprego civil de drones no Brasil

Segundo Jorge [39], um dos primeiros projetos de RPA de asa móvel para uso civil foi designado Helix, entretanto foi desativado por falta do incentivo do governo. Um outro projeto que envolveu o desenvolvimento de um RPA foi a parceira entre a Universidade de Brasília (UnB) e o Departamento Nacional de Produção Mineral (DNPM), atual Agência Nacional de Mineração ( ANM), com o objetivo de monitorar atividades ilegais na mineração. O projeto construiu um RPA, chamado de µVANT, de asa fixa que possuía 1,90 m de envergadura, capacidade de carga (*payload*) de 1 kg, peso total de 2,5 kg, possuía autonomia de voo de aproximadamente 90 min e o alcance de 4km a partir da base [40].

Uma das maiores empresas no setor de drones é brasileira. Trata-se da XMobots. Fundada em 2007 e baseada em São Carlos/SP, a XMobots atua principalmente nos setores de agricultura de precisão e geotecnologias na América Latina. A companhia, classificada como a 14ª maior empresa de drones civis do mundo pela consultoria global *Drone Industry Insights*, é especializada no desenvolvimento e fabricação de

drones que realizam decolagem e pouso vertical (*Vertical Take-Off and Landing* - VTOL) de alto desempenho e de tecnologias correlatas, como sensores multiespectrais, sensores optrônicos giroestabilizados, *softwares* de análise de dados baseados em inteligência artificial e plataforma provedora de serviços com drones.

A empresa lançou em 2022 a terceira versão do drone *Arator 5C*, ilustrado na figura 2.7. Este RPA é o único drone da categoria autorizado pela ANAC a realizar voos acima de 400 pés (120 m). Nessas condições, ele pode ir até a distância de 2Km do operador ou até 5Km com auxílio de um observador. O *Arator 5C* também conta com Autorização de Projeto da ANAC para voos além da linha de visada (*Beyond line Of Sight* - BVLOS). Nesta certificação, o raio de comunicação aprovado é de 5Km e os voos ficam limitados a uma altura de até 120m. Para atender as Autorizações de Projeto da ANAC, o *Arator 5C* conta com modificações estruturais, como seu sistema de iluminação anticolisão. Tudo isso permitiu a expedição do CAER – Certificado de Aeronavegabilidade Especial para RPA.

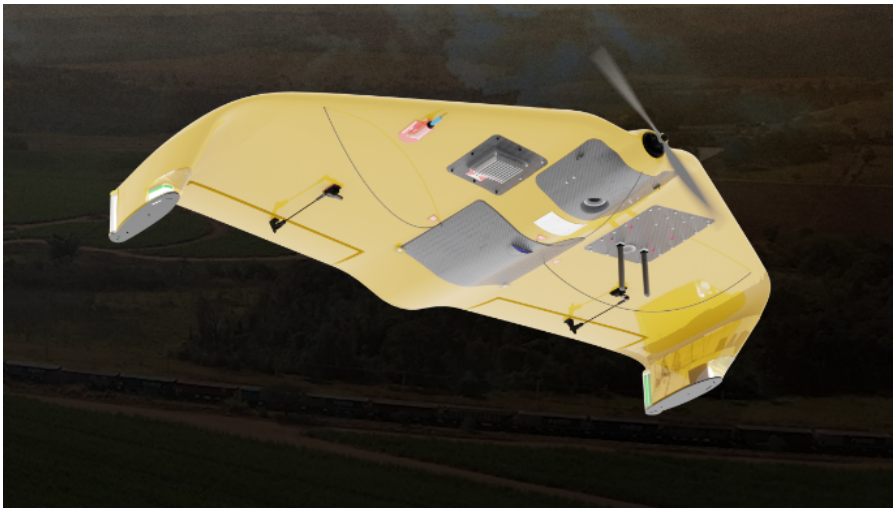

Figura 2.7: *Arator 5C* [7]

Outro produto desenvolvido pela XMobots em 2020 é o *Dractor 25A*, conforme figura 2.8, utilizado para pulverização de lavouras. Para o mapeamento, o *Dractor 25A* realiza seu voo de até 4 horas de duração sobre os talhões. Utilizando um dos sensores desenvolvidos pela XMobots (XM3, XMC ou XM5), o *Dractor* captura as imagens das áreas previamente selecionadas, sejam elas em RGB ou em outras bandas, como o NIR (infravermelho próximo) ou *RedEdge*, para obter o completo mapeamento em altíssima definição.

Com o objetivo de detectar as áreas afetadas com plantas daninhas nas lavouras, é possível realizar o processamento das ortofotos capturadas pelo sensor multiespectral XMC. E utilizando o *software* de inteligência de análise, *XFarming*, faz-se o uso de recursos de Inteligência Artificial para a detecção e delimitação das reboleiras presentes na área mapeada.

Outra linha de drones desenvolvidos pela XMobots é a *Nauru* [9]. Com sua primeira versão lançada em 2012, o *Nauru* apresenta alguns feitos notáveis, tais como ser a primeiro drone civil de asa fixa a sobrevoar a Amazônia, o primeiro a receber um Certificado de Autorização de Voo Experimental, CAVE, da ANAC e o primeiro drone VTOL híbrido desenvolvido no Brasil. Desenvolvido para operações BVLOS, o *Nauru 500C* possui autonomia de até 4 horas de voo e sua capacidade de *payload* permite que ele seja embarcado

Figura 2.8: *Dractor 25A* [8]

simultaneamente com 1 sensor de mapeamento e mais um sistema ISR para aplicações de vigilância. Tudo isso em uma plataforma que reúne o melhor das duas tecnologias de drones: a manobrabilidade da asa rotativa à autonomia da asa fixa, podendo decolar e pousar em áreas confinadas, conforme figura 2.9.

Figura 2.9: *Nauru 500C* [9]

Além disso, o *Nauru 500C* possui uma versão desenvolvida especialmente para o emprego em missões ISR (*intelligence, Surveillance e Reconnaissance*), batizado de *Nauru 500C ISR* e mostrado na figura 2.10. Existe ainda outro sistema mais robusto denominado sistema *Nauru 1000C*, que se constitui em produto que pertence a classe 2, segundo a classificação da ANAC (Peso máximo decolagem de até 150 kg) e se presta para missões ISR em ambiente de fronteira. A aeronave pesa 150Kg, pode atingir velocidades de 100 km/h, autonomia de 10 horas e alcance de 60 Km, a partir da estação de controle de solo. O drone tem oito motores elétricos, que possibilitam o pouso e a decolagem vertical (VTOL). Além disso, a aeronave é equipada com motor de 30 HP na parte traseira, que possibilita voo convencional.

Figura 2.10: *Nauru 500C-ISR* [10]

Tabela 2.2: Drones civis brasileiros empresa XMobots

| Características | Arator 5C | Nauru 500C | Nauru 500C ISR | Dractor 25A |
|---|---|---|---|---|
| Classe ANAC | 3 | 3 | 3 | 3 |
| Envergadura | - | - | - | 2.46m |
| Autonomia voo | 66min | 4h | 4h | 1h |
| Altitude voo | acima 120m | acima 120m | acima 120m | até 120m |
| Velocidade voo | - | 80 - 110km/h | 80 - 110km/h | 10 - 21km/h |
| Peso Máximo decolagem | 3.5kg | 12 kg | 12kg | - |
| Alcance | 5km | 60km | 60 km | 5km |
| Missão | Aerolevantamento | Aerolevantamento | Patrulhamento | Pulverização |

Quanto ao emprego por Órgãos de Segurança Pública (OSP), a Polícia Federal foi a primeira instituição a adquirir RPA no ano de 2009, dentro do contexto de Operações de Segurança para os Grandes Eventos (Copa do Mundo 2014 e Olimpíadas 2016) [41].

### 2.2.2 Emprego militar de drones no Brasil

Ao contrário dos drones civis, que estão em estágio mais avançado de desenvolvimento no país, os drones militares apresentam-se em nível mais incipiente de desenvolvimento. Um dos primeiros relatos de RPA militar, datam da década de 1980 com o projeto Acauã, que foi desenvolvido pelo Centro Tecnológico Aeroespacial (CTA) [39].

Uma iniciativa de empresa brasileira de defesa que não prosperou foi o projeto Falcão. Produzido pela Harpia Sistemas, empresa criada a partir da associação entre a Embraer Defesa e Segurança, e a AEL Sistemas, subsidiária da *Elbit Systems*, de origem israelense. Com grande parte de seus componentes de tecnologia nacional para uso dual (aplicações civis e militares), o Falcão foi idealizado para ser o maior VANT militar nacional, visando atuar em operações de vigilância marítima e de fronteiras, além de atender outros requisitos operacionais básicos das Forças Armadas. Com o fim da parceria da Harpia Sistemas, em janeiro de 2016, o projeto Falcão foi descontinuado. De qualquer forma, a Embraer é uma das maiores fabricantes de aeronave de pequeno porte do mundo e, futuramente, o Falcão pode voltar ao portfólio da empresa.

Outra iniciativa oriunda do segmento civil para emprego militar é o projeto Atobá, da empresa *Stella Tecnologia*, conforme demonstrado na figura 2.11. As grandes vantagens são, segundo a fabricante, a autonomia de até 28 horas de voo e 500 Kg de Peso Máximo de Decolagem (PMD), portanto drone de classe 1 segundo a ANAC. Já existe uma aeronave protótipo construída em 2020.

Também vale destacar o projeto Tupan 300, das empresas *Turbomachine* e SIATT. Apresentado em 2020, o TUPAN 300 apresenta design futurista e velocidade de voo de até 500km/h e autonomia de 300 km, graças ao motor a jato microturbina da *Turbomachine*. Além disso, conta com 3 m de comprimento, 3.2 m de envergadura e peso de 150 kg. O primeiro voo experimental com sucesso da aeronave foi realizado em julho de 2022 [42].

Em relação aos UAS de uso militar em operação, temos os modelos Hermes 450, conforme figura 2.14

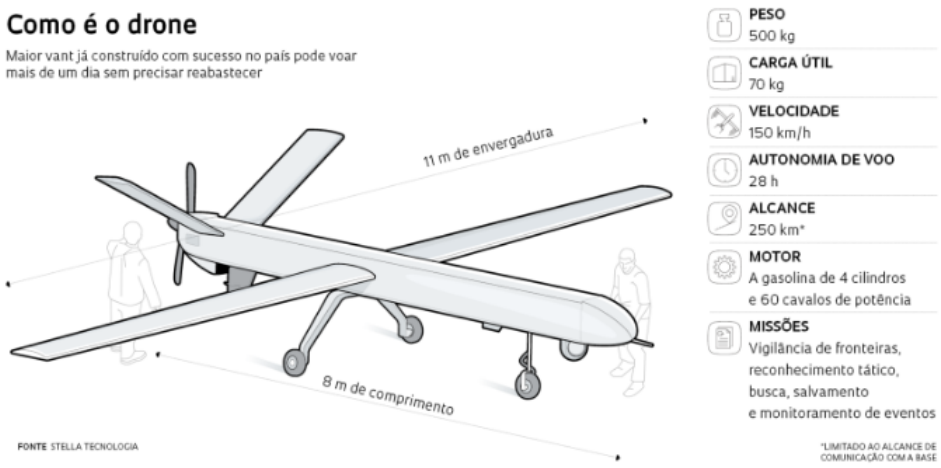


Figura 2.11: Projeto Atobá [11]

Figura 2.12: Projeto Tupan 300 [12]

e Hermes 900, ilustrado em 2.13, adquiridos pela FAB junto à empresa israelense *Elbit Systems* e baseados no Primeiro Esquadrão do Décimo Segundo Grupo de Aviação (1°/12° GAV - Esquadrão Hórus). Esta unidade militar foi criada em 2011, na Base Aérea de Santa Maria/RS, com o objetivo de operar as RPA da FAB, realizando missões de Controle Aéreo Avançado, Posto de Comunicações no Ar, Busca e Salvamento em Combate (C-SAR) e Reconhecimento Aéreo.

Em 2014, o Esquadrão passou a operar as aeronaves RQ-900 Hermes, que possuem capacidade de operação em média altitude e longa duração. Equipada com o sensor eletro-ótico e térmico *DCoMPASS*, com câmera colorida de alta definição, sensor de visão infravermelha e iluminador e designador de alvos a laser, essa aeronave possui também o sistema eletro-ótico *SkyEye*, um conjunto de 10 câmeras de alta resolução que permite a vigilância de várias áreas simultaneamente, com transmissão de dados em tempo real. O RQ-900 Hermes voa a mais de 9.000 metros de altura e tem autonomia superior a 30 horas [43].

A FAB realizou, em 23 de setembro de 2022, o primeiro voo de traslado de uma RPA, a RQ-900 Hermes, de Santa Maria/RS para Campo Grande/MS. A distância entre os aeródromos de decolagem e pouso


Figura 2.13: Hermes 900 [13]

é de aproximadamente mil quilômetros. Até então, as missões não tripuladas conduzidas pela Força Aérea, ainda que tivessem grande alcance devido ao controle realizado por satélite, restringiam-se a decolagem e pouso sempre no mesmo aeródromo.

A operação, conduzida pelo esquadrão Hórus, revestiu-se de grande complexidade, em virtude das peculiaridades do sistema não tripulado, da suscetibilidade à meteorologia e da necessidade de múltiplas coordenações entre órgãos de controle do espaço aéreo e tripulantes, que revezaram a missão estando baseados em Santa Maria/RS, Brasília/DF e Campo Grande/MS. Uma equipe realizou a preparação da aeronave e os tripulantes realizaram o controle com *link* em linha de visada, usando antena de solo apontada diretamente para a aeronave, o que permitiu o comando remoto durante todas as fases da operação.

Na segunda etapa, uma tripulação assumiu o controle do RQ-900 a partir de Brasília/DF, desta vez por *link* satelital, executando a pilotagem remota até o aeródromo de Campo Grande/MS. Já na última fase da operação, antes do início dos procedimentos de descida para pouso, tripulação local assumiu o comando da aeronave, em linha de visada, realizando pouso em Campo Grande/MS.


Figura 2.14: Hermes 450 [14]

O Exército Brasileiro (EB) conta com Seção de Sistema de Aeronaves Remotamente Pilotadas (SARP) com objetivos de supervisionar as atividades decorrentes da continuidade da implantação dos SARP no

Exército Brasileiro, emitir diretrizes que regulam a sua operação e assessorar o Comandante de Operações Terrestres nos assuntos atinentes ao Projeto SARP [44]. Em dezembro de 2022, O Comando da Aviação do Exército, localizado em Taubaté/SP, recebeu a primeira aeronave da classe Nauru 1000C, conforme figura 2.15. Essas aeronaves serão empregadas prioritariamente em missões de ISR nas regiões de fronteira terrestre brasileira [15].

Figura 2.15: *Nauru 1000C* [15]

Já a Marinha do Brasil (MB) ativou o 1º Esquadrão de Aeronaves Remotamente Pilotadas (EsqdQE-1) em julho de 2022 na cidade de São Pedro da Aldeia/RJ. O novo EsqdQE-1 conta com seis modelos do drone *ScanEagle*, projetados pela empresa *Insitu*, subsidiária da *Boeing*.

Figura 2.16: *ScanEagle* [16]

O *ScanEagle* possui envergadura de 3,1 metros, comprimento de 1,67 m e peso máximo de decolagem de 23,4 kg. A carga paga máxima (*payload*) é de 3,4 kg, autonomia de voo de até 20 horas e altitude de voo de 19.500 pés (5.943 metros). O raio de ação máximo é de 100 km, dependendo do tipo de antena utilizada e do *link* da estação de controle de solo (GSC). A velocidade de cruzeiro da aeronave é de cerca de 110 km/h. A meta da Marinha é ampliar a capacidade de suas embarcações em missões de ISR e de busca e salvamento (SAR).

## 2.3 PERSPECTIVAS DE UTILIZAÇÃO DE DRONES

Estudo realizado pela *Skylogic Research* [45] revelou que empresa chinesa DJI continua a dominar o mercado e obteve ganhos em todas as categorias, desde aviões drones em todas as faixas de preço, a cargas úteis adicionais (*payloads*) e *softwares*. Os dados da pesquisa mostram que a DJI é a marca dominante com 74% do mercado global de vendas em todos os níveis de preço.

Estima-se que o mercado mundial de drones crescerá a uma média anual de 7.8% entre 2022 e 2030, quando atingirá aproximadamente U$55.8 bilhões em valores de comercialização [17]. A previsão é de que o mercado global de drones em 2030 seja mais do que o dobro do que era em 2021, conforme figura 2.17 .

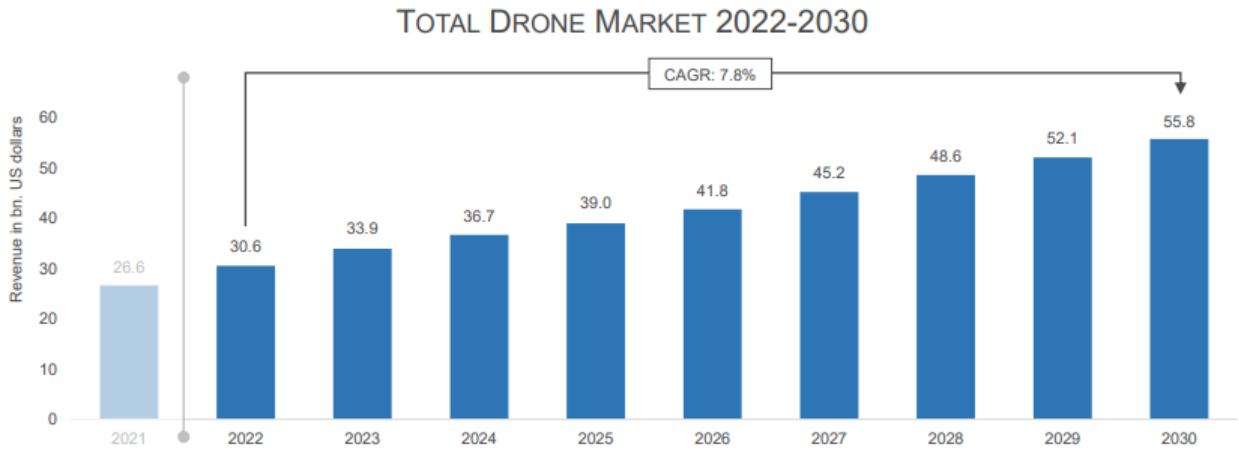


Figura 2.17: Previsão mercado global de drones [17]

A previsão para 2030, ilustrada nas figuras 2.18 e 2.19, é de que haverá cerca de 19,4 milhões de drones na Ásia; 12,2 milhões na América do Norte; 13,4 milhões na Europa; 2,3 milhões na América do Sul; 1,8 milhões na Oceania e 6,6 milhões no Oriente Médio e África [46]. Dados de 2020 apontaram que os maiores mercados consumidores eram: Estados Unidos, China, Japão, Alemanha, Reino Unido, França, Austrália, Canadá, Itália e Índia [17].

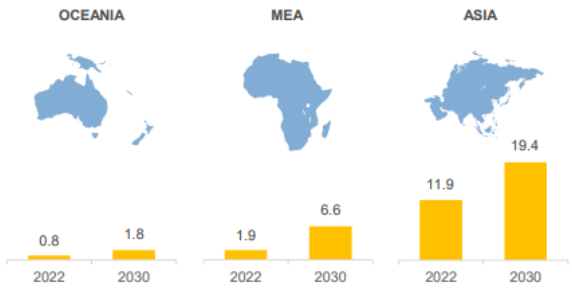


Figura 2.18: Previsão número drones 2030 [17]

À medida que a utilização de drones provê maiores facilidades para o dia a dia das pessoas, os problemas de segurança cibernética são gradualmente expostos. Em estudo da Agência Europeia de Segurança da Aviação (EASA) e citado por Khan [47], realizado para obter informações sobre a perspectiva das pessoas sobre os UAVs, o que pode ajudar no estabelecimento de regras e regulamentos, sugeriu 83% de aceita-

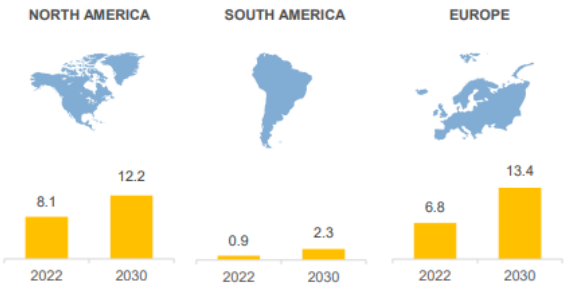


Figura 2.19: Previsão número drones 2030 [17]

ção para o uso de UAVs e também que 71% das pessoas estão prontas para experimentá-los. Como nos primórdios da aviação, a segurança continuará sendo o principal fator que influenciará a aceitação pública dos drones, especialmente porque, ao contrário da aviação comercial e geral, os drones operam em áreas densamente povoadas e em altitudes mais baixas [48].

As possibilidades de emprego são tão amplas que se pode afirmar que os RPAs são um tipo de tecnologia disruptiva, uma vez que provocaram ruptura em modelos, padrões e formas com que determinadas tarefas eram executadas. O uso de imagens e fotografias aéreas é um bom exemplo disso: até pouco tempo atrás aeronaves tripuladas eram utilizadas para realizar reconhecimentos em apoio a operações policiais em ambiente urbano. Esse tipo de atividade implicava num custo elevado composto pela manutenção e combustível da aeronave, além do salário do piloto, copiloto e do cinegrafista. Isso sem falar no risco de acidente que poderia culminar na perda de vidas humanas. Com a utilização de drones, essa tarefa foi radicalmente transformada, ou seja, rompeu-se com um padrão anteriormente estabelecido.

O futurista americano Thomas Frey afirma que os drones se tornarão a tecnologia mais disruptiva da história da humanidade [49]. Mas para que a utilização de uma nova tecnologia se transforme em algo disruptivo é necessário que haja também a inovação e não apenas a invenção. A diferença é que a inovação depende de emprego prático com a demonstração de eficácia na resolução de um problema identificado na vida das pessoas.

No que concerne à segurança pública, a transmissão de imagens em tempo real é uma possibilidade inovadora de emprego, por serem as RPAs munidas de tecnologia via satélite. Elas possibilitam melhor alcance visual por parte do operador, garantindo melhor efetividade para as equipes operacionais, seja identificando e individualizando manifestantes infratores, seja produzindo provas que comprovem a autoria e materialidade dos crimes, seja mapeando áreas para um melhor planejamento de operações contra queimadas e desmatamentos, por exemplo.

## 2.4 TENDÊNCIAS EM DESENVOLVIMENTO PARA USO DE DRONES

### 2.4.1 Remote ID

A *Remote ID* é a nova conformidade da FAA (*Federal Aviation Administration*) para a operação de drones nos Estados Unidos que entrou em vigor em 16 de dezembro de 2022 [50]. A *Remote ID* é uma

tecnologia que transmite, em tempo real, a localização e identificação de drones. A certificação serve para que as autoridades locais de controle tenham as informações do objeto que está ativo em seu espaço aéreo. A *Remote ID* é uma espécie de 'placa digital' para a identificação dos drones.

No Reino Unido, a Autoridade de Aviação Civil (CAA) também prevê a utilização de *Remote ID*, definindo-a como a capacidade de um UAS fornecer informações de identificação que podem ser recebidas por outras partes. O objetivo da *Remote ID* é auxiliar a aplicação da lei para identificar um UAS desonesto ou piloto/operador remoto que pareça operar de forma insegura ou em uma área onde o UAS não está autorizado a voar [51].

Já faz algum tempo que os órgãos de controle do espaço aéreo do mundo inteiro buscam uma solução de maior controle de drones. Os Estados Unidos estão na vanguarda da *Remote ID*, muito pela pressão de órgãos de segurança e pela própria população com a popularização dos drones. A FAA ficou a cargo das definições da *Remote ID* e de todo o processo do novo sistema. Depois de uma análise das considerações que foram enviadas do mundo inteiro e das consultas públicas, chegou-se ao modelo utilizado.

Assim como em qualquer tipo de produto que envolve uso em situações de risco, é natural que a legislação sofra atualizações e modificações para ficar de acordo com o cenário atual e futuro. Com a *Remote ID* as agência de controle e órgãos de segurança podem acessar em tempo real dados completos do drone, do voo e também do piloto, que registrou o drone.

Com a tecnologia *Remote ID* ou através de um módulo de transmissão compatível, os dados serão enviados desde o processo de decolagem até o momento que o drone é desligado. Os dados que serão transmitidos de acordo com a FAA estão listados a seguir: identificação exclusiva do drone; latitude, longitude, altitude e velocidade do drone; indicação da latitude, longitude e altitude do controle (piloto) ou local de decolagem (módulo de transmissão); tempo de voo e *status* de emergência (apenas do drone).

O cerne da questão é o debate jurídico entre os direitos fundamentais de intimidade e privacidade e a necessidade de segurança pública. A *Remote ID* recebeu muitas críticas, especialmente por parte dos usuários e da necessidade de fornecer os dados do drone e piloto em tempo real. Não obstante a isso, é provável que essa tecnologia seja adotada por outros países, como o Brasil, nos próximos anos.

### 2.4.2 First Person View - FPV

FPV quer dizer *First Person View*, com tradução direta para 'visão em primeira pessoa', isso quer dizer que, na prática, o piloto terá a resposta em tempo real da câmera como se ele estivesse pilotando a aeronave.

Em se tratando de formatos e modelos, drones FPV, em sua maioria, são modelos DIY (*Do-It-Yourself* / faça você mesmo). Dessa forma, existe uma grande variedade de modelos. Algumas empresas têm apostado em *kits* prontos, como a *BetaFPV* que combina alguns componentes próprios e outros de outras marcas; outras empresas semelhantes se especializaram em criar seus *kits* personalizados para vender em quantidade, combinando um drone personalizado, um modelo de controle e um óculos. Nesses casos, não é necessário escolher todos os componentes para montar o drone e fazer toda a configuração.

A aplicação de FPV para a ISP é a possibilidade de reconhecimento em áreas perigosas e confinadas de busca e salvamento, tais como incêndios e desastres naturais.

Como conclusão parcial desta seção, pode-se afirmar que são cada vez maiores as possibilidades de emprego desta tecnologia no país. Embora tenha importado sistemas aéreos não tripulados de Israel, o Brasil vem se destacando pelo desenvolvimento de RPAs civis e militares, tornando-se liderança regional no desenvolvimento deste tipo de tecnologia.

# 3 TRABALHOS RELACIONADOS

Em língua portuguesa existem poucos estudos que tratam do emprego de RPAs para fins de Segurança Pública. No Brasil, via de regra, são trabalhos de nível especialização *lato sensu* desenvolvido em escolas militares nos cursos de aperfeiçoamento de oficiais, conforme exemplos de [52], [30], [53], [54], [55], [56], [57], [58], [24], [59], [60], [61], [62], [63], [34], [64], [65] e [66].

Em relação à Portugal, autores como [67], [68], [69], [70] seguem a mesma linha de raciocínio do parágrafo anterior sobre trabalhos em escolas militares e Morgado [71] destaca que a incorporação dos drones no contexto de segurança pública apresenta-se como uma opção vantajosa no cenário operacional daquele país. A tabela 2.1 sintetiza as palavras chaves e os achados mais relevantes na literatura acadêmica em língua portuguesa sobre o emprego de drones em segurança pública.

Tabela 3.1: Tabela de publicacões em língua portuguesa relativa ao emprego de drones em Segurança Pública

| **Autor** | **Palavras Chaves** | **UF** | **Ano** |
|---|---|---|---|
| Neto et al. [52] | Emprego Veículo Aéreo não Tripulado (VANT) ações operações PM | BA | 2009 |
| Chiote [68] | Requisitos Operacionais Veículos Aéreos Não Tripulados (UAV) na GNR | Portugal | 2012 |
| Bispo [34] | Utilização VANT Seguraça Pública | MG | 2013 |
| Alfaro [67] | Veículos aéreos não tripulados na PSP - Aplicabilidade | Portugal | 2015 |
| Silva et al. [62] | VANT: possibilidades de emprego no Corpo de Bombeiros Militar | SC | 2015 |
| Morgado et al. [71] | UAV's na Polícia de Segurança Pública | Portugal | 2017 |
| Pinheiro [53] | SARP: estudo sobre a viabilidade do emprego | ES | 2017 |
| Martins et al. [65] | Viabilidade do uso VANT pela PM | SC | 2017 |
| Moura et al. [56] | RPA: aporte no combate aos incêndios florestais pelo CBM | MA | 2018 |
| Silva [24] | Uso de RPA no campo da Inteligência de Segurança Pública | MG | 2018 |
| Sarte [59] | Padronização do serviço de RPA no CBM | SC | 2018 |
| Burlamaqui [63] | Uso de drones nas atividades operacionais das Polícias no estado | CE | 2018 |
| Terra [61] | Estudos de casos sobre projetos com o emprego de drones | SP | 2019 |
| Vicente [70] | VANT (drones): reforço da vertente aérea na PSP | Portugal | 2019 |
| Silva [55] | Análise organizacional do serviço de RPA no CBMDF | DF | 2020 |
| Correa [58] | RPA no cumprimento de mandados de busca e apreensão: viabilidade | PR | 2020 |
| Oliveira [64] | Emprego de RPA em apoio equipe de precursores em ambiente urbano | RJ | 2020 |
| Leite [66] | Uso do SARP na busca de inteligência para Forças Especiais | RJ | 2020 |
| Gonçalves [54] | Utilização de VANT pelo batalhão da PM na cidade de Canoas | RS | 2021 |
| Souza et al. [60] | Uso de drones pela PMSC: vantagens e limitações | SC | 2021 |
| Nunes [69] | O papel dos VANT na modernização do Exército | Portugal | 2021 |
| Oliveira et al. [30] | A PMPR e as novas tecnologias: o emprego das RPA | PR | 2022 |
| Zattera [57] | Emprego de RPA na área operacional de inteligência | PR | 2022 |

## 3.1 SISTEMA AERONAVE REMOTAMENTE PILOTADA - SARP

Uma RPA é composta pelo corpo (confeccionado para proteger as partes sensíveis e oferecer melhores condições aerodinâmicas para o voo), mecanismo de propulsão (composto pelos rotores e as hélices) e os sensores. Os sensores são essenciais para o controle do voo e incluem: giroscópios, acelerômetros, sensor orientação magnética, módulo do sistema global de navegação (GNSS) e câmera para filmagens e fotos.

Já o sistema de aeronave não tripulada (SARP) é composto por três elementos principais: aeronave propriamente dita, estação de controle de solo (*Ground Control Station* - GCS) e a interface de *link* de dados [72]. Uma vez estabelecida a arquitetura do sistema de drones, conforme descrito na figura 3.1, é possível a operação com este tipo de aeronave.

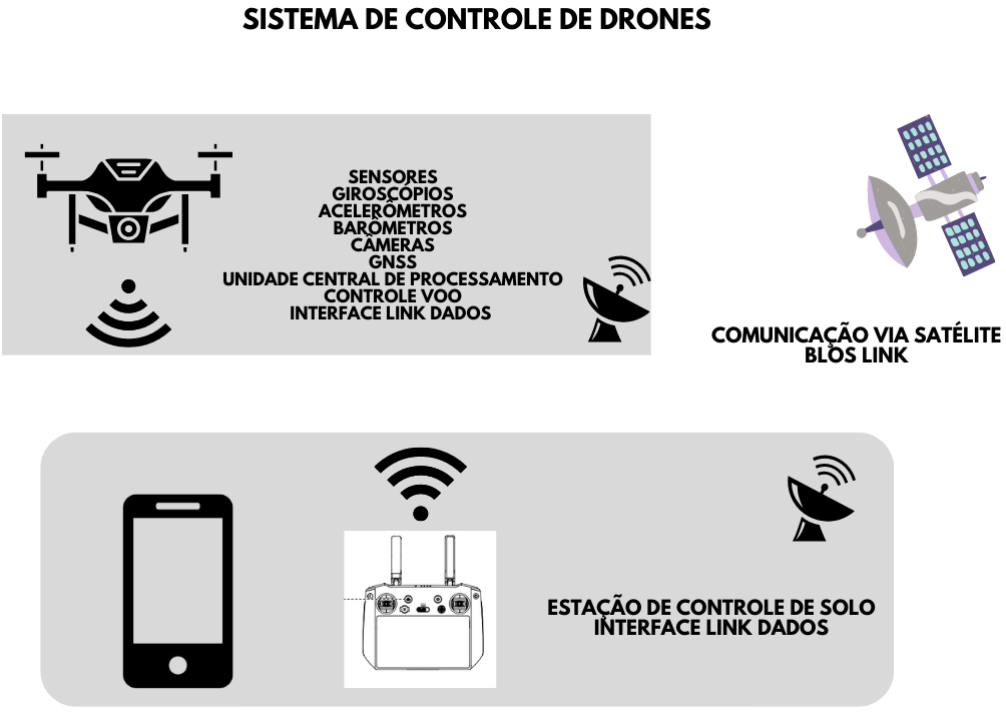


Figura 3.1: Sistema de drones.

De forma mais completa e detalhada, um SARP é constituído pelos seguintes componentes:

• Fuselagem, que é a parte mecânica do veículo, incluindo o sistema de propulsão;

• Sensores de navegação e movimento, que coletam as informações sobre a posição do drone e sua trajetória de voo;

• Sistema de controle de vôo (FCS), que controla o sistema de propulsão e os serviços em aplicação na trajetória de voo;

• *Payload*, que é o equipamento específico para cumprir uma determinada missão;

• Estação de controle terrestre (GCS), que é um sistema de computador ou uma rede de computadores em terra, que monitoram e controlam a operação dos UAS;

• Infraestrutura de comunicação, que é o conjunto de *links* de dados e equipamentos relacionados para a comunicação entre o veículo e a GCS.

Yaacoub et al. [73] realizaram estudo que compreendeu visão geral e análise do uso de drones em vários domínios, como marcos regulatórios de cada país, diferentes possibilidades de comunicações entre RPA, classificação dos drones, domínios de uso de UAV, tipos de ataques contra drones, tipos de sistemas anti drones e técnicas de detecção de UAV. A análise do estudo poderá auxiliar os *hackers* éticos em reconhecer as vulnerabilidades atuais dos UAVs, tanto no meio militar quanto no civil. Além disso, seu estudo futuro proposto permitirá implementação de novas técnicas e tecnologias para a identificação e defesa de ataques de UAV aprimorados.

Bispo et al. [34] pontuam que o uso de RPA por OSP deve ser considerado a partir de um processo de inovação incremental, iniciado com planejamento, objetivos específicos e aprimoramento futuro. Afirmam ainda que o uso dessa tecnologia é compatível com diversas atividades desempenhadas pelo setor de segurança, uma vez que no âmbito militar ela atua para evitar a exposição dos tripulantes ao risco, realizando missões de inteligência e combate, e no campo civil na realização de missões de monitoramento, filmagem, fotografia e medição a custos reduzidos.

A partir de informações coletadas para elaboração desta dissertação, observou-se tendência das Forças Armadas e dos OSP de inserirem aeronaves não tripuladas em suas operações e missões. Quase todas as aquisições ocorreram após 2009, reafirmando que os grandes eventos ocorridos no país (Copa do Mundo e Olimpíadas) provocaram o aumento dos esforços dos órgãos de segurança para incorporação de novas tecnologias [74].

Uma das desvantagens no emprego de drones é a limitada duração das baterias eletro-químicas de polímero de Lítio (LIPO) ou de íon de Lítio (LIIon) permitindo tempo de voo em torno de 15-20 minutos [75]. Além disso, as baterias eletro-químicas representam em torno de 40% da massa de uma RPA multirotor, o que inviabiliza o acoplamento de outros dispositivos na aeronave e limita o alcance dos voos [76]. Para Altawy e Youssef [72], um dos problemas do sistema de uso de drones civis é a sua interferência nos sistemas de aviação. Os sistemas UAV estão expostos tanto a ataques cibernéticos, quanto a ataques físicos de suas aeronaves.

Como gestão do risco, a possibilidade de automação apresenta soluções como retorno automático ao aeródromo de recolhimento ou a destruição controlada em local pré-estabelecido. Em operações reais, a transmissão da imagem proveniente dos sensores a bordo da aeronave é essencial. O cálculo para taxa de transmissão deve considerar a máxima qualidade dos sensores a bordo e os meios disponíveis. Missões de Segurança Pública normalmente aceitam distâncias piloto-aeronave dentro da linha de visada (VLOS), mas o relevo poderá obrigar o uso de controle além da mesma (BLOS) via satélite ou com apoio de observadores [35].

### 3.1.1 Subsistema de navegação

O motivo do amplo emprego do Sistema Global de Navegação por Satélite (GNSS), seja o *Global Positioning System* - GPS (EUA), ou *GLONASS* (Rússia), ou *Galileo* (Europa), ou *BeiDou* (China), nos drones é devido à simplicidade de uso e baixo custo da tecnologia, assim como a boa acurácia na transmissão das

coordenadas [77]. O funcionamento dos sistemas é baseado na triangulação dos dados de localização obtida pela constelação de satélites mantidas por esses países. Quanto maior o número de satélites captados pelo drone, maior a acurácia na sua localização.

As transmissões de sinal de GPS para drones civis são livres de criptografia e de autenticação. A natureza aberta deste tipo de comunicação permite ataques cibernéticos do tipo *spoofing* contra UAV. A errônea coleta de dados por sensores compromete a segurança do voo, podendo causar grave acidente ou queda, porém, antes de ser realizado o ataque cibernético contra o sinal de GNSS é necessário que o drone seja detectado. A estação de controle de solo (GCS) permite ao operador de solo monitorar ou controlar o voo da UAV e normalmente é composta de dispositivo físico que pode ser controle remoto, aparelho celular ou *tablet*.

Alguns fenômenos magnéticos interferem diretamente na acurácia de um sistema de navegação. A Anomalia Magnética da América do Sul (SAMA) apresenta características de baixa intensidade do campo total e coincide com a região de intenso fluxo de partículas cósmicas, muitos problemas com objetos que orbitam a Terra (por exemplo, satélites) são detectados nessa região [78]. Além disso, existem perturbações elétricas da ionosfera, às quais podem resultar em imprecisões dos sinais de GNSS. A região brasileira é um dos locais que apresenta os maiores valores e variações espaciais do conteúdo total de elétrons (*Total Electron Content* - TEC) e onde estão presentes diversas particularidades da ionosfera, tais como, a anomalia equatorial e o efeito da cintilação ionosférica [79]. Erros provocados por estes fenômenos citados devem constar do planejamento de desenvolvimento para sistemas de navegação de voos das RPAs no Brasil.

O sistema de *link* de dados é necessário para o estabelecimento de comunicação com a aeronave, que é realizado via ondas rádio frequência (RF) ou por sinal de telefonia celular (4G ou 5G). A escolha do *link* de comunicação depende do alcance da missão, que pode ser classificada em dentro da linha de visada do operador (*Visual line of sight* - VLOS) ou fora da linha de visada do operador (*Beyond line of sight* - BLOS). Ressalta-se que a diferença entre VLOS e BLOS importa num grau de subjetividade, uma vez que o alcance da visão varia de pessoa para pessoa. A utilização de um auxiliar/observador pode expandir a VLOS, assim como qualquer obstáculo, como uma árvore, pode limitar bastante o alcance da visão e transformar uma operação VLOS em BLOS. Um dos desafios enfrentados pelos países atualmente é justamente definir e regulamentar claramente as condições de voo VLOS e BLOS, que certamente traz implicações para a segurança do voo, conforme se observa na figura 3.2.

O bloqueio do GNSS não é uma técnica diferente do bloqueio de RF. É tratado separadamente devido à sua relevância considerando que os sinais GNSS são tipicamente os mais sujeitos a neutralização. Os sinais recebidos dos satélites são caracterizados pelo baixo valor de potência e, assim, são vulneráveis aos sinais interferentes. O bloqueio do receptor GPS de um drone comercial pode resultar em dificuldades de deriva e controle, além de impedir o procedimento de retorno para casa (RTH) funcionar corretamente.

No estudo de bloqueio GNSS, algumas técnicas foram analisadas e avaliadas em relação aos sinais de GPS por Ferreira et al. [80], juntamente com sucessivos bloqueios de pulsos, que envolvem uma sequência de pulsos ao longo do tempo com um pequeno ciclo de trabalho para a frequência central de interesse. Os melhores resultados são obtidos com bloqueio inteligente (*spoofing*) e bloqueio de varredura (*jamming*). A primeira técnica é a mais eficaz quando comparado à sua finalidade (inutilizar o sinal GPS para o receptor), enquanto a vantagem do segundo método é a simplicidade de implementação, embora deva ser notado que

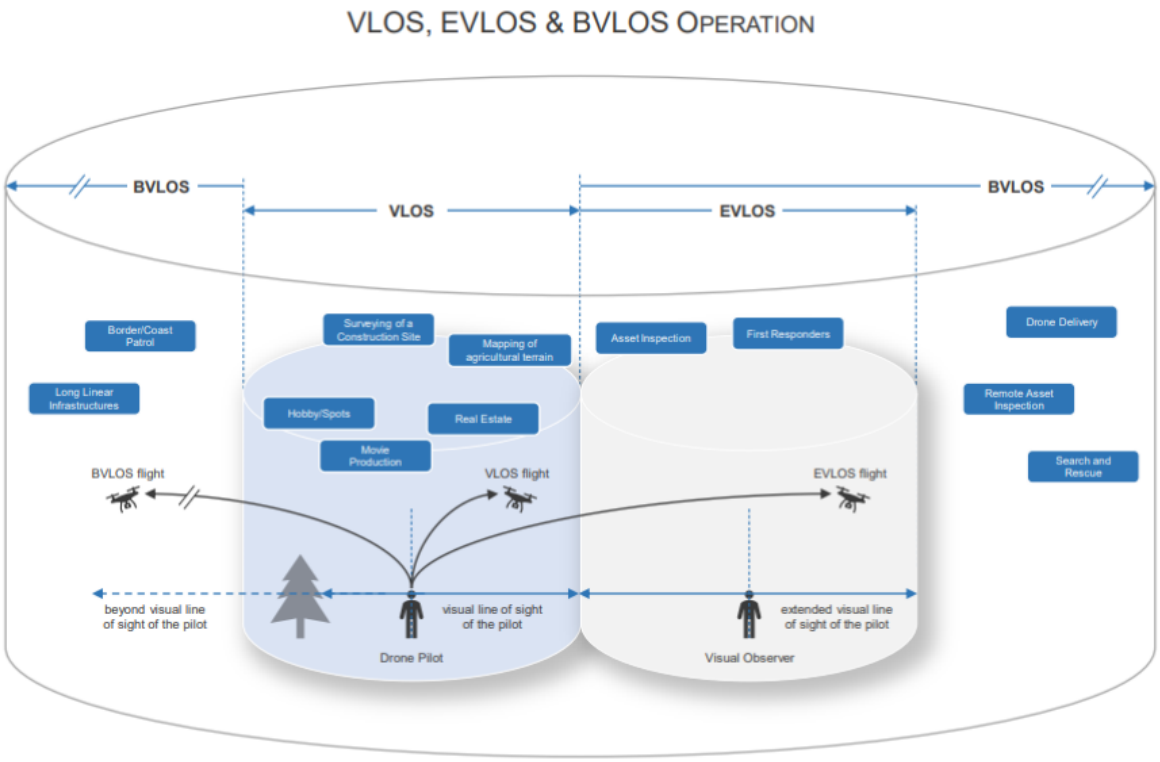


Figura 3.2: Raio de operações com drones[18]

a eficiência obtida depende da velocidade utilizada para varrer a banda de frequência.

Em estudo de Basan et al. [77], sobre identificação de ataque cibernético de GPS *spoofing*, foi proposta metodologia para detecção de ataque por meio da análise de mudança de parâmetros internos da UAV. Em uma tentativa de identificar GPS *spoofing*, Arthur [81] utilizou sistema de detecção de intrusão (IDS) baseado em *Deep Learning* (DL) inteligente o suficiente para diferenciar entre sinais de GPS falsificados e originais. He et al. [82] empregaram sensor visual da câmera monocular e dados da Unidade de Medição Inercial (IMU) do drone para identificar GPS *spoofing*. Além disso, os autores desenvolveram método para auxiliar o drone a retornar para base no caso de um ataque de GPS *spoofing*.

Com a diminuição contínua no tamanho dos sensores, processadores, unidades de câmera, memória digital e conectividade sem fio onipresente, os drones estão sendo utilizados de formas cada vez mais produtivas para melhorar o modo de vida das pessoas. Para isso, os UAV precisam de um sistema de navegação adequado e de gerenciamento do espaço aéreo [83].

### 3.1.2 Subsistema de Comando e Controle

O subsistema de Comando e Controle (C2) é parte essencial e permite a rápida tomada de decisão automatizada. Na verdade, é responsável pela análise das operações de tomada de decisão, tais como previsto por Castrillo et al. [84]:

- Avaliar nível de ameaça, com base nos *feedbacks* provenientes do sistema de monitoramento;
- Permitir o sobrevoo de drones não maliciosos em áreas protegidas específicas;

• Selecionar as técnicas de neutralização adequadas a serem usadas com base no nível de ameaça;

• Planejamento das operações anti RPA e acompanhamento de sua execução.

O sistema C2 deve buscar a automatização das ações por meio do uso de técnicas de Inteligência Artificial (IA), *Machine Learning* (ML) e *Deep Learning* (DL) a fim de otimizar os processos de tomadas de decisão.

Deve haver a coordenação das equipes de drones de campo, observação, meios de detecção e de neutralização, tudo isso sendo acompanhado e coordenado a partir de uma central de controle que pode estar na GCS ou numa sala de situação/Comando e Controle, a depender da área ou instalação a ser protegida. As comunicações entre as equipes devem ser ágeis e com baixa latência o que sugere o emprego ideal de *Flying Ad Hoc Networks - FANET*.

As RPAs proporcionaram uma quebra de paradigmas, como a possibilidade de acompanhamento em tempo real das ações operacionais a partir de um centro de C2 [35]. Na Polônia, por exemplo, o *Fire Service* (equivalente ao Corpo de Bombeiros) em operações de Busca e Salvamento tem utilizado um *software* denominado *Search and Rescue with Unmanned Aerial Vehicle* (SARUAV), que facilita e agiliza as operações de busca e salvamento. Neste tipo de missão, a estação de controle de terra (GCS) é um dos componentes cruciais do sistema de busca, que garante a transmissão de imagem do UAV para os participantes da operação de busca em tempo real, além de ter a missão de amplificar o sinal de comunicação rádio das equipes em terrenos acidentados, que dificultam a propagação de RF [85].

## 3.2 SISTEMA ANTI AERONAVE REMOTAMENTE PILOTADA

Um sistema antidrone é um sistema de monitoramento em tempo real e acionado por eventos críticos que visam detectar e localizar um drone invasor, determinando sua legalidade/ilegalidade, nocividade ou não, e decidindo o melhor método de neutralizar sua operação. Um sistema ideal de detecção de drones e comunicação aérea é um sistema complexo, multitarefa e multimodal, que funde várias tecnologias como sensores heterogêneos, redes, protocolos de segurança, aquisição de dados e mecanismos de sincronização, controladores de rastreamento, enquanto engaja um drone no espaço aéreo. Essas tecnologias entrelaçadas ajudam um sistema antidrone a atingir sua principal tarefa de detecção e localização de drones ou rastreamento e tomada de decisão, consoante preconizado por Ajakwe et al. [86].

Do ponto de vista simplificado de arquitetura, um sistema antidrone deve se constituir a partir dos subsistemas fundamentais [84]:

• Monitoramento;

• Neutralização;

As grandes organizações de segurança internacional estão cada vez mais preocupadas com as ameaças proporcionadas pelo uso malicioso de drones. Para exemplificar, a Organização Internacional de Polícia Criminal (Interpol) realizou exercício de simulação de medidas anti RPA em Oslo, Noruega, entre os dias 28 a 30 setembro de 2021. Esta organização também editou *framework* para resposta a incidentes com UAV [87].

Uma vez detectado o drone podem ser utilizadas medidas de proteção para fazer frente às ameaças, que seriam: utilizar alarmes de drones, fechar janelas com *black out* a fim de impedir a filmagem ou fotografia, desligar sinais de *wi-fi*, pois muitos drones se utilizam desse tipo de sinal para se conectar ou realizar ataques cibernéticos, evacuar a área, utilizar granadas fumígenas e tentar cegar a câmera do drone.

A figura 3.3 descreve o fluxo de ações a serem desencadeados a fim de minimizar os danos causados pelo emprego de drones adversos, dentro de um fluxo de ações: detectar, identificar e rastrear por meio de sensores acústicos, visuais, termais, RF ou radares. Num segundo momento adotar medidas não interativas, tais como o uso de alarmes, cegar as janelas para a observação externa, desligar redes de *wi-fi*, evacuar a área e usar granadas fumígenas para impedir realização de imagens e vídeos pelos drones invasores. Pode-se também utilizar medidas ativas para a interdição da aeronave invasora do perímetro aéreo: raios laser, projéteis, redes, ou uso de ataques cibernéticos de *jamming* ou *spoofing*.

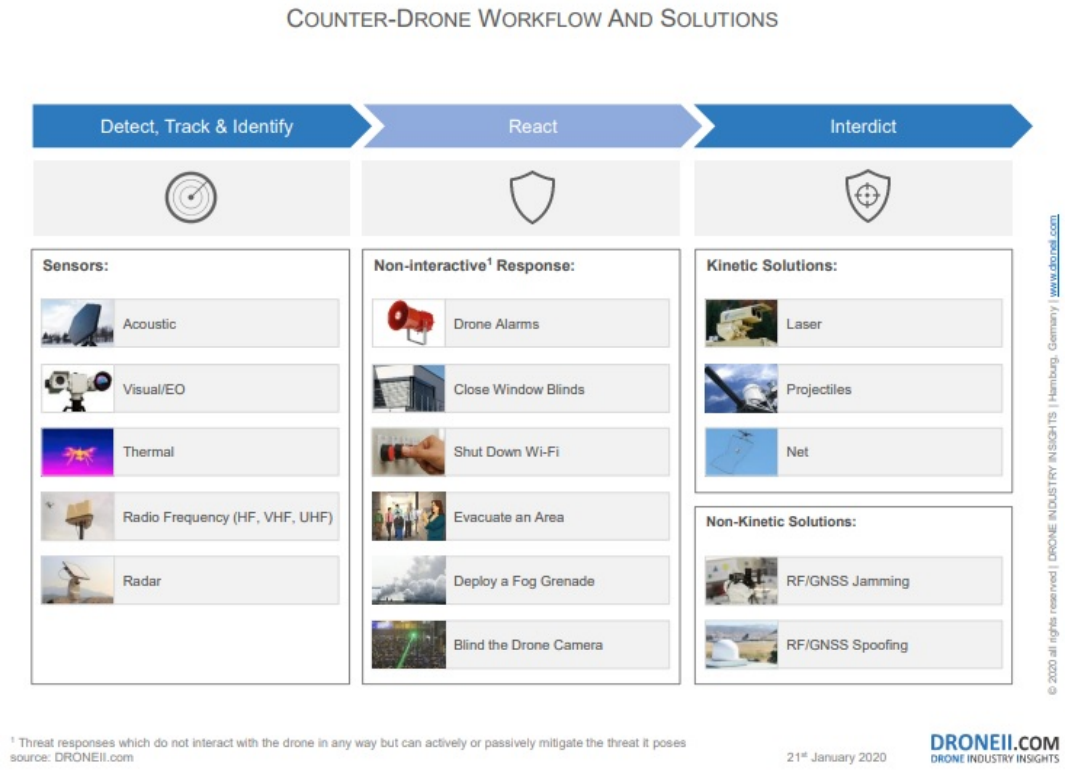


Figura 3.3: Contra medidas de drones.

### 3.2.1 Subsistema de monitoramento

Este subsistema existe para monitorar o nível de ameaça, por meio do uso de um ou mais sensores capazes de coletar as informações extrapoladas do campo eletromagnético ou espectro acústico, dependendo da tecnologia e do processamento do sinal envolvido. Em geral, a operação de monitoramento pode ser dividida nas seguintes fases [84]:

• Detecção: A descoberta de um ou mais objetos dentro do espaço aéreo considerado. Nesta primeira fase, o sistema ainda não é capaz de distinguir se o objeto é na verdade um drone.

• Classificação: Uma vez ocorrida a detecção, é preciso verificar se o objeto detectado é realmente um drone, pois é comum a falsa detecção de um alvo com uma ave, em função das características semelhantes como a seção transversal do radar, o tamanho e a forma geométrica. Para a correta classificação, o sistema deverá extrapolar alguns atributos do drone, como o tipo (tamanho, tipo de propulsão, número de rotores, modelo), a possível localização de um piloto remoto, a presença de uma carga útil e sua tipologia.

• Localização/Rastreamento: O alvo é localizado estimando sua posição em termos de ângulo e distância da instalação alvo. Técnicas de triangulação podem ser usadas para aumentar a precisão. Após isso, o alvo deve ser rastreado durante todo o seu vôo.

**Tecnologias de sensoriamento**

Um sistema anti-RPA, para cumprir seu objetivo, deve ser dotado de um sistema de monitoramento constituído por um ou mais sensores, incluindo diferentes tecnologias, que abordam diferentes fenômenos observados (electromagnéticos, acústicos ou pela banda do espectro que utilizam). Por exemplo, sensores de imagens operam nas frequências visíveis do espectro eletromagnético, ao passo que um radar opera em frequências invisíveis, como as de microondas.

**Sensores Acústicos**

O motor e as hélices dos drones geram ondas acústicas na faixa de frequência entre 20 Hz e 20 kHz, conferindo assinatura acústica ao veículo. Um único microfone pode adquirir esta informação e realizar comparação com uma biblioteca de assinaturas acústicas, distinguindo um drone de outros objetos, além de identificar a aeronave e obter informações sobre o modelo. Por meio da captação do som, é possível estimar o azimute e a elevação de um ou mais alvos na direção de aproximação (DoA) [84].

Este tipo de sensor é particularmente econômico, mas é sensível ao ruído e condições climáticas relacionadas ao vento ou temperatura e normalmente tem alcance limitado de detecção, dependendo do tamanho e do conjunto de microfones empregados.

Os resultados encontrados na literatura variam em uma faixa bastante ampla, de 5 m [88] até 600 m [89]. Em Chang et al. [90], um sistema terrestre de dois arranjos de quatro microfones (espaçados de 1 m) cada um foi usado para a localização de um drone através do cálculo da DoA e foram observados resultados comparáveis com precisão GPS e um alcance de detecção de 100 m. Vale ressaltar que o alcance de classificação pode ser inferior ao alcance de detecção, conforme demonstrado nos testes realizados e descritos em Sedunov et al. [91].

**Sensores de Rádio Frequência (RF)**

Sensores de radiofrequência (RF) captam os sinais eletromagnéticos irradiados por um drone ou pelo controle de rádio do piloto remoto. Trata-se de um método passivo que não requer a transmissão de ondas eletromagnéticas e, portanto, não tem restrições de uso. A maioria dos drones comerciais usa canal de rádio *uplink* para comandos de controle remoto e um canal *downlink* para telemetria e sinal de vídeo. No caso de drones autônomos, pode haver apenas *downlink* direto de transmissão para a estação de controle de solo (GCS). Os sistemas de detecção baseados nesta tecnologia utilizam um sensor de RF receptor entre 400 MHz e 6 GHz e um conjunto de antenas para a possível exploração de técnicas *Multiple Input Multiple Outputs* (MIMO).

Trabalho realizado por Ezuma et al. [92] identificou e classificou 15 tipos de UAV por meio de características de rádio frequência (*RF fingerprints*) emitidas pelos controles dos drones, mesmo com a interferência de sinal de *bluetooth* e *Wi-Fi*, usando sistema de vigilância passiva de RF. Essas técnicas não são muito eficazes se um padrão conhecido não for usado, se a comunicação esquema foi personalizado ou se o banco de dados de endereços MAC não estiver atualizado.

**Sensores Óticos**

Sensores ópticos detectam ondas eletromagnéticas na faixa de frequências do infravermelho (300 GHz) para ultravioleta (790 THz). É uma tecnologia passiva, portanto com baixo consumo de energia, que pode fornecer imagens bidimensionais do ambiente circundante. Os sensores ópticos podem ser divididos em duas categorias principais, dependendo da frequência em que trabalham: visível ou não visível. Por exemplo, a primeira categoria inclui câmeras ópticas, que podem detectar radiação eletromagnética na faixa de 430–790 THz faixa de frequência, enquanto a segunda categoria inclui câmeras térmicas, que convertem radiação infravermelha (300–430 THz) em imagens [84].

A utilização de sensores óticos é um campo muito promissor no desenvolvimento de tecnologias anti-RPA. O tamanho, o peso, a potência necessária e o custo das câmeras é tal que seu uso em drones não encontra impedimentos particulares e certamente torna possível usá-los como um sistema de detecção para todas as operações de detecção, identificação e rastreamento. Umas das arquiteturas em desenvolvimento mais utilizadas é a *You Only Look Once* (YOLO) [84]. Essa técnica é considerada o estado da arte em detecção de objetos em tempo real e consiste num método de detecção de objetos de passada única (*single pass*) que utiliza uma rede neural convolucional como extrator de características (*features*).

**Radares**

Um radar é um sensor ativo, constituído por um segmento transmissor que irradia ondas eletromagnéticas na faixa de frequência de 3 MHz a 300 GHz. As ondas são refletidas pelos objetos alvo e são recebidas pelo receptor. Ao processar adequadamente o sinal recebido, é possível, por exemplo, calcular o tempo de chegada e o deslocamento de frequência devido ao efeito *Doppler* para obter informações sobre a distância e a velocidade do alvo. A potência do sinal recebido é diretamente proporcional à seção transversal do radar (RCS), um parâmetro que mede a facilidade de detecção de um objeto e que depende do tamanho, material, distância e ângulo da onda incidente e refletida.

As principais vantagens do radar estão relacionadas à robustez contra condições ambientais adversas: a operação independe das condições de luz e condições atmosféricas. A desvantagem é que para obter um longo alcance de detecção, é necessário aumentar a potência de transmissão.

Artigo de Likou et al. [93], sobre o emprego de sistemas anti-drones próximos à aeroportos, concluiu que existe a tendência de aumento de ataques a essas infraestruturas com a utilização de drones e que planos de gestão de riscos e de contingência devem ser elaborados pelas autoridades para enfrentar essas ameaças.

Estudo conduzido por Shi et al. [27] abordou as tecnologias de detecção de drones, cujas características estão resumidas na tabela abaixo:

Tabela 3.2: Métodos de detecção de drones adaptado de [27]

| Método | Assinatura drone | Alcance | Características/desafios |
|---|---|---|---|
| Radar | Micro Doppler | 3000 m | Baixa assinatura radar Baixa altitude |
| Áudio | Função de tempo-frequência | 40-300m | Dificuldade de detecção em ambiente barulhento |
| Vídeo | Função do movimento | 100-1000m | Sensível obstrução e pode ser confundido outro alvo |
| RF | Ondas eletromagnéticas de RF | 1000m | Ruídos de RF e interferência visada direta |
| Óticos | Ondas eletromagnéticas GHz e THz | 500m | Ruídos e interferência visada direta |

Dado que existem fortes limitações nos métodos de detecção de drones, então é desejável a utilização combinada de dois ou mais métodos simultaneamente a fim de aumentar a probabilidade de sucesso na detecção.

### 3.2.2 Subistema de neutralização

De acordo com Park et al. [94], os métodos de detecção de drones estão em desenvolvimento incipiente. Em função disso, cerca de 80,96% dos sistemas anti-drones utilizam as técnicas de *jamming* e/ou *spoofing* para realizar a neutralização e/ou interdição de um sistema de drones (de 352 produtos *Counter Unmanned Aircraft Systems* (C-UAS) relatados, 285 utilizam as referidas técnicas [95].

***Drone Jamming***

Qualquer tipo de decodificação de comunicação digital está fortemente relacionada à relação sinal-ruído (*Signal-Noise Ratio*-SNR) no receptor. A SNR define o quão intenso é o sinal em relação ao ruído, sempre presente nos dispositivos de RF. Em uma comunicação digital, conforme aumenta a distância entre o transmissor e o receptor, a potência do sinal recebida diminui, devido às atenuações do meio de propagação [96].

O *jamming* é uma maneira de bloquear a comunicação sem fio entre o transmissor e receptor por meio da propagação de um sinal interferente até o momento em que a sensibilidade do receptor não seja suficiente para identificar os sinais, perdendo assim o enlace de comunicação [96]. Como exemplo, um ataque de GPS *Jamming* foi executado no drone *S-100 Camcopter*, resultando em uma colisão com o controle terrestre que feriu dois pilotos remotos e matou um engenheiro durante os testes [97].

Diferentes técnicas de *jamming* podem ser usadas para interromper a comunicação entre o controlador e o drone, sendo que as mais comuns utilizam antenas omnidirecionais ou direcionais [98]. As omnidirecionais emitem sinal interferidor em todas as direções (360º graus) e não necessitam de detectar o drone, mas tem a desvantagem de possuir menor poder interferidor.

Já as antenas direcionais são mais precisas. Em Multerer et al. [99], foi empregado o radar de ondas contínuas modulada por frequência 3D - *Frequency Modulated Continuous Wave* (FMCW) com múltiplas entradas e múltiplas saídas - *Multiple Input Multiple Output* (MIMO) e a utilização de antena direcional de *jammer* na faixa de 2.4 GHz. O radar escaneia constantemente determinada área até que o alvo entre no seu raio de atuação. O algoritmo de detecção avalia o movimento do alvo e, se ele for identificado como ameaça, a antena direcional emite o sinal interferidor, tornando impossível o controle do drone.

Segundo Park et al. [94], *jamming* apresenta como vantagens a simplicidade e o emprego imediato, além de poder ser usado contra protocolos de comunicação desconhecidos, desde que estejam utilizando a faixa de frequência atacada. Por outro lado, apresenta como desvantagens: interferência em outros dispositivos e não é efetivo contra voos autônomos. Uma vez detectado GPS *jamming*, deve-se utilizar um método alernativo de navegação.

Em termos legais, o uso de *jamming* é controverso. Por exemplo, no Brasil, o uso de *jammers* é permitido somente em unidades prisionais. Já nos EUA, os bloqueadores de sinal são proibidos em todo o território estadunidense. O motivo da proibição do *jamming* é que tal técnica inutiliza toda a faixa do espectro com a adição do sinal interferente, impossibilitando que outros sistemas de comunicação permaneçam operantes na frequência considerada.

Em termos técnicos, o uso de *jamming* é simples de ser executado, sobretudo se forem utilizados antenas omnidirecionais, que não dependem de algoritmo para localização e identificação do drone. Considera-se o uso de *jamming* apenas em drones comerciais com faixas de frequência de 2.4 GHz ou 5 GHz, permitidas pela ANATEL, entretanto podem ser desenvolvidas aeronaves que operem em outras bandas de frequência ou em outros protocolos de comunicação e que escapam desse tipo de ataque.

Atualmente, a maioria dos países têm restrições legais rígidas quanto ao uso de *jammers* por usuários civis [94], portanto os novos sistemas anti drones não militares devem ser desenvolvidos considerando a limitação/proibição de bloqueadores. No Brasil, por exemplo, está em debate a possibilidade de ampliar o uso de *jamming* para proteção de outras instalações estratégicas, além das unidades prisionais.

***Drone Spoofing***

O *spoofing* consiste em gerar um falso sinal eletromagnético com força suficiente para assumir o controle de drone atacado. Os sinais sob falsificação podem estar relacionados a algumas aplicações ou dispositivos diferentes: comunicações de controle remoto, comunicações de dados de carga útil, GNSS ou sensores. Para realizar o *spoofing*, é necessário conhecer as pilhas de pacotes de protocolos de comunicação utilizadas. Portanto, o *spoofing* é um método complexo e nem sempre bem sucedido. Para ocorrer um ataque de GPS *spoofing*, um transmissor é utilizado para enviar sinais falsos de GPS para o controlador de voo do drone, forçando o UAV a sincronizar com os sinais do atacante [100].

Para a realização do GCS-Drone *spoofing* é necessário que seja empregado um *sniffer* de RF capaz de identificar e descobrir os parâmetros de configuração do tipo de drone objeto do ataque, conforme exemplos em [92]. O termo já é empregado na área de Tecnologia da Informação (TI), quando um elemento externo tenta se infiltrar na rede de computadores copiando as credenciais de um computador já pertencente à estrutura. A aplicação de *spoofing* para sinais de RF depende do uso de um dispositivo que se passa pelo controle do drone, possibilitando assim, tomar o seu controle de voo. A técnica de *spoofing* em drones tem como vantagens: largo espectro de emprego e possibilidade de uso em voos autônomos, uma vez que pode confundir o sistema de navegaçao GNSS da aeronave [94].

No experimento, conduzido por Donatti [96], foi utilizado um sistema de intervenção de voo que contorna as barreiras técnicas inerentes ao projeto e permite tomar o controle de drones guiados por rádio frequência, mesmo na presença do controle real, de forma eficiente porque emite sinais de *clock* quase 5 vezes mais rápido do que o sinal do controlador original (tempo de chaveamento original 3.857ms, ao

passo que o chaveamento com o sistema *spoofing* era de apenas 0.8024ms).

O uso de *spoofing* apresenta as seguintes vantagens: ampla disponibilidade de uso e possibilidade de emprego também em voos autônomos por meio de *spoofing* do GNSS [94]. Por outro lado, existe a dificuldade de controle e execução da técnica, além da possibilidade de anulação da ação de *spoofing* com o controle manual da UAV.

Em termos regulatórios, esta técnica não se enquadra na especificação de bloqueador, o que facilita o seu emprego sob o ponto de vista legal. Além disso, o *spoofing* tem duas vantagens técnicas principais sobre o *jamming*: primeiro porque permite que a faixa de frequência seja operada por outros aparelhos e usuários, e segundo porque possibilita o controle da aeronave e, consequentemente, a captura dos objetos e das mensagens transportadas.

Existem ainda, outros métodos de neutralização ainda em fase inicial de desenvolvimento como a utilização de raios *lasers* direcionais ou energia eletromagnética de grande poder [93], que caracterizam uma grande força de intervenção típica de contexto militar. Para este tipo de emprego, os equipamentos demandam grande fonte de energia, tamanho e peso consideráveis. Além disso, ao destruir o drone, eventualmente o equipamento irá cair sobre alguma área, logo não é aconselhável seu uso em local com aglomeração de pessoas. Há, ainda, na literatura métodos menos convencionais de neutralização de drones, como a utilização de pássaros, redes e o emprego de armas de fogo, citados por Altawy e Youssef [72] e por Yaacoub et al. [73].

## 3.3 ATAQUES CIBERNÉTICOS SEGUNDO PRINCÍPIOS DE SEGURANÇA INFORMAÇÃO

Os ataques cibernéticos afetam um ou mais dos princípios de segurança da informação: disponibilidade, integridade, confidencialidade e, em alguns casos, inclui-se a autenticidade. Todos esses princípios são vulneráveis a determinados tipos de ataques e a gestão de riscos atua com a intenção de diminuir a probabilidade de ocorrência de danos ou prejuízos decorrentes destes ataques. Vale destacar Ulrich e Nobre [101], que escreveram artigo em que salientam os ataques cibernéticos a drones baseados nos princípios de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade.

### 3.3.1 Confidencialidade

Confidencialidade significa que os dados não serão vazados para usuários não legítimos [102]. O invasor se disfarça de usuário legítimo e obtém acesso à rede *internet of drones* (IoD) na falsificação de identidade. O acesso não autorizado acontece quando algum usuário não autorizado obtém acesso à rede IoD com as credenciais de outros usuários.

*Eavesdropping* ou Intromissão é um ataque típico contra a confidencialidade e consiste na interceptação de dados/informação mediante a captura de pacotes (*packet sniffers*) que monitoram o tráfego próximo a uma IoD [103].

Os invasores podem direcionar o tráfego e roubar os dados por meio da análise de tráfego, uma vez que os pacotes contêm várias informações como localização, tipo de sensor, endereço MAC e os dados capturados pelos sensores [104]. Os dados criptografados também podem ser coletados e, se descriptografados, toda a rede pode ser comprometida. Mesmo que os dados não sejam descriptografados, a análise de tráfego pode obter metadados importantes, como a localização do sensor que transmite os dados [105].

### 3.3.2 Integridade

Integridade significa que os dados devem estar intactos e precisos. A transferência de dados não deve ser alterada entre o caminho do remetente para o destinatário [106]. A substituição/alteração de informações significa acrescentar informações erradas/falsas/ou novas na mensagem original. A partir desse conceito surgem algumas possibilidades de ataques contra esse princípio, descritos a seguir.

A modificação do controle de acesso é a modificação das regras básicas da rede IoD. O ataque de alteração implica na alteração não autorizada dos dados. A técnica *Man-in-the-middle*, onde um fluxo de rede é interceptado, modificado e retransmitido é um exemplo clássico deste tipo de ataque. A introdução de vírus, que alterem dados críticos de modo a realizarem alguma ação maliciosa é outro exemplo citado por Goodrich e Tamassia [103]. Todos os dados provenientes do sensor podem ser visualizados/alterados pelo invasor e todos os dados provenientes do IoD para o sensor também podem ser vistos e alterados. A falsificação de mensagens significa que as mensagens de solicitação de *login* e outros dados confidenciais são forjados a partir das tentativas anteriores de se conectar ao IoD.

### 3.3.3 Disponibilidade

Disponibilidade significa que os serviços de IoD estão disponíveis quando necessário, ou sempre disponíveis. Os ataques físicos ocorrem nos componentes de *hardware* da rede. Os ataques *Denial of Service* (DoS) e *Distributed Denial of Service* (DDoS) realizam a negação dos usuários legítimos de usar os serviços da rede. Esses ataques incluem ataques de negação de serviço (DoS), que consistem em desabilitar uma máquina (ou rede), tornando-a inacessíveis aos usuários pretendidos. Os ataques de roteamento consistem em inundação do servidor e isolamento de nós. Em ataques de repetição, o invasor detecta alguns dados da rede IoD e tenta contornar a segurança enviando solicitações repetidas vezes ao servidor IoD [107].

Já no ataque DDoS uma máquina mestre utiliza máquinas zumbis para realizarem a inundação, que consiste em enviar uma grande quantidade de tráfego para o alvo, a fim de torná-lo incapaz de processar mensagens legítimas [84].

No bloqueio de canal (*jamming*), o invasor interrompe o canal de comunicação, o que caracteriza um típico ataque contra a disponibilidade. Alguns ataques cibernéticos tentam explorar as vulnerabilidades presentes nos protocolos utilizados em redes de comunicação para perpetrar ações maliciosas.

### 3.3.4 Autenticidade

Autenticidade significa que as entidades que participam da relação de comunicação são autênticas e verdadeiras e é estabelecida confiança entre elas. Um clássico ataque de autenticidade é o de desautenticação, quando o invasor desautentica o dispositivo verdadeiro na rede e se autentica como o tal, geralmente por meio de roubo de credencial de acesso [108]. Uma variação deste tipo de ataque é a desautenticação *Wi-Fi*, que consiste em desconectar um usuário do ponto de acesso relativo (WAP). O ataque de *spoofing* em drones caracteriza ação contra o princípio da autenticidade.

Humphreys [109] relata que uma das principais vulnerabilidades cibernéticas no emprego de drones civis encontra-se no enlace de dados porque a comunicação, tanto do sistema de navegação via satélite, quanto por meio de rádio frequência, *Wi-Fi* ou *bluetooth* ocorre geralmente de forma não protegida por criptografia, uma vez que o uso de recursos criptográficos diminui a performance na transmissão de dados, dentre outras considerações de segurança.

A tecnologia *blockchain* pode ser utilizada para garantir segurança e privacidade em drones inteligentes [110]. Yahuza et al. [108] propõem típico modelo de segurança e privacidade baseado em *blockchain* para a rede IoD em três camadas: uma camada de usuário, uma camada de infraestrutura e uma camada IoD. O *blockchain* fornece segurança e privacidade à rede.

Na última década, a análise de ameaças cibernéticas para drones tem sido um domínio de pesquisa desafiador. Quanto as ameaças cibernéticas em relação aos sensores, a maioria dos trabalhos enfoca na segurança de transmissão de dados, mas geralmente ignora a análise de segurança física dos sensores em si, que dependem de um contato com o dispositivo. Além disso, devido a restrições técnicas ou de custos, sensores comerciais em UAV normalmente são conseguem distinguir entre dados normais e anormais [111]. Esta vulnerabilidade facilita o uso de *spoofing* contra os sensores, especialmente os de sistema de navegação.

## 3.4 CONSIDERAÇÕES EM RELAÇÃO AO 5G E 6G

A velocidade de conexão 5G é cerca de 16 vezes mais rápida do que a RF (de 600 Mbit/s no padrão RF de 2.4GHz para 10.000 Mbit/s no padrão 5G) conforme a figura 3.4 [19]. Isso permite o desenvolvimento de sistemas mais seguros contra ataques cibernéticos, uma vez que possibilita o uso de criptografia sem perda significativa de desempenho de conexão.

Além disso, o 5G permite o desenvolvimento da *Internet of Drones* (IoD) [112], estrutura concebida para possibilitar avanços como o controle do tráfego aéreo de baixa altitude (*UAS Traffic Management*-UTM) ou *Urban Space (U-Space)*. Esse espaço compreende altitude de voo abaixo de 400 pés (ft) ou 121.92 metros, normalmente utilizado como parâmetro para limitação de drones comerciais civis [113].

Em relação ao 5G, Marojevic et al. [114] destacam que os sistemas de comunicações móveis 5G mesclam sistemas e serviços de comunicação e rede tradicionalmente separadas para oferecer suporte eficaz a uma gama de aplicativos heterogêneos. Pesquisadores e grupos de trabalho da indústria estão investigando a integração de nós aéreos, técnicas de espectro compartilhado e novas arquiteturas de rede, que estão

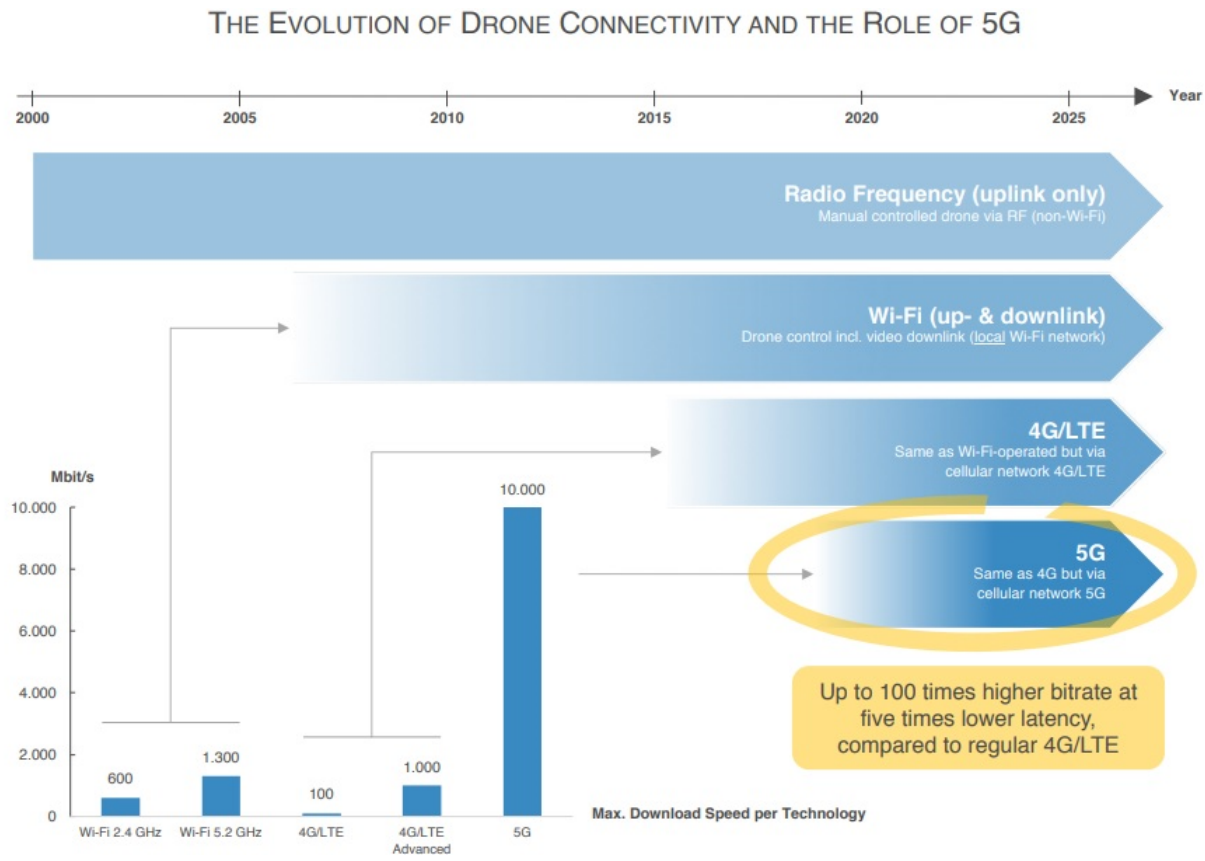


Figura 3.4: Conectividade do 5G [19]

sendo gradualmente introduzidas nos padrões de comunicações.

Outros avanço do 5G foi a possibilidade de coordenação de voos de frotas de drones ou Veículos Conectados e Autônomos (CAVs), onde altas taxas de transmissão de dados, baixa latência e cobertura onipresente permitem que os veículos troquem dados essenciais com o centro de controle e com veículos vizinhos [115].

A conectividade do uso do 5G entre as aeronaves, as entidades de transporte e as de infraestrutura permite Sistemas de Transporte Inteligentes (ITS) que, por sua vez, fornecem uma gama de aplicações, incluindo o gerenciamento de tráfego do *U-Space* [115].

Espera-se que o cenário das futuras redes de acesso 5G possa conectar tudo de forma onipresente e suportar pelo menos 1.000 volumes de tráfego, 100 bilhões dispositivos sem fio conectados e requisitos diversificados de confiabilidade, latência, vida útil da bateria, em oposição às atuais redes celulares de quarta geração (4G). Atualmente, a popularidade da Internet das Coisas (IoT) desencadeou um aumento no número de tráfego de dados móveis para próximas redes sem fio 5G [28].

Segundo Ferreira [116], um aspecto importante no uso da tecnologia 5G para a segurança pública é a escalabilidade, uma vez que a interoperabilidade entre os sistemas de comunicações existentes nas instituições de segurança pública e as redes LTE. Isso porque, como a rede 5G é uma rede heterogênea, ou seja, sua arquitetura é composta por diversas tecnologias incluindo o LTE, ela poderá coexistir com o legado de equipamentos já existentes e em operação pelos órgãos de segurança pública.

O emprego de frotas ou enxames de drone também pode ser realizado a partir do desenvolvimento da tecnologia 5G, como descrito em Grasso e Schembra [117]. Este artigo considerou o problema de suportar um sistema de vigilância por vídeo com pequenos UAVs de baixa altitude, sensores e atuadores que requerem comunicações *Line of Sight* (LOS) para instalações de computação de borda multiacesso (MEC) com propagação em alta velocidade de fluxos de dados de alto volume, possibilitando as transmissões de vídeo ao vivo.

Com a utilização intensa do 5G, os serviços de computação de borda móvel fornecidos por UAVs podem contribuir significativamente para atender às necessidades de processamento de dados de dispositivos IoT, abordando problemas de descarregamento e latência com uso intensivo de computação [118].

De acordo com Abdelmaboud [112], no futuro, a demanda por imagens/vídeos de alta resolução em indústrias verticais e a necessidade de suporte a vídeo HD 4K/8K exigirá uma taxa de dados de nível Gbps mais alta do que o padrão 5G. A transmissão de imagem/vídeo em HD estenderá drasticamente a aplicação dos drones em vários cenários, incluindo o da Inteligência de Segurança Pública.

A segurança cibernética do 5G é um grande desafio porque, com o aumento do uso intensivo de dados e dos aplicativos em tempo real, a privacidade dos dados e os requisitos de segurança também devem ser reforçados [119].

A tecnologia de comunicação 6G operará em frequência de *Terahertz* (THz) para obter uma taxa de transmissão de dados de 1 *Terabits* por segundo (Tbps). A tecnologia 6G promete fornecer alta qualidade de serviços (QoS) e os parâmetros incluem alta taxa de transmissão de dados, banda larga móvel extremamente confiável e aprimorada (FeMBB), comunicação de baixa latência (ERLLC), comunicação de longa distância e alta comunicações de mobilidade (LDHMC) comunicações tipo máquina ultramassivas (umMTC) e comunicações de energia extremamente baixa (ELPC)[120].

O 6G permitirá a Internet de Tudo (*Internet of Everything* - IoE), o que também afetará muitas tecnologias e aplicativos. Com a combinação da tecnologia de comunicação IoE e 6G, muitas aplicações irão aumentar exponencialmente no futuro próximo e, uma delas, será a dos UAV. A tecnologia de comunicação móvel 6G é uma das áreas de pesquisa mais proeminentes e, como tecnologia disruptiva, mudará nossa percepção sobre estilo de vida, sociedade e negócios. Visto que há evidências de que a cada década há uma geração móvel, espera-se que o 5G atenda de 2020 a 2030, o 6G atenda de 2030 a 2040. A Internet das Coisas (*Internet of Things* - IoT) será redefinida como IoE, que possibilitará o advento de novas tecnologias. Alguns países já iniciaram projetos na tecnologia de comunicação 6G, particularmente, Finlândia, EUA, Coréia do Sul, China e Japão [121].

A aplicaçao mais viável relativa aos UAV, no contexto do 6G, é no gerenciamento de tráfego aéreo, uma vez que, nas próximas décadas, o espaço aéreo das grandes cidades tornar-se-á congestionado, o que eleva a preocupação com a segurança de voo. Além disso, poderá possibilitar a construção de aeronaves autônomas baseadas em Inteligência Artificial [122].

Ao final deste capítulo são apresentados *surveys* e *reviews* mais importantes encontrados no domínio *Google Scholar* acerca de comunicações e ataques cibernéticos em UAV. Foram consideradas como contribuições relevantes os artigos com mais de 100 citações até novembro de 2022.

Tabela 3.3: Tabela sobre *surveys* tratando de comunicações em UAV adaptado e ampliado de [28]

| **Publicação** | **Sentença pesquisada** | **Citações** |
|---|---|---|
| Hayat et al.[123] | A survey of the characteristics and requirements of UAV networks | 1074 |
| Gupta et al. [124] | A survey on the main issues in UAV communications networks | 1688 |
| Motlagh et al. [125] | A comprehensive survey on UAVs-based IoT services | 707 |
| Krishna et al. [97] | A review on cybersecurity for UAVs | 159 |
| Jiang et al. [126] | A survey of routing protocols for UAVs | 134 |
| Khawaja et al. [127] | An overview of air-to-ground propagation channel modeling | 464 |
| Khuwaja et al. [128] | Measurement methods proposed for UAV channel modeling | 551 |
| Lu et al. [129] | Review of wireless charging techniques for UAVs | 177 |
| Cao et al. [130] | Overview of airborne communication networks | 228 |
| Mozaffari et al. [131] | A comprehensive tutorial on the use of UAVs in wireless networks | 1625 |
| Altawy et al. [72] | Security, privacy, and safety aspects of civilian drones: A survey | 293 |
| Yaacoub et al. [73] | Security analysis of drones systems: Attacks, limitations, and recommendations | 250 |
| Ezuma et al. [92] | Detection and classification of UAVs using RF fingerprints | 112 |
| Hartmann et al.[106] | The vulnerability of UAVs to cyber attacks | 259 |
| Li et al. [28] | UAV communications for 5G and beyond: Recent advances and future trends | 773 |

# 4 CONCEITOS E BACKGROUNDS

## 4.1 ASPECTOS LEGAIS NA UTILIZAÇÃO DE RPA

Os Órgãos de Segurança Pública (OSP), segundo artigo nº 144 da Constituição Federal de 1988 (CF/88) são: Polícia Federal, Polícia Rodoviária Federal, Polícia Ferroviária Federal, Polícias Civis, Polícias Militares, Corpo de Bombeiros Militares dos estados e Polícias Penais (nível federal, estadual e distrital). Como atividade típica de Estado, que zela pelo emprego moderado da violência para fins de manutenção da ordem pública e paz social, estas instituições buscam aprimorar sua capacidade operacional de forma a oferecer à sociedade brasileira um serviço público de melhor qualidade.

O Sistema Brasileiro de Inteligência (SISBIN) foi criado por meio da lei nº 9.883, de 07 de dezembro de 1999. O decreto nº 4.376, de 13 de setembro de 2002, elencou os órgãos pioneiros do SISBIN. Inicialmente composto por 22 órgãos, o SISBIN atual (2022) é composto por 48 órgãos. Além disso, é possível o intercâmbio de dados com outros órgãos, com a celebração de Acordos de Cooperação Técnica (ACT). Abaixo da estrutura macro do SISBIN, existem subsistemas de inteligência, entre eles, coadnunando-se ao propósito desta dissertação, destaca-se o Subsistema de Inteligência de Segurança Pública (SISP), com seus normativos legais.

O Brasil, em 21 de dezembro de 2000, por meio do decreto n.º 3.695, oficializou em âmbito nacional a criação do SISP dentro do SISBIN, definindo que o SISP tem por finalidade coordenar e integrar as atividades de inteligência de segurança pública em todo o país, bem como suprir os Governos Federal, Estaduais e Distrital de informações que subsidiem a tomada de decisões neste campo. Dentro da estrutura do Ministerio da Justiça e Segurança Pública (MJSP), a Secretaria de Operações Integradas (SEOPI), representada pela Diretoria de Inteligência (DINT), atua como órgão central do SISP.

A Política Nacional de Inteligência de Segurança Pública (PNISP), decreto nº 10.777, de 24 de agosto de 2021 [132] é o documento orientador da Inteligência de Segurança Pública (ISP) de nível federal. Este normativo estabelece os pressupostos, os objetivos, os instrumentos e as diretrizes a serem observadas no âmbito do SISP. Entre uma de suas diretrizes consta: “Fomentar o compartilhamento de informações com o Sistema Brasileiro de Inteligência”.

De acordo com a Doutrina Nacional de Inteligência de Segurança Pública (DNISP), a Inteligência de Segurança Pública (ISP) assessora o processo decisório, por meio da produção de conhecimentos, nos níveis tático, operacional, estratégico e político, o qual tem a finalidade de assessorar o planejamento e o desenvolvimento das políticas de Segurança Pública.

Dentre outros, a PNISP apresenta os conceitos de inteligência e de contrainteligência. A **Inteligência de Segurança Pública** é definida como:

> "A atividade especializada que visa a produção de conhecimentos para assessoramento das autoridades de segurança pública competentes de forma a subsidiar o processo decisório das ações de planejamento e execução das políticas de segurança pública".

Já a **Contrainteligência de Segurança Pública** é designada como:

> "A atividade especializada que visa à prevenção, detecção, neutralização e obstrução de ações adversas que constituam ameaças à consecução das ações da Inteligência de Segurança Pública".

A contrainteligência é a atividade que visa proteger áreas, instalações, documentos, materiais e, principalmente, as pessoas que trabalham na ISP.

Além disso, a PNISP elenca as ameaças inerentes à ISP: 1. criminalidade violenta; 2. criminalidade organizada; 3. corrupção; 4. lavagem de dinheiro e evasão de divisas; 5. ações contrárias à segurança pública no espaço cibernético; 6. ações contrárias ao Estado Democrático de Direito; 7. desastres de causas naturais ou tecnológicas com impacto na segurança pública; e 8. ações contrárias à segurança de infraestruturas críticas com impacto na segurança pública.

Já a Estratégia Nacional de Inteligência de Segurança Pública (ENISP), decreto nº 10.778, de 24 de agosto de 2021 [133] tem o propósito de compreender o ambiente estratégico onde está inserido o SISP e de propiciar as escolhas corretas e necessárias para defender a sociedade e o Estado por meio de ações que irão contribuir com a prevenção e a repressão de crimes, e com o acompanhamento de fenômenos sociais de interesse da segurança pública. A ENISP determina a Missão, os Objetivos, os Valores, o Ambiente Estratégico, os Desafios, os Eixos Estruturantes e os Objetivos Estratégicos da ISP.

A legislação reguladora do emprego de RPA foi atualizada em junho de 2020, marco da permissão do emprego sistemático deste novo tipo de aeronave pelos órgãos públicos. A legislação brasileira que regula a utilização de drones fica a cargo da Agência Nacional de Aviação Civil (ANAC), juntamente com a Agência Nacional de Telecomunicações (ANATEL) e o Departamento de Controle do Espaço Aéreo (DECEA), órgão central do Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB).

Atualmente, os drones existentes são divididos em três categorias: drones de rotor único, asa fixa e multi-rotores. Drones de rotor único: os drones desta categoria possuem uma hélice e apresentam dimensões reduzidas. Drones de asa fixa: o *design* desta categoria é muito parecido ao *design* das aeronaves habituais, onde há um corpo central e duas asas fixas, com apenas uma hélice para impulsionar. Drones multi-rotores: esta categoria possui diversos rotores para movimentar as hélices e manobrar o aparelho. É a categoria mais usada comercialmente.

No Brasil, a ANAC categorizou os RPAs quanto ao peso da aeronave, cada categoria exigindo certos requisitos para a utilização dos equipamentos. Na classe 1 (peso maior que 150kg) as aeronaves devem ser certificadas pela ANAC, devem ser incluídas no Registro Aeronáutico Brasileiro (RAB) e os pilotos devem possuir Certificado Médico Aeronáutico (CMA), licença e habilitação, e todos os voos devem ser registrados.

Para a classe 2 (peso menor ou igual a 150kg e maior que 25kg) as aeronaves não precisam ser certificadas, mas os fabricantes devem observar os requisitos técnicos exigidos e ter o projeto aprovado pela ANAC, também devem ser registradas no RAB e pilotos têm que possuir CMA, licença e habilitação, e todos os voos deverm ser registrados. E, por fim, a classe 3 (peso maior que 250 gramas e menor ou igual a 25kg) se operados até 400 pés acima do nível do solo (aproximadamente 120 m) e em linha de visada

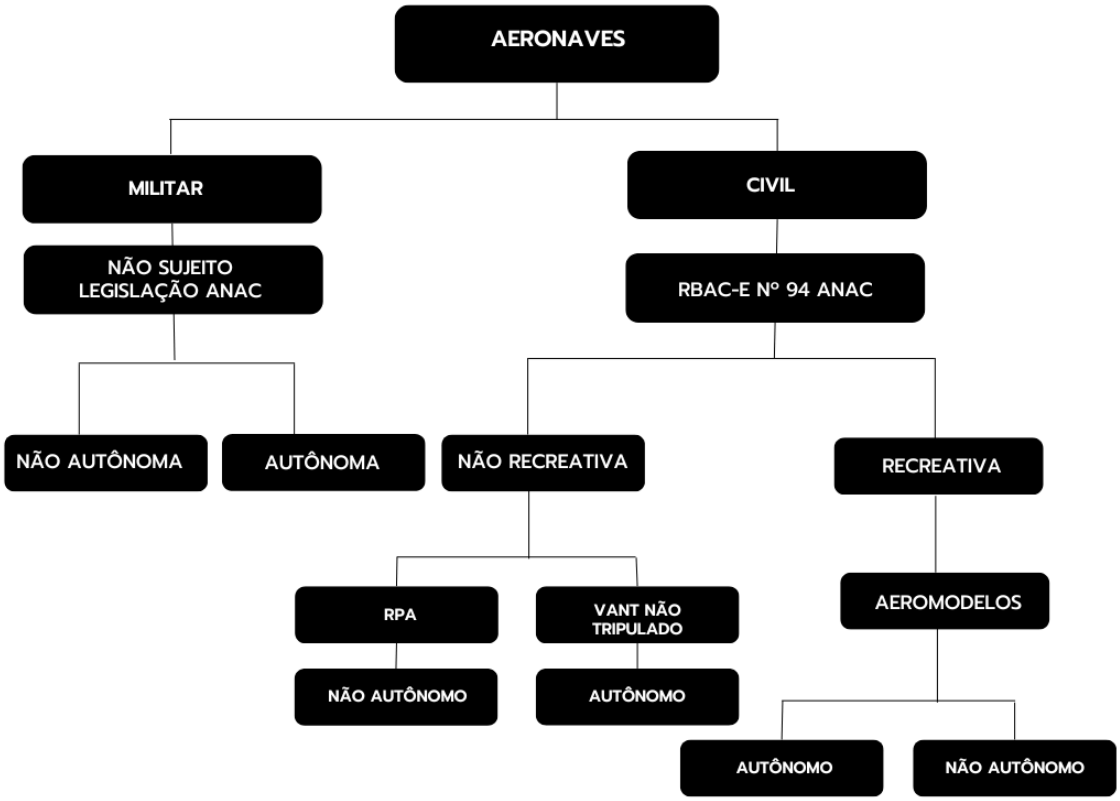


Figura 4.1: Organograma de Aeronaves adaptado de [20]

que permita acompanhamento visual, devem ser apenas cadastrados (apresentação de informação sobre o operador e o equipamento), não será requerido CMA nem será necessário registrar os voos.

A figura 4.1 ilustra as classificações das aeronaves segundo a legislação brasileira. A tabela 4.1 estabelece a diferenciação dos requisitos exigidos para cada classe de drone estipulados pela ANAC.

Tabela 4.1: Tabela de requisitos para operação segundo classes de RPA [29]

| **Requisito** | **Classe 1** | **Classe 2** | **Classe 3** |
|---|---|---|---|
| Idade mínima de 18 anos | sim | sim | sim |
| Necessidade de cadastro | não | não | sim |
| Necessidade de registro | sim | sim | não |
| Necessidade aprovação projeto | não | sim | sim |
| Necessidade processo certificação | sim | não | não |
| Necessidade Certificado Médico Aeronáutico | sim | sim | não |
| Necessidade de licença e habilitação | sim | sim | apenas acima de 400 pés |
| Necessidade registro dos voos | sim | sim | não |
| Apólice de seguro | sim | sim | sim (OSP estão dispensados da obrigação) |
| Placas de identificação | sim | não | não |

Quanto ao uso de RPA recreativa, ela é denominada ‘aeromodelo’. Já a ‘Aeronave Autônoma’, uma

vez programada, não aceita, de forma proposital, a interferência alheia no decorrer do voo. Salienta-se que este modo de operação de aeronave é proibido no território nacional.

Por fim, importante destacar o manual MCA 56-4/2020 [134], do Comando da Aeronáutica, que tem por finalidade regulamentar os procedimentos e responsabilidades necessários para o acesso ao Espaço Aéreo Brasileiro por aeronaves não tripuladas (RPAs), com uso exclusivamente destinado as operações em proveito dos Órgãos de Segurança Pública (OSP), da Defesa Civil (DC) e de Fiscalização da Receita Federal do Brasil (RFB). As ações de inteligência são citadas dentre as ações típicas de segurança pública expostas neste normativo, entretato o referido manual não fez menção à ABIN, o que pode ser interpretado como uma oportunidade de melhoria neste normativo.

No Brasil, compete ao Departamento de Controle de Tráfego Aéreo (DECEA) legislar sobre a utilização do espaço aéreo nacional. O órgão responsável pelo cadastro e controle de pilotos e de aeronaves remotamente pilotadas é a ANAC. Segundo essa Agência, é obrigatória a identificação de todas as RPAs de peso de decolagem superior à 250 gramas com a respectiva vinculação a um Cadastro de Pessoa Física (CPF) ou Cadastro Nacional de Pessoa Jurídica (CNPJ) válido no Brasil. O terceiro órgão de controle da atividade de drones no Brasil é a Agência Nacional de Telecomunicações (ANATEL), uma vez que os drones devem ser homologados por esta agência por serem emissores de radiofrequência.

A legislação, desenvolvida pelo DECEA, que abarca as regras para o acesso ao espaço aéreo é a ICA 100-40. Nela, estão relacionadas, entre outros itens, as regras relativas ao uso em geral e à solicitação de autorização de voo para drones no País. Para tanto, o DECEA criou um site especialmente dedicado ao assunto. O Portal DRONE/UAS [135] reúne documentações, informações, orientações e serviços aos pilotos de drone. As solicitações de autorização de voo de drone no País também podem ser realizadas no portal, por meio do acesso ao sistema SARPAS.

A atividade de aerolevantamento é regulada pelo decreto-lei nº 1.177/1971, decreto nº 2.278/1997 e portaria nº 3726/2020 do Ministério da Defesa (MD). Para a realização do aerolevantamento é necessária Autorização de Voo do Ministério da Defesa (AVOMD). A tabela 4.2 apresenta resumo das principais normas brasileiras abordando RPAs em proveito da atividade de inteligência.

Tabela 4.2: Legislação aplicável à utilização de drones para fins de Inteligência

| **Órgão** | **Legislação** | **Ano** | **Finalidade** |
|---|---|---|---|
| BRASIL | LEI 9.883 | 1999 | Institui o Sistema Brasileiro de Inteligência - SISBIN |
| BRASIL | DECRETO 3.695 | 2000 | Institui o Subsistema de Inteligência de Segurança Pública - SISP |
| DECEA | RESOLUÇÃO 236 | 2016 | Criação do Sistema de Solicitação de Acesso de RPA (SARPAS) |
| ANAC | RBAC-E nº 94 | 2017 | Regulamento Brasileiro de Aviação Civil Especial |
| ANAC | RESOLUÇÃO 419 | 2017 | Criação do Sistema de Aeronaves Não Tripuladas (SISANT) |
| ANATEL | RESOLUÇÃO 715 | 2019 | Regulamento de Homologação de Produtos para Telecomunicações |
| DECEA | ICA 100- 40 | 2020 | Sistemas de RPA e Acesso ao Espaço Aéreo Brasileiro |
| FAB | MCA 56/4 | 2020 | Uso RPA em proveito dos OSP, da Defesa Civil e Fiscalização da RFB |
| BRASIL | DECRETO 10.777 | 2021 | Institui a Política Nacional de Inteligência de Segurança Pública |
| BRASIL | DECRETO 10.778 | 2021 | Institui a Estratégia Nacional de Inteligência de Segurança Pública |

## 4.2 ASPECTOS DOUTRINÁRIOS DE INTELIGÊNCIA

O Brasil é um país que apresenta altos índices de criminalidade. Segundo o relatório do Fórum Brasileiro de Segurança Pública em sua edição de 2022 [136], o Brasil representa apenas 2,7% da população mundial, mas concentra 20,4% dos homicídios do planeta. Em 2021 foram registrados 47.503 homicídios no Brasil. Neste contexto, os crimes violentos, o tráfico de drogas e o crime organizado apresentam-se como ameaças para a segurança da sociedade e a atividade de Inteligência é de fundamental importância para o assessoramento das autoridades decisoras na implementação de políticas públicas de segurança. Dessa forma, faz-se necessário delimitar alguns conceitos da área de Inteligência sob o ponto de vista brasileiro.

A Atividade de Inteligência tem por finalidade precípua o assessoramento do tomador de decisões, sendo esse seu produto final, ao passo que na Investigação Policial o objetivo é a persecução penal, a qual se dá pela produção probatória, pela apuração da autoria e da materialidade da infração penal, sendo portanto uma atividade de natureza executiva e não consultiva, como a Atividade de Inteligência.

A ostensividade dos OSP prejudica a ação de inteligência nos levantamentos de dados para produção de conhecimento. Daí a importância das operações de inteligência serem furtivas e de haver a compartimentação entre as atividades de policiamento ostensivo e de Inteligência. Em razão de sua natureza sigilosa, o emprego de operações de Inteligência requer pessoal especializado, planejamento detalhado e execução cuidadosa.

O arcabouço jurídico para atuação dos Órgãos de Inteligência é precário no Brasil, o que inviabiliza ações operacionais mais efetivas e fragiliza a segurança dos agentes. A utilização de documentos vinculados, por exemplo, é uma demanda legitima que aumentaria o grau de proteção dos agentes de Inteligência e a devida proteção do Estado para a segurança dos agentes ou de seus familiares. Não podemos olvidar do risco inerente à atividade de Inteligência, sobretudo quando se trabalha contra Organizações Criminosas de alta periculosidade.

Operações de Inteligência de Segurança Pública se referem àquelas atividades que buscam obter dado negado, ou seja, informação relevante e que não está disponível. O dado negado vem a ser aquele dado que, devido à sua sensibilidade, encontra-se protegido pelo seu detentor. Para a obtenção desses dados são empregadas as técnicas operacionais. Dentro do escopo deste trabalho podemos citar a Vigilância e o Reconhecimento como as técnicas mais usuais para o emprego de drones.

A Vigilância é a manutenção de um alvo (pessoa, viatura, embarcação, área ou instalação) sob observação contínua. Tudo isso com os seguintes objetivos: levantar dados sobre um alvo; localizar e identificar pessoas, veículos ou objetos; averiguar atividades e contatos dos alvos; controlar o alvo; observar atividades e rotinas de pessoas, instalações/áreas; e buscar, checar, confirmar ou refutar informes [57].

Já para o Reconhecimento vale aquela máxima: "uma imagem vale mais do que mil palavras". A riqueza de detalhes de uma imagem com boa resolução é fundamental para um relatório de Reconhecimento. Esta técnica consiste em uma ação preparatória que visa levantar a maior quantidade possível de dados sobre o ambiente operacional (normalmente uma área geográfica específica). As imagens, os vídeos, a presença de pessoas, o comportamento das pessoas, as vias de acesso, as entradas e as saídas do local, a presença de segurança e as informações de redes sociais são alguns exemplos de itens que devem constar

num relatório de Reconhecimento.

Segundo a Doutrina Nacional Inteligência de Segurança Pública (DNISP – 2016), a Inteligência de Segurança Pública (ISP) possui 5 divisões: 1ª - visa a produção de provas em inquérito ou investigação policial ou assessoramento para formulação de Políticas de Segurança Pública, que seriam atribuições mais afetas ao trabalho da Polícia Federal e das Polícias Civis Estaduais; 2ª - a previsão de acontecimentos que possam trazer consequências negativas para a ordem pública, a incolumidade das pessoas e do patrimônio ou assessoramento para formulação de Políticas de Segurança Pública, que seriam atribuições precípuas das Polícias Militares Estaduais; 3ª - avaliação e acompanhamento de ameaças reais ou potenciais na esfera da Segurança Pública e da Segurança Nacional, no âmbito das rodovias e estradas federais e estaduais, que são missões específicas da Polícia Rodoviária Federal e das Polícias Rodoviárias Estaduais; 4ª - acompanhamento e avaliação de ameaças reais ou potenciais na esfera do Sistema Penitenciário, que são atribuições do Departamento Penitenciário Federal e dos Institutos Penitenciários Estaduais; 5ª - previsão, prevenção e neutralização de riscos referentes a desastres naturais e de causa humana, calamidades, a ordem pública, a incolumidade das pessoas e do patrimônio ou assessoramento para formulação de Políticas de Segurança Pública, missão atribuída aos Bombeiros Militares Estaduais.

As Unidades da Federação podem criar sistemas de inteligência de segurança pública locais, os quais se comunicam com o SISP por meio do canal técnico de inteligência para buscar a troca de dados, informações e conhecimentos.

Uma iniciativa recente do Ministério da Justiça e Segurança Pública (MJSP), que visa dar mais efetividade ao SISP, foi a implantação de Centros Integrados Regionais de Segurança Pública. Ao todo são 5 Centros Integrados de Inteligência de Segurança Pública (CIISP), cada um localizado numa região geográfica do país e, dentro de sua estrutura, comportando representantes dos sistemas de inteligência das Unidades da Federação da região considerada.

## 4.3 SISTEMAS DE CONTROLE DE DRONES NO BRASIL

Para que haja controle efetivo das atividades com RPAs no Brasil, o DECEA e a ANAC operam dois sistemas integrados, que devem ser acessados por aqueles que realizam o emprego de drones, cada um com objetivos diferentes, mas complementares e interdependentes.

### 4.3.1 SARPAS

O SARPAS (Solicitação de Acesso de Aeronaves Remotamente Pilotadas) foi concebido com o objetivo de facilitar a solicitação de acesso ao Espaço Aéreo para o uso de Sistemas de Aeronaves Remotamente Pilotadas (RPAS/DRONES) no espaço aéreo brasileiro. Para isso, é necessário o cadastro do piloto no sistema, bem como das aeronaves e das empresas ou instituições pretendentes dos voos.

A primeira versão do SARPAS entrou em vigor em 2016 e foi aperfeiçoada em julho de 2022, quando o DECEA lançou a segunda versão, denominada de sistema SARPAS NG [137], um sistema mais aprimorado para o usuário solicitar voo de drones. Para o lançamento do novo sistema foram realizadas audiências

públicas com empresas aéreas, fabricantes de UAV, usuários e com o público em geral a fim de coletar dados e ideias para o aprimoramento do compartilhamento seguro do espaço aéreo entre aeronaves tripuladas e drones.

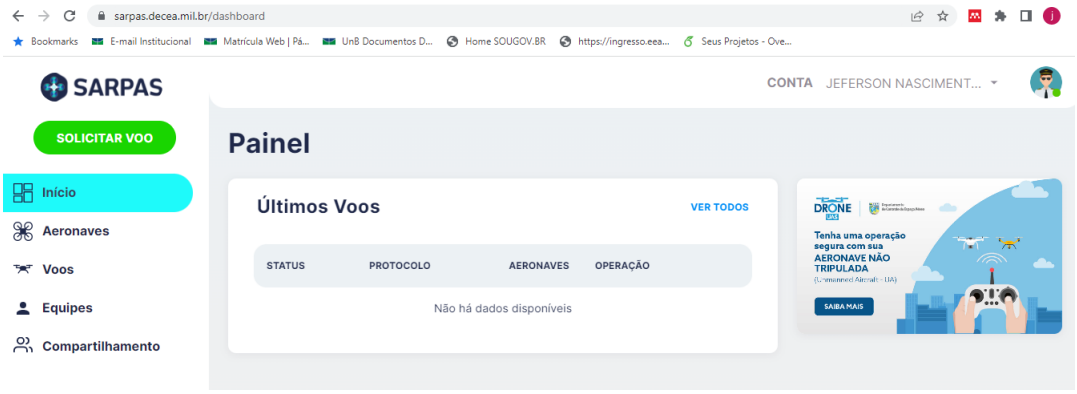


Figura 4.2: Dashboard SARPAS 2022 [21]

As novas funcionalidades possibilitam mais praticidade durante o uso do sistema. A primeira mudança significativa é a viabilidade do uso de *login* e senha únicos do Governo Federal, cadastrados no site www.gov.br. Outra novidade importante é a relação entre Pessoas Físicas e Jurídicas. Com o SARPAS NG, todo CNPJ vai ter um responsável Pessoa Física para gerenciar a conta, possibilitando que as instituições interessadas sempre tenham um elo com o sistema, o que corrobora o rastreamento e o controle das ações.

Além do SARPAS, o DECEA mantém um site especializado com atualizações sobre a legislação, vídeos e dicas úteis de segurança para o emprego de RPAs. Drones são, antes de tudo, aeronaves. Assim, a partir do momento que alguém decola uma aeronave deste gênero, torna-se, sob o ponto de vista legal, um piloto. A partir daí, passa a responder pelos direitos, deveres e penalidades previstos, não só na legislação referente ao voo de drones, como também nas demais que lhe dizem respeito diretamente, como o Código Brasileiro de Aeronáutica, além de responder indiretamente por outros delitos conexos praticados e previstos no Código Penal.

Para solicitação de voos no SARPAS, é obrigatório o registro prévio da RPA no SISANT, uma vez que os sistemas se comunicam e fazem a relação entre o voo solicitado e a aeronave cadastrada [30].

### 4.3.2 SISANT

O Sistema de Aeronaves não Tripuladas (SISANT) foi instituído pela ANAC por meio da resolução nº 419 em 2017 [138]. O cadastro no SISANT é obrigatório para as aeronaves não tripuladas de uso recreativo (aeromodelo) ou não recreativo (RPA), com peso máximo de decolagem superior a 250g. O referido sistema tem priorizando o uso gratuito, o caráter declaratório e os processos automáticos e instantâneos.

Tabela 4.3: Número de drones cadastrados no Brasil - SISANT 2022 [22]

| ANO | DRONES CADASTRADOS |
|---|---|
| 2017 | 30087 |

*Continua na próxima página*

Tabela 4.3 – *Continua página anterior*

| ANO | DRONES CADASTRADOS |
|---|---|
| 2018 | 59491 |
| 2019 | 79671 |
| 2020 | 79256 |
| 2021 | 90030 |
| 2022 | 93729 |

A título de comparação, o número de drones registrados nos EUA, em setembro de 2022, era de 861.669 [37].

O novo SISANT, que começou a ser introduzido em maio de 2022, traz novas funcionalidades e serviços para os usuários, tais como: realizar a transferência de equipamentos diretamente no sistema; cadastrar drones para uso avançado e emitir Certificado de Aeronavegabilidade Especial de RPA (CAER). Além disso, o novo SISANT foi concebido para suportar os desafios do futuro com possibilidade de agregar novas funções e informações como, por exemplo, aquelas que serão requeridas nos espaços aéreos UTM (*Unmanned Aircraft System Traffic Management*).

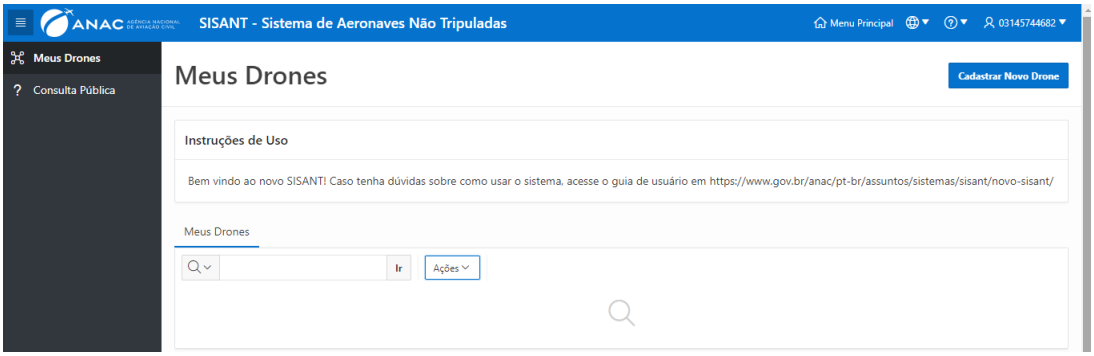


Figura 4.3: Dashboard SISANT 2022 [22]

Como conclusão deste capítulo pode-se afirmar que o Brasil apresenta uma regulamentação especial para veículos aéreos não tripulados que se coaduna às premissas básicas da Organização da Aviação Civil Internacional (ICAO). Isso se dá por meio das regras previstas no Código Brasileiro de Aeronáutica (CBA), na ANAC, compondo o Regulamento Brasileiro da Aviação Civil Especial nº 94 para os Veículos Aéreos Não Tripulados e Aeromodelos.

Em que pese a consonância brasileira, o ideal é que houvesse uma homogeneidade de normas internacionais, à semelhança ao que ocorre na aviação comercial, uma vez que a segurança do espaço aéreo é influenciada cada vez mais pelo uso intensivo dos drones. O descompasso normativo internacional é prejudicial tanto para a segurança aeronáutica, quanto para o mercado, pois os fabricantes devem buscar a produção de aeronaves homogêneas e que atendam ao maior número de países possível.

Após a explanação dos principais conceitos e trabalhos relacionados, a busca pela inovação nos conduz à Seção 5 que apresentará a discussão acerca do estudo proposto sobre o emprego de Aeronaves Remotamente Pilotadas.

# 5 DISCUSSÃO

## 5.1 VANTAGENS E DESVANTAGENS PARA USO DE RPA EM ISP

Como descrito nos trabalhos relacionados, uma das características que diferem o drone de uma aeronave tripulada é sua pequena assinatura radar. Em sua construção são combinados materiais e formas geométricas que reduzem a reflexão das ondas eletromagnéticas emitidas pelo radar, além de terem normalmente pequenas dimensões em relação as aeronaves convencionais.

A figura 5.1 ilustra as razões para uso de drone, segundo consultoria especializada: melhorar qualidade, melhorar segurança, ganhar tempo e diminuir custos.

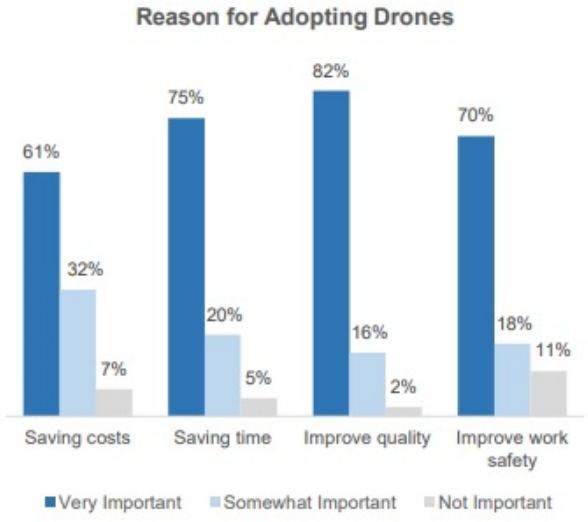


Figura 5.1: Razões para uso de drones [23]

Além da redução dos custos de operação, quando comparados às aeronaves tripuladas, a utilização das RPA traz a possibilidade de monitoramento de atividades ilícitas em tempo real ou em áreas onde o voo tripulado pode representar um risco à tripulação, o que torna esse instrumento uma excelente alternativa para a área de segurança e defesa, abrindo novas perspectivas para o monitoramento de ilícitos ambientais em áreas de difícil acesso.

A qualidade das imagens obtidas pelos sensores embarcados nos SARP também irá depender da altitude de voo da aeronave. Quanto mais baixo operar o vetor, mais detalhes terão as imagens, entretanto o sigilo da operação pode ser comprometido pelos ruídos produzidos. Estes fatores deverão ser analisados pelo chefe da missão.

Agregado a isso, a quantidade de horas de formação inicial do piloto e de treinamento continuado é reduzida, pois os equipamentos contam com sensores e inteligência artificial que facilitam a pilotagem e diminuem os riscos envolvidos nos voos. Os custos para obter a habilitação para pilotar aviões e helicópte-

ros é de aproximadamente R$300.000,00 (trezentos mil reais), devido principalmente ao nível necessário de conhecimento e treinamento, enquanto o custo de habilitação para operar drones é de R$500,00 [60].

Em alusão à furtividade, ressalta-se a capacidade das RPA de realizar as missões de forma dissimulada, característica fundamental para as missões de inteligência tratadas neste estudo, devido ao emprego de motores elétricos, os quais reduzem sensivelmente a emissão de ruídos.

Drones podem desenvolver ações chamadas de ***3D - "dull, dirty and dangerous"-*** monótonas, sujas e perigosas, nas quais as tripulações humanas seriam expostas. ***Dull*** refere-se a caracterítica de monotonia, que engloba um voo de longa duração provocando cansaço na tripulação e, por conseguinte, aumento do risco operacional. ***Dirty*** refere-se aos riscos biológicos, contaminação química ou outras situações em que a exposição possa trazer prejuízo à saúde das pessoas, e ***Dangerous*** refere-se a toda e qualquer situação de perigo que pode expor a tripulação, tal como o sobrevoo em áreas dominadas pelo crime organizado, na qual a aeronave pode ser alvo de tiros [139]. Resulta então que a RPA, em relação as aeronaves tripuladas, congrega as vantagens de não ter o ser humano como limitante em vários aspectos.

Por outro lado, o seu emprego é altamente dependente das condições atmosféricas. A ocorrência de nuvens, ventos fortes, nevoeiros e chuvas podem restringir sua utilização. Ademais, a conformação do relevo exerce importante papel no planejamento de emprego desta plataforma. A presença de elevações e de densa vegetação podem limitar o seu alcance a somente 30% (trinta por cento) de sua capacidade máxima, limitando a obtenção de dados, caso opere por visada direta [35].

Há vários desafios técnicos e operacionais no emprego de drones ( interferência de ruídos, baixa autonomia de voo, influência de condições meteorológicas adversas, dificuldades de comunicação devido a visada direta de ondas de rádio de alta frequencia de 2.4 e 5.8 GHZ, etc.). Outra preocupação é o monitoramento do risco para a aviação, quando aeronaves não tripuladas são empregadas próximas a áreas de infraestruturas críticas como aeroportos e aeródromos, além do risco do drone atingir pessoas em solo.

## 5.2 ESCOLHA DE DRONE POR ÓRGÃOS DE SEGURANÇA PÚBLICA

Nos últimos anos têm crescido dentro da área de conhecimento de Pesquisa Operacional a utilização de tomada de decisão por múltiplos critérios - MDCA (*multi criteria decision analysis*) ou também conhecido como MDCM (*multi criteria decision making*) [140], que analisa múltiplos critérios conflitantes na tomada de decisões. Existem cada vez mais métodos propostos que se tornam mais específicos de acordo com o ramo do conhecimento que se queira explorar. Os problemas de MDCA lidam com a seleção, ordenação e priorização de alternativas dentre uma gama de possibilidades de soluções possíveis.

Artigo de Moreira et al. [141] propõe a sistemática PROMETHEE-SAPEVO-M1 de análise multicritérios para avaliação de drones a serem empregados em missões de segurança pública. Esta referida metodologia se baseia em análise de critérios objetivos e subjetivos, bem como determina o peso relativo de cada critério para o desenvolvimento de uma plataforma que os autores definiram como Sistema de Suporte a Decisão (DSS).

Os autores conjugaram o sistema PROMETHEE (*Preference Ranking Organization Method for En-*

*richment Evaluations*), proposta por Brans e De Smet [142]. Estes autores enfatizam que a maioria dos problemas humanos tem a natureza de serem multicritérios e requerem tratamento apropriado. Este método sugere que os multicritérios sejam estabelecidos por meio de informações que possam ser claramente obtidas e entendidas pelos tomadores de decisão e pelos analistas.

Por outro lado, o método SAPEVO-M (*Simple Aggregation of Preferences Expressed by Ordinal Vectors Group Decision Making*) permite que os tomadores de decisão - *Decision Makers* (DM) estabeleçam preferência entre os critérios de acordo com pesos relativos estipulados pelos DM. Além disso, permite procedimento de agregação baseado na comparação paritária, visando expressar as respectivas preferências do DM [143].

A sistemática PROMETHEE-SAPEVO-M1 possibilita estudo eficaz, fornecendo análise de um problema complexo composto de múltiplas variáveis com diferentes naturezas dos dados, possibilitando avaliar os resultados em três modelos de classificação de preferências diferentes, juntamente com uma avaliação intra-critério.

Moreira et al. [141] elencaram como critérios relevantes na escolha de drone: autonomia de voo, resolução das imagens, alcance de utilização, sensores, portabilidade, resistência ao vento/estabilidade, preço e operabilidade. O peso relativo estabelecido para cada critério na fase da avaliação vai depender do tipo de missão a ser executada.

O uso de RPA exige, necessariamente, uma abordagem sistêmica. Para introduzi-las no âmbito das atividades de ISP demanda-se conhecimento e coordenação de outras partes do sistema de segurança pública, sob pena de mal funcionamento, subemprego, perda de eficiência e desperdício de recursos humanos e financeiros.

## 5.3 ESTUDOS DE CASOS

Nesta seção serão abordados ensinamentos colhidos de experiências relatadas na literatura. Como veremos, existem iniciativas por parte de algumas instituições para realizar o emprego de RPA em missões operacionais. Entretanto, o processo de maturação ocorre geralmente por iniciativa de agentes que estão trabalhando na execução das atividades e, muitas vezes, as autoridades decisoras não tem o discernimento do quão relevante é a adição dessas aeronaves no cotidiano das atividades de segurança pública.

Nos EUA, Gettinger [144] catalogou que 1578 agências governamentais de segurança pública utilizavam drones em março de 2020 e a maioria das RPAs utilizadas eram modelos comerciais classe 3, o que sugere pouca especificidade. Uma forma de mitigar esta fragilidade de aquisição de drones foi proposta por Terra [61], ao abordar a questão de Parcerias Público Privadas (PPP) em proveito da Segurança Pública no Brasil . De fato, para uma Unidade da Federação o investimento para adquirir drone de forma customizada é muito elevado. Entretanto, a União poderia firmar parcerias com a iniciativa privada e viabilizar a adesão de contrato com os Estados da Federação, reduzindo custos e fomentando o desenvolvimento da indústria nacional. Além disso, as cláusulas exorbitantes previstas para as contratações públicas ofereceriam maior segurança jurídica e técnica para a sobrevivência de projetos de longo prazo, como no caso de contratos de aquisição e manutenção de aeronaves [61].

Um exemplo da falta de continuidade de projetos estratégicos no uso de RPA ocorreu com o programa SISVANT do Departamento de Polícia Federal. A PF foi pioneira no emprego desta tecnologia para fins de segurança pública no Brasil, que passou a utilizar RPA em 2009, operando o modelo Heron da *Israel Aerospace Industries* (IAI), mostrada na figura 5.2, nas missões de monitoramento de fronteiras em combate ao narcotráfico e repressão aos crimes de contrabando e descaminho. A aeronave possui autonomia de 40 horas de voo e peso máximo de decolagem de 1.150 kg.


Figura 5.2: Aeronave Heron [24]

Em que pese as vantagens operacionais, a questão orçamentária foi a principal barreira de sustentabilidade do projeto de aquisição das duas RPAs pela PF. Mesmo passando por estudos de viabilidade, não foi possível convencer as autoridades decisoras, já em outro mandato governamental, sobre a imprescindibilidade de investimentos para executar o *upgrade* dos equipamentos e ampliar o projeto, levando ao seu encerramento em 2019, com a transferência dos drones para a FAB.

### 5.3.1 Estudo do Caso em Minas Gerais

Em Minas Gerais, Silva [24] realizou pesquisa de utilização de drones em inteligência de segurança pública. Segundo o autor, tudo começou em 2015, quando a Esquadrilha Pégasus iniciou a homologação e o treinamento para operar RPA, após a aquisição de aeronave modelo *Echar 20-B* da empresa Xmobots, uma aeronave remotamente pilotada de asas fixas, adquirida em virtude de solicitação da Diretoria de Meio Ambiente e Trânsito (DMAT). A Polícia Militar de Minas Gerais (PMMG) seguiu tendência verificada em outros órgãos que passaram a usar como vetor aéreo as RPA para cumprimento de missões ambientais em zona rural, até então realizadas por aeronaves tripuladas.

Em seguida, com intuito de realizar levantamentos aéreos em áreas menores e em locais onde não era possível a decolagem da asa fixa, em dezembro de 2017, o Comando de Aviação do Estado de Minas Gerais (ComAvE) adquiriu uma RPA *DJI Phantom 4 Advanced Plus* de asas rotativas para complementar as atividades da asa fixa da DMAT. Esta RPA também passou a ser empregada em atividades policiais, apresentando bons resultados operacionais, mas limitados pela ausência de *zoom* e grande suscetibilidade a interferências em ambientes urbanos.

Após a citada aquisição, foi realizado o primeiro treinamento de pilotos de RPA de asa rotativa do ComAvE. Foram capacitados 11 pilotos, já habilitados a pilotar RPAs de asa fixa da DMAT, o que facilitou

o processo de aprendizagem, pois a aeronave multirotor é de operação mais simplificada.

Gradativamente algumas unidades passaram a incorporar tal inovação, como a 2ª Região da Polícia Militar (RPM), sediada em Contagem/MG, que recebeu 3 (três) RPA *DJI Inspire 1* equipados com a câmera Z3, como doação da Vara de Execuções da Comarca daquele município. O ComAvE recebeu uma delas e passou a empregá-la em complementação as suas atividades, como monitoramento de perímetro urbano com a transmissão ao vivo das imagens para a sala de comando e controle.

Em agosto de 2018, o ComAvE recebeu uma RPA *DJI Matrice 200*, equipamento robustecido que opera com redundância de baterias e sistemas, além de ser resistente a chuva e a poeira. A aeronave veio equipada com câmera que oferece *zoom* de 180 (cento e oitenta) vezes e permite a operação com segurança sobre pessoas e propriedades.

A 10ª RPM, em Patos de Minas/MG, também viabilizou a aquisição de uma *RPA DJI Matrice 200*, equipada com câmera *DJI Zenmuze XT2*, que capta imagens em infravermelho, sendo a primeira câmera deste modelo a ser entregue na América Latina, com o objetivo principal de potencializar a capacidade de localizar criminosos que se homiziem na zona rural.

**Análise risco das operações policiais**

As ações de repressão qualificada ao tráfico de drogas ocorrem com frequência em ambientes com geografia urbana complexa e de difícil progressão, onde os infratores possuem vantagem no conhecimento da área, o que dificulta a aplicação do fator surpresa nas abordagens policiais. Ainda que sejam aplicadas as técnicas policiais adequadas, a atuação nestes locais apresenta maior risco maior do que aquelas realizadas nas áreas das atividades policiais rotineiras.

Estudo detalhado de Silva [24], contabilizado no período entre dezembro de 2017 e novembro de 2018, registrou 85 operações no SARPAS pelo ComAvE. Destas operações, 43 foram objeto de estudo, pois se referiam à realização de levantamentos de ISP para orientar a repressão qualificada ao tráfico de drogas. Destas 43 operações, 14 foram executadas com a RPA *DJI Matrice 200*, equipamento de uso profissional, com autonomia de voo e alcance maiores, além de ser equipada com câmera *zoom* de 180 vezes, características verificadas como necessárias para este tipo de atividade, as outras 29 foram realizadas com a RPA *DJI Inspire 1*, também de uso profissional e equipada com câmera com *zoom*, mas que permite um aumento da imagem de apenas 7 vezes, o que limita sua capacidade de realizar este tipo de levantamento.

Além desses achados, Silva [24] realizou tabulação de resultados de impressão de policiais após a utilização de RPAs. Os resultados são apresentados na tabela 5.1 a seguir:

Tabela 5.1: Contribuição das RPAs nas ações da PMMG - 2018 adaptado de [24]

| Contribuição | Citações | Percentual |
|---|---|---|
| Identificação da rota de fuga de autores e suspeitos durante abordagens | 64 | 86.5% |
| Identificação do local de esconderijo de autores e suspeitos durante abordagens | 59 | 79.7% |
| Identificação do modus operandi de autores de delitos | 53 | 71.3% |
| Maior segurança para a atuação dos policiais durante a repressão qualificada | 52 | 70.3% |
| Identificação do local de esconderijo de drogas possibilitando sua apreensão | 47 | 63.5% |
| Constatação de flagrante delito e consequente prisão do autor | 44 | 59.5% |

*Continua próxima página*

Tabela 5.1 – *Continuação da página anterior*

| Contribuição | Citações | Percentual |
|---|---|---|
| Possibilidade do fator surpresa nas ações, minimizando o tempo de emprego da tropa | 44 | 59.5% |
| Constatação de vinculações criminais | 26 | 35.1% |
| Identificação do local de esconderijo de armas possibilitando sua apreensão | 25 | 33.8% |

No questionário apresentado aos militares havia a possibilidade da escolha de mais de uma opção, daí porque os percentuais ultrapassam 100%.

A percepção geral dos policiais entrevistados permite inferir que o uso de RPA para levantamentos de ISP, a fim de subsidiar a repressão qualificada ao tráfico de drogas, mostrou-se viável, principalmente para identificar a rota de fuga e local de esconderijo dos autores durante as abordagens. Contudo, os questionários também trouxeram luz sobre quais aspectos podem ser melhorados na operação com RPA a fim de se obter melhores resultados e são citados a seguir:

a) possibilidade de compartilhamento de imagem via *link* em tempo real;

b) Melhor estudo da geografia urbana pelo piloto operador da aeronave;

c) Realização de planejamento prévio do local de operação, a fim de identificar se o voo é pertinente naquele momento;

d) Permissão para altitude de voo acima de 120 (cento e vinte) metros em algumas operações;

e) Possibilidade de utilização de uma base para apoio logístico;

f) investimento em RPAs com maior autonomia de voo e câmeras com infravermelho e visão noturna;

Quanto à hipótese secundária de que a RPA é instrumento capaz de coletar imagens que permitem a identificação de ameaças e avaliação do risco nos locais de atuação, o estudo demonstrou que 95,9% dos militares consideram que a RPA auxiliou na avaliação do risco e identificação de ameaças, enquanto que somente 4,1% apontaram que tal tecnologia não fez diferença ou auxiliou com ressalvas esta atividade.

### 5.3.2 Estudo de Caso no Paraná

Oliveira e Fávero [30] publicaram artigo em 2022 analisando o emprego de RPAs na Polícia Militar do Paraná (PMPR). O estudo traz à baila achados que contribuem para melhor entendimento do emprego operacional dessas aeronaves por forças de segurança. Como exemplo deste tipo de utilização, pode-se citar o Batalhão de Polícia Militar de Operações Aéreas do Estado do Paraná (BPMOA/PR), que utilizou drone para dar apoio às equipes de solo numa operação de busca de captura de assaltantes de uma transportadora. O voo ocorreu na noite de 18 de abril de 2022 e a figura 5.3 ilustra as imagens obtidas com drone *Matrice 300 RTK*.

O drone *Matrice 300 RTK* é fabricado pela empresa DJI, líder mundial em fabricação de drones e possui as seguintes funcionalidades embarcadas: câmera com visão noturna (infravermelho), sobreposição de imagens para mapeamento e alto poder de *zoom* acompanhado com controle de estabilidade. Além disso, com este UAS é possível realizar automatização de trajetos e varreduras de grandes áreas.


Figura 5.3: Imagens aéreas noturnas com drone *Matrice 300 RTK* [25]

Figura 5.4: Imagens aéreas noturnas de visão termal com drone *Matrice 300 RTK* [25]

Além disso, o estudo de Oliveira e Fávero [30] trouxe alguns dados numéricos que podem ser analisados no estudo de caso. De forma geral, os dados apontam o uso cada vez mais intenso dessa tecnologia.

Tabela 5.2: Número de pilotos de drones PMPR e CBMPR até agosto 2022 adaptado de [30]

| **CORPORAÇÃO** | **QUANTIDADE** |
|---|---|
| PMPR | 94 |
| CBMPR | 35 |
| **TOTAL** | 129 |

Conforme pode ser observado na tabela 5.3, as capacitações tiveram ciclo de crescimento interrompido devido à pandemia de COVID 2019, entretanto a realização de eventos de instrução voltou a se tornar expressiva a partir de 2021.

Tabela 5.3: Cursos e capacitações realizados na PMPR até agosto 2022 adaptado de [30]

| ANO | EVENTOS DE CAPACITAÇÃO |
|---|---|
| 2018 | 2 |
| 2019 | 1 |
| 2020 | - |
| 2021 | 11 |
| 2022 | 5 |
| **TOTAL** | 19 |

Em relação as ações com RPAs, conforme pode ser visto na tabela 5.4, constatou-se que a pandemia da COVID 2019 não interferiu significativamente, uma vez que o uso de drone prescinde do contato ou da exposição próxima entre as pessoas. A maioria das ações registradas no período pandêmico foram atinentes a ações de Comunicação Social, em detrimento das ações operacionais de combate à criminalidade.

Tabela 5.4: Ações do BPMOA/PR com emprego de RPA até agosto 2022 adaptado de [30]

| ANO | NÚMERO DE AÇÕES |
|---|---|
| 2018 | 8 |
| 2019 | 7 |
| 2020 | 45 |
| 2021 | 41 |
| 2022 | 55 |
| **TOTAL** | 156 |

A leitura da tabela 5.5 expõe o fato de que, apesar da PMPR possuir considerável número de aeronaves remotamente pilotadas em seu acervo, a maioria pode ser considerada com tecnologia ultrapassada. Os seguintes modelos tiveram sua produção descontinuada pela fabricante DJI: *Inspire 1; Mavic Pro; Mavic 2 Pro; Mavic 2 Zoom; Mavic Air; Mavic Mini; Mavic Pro; Spark; Phantom 4; Phantom 4 Pro* e todos os da série *Phantom 3*. Trata-se do constante processo de renovação promovido pelas inovações tecnológicas, o que se constitui num fator complicador para que a metodologia e a doutrina de emprego de RPAs pelos OSP seja mais efetiva.

Tabela 5.5: Modelos de RPA da PMPR até agosto de 2022 adaptado de [30]

| Modelo Aeronave | Quantidade | Percentual |
|---|---|---|
| Spark | 2 | 2.7% |
| Phantom 4 Pro | 4 | 5.3% |
| Phantom 4 | 15 | 20% |
| Phantom 3 Profissional | 5 | 6.7% |
| Phantom 3 Advanced | 5 | 6.7% |
| Phantom 3 | 18 | 24% |

*Continua próxima página*

Tabela 5.5 – *Continuação da página anterior*

| Modelo Aeronave | Quantidade | Percentual |
|---|---|---|
| Mavic Pro | 9 | 12% |
| Mavic Mini | 1 | 1.3% |
| Mavic Air 2S | 1 | 1.3% |
| Mavic Air 2 | 2 | 2.7% |
| Mavic Air | 1 | 1.3% |
| Mavic 2 Zoom | 4 | 5.3% |
| Mavic 2 Pro | 1 | 1.3% |
| Mavic 2 Enterprise Advanced | 3 | 4% |
| Matrice 300 RTK | 1 | 1.3% |
| Inspire 2 | 1 | 1.3% |
| Inspire 1 | 2 | 2.7% |
| **TOTAL** | 75 | 100% |

Importante também destacar que, dentre todas RPAs presentes no patrimônio da PMPR, apenas 4 (5,3% do total) possuem compatibilidade com tecnologia de detecção de calor (câmeras térmicas), presente apenas nos modelos *Matrice 300 RTK* e *Mavic 2 Enterprise Advanced*. Em relação ao recurso de *zoom*, há 12 aeronaves (16% do total) com possibilidade de uso desse recurso, presente nos modelos *Matrice 300 RTK, Inspire 1, Inspire 2, Mavic 2 Zoom, Mavic Air 2S e Mavic 2 Enterprise Advanced*, sendo que nestes dois últimos modelos o recurso é apenas de *zoom* digital e nas demais há possibilidade de *zoom* óptico que aproxima a imagem sem causar nenhuma distorção, o que não ocorre com o *zoom* digital.

Para concluir, as possibilidades de aplicação das RPAs, para otimizar as atividades de responsabilidade da PMPR, são mais limitadas nos modelos mais antigos, quando comparadas com as tecnologias superiores disponíveis em modelos mais modernos.

### 5.3.3 Estudo de Caso Receita Federal do Brasil - RFB

Embora não seja órgão de segurança pública *stricto sensu*, conforme prevê a Constituição Federal, a Receita Federal do Brasil (RFB) tem poder fiscalizatório em área de fronteira e, inclusive, tem respaldo diferenciado para atuação com drones, conforme preceitua o normativo da FAB MCA-56/4 [134]. Uma iniciativa bem sucedida de atuação pela RFB é o projeto Muralha Inteligente - parceria entre a Receita Federal do Brasil e o Parque Tecnológico de Itaipu, em Foz do Iguaçu/PR [145]. O projeto tem por objetivo a busca por soluções tecnológicas inteligentes, que possam atender ao combate ao contrabando e descaminho de mercadorias, de forma mais intensiva em regiões de fronteira. Esta parceria tem possibilitado, ainda, a formação de pilotos de drones de diversos órgãos públicos no estado do Paraná.

Para isso, uma das metas específicas do projeto é a validação de tecnologias de drone multirotor e asa fixa, no apoio a missões da RFB em áreas fronteiriças. Basicamente os drones *M300* e o *Mavic 2 Enterprise Advanced* foram empregados em Operações ISTAR (inteligência, vigilância, aquisição de alvos e reconhecimento). Alguns resultados e evidências são expostos a seguir:

1. **INTELIGÊNCIA** - as RPAs foram empregadas para o levantamento de placas veiculares que circulam com outros alvos (veículos) identificados. As placas foram fotografadas e repassadas para as equipes que trabalham as informações de câmeras OCR, junto com dados sobre as atividades e locais onde são realizadas as atividades ilícitas, que após análise são colocadas no alerta da missão. A partir de uma denúncia, o drone foi posicionado em local seguro e passou a monitorar a atividade ilícita, que foi confirmada posteriormente pelas equipes de busca.

2. **VIGILÂNCIA** - o drone tem capacidade de *zoom* e visão noturna que possibilitou a vigilância de locais onde antes não era possível, seja pela visibilidade ou pela geografia, como nas margens dos rios e lagos. Numa dessas atividades de vigilância em portos clandestinos, os dados do reconhecimento e da inteligência, conduziram a apreensão de veículos carregados com mercadorias contrabandeadas por quadrilhas criminosas.

3. **AQUISIÇÃO DE ALVOS** - os drones foram responsáveis pela localização, identificação e indicação de veículos, que foram apreendidos pelas equipes de busca. Um exemplo interessante de TA (*target acquisition*) foi a identificação de um ônibus por meio do *zoom* ótico.

4. **RECONHECIMENTO** - o drone possibilitou o levantamento aéreo de áreas onde ocorrem os ilícitos. Em uma operação, a RFB auxiliou na operação de busca a um assassino e estuprador. O primeiro trabalho realizado foi o de reconhecimento do local onde o fugitivo havia se homiziado, após troca de tiros com os policiais durante o cumprimento de um Mandado de Prisão. As equipes de drones se revezaram no reconhecimento da mata, rios e campos da zona rural onde o criminoso havia se escondido, levantando informações sobre o local.

5. **OPERAÇÕES CONJUNTAS** - os drones da RFB em Foz do Iguaçu/PR têm possibilitado realização de operações com outras forças de segurança, tais como a operação Ágata e a Caça ao Novo Cangaço. É notório o incremento em qualidade e em quantidade de informações e de apreensões por conta da sua capacidade de visão com *zoom* e da câmera termal. Os resultados não são representados apenas pela soma dos valores das apreensões de contrabando, descaminho, armas e drogas, mas também com a coleta de dados e informações de inteligência.

Os casos apresentados mostram que as iniciativas, via de regra, partem de agentes operacionais motivados e que perceberam as vantagens evidentes do uso de RPA. Entretanto, a ideia deve ser encampada pelas autoridades decisoras no nível político para que os projetos ganhem impulso e sejam instrumentos de transformação dentro das organizações.

Como conclusão da Discussão, esta dissertação objetiva sensibilizar as autoridades e os pesquisadores acerca desta nova possibilidade de trabalho com RPAs. Muitas ideias aqui discutidas vão ao encontro do que foi observado e pontuado pelos servidores das organizações citadas (PMMG, PMPR e RFB) e se constitui em algo inovador e necessário a ser desenvolvido.

# 6 CONTRIBUIÇÕES PROPOSTAS PARA EMPREGO DE DRONES EM ISP

O uso de Aeronaves Remotamente Pilotadas no Brasil tem muitos pontos positivos devido a sua utilização por militares e civis para fins já descritos na introdução do trabalho. Além disso, existe a expectativa do crescimento do mercado com o avanço dos estudos de empresas e escolas brasileiras sobre a tecnologia.

Este capítulo apresenta a proposta de metodologia para emprego de drone para instituições do Sistema de Segurança Pública no Brasil. Como tratado no capítulo 1, os drones possuem uma gama de possibilidades de emprego ainda não completamente mapeadas e, no contexto de segurança pública, essa premissa é verdadeira. O objetivo deste capítulo é apresentar ideias embasadas em dados e conhecimentos científicos a fim de auxiliar as instituições que lidam com ISP a empregar os drones de forma segura e eficiente.

Consultando a DNISP e realizando estudo de situação, pode-se afirmar que os drones beneficiam o setor de Inteligência de Segurança Pública por meio de várias funções:

- Apoio aéreo em ações policiais e monitoramento de suspeitos;
- Apoio a ações de busca e salvamento;
- Análise de risco em inspeções de áreas e instalações;
- Monitoramento em tempo real de eventos com impacto na Segurança Pública;
- Monitoramento remoto de crimes ambientais (mineração ilegal, queimadas e desmatamentos);
- Visualização remota de áreas perigosas.

## 6.1 DISCUSSÃO DA PROBLEMÁTICA

Compreender e assimilar o conceito de Inteligência de Segurança Pública é o ponto de partida para que seja estabelecida uma metodologia para o seu emprego. Como dito alhures, a grande gama de possibilidade de emprego deve considerar um emprego conjunto das RPAs com os demais sistemas dos Órgãos de Segurança Pública.

É preciso caracterizar que uma ação de inteligência tem caráter predominante de proatividade, ou seja, visa antecipar e assessorar alguma operação. A partir do momento que a ação policial é iniciada, a utilização de drone é absorvida pelo sistema de Comando e Controle (C2) e deixa de fazer parte do sistema de inteligência.

O ambiente operacional de combate à criminalidade organizada em aglomerações urbanas, como comunidades nas periferias das grandes cidades, possui todas as características de uma guerra irregular: longa permanência, oponentes ocultos no meio da população e necessidade de ações pontuais a fim de evitar danos colaterais.

Importante trazer para o contexto da segurança pública lições aprendidas por outros países na guerra ao terror. Primeiramente existem limitações estratégicas sobre redes sociais complexas, ou seja, os dados obtidos por meio dos drones não devem ser a única evidência para se produzir conhecimentos de inteligência, uma vez que a dinâmica complexa de interação dos atores deve ser confirmada por outros meios. Devido a suas facilidades, a utilização de drones não deve se transformar numa armadilha eterna para os OSP, como se essas aeronaves fossem a solução para todas as situações.

Há que se entender que o uso demasiado de drones pode prejudicar a imagem institucional dos OSP, uma vez que pode transmitir mensagem de excessivo controle social em áreas mais desfavorecidas se a ostensividade das ações for demasiado frequente. Essa percepção, ainda que subjetiva, pode ser nociva no longo prazo no que tange a aceitação do emprego das RPAs.

A inovação proporcionada pelo uso das RPAs apresenta relevância no âmbito da Segurança Pública porque se trata de um processo sistemático e deliberado, que minimiza os riscos e proporciona resultados satisfatórios. Nesse sentido, a compreensão das características e dimensões dos processos de inovações se faz necessária para identificação do melhor caminho a se seguir.

Por outro lado, há ainda que se considerar que essa evolução tecnológica tem sido acompanhada pelas organizações criminosas, de modo que os Órgãos de Segurança Pública devem manter-se atualizados, com o fim de combater o uso criminoso das RPAs pelas organizações criminosas e agentes maliciosos avulsos.

Importante ressaltar que se trata de uma contribuição que busca fazer uma integração entre o estado da arte na área de pesquisa científica e a realidade enfrentada pelos gestores públicos brasileiros, mormente casos de limitações orçamentárias, legais e de recursos humanos para a execução das atividades organizacionais.

A implantação de uma metodologia implica necessariamente mudança de cultura organizacional. Porém, tal mudança leva certo tempo para ser realizada, pois as pessoas tendem a internalizar comportamentos e atitudes que estão arraigados ao longo de muito tempo dentro das instituições [146]. Soma-se a isso o fato dos órgãos públicos terem maior dificuldade para implementação de mudanças devido aos entraves burocráticos típicos da máquina pública. Esses obstáculos têm duas linhas de análise: pois ao mesmo tempo em que previnem o autoritarismo, por outro lado limitam iniciativas de inovação, que dependem sempre do crivo legal e da edição de normativas internas.

A problemática delineadora do trabalho desta pesquisa é a necessidade de inclusão deste tipo de aeronave no acervo das organizações de segurança pública, rompendo paradigmas estabelecidos por longo tempo dentro das instituições públicas. Entretanto, estas resistências e dificuldades não devem desestimular a adoção de iniciativas de implementação de inovações e soluções possíveis.

## 6.2 ESCOLHA DE DRONES

A escolha do drone é a primeira tarefa a ser executada para quem se propõe a utilizar este tipo de equipamento. Quando se trata de OSPs , que possuem atribuições distintas a primeira pergunta a ser respondida é: usar para quê? Para ajudar a responder esta pergunta, a figura 6.1 estabelece alguns fatores a

serem considerados na escolha de uma drone.


Figura 6.1: Critérios para escolha de drones

Interessante notar algumas ideias pontuadas por Moreira et al. [141]: em primeiro lugar deve-se definir os requisitos técnicos para a atividade a ser executada. A montagem de uma equipe técnica, desvinculada do processo de aquisição, deve ser considerada. Esse grupo deve ter independência para elencar os critérios e realizar os julgamentos de forma o mais homogênea possível. Também é essencial que as mesmas pessoas avaliem as opções disponíveis ao longo de todo o processo de escolha.

Ressalta-se que os pesos relativos destinados a cada critério devem ser estipulados pelas autoridades políticas e técnicas que irão realizar a aquisição das RPAs. Os seguintes fatores foram listados como relevantes na escolha de drones e não estão classificados em ordem de importância:

1. **Finalidade**: deve se buscar sempre a aeronave que tenha a melhor capacidade para a missão a que se destina, qual a classe de drone que melhor atende e em quais circunstâncias. Dentre as aeronaves comerciais classe 3, por exemplo, existe uma infinidade de modelos e marcas, e os técnicos responsáveis pela elaboração da aquisição devem procurar a que seja mais específica.

2. **Resolução das imagens**: uma das principais finalidades das RPAs é a obtenção de imagens. Nos modelos mais caros, o valor das câmeras fotográficas supera o valor da aeronave em si. Algumas câmeras apresentam *zoom* ótico e outras, o *zoom* digital, sendo que este último tipo apresenta pequena distorção nas imagens. A depender do uso, é preferível adquirir um drone com autonomia de voo inferior, mas com qualidade de imagem superior. A seleção dos sensores a serem instalados na plataforma aérea dependem da realidade do ambiente. Excesso de nuvens, por exemplo, tem impedido o mapeamento satelital da Floresta Amazônica de forma consistente há anos.

3. **Autonomia de voo**: como relatado nos trabalhos relacionados, o reduzido tempo de duração das baterias é um fator limitante no emprego de drones. Existem missões em que é importante ter o maior tempo possível de voo sobre determinada região (áreas rurais, por exemplo). Neste sentido, a autonomia de voo deve ser considerada na escolha de um drone

4. **Alcance de utilização**: o alcance de utilização depende da estrutura da aeronave, as de asa fixa possuem maior alcance de utilização do que as multi-rotores. Outros fatores também influenciam no alcance de voo, tais como a velocidade de voo, além do volume do tanque de combustível ou duração da bateria. A autonomia e o alcance de voo são importantes, enquanto aquela refere-se ao tempo, esta diz respeito a distância percorrida pela aeronave.

5. **Manutenção**: como toda máquina, os drones necessitam de cuidados periódicos programados ou inopinados. Ocorre que alguns modelos apresentam menor incidência de problemas estruturais ou histórico de facilidade de manutenção. Ao se pensar na compra de uma RPA, a facilidade em encontrar peças de reposição deve ser uma variável a ser analisada.

6. **Preço**: todos os órgãos públicos brasileiros devem se pautar por critérios objetivos para realização de compras e licitações e o preço é um dos fatores mais importantes a serem observados. Neste critério, mais do que o valor mais barato, deve-se priorizar o custo benefício de cada opção de compra e, após isso, apresentar justificativa para que o gestor público possa legitimar a sua escolha perante os Tribunais de Contas.

7. **Portabilidade**: uma operação de inteligência exige discrição no ambiente operacional e em algumas situações é necessário que o equipamento seja fácil de ser conduzido e acondicionado. Dessa forma, a portabilidade da RPA é um fator a ser considerado, seja na aquisição ou na escolha para determinada missão.

8. **Manuseio**: alguns aparelhos apresentam dificuldade de operação, seja pela conformação da aeronave, seja pela interface gráfica do aplicativo para o usuário. Os modelos mais modernos primam pela facilidade de manuseio a fim de abarcar o maior número possível de consumidores. A construção de um drone customizado é um projeto que pode ser desenvolvido pelas equipes de pesquisa e desenvolvimento, garantindo maior segurança, maior especificidade e maior profissionalismo ao trabalho.

9. **Estabilidade**: os drones maiores apresentam maior resistência aos ventos e rajadas de vento. Já os drones menores, devido a sua pequena massa, são mais suscetíveis aos fatores climáticos. Essa característica intrínseca de cada aeronave também deve entrar na equação do algoritmo para a escolha do drone. Para ilustrar, em regiões do Brasil, como no Sul, facilmente se encontra ventos superiores ao limite das aeronaves de categoria média em uso pelas forças de segurança, assim como, a Floresta Amazônica possui altos índices pluviométricos, bem como a umidade do ar e o calor elevados. Essa diversidade climática brasileira afeta a estabilidade das aeronaves e, por conseguinte, a segurança dos voos.

10. **Versatilidade**: muitas aeronaves tem excelente desempenho, mas apresentam pouca flexibilidade de uso. A possibilidade de troca de sensores e equipamentos, bem como a capacidade maior de carga (payload) confere um vantagem importante que deve ser ponderado quando da escolha de uma aeronave.

Tão importante quanto a escolha do drone é o treinamento específico para as equipes que irão operar o equipamento. A figura 6.2 ajuda a esclarecer o fluxograma das atividades a serem desepenhadas por uma

unidade de emprego de drones.

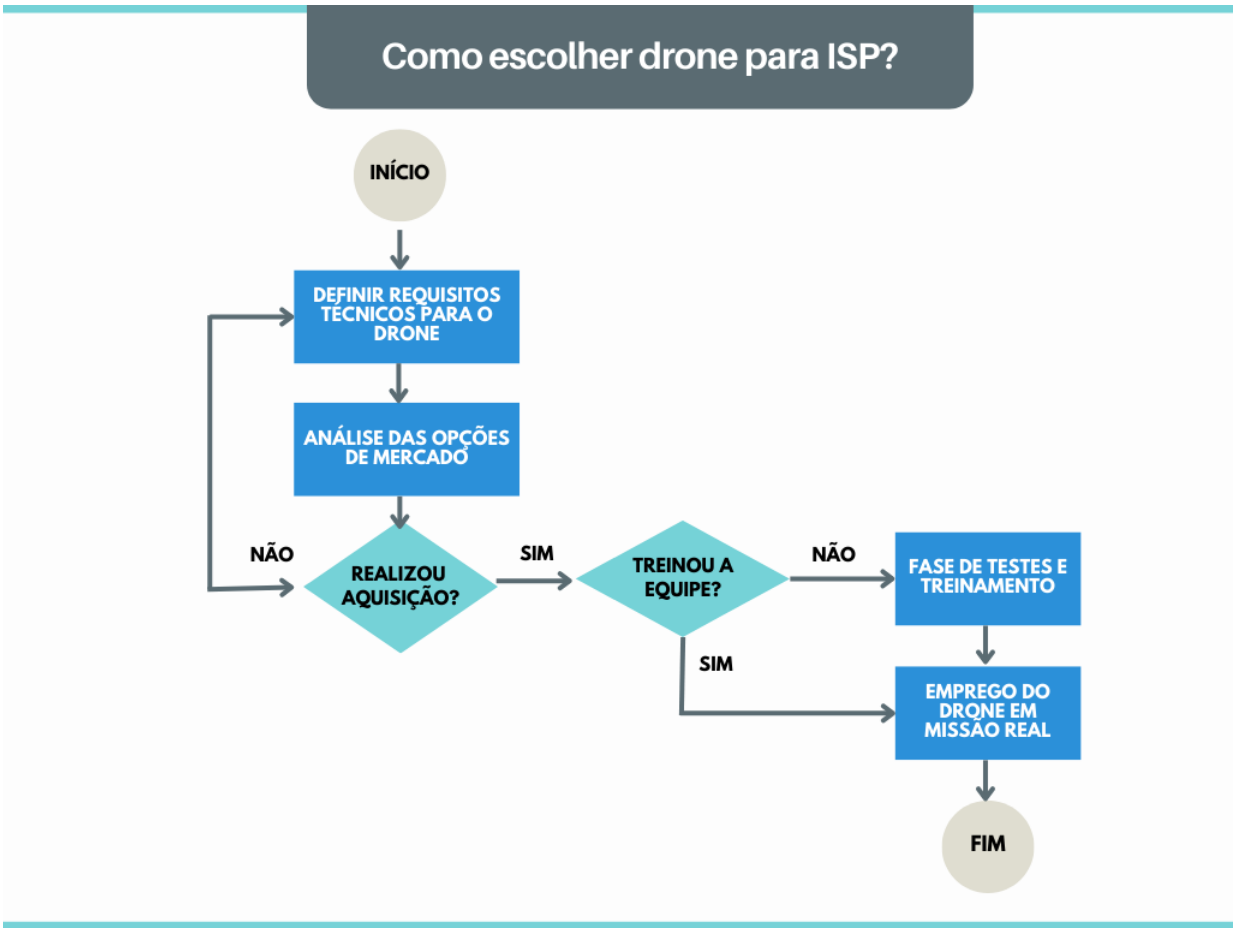


Figura 6.2: Fluxograma para escolha de drones

### 6.2.1 Matriz proposta para escolha de drones

Após a análise e descrição dos critérios para escolha dos drones é preenchida uma planilha. A ideia central de se propor uma matriz de escolha de drone para atividade de ISP é estabelecer critérios técnicos que auxiliem as autoridades decisoras na realização das aquisições, conferindo assim, maior cientificidade e maior legitimidade, mitigando a probabilidade de erros e justificando escolhas perante os tribunais de contas públicas.

A matriz abaixo foi obtida numa simulação de aeronave para **vigilância de ISP num contexto urbano**. Neste caso, em particular, foram atribuídos pesos maiores para as variáveis: imagens (peso 3), Versatilidade (peso 2) e preço (peso 2). As demais variáveis tiveram peso 1. Essa equação vai variar conforme o contexto e a finalidade para o emprego da RPA. Interessante também que haja uma avaliaçao por parte de, pelo menos dois técnicos e que a média de avaliação seja preenchida na planilha. Os técnicos devem avaliar todas as opções de compra para que os parâmetros de comparação sejam homogêneos.

Tabela 6.1: Exemplo de Matriz para escolha de drones em ISP

| **Critério x Peso** | **Drone A** | **Drone B** | **Drone C** |
|---|---|---|---|
| Finalidade x 1 | 8 x 1 = 8 | 9 x 1 = 9 | 9.5 x 1 = 9.5 |
| Imagens x 3 | 9 x 3 = 27 | 9.5 x 3 = 28.5 | 8 x 3 = 24 |
| Autonomia voo x 1 | 8 x 1 = 8 | 9 x 1 = 9 | 9 x 1 = 9 |
| Alcance voo x 1 | 8 x 1 = 8 | 9 x 1 = 9 | 9 x 1 = 9 |
| Manutenção x 1 | 10 x 1 = 10 | 9 x 1 = 9 | 9.5 x 1 = 9.5 |
| Preço x 2 | 9 x 2 = 18 | 9 x 2 = 18 | 8.5 x 2 = 17 |
| Portabilidade x 1 | 10 x 1 = 10 | 9 x 1 = 9 | 10 x 1 = 10 |
| Manuseio x 1 | 8.5 x 1 = 8.5 | 9 x 1 = 9 | 10 x 1 = 10 |
| Estabilidade x 1 | 9 x 1 = 9 | 10 x 1 = 10 | 9.5 x 1 = 9.5 |
| Versatilidade x 2 | 10 x 2 = 20 | 9.5 x 2 = 19 | 9 x 2 = 18 |
| **Pontuação Total** | 126.5 | 129.5 | 125.5 |

No caso esquemático, o drone B obteve a pontuação total de 129.5 pontos para a aquisição destinada à vigilância em ambiente urbano. Dessa forma, esta matriz poderia compor o referencial técnico da licitação, o que iria justificar com maior clareza o motivo da escolha e compra do drone B.

## 6.3 UNIDADE DE EMPREGO DE DRONES

A partir da discussao da problemática e da escolha dos tipos de drones a serem empregados, deve-se organizar de uma unidade específica para a operação das RPAs dentro da estrutura de funcionamento dos Órgãos de Segurança Pública.

No Brasil, de forma geral, a Segurança Pública está a cargo das Unidades da Federação (UF). Cada estado possui uma Secretaria de Segurança Pública (SSP) que tem, dentro de sua estrutura, as Polícias Civil e Militar, além do Corpo de Bombeiros Militares e da Defesa Civil. A maioria dos estados possui uma unidade de emprego de aviação, geralmente subordinada à Secretaria de Segurança Pública.

Dado que as atividades aéreas com uso de aviões, helicópteros e RPA são complementares, o ideal é que a unidade de emprego de drones fique inserida dentro da estrutura de emprego aéreo, a fim de aproveitar as características específicas de cada vetor aéreo. As tendências de uso futuro, definidas como aspectos esperados dos novos projetos, devem considerar o uso simultâneo e coordenado de aeronaves tripuladas e não-tripuladas, elevando ao máximo a complementariedade das unidades aéreas.

Importante ressaltar que a unidade de emprego de drones mantenha autonomia operacional e administrativa a fim de desenvolver doutrina própria de emprego. Além disso, o uso de drones deve ser entendido como uma nova forma de utilização de aeronaves, com peculiaridades que exigem dedicação exclusiva dos profissionais envolvidos nesta área, uma vez que o custo benefício desta atividade apresenta-se bastante vantajoso.

O organograma de uma Unidade de Emprego de Drones, ilustrado na figura 6.5, foi idealizado para

estar enquadrado dentro da estrutura de uma Secretaria de Segurança Pública estadual. Importante destacar o caráter técnico desta atividade, sugerindo que as pessoas designadas sejam especialistas e tenham competências relacionadas ao desempenho de suas funções.

A unidade será composta por uma **chefia**, responsável pelo Comando e Controle (C2), tanto dentro das rotinas do dia a dia, como numa missão aérea real. A todo momento o comandante deve ter consciência situacional das atividades desempenhadas por seus subordinados. O uso intenso da tecnologia, inclusive com imagens em tempo real, é um fator primordial para a liderança e assessoramento para o alto escalão da segurança pública. A chefia também é responsável pelos contatos institucionais e reuniões multilaterais com outras instituições e unidades.

Se a arquitetura de rede não estiver dimensionada corretamente, a inserção de RPA em um complexo de C2 será frustrada pela impossibilidade de transmissão de dados úteis à decisão. Mantida esta situação, a RPA operará ou como simples coletor de dados para posterior transmissão para o centro, ou o processo decisório terá que fornecer autonomia para os operadores na ponta da linha. Estas duas situações não acrescentam ao sistema a capacidade primordial de permitir a decisão no topo da cadeia de comando, onde há informações mais completas e assessores das diversas áreas.

Outro fator importante na coordenação e controle é o aspecto de segurança da aviação, uma vez que um acidente poderá diminuir o apoio a esse tipo de operação pela sociedade ou simplesmente a diminuição de capacidade operativa com a perda de meios.

O grupo de **apoio, pesquisa e desenvolvimento** será composto por equipes específicas: equipe de **manutenção** responsável pela manutenção preditiva e corretiva das aeronaves, seja de asa fixa ou multirotores. A equipe de **apoio** ficará responsável pelas tarefas administrativas, tais como licitações e contratos, pagamentos e almoxarifado. Já a equipe de **pesquisa** terá a função de buscar inovações e levantar ideias que possam ser implementadas pelos grupos operacionais. Por fim, a equipe de **desenvolvimento** será incumbida da missão de testar novos equipamentos e novas doutrinas de emprego formuladas pelo grupo de pesquisa.

O grupo de emprego **contra-drones** será composto por 4 equipes, sendo 2 equipes de **detecção** e 2 equipes de **neutralização**. Quanto as **equipes de detecção**, conforme visto nos estudos relacionados, é aconselhável que haja mais de um meio de detecção de drones e cada uma das equipes poderiam ser especializada em um método específico. Poderia, por exemplo, ter uma equipe especialista no uso de radares e outra equipe especialista na detecção via RF.

Já as **equipes de neutralização**, a exemplo das de detecção, teriam *expertises* complementares. Poderia uma ser especialista na técnica de *jamming* e outra na técnica de *spoofing*. Existem soluções portáteis no mercado e o uso de sistemas anti-drones embarcados em caminhões é uma possibilidade a ser considerada, pois confere versatilidade para uso em eventos críticos e pontuais.

Já existem no mercado algumas soluções possíveis, inclusive com o desdobramento de centros de comando e controle móveis, tal como ilustrado na figura 6.3.

O sistema pode contar com o *upgrade* da *Ground Control Station* (GCS) multifunção, desenvolvida para substituir o *notebook* em missões onde a ergonomia dos controles e a visualização da instrumentação são essenciais para reduzir a carga de trabalho dos operadores. A partir da GCS pode-se monitorar: dados


Figura 6.3: Posto de C2 móvel - GSC XMobots [10]

da instrumentação primária do RPA, mapa móvel da missão e imagem dos sensores para coordenação, como demonstrado na figura 6.4.

Figura 6.4: Interface gráfica do GSC XMobots [10]

O subsistema de **detecção** consiste na utilização de um ou mais sensores capazes de coletar informações do ambiente circundante. O subsistema de **detecção** coleta dados de sensores e executa algoritmos de detecção, baseados em IA, ML e DL, capazes de estabelecer a presença de uma ameaça, identificá-la e decidir o modo de rastreamento e neutralização mais apropriado.

O subsistema de **neutralização** consiste na utilização de um ou mais elementos mitigadores capazes de desabilitar, destruir ou assumir o controle do drone identificado como ameaça.

Existe a possibilidade de emprego integrado da parte de detecção e a parte de neutralização na mesma plataforma, mas o solução mais adequada é segregar as funções a fim de maior eficiência e especificidade do trabalho. Com isso, a probabilidade de sucesso no atingimento de objetivos é maior.

O grupo de emprego **multi-rotores** é especializado na utilização de drones comerciais classe 3 (PMD até 25kg). Devido às particularidades dessas aeronaves, existe a vocação natural para o emprego em ambi-

ente de adensamento populacional, cobrindo ações como eventos esportivos, shows, manifestações públicas, reconhecimento e vigilância em locais com muitas edificações.

Foram previstas 4 equipes, sendo cada equipe composta de 3 agentes e responsável pela utilização de um drone. Um agente será o piloto do drone, outro membro será o observador e o outro agente será responsável pela segurança da equipe. O observador é um membro da equipe de UAS que, por meio da observação visual da RPA, auxilia o piloto remoto na condução segura do voo, necessitando, para tanto, comunicação permanente com o piloto. A observação visual, aos moldes do estabelecido para operação VLOS, deverá ser estabelecida sem o auxílio de outros equipamentos ou lentes, excetuando-se as corretivas.

É aconselhável ter ao menos 2 equipes cobrindo um evento, uma vez que sempre existe a possibilidade de dificuldades técnicas de voo em ambiente urbano, ou mesmo necessidade de troca de bateria, ou em razão de deslocamentos pontuais das equipes. Os veículos utilizados para as operações de ISP, se não forem variados ou diferentes da frota ostensiva, tornam-se facilmente perceptíveis pelos alvos a serem monitorados.

Em áreas de difícil acesso, é possível empregar as RPA na localização de criminosos em áreas de homizio por meio do compartilhamento de *link* de imagens termais em tempo real para as equipes de campo empenhadas na missão de captura. Essa ação minimiza o risco de emprego letal da força.

Os drones conseguem visualizar toda a área abaixo e ao redor deles, captando imagens com amplo ângulo de visão. O monitoramento completo proporciona maior segurança para o vigilante que está no solo, pois extingue a necessidade da sua presença física. Com isso, as RPAs diminuem os fatores de risco, evitando a exposição de profissionais a situações perigosas. A vigilância aérea proporcionada pelos drones oferece, ainda, maior visibilidade da área, além de ser quase imperceptível.

Situações pontuais, como operações de fiscalização de trânsito, monitoramento de rodovias, controle de fluxo, treinamento de servidores e utilização em grandes eventos são facilitadas com o emprego de drones. Nas grandes cidades, existem locais onde não é viável instalar câmeras de segurança. Desse modo, tornam-se pontos vulneráveis dentro de um perímetro, sendo mais sujeitos às ações criminosas. Os drones mitigam este problema, já que podem sobrevoar áreas de difícil acesso físico, como uma ponte ou na cobertura de uma edificação.

O grupo de emprego **asa fixa**, pelas características das aeronaves, é melhor destinado para eventos em área rural, para o monitoramento de crimes ambientais, para ações de busca e salvamento e para atividades de aerolevantamento/reconhecimento. À semelhança dos multi-rotores, há a previsão de 4 equipes, sendo cada equipe com 3 agentes e responsáveis pela operação de uma RPA. Um agente será o piloto do drone, outro membro será o observador do drone e o outro agente será responsável pela segurança da equipe.

Pode-se citar o emprego de equipes de inteligência asa fixa que vão a campo para inspecionar e avaliar áreas onde há suspeitas de queimadas ou desmatamentos apontadas via imagens de satélites. As imagens satelitais possuem algumas limitações quanto ao espaço temporal e são suscetíveis à interferência de nuvens. As imagens obtidas pelos drones reduzem essas deficiências.

Dada as características elencadas de baixa autonomia e curto alcance dos voos, se a região de interesse de uma missão for grande e/ou os objetivos da missão forem vários, a execução de uma missão com um único drone pode exigir uma quantidade considerável de tempo e pode acarretar desempenho ruim

em termos de eficácia da missão. Dessa forma, o emprego coordenado de equipes de drones torna-se imperioso.

Além das atividades de inteligência, o emprego sistemático e detalhado de RPA pode fornecer dados, imagens e vídeos que possam ser utilizados em processos de persecução penal como elementos comprobatórios de delitos criminais.

O organograma de Unidade de Emprego de Drones deve ser flexível e se ajustar a realidade de cada Unidade da Federação. Numa UF com grande área territorial e grande incidência de crimes ambientais pode haver a demanda por um grupo de asa fixa composto por maior número de equipes. Por outro lado, num estado com grande adensamento populacional e alta incidência de crime organizado em áreas reduzidas pode ensejar o emprego de maior número de equipes multi-rotor. Além disso, pode-se começar com número reduzido de euipes e de servidores e ir expandindo o escopo da organização à medida que as demandas forem crescendo.

O treinamento continuado, seja por meio da realização de cursos técnicos, seja por meio da simulação de exercícios reais deve ser uma preocupação constante na gestão de pessoal pela chefia da Unidade de Emprego de Drone, sobretudo porque esse é um tipo de tecnologia que avança muito rapidamente e sempre surgem novidades a serem testadas.

A figura 6.5 ilustra o modelo proposto por este autor como o mais adequado para uma Unidade de Emprego de Drones:

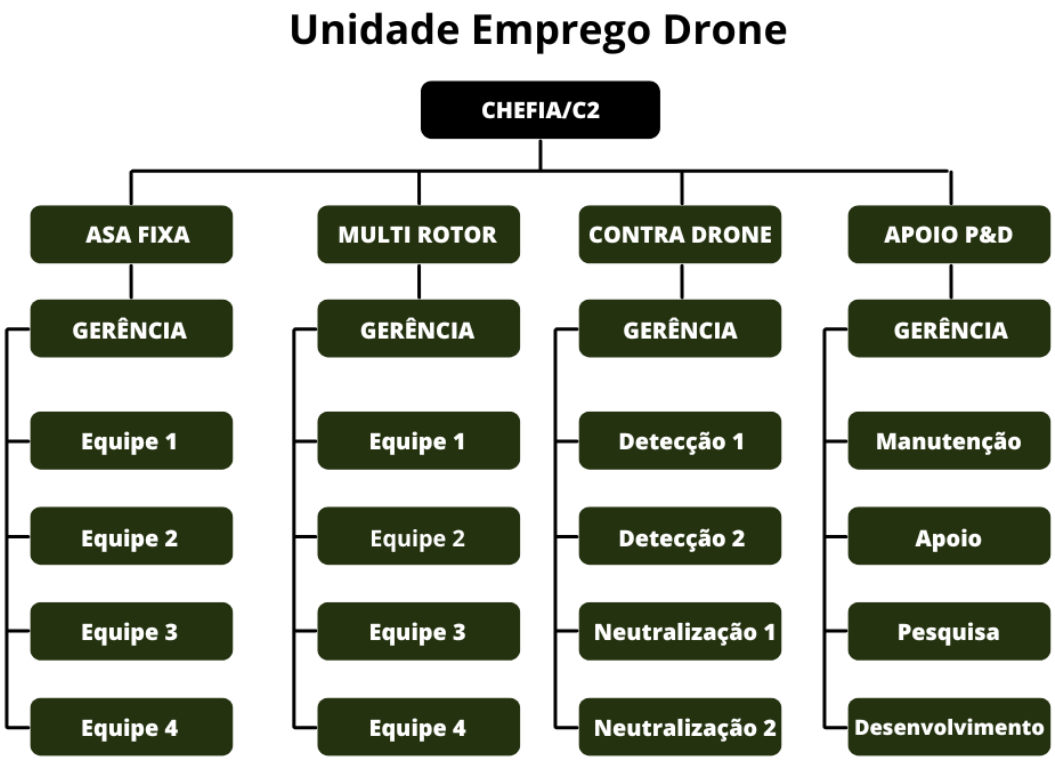


Figura 6.5: Unidade Emprego de Drones

Os voos de SARP devem ser planejados com critério, sendo importante o conhecimento, por parte do piloto, da localização das áreas proibidas, perigosas e restritas, e seus significados. Outras áreas sensíveis, mesmo que não estejam classificadas como áreas proibidas, perigosas e restritas, tais como usinas hidrelétricas, refinarias, plataformas de exploração de petróleo, depósitos de combustível, estabelecimentos penais e áreas militares, não devem ser sobrevoadas sem a prévia autorização das autoridades responsáveis pela área de sobrevoo.

Outro ramo importante na metodologia de emprego de drones é saber proteger-se contra esse tipo de artefato. Em que pese todos os fatores positivos elencados, cabe salientar o risco de utilização dessa tecnologia por facções criminosas e grupos terroristas, que podem aproveitar do fato de não haver fiscalização efetiva e adquirir uma aeronave para facilitar o cometimento de atos criminosos, pondo em risco a segurança da sociedade [20].

Também é necessário pensar a utilização de sistema contra drones para a proteção de infraestruturas estratégicas, compostas por instalações, serviços e bens que, se forem interrompidos ou danificados, provocarão sério impacto social, econômico, político ou à segurança [44]. Podem ser consideradas infraestruturas críticas: redes elétricas, usinas hidrelétricas, usinas termelétricas, usinas nucleares, redes de abastecimento de água ou gás, barragens ou represas, redes de comunicação ou de vigilância da navegação aérea, dentre outras. Segundo o DECEA, O voo com RPA próximo à infraestruturas críticas, é proibido a uma distância inferior a 3 Milhas Náuticas (aproximadamente 5 Km).

Finalmente, a realização de exercícios simulados são uma excelente forma de se avaliar e aprimorar um sistema anti-drones.

Numa tecnologia tão disruptiva não se deve pensar o emprego dos agentes como algo a mais. De fato, o emprego de drones se constitui numa nova qualificação e competência dentro das corporações. Não se trata apenas de operar o equipamento, trata-se de algo muito maior. Trata-se de pensar efetivamente o emprego da tecnologia em conjunto com outros sistemas operacionais, moldar nova doutrina e agregar nova gama de serviços para as forças de segurança pública. Esta metodologia visa trazer esta visão prospectiva para os cenários das próximas décadas quanto ao emprego de RPAs.

# 7 TRABALHOS FUTUROS E CONSIDERAÇÕES FINAIS

## 7.1 POSSIBILIDADES DE APROFUNDAMENTO DA METODOLOGIA PROPOSTA

Existem algumas oportunidades de melhoria a serem implementadas a partir da adoção da metodologia proposta nesta dissertação. Uma delas aponta para estudos sobre a durabilidade de baterias. A limitação de energia é um gargalo em qualquer cenário de utilização UAV. Novos estudos poderiam desenvolver tecnologias de baterias, como baterias de íons de lítio aprimoradas e células de combustível de hidrogênio, e a coleta de energia verde usada para aumentar o tempo de voo utilizando fontes de energia solar.

Estudos futuros devem considerar que os ganhos de conectividade da tecnologia 5G trouxeram novas perspectivas para o uso coletivo de drones e para o controle do espaço aéreo de baixa altitude e que devem possuir um confiável grau de segurança contra ataques de *jamming* e *spoofing*. Quanto ao *spoofing*, seja de RF ou de GNSS, conclui-se que as vulnerabilidades cibernéticas dos drones comerciais civis ainda estão longe de serem sanadas e esta técnica tende a ser cada vez mais utilizada. Os trabalhos futuros de segurança cibernética em UAV devem aprofundar novas formas de detecção de ataques de *spoofing* em drones.

Resultados apontam que o desenvolvimento de sistemas anti-drones deve considerar que o uso da técnica de *jamming* tende a ser cada vez mais restrito, portanto devem ser aprimoradas as técnicas de detecção para que os drones sejam neutralizados de forma pontual. O uso de técnicas combinadas de detecção de UAV é um ramo a ser desenvolvido a fim de aumentar a possibilidade de sucesso dos C-UAS.

Outro caminho a ser trilhado pode ser o estudo de combate ao vazamento de privacidade da comunicação UAV e garantia a integridade dos dados coletados dos UAVs. Espera-se que a tecnologia *blockchain* seja um novo paradigma para manter de forma segura e adaptável as preferências de privacidade durante o processo de comunicação entre as RPAs e GCS.

Os aspectos legais também apresentam-se como área promissora em estudos futuros, uma vez que os normativos e regulamentos geralmente vêm a reboque das inovações tecnológicas. A regulamentação da *Remote ID* é um exemplo ilustrativo desta situação.

## 7.2 CONSIDERAÇÕES FINAIS

Desenvolver um sistema de utilização de RPA é um desafio crucial a ser enfrentado pelas instituições que lidam com a Segurança Pública. Isso não é uma tarefa simples e fácil, pelo contrário, constitui-se num caminho complexo e longo a ser percorrido, mas dele depende a melhoria do desempenho institucional e a relevância futura da corporação.

Cumpre destacar que não existe um modelo único de emprego de RPA nas instituições que lidam com ISP. Sua implantação é baseada em modelos empíricos de tentativas e erros, e de aprimoramento contínuo. Esse modelo representa um verdadeiro jeito de ser de cada instituição que o define de acordo com seus

objetivos estratégicos, modelo de negócio, cultura organizacional e contexto institucional.

O Brasil possui um parque industrial diversificado e, sobretudo na área de aviação e aviônica, abriga empresas que tem o estado da arte na fabricação de aeronaves (Embraer, XMobots, Turbomachine, SIATT e Stella Teconologia, só para citar algumas). O fomento de Parcerias Público Privadas (PPP) seria uma solução viável para a busca e/ou adaptação de soluções de mercado para a utilização em ISP.

Certamente o uso de RPA não se consitui numa panaceia para solução de todos os problemas de segurança pública, uma vez que os problemas que envolvem esta atividade são complexos e multivariados. Entretanto, o emprego de drones em proveito da atividade de Inteligência Segurança Pública tem crescido de importância nos últimos anos e estudos acadêmicos sobre essa temática são cada vez mais necessários.

# REFERÊNCIAS BIBLIOGRÁFICAS


1 MEDEIROS, F. A. et al. Desenvolvimento de um veículo aéreo não tripulado para aplicação em agricultura de precisão. Universidade Federal de Santa Maria, 2007.

2 CENTER, S. T. *Drone Orlan 10 empregado na Guerra Ucrânia*. Disponível em https://www.forbes.com/sites/davidhambling/2021/01/25/russia-enters-military-drone-export-market-with-sale-to-burma/amp/. Acesso em 12 novembro 2022.

3 CENTER, S. T. *Drone Lancet3 empregado na Guerra Ucrânia*. Disponível em https://mil.in.ua/en/news/russians-now-use-lancet-kamikaze-drones-in-ukraine/ Acesso em 12 novembro 2022.

4 IRAN. *Drone Geranium 2 empregado na Guerra Ucrânia*. Disponível em https://www.forte.jor.br/2022/11/11/os-principais-drones-russos-empregados-na-guerra-da-ucrania/. Acesso em 12 novembro 2022.

5 TECHNOLOGY, B. *Drones turcos Bayraktars ajudam Ucrania*. Disponível em https://noticias.uol.com.br/internacional/ultimas-noticias/2022/05/11/o-que-sao-os-drones-bayraktar.htm Disponível em 20 novembro 2022.

6 TECHNOLOGY, B. *Ucrania e Turquia testam novo drone de ataque*. Disponível em https://www.edrotacultural.com.br/ucrania-e-turquia-testam-drone-para-combate-aereo/ Disponível em 20 novembro 2022.

7 XMOBOTS. *Drone Arator 5C*. Disponível em https://xmobots.com.br/arator-5c/. Acesso em 12 novembro 2022.

8 XMOBOTS. *Drone Dractor 25A*. Disponível em https://xmobots.com.br/dractor25a-map/. Acesso em 12 novembro 2022.

9 XMOBOTS. *Drone Nauru C*. Disponível em https://xmobots.com.br/nauru-500c-vtol/. Acesso em 12 novembro 2022.

10 XMOBOTS. *Drone Nauru 500C ISR*. Disponível em https://xmobots.com.br/nauru500c-isr/. Acesso em 12 novembro 2022.

11 TECNOLOGIA, S. *Atobá1*. Disponível em https://revistapesquisa.fapesp.br/o-atoba-alca-voo/. Acesso em 03 setembro 2022.

12 SIATT, T. e. *Drone Tupan 300*. Disponível em https://www.infodefensa.com/texto-diario/mostrar/3056038/siatt-e-turbomachine-avancam-no-desenvolvimento-do-uav-brasileiro-tupan-300. Acesso em 13 novembro 2022.

13 SYSTEMS, E. *Hermes 900*. Disponível em https://www.fab.mil.br/noticias/mostra/18093/REAPARELHAMENTO-Acesso em 03 setembro 2022.

14 SYSTEMS, E. *Hermes 450*. Disponível em https://www.fab.mil.br/noticias/mostra/19817/OPERACIONALAcesso em 03 setembro 2022.

15 CMSE. *Conheça o Nauru 1000C*. Disponível em cmse.eb.mil.br/index.php/ultimas-noticias-categoria/740-conheca-o-nauru-1000c-novo-drone-do-exercito-brasileirogallerye90e6e6b4a-5.

16 BRASIL, M. do. *Marinha do Brasil faz lançamento do drone ScanEagle*. Disponível em https://www.marinha.mil.br/comforaernav/criacao$_esqdqe1Disponvelem22denovembrode$2022.

17 SCHROTH L.; BODECKER, H. *Drone Market Size And Report 2020-2025*. Disponível em https://droneii.com/free-drone-resources. Acesso em 05 setembro 2022.

18 TEAM, D. *VLOS, EVLOS and BLOS Operation 2020*. Https://droneii.com/free-drone-resources. Acesso em 04 setembro de 2022.

19 TEAM, D. *The Evolution of Drone Connectivity and the Role of 5G*. Disponível em https://droneii.com/free-drone-resources. Acesso em 04 setembro 2022.

20 BETÉ, T. de S. Drones: um pequeno histórico e as consequências do seu uso. *Revista Conexão SIPAER*, v. 10, n. 1, p. 2–14, 2019.

21 DECEA. *SARPAS*. Disponível em https://servicos.decea.mil.br/sarpas/. Acesso em 05 setembro 2022.

22 ANAC. *SISANT*. Disponível em https://santosdumont.anac.gov.br/menu/f?p=101:2:109057973525937:::::. Acesso em 05 setembro 2022.

23 WACKWITZ K.; LOTFI, Z. B. H. *Drone Application Report 2022*. Disponível em https://droneii.com/free-drone-resources. Acesso em 04 setembro 2022.

24 GERAIS, P. M. D. M. Efeitos do uso de aeronave remotamente pilotada (rpa/drone) na vigilância e coleta de imagens para produção de conhecimento no campo da inteligência de segurança pública.

25 PM-PR. *Matrice 300*. Disponível em https://www.pilotopolicial.com.br/bpmoapr-usa-aeronaves-remotamente-pilotadas-nas-missoes-policiais/. Acesso em 03 setembro 2022.

26 LATERZA RODOLFO; CABRAL, R. *Drones russos na guerra da Ucrânia*. Disponível em https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-unmanned-aircraft-systems. Acesso em 12 novembro 2022.

27 SHI, X.; YANG, C.; XIE, W.; LIANG, C.; SHI, Z.; CHEN, J. Anti-drone system with multiple surveillance technologies: Architecture, implementation, and challenges. *IEEE Communications Magazine*, IEEE, v. 56, n. 4, p. 68–74, 2018.

28 LI, B.; FEI, Z.; ZHANG, Y. Uav communications for 5g and beyond: Recent advances and future trends. *IEEE Internet of Things Journal*, IEEE, v. 6, n. 2, p. 2241–2263, 2018.

29 ANAC. Rbac–e nº 94, brasil. *Requisitos Gerais para Aeronaves Não Tripuladas de Uso Civil. Resolução*, n. 419, 2018.

30 OLIVEIRA, P. F. de; FÁVERO, W. C. A polícia militar do paraná e as novas tecnologias: o emprego das aeronaves remotamente pilotadas (drones): The military police of paraná and new technologies: the use of remote piloted aircraft (drones). *Brazilian Journal of Development*, v. 8, n. 9, p. 63064–63090, 2022.

31 DRUCKER, P. F. *melhor de Peter Drucker: a administração, O–Exame*. [S.l.]: NBL Editora, 2001. v. 2.

32 EISENBEISS, H. Uav photogrammetry. *Tese de doutorado - Institute of Geodesy and Photogrammetry, ETH-Zurich. Zurich, Switzerland*, 2009.

33 AUSTIN, R. *Unmanned aircraft systems: UAVS design, development and deployment*. [S.l.]: John Wiley & Sons, 2011.

34 BISPO, C. C. et al. A utilização do veículo aéreo não tripulado nas atividades de segurança pública em minas gerais. 2013.

35 GRAMKOW, D. et al. Emprego de aeronaves remotamente pilotadas nas áreas de defesa e de segurança: visão sistêmica. Escola Superior de Guerra (Campus Rio de Janeiro), 2017.

36 DECEA, I. 100-40: http://www. decea. gov. br. *Last access on 15 junho 2022*, v. 10, 2017.

37 DRONES by numbers. FAA.USA. Disponível em https://www.faa.gov/uas. Acesso em 07 de setembro de 2022.

38 EASA. *Diretivas 2019/945 e 2019/947, alteradas pela diretiva 2022/425*. Disponível em https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-unmanned-aircraft-systems. Acesso em 12 novembro 2022.

39 JORGE, L. d. C.; INAMASU, R. Y. Uso de veiculos aereos não tripulados (vant) em agricultura de precisão. In: BERNARDI, AC de C.; NAIME, J. de M.; RESENDE, AV de; BASSOI, LH; INAMASU . . . , 2014.

40 BICHO, C. P.; SILVA, L. S. da; MEDEIROS, W. C.; SILVA, C. A. da; JUNIOR, F. E. K.; GONDIM, R. de O.; JUNIOR, J. C. de S.; CHRISTAKOU, E. D.; FONTELES, H. R. da N.; ALMEIDA, A. B. L. de. Projeto $\mu$vant-uma parceria dnpm/unb para desenvolvimento e uso de $\mu$vants na fiscalização de atividades minerais não tituladas. *Simpósio Brasileiro de Sensoriamento Remoto (SBSR)*, v. 16, p. 9316–9323, 2013.

41 INFODEFENSA. *Cessão de Uso ARP Heron da PF para a FAB 2019*. Disponível em https://www.infodefensa.com/texto-diario/mostrar/3130630/policia-federal-cede-sua-heron-1-fab/. Acesso em 10 novembro 2022.

42 SIATT, T. e. *Voo experimental Tupan 300*. Disponível em https://www.youtube.com/watch?v=LzgZ5eeYLaM. Acesso em 13 novembro 2022.

43 AERONAVE Remotamente Pilotada da FAB realiza primeiro voo de traslado. Disponível em https://www.fab.mil.br/noticias/mostra/39791. Acesso em 29 de setembro de 2022.

44 SARP. Comando de Operações Terrestres. Disponível em http://www.coter.eb.mil.br/index.php/div-aviacao-e-seguranca/secao-de-investigacao-e-prevencao-de-acidentes-aeronauticos-4. Acesso em 06 de setembro de 2022.

45 DRONE market Share 2018. Skylogic Research. Disponível em https://www.thedronegirl.com/2018/09/18/dji-market-share/. Acesso em 05 de setembro de 2022.

46 SCHROTH, L. *Drone Market Size and Forecast 2020-2025*. Disponível em https://droneii.com/free-drone-resources. Acesso em 02 setembro 2022.

47 KHAN, A. Safety and privacy perspective of people towards autonomous drones–a qualitative study. 2021.

48 ÇETIN, E.; CANO, A.; DERANSY, R.; TRES, S.; BARRADO, C. Implementing mitigations for improving societal acceptance of urban air mobility. *Drones*, MDPI, v. 6, n. 2, p. 28, 2022.

49 FREY, T. *Tecnologia Disruptiva*. Disponível em https://www.insiderobotics.com.au/technology/articles-technology/Expert-predicts-1-billion-drones-in-world-by-2030/. Acesso em 06 novembro 2022.

50 ÜAS Remote Identification. Disponível em https://www.faa.gov/uas/getting$_started/remote_id.Acessoem15deoutubrode2022$.

51 AUTHORITY, C. A. *Unmanned Aircraft System Operations in UK Airspace- Guidance*. Disponível em https://www.caa.co.uk/media/uwynsupf/cap722-edition8-p.pdf. Acesso em 05 novembro 2022.

52 NETO, M. et al. A análise do emprego do veículo aéreo não tripulado (vant) nas ações e operações pm. 2009.

53 POLICIAIS, E. S. P. D. C.; POLÍCIA, M. D. E. S. D.; OFICIAIS-CAO, A. D.; PINHEIRO, R. M. Sistema de aeronave remotamente pilotada: estudo sobre a viabilidade do emprego na polícia militar do espírito santo.

54 GONÇALVES, J. M. d. S. A utilização de vant pelo batalhão de polícia militar da cidade de canoas no estado do rio grande do sul. 2021.

55 SILVA, V. S. Análise organizacional do serviço de aeronaves remotamente pilotadas do cbmdf instituído pela portaria nº 16 de 4 de julho de 2019. 2020.

56 MOURA, V. d. C.; SILVA, M. P. Aeronaves remotamente pilotadas (rpa): um aporte no combate aos incêndios florestais em áreas protegidas pelo corpo de bombeiros militar no estado do maranhão. 2018.

57 ZATTERA, C. L. Emprego de aeronaves remotamente pilotadas na área operacional de inteligência, subsidiando ações ostensivas da polícia militar do paraná. *RECIMA21-Revista Científica Multidisciplinar-ISSN 2675-6218*, v. 3, n. 10, p. e3102004–e3102004, 2022.

58 CORREA, E. D.; PARANÁ, P. M. D.; JOSÉ, D. P. S. Academia policial militar do guatupê.

59 SARTE, A. M. Proposta de padronização do serviço de aeronaves remotamente pilotadas no corpo de bombeiros militar de santa catarina. *Ignis: Revista Técnico Científica do Corpo de Bombeiros Militar de Santa Catarina*, v. 3, n. 1, p. 59–73, 2018.

60 SOUZA, M. de; 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, 2021.

61 TERRA, A. C. Interações público-privadas em defesa nacional e segurança pública: estudos de casos sobre projetos com o emprego de drones. 2019.

62 SILVA, P. C. R. da; DUTRA, A. C. Veículos aéreos não tripulados: possibilidades de emprego no corpo de bombeiros militar de santa catarina. *I seminário regional de pesquisa e inovação em segurança pública*, p. 74, 2015.

63 BURLAMAQUI, M. T. O uso de drones nas atividades operacionais das polícias no estado do ceará. *Ciências Aeronáuticas-Unisul Virtual*, 2018.

64 OLIVEIRA, I. R. d. O emprego de meios aéreos remotamente pilotados, na aquisição de dados, e em apoio a inserção de uma equipe de precursores em ambiente urbano negado. 2020.

65 MARTINS, M. et al. Viabilidade do uso de veículos aéreos não tripulados pela polícia militar de santa catarina no 19º bpm. Araranguá, SC, 2017.

66 LEITE, R. G. R. A utilização do sarp na aquisição de dados para produção de conhecimentos de inteligência para o dofesp na intervenção federal do rio de janeiro–rj no ano de 2018. 2020.

67 ALFARO, R. A. F. *Os veículos aéreos não tripulados na PSP: visão estruturante e aplicabilidade operacional*. Tese (Doutorado), 2015.

68 CHIOTE, D. *Requisitos Operacionais para os Veículos Aéreos Não Tripulados (UAV) na Guarda Nacional republicana*. Tese (Doutorado) — Academia Militar. Direção de Ensino, 2012.

69 NUNES, A. A. G. d. O. *O PAPEL DOS VEÍCULOS AÉREOS NÃO TRIPULADOS NA MODERNIZAÇÃO DO EXÉRCITO PORTUGUÊS*. Tese (Doutorado), 2021.

70 VICENTE, A. J. D. F. Os veículos aéreos não tripulados (drones): reforço da vertente aérea na psp. 2019.

71 MORGADO, S.; ALFARO, R. Aproximação da tecnologia em polícia orientada por objectivos: Uav's na polícia de segurança pública em portugal.

72 ALTAWY, R.; YOUSSEF, A. M. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems*, ACM New York, NY, USA, v. 1, n. 2, p. 1–25, 2016.

73 YAACOUB, J.; NOURA, H.; SALMAN, O.; CHEHAB, A. *Security analysis of drones systems: Attacks, limitations, and recommendations. Internet Things 11: 100218*. 2020.

74 SILVA, J. T. M. d. O projeto sistemas de aeronaves remotamente pilotadas (sarp) no exército brasileiro (2018-2020): principais potencialidades e desafios. Escola Superior de Guerra (Campus Brasília), 2020.

75 LONG, T.; OZGER, M.; CETINKAYA, O.; AKAN, O. B. Energy neutral internet of drones. *IEEE Communications Magazine*, IEEE, v. 56, n. 1, p. 22–28, 2018.

76 TRAUB, L. W. Range and endurance estimates for battery-powered aircraft. *Journal of Aircraft*, v. 48, n. 2, p. 703–707, 2011.

77 BASAN, E.; BASAN, A.; NEKRASOV, A.; FIDGE, C.; GAMEC, J.; GAMCOVÁ, M. A self-diagnosis method for detecting uav cyber attacks based on analysis of parameter changes. *Sensors*, Multidisciplinary Digital Publishing Institute, v. 21, n. 2, p. 509, 2021.

78 HARTMANN, G. A. *A anomalia magnética do atlântico sul: causas e efeitos*. Tese (Doutorado) — Universidade de São Paulo, 2005.

79 MATSUOKA, M. T. Influência de diferentes condições da ionosfera no posicionamento por ponto com gps: avaliação na região brasileira. 2007.

80 FERREIRA, R.; GASPAR, J.; SEBASTIÃO, P.; SOUTO, N. Effective gps jamming techniques for uavs using low-cost sdr platforms. *Wireless Personal Communications*, Springer, v. 115, n. 4, p. 2705–2727, 2020.

81 ARTHUR, M. P. Detecting signal spoofing and jamming attacks in uav networks using a lightweight ids. In: IEEE. *2019 international conference on computer, information and telecommunication systems (CITS)*. [S.l.], 2019. p. 1–5.

82 HE, D.; QIAO, Y.; CHAN, S.; GUIZANI, N. Flight security and safety of drones in airborne fog computing systems. *IEEE Communications Magazine*, IEEE, v. 56, n. 5, p. 66–71, 2018.

83 CAVOUKIAN, A. *Privacy and drones: Unmanned aerial vehicles*. [S.l.]: Information and Privacy Commissioner of Ontario, Canada Ontario, 2012.

84 CASTRILLO, V. U.; MANCO, A.; PASCARELLA, D.; GIGANTE, G. A review of counter-uas technologies for cooperative defensive teams of drones. *Drones*, MDPI, v. 6, n. 3, p. 65, 2022.

85 TUŚNIO, N.; WRÓBLEWSKI, W. The efficiency of drones usage for safety and rescue operations in an open area: a case from poland. *Sustainability*, MDPI, v. 14, n. 1, p. 327, 2021.

86 AJAKWE, S.; AKTER, R.; KIM, D.; MOHATSIN, G.; KIM, D.; LEE, J. Anti-drone systems design: Safeguarding airspace through real-time trustworthy ai paradigm. In: *Proceedings of the 2nd Korea Artificial Intelligence Conference (KAIC 2021), Da Nang, Vietnam*. [S.l.: s.n.], 2021. p. 27–28.

87 INTERPOL. *Framework for Responding to a Drone Incident*. Disponível em https://www.interpol.int/News-and-Events/News/2021/INTERPOL-carries-out-full-scale-drone-countermeasure-exercise/. Acesso em 12 novembro 2022.

88 CABRERA-PONCE, A. A.; MARTINEZ-CARRANZA, J.; RASCON, C. Detection of nearby uavs using a multi-microphone array on board a uav. *International Journal of Micro Air Vehicles*, SAGE Publications Sage UK: London, England, v. 12, p. 1756829320925748, 2020.

89 BENYAMIN, M.; GOLDMAN, G. H. *Acoustic detection and tracking of a Class I UAS with a small tetrahedral microphone array*. [S.l.], 2014.

90 CHANG, X.; YANG, C.; WU, J.; SHI, X.; SHI, Z. A surveillance system for drone localization and tracking using acoustic arrays. In: IEEE. *2018 IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM)*. [S.l.], 2018. p. 573–577.

91 SEDUNOV, A.; HADDAD, D.; SALLOUM, H.; SUTIN, A.; SEDUNOV, N.; YAKUBOVSKIY, A. Stevens drone detection acoustic system and experiments in acoustics uav tracking. In: IEEE. *2019 IEEE International Symposium on Technologies for Homeland Security (HST)*. [S.l.], 2019. p. 1–7.

92 EZUMA, M.; ERDEN, F.; ANJINAPPA, C. K.; OZDEMIR, O.; GUVENC, I. Detection and classification of uavs using rf fingerprints in the presence of wi-fi and bluetooth interference. *IEEE Open Journal of the Communications Society*, IEEE, v. 1, p. 60–76, 2019.

93 LYKOU, G.; MOUSTAKAS, D.; GRITZALIS, D. Defending airports from uas: A survey on cyber-attacks and counter-drone sensing technologies. *Sensors*, Multidisciplinary Digital Publishing Institute, v. 20, n. 12, p. 3537, 2020.

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

95 MICHEL, A. *Counter-drone systems . Bard College*. 2019.

96 DONATTI, M. M. et al. Sistema de spoofing para intervenção de voo em aeronaves não tripuladas guiadas por radiofrequência através de modulação multicanais. [sn], 2017.

97 KRISHNA, C. L.; MURPHY, R. R. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In: IEEE. *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*. [S.l.], 2017. p. 194–199.

98 TEDESCHI, P.; OLIGERI, G.; PIETRO, R. D. Leveraging jamming to help drones complete their mission. *IEEE Access*, IEEE, v. 8, p. 5049–5064, 2019.

99 MULTERER, T.; GANIS, A.; PRECHTEL, U.; MIRALLES, E.; MEUSLING, A.; MIETZNER, J.; VOSSIEK, M.; LOGHI, M.; ZIEGLER, V. Low-cost jamming system against small drones using a 3d mimo radar based tracking. In: IEEE. *2017 European Radar Conference (EURAD)*. [S.l.], 2017. p. 299–302.

100 VATTAPPARAMBAN, E.; GüVENç, ; YUREKLI, A. ; AKKAYA, K.; ULUAğAç, S. Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In: *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. [S.l.: s.n.], 2016. p. 216–221.

101 ULRICH, P. H.; NOBRE, J. C. Análise do estado da arte em segurança cibernética com drones. *Revista Eletrônica de Iniciação Científica em Computação*, v. 17, n. 1, 2019.

102 AKRAM, R. N.; MARKANTONAKIS, K.; MAYES, K.; HABACHI, O.; SAUVERON, D.; STEYVEN, A.; CHAUMETTE, S. Security, privacy and safety evaluation of dynamic and static fleets of drones. In: IEEE. *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*. [S.l.], 2017. p. 1–12.

103 GOODRICH, M. T.; TAMASSIA, R. *Introdução à segurança de computadores*. [S.l.]: Bookman, 2013.

104 PAUNER, C.; KAMARA, I.; VIGURI, J. Drones. current challenges and standardisation solutions in the field of privacy and data protection. In: IEEE. *2015 ITU Kaleidoscope: Trust in the Information Society (K-2015)*. [S.l.], 2015. p. 1–7.

105 HASAN, N.; CHAMOLI, A.; ALAM, M. Privacy challenges and their solutions in iot. In: *Internet of things (IoT)*. [S.l.]: Springer, 2020. p. 219–231.

106 HARTMANN, K.; STEUP, C. The vulnerability of uavs to cyber attacks-an approach to the risk assessment. In: IEEE. *2013 5th international conference on cyber conflict (CYCON 2013)*. [S.l.], 2013. p. 1–23.

107 YAMPOLSKIY, M.; HORVATH, P.; KOUTSOUKOS, X. D.; XUE, Y.; SZTIPANOVITS, J. Taxonomy for description of cross-domain attacks on cps. In: *Proceedings of the 2nd ACM international conference on High confidence networked systems*. [S.l.: s.n.], 2013. p. 135–142.

108 YAHUZA, M.; IDRIS, M. Y. I.; AHMEDY, I. B.; WAHAB, A. W. A.; NANDY, T.; NOOR, N. M.; BALA, A. Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access*, IEEE, v. 9, p. 57243–57270, 2021.

109 HUMPHREYS, T. Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing. *University of Texas at Austin (July 18, 2012)*, p. 1–16, 2012.

110 ALDAEJ, A.; AHANGER, T. A.; ATIQUZZAMAN, M.; ULLAH, I.; YOUSUFUDIN, M. Smart cybersecurity framework for iot-empowered drones: Machine learning perspective. *Sensors*, MDPI, v. 22, n. 7, p. 2630, 2022.

111 DAO-JING, H.; XIAO, D.; YIN-RONG, Q.; YAO-KANG, Z.; QIANG, F.; WANG, L. A survey on cyber cecurity of unmanned aerial vehicles. *Jisuanji Xuebao/Chinese Journal of Computers. Science Press. 2019*, 2019.

112 ABDELMABOUD, A. The internet of drones: Requirements, taxonomy, recent advances, and challenges of research trends. *Sensors*, MDPI, v. 21, n. 17, p. 5718, 2021.

113 SHRESTHA, R.; OH, I.; KIM, S. A survey on operation concept, advancements, and challenging issues of urban air traffic management. *Frontiers in Future Transportation*, Frontiers, p. 1, 2021.

114 MAROJEVIC, V.; GUVENC, I.; DUTTA, R.; SICHITIU, M. L.; FLOYD, B. A. Advanced wireless for unmanned aerial systems: 5g standardization, research challenges, and aerpaw architecture. *IEEE Vehicular Technology Magazine*, IEEE, v. 15, n. 2, p. 22–30, 2020.

115 ANSARI, S.; TAHA, A.; DASHTIPOUR, K.; SAMBO, Y.; ABBASI, Q. H.; IMRAN, M. A. Urban air mobility-a 6g use case? *Frontiers in Communications and Networks*, Frontiers, 2021.

116 FERREIRA, J. R. da A. Aplicabilidade da tecnologia 5g para uso dos órgãos de segurança pública. *O Comunicante*, v. 10, n. 1, p. 43–49, 2020.

117 GRASSO, C.; SCHEMBRA, G. A fleet of mec uavs to extend a 5g network slice for video monitoring with low-latency constraints. *Journal of Sensor and Actuator Networks*, MDPI, v. 8, n. 1, p. 3, 2019.

118 ALSAMHI, S. H.; SHVETSOV, A. V.; KUMAR, S.; HASSAN, J.; ALHARTOMI, M. A.; SHVETSOVA, S. V.; SAHAL, R.; HAWBANI, A. Computing in the sky: A survey on intelligent ubiquitous computing for uav-assisted 6g networks and industry 4.0/5.0. *Drones*, MDPI, v. 6, n. 7, p. 177, 2022.

119 PEY, J. N. A.; NZE, G. D. A.; ALBUQUERQUE, R. de O. Analysis of jamming and spoofing cyber-attacks on drones. In: IEEE. *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*. [S.l.], 2022. p. 1–4.

120 ZHANG, Z.; XIAO, Y.; MA, Z.; XIAO, M.; DING, Z.; LEI, X.; KARAGIANNIDIS, G. K.; FAN, P. 6g wireless networks: Vision, requirements, architecture, and key technologies. *IEEE Vehicular Technology Magazine*, IEEE, v. 14, n. 3, p. 28–41, 2019.

121 NAYAK, S.; PATGIRI, R. 6g communications: A vision on the potential applications. arxiv 2020. *arXiv preprint arXiv:2005.07531*.

122 SHRESTHA, R.; BAJRACHARYA, R.; KIM, S. 6g enabled unmanned aerial vehicle traffic management: A perspective. *IEEE Access*, IEEE, v. 9, p. 91119–91136, 2021.

123 HAYAT, S.; YANMAZ, E.; MUZAFFAR, R. Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. *IEEE Communications Surveys & Tutorials*, IEEE, v. 18, n. 4, p. 2624–2661, 2016.

124 GUPTA, L.; JAIN, R.; VASZKUN, G. Survey of important issues in uav communication networks. *IEEE Communications Surveys & Tutorials*, IEEE, v. 18, n. 2, p. 1123–1152, 2015.

125 MOTLAGH, N. H.; TALEB, T.; AROUK, O. Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives. *IEEE Internet of Things Journal*, IEEE, v. 3, n. 6, p. 899–922, 2016.

126 JIANG, J.; HAN, G. Routing protocols for unmanned aerial vehicles. *IEEE Communications Magazine*, IEEE, v. 56, n. 1, p. 58–63, 2018.

127 KHAWAJA, W.; GUVENC, I.; MATOLAK, D. W.; FIEBIG, U.-C.; SCHNECKENBURGER, N. A survey of air-to-ground propagation channel modeling for unmanned aerial vehicles. *IEEE Communications Surveys & Tutorials*, IEEE, v. 21, n. 3, p. 2361–2391, 2019.

128 KHUWAJA, A. A.; CHEN, Y.; ZHAO, N.; ALOUINI, M.-S.; DOBBINS, P. A survey of channel modeling for uav communications. *IEEE Communications Surveys & Tutorials*, IEEE, v. 20, n. 4, p. 2804–2821, 2018.

129 LU, M.; BAGHERI, M.; JAMES, A. P.; PHUNG, T. Wireless charging techniques for uavs: A review, reconceptualization, and extension. *IEEE Access*, IEEE, v. 6, p. 29865–29884, 2018.

130 CAO, X.; YANG, P.; ALZENAD, M.; XI, X.; WU, D.; YANIKOMEROGLU, H. Airborne communication networks: A survey. *IEEE Journal on Selected Areas in Communications*, IEEE, v. 36, n. 9, p. 1907–1926, 2018.

131 MOZAFFARI, M.; SAAD, W.; BENNIS, M.; NAM, Y.-H.; DEBBAH, M. A tutorial on uavs for wireless networks: Applications, challenges, and open problems. *IEEE communications surveys & tutorials*, IEEE, v. 21, n. 3, p. 2334–2360, 2019.

132 BRASIL. *Política Nacional de Inteligência de Segurança Publica*. Disponível em http://www.planalto.gov.br/ccivil$_03/_{A}to2019-2022/2021/Decreto/D10777.htm/$.

133 BRASIL. *Estratégia Nacional de Inteligência de Segurança Publica*. Disponível em https://www.planalto.gov.br/ccivil$_03/_ato2019-2022/2021/decreto/D10778.htm/$.

134 FAB. *Manual Comando Aeronáutica 56/4*. Disponível em https://publicacoes.decea.mil.br/publicacao/mca-56-4. Acesso em 05 novembro 2022.

135 DRONE/UAS. DECEA. Disponível em https://www.decea.mil.br/drone/. Acesso em 07 de setembro de 2022.

136 FBSP. *Anuário do Forum brasileiro de Segurança Pública 2022*. Disponível em https://forumseguranca.org.br/anuario-brasileiro-seguranca-publica/. Acesso em 08 novembro 2022.

137 SARPAS. DECEA. Disponível em https://sarpas.decea.mil.br/. Acesso em 07 de setembro de 2022.

138 SISANT. ANAC. Disponível em https://sistemas.anac.gov.br/sisant. Acesso em 07 de setembro de 2022.

139 WATKINS, S.; BURRY, J.; MOHAMED, A.; MARINO, M.; PRUDDEN, S.; FISHER, A.; KLOET, N.; JAKOBI, T.; CLOTHIER, R. Ten questions concerning the use of drones in urban environments. *Building and Environment*, Elsevier, v. 167, p. 106458, 2020.

140 BELTON, V.; STEWART, T. *Multiple criteria decision analysis: an integrated approach*. [S.l.]: Springer Science & Business Media, 2002.

141 UFF, M. Â. L.; UFF, A. V. T.; PMERJ, M. P. B.; UFF, C. F. S. G. Avaliação de drones para segurança pública: Uma abordagem multicritério mediante a sistemática promethee-sapevo-m1.

142 JEAN-PIERRE, B.; BERTRAND, M. Promethee methods. *Centrum Voor Statistiek Operationeel Onderzoek, Brussel University. Belgia*, 2004.

143 GOMES, C. F. S.; SANTOS, M. d.; TEIXEIRA, L. F. H. d. S. d. B.; SANSEVERINO, A. M.; BARCELOS, M. R. d. S. Sapevo-m: a group multicriteria ordinal ranking method. *Pesquisa Operacional*, SciELO Brasil, v. 40, 2020.

144 GETTINGER, D. *PUBLIC SAFETY DRONES, 3rd EDITION*. Disponível em https://dronecenter.bard.edu/files/2020/03/CSD-Public-Safety-Drones-3rd-Edition-Web.pdf. Acesso em 05 novembro 2022.

145 H2FOZ. *Projeto Muralha Inteligente RFB e Itaipu Binacional*. Disponível em https://www.h2foz.com.br/geral/contrabando-na-mira-projeto-de-itaipu-e-receita-vai-criar-muralha-inteligente-em-foz/. Disponível em 23 de novembro de 2022.

146 CHIAVENATO, I. *Gestão de pessoas*. [S.l.]: Elsevier Brasil, 2008.