DISSERTAÇÃO DE MESTRADO PROFISSIONAL

GESTÃO DO RISCO CIBERNÉTICO À IMPLANTAÇÃO ADS-B NO ÂMBITO DO SISCEAB POR MEIO DO MÉTODO DE GERENCIAMENTO DE RISCOS À SEGURANÇA OPERACIONAL (GRSO)

Luiz Henrique Filadelfo Cardoso

Brasília, Fevereiro de 2023.

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL EM ENGENHARIA ELÉTRICA

CYBER RISK MANAGEMENT FOR ADS-B IMPLEMENTATION IN SCOPE OF SISCEAB THROUGH THE METHOD OF OPERATIONAL SAFETY RISK MANAGEMENT (GRSO)

GESTÃO DO RISCO CIBERNÉTICO À IMPLANTAÇÃO ADS-B NO ÂMBITO DO SISCEAB POR MEIO DO MÉTODO DE GERENCIAMENTO DE RISCOS À SEGURANÇA OPERACIONAL (GRSO)

LUIZ HENRIQUE FILADELFO CARDOSO

ORIENTADOR: GEORGES DANIEL AMVAME NZE, PhD.

DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM
ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPEE.MP.036
BRASÍLIA/DF: FEVEREIRO - 2023.

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

GESTÃO DO RISCO CIBERNÉTICO À IMPLANTAÇÃO ADS-B NO ÂMBITO DO SISCEAB POR MEIO DO MÉTODO DE GERENCIAMENTO DE RISCOS À SEGURANÇA OPERACIONAL (GRSO)

Luiz Henrique Filadelfo Cardoso

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, PhD., FT/UnB _____
Presidente da Banca Examinadora e Orientador

Prof. Rafael Rabelo Nunes, Dr., FT/UnB _____
Examinador Interno

Pesquisador McWillian de Oliveira, Dr., ATECH _____
Examinador externo

Prof. Vinícius Pereira Gonçalves, Dr., FT/UnB _____
Examinador Interno Suplente

FICHA CATALOGRÁFICA

CARDOSO, LUIZ HENRIQUE FILADELFO
GESTÃO DO RISCO CIBERNÉTICO À IMPLANTAÇÃO ADS-B NO ÂMBITO DO SISCEAB POR MEIO DO MÉTODO DE GERENCIAMENTO DE RISCOS À SEGURANÇA OPERACIONAL (GRSO) [Distrito Federal] 2023..
xvi, 60 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2023.).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica
1. SEGURANÇA CIBERNÉTICA
2. AMEAÇA CIBERNÉTICA
3. VIGILÂNCIA AÉREA
4. CNS/ATM

REFERÊNCIA BIBLIOGRÁFICA

CARDOSO, L.H.F. (2023.). *GESTÃO DO RISCO CIBERNÉTICO À IMPLANTAÇÃO ADS-B NO ÂMBITO DO SISCEAB POR MEIO DO MÉTODO DE GERENCIAMENTO DE RISCOS À SEGURANÇA OPERACIONAL (GRSO)*. Dissertação de Mestrado Profissional, Publicação: PPEE.MP.036, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 60 p.

CESSÃO DE DIREITOS

AUTOR: Luiz Henrique Filadelfo Cardoso
TÍTULO: GESTÃO DO RISCO CIBERNÉTICO À IMPLANTAÇÃO ADS-B NO ÂMBITO DO SISCEAB POR MEIO DO MÉTODO DE GERENCIAMENTO DE RISCOS À SEGURANÇA OPERACIONAL (GRSO).
GRAU: Mestre em Engenharia Elétrica ANO: 2023.

Luiz Henrique Filadelfo Cardoso
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho aos que virão depois de mim, e que mesmo com as dificuldades do dia a dia, nunca deixarão de sonhar grande e encontrar caminhos para tornar tais sonhos em realidade, acrescentando sua contribuição ao irrefreável e indispensável progresso científico. E como dito pelo filósofo grego Sócrates (470 - 399 a.C.): "*A vida sem ciência é uma espécie de morte*".

AGRADECIMENTOS

Agradeço a todos que, *"com seus ombros de gigante"*, proporcionaram-me ver além: aos professores e professoras do Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE), pelos seus ensinamentos, motivação, exemplos e conselhos; aos profissionais da Secretaria do PPEE pelo sempre célere e competente suporte acadêmico-administrativo; e, em especial ao Prof. Dr. Georges Daniel Amvame Nze, meu estimado orientador, e a minha amada (e paciente) esposa Lilian. Sem vocês, essa jornada seria infrutífera.

RESUMO

Entre as tecnologias empregadas para a vigilância aérea, a ADS-B é a mais proeminente em discussão atualmente. Tal tecnologia consiste em um conjunto de equipamentos e protocolos destinados a prover meios para determinar a posição de aeronaves em voo a partir de sistemas de navegação via satélite, bem como periodicamente radiodifundir informações de interesse para outras aeronaves em rota e sensores em solo dentro da sua zona de alcance. No entanto, residem sérias vulnerabilidades de segurança no cerne ADS-B, assim como a literatura não é clara quanto aos impactos negativos da exploração de tais brechas na atuação de controladores de tráfego aéreo e pilotos em comando de voo, sobretudo nas fases críticas do voo. Este estudo objetivou lançar um olhar analítico sobre as vulnerabilidades presentes no sistema ADS-B, não só ao mapear as ameaças ao referido protocolo, mas também ao buscar identificar, analisar e avaliar os riscos cibernéticos inerentes à manutenção da segurança operacional quando da sua implantação no âmbito do SISCEAB, por meio de específica modelagem de ameaças cibernéticas e método de gerenciamento de riscos, qual seja, o método GRSO. Entre os principais resultados, foram identificados riscos à segurança operacional inaceitáveis, tais como: a interferência ou a sobreposição intencional de sinal contra aeronaves; e a injeção individual e múltipla de mensagens ADS-B modificadas ou ilegítimas, todas contra aeronaves. Em contrapartida, os outros riscos cibernéticos à segurança operacional identificados, analisados e avaliados como de média gradação, todos voltados contra estações de solo ADS-B e a interceptação de mensagens, ainda que não diretamente passíveis de extrema urgência de tratamento e eliminação, revestem-se da necessidade de mitigação e monitoramento constante, caso venham a ser tolerados ou aceitos pelas autoridades competentes pela segurança operacional brasileira.

Palavras-chave: Segurança Cibernética, Ameaça Cibernética, Vigilância Aérea, CNS/ATM.

ABSTRACT

Among the technologies employed for air surveillance, ADS-B is the most prominent one under discussion today. This technology consists of a set of equipment and protocols designed to provide means for determining the position of aircraft in flight from satellite navigation systems, as well as periodically broadcasting information of interest to other aircraft en route and sensors on the ground within its range. However, there are serious security vulnerabilities at the core of ADS-B, just as the literature is not clear about the negative impacts of exploiting such breaches on the performance of Air Traffic Controllers and pilots in flight command, especially in the critical phases of the flight. This study aims to take an analytical look at the vulnerabilities present in the ADS-B system, not only by mapping the threats to that protocol, but also by seeking to identify, analyze and assess the cyber risks inherent in maintaining operational security and its implementation in the scope of SISCEAB, through specific modeling of cyber threats and risk management method, which is the GRSO method. Among the main results, unacceptable operational safety risks were identified, such as: interference or intentional overlapping of signals against aircraft; and the individual and multiple injection of modified or illegitimate ADS-B messages, all against aircraft. On the other hand, the other cyber risks to operational security identified, analyzed and evaluated as of medium gradation, all directed against ADS-B ground stations and the interception of messages, although not directly subject to the extreme urgency of treatment and elimination, are if there is a need for mitigation and constant monitoring, if they are tolerated or accepted by the competent authorities for Brazilian operational safety.

Keywords: Cybersecurity, Cyber Threat, Air Surveillance, CNS/ATM.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

As abreviaturas e siglas relacionadas encontram-se no corpo do presente documento e têm os significados de acordo com a relação abaixo:

ACAS: Sistema Anticolisão de Bordo (*Airborne Collision Avoidance System*).

ACC: Centro de Controle de Área (*Area Control Center*).

ADS: Vigilância Dependente Automática (*Automatic Dependent Surveillance*).

ADS-B: Vigilância Dependente Automática por Radiodifusão (*Automatic Dependent Surveillance – Broadcast*).

ADS-C: Vigilância Dependente Automática por Contrato (*Automatic Dependent Surveillance – Contract*).

ANS: Serviços de Navegação Aérea (*Air Navigation Services*)

APP: Centro de Controle de Aproximação (*Approach Control*).

ATC: Controle de Tráfego Aéreo (*Air Traffic Control*).

ATCO: Controlador de Tráfego Aéreo (*Air Traffic Controller*).

ATM: Gerenciamento de Tráfego Aéreo (*Air Traffic Management*).

ATS: Serviço de Tráfego Aéreo (*Air Traffic Services*).

CNS/ATM: Comunicações, Navegação e Vigilância/Gerenciamento de Tráfego Aéreo (*Communications, Navigation and Surveillance/Air Traffic Management*).

CPDLC: Comunicações entre Piloto e Controlador por Enlace de Dados (Controller Pilot Data Link Communications).

DCA: Diretriz do Comando da Aeronáutica.

DECEA: Departamento de Controle do Espaço Aéreo.

EPTA: Estações Prestadoras de Serviços de Telecomunicações e de Tráfego Aéreo.

EUROCONTROL: Organização Europeia para a Segurança da Navegação Aérea (*European Organization for the Safety of Air Navigation*).

FAA: Administração Federal de Aviação – Estados Unidos da América (*Federal Aviation Administration*).

GPS: Sistema Global de Posicionamento – Estados Unidos da América (*Global Positioning System*).

HF: Alta Frequência (*High Frequency*).

ICAO: Organização de Aviação Civil Internacional (*International Civil Aviation Organization*).

ILS: Sistema de Pouso por Instrumentos (*nstrument Landing System*).

MCA: Manual do Comando da Aeronáutica.

MLAT: Sistema de Multilateração (*Multilateration System*).

OACI: Organização de Aviação Civil Internacional.

PBN: Navegação Baseada em Performance (*Performance-Based Navigation*).

PCA: Plano do Comando da Aeronáutica.

PSNA: Provedor de Serviços de Navegação Aérea

PSR: Radar Primário de Vigilância (*Primary Surveillance Radar*).

RPA: Aeronave Remotamente Pilotada (*Remotely Piloted Aircraft*).

RPAS: Sistema de Aeronaves Remotamente Pilotadas (*Remotely Piloted Aircraft System*).

SAR: Busca e Salvamento (*Search and Rescue*).

SATCOM: Comunicações Via Satélite (*Satellite Communications*).

SDR: Rádio Definido por Software (*Software-Defined Radio*)

SISCEAB: Sistema de Controle do Espaço Aéreo Brasileiro.

SSR: Radar Secundário de Vigilância (*Secondary Surveillance Radar*).

SWIM: Gerenciamento Total da Informação do Sistema (*System Wide Information Management*).

TCAS: Sistema Anticolisão de Tráfego (*Traffic Collision Avoidance System*)

TIC: Tecnologias da Informação e Comunicações.

TMA Área de Controle Terminal (*Terminal Control Area*).

TWR Torre de Controle de Aeródromo ou Controle de Aeródromo (*Aerodrome Control Tower or Aerodrome Control*).

WAM: Multilateração de Grande Área (*Wide Area Multilateration*).

1 INTRODUÇÃO

"O inventor, como a natureza de Linneu, não faz saltos; progride de manso, evolui."

Alberto Santos Dumont

Neste primeiro capítulo, serão tecidas considerações em relação aos aspectos inerentes (e precedentes) à implantação do sistema ADS-B no âmbito do SISCEAB, às motivações que conduziram o desenvolvimento desta pesquisa, aos objetivos, à definição do problema a ser investigado, à metodologia de estudo proposta bem como às principais contribuições e à estrutura definida para apresentação do estudo.

1.1 CONTEXTUALIZAÇÃO

De acordo com o exposto em [8], o Controle de Trafego Aéreo (ATC) é considerado meio-chave para viabilizar o transporte aéreo seguro de pessoas e cargas, principalmente a partir de um contexto de demanda crescente por tais serviços. Nessa direção, pesquisas de órgãos reguladores e empresas do setor aéreo, como as apresentadas em [9], [10] e [11], apontam que durante as próximas duas décadas (2021-2040) a demanda por transporte aéreo de passageiros aumentará em taxas médias de 4% ao ano e de cargas em níveis próximos de 3,5% anuais, sobretudo a partir de 2023 e 2024, anos nos quais especialistas acreditam que se restabelecerá o patamar vivenciado no inicio do ano de 2019, antes da pandemia de COVID-19.

Por consequência, devido ao cenário emergente apresentado, sistemas de Gerenciamento do Tráfego Aéreo (ATM) cada vez mais estarão expostos e pressionados por diferentes desafios, tais como: busca pela cobertura total de vigilância em qualquer condição climática e de terreno; aumento da complexidade na separação de aeronaves de diferentes performances em voo; ameaças como sabotagens e ataques à infraestrutura aeroportuária, de navegação aérea e a outros sistemas ligados ao controle de tráfego aéreo [8].

Para que tais adversidades não coloquem em perigo a segurança e operacionalidade do tráfego aéreo e seu controle, torna-se necessário que os sistemas de vigilância aérea e procedimentos correlatos permaneçam em constante evolução e aperfeiçoamento tecnológico.

Atualmente, tal qual apontado também por [8], os principais sistemas de vigilância aérea em operação são suportados, sobretudo, pelas seguintes tecnologias: comunicações por voz e dados via rádio (entre controladores e pilotos) e sistemas Radar Primário de Vigilância e Radar Secundário de Vigilância (PSR e SSR, respectivamente).

Quanto às tecnologias radar, mesmo que o funcionamento de tais sistemas já perdure por décadas e suas características se proponham a serem complementares, as citadas tecnologias mostram-se ultrapassadas, sobretudo quanto à baixa acurácia de suas leituras em ambientes de alta densidade de tráfego aéreo e

ao custo envolvido para instalação e manutenção em áreas remotas ou de difícil acesso [8, 12]. Outros fatores de obsolescência patente e que cabem destacar é a limitação de detecção de aeronaves em voos à baixa altitude e a inadequada cobertura em regiões inóspitas, tais como sobre florestas, oceanos e regiões montanhosas [13].

Muito devido às limitações e perspectivas demandantes do futuro já mencionadas e também salientadas por [14], esforços têm sido realizados nas últimas décadas por relevantes órgãos internacionais da aviação civil, como ICAO/OACI, FAA e EUROCONTROL, para o desenvolvimento de novas alternativas para vigilância do espaço aéreo que conjuguem acurácia e confiabilidade com menor custo de implantação e manutenção. Dessas, a mais promissora é a Vigilância Dependente Automática por Radiodifusão (do inglês, Automatic Dependent Surveillance-Broadcast - ADS-B).

Tal qual depreendido em [13] e [14], a tecnologia ADS-B pode ser entendida como um conjunto de equipamentos, procedimentos e protocolo destinados a prover meios para determinar precisa posição em voo ou em solo a partir de sistemas baseados em navegação via satélite, bem como, periodicamente radiodifundir, de maneira automática outras informações também de interesse, indistintamente, para outras aeronaves em rota e sensores em terra dentro da sua zona de alcance.

De acordo com o exposto em [15], a ADS-B pode ser usada em conjunto com a operação radar (PSR e SSR) ou usado de forma independente, chamada de ADS-B NRA (*Non-radar Areas*). No entanto, ainda de acordo com [15], "*nas operações ADS-B NRA, é imprescindível que a integridade dos dados fornecidos pela aeronave esteja adequada para fins de vigilância ATS, pois, nessas operações ADS-B NRA, se houver falha da integridade dos dados ADS-B o sistema de vigilância ATS fica comprometido*".

Porém, a implantação e a adoção da ADS-B como principal solução de vigilância área, em substituição parcial ou total aos legados PSR e SSR, já são realidade na maioria dos espaços aéreos no mundo. Países como EUA, Canadá e Austrália, além do espaço aéreo europeu, já contam praticamente com total cobertura de infraestrutura de solo e transceptores instalados em aeronaves, em suporte ao protocolo ora mencionado [7, 12, 14]. No Brasil, ainda tal adoção encontra-se em estado incipiente, apenas com cobertura parcial, e de maneira experimental, na Bacia de Campos (TMA-MACAÉ), com a finalidade de prover o serviço de vigilância de tráfego aéreo em baixa altitude em área oceânica fora da cobertura radar [16, 12] e no acordo firmado e operacionalmente em curso entre a empresa AIREON e o Departamento de Controle do Espaço Aéreo (DECEA) visando à coleta e ao roteamento de dados de vigilância através da ADS-B Satelital [17].

Entretanto, o DECEA, órgão responsável pelo controle do espaço aéreo e navegação aérea brasileira, salienta que seu objetivo é que até dezembro de 2025 todo espaço aéreo brasileiro continental passe a contar em larga escala com suporte do Sistema ADS-B, assim como todas as aeronaves sob controle do SISCEAB passem a contar de forma obrigatória com equipamentos ADS-B IN e ADS-B OUT [16, 18].

Tais objetivos e outros sobre o tema estão consubstanciados na DCA 351-2 “Concepção Operacional ATM Nacional” e no PCA 351-3 “Plano de Implementação ATM Nacional”. A primeira norma, no que tange em específico à tecnologia ADS-B, define a estratégia e os requisitos que devem ser atendidos, assim como os cenários possíveis para adoção da referida tecnologia para um seguro e eficiente Gerenciamento do Trafego Aéreo (ATM) Nacional [18], destacando-se o espaço aéreo oceânico e o espaço aéreo continental como contextos de interesse. Para esse trabalho, o segundo cenário foi o definido como objeto de estudo.

Desta forma, destacam-se como principais objetivos esperados com a implementação da ADS-B em espaço aéreo continental, tal qual exposto em [18]:

- No espaço aéreo continental, a aplicação da ADS-B contribuirá para o aumento da eficiência do sistema, tanto para o provedor dos serviços de navegação aérea quanto para o usuário do espaço aéreo.
- A cobertura efetiva da ADS-B deverá ser suficiente para prover serviço de vigilância ATS em todo o espaço aéreo superior continental, volumes selecionados do espaço aéreo inferior para operações em rota, TMA e aeródromos selecionados.
- No que tange à consciência situacional a bordo das aeronaves, a ADS-B IN permitirá que a tripulação obtenha informações das aeronaves nas proximidades, contribuindo para o aumento da segurança operacional. Em longo prazo, as informações da ADS-B IN propiciarão os elementos necessários para que a tripulação efetue sua própria separação.
- Dever-se-á dimensionar os sistemas radar de forma a garantir que a vigilância do espaço aéreo atenda às necessidades relacionadas ao volume de tráfego e ao sistema integrado civil/militar, assim como a suportar uma fase de transição, provendo serviços de vigilância aos usuários não equipados com ADS-B.

Já quanto à segunda norma, PCA 351-3, focada na operacionalização e no detalhamento de cada programa, projeto e atividades componentes dos empreendimentos necessários para a evolução do SISCEAB rumo ao Conceito Operacional ATM Global estabelecido pela ICAO, entende-se em relação à ADS-B que, considerada a viabilidade técnica e uma relação benefício/custo vantajosa,

> a evolução da vigilância ATS para o espaço aéreo continental será alcançada por meio da implementação de sistemas baseados na tecnologia da Vigilância Automática Dependente por Radiodifusão (ADS-B) e Multilateração de Grande Área (WAN). Em função de seu baixo custo, se comparado com os equipamentos radares, a ADS-B possibilita ampliar a capacidade de vigilância no espaço aéreo nacional, notadamente em áreas remotas ou de baixo movimento, onde radares não apresentam uma boa relação benefício/custo [19].

Ainda com base no PCA 351-3 “Plano de Implementação ATM Nacional”, visando à melhoria na vigilância no solo de veículos e aeronaves em aeródromo, assim como nas fases de aproximação, subida e em rota em espaço aéreo superior, a implantação da ADS-B na área continental sob responsabilidade do SISCEAB seguirá, conforme exposto em [19], um processo baseado em fases, visando prover a inclusão da tecnologia no Sistema ATM Nacional, de forma segura e coerente com as necessidades operacionais, da seguinte forma:

- **Fase 1**: implantação da ADS-B OUT em um volume limitado do espaço aéreo, com o objetivo de confirmar os benefícios operacionais da ADS-B no espaço aéreo nacional, em rota e terminal;
- **Fase 2**: completar a implantação da infraestrutura de terra, visando garantir o adequado atendimento dos requisitos para prover vigilância ATS baseada na ADS-B em todo espaço aéreo superior nacional;

- **Fase 3**: o volume de cobertura do sistema ADS-B será ampliado para viabilizar a vigilância ATS em outros espaços aéreos de interesse, incluindo TMA; e
- **Fase 4**: implantação e emprego operacional das aplicações de bordo baseadas na ADS-B IN.

Ao se entender, muito do depreendido de [20], que o atual estágio da implantação ADS-B no SISCEAB encontra-se no inicio da Fase 2, visto que a empresa Thales anuciou no final do mês de janeiro de 2023 que será a responsável pelo fornecimento e pela instalação de 66 estações de solo para recepção ADS-B distribuídas em território nacional conforme especificado pelo DECEA em processo licitatório de concorrência internacional. Para a conclusão dessa fase e das outras subsequentes com êxito, considera-se como fator essencial, conforme depreendido de [18] e [19], a operação, tanto na perspectiva de pilotos de aeronaves quanto por parte de controladores de tráfego aéreo (ATCO), em níveis de segurança operacional (*Safety*) e de Segurança na Aviação (*Security*) requeridos e compatíveis com atividade aérea. Na Figura 1.1, é possível observar a representação gráfica e em escala, a partir da ferramenta *web Google Earth*, dos locais previstos para instalação das sessenta e seis estações de solo ADS-B destinadas à vigilância em espaço aéreo continental, em suporte ao SISCEAB [21].

Figura 1.1: Localização das Estações de Solo ADS-B a serem instaladas em suporte ao SISCEAB, elaborada pelo autor.

No entanto, e alinhado ao que defende [22], apesar da tecnologia ADS-B ser pródiga em possuir características como alta taxa de repetição da transmissão de informações para o meio (outras aeronaves e estações em solo), maior acurácia na definição da posição por ser baseada em navegação via satélite e reduzido custo de implantação em relação aos outros sistemas radares já descritos e em operação, o Sistema ADS-B carece em sua origem e desenvolvimento de foco voltado à segurança [23].

Brechas com potencial de serem exploradas por agentes adversos sem a necessidade de extenso conhecimento ou alto poder financeiro já foram apontadas tanto na academia quanto em eventos voltados à segurança da informação em relação ao Sistema ADS-B, conforme exposto por [6], [14] e [24].

Tais lacunas de segurança, passíveis de serem exploradas por diferentes modalidades de ataques cibernéticos especialmente focados em vulnerabilidades presentes em componentes do sistema ou no próprio cerne do referido protocolo, mostram-nos que o risco para a segurança e a continuidade das operações aéreas não pode ser desprezado, sobretudo nas fases de pós-decolagem (subida), aproximação final e pouso, momentos sensíveis nos quais a dependência do Sistema ADS-B já é (ou será) imperiosa, sobretudo em nosso contexto de interesse, qual seja, o âmbito do SISCEAB.

1.2 MOTIVAÇÃO

Diante do exposto na seção anterior, fica claro que não só há a necessidade de constante aperfeiçoamento e evolução dos sistemas componentes do "ecossistema" ATM Nacional com a adequada manutenção da segurança operacional mas, principalmente, a opção do SISCEAB pela ADS-B como alternativa de vigilância ATS a ser amplamente utilizada no espaço aéreo continental brasileiro nos anos subsequentes.

Sendo assim, este trabalho possui como principal motivação o entendimento de que diante do atual estágio de conectividade viabilizado pelo espaço cibernético, sobretudo no contexto do SISCEAB em que o SWIM surge com a perspectiva de prover a interconectividade e interoperabilidade de sistemas CNS/ATM em tal meio, é premente a realização de pesquisa em busca do estado da arte no que tange à nova tecnologia a ser implantada no SISCEAB, não só para o entendimento de suas vulnerabilidades e ameaças cibernéticas aplicáveis a tal contexto, mas também para a identificação, análise, avaliação e tratamento dos eventuais riscos cibernéticos existentes no tocante à manutenção da segurança operacional do espaço aéreo brasileiro quando da sua implantação e operação.

1.3 OBJETIVOS

Esse estudo foi desenvolvido com a finalidade de atender os seguintes objetivos:

1.3.1 Objetivo Geral

Identificar, analisar e avaliar as ameaças e riscos cibernéticos à segurança operacional durante a implantação e a operação do sistema ADS-B no âmbito do SISCEAB com a finalidade de auxiliar na assessoria

técnica e no gerenciamento do risco cibernético em suporte ao Comando da Aeronáutica (COMAER), através da Assessoria de Segurança Operacional do Controle do Espaço Aéreo (ASOCEA).

1.3.2 Objetivos Específicos

E como objetivos específicos deste trabalho, estão:

- Identificar e analisar, com base em revisão bibliográfica, as ameaças cibernéticas com capacidade de explorar vulnerabilidades existentes na estrutura e na operação do Sistema ADS-B e aplicáveis ao SISCEAB.
- Identificar, mapear e avaliar o risco cibernético à segurança operacional com base no método de Gerenciamento de Risco à Segurança Operacional (GRSO).
- Assessorar, com recomendações de segurança, fundamentadas em estudos científicos e em melhores práticas adotadas em âmbito mundial, com a intenção de tratar e mitigar os riscos cibernéticos identificados à segurança operacional no âmbito do SISCEAB.

1.4 DEFINIÇÃO E DELIMITAÇÃO DO PROBLEMA

Devido à miríade de perigos (não intencionais e intencionais) que podem advir de uma mudança no âmbito do SISCEAB, máxime com a implantação da ADS-B, optou-se neste trabalho pela realização de investigação científica para mensurar a extensão dos riscos provocados, intencionalmente, por ameaças cibernéticas à implantação e à operação da ADS-B no âmbito do SISCEAB.

Dessa forma, a partir do entendimento depreendido de [25], em que a Aviação Civil é segregada e organizada em três dimensões interdependentes - quais sejam, Controle de Tráfego Aéreo (ATC), Aeronaves/Indústria da Aviação e Aeroportos - de mesma valia e que requerem atenção quanto à realização de estudos em busca de vulnerabilidades cibernéticas e de soluções mitigadoras, este trabalho possui como escopo e delimitação o estudo das vulnerabilidades, das ameaças cibernéticas e dos riscos inerentes existentes no Sistema ADS-B e capazes de impactarem na segurança operacional e na consciência situacional de pilotos em voo (aeronaves) e (ou) controladores de tráfego aéreo em serviço (ATC) atuantes no SISCEAB. Dentre elas, destacam-se aquelas ameaças voltadas às fases críticas do voo: decolagem, descida, aproximação final e pouso. Para isso, nessa pesquisa foram utilizados estudos e outras informações de interesse produzidas nos últimos doze anos em trabalhos de credibilidade confirmada por pares e depositados em repositórios de amplo conhecimento no meio científico.

Buscou-se também centrar atenção nas normas internas do Comando da Aeronáutica que tratam do tema Segurança Operacional, bem como a utilização de método de gerenciamento de riscos já adotado no contexto do SISCEAB com comprovada efetividade no controle do risco e aderente ao contexto de pesquisa, qual seja: Gerenciamento de Risco à Segurança Operacional (GRSO).

1.4.1 Considerações Éticas

Tal qual será abordado e documentado nesta dissertação através do produto de investigação de diferentes autores do meio acadêmico e da comunidade de segurança da informação, existem diferentes ameaças cibernéticas comprovadamente capazes de explorarem vulnerabilidades existentes na ADS-B e seus subsistemas adjacentes.

Dessa forma, optou-se pela não repetição em laboratório dos métodos e resultados utilizados para conformação dos ataques presentes nas referidas pesquisas por entendermos que os riscos da eventual emissão de sinal ADS-B ilegítimo (ainda que não intencional) poderia ensejar em ameaça para aeronaves em voo e controladores de tráfego aéreo e por acreditarmos que as diversas pesquisas realizadas (e referências utilizadas) com tal objetivo são suficientes e sólidas cientificamente (já comprovadas por pares e abordadas como referências basilares para outros trabalhos publicados). Assim, evitaremos, também, eventuais riscos à segurança operacional devido à localização do pesquisador e da Universidade de Brasília na zona de influência da Área Terminal do Aeroporto Internacional de Brasília - Presidente Juscelino Kubitschek.

Sendo assim, acreditamos ser suficiente a adoção da revisão bibliográfica como abordagem adequada para evitar infligir, desnecessariamente, questões éticas e de segurança.

1.5 METODOLOGIA DE PESQUISA EMPREGADA

A metodologia de pesquisa desenvolvida durante o trabalho, para responder a questão-problema e atingir os objetivos propostos, consiste em:

1) Realizar pesquisa exploratória e qualitativa a partir da revisão bibliográfica em periódicos, livros, dissertações, teses, trabalhos correlatos e outros meios e veículos acadêmicos que dissertem sobre temas e questões que se correlacionem com os assuntos afetos à pesquisa, tais como ADS-B e suas particularidades, segurança cibernética, modelagem de ameaças cibernéticas, gestão de riscos cibernéticos e segurança da aviação (*safety* e *security*).

2) Realizar estudo detalhado das publicações e normas do Comando da Aeronáutica que abordem e organizem o Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB), assim como se ocupem da normatização da Segurança Operacional, com destaque aquelas que tratem do Sistema de Gerenciamento da Segurança Operacional (SGSO) e do método de Gerenciamento de Risco à Segurança Operacional (GRSO).

3) Após o estudo da fundamentação teórica, serão identificadas e modeladas as ameaças cibernéticas que podem emergir no cenário de implantação e operação da ADS-B no SISCEAB.

4) Com a intenção de se estimar os riscos cibernéticos, caso as vulnerabilidades identificadas sejam exploradas pelo rol de ameaças cibernéticas listadas, levando-se em conta a probabilidade de ocorrência e a respectiva severidade (pior cenário), utilizar-se-á o método de Gerenciamento de Riscos à Segurança Operacional (GRSO) como o meio para identificar, analisar, e avaliar, a fim de se propor o tratamento e (ou) a mitigação dos referidos riscos cibernéticos constatados.

5) Após a realização do GRSO à implantação ADS-B, com o foco nos riscos cibernéticos de tal mudança no contexto do SISCEAB, os resultados encontrados serão analisados e discutidos com o fito de apresentar ao leitor as linhas de ação e recomendações identificadas para a condução do tratamento ou controle dos riscos identificados.

1.6 ORGANIZAÇÃO DO TRABALHO

Na sequência dessa dissertação, os conhecimentos apreendidos durante a pesquisa serão estruturados da seguinte forma:

- No Capítulo 2 serão apresentados os conhecimentos tidos como fundamentais para o correto entendimento dos conceitos, argumentos, análises e recomendações a serem apresentados na sequência e convergentes à pesquisa realizada.
- No Capítulo 3, serão descritas, em detalhe, as fases realizadas do Gerenciamento de Risco à Segurança Operacional, com o foco nos riscos cibernéticos identificados na implantação do Sistema ADS-B no contexto do SISCEAB.
- O Capítulo 4 se atém a apresentar as principais considerações que emergem como produto da análise e reflexão acerca da avaliação de riscos realizada no capítulo anterior.
- Por fim, o Capítulo 5 desvela as conclusões finais sobre o trabalho desenvolvido, bem como se propõe a traçar linhas de ação para o desenvolvimento de trabalhos futuros.

1.7 CONTRIBUIÇÕES

Além das contribuições inerentes à finalização deste estudo em tela e consolidado no formato dissertação, residem também como contribuições, já consolidada e esperadas:

- Publicação de artigo completo intitulado “Exploração do Sistema ADS-B: análise do impacto no processo decisório de controladores de tráfego aéreo por meio do método GRSO”, apresentado na 15ª Conferência Ibérica de Sistemas e Tecnologias da Informação (CISTI), realizada na cidade de Sevilha, Espanha, 2020;
- Disponibilização de versão digital dessa dissertação ao órgão responsável pela segurança operacional no âmbito do SISCEAB, qual seja a Assessoria de Segurança Operacional do Controle do Espaço Aéreo (ASOCEA);
- E por fim, objetivam-se, ainda, a publicação e a apresentação de novo artigo completo, resumo das análises e conclusões finais advindas do desenvolvimento desta pesquisa, em primeira oportunidade na *MICRADS’23 - The 2023 Multidisciplinary International Conference of Research Applied to Defense and Security*, a ser realizada em Bogotá, Colômbia, em julho de 2023; e em caso de não

aceite, como alternativa, submissão ao Simpósio de Transporte Aéreo Brasileiro (SITRAER) em sua próxima edição a ser realizada nas instalações da Universidade Federal de Santa Catarina na cidade de Joinville, durante o mês de outubro de 2023.

Não se descarta, preliminarmente, a possibilidade de continuidade de investigações sobre o referido tema (aprofundamento nas formas de mitigação do risco cibernético à ADS-B, sobretudo no que se relaciona à vigilância área aeroembarcada) ou correlato, também em nível stricto sensu (Doutorado Profissional ou Acadêmico), caso seja julgado pertinente pelo orientador e objeto de análise e aprovação de futura banca de seleção.

1.8 TRABALHOS CORRELATOS

Com a finalidade de se obter um panorama acerca da tecnologia ADS-B - suas características, padrões de enlaces adotados em sua implementação, informações de interesse em relação a seus componentes funcionais - e sobre as vantagens e desvantagens em relação a outras tecnologias, sobretudo às PSR e SSR, os trabalhos de Martin Strohmeier et al [6, 22, 26]; e de Mohsen Riahi Manesh e Naima Kaabouch [27] são especialmente esclarecedores, com a profundidade técnica necessária para entendimento da tecnologia sob análise, vindo desta forma a se tornarem referências basilares para este estudo.

Já sobre a existência de vulnerabilidades de segurança na tecnologia ADS-B, as contribuições de Leon Purton, Hussein Abbass e Sameer Alam em [23]; e de Donald McCallie, Jonathan Butts e Robert Mills a partir do presente em [28], são especialmente inovadoras muito por ir além da apresentação das vulnerabilidades e as formas de exploração, mas também ao apontar de maneira inovadora uma taxonomia de ataques possíveis contra o sistema ADS-B. Para esta dissertação, o estudo realizado por Camilo Andres Pantoja Viveros em [29] é complementar e especialmente importante para definição do escopo e taxonomia a ser adotada, não só pela análise realizada dos ataques cibernéticos contra a ADS-B e o rol apresentado de ameaças, mas também pelo panorama traçado acerca do nível de consciência situacional existente entre os especialistas da aviação em relação ao risco à segurança operacional com a implantação ADS-B, principalmente entre controladores de tráfego aéreo e pilotos.

No tocante à conformação de modelos acionáveis para a realização de ataques, os trabalhos de Matthias Schäfer, Vincent Lenders e Ivan Martinovic em [14]; Andrei Costin e Aurelien Francillon em [24]; Brad Haines em [30]; e o realizado em colaboração por Martin Strohmeier, Daniel Moser, Matthias Schäfer, Vincent Lenders e Ivan Martinovic em [31], além de confirmarem a exequibilidade prática de específicos ataques cibernéticos capazes de explorar as vulnerabilidades de segurança existentes na ADS-B, demonstram também o quão acessível são os meios de *software*, *hardware* e conhecimentos disponíveis para a realização de tais ataques. Em relação aos específicos agentes de ameaças contra a aviação civil e as suas principais características e motivações, conhecimento essencial para realização de oportuna modelagem de ameaças cibernéticas à ADS-B, os trabalhos realizados por Martin Strohmeier em [8]; por Martin Strohmeier, Matthias Schäfer, Vincent Lenders, Ivan Martinovic e Matt Smith em [32]; por Georgia Lykou, George Iakovakis e Dimitris Gritzalis em [33]; e por Elochukwu Ukwandu et al em [34] estão entre as referências principais sobre tal tema neste estudo.

Por outro lado, acerca das contramedidas a serem adotadas frente às ameaças cibernéticas à tecnologia ADS-B, os estudos de Martin Strohmeier, Vincent Lenders e Ivan Martinovic em [6]; Mohsen Riahi Manesh e Naima Kaabouch em [27]; e Zhijun Wu, Tong Shang e Anxin Guo em [35] são sólidas referências para este trabalho, não somente para entender quais são as vulnerabilidades ADS-B e como podem ser exploradas, mas sobretudo pela perspectiva de segurança intrínseca em seus estudos, qual seja: a necessidade da adoção de forma complementar e sinérgica de soluções de segurança e meios alternativos CNS/ATM em um modelo de segurança holístico voltado a evitar o risco de degradação parcial ou total de meios e a reduzir a possibilidade da ocorrência de falsos positivos a partir de tráfego aéreo ilegítimo advindos de injeções de mensagens ADS-B maliciosas.

Em relação aos principais estudos sobre a implantação ADS-B em outros espaços aéreos, os trabalhos de Claúdia V. C. Rodrigues em [7]; de Raul S. Cerqueira em [12]; e de Matthias Schäfer, Vincent Lenders e Ivan Martinovic em [14] abordam os contextos europeu, canadense, norte-americano e australiano em detalhes essenciais para obtermos informações acerca de questões técnicas e normativas vivenciadas durante o processo assimilatório, dificuldades encontradas e a dimensão dos esforços adaptativos empregados para adoção de tal tecnologia no rol de alternativas de vigilância ATS nos referidos espaços aéreos. Referencial indispensável para entender e estimar o que será vivenciado no contexto brasileiro.

Porém, entre os estudos que abordam a implantação ADS-B no Brasil, Raul S. Cerqueira em [12] é pródigo em analisar o já adotado em relação à regulação ADS-B existente no Brasil e em âmbito mundial para apresentar suas sugestões em prol do aperfeiçoamento da regulação brasileira a fim de melhor recepcionar tal tecnologia no espaço aéreo nacional. Já os pesquisadores Renan Emílio Scarso e Roberto Márcio dos Santos em [15] traçam um panorama analítico sobre a relação custo-benefício envolvida na instalação e operação ADS-B, tanto para operadores de aeronaves da aviação geral brasileira, quanto para o DECEA; assim como traçam um estudo comparativo entre a ADS-B e as tecnologias de vigilância baseadas em sinais radar existentes. Em complemento, Renato Augusto R. Vilela por meio de seu estudo em [36], propõe identificar e apresentar as vantagens e desvantagens na utilização do sistema ADS-B para controladores de tráfego aéreo, operadores de aeronaves e demais usuários do SISCEAB.

Dessa forma, dos trabalhos relacionados e estudados, apesar de apreendermos um panorama acerca da implantação da tecnologia ADS-B em outros espaços aéreos mundiais, das vulnerabilidades existentes em tal tecnologia, da confirmação da exequibilidade de ataques contra tais brechas de segurança e a abordagem de aspectos regulatórios, a relação custo-benefício e as vantagens e desvantagens da adoção ADS-B em espaço aéreo brasileiro, observamos que não há estudos que correlacionem os eventuais riscos à segurança operacional à implantação da ADS-B em espaço aéreo continental brasileiro, lócus de interesse e sob responsabilidade do SISCEAB. Nesse contexto, pretendemos preencher tal lacuna, ao produzir estudo destinado a identificar, analisar e avaliar as ameaças e riscos cibernéticos à segurança operacional durante a implantação e operação do sistema ADS-B no âmbito do SISCEAB, com a finalidade principal de auxiliar na assessoria técnica e no gerenciamento do risco cibernético em suporte ao Comando da Aeronáutica (COMAER), sobretudo no que tange ao processo decisório e consciência situacional de controladores de tráfego aéreo e pilotos em comando de voo.

2 FUNDAMENTAÇÃO TEÓRICA

"Apenas a teoria decide sobre o que pode ser observado."

Albert Einstein

2.1 ESPAÇO CIBERNÉTICO, SEGURANÇA CIBERNÉTICA E AMEAÇA CIBERNÉTICA

Sobre o que vem ser entendido como espaço cibernético, em [37] afirma-se que "*A literatura técnica define o ciberespaço como ambiente de informação, constituído digitalmente de dados criados, armazenados e compartilhados*". Assim como também "*embora desafie dimensões físicas, não é exclusivamente virtual, por compreender computadores e infraestruturas que permitem aos dados fluir*" [37]. Já de acordo com definição extraída do Glossário de Segurança da Informação do Departamento de Segurança da Informação do Gabinete de Segurança Institucional, Órgão da Presidência da República Federativa do Brasil responsável pelo tema segurança cibernética no âmbito brasileiro, o entendimento é que:

> espaço virtual é composto por um conjunto de canais de comunicação da Internet e outras redes de comunicação, que garantem a interconexão de dispositivos de tecnologia da informação. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas por meio desse ambiente [38].

De forma complementar aos conceitos acima apresentados, e aderente ao defendido por [39], que entende o ciberespaço como um meio centrado na interconectividade entre redes, este trabalho objetiva como definição ideal para espaço cibernético a definida em [40], que afirma sobre tal ambiente ser sobretudo:

> um lócus assimétrico e de intenções não tão claras, no qual sistemas de informações heterogêneos estão conectados por meio de estruturas e recursos distribuídos caoticamente e em que se observa o intenso crescimento e especialização de práticas ilícitas desenvolvidas por indivíduos, grupos organizados e nações em busca de informações privadas, obtenção ilícita de vantagens financeiras e difusão de ideologias e terror. [E desta forma] proteger-se contra a exploração de vulnerabilidades por específicas ameaças consiste em diferencial de grande valia para Estados e organizações que desejam permanecer ativos e operacionais, principalmente a partir do ciberespaço.

Logo, devido a essa necessidade de se contrapor à ação maliciosa de tais ameaças e de proteger adequadamente os ativos presentes ou acessíveis a partir do ciberespaço, emerge como disciplina principal para tal intento a segurança cibernética.

Em [37], Segurança Cibernética é apresentada como a "*arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos*

de informação e suas infraestruturas críticas". Por outro lado e em específico ao setor aéreo, em definição presente no Manual de Conscientização em Segurança Cibernética da Aviação Civil publicado pela ANAC afirma-se que:

> segurança cibernética ou cibersegurança é o estado de proteção contra ciberataques ou qualquer atividade criminosa feita utilizando o ciberespaço como meio. De fato, é um conjunto de ferramentas, políticas, teorias de segurança contra atos de interferência ilícita, capacidades e procedimentos de segurança, práticas de segurança da informação, perícia, gerenciamento de risco e práticas para proteger as organizações do cibercrime [41].

De acordo com o presente novamente em [38], e aderente ao conceito aceito no âmbito do SISCEAB tal qual presente no PCA 351-3 "Plano de Implementação do ATM Nacional"[19], segurança cibernética pode ser interpretada a partir das ações de proteção destinadas a "*garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis*".

Em relação às propriedades essenciais à manutenção da segurança no espaço cibernético, conforme observado na definição anterior, quais sejam Confidencialidade, Integridade, Disponibilidade e Autenticidade, depreendem-se conceitualmente de [38] e [42], que:

- **Confidencialidade**: é a propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;
- **Integridade**: pode ser entendida como a propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- **Disponibilidade**: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados; e
- **Autenticidade**: é entendida como a propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Já sobre Ameaças Cibernéticas, tal qual presente no Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo [43], podem ser entendidas como "*agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas na confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização*". Alinhado a isso, em [37] afirma-se que ataques cibernéticos de atores estatais ou não, proliferam sobretudo frente a Infraestruturas Críticas, dentre elas aquelas ligadas à aviação civil. Esse mesmo autor, ao citar a Política Nacional de Inteligência (PNI) Brasileira também em [37], destaca que ataques cibernéticos podem ser entendidos como:

> Ações deliberadas com o emprego de recursos da tecnologia da informação e comunicações que visem a interromper, penetrar, adulterar ou destruir redes utilizadas por setores públicos e privados essenciais à sociedade e ao Estado, a exemplo daqueles pertencentes à infraestrutura crítica nacional [44].

Entre as principais modalidades de ataques cibernéticos possíveis de serem perpetradas contra ativos e infraestruturas críticas do SISCEAB, de interesse para este estudo, podemos destacar as seguintes:

1. ***Eavesdropping* - Monitoramento e interceptação passiva de mensagens**: um ataque dessa natureza consiste na tentativa de um usuário não autorizado (ilegítimo destinatário da mensagem) interceptar a transmissão de dados entre o emissor e o receptor legítimos, seja para obter o conteúdo de maneira passiva somente, seja para a realização de outros ataques de natureza ativa. A proximidade do alvo e a natureza da transmissão baseada na ampla difusão sem mecanismos de segurança (como criptografia) são características facilitadoras para o êxito em tal modalidade de ataque [42];

2. ***Denial of Service (DoS)* - Negação de serviço**: bloqueio de acesso devidamente autorizado a um recurso ou a geração de atraso nas operações e funções normais de um sistema, com a resultante perda da disponibilidade aos usuários autorizados. O objetivo do ataque *DoS* é interromper atividades legítimas de um computador ou de um sistema. Uma forma de provocar o ataque é aproveitando-se de falhas ou de vulnerabilidades presentes no alvo de interesse, ou enviar um grande número de mensagens que esgotem algum dos recursos da vítima, como CPU, memória, banda, entre outros. Para isso, é necessária uma única fonte emissora, com bom processamento e bastante banda disponível, capaz de gerar o número de mensagens suficiente para causar a interrupção do serviço por exaustação de recursos e serviços no ativo-receptor sob ataque [38, 45, 46];

3. ***Distributed Denial of Service (DDoS)* - Negação de serviço distribuída**: atividade maliciosa, coordenada e distribuída, em que um conjunto de computadores ou de dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Embora os ataques do tipo *DoS* sejam, em geral, perigosos para os serviços de Internet, a forma distribuída é ainda mais perigosa, justamente por se tratar de um ataque feito por várias máquinas ou fontes emissoras, que podem estar espalhadas geograficamente e não terem nenhuma relação entre si, exceto o fato de estarem parcial ou totalmente sob controle do atacante e com a sua transmissão massiva de mensagens centrada para único receptor. Além disso, mensagens *DDoS* podem ser difíceis de identificar por conseguirem facilmente se passar por mensagens de tráfego legítimo, pois enquanto é pouco natural que uma mesma máquina envie várias mensagens semelhantes a um servidor em períodos muito curtos de tempo, como no caso do ataque *DoS*, é perfeitamente natural que várias máquinas enviem mensagens semelhantes de requisição de serviço regularmente a um mesmo servidor ou receptor-alvo, o que disfarça o ataque *DDoS* [38, 45];

4. ***Jamming***: tal modalidade de ataque pode ser definida como uma emissão massiva e direcionada de sinal rádio com a finalidade de causar a degradação parcial ou total por bloqueio, no emissor ou receptor-alvo, em comunicações sem fio [42]. Cabe destacar, que a principal diferença entre *jamming* e interferências causadas por rádio-frequência em canais adjacentes consistem em que a primeira é

intencional e direcionada contra um específico alvo, enquanto as demais são não-intencionais, ocasionais e resultam da presença de emissores próximos que transmitem na mesma ou em frequências muito próximas daquela do receptor impactado [46, 47];

5. ***Spoofing* - Falsificação de identidade/informações**: - ato de falsificar a identidade da fonte de uma comunicação ou interação ou as mensagens propagadas para o meio. Tal ataque permite a possibilidade da retransmissão de dados e informações de interesse legítimos obtidos por meio de *Eavesdropping*, assim como aqueles interceptados, modificados e ilegítimos, todos com o objetivo de enganar ou manipular o receptor-alvo [38, 46, 48];

6. ***Replay Attack* - Ataque de injeção por repetição**: pode ser entendido como uma forma de ataque contra redes ou sistemas na qual uma transmissão de dados válida é maliciosamente repetida ou atrasada de forma fraudulenta. Isso é feito pelo originador ou por um invasor que intercepta os dados e o retransmite, possivelmente como parte de um ataque mascarado por substituição de mensagens, parcial ou total. Assim, um atacante copia um pacote encaminhado e depois envia o cópias repetidamente e continuamente para a vítima, a fim de esgotar os recursos computacionais ou fontes de alimentação da vítima, sensores, estações e pontos de acesso e de degradar a rede alvo de ataque. Além disso, os pacotes repetidos podem travar aplicativos mal projetados ou explorar vulnerabilidades presentes em sistemas também mal projetados no que tange à preocupação com sua segurança [46]; e

7. ***Message modification/Injection attack* - Injeção de falsas mensagens**: desse ataque, procedem-se não somente a modificação maliciosa da mensagem, ao se alterar intencionalmente o conteúdo legítimo da(s) mensagem(s), mas também a ocorrência da injeção de tais mensagens falsas, comprometendo assim a confiança e a integridade dos dados ou informações transacionadas, geralmente com o objetivo de manipular e ludibriar o sistema ou rede-alvo [49].

Cabe ainda destacar, que em caso de êxito na consecução de tais ataques cibernéticos, estes impactarão negativamente na manutenção da segurança cibernética e das seguintes propriedades da segurança da informação: confidencialidade (1, 6 e 7), integridade (5, 6 e 7), disponibilidade (2, 3 e 4) e autenticidade (5 e 7).

Por fim, para um maior entendimento sobre as capacidades, exequibilidade e potenciais efeitos das ameaças cibernéticas a um específico contexto, entendendo quais seriam os principais atores e demais características que possam influenciar nas condições para seu êxito em explorar as vulnerabilidades presentes na aviação civil, e por extensão ao Sistema ADS-B, torna-se necessário o estudo em relação aos aspectos correlatos à disciplina de Modelagem de Ameaças Cibernéticas.

2.2 MODELAGEM DE AMEAÇAS CIBERNÉTICAS

Modelagem de Ameaças é considerada um aspecto importante na garantia da segurança de um sistema ou ativo, visto que é orientada especificamente a descobrir as características intrínsecas e aspectos principais que atuam para a exploração das vulnerabilidades existentes no objeto sob análise [50]. De acordo

com o presente em [51], Modelagem de Ameaças Cibernéticas (do inglês, *Cyber Threat Modeling*) pode ser entendida como o "*processo de desenvolvimento representativo dos aspectos inerentes às ameaças (fontes, atores, comportamentos, cenários, etc.) criadas e presentes no ciberespaço a um específico alvo*".

No entanto, através da visão depreendida de [52], tal termo adquire significados adaptados a depender do contexto de aplicação. Por exemplo, a partir da perspectiva de avaliação de sistemas, através da modelagem de ameaças cibernéticas, "*a arquitetura do sistema é representada e analisada, potenciais ameaças de segurança são identificadas e apropriadas medidas ou técnicas de mitigação são selecionadas*"[53]. Já, com a ótica voltada para sistemas e aplicações industriais de infraestrutura crítica, *Cyber Threat Modeling* é entendida como "*processo destinado a analisar a segurança e as vulnerabilidades de uma aplicação ou serviços em rede, e desta forma prover um sistemático caminho para identificar ameaças que podem vir a comprometer a segurança de acordo com o definido pela boas práticas amplamente aceitas na Indústria*"[52].

Para melhor entender conceitualmente tal definição e seus principais termos correlatos, em sua essência, torna-se necessário o entendimento de sua frações significativas. Ainda de acordo com [51]:

- **Modelo**: é uma representação abstrata de algum domínio da experiência humana, seja para estruturar o conhecimento, seja para prover uma linguagem comum para dissertar sob tal conhecimento com a finalidade de realizar estudos no específico domínio humano sob análise. Neste estudo, o espaço cibernético será o domínio sob análise.

- **Ameaças Cibernéticas**: são eventos provocados intencionalmente e que podem causar prejuízo à confidencialidade, autenticidade, integridade ou disponibilidade da informação ou sistemas da informação, através da divulgação não autorizada, do acesso indevido, alteração ou destruição da informação e sistemas da informação.

- **Fonte(s) de Ameaça(s) Cibernética(s)**: de acordo com o presente em [51] e em [54], existem basicamente quatro fontes de ameaças, quais sejam: adversarial, acidental, estrutural e ambiental. Neste estudo, será objeto de análise apenas os agentes munidos de intenções adversariais e maliciosas, os quais consistem, ainda de acordo com [51], em "*indivíduos, grupos, organizações ou Estados que objetivam explorar vulnerabilidades e a dependência das organizações-alvo em recursos cibernéticos*".

- **Cenário de Ameaças cibernéticas**: uma configuração de eventos únicos facilitadores, interdependentes ou não, associados com uma específica fonte de ameaça ou múltiplas fontes de ameaças, ordenadas ou instrumentalizadas no tempo e capazes de viabilizar o meio ideal para a consecução com êxito da ameaça. Cenários de ameaças podem ser representados graficamente através de esquemas conjunturais ou de forma individualizada, ainda que contextualizado.

- **Agentes de Ameaças**: as ameaças advêm a partir de específicos agentes (também referenciados como atores e adversários) que possuem diferentes capacidades, comportamentos (técnicas, táticas e procedimentos - TTPs), motivações e requerem diferentes tipos de controles de segurança e ações para a gestão de riscos.

- **Técnicas, Táticas e Procedimentos - TTPs**: são representações do comportamento ou *modus operandi* de atores cibernéticos com intenções maliciosas e capazes de cometer ataques. É um termo originário do meio militar e usado para caracterizar o que um adversário é capaz de fazer, assim como procederá para tal intento (ferramentas, estratégia, etc.) [55].

Em complemento aos conceitos apresentados, cabe acrescentar que a modelagem de ameaças cibernéticas é um componente indissociável e fonte para três ramos subsidiadores para a manutenção da segurança cibernética, quais sejam: Gestão de Riscos Cibernéticos; Jogos de Guerra Cibernética; e Mapeamento do Perfil das Ameaças aplicáveis a Tecnologias ou Sistemas [51].

Gestão de Riscos Cibernéticos (do inglês, *Cyber-risk Management*) pode ser entendida como a disciplina que se ocupa com a identificação, análise, avaliação, monitoramento e (ou) tratamento dos riscos causados por ameaças cibernéticas [56]. É relevante pontuar, que durante o processo de gestão de riscos cibernéticos é necessário possuir um olhar holístico em relação aos aspectos técnicos, humanos e processuais inerentes às ameaças criadas ou perpetradas através do meio cibernético, sob pena de não se ter um panorama completo e real da probabilidade de ocorrência e extensão do impacto do risco existente [57, 58].

Porém, em relação aos Jogos de Guerra Cibernética (do inglês, *Cyber Wargaming*), [51] classifica-os como "*um método de exercício, estruturado a partir de um ambiente modelado ou simulado, capaz de analisar a performance e a tomada de decisão humana e (ou) as características de um sistema e a sua capacidade (de proteção ou vulnerabilidade) em um contexto ou cenário de ataques cibernéticos*". Por exemplo, a modelagem de ameaça cibernética apoia os jogos de guerra cibernética ao viabilizar a criação de perfis de ameaças adversariais a serem utilizados por equipes de segurança ofensiva (do inglês, *red team*), na identificação e classificação de eventos por parte das equipes de segurança protetiva (do inglês, *blue team*) e outros cenários a serem realizados em testes simulados em diferentes combinações [51, 55].

Já sobre o Mapeamento do Perfil das Ameaças Cibernéticas aplicáveis em Tecnologias ou a Sistemas (do inglês, *Technology Profiling and Technology Foraging*), sua finalidade reside na diagramação de um panorama das características, vulnerabilidades existentes, oportunidades de melhoria e na identificação de possíveis cenários e (ou) ameaças capazes de impactar negativamente na tecnologia ou sistema sob análise em um dado contexto [51].

Para esse estudo, modelagem de ameaça cibernética será subsidiadora, oportunamente em específico momento, para o mapeamento do perfil de ameaças cibernéticas, assim como insumo para a realização do Gerenciamento dos Riscos Cibernéticos por meio do método GRSO.

2.2.1 Modelagem de Ameaças Cibernéticas à Aviação Civil

De acordo com [33], embora a indústria de transporte aéreo de carga e passageiros tenha uma longa história na gestão de riscos com especial atenção à segurança de voo (*safety*) e à segurança física de instalações e plataformas aéreas (*security*), a gestão de riscos cibernéticos tem introduzido um novo panorama ao rol de ameaças à segurança contra atos de interferência ilícita na aviação civil (AVSEC), sobretudo devido à crescente evolução tecnológica e à prevalência do fator computacional nos sistemas aéreos e meios de Comunicações, Navegação, e Vigilância (CNS) em âmbito mundial [59]. Isso corrobora para a visão

defendida por [37], em que um "*axioma básico da eficácia do ataque cibernético reside na extensão da dependência do adversário em relação à TIC*"; e a exposta em [60], em que a "*infraestrutura da aviação civil consiste em um "sistema de sistemas" interconectados por componentes computacionais, os quais aumentam a suscetibilidade a ataques cibernéticos*".

Ao estender nossa interpretação somada ao firme entendimento depreendido do parágrafo anterior, e o advindo do presente em [25], em que se afirma que os principais alvos (inclusive cibernéticos) da aviação civil podem ser assentados no arcabouço conceitual de três áreas formadas pelas infraestruturas críticas relativas ao Controle de Tráfego Aéreo (ATC), Aeronaves/Indústria da Aviação e Aeroportos; em [37], propõe-se uma taxonomia para classificação de prováveis alvos da aviação civil, também baseada em uma tríade, mas esta pensada em infraestruturas, sistemas e plataformas. Como fica claro na seguinte afirmação:

> Dentre as infraestruturas críticas, destacam-se os aeródromos e as instalações físicas do controle de tráfego aéreo. São exemplos de sistemas críticos aqueles destinados ao emprego comercial na gestão de passageiros e cargas, além daqueles relacionados ao controle de tráfego aéreo. As plataformas críticas são as aeronaves comerciais, cargueiras, privadas ou não tripuladas [37].

Para este trabalho, com a finalidade de delimitação de escopo e similaridade conceitual com o sistema de vigilância aérea a ser analisado em capitulo vindouro e o modelo adversarial a ser desenvolvido, o rol de alvos a serem considerados nesta subseção estarão restritos dentre os sistemas CNS/ATM, aqueles afetos à vigilância ATS e de apoio a tal finalidade, inclusive em voo. A partir do Glossário presente no *website* do Programa Sirius do DECEA, presente em [61], e de outras referências importantes, temos as seguintes tecnologias críticas sob análise:

- **Radar Primário de Vigilância- PSR**: pode ser entendido como um sistema de localização de aeronaves não-cooperativas (sobretudo por não ser dependente de resposta-*transponder*). Seu funcionamento baseia-se na transmissão de pulsos eletromagnéticos em uma determinada direção e captação dos sinais de rádio eventualmente refletidos por aeronave ou qualquer objeto que estiver no caminho da energia transmitida na zona de alcance de sua antena giratória e a despeito das atenuações através do meio. Os sinais assim refletidos são processados e podem ser visualizados em uma tela própria, semelhante a uma tela de monitor de computador pessoal ou mesmo de um televisor. Esses sinais, também chamados de ecorradares, podem ser utilizados para controlar o tráfego aéreo ou, ademais, para fins de defesa aérea em caso de conflito, sobretudo por sua natureza de não dependência da cooperação das aeronaves em voo [8, 13, 61].
  QUESTÕES DE SEGURANÇA: apesar de o PSR ser resistente a praticamente à totalidade de ataques cibernéticos identificados, devido a sua abordagem ser baseada em sinais ou pulsos eletromagnéticos (sem transferência de conteúdo ou mensagem), ainda assim a referida tecnologia radar é suscetível a ataques do tipo *jamming* [22, 62].

- **Radar Secundário de Vigilância - SSR**: é um sistema de vigilância cooperativo do espaço aéreo que utiliza transmissores-receptores (interrogadores de solo em órgão ATC e respondedores de bordo em aeronaves) e que fornece, basicamente, informações de identificação das aeronaves (Modo A), altitude (Modo C) e os dois parâmetros (Modo S) para os órgãos de controle de tráfego aéreo. SSR utiliza mensagens digitais em diferentes frequências para transmissão (1030MHz) e para recepção

(1090MHz). Uma limitação desse sistema é que não é possível obter a posição da aeronave em voo, o que pode ser suprido por outros meios de vigilância aérea, tais como PSR, MLAT e ADS-B [8, 13, 61].

QUESTÕES DE SEGURANÇA: em [33], destaca-se que por ter sido desenvolvido com lacunas de confidencialidade (a mensagem trafega em texto-claro, sem mecanismos de autenticação e verificação do emissor) para fins de maior interoperabilidade entre equipamentos, o sistema SSR está sujeito a ataques do tipo *Eavesdropping*; e em [22] e [62], adiciona-se a constatação comprovada da vulnerabilidade SSR a ataques performados a partir de SDRs, nos quais é possível a alteração, bloqueio (*jamming*), negação e injeção de mensagens de interrogação SSR nos Modos A, C e S em seus *tranponders*. Esse risco de exploração aumenta, ainda conforme exposto em [22], quando o agente adverso utiliza-se de identificadores legítimos e de aeronaves já existentes, o que reduz a probabilidade de detecção de inconsistências comparada a uma leitura advinda de uma "nova" aeronave ou objeto até então não identificado em radar.

- **Multilateração - MLAT**: é uma forma de vigilância independente e cooperativa, que emprega os sinais transmitidos através do transponder de uma aeronave para calcular a sua própia posição. Um sistema de multilateração é constituído por várias antenas em solo, que recebem o mesmo sinal de rádio de aeronave ou outro veículo, e uma unidade central de processamento, que calcula a posição da aeronave ou veículo através da medição da diferença do tempo da chegada (do inglês, *Time Difference Of Arrival - TDOA*) do sinal nas diferentes antenas. Em [7], observa-se que, para uma visualização em 3D dos movimentos em solo ou aéreo, torna-se necessária a presença de quatro ou mais receptores/sensores MLAT. Uma vez que os sistemas de multilateração podem utilizar transmissões oriundas da aeronave em voo (emissões SSR e ADS-B, ambas na frequência 1090MHz), podem ser empregados, em princípio, sem nenhuma mudança nos equipamentos de bordo, assim como pode exercer um papel acessório e redundante para estações ADS-B em solo [7, 61, 35]. Importante destacar que quando as antenas de recepção estão dispostas em grande número para detecção de emissões em uma grande área de cobertura (metropolitana, regional, etc.) e para um grande número de alvos, a designação mais utilizada na literatura é a de *WAMLAT* (do inglês, *Wide Area Multilateration*) [63].
  QUESTÕES DE SEGURANÇA: ainda que teoricamente por ser uma resistente tecnologia em relação a ataques cibernéticos, de maneira similar à tecnologia PSR, e por atuar com a recepção de mensagens para estimar a distância de tais aeronaves emissoras, de acordo com [22], é possível, em caso de ameaças cibernéticas avançadas, a realização de ataques através da injeção de mensagens modificadas (como ocorre em ataques nos sistemas SSR e ADS-B), com o foco na manipulação do tempo de chegada (do inglês, *Time Of Arrival - TOA*) da mensagem com a intenção de influenciar no TDOA resultante e bloqueio na recepção por meio de *jamming*.

- **ACAS/TCAS**: mais conhecido como TCAS, é a sigla estabelecida pela OACI para o sistema que mostra ao piloto em comando de uma aeronave a posição relativa de outra aeronave voando nas proximidades, sempre que esta estiver com o transponder em funcionamento. Em caso de ameaça de colisão, o sistema indicará, de forma visual e sonora, uma manobra de subida ou descida, necessária para evitar a colisão. Os sistemas das aeronaves se comunicam de tal maneira que, se uma aeronave recebe ordem para subir, o outro receberá para descer ou manter o nível. O ACAS I fornece informações de auxílio às manobras de “ver e evitar”, gerando avisos de tráfego (do inglês, *Traffic Advisory*

- TA), que apenas informam sobre a localização de uma ou mais aeronaves na mesma área, porém, não inclui a capacidade de gerar avisos de resolução (do inglês, *Resolution Advisory* - RA). O ACAS II fornece os avisos de resolução (RA) verticais, indicando ao piloto a necessidade de iniciar uma manobra de subida ou descida para evitar uma colisão iminente, além dos avisos de tráfego (TA). Os sistemas ACAS/TCAS, atualmente, ainda não são capazes de indicar manobras evasivas do tipo curva à direita ou à esquerda, em virtude da complexidade de se avaliar, automaticamente, o impacto que isto traria para os voos em rotas adjacentes [61, 64].
  QUESTÕES DE SEGURANÇA: cabe expor que, uma vez que o TCAS é baseado em Modo S, ele usa um canal sem autenticação. Dessa forma, interrogações ou respostas advindas de mensagens SSR e ADS-B modificadas podem ser injetadas através do uso de SDRs e técnicas específicas para ataque [62, 34]. As implicações de um ataque direcionado ao TCAS incorrem em sérios riscos à aviação em caso de êxito, visto que ocasionará sobrecarga no processo decisório e até mesmo perda de consciência situacional das tripulações, sobretudo em fases críticas do voo e em espaços aéreos de alta densidade, com efeitos colaterais prejudiciais ao controle de tráfego aéreo responsável [22, 32, 65].

- **Sistema de Vigilância Dependente Automática por Radiodifusão (ADS-B)**: será abordado em detalhe na seção 2.5 deste estudo.

Dessa forma, para melhor entender a natureza das ameaças cibernéticas especializadas e capazes de impactar negativamente os sistemas e infraestruturas críticas de interesse da aviação civil acessíveis a partir do ciberespaço, é necessário também conhecer os potenciais agentes perpetradores de tais eventos. A partir de [8, 32, 35, 33, 34], chegamos à seguinte taxonomia relativa aos principais agentes adversos capazes de realizar ataques cibernéticos contra os sistemas CNS/ATM, operados a partir do solo ou em voo. São eles:

- **Entusiastas da aviação e observadores passivos**: exploram a natureza "aberta" e em "claro" dos protocolos e mensagens de alguns sistemas CNS/ATM. Tais agentes também fazem uso dos dados coletados e veiculados por terceiros em plataformas web e aplicações móveis, as quais possibilitam o acompanhamento em tempo real do tráfego aéreo e de suas comunicações. Alternativamente, podem fazer uso de receptores SDR de baixo custo para colher e reunir informações para seu próprio estudo e análise do tráfego aéreo em sua redondeza de interesse em tempo real. A informação coletada pode ter múltiplas origens, inclusive de tráfego aéreo de aeronaves privadas, militares ou de caráter sigiloso. O risco de exposição ao sistemas CNS/ATM proporcionado por tais agentes é considerado baixo, devido ao pouco conhecimento técnico e à natureza passiva de suas ações.

- **Ciberativistas e *hacktivistas***: esses são os agentes com médio potencial ativo de oferecer ameaça. Tal entendimento baseia-se em suas habilidades presumidas em hardware, software e conhecimentos correlatos, ainda que de forma superficial. O principal objetivo de tais agentes é explorar a segurança dos sistemas ligados à aviação, por meio de ferramentas de baixo custo e pouca sofisticação, com a finalidade de habilitá-los a monitorar e (ou) interferir em canais de comunicação da aviação. Em regra, suas motivações não são apenas racionais, mas baseadas principalmente em obtenção de publicidade e reconhecimento de seus feitos (em redes sociais, comunidade, fóruns *hackers*, etc). O risco de exposição dos sistemas CNS/ATM a tais agentes pode ser considerado baixo a médio, desde que existam soluções para detecção em caso de interferência e sistemas CNS/ATM redundantes ou acessórios para continuidade da prestação dos serviços.

- ***Insiders* (agentes internos)**: tais agentes adversos podem representar uma séria ameaça à aviação civil, visto que compartilham do dia a dia dos órgãos prestadores de serviço (EPTAs e PSNAs) e da rotina operacional de empresas aéreas, com acesso privilegiado a informações, outros profissionais (alguns em posições-chave), sistemas e outros ativos críticos. De fato, uma vez que o *insider* tem acesso a uma aplicação, plataforma ou sistema crítico, ele representa, por vezes, um risco maior do que o representado por cibercriminoso que tenta acessar tais ativos sem conhecimento prévio do alvo. Esse agente pelo acesso que possui pode incorrer diretamente para a realização de ataques cibernéticos ou na facilitação para a realização de tais ataques por terceiros, por isso representam um risco médio para a segurança dos ativos cibernéticos CNS/ATM.

- **Cibercriminosos**: tais atacantes objetivam explorar sistemas ou ativos da aviação civil em busca de benefícios financeiros e (ou) informacionais através do ganho de conhecimento acerca da infraestrutura crítica sob ataque ou da extorsão de seus gestores. Muitas vezes, fazem uso de sistemas complexos e custosos, tais como tecnologias baseadas em SDR e até mesmo uso de RPA com o intuito de interceptar, injetar mensagens interceptadas e (ou) modificadas com a finalidade de explorar e manter anonimidade frente aos sistemas de detecção existentes. Tais agentes tentam acessar o máximo de informação possível e imprimir credibilidade às suas ações realizadas para manter seu acesso no ativo comprometido. Dessa forma, eles usam todos os meios possíveis (pessoas, equipamentos e TTPs comuns ao crime organizado) para explorar com êxito os sistemas aeroembarcados e os sistemas de controle do tráfego aéreo. O risco de exploração dos sistemas CNS/ATM por cibercriminosos é considerado em nível médio para alto, a depender do grau de especialização técnica, capacidade de financiamento e nível de estruturação, individual ou em grupo, observado em oportuna gestão de riscos cibernéticos para tais atores.

- **Ciberterroristas**: tais agentes têm como motivação principal atingir seus objetivos através do terror causando o máximo de dano possível, ao ameaçar a segurança nacional ou regional com suas ações, infligir danos à vida humana, bem como danos financeiros e psicológicos à sociedade. Por exemplo, ao explorarem as vulnerabilidades existentes nas comunicações sem fio aeroembarcadas ou em sistemas ATS de solo, os grupos terroristas, os quais tradicionalmente sequestram e (ou) atingem decisivamente aeronaves por meio de armas e artefatos explosivos, podem vir a conformar ataques cibernéticos contra aeronaves ou órgão ATC através do solo e a uma distância segura que lhe propiciem liberdade de ação e anonimidade de seus atos. O risco de exposição dos sistemas CNS/ATM é alto devido à facilidade de acesso a meios exploratórios de TIC, assim como ao aumento da capacidade cibernética de tais agentes e grupos extremistas em TTPs destinadas a ataques cibernéticos, sobretudo, a partir da crescente instabilidade social e política, com origem religiosa e ideológica.

- **Estado-Nação e (ou) grupos patrocinados**: tais agentes adversos possuem praticamente ilimitado acesso a recursos financeiros, grande capacidade de pesquisa e desenvolvimento, e suficiente conhecimento de TTPs para intrusão nas redes adversárias (ou capacidade de adquiri-la em menor tempo e maior facilidade que outros atores) sem grandes limitações, até mesmo nos sistemas CNS/ATM. O risco é considerado alto, sobretudo se o Estado ou grupo patrocinado faça uso de ferramentas e TTPs típicas de ameaças cibernéticas avançadas persistentes (do inglês, *Advanced Persistent Threats* - APTs) [66], assim como seja desenvolvedora ou aliada de Estado-nação detentor da tecnologia CNS/ATM alvo.

No entanto, naquilo que concerne aos potenciais impactos negativos pretendidos por tais agentes adversos, ainda que de maneira holística, o objetivo principal reside em acessar e degradar a precisão e a performance de sistema CNS/ATM alvo, com a possibilidade de causar sobrecarga no processo decisório de ATCOs e pilotos em voo, ou até mesmo causar acidentes fatais e interrupções totais ao normal fluxo de tráfego aéreo. Entre os principais impactos objetivados pela ação de ameaças cibernéticas, baseado na taxonomia presente em [41], destacamos os seguintes:

- **Dano à Reputação e à Imagem**: o objetivo é macular a imagem do Estado, setor aéreo, prestadora de serviço ou empresa aérea através de ataque que gere grande repercussão na mídia e prejuízo à percepção pública em relação à segurança na prestação de serviços da aviação civil, com a finalidade de infligir perda de clientes; redução de lucros e da possibilidade de novos negócios; pagamento de compensações financeiras e multas regulatórias; demissões em massa e descrédito perante parceiros e fornecedores em âmbito nacional e internacional.

- **Dano Físico e Material**: o intento principal é degradar ou destruir totalmente a infraestrutura aeroportuária, sistemas CNS/ATM e plataformas aéreas, através do ataque direto visando sobrecarregar ou comprometer ao limite o desempenho de sistemas, plataformas aéreas e performance do pessoal, até que estes incorram em erros, causando assim, incidentes ou acidentes aéreos.

- **Dano Psicossocial**: nessa modalidade, o mote principal é atingir "corações e mentes", as emoções e sentimentos das pessoas sob ataque. E desta forma, gerar sentimentos de desconforto, confusão, frustração, ansiedade e depressão causados pela sensação de insegurança e imprevisibilidade, com os efeitos sentidos na esfera individual, coletiva, nacional e até mesmo internacional (a depender da expressão e impacto do ataque cibernético perpetrado).

- **Dano à Vida Humana**: a intenção principal da ameaça cibernética é causar o máximo de perdas de vidas humanas possível; e, quando não, gerar danos e ferimentos permanentes e de grande expressão nos sobreviventes do ataque realizado.

- **Dano Econômico-financeiro**: esse dano, como depreende-se de sua designação, tem como finalidade a perda financeira, seja diretamente pelo roubo de informação corporativa e/ou financeira ou pela perda de ativos e capital, seja de forma indireta pelos efeitos da interrupção das operações e comercialização de serviços.

A partir do mapeamento realizado do perfil das ameaças cibernéticas capazes de performar ataques aos sistemas de vigilância elencados, e conceitualmente baseado nos modelos presentes em [33, 32], chega-se a seguinte modelagem contendo os principais agentes de ameaça, suas principais características e o risco envolvido a partir de suas ações, tal qual observado na Figura 2.1.

Atores	Recursos	Motivações	Capacidades	Sistema-Alvo	Dano presumido	Risco
Entusiastas	Baixo	Coleta de dados e informações sobre tráfego aéreo	*Eavesdropping*	SSR, ADS-B	À Reputação e à Imagem	Baixo
Ciberativistas	Baixo-médio	Qualquer impacto que gere notícias e reconhecimento	*Eavesdropping* , *Replay Attacks* e Negação de Serviço	SSR, ADS-B	À Reputação e à Imagem, Psicossocial	Baixo-médio
Insiders	Baixo-médio	Vingança, ganhos financeiros ao vender informações/ativos ou proporcionar acesso a terceiros	Acesso direto a informações operacionais e a meios de TIC.	PSR, SSR, ADS-B, TCAS	À Reputação e à Imagem, Psicossocial, Econômico-Financeiro	Médio
Cibercriminosos	Médio-alto	Maximizar os impactos financeiros de si ou do contratante	Acesso a recursos (financeiros e técnicos) em larga escala, como sofisticados *transponders*	PSR, SSR, ADS-B, TCAS	À Reputação e à Imagem, Econômico-Financeiro, Material, Psicossocial	Médio-Alto
Ciberterroristas	Médio-alto	Motivação política ou religiosa; e causar o máximo de dano possível através do terror com a finalidade de propogar ideais políticos ou religiosos de cunho extremista	Acesso a financiamento e a recursos para específico ataque de alto impacto nas operações aéreas	PSR, SSR, ADS-B, TCAS	À Reputação e à Imagem, Econômico-Financeiro, Material, Psicossocial, à Vida Humana	Alto
Estados-nação	Ilimitado	Gerar o máximo de dano possível em infraestruturas críticas, objetivos militares e economia da nação-alvo	Qualquer tipo de ataque físico e computacionalmente possível, inclusive com apoio de P&D.	PSR, SSR, ADS-B, TCAS, WAMLAT	À Reputação e à Imagem, Econômico-Financeiro, Material, Psicossocial, à Vida Humana	Alto

Figura 2.1: Modelagem de Ameaças Cibernéticas aos Sistemas de Vigilância Aérea da Aviação Civil, elaborada pelo Autor.

Por fim, cabe acrescentar que outra variável importante e que não pode ser desconsiderada na modelagem de ameaça cibernética à aviação civil é a relativa aos cenários de ameaças possíveis de ocorrência. Em complemento ao conceito já apresentado na Seção 2.1, um aspecto essencial e capaz de impactar a análise do risco (probabilidade de ocorrência e a severidade dos danos) à aviação civil é o entendimento das fases do voo e como estas interferem no comportamento de pilotos em comando (aeronaves em voo) e em controladores de voo (órgãos ATC). De acordo com presente em [67] e em [68], as fases de voo podem ser assim entendidas:

- **Fase 1 - Manobra ou Táxi**: após o momento de pré-voo, no qual a tripulação despacha formalmente sua intenção e rota de voo junto aos órgãos ATC competentes por meio do Formulário de Plano de Voo, a aeronave inicia seu trajeto do pátio de estacionamento, via pista de táxi, até à pista de pouso e decolagem, sob orientação e acompanhamento do ATCO em TWR encarregado a fim de se evitar colisões em solo com veículos terrestres de apoio ou outras aeronaves.

- **Fase 2 - Decolagem**: essa fase do voo só ocorre por meio de autorização expedida por ATCO em TWR. Esse profissional tem a visão geral do tráfego em solo ao longo das pistas (do inglês, *runways*), no entorno do aeródromo e nas aerovias em espaços aéreos controlados, para que somente assim determine o momento ideal em que a aeronave deve iniciar seu voo e, em coordenação com outros órgãos ATC, para qual nível e aerovia deve se deslocar a aeronave após a decolagem. ATCOs fazem uso dos dados advindos de sistemas CNS/ATM a sua disposição (radares, sistemas de radio navegação, comunicações via rádio, etc.), assim como de mensagens meteorológicas e observação visual do aeródromo e entorno próximo.

- **Fase 3 - Subida**: nessa fase, logo após a decolagem e a certo afastamento do aeródromo de partida, o controle ATC da aeronave em razão de subida de nível é transferido do controlador TWR para a supervisão do APP responsável. Tal aeronave ficará sob responsabilidade do referido APP enquanto estiver na esfera de influência da TMA e até atingir o nível e a aerovia adequada para estabelecer o voo de cruzeiro.

- **Fase 4 - Voo de Cruzeiro**: na fase em voo de cruzeiro, a aeronave passa a ser controlada e a receber informações de interesse (meteorológicas, informações de tráfego etc.) através de ATCOs em ACC durante toda sua progressão na aerovia em espaço aéreo controlado (CTA), até iniciar procedimentos de descida. Tal fase de voo é considerada a menos crítica, muito pela separação estabelecida entre as aeronaves e o voo nivelado em aerovia, bem como pela baixa densidade de aeronaves em voo.

- **Fase 5 - Descida**: quando autorizado pelo controle ACC em coordenação com o próximo APP responsável e confirmado por cálculos realizados pela tripulação e (ou) automaticamente pelos computadores de bordo da aeronave, inicia-se uma descida gradativa em escalonamento vertical por níveis até que se inicie o procedimento de aproximação final ou espera em setor do espaço aéreo nas proximidades do aeródromo, na esfera de influência do ATCO em APP e em TMA nas imediações do aeródromo de pouso.

- **Fase 6 - Aproximação final**: nesta fase, sob acompanhamento radar do APP, a tripulação estabelece contato com ATCOs em TWR. Em coordenação direta entre o APP e a TWR do aeródromo de pouso, define-se uma sequência ordenada para pouso de aeronaves com base em alguns fatores (ordem de chegada na TMA, performance da aeronave, autonomia de combustível, situações de emergência ou urgência, etc.). A fase de aproximação final é considerada, junto com a fase do pouso, uma das mais críticas do voo, representando cerca de 50% dos acidentes fatais registrados, somados a todas as outras fases de voo, sobretudo se nos atermos ao espaço amostral mais recente compreendido entre os anos de 2012 e 2021 [69, 70]. A criticidade de tais fases advém da complexidade proveniente da maior densidade de aeronaves em circuito para pouso e decolagem, menor separação entre aeronaves comparada a outras fases, bem como a necessidade de atenção total por parte de tripulações e controladores de tráfego aéreo nas leituras e parâmetros advindos de sistemas CNS/ATM e nos procedimentos e decisões a serem realizados para pouso, seja ele a ser realizado em modo visual ou orientado por instrumentos.

- **Fase 7 - Pouso**: após autorizado pelo ATCO em TWR, a aeronave procede seu pouso ao tocar o solo até a sua total parada em pátio de estacionamento. O pouso pode ocorrer de duas maneiras básicas, visual ou por instrumentos. A primeira modalidade se dá quando as condições meteorológicas, visibilidade, condições da aeronave e do aeródromo encontram-se favoráveis de acordo com o julgamento da TWR e do piloto em comando. Na segunda configuração, caso existam situações climáticas ou técnicas adversas, bem como auxílios destinados a pousos por instrumentos (ILS), a aeronave segue prioritária e procedimentalmente o recomendado em instrumentos de bordo e sistemas em solo, sob coordenação do controlador responsável pelo tráfego local.

A seguir, na Figura 2.2 é possível visualizar as sete fases do voo descritas; assim como, na Figura 2.3, os Espaços Aéreos Controlados e os Órgãos ATC em suas respectivas zonas de responsabilidade para o controle ATC em cada fase de voo apresentada.

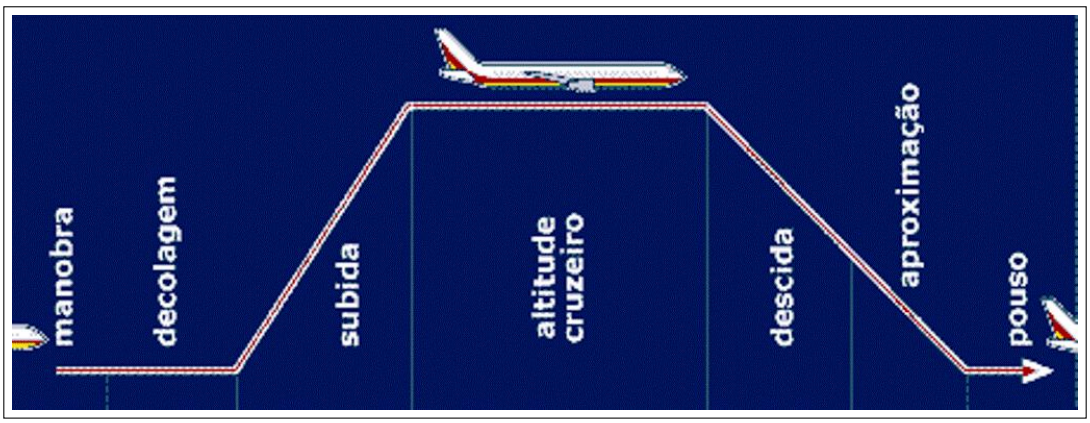

Figura 2.2: Fases do Voo [1].

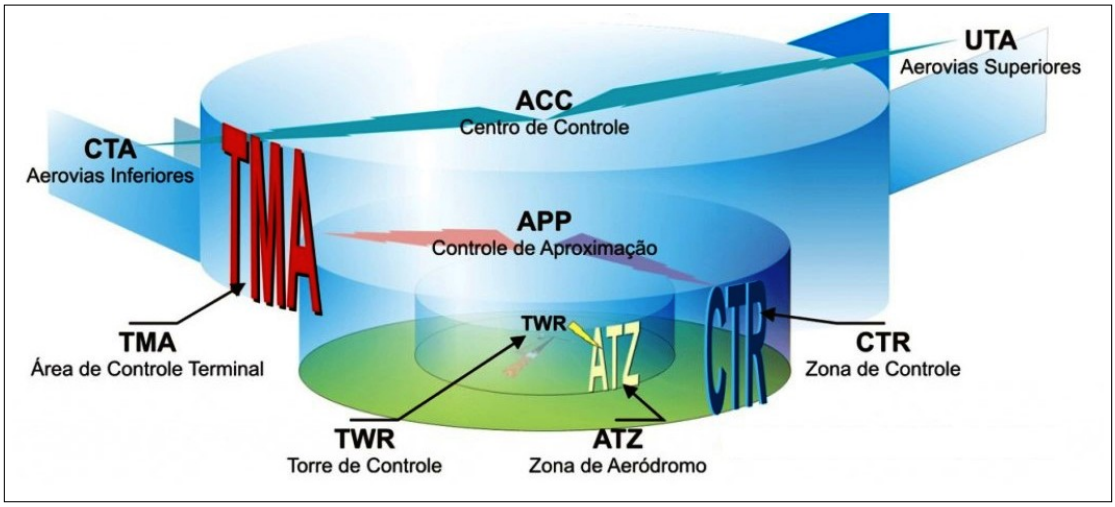

Figura 2.3: Espaços Aéreos Controlados e Controles do Espaço Aéreo [2].

Na sequência deste estudo, na seção 2.3, serão apresentadas algumas considerações acerca dos principais objetivos, atividades e benefícios esperados com a estruturação do Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB).

2.3 SISTEMA DE CONTROLE DO ESPAÇO AÉREO BRASILEIRO - SISCEAB

De acordo com [71], o Controle do Espaço Aéreo é uma importante atividade do Comando da Aeronáutica (COMAER) que contribui diretamente para o atendimento da missão de garantir a soberania do espaço aéreo brasileiro e integrar o território nacional, permitindo que as atribuições subsidiárias particulares relacionadas à segurança da navegação aérea sejam desenvolvidas dentro dos padrões de qualidade estabelecidos mundialmente.

O desenvolvimento das ações nessa área envolve uma ampla infraestrutura espalhada por todas as regiões do Brasil, caracterizada por empregar tecnologia de ponta, sendo operada e mantida por cerca 12 mil profissionais de elevada qualificação técnica, responsáveis pelo controle de uma área continental e

marítima estimada em 22 milhões de km² [72].

A gestão de todo esse ecossistema está sob a responsabilidade do DECEA, órgão central do SISCEAB, que disponibiliza meios em prol do gerenciamento e do controle do espaço aéreo, de forma integrada, civil e militar, com vistas à vigilância, à segurança e à defesa do espaço aéreo sob a jurisdição do Brasil. Na Figura 2.4 é possível visualizar alguns dados em prol de um melhor entendimento sobre a complexidade envolvida na conformação do SISCEAB.

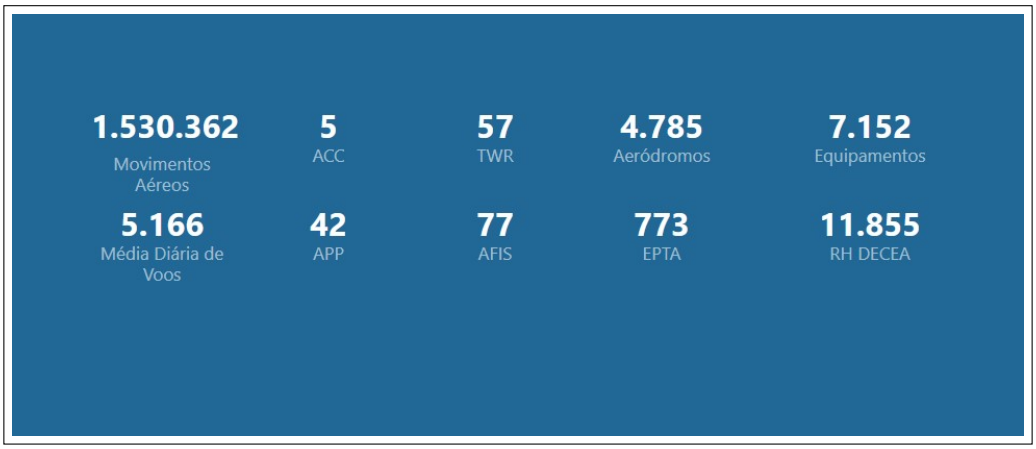

Figura 2.4: SISCEAB em números [3].

Para que o SISCEAB atue de maneira harmônica, eficiente e colaborativa, é mister que o seu órgão central atue de forma integrada com os seus elos e seus principais usuários, sejam eles civis ou militares.

Como elos do SISCEAB, podemos destacar as organizações subordinadas ao DECEA; órgãos operacionais, estações prestadoras de serviços de telecomunicações e de tráfego aéreo ; entidades da administração pública direta ou indireta vinculadas ou não ao COMAER; e entidades privadas, independentemente de seu nível ou grau, mediante convênio, contrato, concessão ou autorização específica, outorgada pelo DECEA [73].

Como principais usuários do SISCEAB, de acordo também com o presente em [73], podemos listar as unidades da Marinha do Brasil, do Exército Brasileiro e do Comando da Aeronáutica; empresas aéreas; operadores de aeronaves públicas e civis; pilotos militares e civis; EPTA; e assinantes cadastrados.

Ainda com base no presente em [61], e em [71], que definem o SISCEAB como "*o conjunto de órgãos e instalações – tais como auxílios à navegação aérea, radares de vigilância, centros de controle e torres de controle de aeródromo, estações de telecomunicações, recursos humanos etc. – que tem como objetivo proporcionar regularidade, segurança e eficiência do fluxo de tráfego nos aeroportos e no espaço aéreo*", podemos elencar como as principais atividades desenvolvidas em tal âmbito sistêmico, de acordo com exposto em detalhe por [74]:

- **Vigilância Aérea**: para garantir a segurança das operações aéreas e prover uma distribuição ágil aos voos, é indispensável precisar a localização das aeronaves e estimar seus posicionamentos futuros. Desse modo, através de recursos que identificam os voos - como radares e dispositivos de Vigilância Automática Dependente (ADS - Automatic Dependent Surveillance) - é possível visualizar, ininter-

ruptamente, os movimentos no espaço aéreo sob responsabilidade do Estado brasileiro. Uma vez expostas, por meio de softwares específicos nas telas das consoles, as movimentações aéreas passam a ser acompanhadas e orientadas pelos centros de controle, conforme as estratégias adotadas pelo gerenciamento do tráfego aéreo.

- **Telecomunicações Aeronáuticas**: o DECEA é o órgão que conduz o planejamento, a implantação, a operação e a manutenção da infraestrutura de comunicação relacionada ao controle do espaço aéreo no país. Essa complexa rede inclui equipamentos de tecnologia de ponta - que operam por meio de rádios, redes de computadores, satélites ou fibras ópticas - bem como canais alugados junto a concessionárias e outros recursos distribuídos por todo o território nacional. As comunicações são executadas, dentre outras ocasiões em que se fizerem necessárias, para acompanhar a evolução de cada voo, para autorizar ou restringir procedimentos de aeronaves e para fornecer informações de apoio, tais como as referentes às condições meteorológicas.

- **Gerenciamento de Tráfego Aéreo**: o termo incorpora os processos empregados para garantir o movimento seguro e eficiente das aeronaves durante todas as fases de voo e, por extensão, a gestão da circulação aérea. Mediante o fornecimento de instalações, sistemas e serviços contínuos, seu principal objetivo é garantir voos seguros, eficazes, pontuais e regulares, respeitando as condições meteorológicas e de infraestrutura operacional aeronáutica existentes, bem como assegurar o balanceamento entre a capacidade de atendimento do SISCEAB e a demanda de voos no Brasil. O Gerenciamento de Tráfego Aéreo compreende três esferas de atuação: Gerenciamento do Espaço Aéreo, Gerenciamento de Fluxo de Tráfego Aéreo e Serviço de Tráfego Aéreo.

- **Meteorologia Aeronáutica**: a meteorologia é uma ciência. Como tal, busca compreender os fenômenos que ocorrem na atmosfera e as interações entre seus estados dinâmico, físico e químico com a superfície terrestre subjacente. No que diz respeito à aviação, a informação meteorológica é vital para a segurança das operações, contribuindo para o conforto dos passageiros e facilitando o estabelecimento de rotas mais rápidas e econômicas e de voos regulares. Desse modo, requer um campo dessa ciência especificamente destinado às suas necessidades: a Meteorologia Aeronáutica. O DECEA é a organização do Comando da Aeronáutica responsável por essa atividade e a exerce por meio do Centro Integrado de Meteorologia Aeronáutica (CIMAER), sua unidade subordinada, e de uma complexa estrutura de radares, estações meteorológicas, centros de coordenação e outros recursos instalados no país.

- **Cartografia Aeronáutica**: a Cartografia Aeronáutica abrange o conjunto de estudos e operações técnicas para elaboração das cartas aeronáuticas padronizadas, destinadas à navegação aérea. No Brasil, a atividade é exercida pelo Instituto de Cartografia Aeronáutica (ICA), unidade subordinada ao DECEA que vem oportunamente incorporando inovações tecnológicas nos processos de gestão e desenvolvimento das mesmas. De posse dessas cartas, geridas, desenvolvidas e atualizadas regularmente pela organização, as aeronaves obtêm a orientação espacial adequada para cruzar os céus, com segurança e eficácia, ao longo dos cerca de 22 milhões de km² de espaço aéreo sob responsabilidade brasileira.

- **Informações Aeronáuticas**: é o conjunto de atividades executadas com o objetivo de gerar, coletar, processar e divulgar as informações necessárias à segurança, à regularidade e à eficiência da navega-

ção aérea. Sua principal responsabilidade é disponibilizar toda a informação para o planejamento e a execução de um voo seguro aos usuários do SISCEAB. Nelas estão incluídas publicações técnicas, emitidas conforme padrão adotado internacionalmente, de modo a atender a pilotos, controladores e operadores do transporte aéreo de qualquer país. Destinadas à orientação dos profissionais da aviação, é através delas que os usuários conseguem realizar procedimentos de voo eficazes e adequar-se ao conjunto de normas empregadas para a execução de um voo seguro.

- **Busca e Salvamento**: o Sistema de Busca e Salvamento Aeronáutico (SISSAR) atua numa área de 22 milhões de km², grande parte sobre o Oceano Atlântico e a Amazônia. Está organizado e estruturado para desenvolver operações de Busca e Salvamento em consonância com os compromissos e as normas nacionais e internacionais. O DECEA é o órgão responsável pelo planejamento, pela normatização e pela supervisão da atividade, que tem por objetivo localizar ocupantes de aeronaves ou embarcações em perigo, resgatar vítimas de acidentes aeronáuticos ou marítimos com segurança e interceptar/escoltar aeronaves em emergência. Como membros integrantes do SISSAR, há ainda os elos de coordenação, formados pelos Centros de Coordenação de Salvamento Aeronáuticos (ARCC), instalados nos Centros Integrados de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA), e os elos de execução, compostos por Unidades Aéreas da FAB, embarcações da Marinha e de outras organizações que colaboram na consecução das operações.

- **Inspeção em Voo**: a inspeção em voo de equipamentos e de procedimentos de navegação aérea garante a qualidade e a segurança dos serviços prestados pelo DECEA ao aferir, regularmente, os equipamentos de auxílio à navegação aérea, à aproximação e ao pouso, bem como procedimentos de voo de alta precisão. A inspeção afere a execução dos perfis de voo e verifica a qualidade dos sinais desses equipamentos ou de procedimentos de navegação aérea, em voo, fazendo análises, medições e, quando necessário, correções para que esses atendam aos parâmetros previstos. O Grupo Especial de Inspeção em Voo (GEIV) é a unidade, subordinada ao DECEA, que tem por missão executar essa tarefa, de modo a garantir uma operação segura às aeronaves em circulação no país durante todas as fases de voo, mesmo em condições meteorológicas adversas.

- **Auxílios à Navegação Aérea**: a navegação aérea é convencionalmente exercida com base em orientações de instrumentos e dispositivos que norteiam o voo das aeronaves, conforme as rotas, os procedimentos e os planos de voo preestabelecidos. O DECEA provê esses meios que orientam o curso dos pilotos, sem os quais seria impossível a existência de um grande fluxo de tráfego aéreo, como o atual, sobretudo, no que tange às chegadas e às saídas dos aeroportos. Sistemas e dispositivos que dão suporte à navegação aérea estão distribuídos ao longo de toda a extensão do território nacional e atualmente vêm se somando aos modernos recursos que propiciam a navegação orientada por sistemas de bordo e satélites, como a Navegação Baseada em Performance.

Sobre tais atividades listadas, e desempenhadas pelo SISCEAB sob coordenação do DECEA, é especialmente de interesse para este estudo a de Vigilância Aérea. Tal atividade é um dos pontos focais sistêmicos do Programa SIRIUS [61], o qual visa desenvolver e implementar soluções voltadas para a elevação da consciência situacional de controladores de tráfego aéreo e pilotos, por meio do emprego de sistemas de vigilância ATS, e para o aumento do intercâmbio de dados de vigilância com Órgãos ATS dos países vizinhos. Para este trabalho, Sistemas de Vigilância ATS são aqueles capazes de, em tempo real,

fornecer ao controlador de tráfego aéreo, na sua posição operacional, dados de posição e de identificação da aeronave. Como exemplos temos os Radares Primários e Secundário (PSR e SSR), os Sistemas de Multilateração (MLAT) e os Sistemas de Vigilância Dependente Automática por Radiodifusão (ADS-B) [61]. Entre os objetivos (1) e benefícios esperados (2) para a atividade de Vigilância do Espaço Aéreo proposta pelo Programa SIRIUS, sobretudo após a conclusão do emanado no *PFF 011 - Melhoria da Vigilância no Espaço Aéreo* detalhado em [19], estão:

(1) Objetivos:

- Elevar a consciência situacional de controladores e pilotos nas operações em rota, nas Áreas de Controle Terminal (TMA) e na superfície de aeródromos.
- Aumentar a capacidade de coordenação entre Órgãos ATS.
- Aumentar a capacidade do espaço aéreo sob a jurisdição do Brasil.

(2) Benefícios esperados:

- Elevação dos níveis de Segurança Operacional.
- Redução do impacto ambiental referente às emissões de CO_2.
- Redução da carga de trabalho de Controladores de Tráfego Aéreo e de Pilotos.
- Aumento da capacidade de detecção e resolução de conflitos de tráfego, inclusive em voo entre aeronaves, de maneira independente da interação com o ATCO.
- Aumento da eficiência das operações de superfície de aeródromos.

Para que tais objetivos e benefícios tornem-se realidade no contexto brasileiro e seu entorno próximo, sobretudo em consonância ao desejado pelo DECEA quanto à evolução do SISCEAB em direção ao Conceito ATM Global, de acordo com as recomendações e padrões estabelecidos pela OACI [18], é necessário que toda mudança significativa na prestação dos Serviços de Navegação Aérea seja acompanhada para além do estudo da relação custo-benefício de tal implementação, como também por uma avaliação da segurança operacional que ateste que o Nível Aceitável da Segurança Operacional (NADSO) está assegurado com a mudança desejada [4].

Para isso, além do oportunamente apresentado em [75], em que se afirma que, considerando o cenário de riscos cibernéticos voltado a infraestruturas críticas, "*entende-se que é de grande importância tratar a questão a partir da abordagem de gerenciamento de risco*", e a partir do depreendido em [4], [18], [19] e [76] considerando os ativos do SISCEAB como cenário de análise, a ferramenta integrante do Sistema de Gerenciamento da Segurança Operacional (SGSO) normativamente definida para tal finalidade é o método de Gerenciamento de Riscos à Segurança Operacional (GRSO).

2.4 GERENCIAMENTO DE RISCOS À SEGURANÇA OPERACIONAL - GRSO

Tal qual depreendido de [4], a OACI estabeleceu, por meio da Convenção de Aviação Civil Internacional, a necessidade de implementação de Sistemas de Gerenciamento da Segurança Operacional (SGSO), com o objetivo de aperfeiçoar os processos necessários à elevação do nível da segurança operacional da aviação civil mundial.

Em linhas gerais, o SGSO deve coordenar processos, procedimentos, políticas, programas e avaliações que identifiquem os perigos e gerenciem os riscos à segurança operacional na provisão dos serviços de navegação aérea [76]. Em relação à segurança operacional, conforme presente também em [76], esta pode ser entendida como "*o estado no qual os riscos no ATS são reduzidos e mantidos em um nível aceitável, ou abaixo deste, mediante um processo contínuo de identificação de perigos e gerenciamento de riscos.*".

No Brasil, cada PSNA componente do SISCEAB deve implementar o seu próprio SGSO, de acordo com metas de desempenho preconizadas pelo DECEA e com as recomendações de segurança emanadas da ASOCEA. Nessa direção, sobre importante instrumento acessório para o SGSO, em [4] afirma-se que:

> Uma das principais ferramentas do SGSO é o Gerenciamento do Risco à Segurança Operacional (GRSO), que identifica os perigos e avalia os riscos, de modo a concentrar as atividades de segurança operacional na eliminação ou mitigação dos riscos avaliados. O Gerenciamento do Risco será empregado nas mudanças a serem estabelecidas no SISCEAB e nas operações correntes dos Provedores dos Serviços de Navegação Aérea (PSNA).

Já em [5], pontua-se a relevância do GRSO como principal ferramenta para análise da segurança operacional do Sistema de Controle do Espaço Aéreo Brasileiro, sendo esta focada na análise da probabilidade e da severidade dos riscos associados a cada perigo identificado. O escopo de atuação do GRSO é voltado para os aspectos ligados às mudanças planejadas ou em curso nos Serviços de Navegação Aérea (ANS), em sistemas, equipamentos, procedimentos, fatores organizacionais e humanos, cujo funcionamento inadequado possa interferir na segurança do Controle do Espaço Aéreo. Tal método também pode ser utilizado caso se identifique, a qualquer momento, algum perigo associado aos serviços providos pelo SISCEAB [5].

Observa-se, também, a partir do presente em [4], que o Gerenciamento do Risco à Segurança Operacional consiste em cinco fases sequenciais: Descrição do Sistema, Identificação dos Perigos, Análise dos Riscos, Avaliação dos Riscos e Tratamento dos Riscos. Na Figura 2.5, são apresentados mais detalhes sobre cada fase do GRSO.

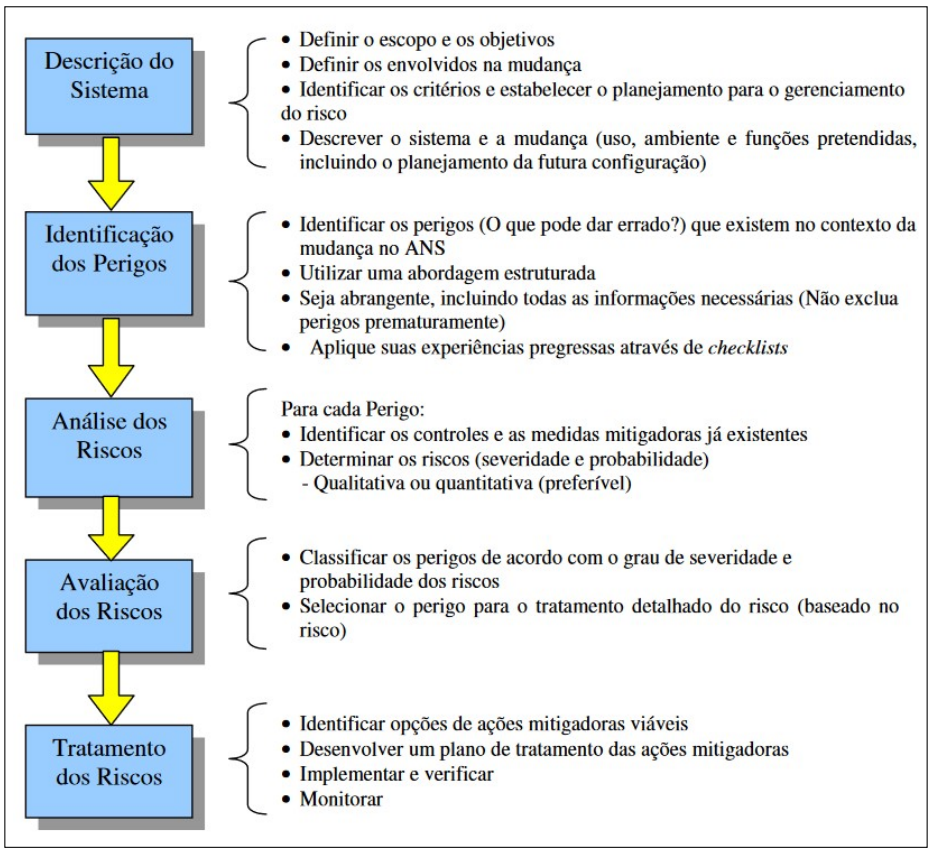

Figura 2.5: Fases do Gerenciamento de Risco à Segurança Operacional [4].

Dois aspectos devem ser levados em conta para se iniciar o processo GRSO. O primeiro é a realização de uma análise de segurança preliminar quanto à pertinência ou não da realização efetiva do GRSO, com a qual deve-se analisar se as respostas aos questionamentos abaixo, extraídos de [5], indicam a presença de risco operacional quando de eventual mudança nos Serviços de Navegação Aérea no SISCEAB. São eles:

- A modificação pretendida acarreta risco em potencial para a segurança operacional?
- A modificação pretendida afeta a interação entre pilotos e controladores?
- A modificação pretendida afeta os processos e/ou procedimentos operacionais existentes?
- A modificação pretendida acarreta alteração nas operações de serviços de tráfego aéreo e sistemas de manutenção?
- A modificação pretendida impõe a necessidade de qualificação dos recursos humanos?

Já o segundo aspecto concerne ao correto entendimento conceitual do que vêm a ser probabilidade, severidade e risco no contexto GRSO. Em [5], tais conceitos são assim definidos:

- **Probabilidade**: é a mensuração, em termos qualitativos e quantitativos, da possibilidade de uma situação de perigo ocorrer. Para a avaliação da probabilidade de ocorrência, deve-se utilizar, como referência e exemplo, o presente na Figura 2.6 abaixo apresentada.

Frequência	Sistema ATC			Valor
	Qualitativo		Quantitativo	
	AUXÍLIOS	ATC	ATC	
Frequente	Esperado acontecer mais de uma vez por semana.	Esperado acontecer uma vez a cada período de 2 dias.	$P \geq 10^{-3}$ Ocorrência por movimentos	5
Ocasional	Esperado acontecer, aproximadamente, uma vez todos os meses.	Esperado acontecer várias vezes por mês.	$10^{-3} > P \geq 10^{-5}$ Ocorrência por movimentos	4
Remoto	Esperado acontecer, aproximadamente, uma vez todos os anos.	Esperado acontecer uma vez em poucos meses.	$10^{-5} > P \geq 10^{-7}$ Ocorrência por movimentos	3
Improvável	Esperado acontecer, aproximadamente, uma vez entre 10 e 100 anos.	Esperado acontecer uma vez a cada 3 anos.	$10^{-7} > P \geq 10^{-9}$ Ocorrência por movimentos	2
Extremamente Improvável	Esperado acontecer menos que uma vez em 100 anos.	Esperado acontecer menos que uma vez a cada 30 anos.	$P < 10^{-9}$ Ocorrência por movimentos	1

Figura 2.6: Probabilidade de Ocorrência [5].

- **Severidade**: está baseada nas consequências possíveis de uma situação de perigo à segurança operacional, tomando como referência a pior condição possível. A Figura 2.7 exemplifica as eventuais consequências de um perigo à segurança operacional.

SEVERIDADE DO EVENTO (nos serviços de navegação aérea)		
DEFINIÇÃO	SIGNIFICADO	VALOR
Catastrófica	Colisão com outra aeronave, obstáculos, ou terreno.	A
Perigosa	Redução da separação com um erro operacional de Severidade Alta ou uma perda total da capacidade ATC (ATC Zero).	B
Maior	Redução da separação com um erro operacional de Severidade baixa/moderada ou redução significativa em capacidade ATC.	C
Menor	Redução leve da capacidade ATC, ou aumento significativo da carga de trabalho ATC.	D
Insignificante	Aumento leve na carga de trabalho ATC.	E

Figura 2.7: Severidade do Evento [5].

- **Risco**: é a avaliação das consequências potenciais de um perigo, expresso em termos de probabilidade e severidade, tomando como referência o pior cenário possível. Na Figura 2.8, é possível verificar o modelo de matriz utilizado para classificar os riscos identificados e analisados, após a fase de Avaliação de riscos do processo GRSO.

PROBABILIDADE DO RISCO	SEVERIDADE DO RISCO				
	Catastrófico A	Perigoso B	Maior C	Menor D	Insignificante E
Frequente (5)	5A	5B	5C	5D	5E
Ocasional (4)	4A	4B	4C	4D	4E
Remoto (3)	3A	3B	3C	3D	3E
Improvável (2)	2A	2B	2C	2D	2E
Extremamente Improvável (1)	1A	1B	1C	1D	1E

Figura 2.8: Matriz de Avaliação de Riscos GRSO [4].

Porém, a partir do resultado da avaliação de riscos realizada, é necessário proceder a sua classificação e consequente priorização para tratamento. Os riscos são classificados, quanto à aceitabilidade, de acordo com o presente em [5]:

- **Alto Risco - Risco inaceitável (5A, 5B, 5C, 4A, 4B e 3A)**: nos casos de Risco Inicial, significa que as mudanças não devem ser implementadas até que os riscos associados aos perigos sejam mitigados e reduzidos a Médio ou Baixo Risco (Risco Previsível). Nos casos de Risco Corrente, as operações/atividades nas condições atuais devem cessar até que o risco seja reduzido, pelo menos, a um nível tolerável. Nesse caso, a mitigação e a supervisão dos riscos (residuais) serão necessárias.
- **Médio Risco – Risco tolerável (5D, 5E, 4C, 4D, 4E, 3B, 3C, 3D, 2A, 2B e 2C)**: significa que o risco (Inicial ou Corrente) deve ser mitigado a um nível tão baixo quanto praticável. Em tais condições, a mudança pode ser implementada ou as operações podem ser mantidas, desde que haja a supervisão do desempenho da segurança operacional e o monitoramento dos riscos correntes.
- **Baixo Risco – Risco aceitável (3E, 2D, 2E, 1C, 1A, 1B, 1C, 1D e 1E)**: significa que não precisa ser tomada nenhuma medida e que os riscos assumidos (Inicial ou Corrente) compensam os benefícios auferidos, sem a presença de restrições ou limitações de segurança das operações. Os perigos não precisam ser gerenciados ativamente, porém precisam ser documentados. No entanto, se a organização entender que uma mitigação representa baixo custo ou pequeno esforço, o risco poderá ser mitigado.

Por fim, e ainda de acordo com [5], a partir da avaliação dos riscos deve-se dar a estes uma ordem de prioridade, considerando o potencial de perdas e danos que cada risco oferece à segurança operacional. Tal procedimento é fundamental para que se possa adotar medidas racionais e destinar recursos e esforços, priorizando os perigos que apresentam os maiores índices de risco para a organização.

2.5 SISTEMA DE VIGILÂNCIA AUTOMÁTICA DEPENDENTE POR RADIODIFUSÃO - ADS-B

Em continuidade ao já inicialmente apresentado sobre o protocolo ADS-B no Capítulo 1, em [6], os autores acrescentam que o desenvolvimento e implementação da ADS-B, entendido por eles como "*um novo paradigma para o controle de tráfego aéreo mundial*", objetivou a um formato diferente de prover informações atualizadas e precisas em todas as fases do voo, de maneira independente, ampla e resiliente. Ainda conforme [6]:

> Todo participante [do Sistema ADS-B] recupera sua própria posição e velocidade, usando um receptor GPS integrado. A posição é então transmitida periodicamente em uma mensagem (normalmente duas vezes por segundo) pelo subsistema de transmissão chamado ADS-B Out. As mensagens são então recebidas e processadas pelas estações ATC em terra, bem como por aeronaves próximas se equipadas com o receptor e subsistema ADS-B In. As mensagens podem possuir outros campos como ID, intenção, código de urgência e nível de incerteza.

Já em [22], é citado que para além da finalidade principal do protocolo ADS-B consistir na difusão contínua de dados de interesse para vigilância aérea e com isso propiciar o incremento da consciência situacional de tripulações em voo e ATCOs em solo, o papel exercido por tal tecnologia reforça um consistente movimento da aviação civil mundial no sentido da adoção de soluções e padrões CNS/ATM mais cooperativos e menos dispendiosos durante o seu ciclo de vida. Na Figura 2.9, é possível observar os componentes funcionais do Sistema ADS-B, quais sejam: ADS-B Out (módulo de transmissão aeroembarcado), ADS-B In (módulo de recepção aeroembarcado) e ADS-B *Ground Station* (estação de recepção de solo).

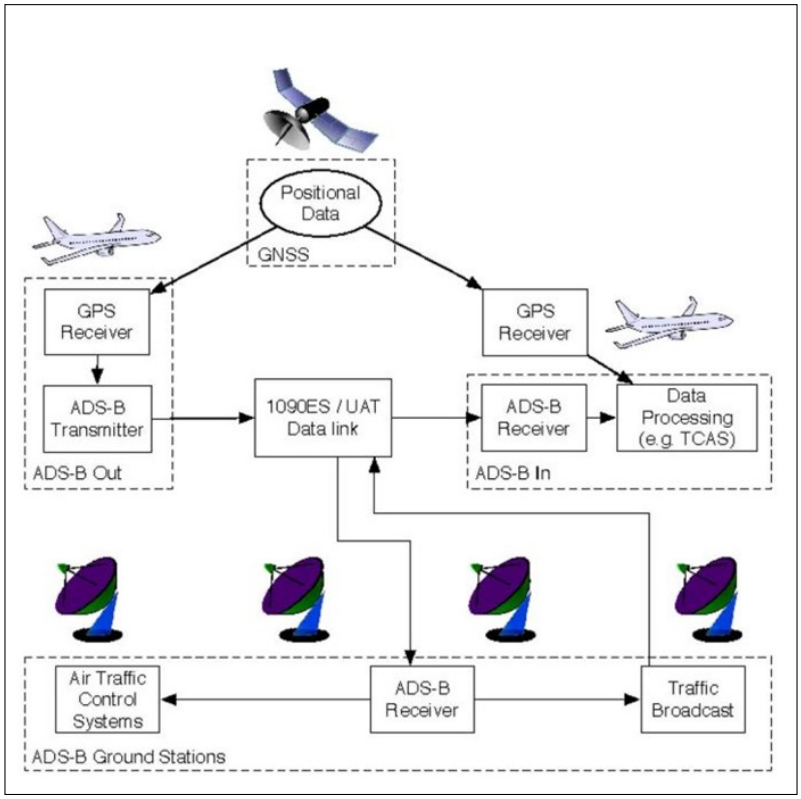

Figura 2.9: Representação do Sistema ADS-B [6]

De acordo com o apresentado conceitualmente em [12] sobre os componentes funcionais aeroembarcados ADS-B, "*é importante destacar os dois conceitos distintos: ADS-B Out, a capacidade primária, meio pelo qual a aeronave transmite suas informações de maneira padronizada, e ADS-B In, a capacidade de um veículo ou aeronave de receber e processar a informação veiculada por outrem*". E, para que o componente ADS-B Out adquira plena usabilidade prática, torna-se necessária a ampla adoção de equipamentos de recepção compatíveis em solo (*ADS-B Ground Station*), via satélite (modalidade ADS-B Satelital) e do componente ADS-B In instalado em aeronaves ou em veículos terrestres de apoio à aviação [12].

Em complemento, e conforme exposto de maneira pragmática por [26], a ADS-B foi desenvolvida para atender as seguintes finalidades:

1. **Controle em área de aeródromo - área de influência TWR/APP**:
    - **Controle em pátio de manobras e pistas de táxi**: a partir da localização baseada por GPS, a qual a ADS-B é dependente, as mensagens proveem a precisão necessária para o controle de veículos terrestres de apoio e aeronaves em solo.
    - **Fases de aproximação final e decolagem**: objetiva-se reforçar a acurácia necessária para a manutenção da segurança operacional ATC, vindo a propiciar a redução de custos a partir da diminuição da densidade de aeronaves nas fases de aproximação final e decolagem, principalmente em aeroportos com intenso fluxo aéreo.
2. **Voos em rota e em espaços aéreos controlados - área de influência ACC**:
    - **Regiões inóspitas de difícil cobertura para controle ATC**: ADS-B propicia o controle e a redução de custos nas operações, devido a sua total cobertura por toda rota, sobretudo em áreas de baixa densidade (de aeronaves e dados de outros sistemas de vigilância aérea), provendo mensagens para outras aeronaves em voo, estações em solo e inclusive através de SATCOM por meio da ADS-B Satelital.
    - **Anticolisão em voo**: incrementa a precisão da localização fornecida ao TCAS, reduzindo, assim, o perigo de colisões aéreas. Modernos TCAS já utilizam a ADS-B para aperfeiçoar sua performance e acurácia.
    - **Voo de aeronaves remotamente tripuladas - RPA**: os dados presentes na mensagem ADS-B irão aperfeiçoar o senso de navegação, anticolisão e separação entre RPAS e, entre RPAS e aeronaves tripuladas em futuro próximo de espaço aéreo compartilhado entre tais modalidades de voo.

Ainda em [26], depreende-se que dois padrões para o estabelecimento de enlace de dados e comunicação foram propostos para o protocolo ADS-B: Transceptor de Acesso Universal (do inglês, *Universal Access Transceiver* – UAT) e o 1090 *Extended Squitter* (1090ES). Diferente do padrão UAT, que por possuir configuração dedicada ao protocolo ADS-B e assim necessitar de adaptações em equipamentos e dispositivos para seu funcionamento, o padrão largamente adotado mundialmente, sobretudo pela aviação comercial é o 1090ES, visto que o hardware necessário para seu funcionamento é compatível ao tradicional transceptor Modo S (já amplamente utilizado para a modalidade de vigilância SSR) [14]. Pelo exposto,

e similar ao optado também em [6] e [26], este trabalho retringe seu foco ao padrão de enlace de dados 1090ES.

Dessa forma, e de acordo com [14] e [26], o padrão 1090ES usa a frequência de 1090 MHz para comunicação entre aeronaves em voo e destas com estações de solo. Não menos importante é acrescentar que o transceptor utilizado para 1090ES pode se valer adicionalmente da frequência de 1030MHz para interrogações e outros serviços de informação a partir de estações de solo para aeronaves em voo. Sobre o tamanho de mensagem, no modo S (como já dito também utilizado para SSR), há dois possíveis formatos, quais sejam: curto de 56 bits e longo de 112 bits [6]. Já para o padrão 1090ES, destinado ao ADS-B, é utilizado formato longo de mensagem de 112 bits, o qual pode ser observado na Figura 2.10.

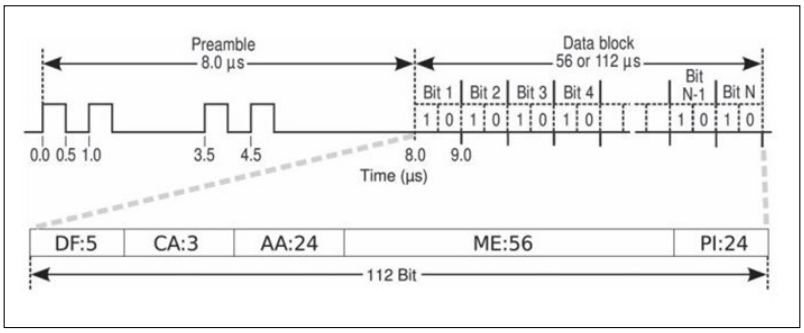

Figura 2.10: Formato da mensagem 1090ES ADS-B [6].

Para um melhor entendimento da finalidade de cada campo da mensagem 1090ES ADS-B, tal qual presente em [27], cabe expor que antes do envio do Bloco de Dados (do inglês, *Data Block*), há um espaço reservado denominado preâmbulo, o qual contém uma sequência especial de bits para sincronização da mensagem antes de seu efetivo envio. No tocante ao Bloco de Dados, o campo "DF (*Downlink Format*)" refere-se ao tipo de mensagem a ser enviada; o campo "CA (*Capability*)" indica a capacidade de comunicação do transponder utilizado; assim como o campo "AA (*Aircraft Address*)" é destinado a alocar o endereço único ICAO, o qual designa um código particular para cada aeronave (*transponder*), essencial, sobretudo, para desconflito na recepção com outras aeronaves em rota e estações de solo. Por outro lado, o campo "PI (*Parity Check*)" provê um CRC de 24 bits, com a finalidade de auxiliar na verificação de integridade da mensagem, assim como para detectar e corrigir possíveis erros na transmissão e na recepção [27].

Cabe expor, ainda sobre o Bloco de Dados, que o campo "ME (ou *ADS-B data*)" de 56 bits é o destinado a transmitir os dados de interesse para vigilância, como por exemplo: dados de posição, velocidade, código de urgência e outros afins para uma melhor consciência situacional entre os integrantes do Sistema ADS-B.

Em relação ao alcance das emissões ADS-B (ADS-B Out), ainda que residam variáveis exógenas e influenciadoras como a altitude da aeronave em voo, relevo do terreno, condições climáticas e outras limitações e atenuantes na linha de visada até as estações de solo e outras aeronaves em rota (ADS-B In), bem como limites técnicos devido à potência envolvida na transmissão, tamanho e ganho da antena, e a sensibilidade presente nos receptores, de acordo com depreendido em [26] e [31], o alcance máximo ideal e teórico pode ser estimado para transceptores 1090ES (1090MHz) em cerca de 500km (270NM) e para transceptores UAT (978MHz) em cerca de 300km (160NM).

Ainda sobre a vigilância ADS, cabe citar um caso particular e complementar à tecnologia ADS-B,

qual seja a ADS-C. Baseado em definição extraída a partir de entendimento do corpo técnico da OACI, em [7] afirma-se que "*ADS-C é um meio pelo qual os termos do contrato ADS-C são trocados entre os sistemas de solo e a aeronave, por uma ligação de dados, especificando sob que condições os reportes devem ser iniciados, e que dados devem ser incluídos nos seus reportes*". Ou seja, com a ADS-C, as trocas de mensagens sob demanda estabelecidas entre as estações em solo e as aeronaves ocorrem através de enlaces de comunicações dedicados e previamente acordados entre as partes registradas.

Tal alternativa é ideal para zonas oceânicas e remotas, às quais se impõem dificuldades inerentes ao meio para instalação e manutenção de outras alternativas de vigilância aérea e por possuir o alcance ilimitado devido a seus enlaces de dados serem suportados por tecnologias HF e SATCOM, facilitando assim o controle de tráfego aéreo em tais regiões [77]. Na Figura 2.11, é possível visualizar o esquema básico de funcionamento do Sistema ADS-C.

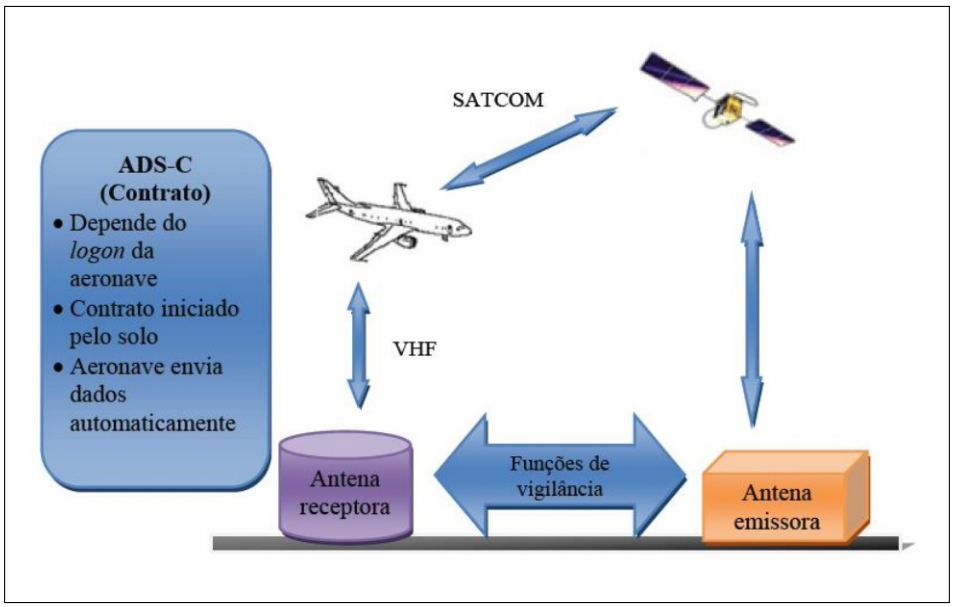

Figura 2.11: Funcionamento do Sistema ADS-C [7].

Na próxima subseção, serão realizadas considerações sobre as vulnerabilidades existentes e já documentadas sobre o protocolo ADS-B.

2.5.1 Vulnerabilidades ADS-B

Ainda que de acordo com o Relatório Técnico da FAA, presente em [78] e citado por [6], não residam preocupações de segurança adicionais com a implantação da ADS-B no espaço aéreo norte-americano além daquelas já existentes em cenários de vigilância área suportados pelos sistemas radar primário (PSR) e radar secundário (SSR), a preocupação com a eventual exploração de lacunas de segurança existentes no referido protocolo permanecem e advêm de algumas de suas características intrínsecas, tais como sua forma de propagação das mensagens com conteúdo em claro, além do exíguo espaço disponível na mensagem 1090ES ADS-B para integração de possíveis soluções de segurança para o protocolo, sobretudo correlatos à verificação da autenticidade e manutenção da confidencialidade da mensagem com a finalidade de se evitar o acesso e a manipulação indevida do conteúdo transmitido [79].

Também em [6], os autores ainda acrescentam que além da transmissão da mensagem ADS-B por meio do padrão 1090ES ocorrer por meio de modulação por posição de pulso (do inglês, *Pulse Position Modulation – PPM*), e tal modulação ser sensível aos efeitos negativos de ondas refletidas e dispersas por multipercurso, também residem potenciais vulnerabilidades quanto à sobreposição intencional de sinal (do inglês, *jamming*).

Já em relação ao modo de comunicação adotado pelo protocolo ADS-B, de irrestrita radiodifusão das mensagens em texto-claro, em [28] depreende-se que devido a toda mensagem ADS-B transmitida ser direcionada para o meio de maneira indistinta quanto ao receptor, qualquer agente malicioso dentro do espaço de detecção da mensagem legítima pode recebê-la, modificá-la e enviá-la para o meio novamente de maneira ilegítima, facilitando a realização da modalidade de ataque conhecido como *spoofing*, visto que a mensagem legítima contém informações detalhadas e relevantes sobre o tráfego de voos privados, militares e regulares de passageiros que podem ser inclusive facilmente falsificadas [24].

Uma outra característica, não menos importante da mensagem ADS-B, é que não há a autenticação para verificação da identidade do emissor da(s) mensagem(ens) ADS-B, de maneira similar ao observado na modalidade ADS-C, assim como ausência de soluções implementadas para a verificação de dados, ou outras funcionalidades voltadas a confirmar ou questionar o status da aeronave em longos tempos sem detecção de novas mensagens [79, 28].

Porém, enquanto esse cenário ainda que sensível é em certa medida gerenciável pelos órgãos ATC para a maioria dos ataques cibernéticos, ao se considerar o acesso a dados oriundos de meios redundantes de vigilância aérea e das capacidades proporcionadas pela fusão de dados a partir de sistemas CNS/ATM em alta velocidade de interconectividade em solo, a partir da perspectiva das tripulações em voo e dos sistemas aeroembarcados os perigos emergem em complexidade e em nível de risco, visto que, por vezes, a exequibilidade e os impactos diretos e indiretos permanecem subestimados [24].

Também nessa linha, em [80], o pensamento é que, diferente do que é vivenciado pelas estações e órgãos ATC em solo, que possuem meios que possibilitam verificar posição a partir da recepção de mensagens ADS-B e das características como intensidade do sinal e do tempo de chegada por meio da multilateração, além do suporte acessório dos dados produzidos pelos sistemas de radar de vigilância, aeronaves civis encontram-se limitadas em meios e soluções para proceder a legitimação e averiguação dos dados para verificação de posição advindos da ADS-B.

Em [6, 14, 24], é uníssono que em paralelo às publicações produzidas pela comunidade acadêmica, a comunidade internacional de profissionais responsáveis pela segurança da informação e cibernética tem contribuído para uma maior conscientização dos perigos presentes nas vulnerabilidades existentes no protocolo ADS-B, sobretudo ao demonstrar a praticabilidade de ataques cibernéticos contra tal sistema, por exemplo através do depreendido e demonstrado por [31] e [30].

Dito isso, no Capítulo 3, serão realizados estudos para auxiliar na identificação, análise e tratamento de tais ameaças cibernéticas já mapeadas e aplicáveis ao contexto do SISCEAB, a serem estruturadas com o auxílio do método GRSO.

3 GRSO APLICADO ÀS AMEAÇAS CIBERNÉTICAS IDENTIFICADAS NA IMPLANTAÇÃO ADS-B NO ÂMBITO DO SISCEAB

"Para que a Segurança seja maximizada é necessário que todos cultuem atitudes preventivas nas suas atividades, sejam elas operacionais ou administrativas."

Departamento de Controle do Espaço Aéreo (DECEA)

Neste capítulo, serão apresentadas as fases presentes no Gerenciamento de Risco à Segurança Operacional (GRSO) e fase anterior para julgamento de sua pertinência, com o foco na análise dos riscos cibernéticos envolvidos na implantação do Sistema ADS-B no contexto do SISCEAB, quais sejam: Análise Preliminar; Descrição do Sistema; Identificação do Perigo; Análise do Risco; Avaliação do Risco e Tratamento do Risco.

3.1 ANÁLISE PRELIMINAR

Com a finalidade de proceder a Análise Preliminar da Segurança Operacional em relação à nova tecnologia de vigilância aérea a ser adotada (Mudança no ANS), qual seja, a ADS-B, partimos dos seguintes argumentos para se chegar a nossa conclusão. São eles:

1. Ao retomar as considerações presentes no Capítulo 1, especificamente aquelas que confirmam normativamente a adoção em etapas progressivas da tecnologia ADS-B no âmbito do SISCEAB, mais especificamente através das publicações DCA 351-2 “Concepção Operacional ATM Nacional” [18] e PCA 351-3 “Plano de Implementação ATM Nacional” [19], em que pese à primeira norma definir a estratégia e os requisitos que devem ser atendidos, assim como os cenários possíveis para adoção da referida tecnologia para um seguro e eficiente Gerenciamento do Trafego Aéreo (ATM) Nacional, destacando-se o espaço aéreo oceânico e o espaço aéreo continental como contextos de interesse; e à segunda norma, focar na operacionalização e no detalhamento de cada programa, projeto e atividades componentes dos empreendimentos necessários para a evolução do SISCEAB rumo ao Conceito Operacional ATM Global estabelecido pela OACI, em que a ADS-B é protagonista.

2. Somado ao já amplamente documentado na comunidade acadêmica e de segurança, referenciado e descrito em seções anteriores deste estudo (em destaque o presente na subseção 2.5.1) em relação ás ameaças cibernéticas existentes à aviação civil, suas capacidades e exequibilidade em explorar as vulnerabilidades existentes no Sistema ADS-B.

Assim, pelo exposto, ao representar a presença de risco à segurança operacional, com base no também depreendido de [4, 5], resta claro para esse autor a necessidade de se proceder a aplicação do Gerenciamento de Risco à Segurança Operacional (GRSO) para tal Mudança ANS.

Mas, ainda sim, conforme também recomendando em [5], ao expor que *"adicionalmente à análise preliminar, acima citada, para subsidiar a decisão pela aplicação do GRSO, deve-se analisar se as respostas às perguntas"* [as mesmas presentes na seção 2.4, p. 28, deste estudo] "*indicam a presença de risco à segurança operacional*", procedemos da seguinte forma ao responder tais indagações:

1. **A modificação pretendida acarreta risco em potencial para a segurança operacional?** Sim. Acreditamos na existência do risco à segurança operacional devido à existência de vulnerabilidades comprovadas e documentadas capazes de serem exploradas em tal protocolo, e que, por extensão, residem em estado latente também no âmbito do SISCEAB, conforme depreendido nos capítulos anteriores, em especial no presente na subseção 2.5.1 deste estudo.

2. **A modificação pretendida afeta a interação entre pilotos e controladores?** Sim, uma vez que pilotos e controladores não serão apenas usuários individuais dos dados advindos da tecnologia ADS-B a ser implantada no SISCEAB, mas também tal inovação irá impactar nas interações, coordenações e procedimentos em todas as fases do voo, sobretudo nas fases de aproximação final e pouso, assim como nos parâmetros de outros sistemas CNS/ATM, também fonte de apoio aos mesmos.

3. **A modificação pretendida afeta os processos e/ou procedimentos operacionais existentes?** Sim, visto que com a implantação da ADS-B no SISCEAB, o DECEA procederá mudanças em vários procedimentos e regramentos relativos ao controle de tráfego e utilização do espaço aéreo [18, 19]. Por exemplo, no tocante à redução da separação mínima entre aeronaves em certos espaços aéreos controlados em relação ao praticado hoje e suportado por outras tecnologias de vigilância aérea, devido ao aumento da consciência situacional de pilotos e ATCOs proporcionado a partir das mensagens ADS-B.

4. **A modificação pretendida acarreta alteração nas operações de serviços de tráfego aéreo e sistemas de manutenção?** Sim, por representar a evolução de uma geração de vigilância aérea cooperativa baseada em radares (máxime, tecnologia SSR) e suportada por equipamentos legados, bem como procedimentos particulares de operação e manutenção; para uma tecnologia mais moderna, torna-se assim necessária a realização de adaptações na operação e manutenção (ainda que reduzidas e pontuais) em equipamentos e sistemas já existentes no SISCEAB [18] e outros a serem inseridos no repertório de tecnologias acessórias à ADS-B, tais como MLAT.

5. **A modificação pretendida impõe a necessidade de qualificação dos recursos humanos?** Sim. Com a implantação da referida nova tecnologia como um dos pilares para a vigilância aérea no SISCEAB, ainda que sua implementação ocorra em etapas e em áreas específicas, surge a necessidade de adequação e desenvolvimento de novos procedimentos e regramento para pilotos e controladores de tráfego aéreo, seja para condução das atividades normais a partir dos novos dados de vigilância aérea e equipamentos oriundos da ADS-B, seja para ações contingenciais em caso de degradação de meios ou identificação de quaisquer anormalidades no funcionamento ou proporcionado por tal tecnologia.

Dessa forma, cumprido o rito inicial recomendando por [4] e [5] para aplicação do GRSO, e superadas as eventuais dúvidas a respeito da presença do risco à segurança operacional na mudança ANS propiciada pela implantação da ADS-B no âmbito do SISCEAB, torna-se necessária a continuidade em progressão para as etapas subsequentes e componentes do Gerenciamento de Risco à Segurança Operacional.

3.2 DESCRIÇÃO DO SISTEMA

Conforme descrito nos capítulos anteriores, principalmente o presente na seção 2.5, p. 33-37, deste estudo.

3.3 IDENTIFICAÇÃO DE PERIGOS

Tal qual depreendido de [6, 27], e abordado na seção 2.5.1 deste estudo, a maioria das vulnerabilidades presentes no Sistema ADS-B residem na própria natureza do protocolo e na sua forma de propagação, mas sobretudo pela ausência em seu desenvolvimento de soluções criptográficas e (ou) de autenticação entre as partes envolvidas no sistema.

Entre as principais ameaças à ADS-B, destinadas a explorar suas fragilidades como sistema e protocolo, em [35, 27] encontramos a seguinte taxonomia das formas de ataques cibernéticos entendidos como fundamentais, assim como de interesse e modelo para este estudo: interceptação de mensagens (*eavesdropping*); modificação de mensagens recebidas; deleção de mensagens legítimas; injeção de mensagens; interferência sobrepujante de sinal (do inglês, *jamming*); e envio de múltiplas mensagens ilegítimas em excesso (do inglês, *flooding*).

Cabe destacar que, para exposição das consequências inerentes aos ataques com foco em dois sensíveis alvos do Sistema ADS-B, quais sejam a aeronave (em voo ou no pátio de manobras) e a estação de solo ATC, assim como abordagem presente em [28], e aderente ao já apresentado em [81], este estudo optou por expor de maneira agregada as técnicas de ataques fundamentais, associadas à dificuldade de emprego e ao alvo a ser atacado.

Sendo assim, chega-se à conformação de sete modalidades de ataques passíveis de análise, que podem ser complementares ou não, a depender do cenário de emprego. São elas, com base em [27, 28, 29]:

1. **Interceptação de mensagens ADS-B - IM**: nessa modalidade, devido a a emissão de mensagens ADS-B ocorrer em ampla difusão e "em claro", um potencial agente malicioso pode facilmente interceptar e decodificar as mensagens transmitidas (via ADS-B Out) com o objetivo de obter informações acerca de aeronaves em movimento. Essa modalidade também é considerada o passo inicial para a perpetração de outros tipos de ataques.

    - **Alvo**: aeronaves e estações de solo ATC.
    - **Agentes adversariais**: observadores passivos, ciberativistas, *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados pelo Estado.

- **TTPs de Ataque**: interceptação de mensagens ADS-B Out através de SDRs de baixo custo.
- **Dificuldade Técnica**: a dificuldade para sua execução pode ser entendida como de baixa complexidade, sobretudo pela fácil disponibilidade de *hardwares*, *softwares*, dados e conhecimento, via tutoriais e disponibilizados em plataformas web de interesse, como por exemplo o presente em FlightRadar24.com e OpenSkyNetwork.org.
- **Cenário de Ataque**: todas as fases do voo.
- **Impacto**: não há impacto negativo direto, visto que a interceptação de mensagens ocorre de maneira passiva. No entanto, há de se ressaltar que, de maneira indireta, o conteúdo de tais mensagens poderão ser utilizados como insumo para a realização de ataques ativos.

2. **Interferência ou sobreposição intencional de sinal (*jamming*) contra estações de solo - ISE**: ao proceder a uma interferência intencional de sinal contra uma estação de solo de recepção de mensagens ADS-B, um eventual agente adverso objetiva impedir que toda e qualquer mensagem enviada através do ADS-B Out seja recebida pela referida estação. Tal ataque foca na degradação parcial ou total do canal de recepção (no caso do sistema ADS-B, em frequência 1090 MHz), objetivando a perda de consciência situacional dos operadores de órgãos ATC, forçando-os a fazer uso de meios alternativos de vigilância aérea com menor eficiência ou acurácia, impelindo, assim, riscos de segurança às operações, sobretudo em áreas de alta densidade de fluxo aéreo [14]. A efetividade do ataque correlaciona-se à potência e à diretividade da emissão do sinal, à proximidade do atacante da estação-alvo, assim como os meios que o ATCO possui para a continuidade das operações enquanto perdurar o ataque.

   - **Alvo**: estações de solo ATC.
   - **Agentes adversariais**: ciberativistas, *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados pelo Estado.
   - **TTPs de Ataque**: sobreposição intencional de sinal com a intenção de causar a degradação, parcial ou total, no canal de frequência 1090MHz, e de maneira indireta também na recepção de sinais SSR.
   - **Dificuldade Técnica**: a dificuldade do ataque pode ser mensurada como de baixa a média complexidade, pois ainda que haja disponibilidade de ferramentas de baixo custo para o referido fim, tal qual exposto em [82], há de se levar em conta também a potência e os *hardwares* empregados para sobreposição de sinal em grandes áreas, assim como a proximidade do ator à estação-alvo.
   - **Cenário de Ataque**: todas as fases de voo.
   - **Impacto**: dano à reputação e à imagem, dano físico e material, dano psicossocial, dano à vida humana e dano econômico-financeiro.

3. **Interferência ou sobreposição intencional de sinal (*jamming*) contra aeronaves - ISA**: esta modalidade de ataque se vale da mesma técnica empregada contra estações de solo, porém é focada em degradar a recepção ADS-B em aeronaves, com efeitos colaterais em outros sistemas aeroembarcados que fazem uso de tal fonte de dados e atuantes no mesmo canal e frequência. Seu objetivo

principal é causar perda de consciência situacional da tripulação sob influência do referido ataque, sobretudo nas fases críticas do voo. Há, ainda que remota, a possibilidade de execução do ataque dentro da própria aeronave-alvo.

- **Alvo**: aeronaves em voo.
- **Agentes adversariais**: *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados pelo Estado.
- **TTPs de Ataque**: sobreposição intencional de sinal com a intenção de causar a degradação, parcial ou total, no canal de frequência 1090MHz, e de maneira indireta também na recepção de sinais SSR.
- **Dificuldade Técnica**: a dificuldade desse ataque é classificada entre baixa e média complexidade, pois, ainda que haja disponibilidade de ferramentas de baixo custo para o referido fim, também deve ser levado em conta a limitação em se ganhar acesso próximo às aeronaves no pátio de manobras em solo ou em movimento aéreo e a potência e o *hardware* empregados para sobreposição de sinal em grandes áreas e sobre um alvo em movimento.
- **Cenário de Ataque**: fases de decolagem, aproximação final e pouso, caso o ataque ocorra nas imediações do aeródromo-alvo.
- **Impacto**: dano à reputação e à imagem, dano físico e material, dano psicossocial, dano à vida humana e dano econômico-financeiro.

4. **Injeção de mensagens ADS-B contra estações de solo - IME**: essa ameaça tem o fim de injetar mensagens ADS-B interceptadas, modificadas ou falsas em estações de solo ATC.

    - **Alvo**: estações de solo ATC.
    - **Agentes adversariais**: *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados pelo Estado.
    - **TTPs de Ataque**: interceptação de mensagens ADS-B emitidas, modificação e injeção de mensagens através de equipamentos baseados em SDR e emulador do comportamento ADS-B Out.
    - **Dificuldade Técnica**: a dificuldade do ataque pode ser mensurada como de média a alta complexidade, pois, além da necessidade de o agente perpetrador possuir o acesso interno ou as imediações do aeródromo, assim como conhecimento da infraestrutura-alvo (tipo de equipamento, versão, localização, etc), também torna-se mandatório para executar tal ataque possuir conhecimento detalhado sobre o protocolo para modificar as mensagens legítimas interceptadas ou construir outras falsas que simulem o comportamento de aeronaves para serem apresentadas como legítimas para órgãos de vigilância e controle do trafego aéreo, assim como ter a capacidade tecnológica para a injeção com sucesso de mensagens (similar ao funcionamento do ADS-B Out).
    - **Cenário de Ataque**: todas as fases de voo.
    - **Impacto**: dano à reputação e à imagem, dano físico e material, dano psicossocial, dano à vida humana e dano econômico-financeiro.

5. **Injeção de mensagens ADS-B contra aeronaves - IMA**: a configuração desse ataque se assemelha à modalidade anterior, ao também se objetivar a interceptação, modificação e injeção de mensagens ADS-B, só que contra aeronaves. Porém, como não há o amplo acesso à correlação ou fusão de dados de diferentes fontes (como dados de plano de voo, leitura de sistemas radares, etc.) com dados advindos da ADS-B, tal qual é possível a partir de estações de solo para desconflito de tráfegos legítimos ou não, a injeção de mensagens em aeronaves mostra-se mais promissora, ainda que resida a necessidade de proximidade ou acesso ao referido vetor.

    - **Alvo**: aeronaves em voo.
    - **Agentes adversariais**: *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados pelo Estado.
    - **TTPs de Ataque**: interceptação de mensagens ADS-B emitidas, modificação e injeção de mensagens através de equipamentos baseados em SDR e emulador do comportamento ADS-B Out.
    - **Dificuldade Técnica**: a dificuldade do ataque pode ser mensurada como de média a alta complexidade, pois além da necessidade de o agente perpetrador possuir o acesso interno ou às imediações do aeródromo, assim como conhecimento dos sistemas aeroembarcados (tipo de equipamento, versão, etc), também torna-se mandatório para executar tal ataque possuir conhecimento detalhado sobre o protocolo para modificar as mensagens legítimas interceptadas ou construir outras falsas que simulem o comportamento de aeronaves para serem apresentadas como legítimas para órgãos de vigilância e controle do trafego aéreo, assim como ter a capacidade tecnológica para a injeção com sucesso de mensagens (similar ao funcionamento do ADS-B Out).
    - **Cenário de Ataque**: fases de decolagem, aproximação final e pouso, caso o ataque ocorra nas imediações do aeródromo-alvo.
    - **Impacto**: dano à reputação e à imagem, dano físico e material, dano psicossocial, dano à vida humana e dano econômico-financeiro.

6. **Injeção de múltiplas mensagens (*flooding*) ADS-B contra estações de solo - IMME**: Como também descrito em [14], esse ataque busca multiplicar os efeitos advindos da injeção de mensagens ADS-B simultâneas na estação-alvo, com o objetivo de "inundar" e degradar sistemas e a atuação de controladores de tráfego aéreo. Essa ameaça é especialmente sensível caso um agente adverso queira impelir retardos, desinformação e danos diretos e indiretos ao normal funcionamento do tráfego aéreo, máxime em aeródromos de grande fluxo e alta densidade aérea.

    - **Alvo**: estações de solo ATC.
    - **Agentes adversariais**: *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados pelo Estado.
    - **TTPs de Ataque**: interceptação de mensagens ADS-B emitidas, modificação e injeção de múltiplas mensagens através de SDRs e emuladores do comportamento ADS-B Out.

- **Dificuldade Técnica**: a dificuldade do ataque pode ser mensurada como de alta complexidade, pois além da necessidade de o agente perpetrador possuir o acesso interno ou às imediações do aeródromo, assim como conhecimento da infraestrutura-alvo (tipo de equipamento, versão, localização, etc), também torna-se mandatório para executar tal ataque possuir conhecimento detalhado sobre o protocolo para modificar as mensagens legítimas interceptadas ou construir outras falsas que simulem o comportamento de aeronaves para serem apresentadas como legítimas para órgãos de vigilância e controle do trafego aéreo, assim como ter a capacidade tecnológica e meios para a múltipla injeção com sucesso de mensagens (similar ao funcionamento de múltiplos equipamentos ADS-B Out).
- **Cenário de Ataque**: todas as fases de voo.
- **Impacto**: dano à reputação e à imagem, dano físico e material, dano psicossocial, dano à vida humana e dano econômico-financeiro.

7. **Injeção de múltiplas mensagens (*flooding*) ADS-B contra aeronaves - IMMA**: Esse ataque também almeja multiplicar os efeitos advindos da injeção de mensagens ADS-B simultâneas contra aeronaves, ao ponto de degradar a consciência situacional de tripulantes, podendo vir a causar sérios riscos à segurança operacional e de voo caso não haja sistemas ou meios capazes de prover tais tripulações com dados legítimos e desconflitantes, máxime em espaços aéreos de grande densidade e em fases críticas do voo.

    - **Alvo**: aeronaves em voo.
    - **Agentes adversariais**: *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados pelo Estado.
    - **TTPs de Ataque**: interceptação de mensagens ADS-B emitidas, modificação e injeção de múltiplas mensagens através de SDRs e emuladores do comportamento ADS-B Out.
    - **Dificuldade Técnica**: a dificuldade do ataque pode ser mensurada como de alta complexidade, pois além da necessidade de o agente perpetrador possuir o acesso interno ou às imediações do aeródromo, assim como conhecimento dos sistemas aeroembarcados (tipo de equipamento, versão, etc), também torna-se mandatório para executar tal ataque possuir conhecimento detalhado sobre o protocolo para modificar as mensagens legítimas interceptadas ou construir outras falsas que simulem o comportamento de aeronaves para serem apresentadas como legítimas para órgãos de vigilância e controle do tráfego aéreo, assim como ter a capacidade tecnológica e meios para a múltipla injeção com sucesso de mensagens ADS-B (similar ao funcionamento de múltiplos equipamentos ADS-B Out) em um alvo em movimento.
    - **Cenário de Ataque**: fases de decolagem, aproximação final e pouso, caso o ataque ocorra nas imediações do aeródromo-alvo.
    - **Impacto**: dano à reputação e à imagem, dano físico e material, dano psicossocial, dano à vida humana e dano econômico-financeiro.

3.4 ANÁLISE DO RISCO CIBERNÉTICO

Nessa fase, torna-se necessário identificar os controles e as medidas mitigadoras já existentes para cada perigo ou ameaça cibernética, assim como os riscos envolvidos [4]. Logo, para cada ameaça já identificada para o Sistema ADS-B, os seguintes controles, ações mitigadoras e grau de probabilidade e severidade foram assim atribuídos:

1. **Interceptação de mensagens ADS-B - IM**: pode ser entendido como ações mitigadoras, tal qual exposto em [26], a implementação de soluções criptográficas (baseada em chaves públicas) ou solução baseada em saltos de frequência, ainda que a implementação de ambas seja de alta complexidade e alto custo. **O grau de severidade do risco pode ser considerado como insignificante; e a probabilidade de ocorrência, como frequente**.

2. **Interferência ou sobreposição intencional de sinal contra estações de solo - ISE**: pela natureza do ataque, residem dificuldades em definir controles ou ações mitigadoras efetivas, sobretudo se o atacante estiver próximo ou possuir robustos, ainda que portáteis, equipamentos para potente emissão. Porém, como soluções possíveis emergem a adoção de saltos de frequência e de soluções voltadas a detecção e *antijamming*, ainda que a implementação seja de alta complexidade, assim como o acesso a dados de outros sistemas CNS/ATM redundantes reside eficaz contramedida para a manutenção da consciência situacional ATC. **O grau de severidade é considerado como perigoso; e a probabilidade de ocorrência, como remota**.

3. **Interferência ou sobreposição intencional de sinal contra aeronaves - ISA**: diferente da ameaça voltada às estações de solo, o *jamming* contra aeronaves mostra-se mais danoso sobretudo se o vetor estiver em fases críticas de voo, como em decolagem ou em procedimento de descida, bem como em voo por instrumentos. Destaca-se o caráter sensível e particular do canal de frequência 1090MHz em voo, uma vez que também é utilizado por aeronaves para tráfego de resposta a interrogações realizadas por equipamentos anticolisão em voo (TCAS). Soluções baseadas em enlace de dados diretos e dedicados entre outras aeronaves ou estações de solo atuantes em frequências não adjacentes, inclusive baseada em fonia ou dados, podem ser eficazes para mitigar a chance de acidente ou incidente aeronáutico. **O grau de severidade é entendido como catastrófico; e a probabilidade de ocorrência, como remota**.

4. **Injeção de mensagens ADS-B contra estações de solo - IME**: entre alguns controles e ações mitigadoras já existentes e factíveis situam-se a fusão de dados (como dados de plano de voo, leitura de sistemas radares, etc.), as leituras de outros equipamentos de vigilância aérea (radares, multilateração, confirmação via fonia, etc) e a filtragem estatística das leituras pelo método Kalman [26]. **O grau de severidade pode ser entendido como maior; e a probabilidade de ocorrência, como remota**.

5. **Injeção de mensagens ADS-B contra aeronaves - IMA**: como os controles e as ações mitigadoras hoje existentes para inibir a injeção de mensagens arbitrárias ou ilegítimas ADS-B são implementados principalmente para estações de solo, neste caso abordagens baseadas em soluções criptográficas (baseada em chaves públicas) para autenticação ou na filtragem estatística das leituras pelo

método Kalman para estimar localizações podem ser aplicáveis, ainda que com considerável custo de implantação e processamento devido às peculiaridades das plataformas aéreas, bem como à heterogeneidade e à complexidade inerente aos seus sistemas aeroembarcados. **O grau de severidade é entendido como catastrófico; e a probabilidade de ocorrência, como remota**.

6. **Injeção de múltiplas mensagens ADS-B contra estações de solo - IMME**: de maneira similar à injeção individual de mensagens ADS-B contra estações de solo (IME), os controles e as ações mitigadoras consistem nas mesmas soluções apontadas. **O grau de severidade pode ser entendido como maior; e a probabilidade de ocorrência, como remota**.

7. **Injeção de múltiplas mensagens ADS-B contra aeronaves - IMMA**: nesse caso, controle e as ações mitigadoras contra ataques similares a estações de solo não se mostram adequadamente factíveis e efetivos. No entanto, as soluções apontadas para a injeção individual de mensagens ADS-B contra aeronaves (IMA) podem se mostrar promissoras. **O grau de severidade é entendido como catastrófico; e a probabilidade de ocorrência, como remota**.

Quanto ao grau de severidade e à probabilidade de ocorrência atribuída para as ameaças cibernéticas acima listadas, a base conceitual qualitativa para a gradação de ambos os aspectos foi extraída de [5] e como também depreendido em [4]. Também é relevante expor que as opções de controles e ações mitigadoras apresentadas não se encerram em um rol exaustivo e definitivo de soluções possíveis, mas foram as encontradas e entendidas como aplicáveis pelo autor durante o presente estudo.

3.5 AVALIAÇÃO DO RISCO CIBERNÉTICO

Tal qual presente em [4], nessa fase é necessário avaliar e classificar os perigos de acordo com grau de severidade e probabilidade de ocorrência dos riscos estimados, com a finalidade de priorizar e tratar detalhadamente os riscos encontrados a partir do pior cenário identificado. Dessa forma, mostra-se oportuno a utilização da Matriz de Avaliação de Riscos como ferramenta acessória ao processo de GRSO no Sistema ADS-B.

PROBABILIDADE DO RISCO	SEVERIDADE DO RISCO				
	CATASTRÓFICO	PERIGOSO	MAIOR	MENOR	INSIGNIFICANTE
FREQUENTE					1
OCASIONAL					
REMOTO	3, 5, 7	2	4, 6		
IMPROVÁVEL					
EXTREMAMENTE IMPROVÁVEL					

Figura 3.1: Matriz de Avaliação de Riscos para o Sistema ADS-B, elaborada pelo autor.

Na Figura 3.1, é possível verificar o resultado da Avaliação de Riscos realizada com as respectivas siglas atribuídas a cada ameaça identificada contra o Sistema ADS-B.

Logo, as ameaças podem ser organizadas e priorizadas, do maior para o menor índice de risco para tratamento, da seguinte maneira: ISA, IMA e IMMA (Alto Risco – não tolerável); ISE, IME, IMME e IM

(Médio Risco – tolerável). A ameaça IM pode também ser classificada como de Baixo Risco, e assim considerada aceitável, devido à natureza indireta e não invasiva de seus efeitos para o normal funcionamento e segurança operacional do SISCEAB, tal qual depreendido de [4, 5].

3.6 TRATAMENTO DO RISCO CIBERNÉTICO

Sempre que os riscos não puderem ser eliminados por completo, devem ser reduzidos ao máximo a fim de minimizar os efeitos de sua ocorrência. O presente em [5] ainda aponta que: "*Na avaliação das opções para mitigar os riscos deve-se considerar, antes de tomar uma decisão, o esforço para a implementação e a eficácia das medidas mitigadoras para que se possa adotar a solução ótima [e viável]*".

Por outro lado, caso se opte pela aceitabilidade de eventual risco, seja pela complexidade intrínseca à eliminação ou mitigação no momento (financeira, tecnológica, operacional etc.), seja pelo entendimento que o risco é de médio ou baixo nível e passível de ser aceito, deve-se ter em mente que tal posicionamento deve ser adequadamente fundamentado e revestido de constante acompanhamento do risco aceito para que não se incorra em danos à segurança operacional.

Nos casos em análise, os riscos ao Sistema ADS-B entendidos como Risco Alto (ISA, IMA e IMMA) residem em riscos inaceitáveis. Ou seja, que as mudanças ou implementações concernentes à ADS-B e diretamente correlatas às referidas ameaças não devem ser implementadas até que os riscos associados aos perigos sejam mitigados e reduzidos a Médio ou Baixo Risco. Porém, no tocante às ameaças entendidas como de Médio Risco (ISE, IME, IMME e IM), estas podem ser aceitas e toleradas, desde que mitigadas a um patamar tão baixo quanto praticável, sem se prescindir do constante monitoramento da segurança operacional para que não incorram em danos para a consciência situacional e o processo decisório dos envolvidos no SISCEAB, em especial aos controladores de tráfego aéreo e os pilotos em comando de aeronaves em voo.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS OBTIDOS

"Saber muito não lhe torna inteligente. A inteligência se traduz na forma que você recolhe, julga, maneja e, sobretudo, onde e como aplica esta informação."

Carl Sagan

Neste capítulo, serão discutidos os resultados obtidos a partir da análise de riscos cibernéticos realizada através do método de Gerenciamento de Risco à Segurança Operacional (GRSO), e que possuiu como objeto de análise aqueles afetos à implantação ADS-B no SISCEAB.

Porém, neste momento, cabe uma ressalva sobre a ameaça cibernética configurada a partir da Interceptação de mensagens ADS-B - IM. Tal ameaça, ainda que se correlacione de forma comum aos dois contextos em análise - ATCOs e tripulações -, devido a sua natureza passiva e não causadora de impacto direto no processo decisório de ambos, não será abordada na sequência, visto que foi analisada de maneira suficiente no capítulo anterior.

Diante disto, a seguir, dissertaremos sobre os outros riscos cibernéticos identificados na perspectiva de seus principais interessados, quais sejam os controladores de tráfego aéreo e os pilotos em voo, com o foco no impacto de cada risco em seus respectivos processos decisórios.

4.1 RISCOS AO PROCESSO DECISÓRIO DE CONTROLADORES DE TRÁFEGO AÉREO

Em relação à perspectiva de controladores de tráfego aéreo, três riscos cibernéticos emergem de forma direta, quais sejam, interferência ou sobreposição intencional de sinal contra estações de solo - ISE; injeção de mensagens ADS-B contra estações de solo - IME; e injeção de múltiplas mensagens ADS-B contra estações de solo - IMME.

4.1.1 Interferência ou sobreposição intencional de sinal contra estações de solo - ISE

Em relação à primeira ameaça cibernética identificada contra estações de solo, os resultados encontrados a partir da modelagem sobre tal ameaça e revisão bibliográfica, sobretudo com o presente em [14, 82, 83], atestam para a exequibilidade e efetividade do ataque a ser conflagrado ao canal de frequência 1090MHz com efeitos não somente na recepção de sinais ADS-B, mas também na recepção de sinais SSR, estes também usuários do referido canal receptor. Tal questão pode ser potencializada e explorada devido ao já existente e conhecido cenário de congestionamento observado em tal frequência, facilitando, assim, a ação adversa, ao reduzir a complexidade e os parâmetros técnicos envolvidos na construção e emprego do(s) equipamento(s) interferidor(es).

Neste estudo, para tal ameaça, optou-se por um cenário de ameaça cibernética ISE, em que a ação é procedida nas imediações da antena receptora/emissora de sinal ADS-B e em que os agentes adversos possuem motivações e capacidades compatíveis às observadas por ciberativistas, *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados. Ainda que a probabilidade de ocorrência esteja classificada como remota, a probabilidade pode se elevar caso tal cenário ocorra próximo a aeroportos localizados em centros populacionais com a presença de alta densidade urbana e intenso fluxo aéreo, principalmente em operações ADS-B NRA, facilitando a alocação de meios e a manutenção da anonimidade de tais agentes durante a realização do ataque.

Já quanto à severidade do risco, observou-se a classificação em nível perigoso, uma vez que se assume a existência de outras fontes redundantes provedoras de dados e informações CNS/ATM disponíveis e passíveis de auxiliarem no processo decisório de ATCOs, enquanto perdurar os efeitos da degradação parcial ou total imposta pela ameaça ISE.

Ainda que o risco tenha sido classificado como Risco Médio (Tolerável) para tal ameaça, recomendam-se estudos de viabilidade (custo x benefício) no sentindo da adoção, quando não já implementadas, de soluções baseadas em saltos de frequência, detecção e antijamming; no intuito de se mitigar a chance de sobrecarga ou degradação da consciência situacional ATCO, sobretudo nas fases críticas de descida, aproximação final e pouso de aeronaves em espaços aéreos com alta densidade de fluxo aéreo. De forma indireta, o processo decisório de pilotos de aeronaves em fase de descida, aproximação final e pouso também pode ser afetado, seja por procedimentos contingenciais e de segurança (manutenção de longa espera para pouso, arremetida, etc) realizados por ATCOs, seja pelos efeitos da residual ação da interferência observada em seus próprios sistemas de bordo (por exemplo, TCAS, ADS-B In, etc.)

4.1.2 Injeção de mensagens ADS-B contra estações de solo - IME/IMME

Por outro lado, em relação à ameaça consubstanciada na injeção de mensagens ADS-B contra estações de solo - IME/IMME, os resultados obtidos a partir de extensa revisão bibliográfica referenciada neste estudo, inclusive de viés prático [14, 24, 30], também atestaram a exequibilidade e efetividade dos ataques, sobretudo a partir de transceptores de baixo custo e (ou) suportados por SDR. Há de se destacar, que, devido à existente e considerável disponibilidade já documentada de soluções baseadas em softwares livres e em SDRs para tal intento, a realização do ataque IMME mostra-se ainda mais factível, ao objetivar a emulação computacional dos efeitos de múltiplos módulos ADS-B Out sem o custo e os equipamentos que seriam necessários no mundo real.

Em relação às ameaças IME e IMME, optou-se por um cenário de ameaça cibernética em que a ação é procedida nas imediações da antena receptora de sinal ADS-B e em que os agentes adversos possuem motivações e capacidades compatíveis as de *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados. Ainda que a probabilidade de ocorrência esteja classificada como remota, a probabilidade pode se elevar caso tal cenário ocorra próximo a aeroportos localizados em centros populacionais com a presença de alta densidade urbana e intenso fluxo aéreo, principalmente em operações ADS-B NRA, facilitando a alocação de meios e a manutenção da anonimidade de tais agentes durante a realização dos ataques de injeção.

Já quanto à severidade do risco, observou-se a classificação em nível maior, pois se assume a existência de outras fontes redundantes provedoras de dados e informações CNS/ATM, assim como de fusão de dados acessórios para a determinação de posições de aeronaves em voo como as tecnologias PSR e MLAT, disponíveis e passíveis de auxiliarem no processo decisório de ATCOs enquanto perdurar os efeitos negativos da sobrecarga e (ou) degradação em performance parcial ou total imposto pelas injeções de mensagens ADS-B ilegítimas a partir dos ataques IME e IMME.

Ainda que o risco tenha sido classificado como Risco Médio (Tolerável) para tais ameaças, recomendam-se estudos de viabilidade no sentido da adoção conjunta à ADS-B, caso ainda não já implementadas, de soluções baseadas em fusão de dados (como dados de plano de voo, leitura de sistemas radares, etc.) e leituras de outros equipamentos de vigilância aérea (radares PSR e SSR, multilateração, confirmação via fonia, etc) para identificação e desconsideração do tráfego injetado; no intuito de se mitigar a chance de sobrecarga ou degradação da consciência situacional ATCO, sobretudo em fases críticas de decolagem, aproximação final e pouso de aeronaves em espaços aéreos com alta densidade. De forma indireta, o processo decisório de pilotos de aeronaves em fase de descida, aproximação final e pouso poderá também ser afetado, seja por procedimentos contingenciais e de segurança (manutenção de espera para pouso, arremetida, etc) orientados por ATCOs, seja pela eventual e colateral ação de injeção de mensagens ADS-B observada em seus próprios sistemas de bordo (por exemplo, TCAS, ADS-B In, etc.).

4.2 RISCOS AO PROCESSO DECISÓRIO DE PILOTOS EM COMANDO DE VOO

Ainda no que se relaciona aos riscos cibernéticos à implantação ADS-B na área de atuação do SIS-CEAB, três ameaças identificadas atuam diretamente e de maneira sensível no processo decisório de pilotos em comando de voo, quais sejam, interferência ou sobreposição intencional de sinal contra aeronaves - ISA; injeção de mensagens ADS-B contra aeronaves - IMA; e injeção de múltiplas mensagens ADS-B contra aeronaves - IMMA.

4.2.1 Interferência ou sobreposição intencional de sinal contra aeronaves - ISA

Em relação à ameaça ISA, os resultados encontrados a partir da modelagem sobre tal ameaça e revisão bibliográfica, sobretudo com o presente em [14, 82], atestam para a exequibilidade e efetividade do ataque a ser conflagrado ao canal de frequência 1090MHz com efeitos não somente na recepção de sinais ADS-B, mas também na recepção de sinais SSR, também usuário do mesmo canal receptor. Tal questão pode ser potencializada e explorada devido ao já existente cenário de congestionamento observado em tal banda de frequência - inclusive na recepção em voo -, facilitando assim, a ação adversa, ao reduzir a complexidade e os parâmetros técnicos envolvidos na construção e emprego do equipamento interferidor.

Cabe ainda expor, que em comparação à ameaça ISE, o ataque performado pela ISA mostra-se mais desafiador por ser tratar de alvo em movimento e durante curto espaço de tempo para atuação, ainda que em caso de êxito os efeitos configurem-se como catastróficos. Uma possibilidade que também cabe citar é a da utilização de RPAs como vetores de interferência intencional na frequência 1090MHz (comum às mensagens direcionadas ao módulo ADS-B In e às respostas SSR direcionadas ao TCAS), o que facilitaria

a aproximação de aeronaves para conformação de ataques ISA.

Para tal ameaça, optou-se por um cenário de ameaça cibernética em que a ação é procedida à curta e média distância da antena receptora/emissora de sinal ADS-B da aeronave-alvo e em que os agentes adversos possuem motivações e capacidades compatíveis as de *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados pelo Estado. Ainda que a probabilidade de ocorrência esteja classificada como remota, a probabilidade pode se elevar caso tal cenário ocorra próximo a aeroportos localizados em centros populacionais com a presença de alta densidade urbana e intenso fluxo aéreo, principalmente em operações ADS-B NRA, facilitando a alocação de meios e a manutenção da anonimidade de tais agentes durante a realização do ataque ISA.

Já quanto à severidade do risco, observou-se a classificação em nível catastrófico, uma vez que o *jamming* contra aeronaves mostra-se mais danoso sobretudo por configurar dano direto ao material e (ou) à vida humana em caso de sucesso da ameaça ISA, máxime em fases críticas de voo, como em decolagem ou em procedimento de aproximação final e pouso, bem como em voo por instrumentos. Outro fator que fundamentou tal classificação do risco reside em que diferente da ameaça voltada às estações de solo, o vetor aéreo não possui os mesmos meios observados em solo, em variedade de fontes redundantes provedoras de dados e informações CNS/ATM disponíveis e passíveis de auxiliarem no processo decisório de pilotos, como o observado para ATCOs, enquanto perdurar os efeitos da degradação parcial ou total imposto pela ameaça ISA.

Dessa forma, a ameaça ISA foi classificada como de Alto Risco (Não Tolerável), o que demanda ações diretas e preventivas antes da implantação da ADS-B no SISCEAB (sobretudo em espaço aéreo continental), no sentido de implantação conjunta, quando não já implementadas, de soluções aeroembarcadas baseadas em saltos de frequência, e enlaces de dados digitais seguros para troca de informações (CPDLC etc.), a fim de reduzir o risco de tal ameaça aos níveis considerado Médio ou Baixo, ambos toleráveis pelo GRSO.

Tais ações visam a mitigar a chance de sobrecarga ou degradação da consciência situacional de pilotos em voo durante o período de interferência intencional em seus próprios sistemas de bordo (por exemplo, TCAS, ADS-B In, etc.), sobretudo durante fases críticas de descida, aproximação final e pouso de aeronaves em espaços aéreos com alta densidade, e, de forma indireta, reduzir os efeitos colaterais e negativos de tais ações no processo decisório de ATCOs, para que estes não incorram em erro procedimental ou de julgamento no tocante à manutenção da segurança e à organização do espaço aéreo sob controle.

4.2.2 Injeção de mensagens ADS-B contra aeronaves - IMA/IMMA

Em relação às ameaças IMA e IMMA, os resultados obtidos concernentes a tais ameaças cibernéticas pós-análise, a partir de revisão bibliográfica referenciada neste estudo, inclusive de viés prático [14, 24, 30], também atestaram para a exequibilidade e efetividade do ataque de maneira similar ao observado às ameaças IME e IMME. Assim, os ataques cibernéticos IMA e IMMA também podem ser realizados a partir de transceptores de baixo custo e (ou) suportados por SDR. Há de se destacar também, que, devido à disponibilidade de soluções baseadas em softwares livres e em SDR para tal intento como descrito, a realização do ataque IMMA mostra-se ainda mais factível, ao objetivar a emulação computacional dos

efeitos de múltiplos módulos ADS-B Out sem o custo e os equipamentos que seriam necessários no mundo real.

No entanto, tais ameaças possuem um componente adjacente e especialmente malicioso que se mostra especificamente pernicioso ao meio aéreo: as injeções de mensagens interceptadas, modificadas ou falsificadas ADS-B contra aeronaves (IMA/IMMA) não só consistem em fontes de dados para o módulo ADS-In, mas também para o Sistema Anticolisão de Tráfego - TCAS. A injeção de tais mensagens, assim como leitura e interpretação dos dados presentes nas mensagens ADS-B falsificadas pelo TCAS, sobretudo em fases críticas do voo como aproximação final e pouso, podem influenciar na condução de manobras inadequadas a partir de falsos positivos em tela e alarmes sonoros (tais como tráfego em rota, subida ou descida), a depender se a aeronave ilegítima constar em área reservada para alerta de tráfego (TA) ou em área reservada para alertas de resolução (RA).

Em caso de sucesso dos ataques IMA e (ou) IMMA, em que aeronaves ilegítimas apareçam no TCAS em área reservada para RA, a gravidade se acentua, tal qual depreendido de [84], o qual aponta que caso o piloto receba um alerta de resolução, o mesmo deve "*seguir o RA mesmo se houver conflito entre o RA e a instrução do controle de tráfego aéreo (ATC) para manobra*", assim como em tal momento o piloto "não [deve] efetuar manobra contrária ao sentido de um RA".

Assim, este autor acredita, a partir dos estudos empreendidos neste trabalho, que os efeitos do ataque IMA e IMMA ao TCAS mostram-se tão ou mais perigosos do que os efeitos causados no módulo ADS-B In aeroembarcado, uma vez que a depender do modelo, nível de automação e equipamentos de vigilância disponíveis na aeronave sob ataque, ações podem ocorrer de forma automatizada levando o piloto em comando ao erro, com impactos diretos e catastróficos à segurança operacional. Inclusive, com reflexos peremptórios para a manutenção da segurança e o processo decisório dos ATCOs em TWR e APP, bem como de outras aeronaves que compartilham o mesmo espaço aéreo controlado.

Ainda em relação às ameaças IMA e IMMA, optou-se por um cenário de ameaça cibernética em que a ação é procedida à curta e média distância da antena receptora de sinal ADS-B e em que os agentes adversos possuem motivações e capacidades compatíveis as de *insiders*, cibercriminosos, ciberterroristas e Estado-Nação e (ou) grupos patrocinados. Ainda que a probabilidade de ocorrência esteja classificada como remota, e como descrito para ameaça ISA, a probabilidade pode se elevar caso tal cenário ocorra próximo a aeroportos localizados em centros populacionais com a presença de alta densidade urbana e intenso fluxo aéreo, principalmente em operações ADS-B NRA, facilitando a alocação de meios e a manutenção da anonimidade de tais agentes durante a realização de tais ataques de injeção.

Já quanto à severidade do risco, observou-se a classificação em nível catastrófico, uma vez que se assume que não há meios aeroembarcados similares aos observados para contraposição de ataques IME e IMME, como por exemplo fontes provedoras de dados e informações CNS/ATM, assim como a fusão de dados acessórios para a determinação de posições de aeronaves em voo, como as proporcionadas pelas tecnologias PSR e MLAT; e por configurar, em caso de êxito, dano direto ao material e (ou) à vida humana, máxime em fases críticas do voo, como em decolagem ou em procedimento de aproximação final e pouso, bem como em voo por instrumentos.

Dessa forma, as ameaças IMA e IMMA foram classificadas como de Alto Risco (Não Tolerável), o que demanda ações diretas e preventivas antes da implantação ADS-B no SISCEAB (sobretudo em

espaço aéreo continental), no sentido de implantação conjunta, quando não já implementadas, de soluções aeroembarcadas baseadas em soluções criptográficas (suportadas por chaves públicas) para autenticação ou na filtragem estatística das leituras pelo método Kalman para estimar localizações ou em enlaces de dados digitais para troca de informações (CPDLC etc.), a fim de reduzir o risco de tal ameaça aos níveis considerado Médio ou Baixo, ambos toleráveis pelo GRSO.

Tais ações visam a mitigar a chance de sobrecarga ou degradação da consciência situacional de pilotos em voo enquanto perdurar os efeitos da sobrecarga e (ou) degradação em performance parcial ou total impostos pelas injeções de mensagens ADS-B ilegítimas a partir dos ataques IMA e IMMA em seus próprios sistemas de bordo (por exemplo, TCAS, ADS-B In, etc.), sobretudo durante fases críticas de descida, aproximação final e pouso de aeronaves em espaços aéreos com alta densidade de aeronaves, e, de forma indireta, reduzir os efeitos colaterais e perniciosos das ações realizadas contra a tripulação sob ataque, no tocante à manutenção da segurança e organização do espaço aéreo sob controle, auxiliando, assim, o processo decisório de ATCOs e para que estes não incorram em erro de julgamento ou procedimental.

5 CONCLUSÃO

"Não há nada a temer na vida, apenas tratar de compreender."

Marie Curie

Ainda que a ADS-B mereça todo destaque por suas capacidades em prover cobertura em todas as fases do voo, possuir taxa de atualização superior e economicidade durante seu ciclo de vida em comparação a suas alternativas baseadas em tecnologia radar, questionamentos sobre os aspectos de segurança presentes em seu cerne não devem ser silenciados sem antes o devido escrutínio. Assim, este estudo objetivou, por meio de uma investigação inicial, cobrir uma das lacunas existentes e a ser respondida: em que grau a exploração do Sistema ADS-B impacta no processo decisório dos responsáveis pelo controle do tráfego aéreo e nas ações de tripulações em voo atuantes no SISCEAB.

Para isso, valemo-nos do principal método de análise do risco à segurança operacional utilizado pelo SISCEAB para identificar, analisar, avaliar e tratar riscos, conhecido como GRSO, com a finalidade de analisar os riscos cibernéticos envolvidos na implantação ADS-B no contexto nacional.

Foram encontrados riscos inaceitáveis, tais como: a interferência ou sobreposição intencional de sinal contra aeronaves; e a injeção individual e múltipla de mensagens ADS-B modificadas ou ilegítimas, todas contra aeronaves. Esses riscos mostram-se sensíveis ao passo que podem ser diretamente danosos a um elemento essencial na "engrenagem" do tráfego aéreo, quais sejam, as aeronaves em voo, não só em perdas materiais, mas, sobretudo, humanas; e, indiretamente, quando incorre em perda de consciência situacional ou aumento de carga de trabalho para controladores devido à coordenação extra em caso de ataques.

Em contrapartida, os outros riscos cibernéticos à segurança operacional identificados, analisados e classificados como de média gradação, ainda que não diretamente passíveis de extrema urgência de tratamento e eliminação, revestem-se da necessidade de mitigação e monitoramento constante, caso venham a ser tolerados ou aceitos pelas autoridades competentes pela segurança operacional brasileira.

5.1 TRABALHOS FUTUROS

Como sugestão para trabalhos futuros, destacamos a necessidade da realização de pesquisas e avaliações operacionais em campo para verificar o nível de suscetibilidade dos equipamentos a serem utilizados na implantação em larga escala da ADS-B no âmbito do SISCEAB a tais ameaças cibernéticas analisadas neste trabalho, sobretudo as direcionadas aos equipamentos aeroembarcados, como TCAS (ainda pouco explorado pela academia), assim como o estudo para definição e condução de procedimentos preventivos e contingenciais a serem seguidos por controladores ATC e pilotos em voo, no caso de identificação de ataques realizados contra o Sistema ADS-B e outros sistemas acessórios, embarcados ou em solo, que utilizem tais mensagens como fonte de dados de interesse, principalmente durante as fases críticas de voo.

REFERÊNCIAS BIBLIOGRÁFICAS

1 FOLHAONLINE. *Voar é seguro? Qual o procedimento que oferece mais risco num vôo?* Jornal Folha de São Paulo, 2021. Disponível em: <https://www1.folha.uol.com.br/folha/turismo/preparese/aviao-voar_e_seguro-04.shtml>. Acesso em: 24 jan. 2023.

2 RODRIGUES, R. *Estrutura do Espaço Aéreo Brasileiro*. IVAO Brasil Academy, Departamento de Treinamento, 2013. Disponível em: <https://academia.br.ivao.aero/view/21>. Acesso em: 24 jan. 2023.

3 DECEA. *Website Perfomance do SISCEAB*. 2022. Disponível em: <https://performance.decea.mil.br/>. Acesso em: 24 jan. 2023.

4 BRASIL. *Manual do Comando da Aeronáutica (MCA) 63-14: Manual de Gerenciamento do Risco à Segurança Operacional no SISCEAB*. [S.l.], 2012. Disponível em: <https://publicacoes.decea.mil.br/publicacao/mca-63-14>. Acesso em: 24 jan. 2023.

5 BRASIL. *Instrução do Comando da Aeronáutica (ICA) 63-26: Gerenciamento do Risco à Segurança Operacional no SISCEAB*. [S.l.], 2010. Disponível em: <https://publicacoes.decea.mil.br/publicacao/ica-63-26>. Acesso em: 24 jan. 2023.

6 STROHMEIER, M.; LENDERS, V.; MARTINOVIC, I. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Communications Surveys & Tutorials*, IEEE, v. 17, n. 2, p. 1066–1087, 2014.

7 RODRIGUES, C. V. C. *ADS-B-automatic dependent surveillance broadcast: estudo do impacto em Portugal*. Tese (Doutorado) — Universidade da Beira Interior (Portugal), 2010.

8 STROHMEIER, M. *Security in next generation air traffic communication networks*. Tese (Doutorado) — University of Oxford, 2016.

9 BOEING. *Boeing Current Market Outlook 2021-2040*. [S.l.], 2021. Disponível em: <https://www.boeing.com/commercial/market/commercial-market-outlook/>. Acesso em: 24 jan. 2023.

10 ICAO. *Forecasts of Scheduled Passenger and Freight Traffic 2018-2038*. [S.l.], 2018. Disponível em: <https://www.icao.int/sustainability/Pages/eap-fp-forecast-scheduled-passenger-traffic.aspx>. Acesso em: 24 jan. 2023.

11 EMBRAER. *Embraer Market Outlook 2020-2039*. [S.l.], 2020. Disponível em: <https://www.embraermarketoutlook2020.com/wp-content/uploads/2020/12/Embraer_MarketOutlook_8_12_2020.pdf>. Acesso em: 24 jan. 2023.

12 CERQUEIRA, R. S. Ads-b no espaço aéreo brasileiro: Propostas de melhorias da regulação. *Revista da UNIFA*, v. 34, n. 2, 2021.

13 ALI, B. S.; OCHIENG, W. Y.; SCHUSTER, W.; MAJUMDAR, A.; CHIEW, T. K. A safety assessment framework for the automatic dependent surveillance broadcast (ads-b) system. *Safety Science*, v. 78, p. 91–100, 2015. ISSN 0925-7535. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0925753515001034>.

14 SCHÄFER, M.; LENDERS, V.; MARTINOVIC, I. Experimental analysis of attacks on next generation air traffic communication. In: JACOBSON, M.; LOCASTO, M.; MOHASSEL, P.; SAFAVI-NAINI, R. (Ed.). *Applied Cryptography and Network Security*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. p. 253–271. ISBN 978-3-642-38980-1.

15 SCARSO, R. E.; SANTOS, R. M. dos. Ads-b: Custo-benefício para a aviação geral brasileira. *RETEC-Revista de Tecnologias*, v. 11, n. 1, 2018.

16 MARINHO, D. *Comitiva oficializa operação ADS-B na Bacia de Campos*. DECEA, 2018. Disponível em: <https://www.decea.mil.br/?i=midia-e-informacao&p=pg_noticia&materia=comitiva-oficializa-obrigatoriedade-do-uso-do-ads-b-na-bacia-de-campos>. Acesso em: 24 jan. 2023.

17 MEIRELES, D. *Acordo entre DECEA e AIREON visa à coleta de dados de vigilância para aeronaves pelo ADS-B Satelital*. DECEA, 2019. Disponível em: <https://www.decea.mil.br/?i=midia-e-informacao&p=pg_noticia&materia=artigo-decea-ads-b-satelital>. Acesso em: 24 jan. 2023.

18 BRASIL. *Diretriz do Comando da Aeronáutica (DCA) 351-2: Concepção Operacional ATM Nacional*. [S.l.], 2021. Disponível em: <https://publicacoes.decea.mil.br/publicacao/dca-351-2>. Acesso em: 24 jan. 2023.

19 BRASIL. *Plano do Comando da Aeronáutica (PCA) 351-3: Plano de Implementação ATM Nacional*. [S.l.], 2022. Disponível em: <https://publicacoes.decea.mil.br/publicacao/pca-351-3>. Acesso em: 24 jan. 2023.

20 PADILHA, L. *Thales fornecerá 66 estações de vigilância para o DECEA ampliar segurança em voos comerciais*. Defesa Aérea e Naval, 2023. Disponível em: <https://www.defesaaereanaval.com.br/defesa/thales-fornecera-66-estacoes-de-vigilancia-para-o-decea-ampliar-seguranca-em-voos-comerciais>. Acesso em: 02 fev. 2023.

21 CTCEA. *ESPECIFICAÇÃO TÉCNICA, LOGÍSTICA E INDUSTRIAL PARA IMPLANTAÇÃO DE UM SISTEMA DE VIGILÂNCIA DEPENDENTE AUTOMÁTICA POR RADIODIFUSÃO (ADS-B) NO ESPAÇO AÉREO CONTINENTAL BRASILEIRO 000.06.T03.EP.001.06*. Comissão de Implantação do Sistema de Controle do Espaço Aéreo - CISCEA, 2019. Disponível em: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiF896-oaT9AhVypJUCHalfDSYQFnoECBEQAQ&url=https%3A%2F%2Fwww2.fab.mil.br%2Fcabw%2Fattachments%2Farticle%2F277%2FESPECIFICAC%25CC%25A7A%25CC%2583O%2520TE%25CC%2581CNICA%2520-%2520ADS-B%2520NACIONAL%2520-%2520REV%252006%2520-%252015_10_19.docx&usg=AOvVaw2bZP2dGIUR34AdFOdTrhmR>. Acesso em: 14 fev. 2023.

22 STROHMEIER, M.; SCHäFER, M.; PINHEIRO, R.; LENDERS, V.; MARTINOVIC, I. On perception and reality in wireless air traffic communication security. *IEEE Transactions on Intelligent Transportation Systems*, v. 18, n. 6, p. 1338–1357, 2017.

23 PURTON, L.; ABBASS, H.; ALAM, S. Identification of ads-b system vulnerabilities and threats. In: *Australian Transport Research Forum, Canberra*. [S.l.: s.n.], 2010. p. 1–16.

24 COSTIN, A.; FRANCILLON, A. Ghost in the air (traffic): On insecurity of ads-b protocol and practical attacks on ads-b devices. *black hat USA*, v. 1, p. 1–12, 2012.

25 LEŚNIKOWSKI, W. Threats from cyberspace for civil aviation. *Wiedza Obronna*, v. 276, n. 3, p. 124–153, 2021.

26 STROHMEIER, M.; SCHÄFER, M.; LENDERS, V.; MARTINOVIC, I. Realities and challenges of nextgen air traffic management: the case of ads-b. *IEEE Communications Magazine*, IEEE, v. 52, n. 5, p. 111–118, 2014.

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

28 MCCALLIE, D.; BUTTS, J.; MILLS, R. Security analysis of the ads-b implementation in the next generation air transportation system. *International Journal of Critical Infrastructure Protection*, Elsevier, v. 4, n. 2, p. 78–87, 2011.

29 VIVEROS, C. A. P. *Analysis of the cyber attacks against ADS-B perspective of aviation experts*. Dissertação (Mestrado) — University of Tartu Tartu, Estonia, 2016.

30 HAINES, B. Hacker + airplanes = no good can come of this. In: DEFCON. 2012. Disponível em: <https://www.youtube.com/watch?v=CXv1j3GbgLk>. Acesso em: 24 jan. 2023.

31 STROHMEIER, M.; MOSER, D.; SCHAFER, M.; LENDERS, V.; MARTINOVIC, I. On the applicability of satellite-based air traffic control communication for security. *IEEE Communications Magazine*, IEEE, v. 57, n. 9, p. 79–85, 2019.

32 STROHMEIER, M.; SCHÄFER, M.; SMITH, M.; LENDERS, V.; MARTINOVIC, I. Assessing the impact of aviation security on cyber power. In: IEEE. *2016 8th International Conference on Cyber Conflict (CyCon)*. [S.l.], 2016. p. 223–241.

33 LYKOU, G.; IAKOVAKIS, G.; GRITZALIS, D. Aviation cybersecurity and cyber-resilience: assessing risk in air traffic management. In: *Critical Infrastructure Security and Resilience*. [S.l.]: Springer, 2019. p. 245–260.

34 UKWANDU, E.; BEN-FARAH, M. A.; HINDY, H.; BURES, M.; ATKINSON, R.; TACHTATZIS, C.; ANDONOVIC, I.; BELLEKENS, X. Cyber-security challenges in aviation industry: a review of current and future trends. *Information*, MDPI, v. 13, n. 3, p. 146, 2022.

35 WU, Z.; SHANG, T.; GUO, A. Security issues in automatic dependent surveillance-broadcast (ads-b): a survey. *IEEE Access*, IEEE, v. 8, p. 122147–122167, 2020.

36 VILELA, R. A. R. *ADS-B: Implementação e modernização do espaço aéreo brasileiro*. 50 p. Monografia (Graduação em Ciências Aeronáuticas) — Universidade do Sul de Santa Catarina - UNISUL, Palhoça-SC, 2017.

37 SILVA, M. V. A. Panorama da ameaça cibernética à aviação civil. *Revista Brasileira de Inteligência*, n. 14, p. 67–84, 2019.

38 GSI/PR. *Glossário de Segurança da Informação*. Departamento de Segurança da Informação do Gabinete de Segurança Institucional GSI/PR, 2021. Disponível em: <https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1>. Acesso em: 24 jan. 2023.

39 ZHANG, H.; HAN, W.; LAI, X.; LIN, D.; MA, J.; LI, J. Survey on cyberspace security. *Science China Information Sciences*, Springer, v. 58, n. 11, p. 1–43, 2015.

40 CARDOSO, L. H. F. Anatomia de um ataque cibernético: conhecer e entender para melhor defender os ativos e meios de interesse da força aérea brasileira. *SPECTRUM: Revista do Comando de Preparo - COMPREP*, Força Aérea Brasileira, v. 20, p. 51–57, 2017.

41 ANAC. *Manual de Conscientização em Segurança Cibernética da Aviação Civil*. [S.l.], 2021. Disponível em: <https://www.gov.br/anac/pt-br/assuntos/regulados/aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf>. Acesso em: 24 jan. 2023.

42 ZOU, Y.; ZHU, J.; WANG, X.; HANZO, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, IEEE, v. 104, n. 9, p. 1727–1765, 2016.

43 BRASIL. *Manual do Comando da Aeronáutica (MCA) 7-1: Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo (DECEA)*. [S.l.], 2012. Disponível em: <https://publicacoes.decea.mil.br/publicacao/mca-7-1>. Acesso em: 24 jan. 2023.

44 BRASIL. *Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. Diário Oficial da União: seção 1*. [S.l.], 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>. Acesso em: 24 jan. 2023.

45 KUMAR, S. A.; XU, B. Vulnerability assessment for security in aviation cyber-physical systems. In: IEEE. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. [S.l.], 2017. p. 145–150.

46 VENKATRAMAN, K.; DANIEL, J. V.; MURUGABOOPATHI, G. Various attacks in wireless sensor network: Survey. *International Journal of Soft Computing and Engineering (IJSCE)*, Citeseer, v. 3, n. 1, p. 208–212, 2013.

47 MPITZIOPOULOS, A.; GAVALAS, D.; KONSTANTOPOULOS, C.; PANTZIOU, G. A survey on jamming attacks and countermeasures in wsns. *IEEE communications surveys & tutorials*, IEEE, v. 11, n. 4, p. 42–56, 2009.

48 KOŽOVIĆ, D. V.; ĐURđEVIĆ, D. Ž. Spoofing in aviation: Security threats on gps and ads-b systems.

49 JEBA, S.; PARAMASIVAN, B. False data injection attack and its countermeasures in wireless sensor networks. *European Journal of Scientific Research*, v. 82, n. 2, p. 248–257, 2012.

50 FERRO, L. S.; MARRELLA, A.; CATARCI, T. A human factor approach to threat modeling. In: SPRINGER. *International Conference on Human-Computer Interaction*. [S.l.], 2021. p. 139–157.

51 BODEAU, D. J.; MCCOLLUM, C. D.; FOX, D. B. *Cyber threat modeling: Survey, assessment, and representative framework*. [S.l.], 2018.

52 XIONG, W.; LAGERSTRÖM, R. Threat modeling–a systematic literature review. *Computers & security*, Elsevier, v. 84, p. 53–69, 2019.

53 XIONG, W.; LEGRAND, E.; ÅBERG, O.; LAGERSTRÖM, R. Cyber security threat modeling based on the mitre enterprise att&ck matrix. *Software and Systems Modeling*, Springer, v. 21, n. 1, p. 157–177, 2022.

54 ROSS, R.; SP, N. 800-30rev1 guide for conducting risk assessments. *The National Institute of Standards and Technology (NIST), Gaithersburg*, v. 8, 2012.

55 BODEAU, D.; GRAUBART, R. *Characterizing effects on the cyber adversary: A vocabulary for analysis and assessment*. [S.l.], 2013.

56 REFSDAL, A.; SOLHAUG, B.; STØLEN, K. Cyber-risk management. In: *Cyber-risk management*. [S.l.]: Springer, 2015. p. 33–47.

57 LEE, I. Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, v. 64, n. 5, p. 659–671, 2021. ISSN 0007-6813. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0007681321000240>.

58 ELING, M.; MCSHANE, M.; NGUYEN, T. Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, Wiley Online Library, v. 24, n. 1, p. 93–125, 2021.

59 EMANUELLI, G. B. Cibersegurança na aviação civil brasileira (2016–2019). *Territorium*, n. 29 (I), p. 149–160, 2022.

60 NOBLES, C. Cyber threats in civil aviation. In: *Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications*. [S.l.]: IGI Global, 2019. p. 119–141.

61 DECEA. *Programa SIRIUS*. 2022. Disponível em: <https://sirius.decea.mil.br/>. Acesso em: 24 jan. 2023.

62 DAVE, G.; CHOUDHARY, G.; SIHAG, V.; YOU, I.; CHOO, K.-K. R. Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*, Elsevier, v. 112, p. 102516, 2022.

63 KAUNE, R.; STEFFES, C.; RAU, S.; KONLE, W.; PAGEL, J. Wide area multilateration using ads-b transponder signals. In: IEEE. *2012 15th International Conference on Information Fusion*. [S.l.], 2012. p. 727–734.

64 XU, Y. Tcas/ads-b integrated surveillance and collision avoidance system. In: ATLANTIS PRESS. *Conference of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)*. [S.l.], 2013. p. 666–669.

65 SMITH, M.; STROHMEIER, M.; LENDERS, V.; MARTINOVIC, I. On the security and privacy of acars. In: IEEE. *2016 Integrated Communications Navigation and Surveillance (ICNS)*. [S.l.], 2016. p. 1–27.

66 CHEN, P.; DESMET, L.; HUYGENS, C. A study on advanced persistent threats. In: SPRINGER. *IFIP International Conference on Communications and Multimedia Security*. [S.l.], 2014. p. 63–72.

67 RAPOSO, A.; OLVEIRA, B.; BORGES, R.; CARDOSO, S.; MARTINS, V. *Controlo de Tráfego Aéreo*. Dissertação (Mestrado Integrado em Engenharia Aeroespacial) — Universidade de Lisboa, Instituo Superior Técnico, 2015. Disponível em: <https://docplayer.com.br/52889369-Controlo-de-trafego-aereo.html>. Acesso em: 24 jan. 2023.

68 BRASIL. *Instrução do Comando da Aeronáutica (ICA) 100-12: Regras do Ar*. [S.l.], 2016. Disponível em: <https://publicacoes.decea.mil.br/publicacao/ica-100-12>. Acesso em: 24 jan. 2023.

69 BOEING. *Boeing Statistical Summary of Commercial Jet Airplane Accidents: Worldwide Operations | 1959 – 2021*. [S.l.], 2022. v. 53. Disponível em: <https://www.boeing.com/resources/boeingdotcom/company/about_bca/pdf/statsum.pdf>. Acesso em: 24 jan. 2023.

70 JASRA, S. K.; VALENTINO, G.; MUSCAT, A.; ZAMMIT-MANGION, D.; CAMILLERI, R. Evaluation of flight parameters during approach and landing phases by applying principal component analysis. In: *AIAA Scitech 2020 Forum*. [S.l.: s.n.], 2020. p. 0674.

71 BRASIL. *Plano do Comando da Aeronáutica (PCA) 11-368: Plano Geral de Controle do Espaço Aéreo*. [S.l.], 2020. Disponível em: <https://publicacoes.decea.mil.br/publicacao/pca-11-368>. Acesso em: 24 jan. 2023.

72 DECEA. *Vídeo Institucional do DECEA (PORT) / Leg ENG - 2019*. 2019. Disponível em: <https://www.youtube.com/watch?v=mwF0DFZogGQ&t=197s>. Acesso em: 24 jan. 2023.

73 BRASIL. *Norma de Sistema do Comando da Aeronáutica (NSCA) 351-1: Sistema de Controle do Espaço Aéreo*. [S.l.], 2022. Disponível em: <https://publicacoes.decea.mil.br/publicacao/nsca-351-1>. Acesso em: 24 jan. 2023.

74 DECEA. *Portal do Departamento de Controle do Espaço Aéreo (DECEA). Áreas de Atuação*. DECEA, 2023. Disponível em: <https://www.decea.mil.br/>. Acesso em: 24 jan. 2023.

75 LIMA, E. D. O.; MOREIRA, F. R.; DEUS, F. E. G. de; NZE, G. D. A.; JÚNIOR, R. T. de S.; NUNES, R. R. Avaliação da rotina operacional do operador nacional do sistema elétrico brasileiro (ons) em relação às ações de gerenciamento de riscos associados à segurança cibernética. *Revista Ibérica de Sistemas e Tecnologias de Informação*, Associação Ibérica de Sistemas e Tecnologias de Informacao, n. E49, p. 301–312, 2022.

76 BRASIL. *Instrução do Comando da Aeronáutica (ICA) 81-2: Gerenciamento da Segurança Operacional do SISCEAB*. [S.l.], 2022. Disponível em: <https://publicacoes.decea.mil.br/publicacao/ica-81-2>. Acesso em: 24 jan. 2023.

77 HAAN, S. D.; BAILEY, L.; KÖNNEN, J. Quality assessment of automatic dependent surveillance contract (ads-c) wind and temperature observation from commercial aircraft. *Atmospheric Measurement Techniques*, Copernicus GmbH, v. 6, n. 2, p. 199–206, 2013.

78 FAA. Automatic dependent surveillance-broadcast (ads-b) out performance requirements to support air traffic control (atc) service; final rule, 14 cfr part 91, federal register 75. Federal Aviation Administration, 2010. Disponível em: <https://www.federalregister.gov/documents/2010/05/28/2010-12645/automatic-dependent-surveillance-broadcast-ads-b-out-performance-requirements-to-support-air-traffic>. Acesso em: 24 jan. 2023.

79 HAASS, J. C.; CRAIGER, J. P.; KESSLER, G. C. A framework for aviation cybersecurity. In: IEEE. *NAECON 2018-IEEE National Aerospace and Electronics Conference*. [S.l.], 2018. p. 132–136.

80 SAMPIGETHAYA, K.; POOVENDRAN, R.; BUSHNELL, L. Assessment and mitigation of cyber exploits in future aircraft surveillance. In: IEEE. *2010 IEEE Aerospace Conference*. [S.l.], 2010. p. 1–10.

81 CARDOSO, L. H. F.; SOUSA, R. T. de et al. Ads-b system exploitation: Analysis of the impact on the decision-making process of air traffic controllers through of the grso method. In: IEEE. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. [S.l.], 2020. p. 1–8.

82 LEONARDI, M.; PIRACCI, E.; GALATI, G. Ads-b vulnerability to low cost jammers: Risk assessment and possible solutions. In: IEEE. *2014 Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)*. [S.l.], 2014. p. 41–46.

83 PIRAYESH, H.; ZENG, H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, IEEE, 2022.

84 BRASIL. *Instrução do Comando da Aeronáutica (ICA) 100-32: Procedimentos operacionais e orientações de treinamento para pilotos e controladores de tráfego aéreo com relação ao Sistema Anticolisão de Bordo (ACAS)*. [S.l.], 2008. Disponível em: <https://publicacoes.decea.mil.br/publicacao/ica-100-32>. Acesso em: 24 jan. 2023.