Exploração do sistema ADS-B: Análise do impacto no processo decisório de controladores de tráfego aéreo por meio do método GRSO

ADS-B system exploitation: Analysis of the impact on the decision-making process of air traffic controllers through of the GRSO method

Luiz Henrique F. Cardoso[1], Georges D. Amvame N.[2], Rafael T. de Sousa Jr[3] e Fábio L. L. Mendonça[4]
Departamento de Engenharia Elétrica, Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE
Universidade de Brasília (UnB)
Brasília-DF, Brasil
cardoso.luiz@aluno.unb.br[1], georges@unb.br[2], desousa@unb.br[3], fabio.mendonca@redes.unb.br[4]

Resumo — **Dentre as mais modernas tecnologias empregadas em sistemas de vigilância do tráfego aéreo, o Sistema ADS-B é o que está em destaque 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 embarcados, 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 do protocolo ADS-B, assim como a literatura não é clara quanto ao impacto da exploração de tais brechas na atuação direta de Controladores de Tráfego Aéreo e pilotos de aeronaves. Este artigo objetiva lançar um olhar analítico sobre as vulnerabilidades presentes no sistema ADS-B, não só ao mapear ataques ao referido protocolo, mas também ao buscar identificar, analisar, avaliar e classificar os riscos inerentes à segurança operacional por meio do método GRSO, com foco no impacto ao processo decisório de Controladores de Tráfego Aéreo**.

Palavras-chave - ADS-B; segurança cibernética; segurança aérea; controle de tráfego aéreo; GRSO.

Abstract — **Among the most modern technologies used in air traffic surveillance systems, the ADS-B System is the one that stands out today. Such technology consists of a set of equipments and protocols designed to provide the means to determine the position of aircraft in flight from embedded navigation systems, as well as to periodically broadcast information of interest to other aircrafts en route and sensors on the ground within your range. However, serious security vulnerabilities lie at the heart of the ADS-B protocol, and the literature is unclear about the impact of exploitations in these breaches on the direct action of Air Traffic Controllers and aircraft pilots. This article aims to take an analytical look at the vulnerabilities present in the ADS-B system, not only when mapping attacks to that protocol, but also when seeking to identify, analyze, evaluate and classify the risks inherent to operational security through the GRSO method, focusing on the impact upon the Air Traffic Controllers decision-making process.**

Keywords - ADS-B; cyber security; air security; air traffic control; GRSO.

I. INTRODUÇÃO

Sistemas de controle do espaço aéreo mundo afora estão expostos a diferentes desafios: 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; e ameaças como sabotagens e ataques à infraestrutura aeroportuária, de navegação aérea e outros sistemas ligados ao controle de tráfego aéreo estão como alguns exemplos dos desafios a serem superados [1].

Para que tais adversidades não coloquem em risco a segurança e operacionalidade do controle de tráfego aéreo mundial, torna-se necessário que os sistemas de vigilância aérea e procedimentos correlatos estejam em constante evolução tecnológica.

Atualmente, tal qual apontado por [1], os principais sistemas de vigilância aérea em operação são suportados, sobretudo, por duas tecnologias: comunicações por voz e dados via rádio (entre controladores e pilotos) e pelos sistemas Radar Primário de Vigilância e Radar Secundário de Vigilância (do inglês, *Primary Surveillance Radars* – PSR e *Secondary Surveillance Radars* – SSR, respectivamente).

No entanto, mesmo que o funcionamento de tais sistemas 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 a instalação e manutenção de tais radares. 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 montanhas [2].

Muito devido às limitações já mencionadas e conforme exposto por [3], esforços tem sido realizados por relevantes

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

órgãos internacionais da aviação civil, como ICAO (*International Civil Aviation Organization)*, FAA (*Federal Aviation Administration)* e EUROCONTROL (*European Organization for the Safety of Air Navigation*) para o desenvolvimento de novos sistemas de vigilância e controle do tráfego aéreo que conjuguem acurácia e confiabilidade com menor custo de implantação e manutenção. Destes, o mais promissor é o Sistema ADS-B (do inglês, *Automatic Dependent Surveillance-Broadcast*).

Tal qual depreendido de [2], o Sistema ADS-B é um conjunto de equipamentos, procedimentos e protocolo destinados a prover meios para determinar precisa posição em voo a partir de sistemas baseados em 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.

A implantação e adoção do sistema ADS-B como principal sistema de vigilância área já é realidade na maioria dos espaços aéreos no mundo. Países como EUA, Canadá e Austrália já contam praticamente com total cobertura de infraestrutura de solo e transceptores instalados em aeronaves, em suporte ao protocolo ora mencionado [3]. No Brasil, ainda tal adoção encontra-se em estado incipiente, apenas com cobertura parcial, e de maneira experimental, na Bacia de Campos-RJ [4]. Porém, o Departamento de Controle do Espaço Aéreo (DECEA), órgão responsável pelo controle do espaço aéreo e navegação aérea brasileira, salienta que o objetivo é que até dezembro de 2022 todo espaço aéreo brasileiro passe a contar em larga escala com suporte do Sistema ADS-B [4,5].

No entanto, e alinhado ao que defende [6], apesar de 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 baseado 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.

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 [3], [7] e [8].

Tais lacunas de segurança, passíveis de serem exploradas por diferentes modalidades de ataques especialmente focadas em vulnerabilidades presentes em componentes do sistema e no próprio protocolo, nos mostram que o risco para a segurança e continuidade das operações áreas não pode ser desprezado, sobretudo em contextos nos quais a dependência do Sistema ADS-B já é (ou será) imperiosa.

Diante do exposto, emerge o seguinte questionamento: em que nível tais ataques podem impactar no processo decisório e (ou) perda de consciência situacional de Controladores de Tráfego Aéreo? Esse artigo visa a intentar responder esse questionamento.

Sendo assim, o restante deste artigo está organizado da seguinte forma: Na Seção II, serão apresentados aspectos essenciais e o estado da arte presente na literatura para o entendimento do sistema ADS-B, seu funcionamento, componentes e principais vulnerabilidades de segurança existentes; Já na Seção III, serão expostos e analisados os principais ataques direcionados ao sistema ADS-B, com maior atenção àqueles que tenham potencial de impactar a normalidade do controle de tráfego aéreo; Na sequência, Seção IV, será apresentado o principal método empregado pelo Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB) para análise de riscos das tecnologias de comunicação, navegação e vigilância sob sua responsabilidade, conhecido como Gerenciamento de Riscos à Segurança Operacional (GRSO); À luz das percepções das potenciais consequências dos ataques listados na Seção III, e dos procedimentos presentes no método GRSO apresentado na Seção IV, será realizada a análise dos riscos identificados com a finalidade de avaliação, priorização e proposição do tratamento dos perigos presentes no ADS-B, com foco no potencial impacto na conduta e consciência situacional dos Controladores de Tráfego Aéreo (do inglês, *Air Traffic Controller – ATCo*), máxime os componentes do SISCEAB; Por fim, na Seção VI, serão expostas as conclusões depreendidas ao final do trabalho.

II. PROTOCOLO ADS-B

Em continuidade ao já inicialmente apresentado sobre o protocolo ADS-B, em [8] os autores acrescentam que o desenvolvimento e implantação do ADS-B, entendido por eles como "*um novo paradigma para o controle de tráfego aéreo mundial*", objetivou um formato diferente de prover informações atualizadas e precisas em todas as fases do voo, de maneira independente e resiliente. Ainda conforme [8]:

> 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 (do inglês, *Air Traffic Control)* 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.

Na Fig. 1, é possível observar os componentes funcionais do Sistema ADS-B, quais sejam: *ADS-B Out* (módulo de transmissão embarcado na aeronave), *ADS-B In* (módulo de recepção embarcado) e *ADS-B Ground Station* (estação de recepção de solo).

Conforme exposto em [10], basicamente, dois padrões para 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 legados 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

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

utilizado para SSR) [3]. Pelo exposto, e similar ao optado também em [8] e [10], este trabalho dedica seu foco ao padrão de enlace de dados 1090ES.

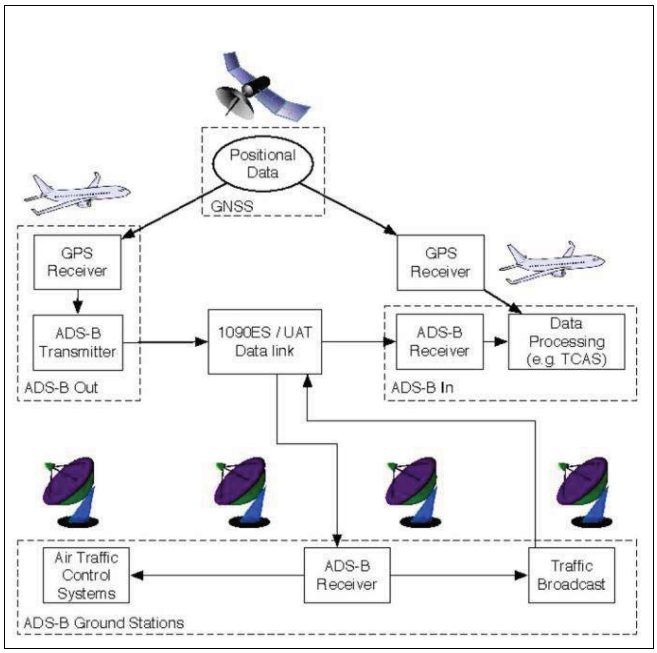

Figura. 1. Representação do Sistema ADS-B [8].

Desta forma, e de acordo com [3] e [10], 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 (também em modo S, para SSR) 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 especificado no modo S, há dois possíveis formatos, quais sejam: curto de 56 *bits* e longo de 112 *bits* [8]. Para o padrão 1090ES destinado ao ADS-B é utilizado formato longo de mensagem, o qual pode ser observado na Fig. 2.

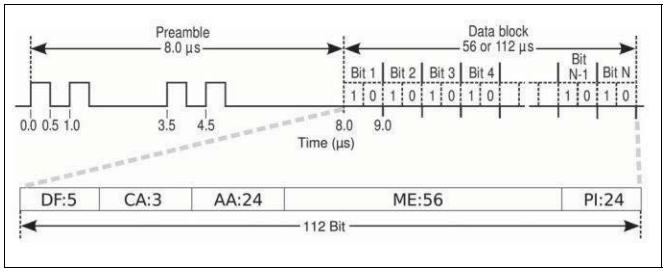

Figura 2. Formato da mensagem 1090ES ADS-B [8].

Para um melhor entendimento da finalidade de cada campo da mensagem 1090ES ADS-B, cabe expor, tal qual presente em [11], que antes do envio do bloco de dados, há um espaço reservado denominado preâmbulo, o qual contém uma sequência especial de bits para sincronização da mensagem (bloco de dados) 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 campo "AA (*Aircraft Address*)" é destinado a alocar o endereço único ICAO, o qual designa um código particular para cada aeronave (transponder), 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 recepção [11]. Cabe ainda expor que o campo "ME (ou *ADS-B data*)" de 56 bits é o único 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. Devido ao exíguo espaço disponível, tal fato limita a integração de possíveis soluções de segurança para o protocolo ADS-B, sobretudo correlatos à verificação de autenticidade do emissor e à privacidade a fim de evitar o acesso e manipulação indevida do conteúdo transmitido.

Também em [8], os autores ainda acrescentam que devido à 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, residem potenciais vulnerabilidades quanto à sobreposição intencional de sinal e à manutenção da integridade da mensagem recebida.

Em relação ao modo de comunicação adotado pelo protocolo ADS-B, qual seja de irrestrita radiodifusão, em [12] depreende-se que devido a toda mensagem ADS-B transmitida ser direcionada para o meio de maneira indistinta quanto ao receptor, qualquer agentes malicioso dentro do espaço de detecção pode recebê-la e decodificar a mensagem em tela visto que a mesma encontra-se em texto claro. Outro fator particular da mensagem ADS-B é que não há confirmação de recebimento pelo receptor ou funcionalidades voltadas a confirmar ou questionar o status da aeronave em longos tempos sem detecção de novas mensagens.

Em resumo, lacunas nos aspectos de segurança afetos ao Sistema ADS-B, como falhas na manutenção da integridade, autenticação, confidencialidade e disponibilidade das mensagens, são especialmente passíveis de serem exploradas por uma miríade de ataques, como será visto na seção a seguir.

III. AMEAÇAS AO SISTEMA ADS-B.

Tal qual exposto por [11], a maioria das vulnerabilidades presentes no Sistema ADS-B residem na própria natureza do protocolo e por ser baseado em aspectos de redes sem fio, sobretudo pela ausência em seu desenvolvimento de soluções criptográficas e de autenticação entre as partes envolvidas no sistema.

Entre as principais ameaças ao ADS-B, destinadas a explorar suas fragilidades como sistema e protocolo, [11] também apresenta a seguinte taxonomia das formas de ataque que entende como fundamentais: interceptação de mensagens; modificação de mensagens recebidas; deleção de mensagens legítimas; injeção de mensagens; interferência sobrepujante de

ISBN: 978-989-54659-0-3

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 [12], este trabalho 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 [11] e [12]:

1) **Interceptação de mensagens**: nessa modalidade, devido à difusão de mensagens ADS-B ocorrerem em larga escala 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. Esta modalidade pode ser o passo inicial para a perpetração de outros ataques. A dificuldade para sua execução pode ser entendida como de baixa complexidade, sobretudo pela fácil disponibilidade de dispositivos e conhecimento (por exemplo, via tutoriais e ferramentas disponibilizados em plataformas *web* de interesse como *FlightRadar24.com* e *OpenSkyNetwork.org)*.

2) **Interferência ou sobreposição intencional de sinal (*jamming*) contra estações de solo**: ao proceder a uma interferência intencional de sinal contra uma estação de solo de recepção de mensagens ADS-B, um eventual atacante objetiva impedir que toda e qualquer mensagem enviada seja recebida pela referida estação. Tal ataque foca na degradação parcial ou total do canal de recepção (no caso do sistema ADS-B a frequência de 1090 MHz), objetivando a perda de consciência situacional dos operadores de órgãos ATC. A efetividade do ataque correlaciona-se à potência e diretividade da emissão do sinal, como também a proximidade do atacante da estação-alvo. Desta forma, a dificuldade do ataque pode ser mensurada como de baixa complexidade, pois além das características expostas, atualmente há disponibilidade de ferramentas de baixo custo para o referido fim, tal qual exposto em [13].

3) **Interferência ou sobreposição intencional de sinal (*jamming*) contra aeronaves**: esta modalidade de ataque se vale da mesma técnica empregada contra estações de solo, no entanto esta última é focada em degradar a recepção ADS-B em aeronaves. Seu objetivo principal é causar perda de consciência situacional da tripulação sob influência do referido ataque, sobretudo nas fases de decolagem e aproximação para pouso. Há, ainda que remota, a possibilidade de execução do ataque dentro da própria aeronave-alvo. A dificuldade deste ataque é classificada em média complexidade devido à limitação em se ganhar acesso próximo às aeronaves no pátio de manobras em solo ou em voo.

4) **Injeção de mensagens modificadas ou ilegítimas contra estações de solo**: essa ameaça tem o fim de injetar mensagens ADS-B modificadas ou falsas em estações de solo ATC. No entanto, para executar tal ataque é necessário possuir conhecimento detalhado sobre o protocolo para modificar as mensagens 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*). Sendo assim, a dificuldade de tal ataque pode ser definida como de alta complexidade.

5) **Injeção de mensagens modificadas ou ilegítimas contra aeronaves**: A configuração deste ataque se assemelha à modalidade anterior. Porém, como não há previsão de correlação ou fusão de dados de diferentes fontes (como dados de plano de voo, leitura de sistemas radares, etc.) com dados advindos do 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. Ataque entendido como de média complexidade.

6) **Injeção de múltiplas mensagens (*flooding*) modificadas ou ilegítimas contra estações de solo:** Como também descrito em [3], este 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. Este ataque é definido como de alta complexidade.

7) **Injeção de múltiplas mensagens (*flooding*) modificadas ou ilegítimas contra aeronaves**: Este 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. A dificuldade de realizar esse ataque é entendida como sendo de média complexidade.

As modalidades listadas acima comporão o rol de ameaças a ser objeto de análise de segurança por meio do método de Gerenciamento de Risco à Segurança Operacional – GRSO, conforme será visto na sequência deste trabalho.

IV. GERENCIAMENTO DE RISCO À SEGURANÇA OPERACIONAL (GRSO)

Tal qual depreendido de [9], 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

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3

processos necessários à elevação do nível da segurança operacional mundial. Ainda conforme em [9]:

> 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).

Em [14], 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, do termo em inglês, *Air Navigation Services*), 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.

Novamente em [9], observa-se 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 Fig. 3, são apresentados mais detalhes sobre cada fase do GRSO.

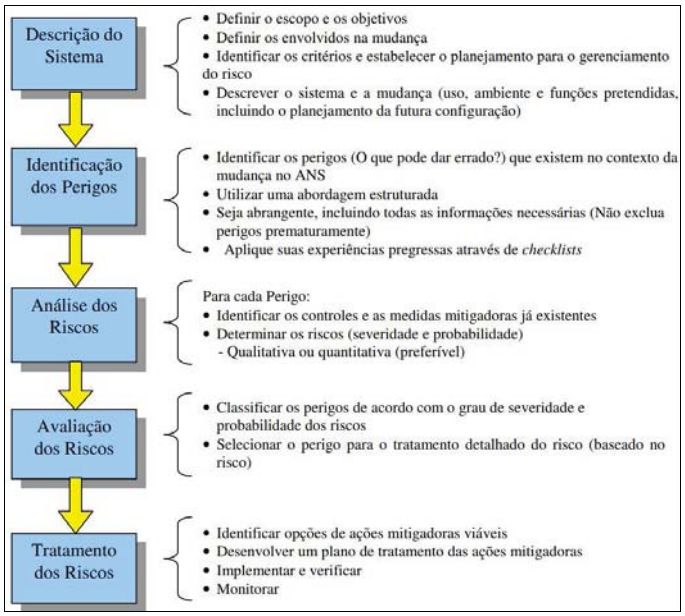

Figura. 3. Fases do Gerenciamento de Risco à Segurança Operacional [9].

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, e o segundo aspecto concerne ao correto entendimento conceitual do que vem a ser risco, probabilidade e severidade. Em [14], tais conceitos são assim definidos:

- Risco: é a avaliação das consequências potenciais de um perigo, expresso em termos de probabilidade e severidade, tomando como referência o pior cenário possível.
- Probabilidade: é a mensuração em termos qualitativos e quantitativos, da possibilidade de uma situação de perigo ocorrer.
- Severidade: esta baseada nas consequências possíveis de uma situação de perigo à segurança operacional, tomando como referência a pior condição possível.

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. 4. Matriz de Avaliação de Riscos GRSO [9].

Na Fig. 4, 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.

V. Análise do Sistema ADS-B por Meio do Método GRSO

Conforme exposto na seção anterior e reforçado também em [9] e [16], o GRSO é destinado, sobretudo, a mudanças nos serviços de navegação aérea do SISCEAB. Sendo assim, entendemos que a aplicação de tal processo de análise de riscos mostra-se oportuno para identificar, avaliar, classificar e priorizar o tratamento dos riscos à incipiente implantação do ADS-B no cenário brasileiro, tal qual previsto na concepção operacional ATM Nacional, detalhado em [5].

Para que a narrativa mantenha-se objetiva, e ao depreendermos que as fases de Descrição do Sistema e Identificação dos Perigos, foram ainda que de maneira sucinta e parcial descritas nas seções II e III, respectivamente, na sequência serão apresentadas as fases de Análise, Avaliação e Tratamento dos Riscos, também do processo GRSO com foco no Sistema ADS-B.

A. Análise dos Riscos

Nesta fase, torna-se necessário identificar os controles e as medidas mitigadoras já existentes para cada perigo, assim como os riscos envolvidos [9]. Logo, para cada perigo já identificado para o Sistema ADS-B, os seguintes controles, ações mitigadoras e grau de probabilidade e severidade foram assim atribuídos:

1) **Interceptação de mensagens (IM):** pode ser entendido como ações mitigadoras, tal qual exposto em [10], a

ISBN: 978-989-54659-0-3

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. Já o grau de severidade do risco pode ser entedida como insignificante e a probabilidade de ocorrência frequente.

2) **Interferência ou sobreposição intencional de sinal contra estações de solo (ISE):** pela natureza do ataque, reside dificuldade em definir controles ou ações mitigadoras efetivas, sobretudo se o atacante estiver próximo ou possuir robustos equipamentos. Uma solução possível seria a adoção de saltos de frequência, ainda que a implementação seja de alta complexidade. 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 decolagem ou em procedimento de descida, bem como em voo por instrumentos. Soluções baseadas em enlace de dados diretos e dedicados entre outras aeronaves ou estações de solo, inclusive baseada em fonia, podem ser eficazes para mitigar a chance de acidente ou incidente aeronáutico. O grau de severidade é entedido como catastrófico e remota a probabilidade de ocorrência.

4) **Injeção de mensagens modificadas ou ilegítimas contra estações de solo (IME):** entre alguns controles e ações mitigadoras já existentes e factíveis situam-se a fusão de dados e leituras de outros equipamentos de vigilância aérea (radares, multilateração, confirmação via fonia, etc) e a filtragem estatistica das leituras pelo método Kalman [10]. O grau de severidade pode ser entedido como maior e a probabilidade de ocorrência como remota.

5) **Injeção de mensagens modificadas ou ilegítimas contra aeronaves (IMA):** Como os controles e ações mitigadoras hoje existentes para inibir a injeção de mensagens arbitrárias ou ilegítimas ADS-B são implementadas principalmente para estações de solo, neste caso soluções baseadas em soluções criptográficas (baseada em chaves públicas) para autenticação ou na filtragem estatistica das leituras pelo método Kalman para estimar localizações podem ser aplicáveis, ainda que com considerável custo de implantação e processamento devido as peculiaridades da plataforma área. O grau de severidade é entedido como perigoso e a probabilidade de ocorrência como remota.

6) **Injeção de múltiplas mensagens modificadas ou ilegítimas contra estações de solo (IMME):** De maneira similar à injeção individual de mensagens ADS-B, os controles e ações mitigadoras consistem nas mesmas soluções apontadas. Quanto ao grau de severidade pode ser entedido como maior e a probabilidade de ocorrência como remota.

7) **Injeção de múltiplas mensagens modificadas ou ilegítimas contra aeronaves (IMMA):** Nesse caso, controle ou ações mitigadoras contra ataques similares a estações de solo não mostram-se adequadamente factiveis e efetivos. No entanto, solução baseada em saltos de frequência pode se mostrar promissora. O grau de severidade é entedido como catastrófico e a probabilidade de ocorrência como remota.

Quanto ao grau de severidade e probabilidade de ocorrência atribuída para as ameaças listadas, a base conceitual qualitativa para a gradação de ambos os aspectos foi extraída de [14] e com o também depreendido em [9]. Também é relevante expor que as opções de controles e ações mitigadoras apresentadas não se encerram em um rol exaustivo de soluções possíveis; para aprofundamento deve-se acessar [6], [8] e [10].

B. Avaliação dos Riscos

Tal qual presente em [9], nesta 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. É oportuna 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					IM
OCASIONAL					
REMOTO	ISA, IMMA	ISE, IMA	IME, IMME		
IMPROVÁVEL					
EXTREMAMENTE IMPROVÁVEL					

Figura. 5. Matriz de Avaliação de Riscos para o Sistema ADS-B.

Na Fig. 5, 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 e IMMA (Alto Risco – não tolerável); ISE, IMA, IME, IMME e IM (Médio Risco – tolerável). A ameaça IM pode também ser classificada como de Baixo Risco, e assim aceitável, devido à natureza indireta e não invasiva de seus efeitos para o normal funcionamento e segurança do SISCEAB.

C. Tratamento dos Riscos

Sempre que os riscos não puderem ser eliminados por completo, devem ser reduzidos a fim de minimizar os efeitos de sua ocorrência. Recomendação em [14] afirma 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

ISBN: 978-989-54659-0-3

revestido de constante acompanhamento do risco aceito para que não incorra em danos à segurança operacional.

No caso em análise, os riscos ao Sistema ADS-B entendidos como Risco Alto (ISA e IMMA) residem em riscos inaceitáveis. Ou seja, que as mudanças ou implementações concernentes ao referido Sistema 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 as ameaças entendidas como de Médio Risco (ISE, IMA, 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 de segurança operacional para que não incorram em danos para a consciência situacional e processo decisório dos envolvidos no SISCEAB, em especial aos Controladores de Tráfego Aéreo.

VI. CONCLUSÕES

Ainda que o Sistema ADS-B mereça todo destaque por suas capacidades inovadoras em prover cobertura, atualização acima da média e economicidade, questionamentos sobre os aspectos de segurança presentes em seu cerne não devem ser silenciados sem antes do devido escrutínio. Como apresentado, este trabalho 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.

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

Foram encontrados riscos inaceitáveis, tais como a interferência ou sobreposição intencional de sinal e a injeção de múltiplas mensagens modificadas ou ilegítimas, ambas contra aeronaves. Esses riscos mostram-se sensíveis ao passo que podem ser diretamente danosos a um elemento essencial na "engrenagem" do tráfego aéreo qual seja as aeronaves, não só em perdas materiais, mas sobretudo humano; e indiretamente quando incorre em perda de consciência situacional ou aumento de carga de trabalho e esforço para controladores devido a coordenação extra em caso de ataque.

Em contrapartida, os outros riscos analisados e classificados como de média (ou baixa, no caso da IM) 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.

Como trabalho futuro, destaca-se a necessidade da realização de pesquisas e avaliações operacionais em campo para verificar a suscetibilidade a ataques (sobretudo os apresentados neste trabalho e os resultados do processo GRSO realizado) dos equipamentos a serem utilizados para futura implantação em larga escala do ADS-B no âmbito do SISCEAB.

AGRADECIMENTOS

Os autores agradecem ao Programa de Pós-Graduação Profissional em Engenharia Elétrica (PPEE); Coordenação Brasileira de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), bolsas 23038.007604 / 2014-69 FORTE e 88887.144009 / 2017-00 PROBRAL; Conselho Nacional Brasileiro de Desenvolvimento Científico e Tecnológico (CNPq), Bolsas 303343 / 2017-6, 312180 / 2019-5 PQ-2, BRICS2017-591 LargEWiN e 465741 / 2014-2 INCT sobre segurança cibernética; A Fundação de Apoio à Pesquisa do Distrito Federal (FAP-DF), doações 0193.001366 / 2016 UIoT e 0193.001365 / 2016 SSDDC; o laboratório LATITUDE / UnB (Grant 23106.099441 / 2016-43 SDN); o Ministério da Economia (TEDs DIPLA 005/2016 e ENAP 083/2016); o Gabinete de Segurança Institucional da Presidência da República (TED ABIN 002/2017); o Conselho Administrativo de Defesa Econômica (TED CADE 08700.000047 / 2019-14); e o Procurador Geral da República (TED AGU 697.935 / 2019).

REFERÊNCIAS BIBLIOGRÁFICAS

[1] STROHMEIER, Martin. **Security in next generation air traffic communication networks**. 2016. Tese de Doutorado. University of Oxford.

[2] ALI, Busyairah Syd et al. A safety assessment framework for the Automatic Dependent Surveillance Broadcast (ADS-B) system. **Safety science**, v. 78, p. 91-100, 2015.

[3] SCHÄFER, Matthias; LENDERS, Vincent; MARTINOVIC, Ivan. Experimental analysis of attacks on next generation air traffic communication. In: **International Conference on Applied Cryptography and Network Security**. Springer, Berlin, Heidelberg, 2013. p. 253-271.

[4] MARINHO, Daniel. *Website* DECEA. **Comitiva oficializa operação ADS-B na Bacia de Campos**. 2018. Disponível em: < https://www.decea.gov.br/?i=midia-e-informacao&p=pg_noticia&materia=comitiva-oficializa-obrigatoriedade-do-uso-do-ads-b-na-bacia-de-campos>. Acesso em: 22 out. 2019.

[5] BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. **Diretriz do Comando da Aeronáutica (DCA) 351-2**: Concepção Operacional ATM Nacional, 2011. Disponível em: < https://publicacoes.decea.gov.br/?i=publicacao&id=3678>. Acesso em 19 nov. 2019.

[6] STROHMEIER, Martin et al. On perception and reality in wireless air traffic communication security. **IEEE transactions on intelligent transportation systems**, v. 18, n. 6, p. 1338-1357, 2017 .

[7] COSTIN, Andrei; FRANCILLON, Aurélien. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. **Black Hat USA**, p. 1-12, 2012.

[8] STROHMEIER, Martin; LENDERS, Vincent; MARTINOVIC, Ivan. On the security of the automatic dependent surveillance-broadcast protocol. **IEEE Communications Surveys & Tutorials**, v. 17, n. 2, p. 1066-1087, 2014.

[9] BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. **Manual do Comando da Aeronáutica (MCA) 63-14**: Manual de Gerenciamento do Risco à Segurança Operacional no SISCEAB, 2012. Disponível em: <http://publicacoes.decea.gov.br/?i=publicacao&id=3736>. Acesso em 19 nov. 2019.

[10] STROHMEIER, Martin et al. Realities and challenges of nextgen air traffic management: the case of ADS-B. **IEEE Communications Magazine**, v. 52, n. 5, p. 111-118, 2014.

[11] MANESH, Mohsen Riahi; KAABOUCH, Naima. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. **International Journal of Critical Infrastructure Protection**, v. 19, p. 16-31, 2017.

ISBN: 978-989-54659-0-3

[12] MCCALLIE, Donald; BUTTS, Jonathan; MILLS, Robert. Security analysis of the ADS-B implementation in the next generation air transportation system. **International Journal of Critical Infrastructure Protection**, v. 4, n. 2, p. 78-87, 2011.

[13] LEONARDI, Mauro; PIRACCI, Emilio; GALATI, Gaspare. ADS-B vulnerability to low cost jammers: Risk assessment and possible solutions. In: **2014 Tyrrhenian International Workshop on Digital Communications-Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV)**. IEEE, 2014. p. 41-46.

[14] BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. **Instrução do Comando da Aeronáutica (ICA) 63-26**: Gerenciamento do Risco à Segurança Operacional no SISCEAB, 2010. Disponível em: <https://publicacoes.decea.gov.br/?i=publicacao&id=3491>. Acesso em 19 fev. 2020. 1,3, 7, 13

2020 15th Iberian Conference on Information Systems and Technologies (CISTI)
24 – 27 June 2020, Seville, Spain
ISBN: 978-989-54659-0-3