RISCOS

territorium 29 (I), 2022, 149-160
journal homepage: https://territorium.riscos.pt/numeros-publicados/
DOI: https://doi.org/10.14195/1647-7723_29-1_13
Nota / Note

CIBERSEGURANÇA NA AVIAÇÃO CIVIL BRASILEIRA (2016 – 2019)*

CYBERSECURITY IN BRAZILIAN CIVIL AVIATION (2016-2019)

Gisela Biacchi Emanuelli
Agência Nacional de Aviação Civil (Brasil)
ORCID 0000-0001-5793-753X giselabiacchi@gmail.com

RESUMO

Este texto tem o objetivo de constatar ações de segurança cibernética na proteção da aviação civil brasileira desde o encaminhamento da Resolução A39-19 da Organização da Aviação Civil Internacional (OACI) em 30 de maio de 2016 até 2019. Vale-se de estudo de caso e análise bibliográfica, documental e legislativa. Como resultado da pesquisa, constata-se o equilíbrio entre as políticas recomendadas pela OACI e as medidas conduzidas pelo Brasil por meio do Gabinete de Segurança Institucional (GSI) e da Agência Nacional de Aviação Civil (ANAC). Além disso, observa-se que o Brasil se antecipou às recomendações internacionais ao elaborar o Planejamento Estratégico 2015-2019 da ANAC. Por fim, conclui-se que a segurança cibernética será uma realidade em permanente evolução, dependente de ações concertadas de todos os atores do ecossistema da aviação civil e do poder público em direção ao cumprimento das orientações da Política e da Estratégia Nacional de Defesa e da segurança do Estado brasileiro.

Palavras-chave: Ataques cibernéticos, interferência ilícita, segurança na aviação, OACI.

ABSTRACT

This text aims to support cybersecurity actions in the protection of Brazilian civil aviation since the submission of Resolution A39-19 of the International Civil Aviation Organization (ICAO) on May 30, 2016, until 2019. It uses a case study and a literature, documentary, and legislative analysis. As a result of the analysis, there is a balance between the policies recommended by ICAO and the measures adopted by Brazil through the Institutional Security Office (GSI) and the National Civil Aviation Agency (ANAC). Also, it is worthy of note that Brazil anticipated international recommendations when preparing the ANAC Strategic Planning 2015-2019 document. Finally, we conclude that cybersecurity will be a permanently evolving situation, dependent on concerted actions by all the actors in the civil aviation ecosystem and the public authorities towards complying with the guidelines of the National Defence Policy and Strategy and the security of the Brazilian State.

Keywords: Cyber-attacks, unlawful interference, aviation security, ICAO.

* *O texto desta nota foi apresentado em conclusão do Curso de Altos Estudos em Defesa (CAED) da Escola Superior de Guerra (ESG), campus Brasília, Brasil, 2019, tendo sido submetido em 02-03-2020, sujeito a revisão por pares a 24-03-2020 e aceite para publicação em 19-07-2020.*

Introdução

O transporte aéreo civil brasileiro apresenta números robustos. Entre 2002 e 2016 as companhias nacionais transportaram um bilhão de passageiros. Em apenas um dia, o Brasil leva, de um lugar ao outro, 263 mil pessoas. É a segunda nação em número de aeroportos, com 2.463 aeródromos registrados na Agência Nacional de Aviação Civil (ANAC). A categoria gera 6,4 milhões de empregos no País, de acordo com os dados da Associação Brasileira das Empresas Aéreas (ABEAR, 2019).

Em 1947, quando foi fundada a Organização da Aviação Civil Internacional (OACI), os objetivos declarados pelos países-membros visavam evitar abusos na aviação que pudessem atentar contra a segurança ou a paz mundial, estabelecer uma base de igualdade de oportunidades no serviço do transporte aéreo e propiciar a exploração eficaz e econômica do setor (BRASIL, 1946). Na realidade, é possível entender que os países, então, voltavam-se ao mercado competitivo que alvorecia.

Atualmente, novos conteúdos desafiam a atividade aérea em um contexto de envergadura global em que as operações se entrelaçam, sobretudo, em ambiente cibernético. No portal da OACI estão explicitados seus atuais c*inco* objetivos estratégicos: desenvolvimento econômico, capacidade e eficiência da navegação, segurança operacional, segurança contra atos de interferência ilícita e facilitação e proteção ambiental (ICAO, 2019). Percebe-se que os dois últimos são desdobramentos de um processo evolutivo do setor e da sociedade em si, haja vista que, em 1944 aeroportos não eram percebidos como fontes de disrupção.

Neste trabalho, foca-se na cibersegurança como meio de proteção dessa infraestrutura crítica. Fundamenta-se na Resolução A39-19 da Assembleia da OACI, de maio de 2016, que convoca a comunidade da aviação civil a implementar ações para entender e debelar ameaças cibernéticas contra os sistemas e os dados da aviação civil, impelindo os países a trabalharem colaborativamente no desenvolvimento de um protocolo para enfrentar desafios da cibersegurança (ICAO, 2016).

Alicerça-se também na Política Nacional de Defesa (PND), na medida em que o objetivo nacional de garantir a soberania, o patrimônio nacional e a integridade territorial é ameaçado pelo risco cibernético, atingindo o exercício da autoridade do Estado (BRASIL, 2016a, p. 12). Embasa-se na contribuição para a percepção de um estado de segurança nacional, livre de pressões e ameaças de qualquer natureza, nos termos daquela Política (id., p. 5) e de aprestamento das infraestruturas críticas disponíveis, de acordo com a Ação Estratégica de Defesa de coordenar com órgãos da Administração Pública o atendimento aos requisitos necessários para a otimização da capacidade de mobilização nacional (BRASIL, 2016b, p. 35).

A manutenção de ótimos resultados sobre a segurança no setor é um constante compromisso dos Estados-membro. Ações de detecção e neutralização de atos de interferência ilícita (AVSEC) se sofisticaram desde a criação da OACI e, atualmente, identificar e combater atos cibernéticos de interferência ilícita é o mais novo desafio. Nesse sentido, a Assembleia da OACI elencou onze propósitos contra ameaças cibernéticas que orientam Estados e operadores.

Por isso, o presente estudo justifica-se na medida em que o Brasil é um dos fundadores da OACI, participando ativamente na Organização e sendo eleito sucessivamente para o Grupo I do Conselho da OACI: o Grupo de Importância Principal no transporte aéreo (BRASIL, 2016). Para o triênio 2016-2019 foram eleitos ao citado Grupo, que pertence ao Conselho permanente da OACI, os seguintes países: Alemanha, Austrália, Brasil, Canadá, China, Estados Unidos, França, Itália, Japão, Reino Unido e Rússia. Sobre a pauta da segurança cibernética, o Brasil é membro do grupo de estudos da OACI voltado à cibersegurança, o Grupo de Estudos do Secretariado sobre Cibersegurança.

O objetivo geral deste trabalho é averiguar ações de cibersegurança na proteção da aviação civil brasileira desde a publicação daquela Resolução.

Como hipótese, assume-se que as orientações da OACI contribuíram para o Brasil adotar medidas de cibersegurança na aviação civil entre os anos de 2016 e 2019, tendo em conta a sua natureza jurídica de *soft law*. Segundo Portela (2011, p. 83-4), atos de organizações internacionais não obrigatórios oferecem soluções rápidas para problemas comuns entre sujeitos de Direito Internacional e, embora não tenham a força cogente de uma norma, enunciados de *soft law* são cumpridos em nome do interesse conjunto de harmonizar dado tema.

Trata-se de um estudo de caso, que se vale de pesquisa bibliográfica, documental e legislativa com o objetivo de averiguar a promoção de ações no Brasil posteriores à citada Resolução. A revisão de literatura indica que o assunto tem levado estudiosos a refletirem sobre segurança cibernética na aviação civil, entretanto, é um campo relativamente novo.

O período exploratório concentra-se entre os anos de 2016, quando foi editada a Resolução, e 2019, período de conclusão da fase de coleta de material para a pesquisa realizada.

Para melhor compreensão do assunto, dividiu-se o trabalho em três partes, conforme os objetivos específicos. Na primeira, buscar-se-á contextualizar a criação da OACI, destacar seus objetivos originais e esclarecer o elemento marcante do tópico que é extremar os conceitos de segurança contra atos de interferência ilícita (*security*) e atos contra a segurança operacional (*safety*). Na segunda parte, serão abordadas a segurança contra atos ilícitos e,

especialmente, a política de cibersegurança conduzida pela OACI. Ao final, discorre-se sobre políticas adotadas pelo Brasil para o enfrentamento do risco cibernético na aviação civil brasileira, desencadeadas pela Resolução da OACI em consonância com o objetivo de segurança e defesa nacionais.

A Convenção de Chicago e o tema da segurança

A OACI é uma agência especializada da Organização das Nações Unidas (ONU), criada sob os escombros da Segunda Guerra Mundial.

No portal da Organização lê-se que a OACI nasceu pela Convenção de Chicago em 1944, quando delegados de 54 países estiveram reunidos em uma conferência, na qual 32 — entre eles Brasil — firmaram o compromisso de assegurar a cooperação e o mais alto grau de uniformidade regulatória e organizacional em assuntos de aviação civil. Segundo o que consta no sítio, o resultado mais significativo da Conferência foi técnico:

> "[…] *porque a Conferência lançou sua fundação em um conjunto de regras e regulamentos referentes à navegação aérea como um todo, o que trouxe à segurança em voo um grande passo adiante e pavimentou o caminho para a adoção de um sistema comum de navegação aérea para todo o mundo*" (ICAO, ..., 2019, tradução nossa).

Esse avanço técnico abrangeu treinamento de pessoal, sistema de comunicação, regras e controle de tráfego, certificações em aeronavegabilidade e registro de operadores, cartas e meteorologia (ibid.). As questões de segurança à época referiam-se à operação aérea e eram dirigidas às certificações de equipamentos e pessoal. Objetivava a manutenção de poder soberano e ao cumprimento de padronizações operacionais que permitissem a construção da rede aérea internacional que se estruturava. O término da Segunda Grande Guerra pressionou o mercado a absorver os excedentes de aviões sem emprego e a usar a infraestrutura estabelecida para as operações de beligerância (Portilho, 2015, p. 23).

Nesse cenário, o conceito de segurança pretendido para a aviação civil estava significativamente voltado para o que se considera *Safety*, isto é, o aspecto de segurança que visa mitigar acidentes e incidentes aeronáuticos. É reconhecidamente assim entendido quando relacionado ao gerenciamento da segurança operacional "*fruto de uma cultura de segurança que é continuamente formada dentro de uma organização em que todos os riscos às operações são conhecidos, avaliados e devidamente reduzidos*" (BRASIL, [200-]a). Para a ANAC a segurança operacional é o "*estado no qual o risco de lesões a pessoas ou danos a bens se reduzem e se mantêm em um nível aceitável ou abaixo deste, por meio de um processo contínuo de identificação de perigos e gerenciamento de riscos*" (BRASIL, [200-]b).

No que concerne à *Safety*, a Convenção de Chicago recebeu o Anexo 19 adotado em 2013, e sua segunda e atual reedição ultimou-se em 2016. Esse dado reforça que as questões de *Safety* representam um componente de base da OACI com presença desde a origem e merecendo atualização tardia.

Contudo, a ideia de segurança na aviação se desdobra ainda no que se denomina *Security*. Nesse caso, segurança tem a ver com medidas contra atos de interferência ilícita ou *aviation security* (AVSEC). Esse entendimento precisou ser incorporado à convenção da OACI no "calor" da onda terrorista das décadas de 1960-70.

O tratado internacional de 1944 não contemplou segurança contra atos de interferência ilícita na oportunidade da criação da OACI. Esse assunto seria objeto de um anexo à convenção em 1975, quando a Assembleia aprovou o *Annex 17 to the Convention on International Civil Aviation. Security, Safeguarding International Civil Aviation Against Acts of Unlawful Interference*.

O documento sofreu dez reedições. Somente a partir da nona, em 2011, houve menção a ameaças cibernéticas.

Diante disso, constata-se que AVSEC tornou-se, com o tempo, assunto prioritário e recorrente, que demanda renovadas inserções no Anexo 17 da Convenção, dada a evolução das possíveis ameaças.

Segundo as definições desse documento, entende-se por *Security* a salvaguarda da aviação civil contra interferências ilícitas, obtida pela combinação de medidas e recursos materiais e humanos (ICAO, 2017, p. 16). Essas interferências são atos consumados ou tentados que põem em risco a segurança da aviação civil, tais como, apreensão ilegal de uma aeronave, destruição de uma aeronave em serviço, sequestro a bordo de aeronave ou de aeródromo, invasão a bordo de aeronave ou de aeródromo, uso de aeronave em serviço para causar morte, lesões graves e danos ao patrimônio ou ao meio ambiente, comunicação de falsa informação que ameace a segurança de uma aeronave em voo ou aterrissada, dos passageiros, da tripulação, do pessoal de pista ou do público em geral no sítio aeroportuário (id., p. 15, tradução nossa).

Diante desse rol não exaustivo de ameaças, em uma interpretação *lato sensu*, a interferência cibernética pode alcançar diversos elementos no âmbito da aviação civil, podendo redundar em ameaça à segurança e tipificar um ato de interferência ilícita.

Para cumprir o princípio de que todo Estado tem o objetivo primordial de garantir a segurança do passageiro e de todos os envolvidos na operação, seja a bordo, seja no pátio (id., p. 19), a OACI recomendou que se estabelecessem e implementassem regulação, práticas e procedimentos para salvaguarda da aviação civil capazes de responder, de imediato, a qualquer ameaça iminente à segurança (*ibid.*).

Nesse aspecto, a Organização aconselha, no capítulo 4.9 *Measures relating to cyber threats* do Anexo 17, que os Estados assegurem a operadores e entidades do setor aéreo a possibilidade de identificarem as informações críticas e os sistemas de comunicação e de dados usados na aviação civil e, conforme a avaliação de risco, desenvolver e efetivar medidas apropriadas para protegê-los contra interferência ilícita (id., p. 29).

Em consequência, recomenda a OACI que essa proteção inclua segurança em projetos, segurança na cadeia de fornecimento de suprimentos, proteção e limitação de qualquer capacidade de acesso remoto e, de acordo com a avaliação das autoridades nacionais, proteção a qualquer outra estrutura crítica que possa sofrer risco (*ibid.*).

A preocupação do setor em proteger infraestruturas críticas contra atos de interferência ilícita cibernéticos vem crescendo e provocando debates sobre possíveis ações frente à perspectiva de ameaças desconhecidas perpetradas no ambiente da rede mundial de computadores. No próximo item será abordada a construção de rumos a partir do conceito de segurança e de segurança contra atos ilícitos, para a adoção de medidas de cibersegurança.

Segurança, cibersegurança e direcionamentos iniciais

Na visão de Buzan (2012, p. 37) segurança é um conceito hifenizado por vir acompanhado de adjetivações. É conceito que transbordou o setor militar e alcançou aspectos sociais, econômicos, ambientais, de saúde, desenvolvimento e gênero (id., p. 39). Por fim, segurança para Buzan, está inextrincavelmente ligada à dinâmica de ameaças, perigos e urgências.

Em sua obra, o professor britânico refere que os estudiosos lograram ampliar o conceito de segurança internacional com o passar do tempo (id. *passim*).

Nesse sentido, a Assembleia Geral da ONU aprovou a Resolução n.º 44/118 de 15 de novembro de 1989, que trata dos avanços científicos e tecnológicos e sua repercussão na segurança internacional. Esse recorte do contexto de então, expõe o alargamento do espectro da segurança. O documento ressalta a preocupação das nações com o avanço tecnológico como uma categoria nova do sistema armamentista, causando efeito negativo no ambiente de segurança e que os países deveriam manter cuidadoso monitoramento sobre essas melhorias.

A Resolução estabeleceu o programa "Avanços científicos e tecnológicos e sua repercussão na segurança internacional", entretanto, embora essa ação exortasse o uso pacífico da tecnologia, dá indícios de que a humanidade se voltava para uma nova possível ameaça: a tecnológica. É sabido que o mundo está conectado em rede. Castells (2006) alega que "as redes interativas de computadores estão crescendo exponencialmente, criando novas formas e canais de comunicação". Para o estudioso:

> "*Simultaneamente, as atividades criminosas e organizações ao estilo da máfia de todo o mundo também se tornaram globais e informacionais propiciando os meios para o encorajamento de hiperatividade mental e desejo proibido juntamente com toda e qualquer forma de negócio ilícito procurado pelas nossas sociedades, de armas sofisticadas a carne humana*" (Castells, 2006, p. 40).

Ao que se percebe, as sugestões elencadas pela ONU, com alguma adaptação, podem ser trazidas para a realidade do século XXI, na qual certas ameaças são efetivamente comuns e não tradicionais em um contexto difuso, como o terrorismo e os ataques cibernéticos.

O espaço cibernético também condiciona o setor aéreo. É de conhecimento que compras de passagens e reservas de assentos, eleição de serviços acessórios e procedimento de embarque, por exemplo, são realizados por meio da rede mundial de computadores. Além disso, os sistemas operacionais e de segurança estão impactados pela cibernética. Ora, assim como a *web*, esse setor funciona em uma rede mundial de operações e conexões de voos, criando interdependência de magnitude global.

Considerando a tessitura que condiciona esse campo, qualquer perturbação contra a segurança afeta o desfecho de uma operação. Por esse motivo, a vulnerabilidade no sistema global da aviação tornou-se foco de atenção da OACI, sendo a cibersegurança a mais nova fronteira de enfrentamento dos países partes.

Cibersegurança na aviação civil envolve a proteção, a prevenção, a detecção e a resposta a ataques cibernéticos contra a infraestrutura crítica do sistema de aviação civil. De acordo com a *European Authority Aviation Safety* (EASA):

> "*No contexto da certificação de aeronaves, a segurança cibernética é comumente entendida como a proteção dos sistemas de informação da aviação contra interações eletrônicas intencionais não autorizadas (IUEI) e os meios para mitigar suas consequências na segurança. Os sistemas e peças de aeronaves estão cada vez mais conectados e essas interconexões são suscetíveis a ameaças à segurança. Essas ameaças têm o potencial de afetar a aeronavegabilidade de uma aeronave devido ao acesso, uso, divulgação, negação, interrupção, modificação ou destruição não autorizada de informações eletrônicas ou interfaces do sistema eletrônico da aeronave. As ameaças mencionadas não incluem ataques físicos*" (EASA, 2019, p. 4, tradução nossa).

Como descrito no Livro Verde: Segurança Cibernética no Brasil, segurança cibernética é um conceito em construção, porém entende-se que "*compreende aspectos e atitudes tanto de prevenção quanto de repressão*" (BRASIL, 2010, p. 19). De início, seria "*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*" (ibid.). Conclui-se que "*a proteção efetiva das infraestruturas críticas requer, comunicação em escala mundial, coordenação e cooperação entre todas as partes interessadas*" (id., p. 20).

Dada essa necessidade envolvendo o contexto internacional, em 2014, a OACI lançou o Plano de Ação em Cibersegurança da Aviação Civil (*Civil Aviation Cybersecurity Action Plan*), no qual os países participantes reconhecem a premência de trabalharem juntos para fortalecer a proteção do sistema contra ataques cibernéticos e unem esforços para se preparar contra os desafios futuros provocados por atos de interferência ilícita cibernéticos (ICAO, 2014, p.1), entre outros compromissos. O documento traça um programa de metas de curto, médio e longo prazos com 11 objetivos a serem atendidos pelos países.

Em 2016, reunido na 39ª sessão da Assembleia da OACI, o Conselho da Organização propôs o assunto da cibersegurança na aviação civil. Então, aos países foram convidados a adotar a minuta da Resolução que endereça a Cibersegurança na Aviação Civil (ICAO, 2016, p.1.) sobre política da segurança da aviação, com o fundamento de que a proteção e a resiliência dos sistemas afetos à aviação civil somente avançarão se houver trabalho colaborativo, harmônico e global.

A Resolução, por sua vez, salienta que ameaças impostas por incidentes cibernéticos evoluem rápida e continuamente, perpetradores de ameaças estão motivados a causar danos aos negócios, furtar dados e informações por propósitos políticos, financeiros, entre outros. Ademais, destaca que ameaças podem facilmente evoluir para risco concreto contra o sistema crítico da aviação civil no mundo (ibid, p. 3). Diante disso, encoraja os estados e a indústria a adotar as seguintes medidas de segurança cibernética:

a) Identificar ameaças e riscos cibernéticos à operação da aviação civil e seu sistema crítico, bem como suas consequências;

b) Definir as responsabilidades das agências e da indústria;

c) Encorajar o desenvolvimento de um entendimento comum sobre riscos e ameaças cibernéticas e um critério comum que determine a criticidade de ativos e sistemas que precisam ser protegidos;

d) Alentar a coordenação entre governo e indústria em relação às estratégias, políticas e planos e de cibersegurança, assim como, a troca de informações para identificar vulnerabilidades críticas;

e) Desenvolver parceria e mecanismos entre governo e indústria, nacional e internacionalmente, para troca de informação sobre risco cibernético;

f) Adotar com base em entendimento comum, abordagem resiliente e baseada em risco para proteger os sistemas críticos da aviação por meio de implementação de sistema de administração de cibersegurança;

g) Incentivar robusta cultura em cibersegurança nas agências reguladoras e no setor de aviação;

h) Estabelecer consequências legais contra a prática atividades que explorem vulnerabilidades cibernéticas que comprometam a segurança da aviação;

i) Promover o desenvolvimento e a adoção de padrões internacionais, estratégias e boas práticas para a proteção de informações críticas e sistemas de comunicação usados na aviação civil contra a interferência que possa ameaçar a segurança do setor;

j) Estabelecer políticas e destinar recursos para garantir que os sistemas críticos da aviação civil: tenham arquitetura segura, sejam resilientes, adotem métodos de transferência de dados seguros, certifiquem integridade e confidencialidade, afiancem monitoramento de sistema e detecção de incidentes e desencadeiem análise forense desses incidentes; e

k) Colaborar com o desenvolvimento da estrutura de cibersegurança da OACI, numa abordagem horizontal e transversal envolvendo navegação aérea, comunicação, vigilância, operação aérea, aeronavegabilidade e outras disciplinas. (id., p. 3 - 4, tradução nossa).

No ano seguinte, os países reuniram-se em Dubai para participar de uma cúpula sobre cibersegurança na aviação civil. O encontro resultou na Declaração sobre Cibersegurança na Aviação Civil (*Declaration on Cybersecurity in Civil Aviantion*), que ratificou os termos da Resolução A39-19 e enfatizou a importância e a urgência em proteger a infraestrutura crítica e os dados da aviação civil contra ciberameaças (ICAO, 2017, p. 1).

No ano de 2018, em Bucareste, a Organização reconheceu ser necessário desenvolver uma estrutura de cibersegurança a mais ampla possível, incentivando a cooperação regional para definir estratégias comuns, expedindo recomendações aos Estados e à indústria (ICAO, 2018, p. 2). Em novembro deste mesmo ano, ocorreu a segunda conferência de alto nível da OACI sobre segurança da aviação (*Second High-Level Conference on Aviation Security* - HLCAS/2). Os países concordaram que esse é assunto a ser tratado em nível doméstico e em escala mundial, porque ataques cibernéticos podem acometer o controle do tráfego, as aeronaves e os aeroportos (id., p. 15).

Para tanto, a OACI incentivou o desenvolvimento de uma Estratégia Global de Cibersegurança e a manutenção do painel de discussão sobre a matéria. Em consequência, instituiu-se o Grupo de Estudos do Secretariado sobre Cibersegurança (SSGC) dedicado a estabelecer ações a serem adotadas de forma transversal, horizontal e colaborativa pelos Estados e pelas partes interessadas do sistema aéreo, para se contrapor a ameaças cibernéticas (ICAO, ca. 2018).

O SSGC é o ponto focal dos trabalhos desenvolvidos no sistema da OACI, definindo as áreas que devem ser consideradas pelos grupos de trabalho. Além disso, o Grupo ocupa-se de revisar os anexos e consolidar em um só documento padrões e práticas recomendadas (SARPS) sobre cibersegurança existentes. Está, igualmente, imbuído de encorajar o desenvolvimento da parceria entre governos e indústrias, no espaço doméstico e internacional, para a troca sistemática de informações sobre ameaças cibernéticas, incidentes, tendências e esforços de mitigação.

A estrutura do Secretariado compõe-se de representantes de 20 países e 13 organizações internacionais e seu produto mais importante é o desenvolvimento de uma estratégia de cibersegurança global (ICAO, 2019, p. 2).

Ao que se percebe desse resumo histórico, a cibersegurança é assunto relativamente recente sobre o qual a aviação civil começa a se debruçar.

A comunidade internacional entende a importância e premência de se dedicar ao assunto. Um exemplo é a 40ª Assembleia da OACI, realizada entre os dias 24 de setembro a 04 de outubro de 2019, com desdobramentos da Resolução A39-19.

No item 12 da Agenda do Comitê Executivo encontra-se apresentação do Trabalho sobre Estratégia de Cibersegurança da OACI (*Working Paper ICAO Cibersecurity Strategy*) que, em seu anexo, traz uma nova versão da Resolução e encaminha um estudo holístico sobre a estratégia da OACI em cibersegurança, que:

> "[...] *assinala sua urgência e importância, inclui emenda à Resolução A39-19 Endereçando a Cibersegurança na Aviação Civil, apoiando sua implementação pelos Estados Membros. A Estratégia está construída sobre a visão da OACI de uma cibersegurança global – onde o setor da aviação deve ser resiliente a ataques cibernéticos e manter-se globalmente a salvo e confiável, enquanto cresce e inova continuamente. Será necessário apoio por planos de ação para ser desenvolvida com mecanismos apropriados. A Estratégia é o resultado de deliberações do Grupo de Estudos do Secretariado sobre Cibersegurança*" (ICAO, 2019, p. 1, tradução nossa).

De acordo com o documento, a estratégia de cibersegurança está alinhada com os padrões de *safety* e *security* e sublinha a importância de se reconhecer a cibersegurança como um tema transversal que envolve todos os domínios do setor da aviação (id., p. 7). Objetiva a proteção contra ameaças que possam afetar não só a segurança, mas também a confiabilidade no sistema transporte aéreo, a continuidade dos serviços, o reconhecimento pelos Estados da obrigação de garantir segurança frente a ameaças cibernéticas e a coordenação das autoridades de cada Estado para administrar os riscos em cibersegurança (id., p. 2 - 3).

O Anexo ao *Working Paper*, por sua vez, apresenta as emendas às recomendações estabelecidas na Resolução A39-19; defende que as ameaças cibernéticas podem afetar uma gama de áreas, espalhando-se rapidamente e perfilha: "*cibersegurança da aviação civil deve ser harmonizada em nível global, nacional e regional para promover uma coerência global e assegure total interoperabilidade de medidas de proteção e de sistemas de administração de riscos*" (id., p. A-2, tradução nossa).

Outrossim, a questão recebeu contribuições dos participantes da 40.ª Assembleia. Com o prazo até 2 de agosto de 2019 para apresentação de *working papers*, a tabela a seguir mostra a participação nos debates sobre cibersegurança (Tabela I).

Percebe-se que se repetem pedidos de entendimento entre os diversos participantes do sistema, indo ao encontro das ações "c", "d" e "f" previstas na Resolução. No que tange ao Brasil, embora não tenha apresentado proposta sobre cibersegurança para a 40ª Assembleia, a coordenação entre autoridades já acontece e estrutura-se no âmbito da Agência Nacional de Aviação Civil e do Gabinete de Segurança Institucional da Presidência da República (GSI-PR), que congrega os debates em torno da segurança de infraestruturas críticas, como será visto na próxima seção.

Ações autóctones rumo à cibersegurança no setor aéreo

No Brasil, a ANAC é o órgão competente para regular e fiscalizar o setor da aviação civil. Segundo a lei n. 11.182/2005, que criou a Agência, compete a essa autarquia observar e implementar as orientações, diretrizes e políticas estabelecidas pelo governo federal, especialmente no que se refere à representação do Brasil em convenções, acordos, tratados e atos de transporte aéreo internacional com organizações internacionais de aviação civil (art. 3º, I), entre outras atribuições.

Nesse aspecto, padrões e recomendações emanados da OACI e assumidos pelo governo brasileiro são interpretados e normatizados por essa Agência. A adoção de medidas necessárias para a promoção das normas e recomendações internacionais de aviação civil observados

Tabela I - *Working Papers* sobre Cibersegurança para a 40ª Assembleia da OACI.
***Table I -** Cybersecurity Working Papers for the 40th Triennial Assembly.*

Participante	Documento	Síntese da contribuição
Civil Air Navigation Services Organization (CANSO)	A40-WP/172	Criar anexo próprio e painel multidisciplinar para maior eficiência.
International Coordinating Council of Aerospace Industries Associations (ICCAIA)	A40-WP/219	Trabalhar o tema transversalmente com a Indústria e reconhecer a inadequação do SSGC.
Emirados Árabes	A40-WP/221	Adotar mecanismo que abranja todos os domínios da aviação e estrutura multidisciplinar para o tema.
Airport Council International (ACI)	A40-WP/243	Fazer abordagem holística e multidisciplinar, criando painel específico.
França	A40-WP/283	Criar fórum específico com participação todos os domínios, coordenando debates entre Estado e Indústria.
Nova Zelândia	A40-WP/295	Elaborar guia principiológico para evitar conflito com padrões nacionais de cibersegurança.
Venezuela	A40-WP/348	Implementar rede de cibersegurança, criando o *Pontos de Contacto em Cibersegurança (PoC)*.
Venezuela	A40-WP/394	Elaborar guia de orientação dada a ausência de material e incapacidade do Anexo 17.
International Air Transport Association (IATA)	A40-WP/395	Incentivar cultura de cibersegurança. Investigar aspectos de cibersegurança em acidentes e incidentes. Fortalecer contribuições entre os envolvidos no setor.
Estados Unidos	A40-WP/427	Criar grupo técnico multidisciplinar e transversal.

Fonte dos dados: Documentos de Trabalho apresentados até 02/09/2019 pelos participantes.
Data source: Working Papers presented by the participants up to 02/09/2019.

acordos, tratados e convenções internacionais de que o Brasil seja parte compõem seu rol de imputações legais (BRASIL, 2005). Também merece destaque a atribuição de deliberar, na esfera técnica, a interpretação das normas e recomendações internacionais relativas ao sistema de segurança de voo da aviação civil.

A ANAC tem como missão "*garantir a todos os brasileiros a segurança e a excelência da aviação civil*" (BRASIL, [2014?], p. 22). Para elaborar o planejamento estratégico vigente, a Agência questionou seus servidores sobre qual a probabilidade de, até 2025, ocorrer ato de interferência ilícita contra a aviação civil brasileira de, ao menos, média proporção. O Resultado foi a possibilidade de 40,24%, (id., p. 19), o que denota estar a Agência relativamente preparada para entregar à sociedade brasileira um serviço seguro.

Considerando a visão da ANAC de "*ser uma autoridade de referência internacional na promoção da segurança e do desenvolvimento da aviação civil*" (ibid., p. 22), ao traçar o plano estratégico, a Agência adotou como objetivo na perspectiva da sociedade a consolidação da confiança no serviço:

> "[...] *as atividades da Agência buscam promover o acesso amplo a um transporte aéreo de qualidade e com segurança para toda a comunidade aérea. [...] E, no quesito da segurança, as atividades se concentram entre os aspectos operacionais e as precauções contra atos de interferência ilícita. Ambos contribuem para o aumento da confiança dos usuários do sistema de aviação civil*" (id., p. 29).

Igualmente elencou objetivos sob a perspectiva dos seus processos internos. Nesse caso, planejou otimizar o modelo de fiscalização nos diversos ramos da aviação civil: segurança operacional, segurança contra atos de interferência ilícita, prestação de serviço aos passageiros, entre outros, por meio de iniciativas de aprimoramento do modelo de controle de qualidade AVSEC (id. p. 32 e 49, *passim*).

Alinhado com o Plano Estratégico 2015-2019 da Agência, o Plano de Atuação Internacional, renovado anualmente desde 2017, reforça o objetivo estratégico voltado para a segurança. Tratando da intensa padronização do setor, menciona que:

> "*Na literatura especializada, existem evidências de que o nível de segurança do sistema de aviação civil de um determinado país seja determinado, dentre outros fatores, pelo grau de harmonização do marco regulatório desse país com os parâmetros normativos internacionais*" (BRASIL, 2019b, p.11).

Para um transporte aéreo seguro, é necessário o "*constante engajamento da autoridade de aviação civil brasileira nos fóruns técnicos internacionais*" (ibid. p. 11). A agenda para a AVSEC no plano internacional encontra-se voltada, entre outros aspectos, à cibernética (id., p. 25).

Diante disso, pode-se constatar que há relativo atendimento pela ANAC de alguns dos objetivos da Resolução. Ao buscar robustecer a qualidade da segurança na aviação (AVSEC), está em consonância

com o propósito "i", de desenvolver e implementar as melhores práticas na proteção de sistemas contra ameaças cibernéticas.

Na atuação internacional, identificam-se objetivos de atingir entendimento comum sobre cibersegurança e risco cibernético, eis que atua para alcançar a harmonização regulatória com parâmetros internacionais, propósitos "c", "i" e "f" da Resolução.

O tema da segurança cibernética, como referido, está sendo conduzido, no âmbito do Secretariado da OACI, pelo SSGC, que reúne representantes de governos nacionais e da indústria, especializados em áreas como segurança da informação, telecomunicações, gestão da informação, operação de aeródromos, aeronavegabilidade, política em segurança de aviação, facilitação, sistemas e infraestrutura de navegação aérea, operações de aeronaves, *internet* das coisas e operação de sistemas de aeronaves tripuladas remotamente (BRASIL, 2019, p. 26) e tem como escopo encorajar o compartilhamento de informações relacionadas a ameaças, incidentes e ações de mitigação de riscos.

O Brasil, ao participar diretamente do grupo que trata de aspectos normativos da segurança cibernética, trabalha para o estabelecimento de responsabilidades dos atores (propósito "b"), de consequências legais de atividades atentatórias (propósito "h") e de submissão de ameaças à análise forense (propósito "j").

Segundo a ANAC (ibid.), envolver-se nos debates de *security* garante que os processos e as normas nacionais cumpram as SARPS e que, dessa maneira, estas possam ser auditadas pelo Programa USAP (*Universal Security Audit Program*), entregando confiabilidade internacional do sistema de aviação civil brasileiro, além de permitir a avaliação da efetividade de processos, normas e do sistema de vigilância da segurança da aviação contra atos de interferência ilícita.

Para realizar ações de segurança e participar dos fóruns da Organização, o Brasil engajou-se ainda no programa do GSIPR de proteção de infraestruturas críticas. Nesse órgão, por meio da Portaria n. 02, de 8 fev. 2008/ GSIPR, foram criados os Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC), com a finalidade de propor medidas para a proteção em áreas prioritárias, dentre elas, o transporte aéreo.

Em síntese, nos termos do art. 7º da Portaria, cada Grupo deverá identificar instalações críticas de sua área, levantar vulnerabilidades, avaliar riscos que afetem sua segurança, propor medidas de segurança e por em prática um sistema de informações que conterá dados para a tomada de decisões (BRASIL, 2008). São consideradas infraestruturas críticas as "*instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional*" (id.). O documento também definiu o que seriam áreas prioritárias de infraestrutura crítica, sendo o transporte uma das cinco elencadas (ibid.).

Em 2010, foi instituído, por meio da Portaria do GSIPR n. 28, de 27 de abril, o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Transportes Aéreos (SGTSIC-TA), voltado especialmente para as infraestruturas críticas desse setor. Conforme as atribuições estabelecidas, o Subgrupo levanta e avalia vulnerabilidades das infraestruturas identificadas como críticas no setor, avaliando riscos, articulando medidas e implementando sistema de informações sobre essas infraestruturas para apoio a decisões (BRASIL, 2010).

O advento dessa estrutura regimental do GSIPR a partir do Decreto n. 9.668, de 1 jan. 2019, conferiu à sua Secretaria de Assuntos de Defesa e Segurança Nacional (SADSN) a competência do acompanhamento de assuntos relacionados à segurança de infraestruturas críticas. Na esfera dessa sua atuação, elaborou a pauta para debates do Subgrupo, que relaciona ameaças e impactos em aeroportos no Brasil. Entre as ameaças, constam "*falha de comunicação e ou interferência cibernética*", com a seguinte descrição: "*interrupção dos serviços de comunicações intencional ou não, como, telefonia e dados entre sistemas das empresas aéreas, sistemas de operador de aeródromo, sistemas dos órgãos públicos* […]" (BRASIL, 2019a).

Estão sob apreciação, consequências referentes à interferência cibernética em dez frentes no cenário analisado. Destaca-se o plano internacional, no qual se preveem repercussões diplomáticas, em razão de *hacker* estrangeiro ou ataque à aeronave estrangeira, com suspensão ou revisão de tratados e acordos e descumprimento de contratos por importadores ou exportadores. No plano operacional, uma interferência de natureza cibernética impactaria as operações reduzindo a capacidade do nível de segurança AVSEC, especialmente a vigilância. No plano social, limitaria a integração nacional, restringindo movimentações de aeronaves, ameaçaria a integridade física das pessoas (ibid.).

Além disso, a Secretaria entendeu que o risco cibernético atinge a segurança do Estado por dificultar o emprego (deslocamento aéreo e no tempo de atuação) das Forças de Segurança; reduzir a capacidade operacional das Forças Armadas, dos órgãos de segurança (poder de polícia) e dos órgãos de fiscalização; e possibilitar a desestabilização da ordem pública localizada, dificultando o controle da situação pelo Estado (ibid.) indo de encontro ao objetivo de garantir a soberania, o patrimônio nacional e a integridade territorial constante na Política de Defesa Nacional - PDN (BRASIL, 2016a, p. 12).

Quando da aprovação da Política Nacional de Segurança de Infraestruturas Críticas – PNSIC (BRASIL, 2018), que exigia

da administração autárquica considerar em seus planejamentos ações que concorressem para a segurança das infraestruturas críticas, a ANAC já se antecipara e apresentara seu Planejamento Estratégico 2015–2019, contemplando ações para a desejada Política. No período de 4 anos, a Agência reforçou o objetivo estratégico voltado para a segurança, focada no alcance dos mais altos *standards* internacionais pautados pela OACI. Porém, desde a instalação do Subgrupo, em 2010, a ANAC dedica-se a participar e contribuir para a persecução dos objetivos da PNSIC.

A estratégia, portanto, é engajar a ANAC na política nacional de segurança conduzida pelo GSIPR, a fim de dar vazão à necessidade de ampliar o escopo da segurança contra atos de interferência ilícita, especificamente afetos à cibersegurança e corresponder ao preparo esperado pela PND diante de cenários propícios "*para o desenvolvimento da denominada 'guerra híbrida', que combina distintos conceitos de guerra*" (BRASIL, 2016a, p. 9).

Todo o esforço do Brasil em debruçar-se sobre as recomendações da OACI e elaborar o plano estratégico da ANAC pareceu eclipsar-se diante do Decreto n.º 9.759/2019, que extinguiu colegiados da administração pública federal e, com isso, o grupo que debatia a segurança das infraestruturas críticas. Contudo, dada a relevância do programa de trabalho os encontros permaneceram.

Em paralelo, no intuito de estruturar seu planejamento estratégico para o próximo quadriênio (2020–2024), a ANAC convidou *stakeholders* do setor para proferirem palestras que tratassem de desafios da aviação civil diante das diversas realidades representadas (BRASIL, 2019c). Entre eles, encontram-se órgãos estatais de segurança e inteligência, administradores aeroportuários, operadores de transporte de passageiros e de cargas, órgãos de fiscalização e instituições de ensino superior.

Das contribuições, destaca-se a frequente menção sobre cibersegurança como um enfrentamento imediato e contínuo. A participação da Universidade de Brasília sublinhou que se está vivendo a quarta revolução industrial, cuja característica mais evidente é a rapidez com que artefatos são criados e alterados (CELESTINO, 2019). *Security* seria o maior desafio da evolução tecnológica desse tempo, e a segurança somente seria possível compartilhando dados com órgãos governamentais (id.) e todos os *players* envolvidos.

Diante disso, percebe-se que outros objetivos previstos na Resolução A39-19 da OACI foram, em alguma medida, alcançados. O Brasil estabeleceu mecanismos de troca de informações, de promoção dos meios de proteção e de boas práticas ao engajar a ANAC e o GSIPR no contexto do Subgrupo de Trabalho sobre infraestruturas críticas nacionais, correspondendo aos propósitos "d", "e", "i" da Resolução.

Na preparação do próximo Planejamento Estratégico da ANAC, o Brasil atentou especialmente à troca de informações sobre ameaças cibernéticas, tendências e mitigação de esforços (propósito "e"), envolvendo os participantes no debate sobre cibersegurança e aproximando a regulação dos atores de diversos meios.

Conclusão

A Resolução A39-19 da OACI contribuiu para o Brasil aperfeiçoar medidas de cibersegurança na aviação civil entre os anos de 2016 e 2019, atingindo o objetivo deste artigo de demonstrar encaminhamentos do emergente tema da cibersegurança.

Constatou-se que a arquitetura dos mecanismos em implementação pelo Brasil está em consonância com a postura em desenvolvimento na OACI. O Brasil envolveu-se em ações que correspondem aos propósitos da Resolução e, se ainda não foram esgotados em solo doméstico, estão encaminhados para alcançá-los.

Ficou demonstrado que o tema, pelo viés de *security*, não nasceu com a OACI, mas chegou com o passar do tempo, devido à evolução da sociedade e das tecnologias. Percebeu-se que o princípio da segurança previsto na Convenção de Chicago voltava-se ao *safety*, à segurança operacional.

Pôs-se, igualmente, em relevo, que segurança é um entendimento em evolução. Dada a intrincada tessitura das relações sociais, a dinâmica da segurança torna-se complexa e passa a compor-se de outras nuances. Atos de interferência ilícita passaram de exemplos previstos no Anexo 17 da Convenção, para o fortuito das ameaças cibernéticas.

Nesse raciocínio dedutivo, no qual se partiu da OACI para a abordagem da cibersegurança, à luz da Resolução A39-19, chegou-se à constatação de que o Brasil, por meio dos mais altos órgãos do Poder Executivo, o GSIPR e o SGTIC e de sua Agência dedicada, trabalha para a adoção de medidas preventivas consoantes às recomendadas internacionalmente, em harmonia aos objetivos nacionais de defesa.

Embora sejam normas de *soft law*, nota-se que a adesão às recomendações da Resolução A39-19 coincide com o interesse nacional. Desdobramentos são esperados nas próximas Assembleias da OACI. Na 40ª edição, o Comitê Executivo propôs o adensamento da Resolução A39-19, o que demonstra que a cibersegurança estenderá seus domínios sobre as discussões vindouras, onde quer que pouse uma aeronave.

Nesse passo, as sugestões contidas na Resolução, como o incentivo à cooperação entre as autoridades brasileiras, a indústria e os demais operadores do sistema de aviação civil; a promoção da cultura de cibersegurança

e o estabelecimento de mecanismos para a troca de informações estão em aplicação no Brasil em certa medida.

Como lição aprendida, entende-se que a relevância da segurança cibernética permitiu que o SGTIC não fosse descontinuado. Seu grau de tecnicidade, congregando representação de diversos órgãos de inteligência e de operação, tornou-se um instrumento de aplicação dos objetivos da PND voltados para a garantia da soberania, do patrimônio e da integridade nacionais à luz da cibersegurança.

Diante disso, um *framework* normativo seria bem-vindo a fim de robustecer os direcionamentos de políticas, ações e contribuições, para muito além das SARPS do ecossistema da aviação internacional.

Por sua vez, a PND e a END, que orientam ações de proteção às infraestruturas críticas, ao estabelecerem meios de afirmação da soberania sobre o patrimônio e a integridade nacionais, congregam a segurança cibernética do setor aéreo como forma de corresponder àquelas orientações, contribuindo para a segurança e defesa do Estado e consolidando a coordenação entre agentes da Administração Pública como instrumento ponderável para cibersegurança.

Referências bibliográficas

ABEAR — ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS AÉREAS. Panorama da Aviação Brasileira. Aviação no Brasil. Protocolo disponível: http://panorama.abear.com.br/a-aviacao-no-brasil/introducao [27 jul. 2019].

ANAC - AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL. Anacpédia. Brasília, [200-]a. Protocolo disponível: https://www2.anac.gov.br/anacpedia/por_esp/tr449.htm [31 ago. 2019].

ANAC - AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL . Workshop Desafiso do Sector de Aviação Civil - 2019. Brasília: Agência Nacional de Aviação Civil, 2019c.

BRASIL. Decreto n.º 9.668, de 2 de janeiro de 2019a. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Gabinete de Segurança Institucional da Presidência da República e altera o quantitativo de Gratificações de Exercício de Cargo em Confiança devida a Militares - RMP. Diário Oficial da União, Brasília, DF, 2 jan. 2019. Edição Extra n. 1-C. Protocolo disponível: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9668.htm [16 set. 2019].

BRASIL. Decreto n.º 9.759, de 11 de abril de 2019. Extingue e estabelece diretrizes, regras e limitações para colegiados da administração pública federal. Diário Oficial da União, Brasília, DF, 11 abr. 2019. Protocolo disponível: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D9759.htm [29 ago. 2019].

BRASIL. Decreto n.º 21.713, de 27 de agosto de 1946. Promulga a Convenção sobre Aviação Civil Internacional, concluída em Chicago a 7 de dezembro de 1944 e firmada pelo Brasil, em Washington, a 29 de maio de 1945. Diário Oficial da União, Rio de Janeiro, RJ, 12 set. 1946. Protocolo disponível: http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/D21713.htm [1º jul. 2019].

BRASIL. Estratégia Nacional de Defesa. Brasília, DF: MD, 2016b. Protocolo disponível: https://www.defesa.gov.br/arquivos/2017/mes03/pnd_end.pdf [28 jul. 2019].

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Portaria n° 2/GSIPR, de 8 de fevereiro de 2008. Institui Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC) e dá outras providências. Diário Oficial da União, Brasília, DF, 11 fev. 2008. Protocolo disponível: https://www.diariodasleis.com.br/legislacao/federal/198823-infra-estruturas-cruticas-gtsic-institui-grupos-tucnicos-de-seguranua-de-infra-estruturas-cruticas-gtsic-e-du-outras-providuncias.html [3 ago. 2019].

BRASIL. Lei n.º 11.182, de 27 de setembro de 2005. Cria a Agência Nacional de Aviação Civil – ANAC, e dá outras providências. Diário Oficial da União, Brasília, DF, 28 set. 2005. Protocolo disponível: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11182.htm [28 jul. 2019].

BRASIL. OACI ratifica o Brasil entre os melhores avaliados em segurança operacional. Brasília: Agência Nacional de Aviação Civil, 09 mai. 2016. Protocolo disponível: https://www.anac.gov.br/noticias/2016/oaci-ratifica-o-brasil-entre-os-melhores-avaliados-em-seguranca-operacional [13 abr. 2019].

BRASIL. Organização da Aviação Civil Internacional (OACI). Publicado em 7 mar. 2016. Protocolo disponível: https://www.anac.gov.br/A_Anac/internacional/organismos-internacionais/organizacao-da-aviacao-civil-internacional-oaci [04 jul. 2019].

BRASIL. Planejamento Estratégico. Plano Estratégico 2015-2019. Brasília, [2014?]. Protocolo disponível: https://www.anac.gov.br/acesso-a-informacao/acoes-e-programas/arquivos/anexoi-1.pdf [04 ago. 2021] .

BRASIL. Plano de Atuação Internacional 2019. Brasília, abr. 2019b. Protocolo disponível: https://www.anac.gov.br/A_Anac/internacional/publicacoes/plano-de-atuacao-internacional-1/plano-de-atuacao-internacional-2019/plan_atuacao_inter_anac_19.pdf [28 jul. 2019].

BRASIL. Política Nacional de Defesa. Brasília, DF: MD, 2016a. Protocolo disponível: https://www.defesa.gov.br/arquivos/2017/mes03/pnd_end.pdf [28 jul. 2019].

BRASIL. Portaria n.º 2, de 8 de fevereiro de 2008. Gabinete de Segurança Institucional da Presidência da República. Institui Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC) e dá outras providências. Diário Oficial da União, Brasília, DF, 11 de fevereiro de 2008. Protocolo disponível: https://www.diariodasleis.com.br/legislacao/federal/198823-infra-estruturas-cruticas-gtsic-institui-grupos-tucnicos-de-seguranua-de-infra-estruturas-cruticas-gtsic-e-du-outras-providuncias.html [31 ago. 2019].

BRASIL. Portaria n.º 28, de 27 de abril de 2010. Gabinete de Segurança Institucional da Presidência da República. Institui o Subgrupo Técnico de Segurança de Infraestruturas Críticas de Transportes Aéreos (SGTSIC - Transportes Aéreos) e dá outras providências. Diário Oficial da União, Brasília, DF, 28 de abril de 2010. Protocolo disponível: https://www.diariodasleis.com.br/legislacao/federal/214062-subgrupo-tecnico-de-seguranca-de-infraestruturas-criticas-de-transportes-aereos-sgtsic-transportes-aereos [31 ago. 2019].

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Livro verde: segurança cibernética no Brasil. Organização Claudia Canongia e Raphael Mandarino Junior. Brasília: GSIPR/SE/DSIC, 2010. Protocolo disponível: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf [04 ag. 2021].

BRASIL. Resolução n.º 499, de 12 de dezembro de 2018. Programa de Segurança Contra Atos de Interferência Ilícita da Agência Nacional de Aviação Civil (PAVSEC-ANAC). Brasília, 2018. Protocolo disponível: http://www.anac.gov.br/assuntos/legislacao/legislacao-1/resolucoes/2018/resolucao-no-499-12-12-2018 [13 abr. 2019].

BRASIL. SECRETARIA DE ASSUNTOS DE DEFESA E SEGURANÇA NACIONAL (SADSN). Gabinete de Segurança Institucional da Presidência da República. *Relação de Ameaças x Consequências (Impactos) - Aeroportos*.

BRASIL. Safety. Brasília, [200-]b. Protocolo disponível: https://www.anac.gov.br/assuntos/setor-regulado/aerodromos/safety [26 jul. 2019].

Buzan, B., Hansen, L. (2012). *A evolução dos estudos de segurança internacional*. São Paulo: UNESP.

Castells, M. (2006) *A sociedade em rede*. São Paulo: Paz e Terra.

Celestino, V. R. V. (2019). *Palestra ministrada no Workshop Desafios do Setor de Aviação Civil*. Brasília: Agência Nacional de Aviação Civil, 22 ago.

Costa, C. E. P., Camargo, D. C. de (2016). A corpus-based study of simple terms "segurança", "safety" and "security" in aviation language. *Aviation in Focus, Journal of aeronautical sciences*. Volume 7, Number 1, 4-12, January-June. Disponível em: http://revistaseletronicas.pucrs.br/ojs/index.php/aviation/article/view/23738. [31 ago. 2019].

EASA – EUROPEAN UNION AVIATION SAFETY AGENCY. (2019). Notice of Proposed Amendment 2019-01. União Europeia: European Union Aviation Safety Agency. Protocolo disponível: https://www.easa.europa.eu/sites/default/files/dfu/NPA%202019-01.pdf [30 ago. 2019].

ICAO – CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. Executive Committee. Protocolo disponível: https://www.icao.int/Meetings/a40/Pages/WP_Num.aspx?Category=(EX) [8 ago. 2019].

ICAO – CONVENTION ON INTERNACIONAL CIVIL AVIATION (2017). Assembly Working Papers. Annex 17 to the Convention on International Civil Aviation. Security. Safeguarding International Civil Aviation Against Acts of Unlawful Interference. 10. ed. Quebec.

ICAO – CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. Civil Aviation Cybersecurity Action Plan. Protocolo disponível: https://www.icao.int/cybersecurity/SiteAssets/ICAO/Civil%20Aviation%20Cybersecurity%20Action%20Plan%20-%20SIGNED.pdf [8 jun. 2019].

ICAO – CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. Civil aviation cybersecurity information repository. Protocolo disponível: https://www.icao.int/cybersecurity/Pages/default.aspx [30 ago. 2019].

ICAO – CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. Convention on International Civil Aviation. Chicago, 7 de dezembro de 1944. Protocolo disponível: https://www.icao.int/publications/Documents/7300_orig.pdf [26 jul. 2019].

ICAO – CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. Council States 2016-2019. Montreal, [ca. 2016]. Protocolo disponível: https://www.icao.int/about-icao/Council/Pages/council-states-2016-2019.aspx [17 set. 2019].

ICAO – CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. Declaration on Cybersecurity in Civil Aviation Dubai. United Arab Emirates, 4 to 6 april 2017. Protocolo disponível: https://www.icao.int/Meetings/CYBER2017/Documents/Draft%20Dubai%20DECLARATION%20ON%20CYBERSECURITY%20IN%20CIVIL%20AVIATION_10%20March%202017.pdf [10 jul. 2019].

ICAO — CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. History: Foundation of the International Civil Aviation Organization (ICAO). Protocolo disponível: https://www.icao.int/EURNAT/Pages/HISTORY/history_1944.aspx [26 de jul. 2019].

ICAO — CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. ICAO Europe, Middle East and Africa Summit on Cybersecurity in Civil Aviation. Bucharest Communique Recommendations for a Cybersecurity Strategy in International Civil Aviation. Bucharest, Romania, 7 to 9 may 2018. Protocolo disponível: https://www.icao.int/cybersecurity/Documents/Bucharest%20Communique.9%20May%202018.pdf [10 jul. 2019].

ICAO — CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. In Focus: ICAO'S Strategic Objectives. Protocolo disponível: https://www.icao.int/Pages/default.aspx [31 ago. 2019].

ICAO — CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. The History of ICAO and the Chicago Convention. Protocolo disponível: https://www.icao.int/about-icao/History/Pages/default.aspx [26 jul. 2019].

ICAO — CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. Working Paper A39. Addressing Cybersecurity in Civil Aviation. Assembly – 39th Session. May 30, 2016. Protocolo disponível: https://www.icao.int/Meetings/a39/Documents/WP/wp_175_en.pdf [25 maio 2019].

ICAO — CONVENTION ON INTERNACIONAL CIVIL AVIATION. Assembly Working Papers. Working Paper A40. ICAO Cybersecurity Strategy. Assembly – 40th Session. June 25, 2019. Protocolo disponível: https://www.icao.int/Meetings/A40/Documents/WP/wp_243_en.pdf [22 ago. 2019].

ONU. Resolución A/44/118. Avances científicos y tecnológicos y su repercusión en la seguridad internacional. Protocolo disponível: https://undocs.org/es/A/RES/44/118 [6 set. 2019].

Portela, P. H. (2011). *Direito internacional público e privado*. Salvador: Podivm.

Portilho, F., Bukzem, S. (2015). Os precedentes históricos da navegação aérea baseada em instrumentos: necessidade, surgimento e evolução. *Aviation in Focus, Journal of aeronautical sciences*. Volume 6, Number 1, 17-27, January-June. Disponível em: http://revistaseletronicas.pucrs.br/ojs/index.php/aviation/article/view/21165 [04 nov. 2019].