PANORAMA DA AMEAÇA CIBERNÉTICA À AVIAÇÃO CIVIL

Mateus Vidal Alves Silva *

Resumo

O artigo apresenta abordagem inicial da ameaça de ataque cibernético à aviação civil, sob a ótica conceitual da inteligência da aviação civil. Formulou-se o seguinte problema de pesquisa: quais os parâmetros essenciais para estruturar um panorama da ameaça cibernética como fenômeno que interage e desafia a inteligência da aviação civil? A metodologia propõe pesquisa básica, exploratória e qualitativa, mediante revisão da literatura, utilizada para delinear os marcos teórico-conceituais, as estruturas, as análises e a casuística. A Política Nacional de Inteligência (PNI) destaca a ameaça cibernética, com crescimento exponencial e ampla gama de alvos elegíveis e interconectados. É ameaça assimétrica dinâmica, que apresenta múltiplos formatos e atores possíveis e tem potencial de danificar ativos e infraestruturas críticas. A aviação civil é alvo recorrente de interferências ilícitas. Nessa área, a ameaça cibernética é real e poderia resultar em episódio classificável como "cisne negro", nos moldes dos ataques terroristas de 11 de setembro de 2001. Ao abordar a ameaça de ataque cibernético à aviação civil contemplam-se os conceitos aplicáveis, o estado da arte da inteligência da aviação civil, a irrefutabilidade de possíveis falhas, os alvos potenciais, as categorias de atores e suas motivações, a capacidade de agir e os possíveis métodos de ataque. As considerações finais apontam para a possibilidade de evoluções intermediadas por uma política de mitigação de riscos relacionados à ameaça cibernética na aviação civil subsidiada por análises estruturadas de inteligência.

Palavras-chaves: ameaças, ataque cibernético, aviação civil, inteligência da aviação civil, infraestruturas críticas.

A PANORAMA OF THE CYBERNETIC THREAT TO CIVIL AVIATION

Abstract

The article presents an initial approach to the threat of cyberattacks on civil aviation, from the conceptual perspective of civil aviation intelligence. The following research problem was formulated: what are the essential parameters for structuring a panorama of the cyber threat as a phenomenon that interacts with and challenges civil aviation intelligence? The methodology proposes basic, exploratory, and qualitative research, using a literature review which outlines conceptual theoretical frameworks, structures, analyses and case studies. The Brazilian National Intelligence Policy (PNI) highlights the cyber threat, which has been growing exponentially and has a wide range of eligible and interconnected targets. It is a dynamic asymmetric threat that presents multiple formats and possible actors with the potential to damage critical assets and infrastructure. Civil aviation is a recurring target of unlawful interference, where the cyber threat is real – and could result in a "black swan" episode like the September 11, 2001 terrorist attacks. Addressing the threat of cyberattacks on civil aviation includes applicable concepts, the state of the art of civil aviation intelligence, the irrefutability of possible failures, potential targets, the categories of actors and their motivations, the ability to act and possible attack methods. The final considerations indicate the possibility of developments mediated by a policy to mitigate risks related to cyber threats in civil aviation subsidized by structured intelligence analysis.

Keywords: *threats, cyberattack, civil aviation, civil aviation intelligence, critical infrastructures.*

* Bacharel em Direito. Especialista em Inteligência de Estado e Inteligência de Segurança Pública (INASIS).

Introdução

A história da aviação e da atividade de inteligência comungam de diversos liames. A evolução técnica das aeronaves e de seu emprego como plataformas modais das atividades humanas consignou progressos à atividade de inteligência. Noutro giro, os ataques terroristas de 11 de setembro de 2001, nos Estados Unidos da América (EUA), estigmatizaram a atividade de inteligência e a aviação civil (SILVA, 2017, p. 16). Do paradigma do terrorismo, surgem diversas questões. Para a atividade de inteligência, importa otimizar suas capacidades. Caberá à inteligência, especialmente aplicada ao contexto da aviação civil, ser mais eficaz para se antecipar na mitigação das ameaças[1]. Após o 11 de Setembro de 2001, instaurou-se comissão investigatória no congresso estadunidense, que editou relatório. A análise indicou que condutas preparatórias dos atos terroristas ocorreram no cerne da aviação civil e que o conjunto das agências de inteligência tinha ciência disso. Falhas se impuseram na integração, análise e difusão adequada da inteligência que oportunizaria a neutralização da ação (ESTADOS UNIDOS DA AMÉRICA, 2004, tradução nossa).

Segundo Betts (2007, p. 107), o relatório de inteligência do Departamento Federal de Investigação dos EUA (FBI, na sigla em inglês) conhecido como *Phoenix Memo*, difundido cerca de um mês antes do atentado, esclarecia a existência de atividades terroristas em escolas de aviação civil ianques. A adequada percepção do memorando nos altos escalões, agregada a outros produtos de inteligência existentes, teria sido crucial para desmantelar o plano terrorista. É falacioso atribuir as falhas incidentes à inexperiência ou à ignorância sobre a relevância da inteligência para a aviação. A unidade de inteligência da aviação civil da Administração Federal de Aviação dos EUA (FAA, na sigla em inglês)[2] foi criada em 1986, porque a aviação era alvo recorrente de terrorismo (ESTADOS UNIDOS DA AMÉRICA, 1990, p. 74, tradução nossa).

Diante da complexidade, multiplicidade e inexatidão de resultados, Heuer e Pherson (2016) enaltecem as técnicas estruturadas de análise de inteligência, como a análise de cenários, que embora não revelem o futuro, criam limiar de eventos plausíveis a fim de preparar o decisor. A seu turno, Barreto (2007, p. 63-76) lecionou sobre o terrorismo cibernético em cenários especulativos. Especula-se que atores adversos, suas motivações e capacidades de agir podem extrapolar a paradigmática ação cinética[3] no solo americano. A ação terrorista ocorreu na dimensão tangível, a inteligência estadunidense padeceu na detecção e falhou na neutralização. Exorbitando a concepção

1 Das ameaças destacadas na Política Nacional de Inteligência (PNI) atribuíveis ao contexto do ecossistema da aviação civil, arrolam-se: 1) a espionagem; 2) a sabotagem; 3) a interferência externa; 4) a corrupção; 5) a criminalidade organizada; 6) as ações contrárias à soberania nacional; 7) as atividades ilegais envolvendo bens de uso dual e tecnologias sensíveis; 8) o terrorismo; e 9) os ataques cibernéticos (BRASIL, 2016b).

2 Autoridade de aviação civil nos Estados Unidos da América, sendo comparável, guardadas as devidas proporções analógicas e contextuais históricas, à Agência Nacional de Aviação Civil (ANAC) no Brasil.

3 Ações cinéticas são aquelas desencadeadas no interior da Área de Operações, que envolvem movimentos (fogos, voos, deslocamento de tropas e de blindados) e produzem resultados tangíveis (destruição, captura, conquista etc.) (BRASIL, 2015a, p.17).

preditiva, sob os augúrios de uma técnica estruturada[4], surge uma questão: e se as ações antagônicas ocorrerem no espaço cibernético, intangível, mediante ações não cinéticas?

Com o objetivo de explicitar um panorama da ameaça de ataque cibernético, sob a ótica da inteligência da aviação civil, formulou-se o seguinte problema de pesquisa: quais os parâmetros essenciais para estruturar um panorama da ameaça cibernética como fenômeno que interage e desafia a inteligência da aviação civil? Em uma abordagem inicial e não exaustiva, a metodologia do trabalho propõe pesquisa básica, exploratória e qualitativa, por meio de revisão da literatura. Busca-se delinear os marcos teórico-conceituais, as estruturas, as perspectivas analíticas e as explorações casuísticas. Ao estruturar a ameaça de ataque cibernético à aviação civil, contemplam-se os conceitos preliminares, o estado da arte da inteligência da aviação civil, a irrefutabilidade de possíveis falhas, os alvos potenciais, as categorias de atores e suas motivações, a capacidade de agir e os possíveis métodos de ataque.

Conceitos Preliminares

O neologismo *ciberespaço* remonta à obra *Neuromancer* de Willian Gibson: "uma alucinação consensual, experimentada diariamente por bilhões de operadores legítimos [...]. Linhas de luz dentro do não espaço da mente; aglomerados e constelações de dados". Não há conceitos unívocos em cibernética. A literatura técnica define o ciberespaço como ambiente de informação, constituído digitalmente de dados criados, armazenados e compartilhados. Embora desafie dimensões físicas, não é exclusivamente virtual, por compreender computadores e infraestruturas que permitem aos dados fluir (SINGER e FRIEDMAN, 2017, p. 22 e 23).

O ciberespaço ou espaço cibernético é a dimensão da cibernética. É o mais novo espaço de batalha do teatro de guerra, ao lado dos espaços marítimos, terrestres, aéreos e espaciais (BRASIL, 2015a, p. 105 e p. 265). A cibernética "se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação" (BRASIL, 2015a, p. 62). A Política Nacional de Defesa (PND) relata que "para que o desenvolvimento e a autonomia nacionais sejam alcançados é essencial o domínio crescentemente autônomo de tecnologias sensíveis, principalmente nos estratégicos setores espacial, cibernético e nuclear" (BRASIL, 2012, p. 11). Dos três setores estratégicos destacados, a Estratégia Nacional de Defesa (END) destinou ao Exército Brasileiro a

4 A técnica de análise estruturada "e se?" imagina que um evento inesperado ocorreu com potencial de impacto majorado. Diante da "retrospectiva", o analista presume o desenrolar e as consequências desencadeadas no evento. Gera-se consciência situacional, preparando a mente para reconhecer sinais antecedentes de mudanças significativas e propiciar assessoramento preditivo ao decisor (HEURER E PHERSON, 2016, l.3934, tradução nossa).

defesa cibernética[5]. O Exército Brasileiro também se debruça sobre os teclados e fluxos informacionais (BRASIL, 2012, p. 73) no Sistema Militar de Defesa Cibernética[6] (SMDC). Os computadores nos cercam no cotidiano e o teatro de operações cibernético oportuniza ampla gama de ações inéditas diante das tecnologias emergentes. São exemplos arquétipos a computação quântica, a inteligência artificial e a evolução da comunicação sem fio. Quanto à reformatação no campo bélico Barbosa da Costa (2012, p. 62) afirma que:

> O conflito armado permanecerá sendo um esforço intrinsecamente humano, com todas as incertezas que isso implica. No entanto, o caráter dos conflitos continuará a evoluir, permanecendo inerentemente instável, mas intenso e sujeito às novas condicionantes impostas pela revolução digital. Os contendores buscarão empregar métodos convencionais, irregulares e assimétricos, combinando, no tempo e no espaço, ações marítimas, terrestres, aéreas, espaciais e cibernéticas.

Proliferam-se, em todo o mundo, ataques cibernéticos de atores estatais ou não, inclusive contra infraestruturas críticas, além do epidêmico plantio de *fake news,* armas do conflito informacional. Assim, a escolha pelo estudo da ameaça cibernética na aviação civil é justificável. A ameaça cibernética é a "causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético de interesse" (BRASIL, 2015a, p. 27). A variedade de ações adversas possíveis dificulta a mitigação de ataques cibernéticos e impõe obstáculos a sua definição e atribuição. Vários conceitos interagem no vulto da ameaça. O que é um ataque cibernético? Eis a terminologia da Política Nacional de Inteligência (PNI) (BRASIL, 2016b):

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

O estado da arte da inteligência da aviação civil

Ao estruturar uma ameaça à aviação, é preciso conceituar a inteligência da aviação civil, tão recente na literatura técnica. O documento *DoD Instruction Number 3115.14* traz um rol de atividades da inteligência, sob o estudo de tendências da indústria global que impactam os interesses estadunidenses e da capacidade de "detectar, analisar, monitorar e alertar sobre atividades ilícitas ou ameaças contra os Estados Unidos, seus aliados ou seus interesses envolvendo aviação civil" (ESTADOS UNIDOS DA AMÉRICA, 2011a, p. 6, tradução nossa). Refletindo a trindade conceitual de Sherman Kent e inspirado no paradigma do

5 A defesa cibernética é o "conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente" (BRASIL, 2015a, p. 85).

6 O Sistema Militar de Defesa Cibernética é o "conjunto de órgãos, meios, disponibilidades e relacionamentos, de natureza predominantemente militar, aptos a serem empregados de forma coordenada, no espaço cibernético, com efeitos no campo cinético, em defesa dos interesses nacionais em uma situação definida" (BRASIL, 2015a, p. 257).

departamento de Defesa dos EUA (DoD, na sigla em inglês), surgiu um conceito de inteligência da aviação civil, apto às doutrinas brasileiras (SILVA, 2017, p. 114):

> A inteligência da aviação civil é a expressão das atividades especializadas das autoridades competentes para entender como tendências na aviação civil impactam os interesses das nações, por intermédio da detecção, análise, monitoramento e alerta sobre atividades ilícitas ou ameaças contra os interesses envolvendo a aviação civil, objetivando salvaguardar ativos e produzir conhecimentos para assessorar o processo decisório.

A autoridade de aviação civil brasileira é a Agência Nacional de Aviação Civil (ANAC), autarquia especial criada pela Lei nº 11.182, de 27 de setembro de 2005 (BRASIL, 2005), sucessora do Departamento de Aviação Civil (DAC). A ANAC ingressou no Sistema Brasileiro de Inteligência (SISBIN) mediante edição de decreto (BRASIL, 2017b). Aduz-se que as atividades de inteligência da aviação civil do sobredito conceito circunscrevem-se às competências da ANAC, no escopo de inteligência fiscal e de colaboração no âmbito do SISBIN.

Restam sedimentados na memória popular, como ações ilícitas das últimas décadas relacionadas à aviação civil, os sequestros de aeronaves, os atentados à bomba e, finalmente, as ações suicidas que atingiram o *World Trade Center* e o Pentágono. Todavia o universo real e potencial de ameaças é dinâmico e evolui constantemente, ou seja, não se restringirá ao que já foi historicamente comprovado[7]. Versa a Doutrina Nacional da Atividade de Inteligência (DNAI) (BRASIL, 2016a, p. 63 e 64):

> Os atentados terroristas de 11 de setembro de 2001 deram ensejo a que Estados intensificassem o manejo da informação como instrumento e garantia de segurança coletiva. A exploração do espaço cibernético passou a utilizar sistemas de vigilância eletrônica ainda mais sofisticados e abrangentes. Muitas das ameaças tradicionais encontram correspondente no espaço cibernético, a exemplo da espionagem, do terrorismo, do ativismo extremista, da guerra e das atividades criminais. Nas duas últimas décadas, prejuízos advindos de crimes cibernéticos e desafios à segurança cibernética tornaram-se assunto de amplo debate. Além dos danos causados por crimes comuns, destacam-se aqueles que afetam a esfera econômica e a segurança nacional.

A inteligência perfaz assessoria especializada e preditiva, diante da qual a doutrina interpõe os desafios da segurança cibernética, subentendida como "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" (BRASIL, 2015a, p. 249). Na evolução histórica da aviação civil, o ataque cibernético desponta como ameaça mais recente. Para Shulsky e Schmitt (2002, l.1531), uma das funções da inteligência é criar sistema de indicadores e alertas para a mitigação de ameaças, baseado na análise de passos que o adversário tomaria ao

7 O manual de campanha do Exército Brasileiro preceitua: "os combates modernos têm se caracterizado pelo uso maciço de tecnologia, pela presença de civis e da mídia no ambiente operacional, pelo emprego de estruturas de combate com maior proteção coletiva, velocidade e letalidade seletiva, pela utilização de aeronaves remotamente pilotadas e pela capacidade de operar no espaço cibernético" (BRASIL, 2015b, p. 13).

preparar um ataque. Sublinhe-se, quanto aos indicadores e alertas (HERMAN, 1999, p. 235-236, tradução nossa):

> A guerra fria também produziu sistemas especializados, em sua maioria militares, de alerta engendrados por "indicadores", começando desde 1948. Os méritos dos arranjos variaram; claramente eles não preveniram falhas nos alertas. Subsiste certa vantagem em designar alguém com a especial responsabilidade de guiar a coleta de alvos de potencial alerta, e para procurar por evidências de alerta. Mas os sistemas de indicadores tem armadilhas, parcialmente porque se tratam de presunções sobre contingências esperadas ao invés de inesperadas e parcialmente porque eles sacam os indicadores fora de seu contexto. Alertar não é uma atividade separada do restante da compreensão de inteligência. A principal conclusão organizacional é que o alerta não pode ser separado da atividade de análise corrente; que noutro giro não pode ser isolada do trabalho a médio e longo termo. Alertar envolve aportar acuradas compreensões de longo termo para lidar em situações correntes; tais falhas tendem a refletir percepções errôneas de longo termo. [...] Então, alertar e avaliar em longo termo são peças de um contexto geral. Avaliações de curto e longo termo devem ser ajustadas não como atividades separadas, mas sim com retroalimentações e intercâmbios entre ambos. Buscar a compreensão dos alvos tem que ser combinado com a manutenção de um olho aberto para ameaças incomuns e comportamentos atípicos.

Ampliando o entendimento de ataque cibernético ao explorar a guerra cibernética[8], definem-se características e tipologias. Consideram-se, no domínio da guerra cibernética, o uso de medidas ofensivas ou defensivas. São verbos reitores de ações no espaço cibernético: negar, explorar, corromper, degradar e destruir. Identificam-se as plataformas utilizadas e os espaços onde o ataque cibernético incide, respectivamente: as ferramentas de tecnologia da informação e comunicações (TIC) e os sistemas de tecnologia da informação e comunicações e comando e controle (STIC2), que são valores baseados em informações, sistemas e redes de computadores. Eis o axioma básico da eficácia do ataque cibernético: a oportunidade de seu emprego é proporcional à dependência do adversário em relação à TIC. A finalidade é obter vantagens, tanto em objetivos militares quanto civis (BRASIL, 2015a, p. 134). Sobreleva notar a estratégica dependência da integração brasileira em relação à aviação civil e ao preparo da mobilização nacional (CHEREM, 2011, p. 34):

> Considerando a extensão territorial do Brasil, com mais de 8,5 milhões de km² – a quinta maior área do mundo – e mais de 5 mil municípios, observa-se com certa facilidade a razão pela qual o modal aeroviário tem sido privilegiado diante dos demais modais, por sua importância para integração nacional, sendo contemplado frequentemente pelas políticas públicas. Adiciona-se a esta assertiva, o fator preponderante da aviação no desenvolvimento nacional,

8 Interpreta-se verbete do glossário das forças armadas: "Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC" (BRASIL, 2015a, p.134).

> especialmente, quanto à fixação da população em regiões mais longínquas do país, fornecendo suporte para atividades econômicas, como por exemplo, a migração da fronteira agrícola no Centro-Oeste, ou ainda, na Região Amazônica, onde não se pode chegar pelo transporte fluvial, de forma perene ou temporária.

Quanto à severidade dos potenciais danos de ataques cibernéticos à aviação, analogia com a potência hegemônica é viável, visto que a estratégia nacional para a segurança da aviação ianque declara o valor do vetor aéreo (ESTADOS UNIDOS DA AMÉRICA, 2018a, p. 8, tradução nossa):

> As atividades relacionadas à aviação representam na atualidade aproximadamente cinco pontos percentuais no produto interno bruto da nação, com previsão de crescimento com o advento de tecnologias avançadas. Este horizonte dinâmico requer que os Estados Unidos desenvolvam e sustentem uma persistente metodologia de várias camadas para proteger tal recurso vital. Além disso, o ecossistema da aviação suporta o setor público, a segurança interna e operações aéreas militares contínuas e sob demanda para impedir o desmantelamento da nação.

Da irrefutabilidade de possíveis falhas

Duas características intensificam os riscos de ataque cibernético: é ameaça assimétrica e ação não cinética. A PNI ressalta o perfil não convencional do ataque cibernético ao listar os potenciais atores, evidenciando que são realizáveis por governos, organizações criminosas e "simpatizantes de causas específicas; ou mesmo por nacionais que apoiem ações antagônicas aos interesses de seus países" (BRASIL, 2017). O sinal não ortodoxo do ataque cibernético serve à didática da definição de ameaça assimétrica (BRASIL, 2015a, p. 27):

> Ameaça Assimétrica – Ameaça decorrente da possibilidade de serem empregados meios ou métodos não ortodoxos, que incluem terrorismo, ataques cibernéticos, armas convencionais avançadas e armas de destruição em massa para anular ou neutralizar os pontos fortes de um adversário, explorando suas fraquezas, a fim de obter um resultado desproporcional.

Enquanto as ameaças tangíveis são mais previsíveis no espectro de dados conhecidos oriundos das experiências históricas, o desconhecimento potencial das ameaças cibernéticas é real, e a possibilidade de surpresa estratégica em seu emprego é maior. O traço de ação não cinética do ataque cibernético complica sua detecção (BRASIL, 2015a, p. 19):

> Ações Não Cinéticas – São aquelas desencadeadas no interior da Área de Operações, que não envolvem movimentos (ações de guerra eletrônica, operações psicológicas, ações de assuntos civis, ações no ciberespaço) e produzem resultados intangíveis (interferências eletromagnéticas, bloqueio, percepção positiva da população sobre as forças amigas e suas operações), mas que contribuem para o sucesso da operação.

Há vastos recursos humanos sensibilizados na comunidade de inteligência e segurança pública, com décadas de investimentos em recursos materiais, lidando com ameaças tangíveis. É impossível afirmar o mesmo perante a intangibilidade das ameaças cibernéticas, apesar dos esforços institucionais. Abnegados pesquisadores, integrantes da comunidade de inteligência e militares comungam de tais esforços, dos quais são exemplos o pioneiro grupo de

trabalho editor do "Livro Verde: segurança cibernética no Brasil" e os membros do Comando de Defesa Cibernética do Exército Brasileiro e do Gabinete de Segurança Institucional (BRASIL, 2010). A dinâmica da ameaça cibernética e das tecnologias disruptivas renova-se diariamente. Já a mão de obra destinada à sua neutralização demanda maior tempo de preparação e investimentos, extravasando o interstício de renovação das ameaças. O vácuo de conhecimento sobre segurança cibernética não é exclusividade brasileira e foi destacado pelo general Michael Vincent Hayden, ex-diretor da Agência Central de Inteligência dos EUA (CIA, na sigla em inglês). A incapacidade de decidir linhas de ação pelos líderes decorre da pouca familiaridade de sua geração com computadores, sendo a segurança cibernética discutida com imprecisão e parco entendimento (SINGER e FRIEDMAN, 2017, p. 13). Aportando os raciocínios para as capacidades instaladas na segurança da aviação civil, a possibilidade de detectar ações de atores adversos no espaço tangível é maior do que no espaço cibernético. Na evolução histórica da aviação, a novel ameaça cibernética é aquela com o menor tempo de tratamento dedicado a sua mitigação. A produção técnica ianque coaduna-se com o raciocínio ora apresentado (ESTADOS UNIDOS DA AMÉRICA, 2018a, p. 3, tradução nossa):

> Nossos inimigos, continuam a enxergar a aviação como um alvo especial, e o ecossistema da aviação enfrenta ameaças multifacetadas e mudanças constantes nas táticas que constituem um desafio a superar. A última década observou o avanço de tecnologias que geraram benefícios sociais e econômicos, mas que também podem ser usados para desafiar a conformidade e a segurança do ecossistema da aviação. O uso de "tecnologias disruptivas", tais como a conectividade cibernética e as aeronaves não tripuladas, de forma inconsequente ou maliciosa, em conjunto com a constante evolução das ameaças terroristas à aviação tripulada, demandam um tratamento novo e universal pela comunidade.

Rejeitando o alarmismo midiático, é importante enaltecer um século de aprendizado de segurança na aviação: quando a engenharia aeronáutica implementou computadores nas aeronaves, o fez com redundâncias e camadas de segurança. A automação das aeronaves avança e, paulatinamente, prescinde e remodela a manipulação presencial do ser humano. As falhas são raras, como a que supostamente afetou o *software* do sistema de aumento das características de manobra (MCAS) de aeronaves *Boeing 737 MAX,* em evidência por talvez haver contribuído para acidentes aéreos recentes (BOEING, 2019). O erro é imanente à condição humana. Ainda mais raro seria explorar maliciosamente, por meio de violação, falha de concepção similar em ataque cibernético. Entretanto, dada a antítese em elogio à dialética, é improvável negar a miríade de possíveis falhas de engenharia ou execução em salvaguardas que obstaculizam potencial ataque cibernético a sistemas da aviação. Boas práticas da engenharia aeronáutica em aeronaves e sistemas embarcados não extinguem as

possíveis falhas[9]. É improvável também refutar a ocorrência de falhas ocultas na conformação dos sistemas aplicados na aviação civil: cite-se o exemplo da ameaça do *hardware trojan* (BRUZZEGUEZ, NEUMANN e SOUZA, 2018). Qualquer falha em qualquer sistema é potencialmente explorável em um ataque cibernético (BARRETO, 2007, p. 64):

> Qualquer infraestrutura TIC poderia ser alvo de uma ação terrorista. Um exemplo seria a paralisação do sistema de controle de tráfego aéreo de um aeroporto importante. Por outro lado, a infraestrutura TIC poderia ser, não mais o alvo, mas a ferramenta utilizada em um ataque, como uma intencional alteração de dados de voo que objetivasse produzir um acidente aéreo.

Os alvos elegíveis e as categorias de atores motivados que desafiam à Inteligência da Aviação Civil

Subsiste uma profusão de alvos eventuais de ataques cibernéticos na aviação civil: empresas aéreas, fabricantes de aeronaves, infraestruturas aeronáuticas, sistemas dedicados e órgãos de aviação civil. Em reverência à contrainteligência, declinar detalhes de alvos elegíveis é temerário. Em uma simples taxonomia, declina-se uma tríade de alvos elegíveis no ecossistema de aviação civil: infraestruturas críticas, sistemas críticos e plataformas críticas. Dentre as infraestruturas críticas, destacam-se os aeródromos e as instalações físicas do controle de tráfego aéreo. São exemplos de sistemas críticos aqueles destinados ao emprego comercial na gestão de passageiros e cargas, além daqueles relacionados ao controle de tráfego aéreo. As plataformas críticas são as aeronaves comerciais, cargueiras, privadas ou não tripuladas.

No campo teórico, são multitudinários os possíveis atores e motivações finalísticas de um ataque cibernético, por causa das subjetividades inerentes ao agente adverso que conduz a ação. Porém, é possível considerar categorias de atores motivados, tais como o crime organizado, as organizações ou atores terroristas e as nações hostis. As categorias detêm vicissitudes próprias. Na lição de Shulsky e Schmitt (2002), observar as distinções entre os atores motivados possibilita avaliar os indicadores para estruturar alerta preditivo apto ao assessoramento de inteligência.

Os atores motivados pelo crime organizado empregam sistematicamente o ambiente cibernético para o ilícito, atentos ainda à crescente convergência de suas ações com terroristas. Silva (2017, p. 153) destaca que

9 "Muitos sistemas operacionais comerciais são inauditáveis até o presente, uma vez que seus códigos-fonte não são disponibilizados pelos fabricantes. Sob tal análise, poder-se-ia inferir serem tais sistemas operacionais (ditos "fechados") ferramentas dotadas de eficácia potencial para emprego por forças armadas ou serviços de Inteligência adversos. Por exemplo, uma determinada chave criptográfica embutida secretamente em um sistema operacional poderia viabilizar o rompimento remoto de seus mecanismos naturais de segurança, como senhas e controle de portas lógicas. [...] Sistemas computacionais, mesmo aqueles pré-implantados e que não permitam a atualização de seu software, podem ser corrompidos com o passar do tempo. Classificam-se aqui, por exemplo, os equipamentos de controle empregados em aeronaves (denominados aviônicos), que são passíveis de ataques precedidos da infiltração por um programador especializado *(insider)*, ainda na fase de desenvolvimento" (BARRETO, 2007, p. 66 e 70).

"a exploração da aviação civil como vetor de atividades criminosas integra um conjunto de ameaças que demanda estreita interação com os órgãos de inteligência de segurança pública". A estratégia de segurança da aviação ianque aborda o crime organizado, a dimensão cibernética e a aviação civil (ESTADOS UNIDOS DA AMÉRICA, 2018a, p. 11, tradução nossa):

> Organizações criminosas transnacionais e outros criminosos afiliados rotineiramente buscam a assistência de funcionários da aviação simpáticos ou volúveis a facilitar o movimento ilícito de mercadorias ou pessoas. [...] Criminosos têm utilizado técnicas cibernéticas para atingir companhias relacionadas à aviação ao cometer crimes financeiros e empregar aeronaves não tripuladas para o tráfico, a vigilância e o reconhecimento de inteligência. Criminosos cibernéticos cometem crimes que têm como alvos redes e websites relacionados à aviação. As capacidades e motivações desse tipo de atores tornam difícil predizer seus alvos e o impacto de suas atividades. Ademais, o anonimato dos criminosos cibernéticos torna a atribuição de suas atividades extremamente complicada.

Para Barreto (2007, p. 63), o terrorismo cibernético é o "emprego, por terroristas, de técnicas de destruição ou incapacitação de redes computacionais de informação". Silva (2017, p. 152) anota que "ameaça terrorista pode se revestir de inúmeras condutas e abordar diversos alvos relacionados direta e indiretamente à aviação civil. De fato, os ativos da aviação civil poderão ser o alvo, o vetor e até a arma empregada na violência terrorista". Os atores e organizações motivadas pelo terrorismo adotam preferência histórica por alvos da aviação civil, cientes do impacto midiático e social. Uma tipologia possível de ataque terrorista cibernético percorre uma tríade de possibilidades: ataque técnico, destruição física ou pessoa infiltrada (BARRETO, 2007, p. 65-67). A probabilidade de terroristas realizarem ataques cibernéticos cresce com a evolução informacional das organizações terroristas. A estratégia da segurança da aviação estadunidense endossa a assertiva (ESTADOS UNIDOS DA AMÉRICA, 2018a, p. 10, tradução nossa):

> Terroristas continuam interessados em atacar o domínio da aviação como demonstrado no ataque do *Al-Shabaab a Daallo Airlines* (2016) e no ataque ao voo 9268 da *MetroJet* no Egito (2015), pelo qual ISIS assumiu responsabilidade. Ambos os ataques foram parcialmente assessorados pelo trabalho interno de radicalizados. Adicionalmente, os ataques catastróficos aos aeroportos de Bruxelas e Istambul (2016) demonstraram a intenção e a capacidade dos terroristas de atacar áreas públicas dos aeroportos, o que pode influenciar extremistas violentos domésticos a selecionar alvos similares.

O típico antagonismo entre as nações conduz à promoção de ataques exploratórios, com o objetivo de angariar vantagens na obtenção sub-reptícia de dados classificados. Silva (2017, p. 207) afirma que "o Brasil é um alvo substancial e conveniente para a exploração da inteligência econômica por atores de inteligências adversas, com especial enfoque na ameaça da espionagem industrial, bem como a obtenção de dados dos recursos naturais brasileiros". A exploração da fonte cibernética[10] é vulnerabilidade

10 A fonte cibernética é o "recurso por intermédio do qual se pode obter dados no Espaço Cibernético utilizando-se ações de busca ou coleta, normalmente realizadas com auxílio de ferramentas computacionais. A Fonte Cibernética poderá ser integrada a outras fontes (humanas, imagens e sinais) para produção de conhecimento de Inteligência" (BRASIL, 2015a, p. 119).

latente na espionagem industrial. Entre os meios para a consecução da espionagem industrial, evidencia-se a execução de ataque cibernético (ESTADOS UNIDOS DA AMÉRICA, 2018a, p.10-12):

> Nações já conduziram ataques cibernéticos e ciberespionagem contra alvos do ecossistema da aviação. [...] As nações tem cada vez mais visualizado as capacidades cibernéticas ofensivas como meios para avançar nos campos de objetivos militares, políticos e econômicos. [...] Nações hostis e outras entidades de inteligência usam o ecossistema da aviação para conduzir furtos de propriedade intelectual que custam enormes somas monetárias e criam ameaças profundas à nossa segurança nacional.

A CAPACIDADE DE AGIR E MÉTODOS DE ATAQUE: UM RASANTE CASUÍSTICO

Em julho de 2018, soube-se que manuais técnicos secretos do sistema de aeronaves remotamente pilotadas (SARP) militar MQ-9 *Reaper* estavam à venda na internet, pelo preço de cento e cinquenta dólares (MCLAUGHLIN, 2018). Em outubro de 2018, um cidadão chinês foi preso e deportado da Bélgica para os Estados Unidos. Um relatório técnico do FBI, após operação de contrainteligência, originou a acusação judicial de espionagem industrial e furto de segredos comerciais. O agente Xu Yanjun foi relacionado ao ministério da Segurança do Estado da China (MSS, na sigla em inglês). A denúncia à justiça alega que ele recrutava operacionalmente especialistas em patentes de motores de aeronaves comerciais. O principal alvo era a *GE Aviation,* uma das líderes mundiais no segmento (ESTADOS UNIDOS DA AMÉRICA, 2018b).

É também relevante a capacidade de agir da inteligência adversa em ataque cibernético, sintetizável em três pilares: acessibilidade do alvo, uso de artefato cibernético e emprego do poder cibernético. A acessibilidade do alvo depende de fatores ambientais e de segurança orgânica, que adentram a segurança da aviação civil *(security)*, estruturada em camadas. Recente vazamento de dados indica que a inteligência cubana pode haver recrutado operacionalmente servidores no aeroporto de Miami, para obter acesso a áreas restritas de segurança (HANKS e TORRES, 2019). Há múltiplos artefatos cibernéticos. Esse termo significa "equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataque cibernéticos" (BRASIL, 2015a, p. 37). Usar o poder cibernético é a meta de quem opera um artefato no ciberespaço. O poder cibernético é a "capacidade de utilizar o espaço cibernético para criar vantagens e eventos de influência neste e nos outros domínios operacionais e em instrumentos de poder" (BRASIL, 2015a, p. 211). Presume-se capaz de agir qualquer ator motivado que detenha acesso ao alvo, possua artefato cibernético e seja eficaz no uso do poder cibernético.

E quais são os métodos de ataques cibernéticos? Não há lista exaustiva ou definições unívocas, abundam variações terminológicas. Didaticamente, as ações no campo cibernético constituem medidas defensivas, medidas ofensivas e medidas exploratórias. São vários os métodos possíveis de ataque cibernético: a injeção

de *malware*[11], o ardil do *phishing*[12], o ataque de força bruta[13], o ataque de negação de serviço[14], o ataque de negação de serviço distribuído[15], a interferência por dissimulação de autenticidade no canal *(spoofing)*[16], a interferência por saturação e embaraço *(jammers)*[17], a extorsão criptográfica do *ransomware*, etc.

O desafio da proteção cibernética da aviação civil se amplifica diante das autoridades. Em agosto de 2013, um *jammer* do sistema de posicionamento global (GPS, na sigla em inglês) inadvertidamente usado por um caminhoneiro interferiu nas operações aéreas do aeroporto de Newark, atrapalhando sistemas de navegação aérea. Em junho de 2015, o aeroporto internacional de Varsóvia, capital da Polônia, sofreu ataque cibernético nos *softwares* que influenciam nos planos de voos das aeronaves, afetando milhares de passageiros. Em dezembro de 2016, a agência de aviação civil da Arábia Saudita padeceu de ataque cibernético que danificou vários computadores, apagando e roubando dados críticos (SILVA, 2017, p. 197, 199 e 203). Em abril de 2015, relatório de governança concluiu que a FAA deve abordar com maior abrangência a segurança cibernética nas evoluções do tráfego aéreo (ESTADOS UNIDOS DA AMÉRICA, 2015, p. 40). Entre outros exemplos relacionados às infraestruturas críticas além da aviação, a DNAI indica os ataques cibernéticos aos sistemas governamentais da Estônia em 2007 e da Geórgia em 2008, o uso do *Stuxnet* em 2010 contra a infraestrutura nuclear no Irã e os vazamentos de dados da Agência Nacional de Segurança dos EUA (NSA, na sigla em inglês) promovidos por Edward Snowden em 2013 (BRASIL, 2016a, p. 64). Em 2014, ataque cibernético danificou a indústria siderúrgica alemã ao desligar inopinadamente

11 O termo *malware* relaciona-se ao "ataque cibernético que consiste em infiltrar programas nocivos ou maliciosos em computadores e sistemas do(s) alvo(s). Com o programa infiltrado, o atacante pode corromper ou alterar sistemas, provocar danos e até mesmo roubar informações" (OLIVEIRA et al, 2017, p. 6).

12 O *phishing*, termo que remete à "pescaria", é "ataque cibernético utilizado na prática de fraudes. Esse ataque ocorre de diferentes formas, com uso técnico de informática ou apenas estratagemas que levam os alvos a se comprometerem. Em virtude disso, ele pode ser utilizado tanto para ofensivas contra a segurança cibernética, quanto para afetar a defesa cibernética de um país" (OLIVEIRA et al, 2017, p. 6).

13 O ataque de força bruta *(brute force attack)* ocorre quando "o atacante adivinha, por tentativa e erro, um nome de usuário e sua respectiva senha, permitindo-lhe executar processos e acessar sites, computadores e serviços com o mesmo nome e privilégios do usuário alvo do ataque" (BRASIL, 2015a, p. 39).

14 O ataque de negação de serviço (*denial of service* – DOS) ocorre quando "um atacante utiliza um computador ou dispositivo móvel conectado a uma rede ou à Internet para inundar um servidor em uma determinada rede com um número excessivo de solicitações de modo a tirar de operação um serviço por sobrecarga" (BRASIL, 2015a, p.39).

15 O ataque de negação de serviço distribuído (*distributed denial of service* – DDOS) ocorre quando "o ataque é lançado simultaneamente por um grande número de computadores escravos, atuando em rede, controlados por um atacante mestre por meio de infecção prévia (*vírus, worms*) de modo a aumentar consideravelmente sua eficácia na paralisação de um determinado serviço por sobrecarga" (BRASIL, 2015a, p. 39).

16 "Tipo de ataque em rede de dados em que um elemento da rede falsifica dados para se fazer passar por outro elemento da rede e, assim, obter algum tipo de vantagem" (BRASIL, 2016c, p. 292).

17 Os *jammers* são transmissores ilegais de frequências de rádio, planejados para bloquear, embaraçar ou interferir em comunicações de rádio autorizadas (ESTADOS UNIDOS DA AMÉRICA, 2011b, p. 2).

maquinário de usinagem (BBC, 2014). Em 2015, o Exército Brasileiro foi alvo de ataque cibernético, resultando em vazamento de dados (OLIVEIRA et al, 2017, p. 66). Em junho de 2017, anomalia foi reportada pela Administração Marítima americana (MARAD, na sigla em inglês) (ESTADOS UNIDOS DA AMÉRICA, 2017). Consistia no embaraço eletromagnético de GPS na região do mar Negro, estratégica à influência político-militar russa, prejudicando sistemas que evitam a colisão entre navios. Análises especializadas posteriores dão conta da deliberação do incidente, similar a ataque cibernético de *spoofing* (GOWARD, 2017). Em teoria, os ataques cibernéticos citados são adaptáveis contra alvos na aviação civil. A escassa produção científica sobre riscos cibernéticos contra tal ecossistema, isoladamente, já deveria inquietar a inteligência da aviação civil. O conjunto de amostras casuísticas traça devir de ameaças reais e potenciais exploráveis por atores motivados e capazes, que podem englobar, eventualmente, ações de inteligências adversas.

Derivam da Agência de Segurança de Redes e Informações da União Europeia (ENISA) possíveis soluções perante os ataques cibernéticos, na forma de guia de boas práticas na implementação de estratégias de segurança cibernética[18] (ENISA, 2016). Os objetivos das boas práticas estão organizados em quatro grupos: estruturação, capacitação, cooperação e fomento. Quanto à estruturação, recomenda-se desenvolver planos nacionais de contingência cibernética, proteger informações de infraestruturas críticas, estabelecer linha basal de medidas de segurança, estabelecer mecanismos de comunicação de incidentes, estabelecer capacidade de resposta a incidentes, balancear segurança e privacidade e tratar os crimes cibernéticos. Entre as boas práticas de capacitação, é preciso fortalecer treinamentos e programas educacionais, aumentar a consciência do usuário e organizar exercícios de segurança cibernética. No grupo de cooperação, é recomendável institucionalizar cooperação entre agências públicas, engajar-se na cooperação internacional e estabelecer parcerias público-privadas. Finalmente, nas boas práticas de fomento, é preciso incentivar o setor privado a investir em medidas de segurança e promover a pesquisa e desenvolvimento (ENISA, 2016, p. 23-39).

Considerações finais

O panorama ora estruturado e a experiência histórica apontam que o ecossistema da aviação civil é alvo primário de diversos atores motivados, com variados objetivos finalísticos, relacionáveis à ameaça de ataque cibernético. Embora os paradigmas comparativos auxiliem a compreensão da ameaça, não podem ser adotadas soluções por espelhamento. A título de exemplo, a realidade da inserção brasileira no horizonte de ameaças é distinta e peculiar em relação à realidade estadunidense. A Estratégia Nacional de Inteligência (ENINT) define o eixo estruturante da tecnologia e capacitação, donde sobressai objetivo estratégico crucial à mitigação da ameaça: "ampliar a capacidade do Estado na obtenção de dados por meio da Inteligência cibernética" (BRASIL, 2017,

18 O título original do documento em língua inglesa é: *NCSS good practice guide: designing and implementing national cyber security strategies.*

p. 26). A DNAI divisa o caminho para tal maturidade (BRASIL, 2016a, p. 64):

> Os procedimentos tradicionais da Atividade de Inteligência executados na realidade física estendem-se à realidade virtual. A segurança cibernética não se fundamenta apenas na prevenção e no enfrentamento de ameaças, mas também na antecipação da identificação de intenções e potencialidades de adversários. Ataques cibernéticos implicam atividades que se situam além da rede em si, uma vez que se inserem em questões concorrenciais, geralmente de caráter político e econômico. Há, portanto, uma dimensão humana que não pode ser negligenciada em face dos dados técnicos; o técnico e o comportamental devem ser justapostos no estudo de cada situação.

Aprofundar os conhecimentos existentes sobre a ameaça cibernética na aviação civil, fomentando ações de contrainteligência, é o primeiro passo para incrementar a resiliência cibernética. Na esfera executiva, o início de uma solução factível demanda a interação da atividade de inteligência da aviação civil com órgãos de defesa cibernética instituídos. O ataque cibernético é ameaça extremamente dinâmica, e a casuística corrobora a pluralidade de métodos. É imprescindível a constante atualização nos estudos para mitigar sua ocorrência, especialmente, devido ao despreparo de parte da mão de obra da aviação face à ameaça. É inconteste que a aviação evoluiu sobretudo por meio da investigação de falhas em acidentes e incidentes aeronáuticos, ou seja, de enfoque reativo. A inteligência tem foco preditivo, devendo antecipar-se à recente ameaça cibernética aos ecossistemas da aviação civil. Pelos elementos colecionados, é possível retomar a iniciativa, propondo evolução intermediada pela criação de política de mitigação de riscos relacionados à ameaça cibernética na aviação civil, antes de suportar tragédias decorrentes de omissão. Para tanto, demandam-se análises estruturadas de cenários específicos (HEUER e PHERSON, 2016), contextualizadas aos alvos elegíveis da aviação civil, que considerem os métodos de ataque, os atores motivados e suas respectivas capacidades de agir e gerem indicadores e alertas aptos à assessoria do processo decisório.

Referências

BBC News. *Hack attack causes 'massive damage' at steel works*. Londres: British Broadcast Corporation, 2014. Disponível em: https://www.bbc.com/news/technology-30575104. Acesso em: 20 jul. 2019.

BARBOSA DA COSTA, Carlos Eduardo. Tendências mundiais e seus reflexos para a defesa brasileira. *Revista Brasileira de Inteligência*, Brasília, v. 7, p. 54-66, 2012.

BARRETO, Eduardo Müssnich. Terrorismo Cibernético e cenários especulativos. *Revista Brasileira de Inteligência*, Brasília, v. 4, p. 63-76, 2007.

BETTS, Richard K. *Enemies of intelligence:* knowledge and power in American national security. New York: Columbia University Press, 2007.

BRASIL. Lei n° 11.182, de 27 de setembro de 2005. Cria a Agência Nacional de Aviação Civil – ANAC. *Diário Oficial da União:* seção 1, Brasília, DF, 28 set. 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11182.htm. Acesso em: 12 maio 2019.

_____. Presidência da República. Gabinete de Segurança Institucional. *Livro verde:* segurança cibernética no Brasil. Brasília: Departamento de Segurança da Informação e Comunicações, 2010. Disponível em: <http://dsic.planalto.gov.br/legislacao/1_Livro_Verde_SEG_CIBER.pdf/view >. Acesso em: 10 maio 2019.

_____. Ministério da Defesa. *Política Nacional de Defesa e Estratégia Nacional de Defesa*. Brasília: Ministério da Defesa, 2012. Disponível em: https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf. Acesso em: 01 maio 2019.

_____. Ministério da Defesa. Portaria normativa nº9/GAP/MD, de 13 de janeiro de 2016. Aprova o Glossário das Forças Armadas – MD35-G-01 (5ª.edição/2015). Brasília: 2015a. Disponível em: http://bdex.eb.mil.br/jspui/bitstream/123456789/141/1/MD35_G01.pdf. Acesso em: 11 maio 2019.

_____. Ministério da Defesa. Exército Brasileiro. Portaria nº032-EME, de 23 de fevereiro de 2015. Aprova o manual de campanha EB20-MC-10.207 Inteligência, 1ª.ed. *Boletim do Exército*, Brasília, n.9, 27 fev. 2015b. Disponível em: http://bdex.eb.mil.br/jspui/bitstream/1/2595/1/EB20-MC-10.207.pdf. Acesso em: 16 jul. 2019.

_____. Presidência da República. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Doutrina Nacional da Atividade de Inteligência:* fundamentos doutrinários. Aprovada pela Portaria nº 244 - ABIN/GSI/PR, de 23 de agosto de 2016. Brasília: ABIN,

2016a.

_____. Decreto nº 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. *Diário Oficial da União:* seção 1, Brasília, DF, 30 jun. 2016b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm. Acesso em: 01 maio 2019.

_____. Ministério da Justiça. Polícia Federal. *Glossário de ciências forenses:* termos técnicos mais usados pela perícia criminal federal. Brasília: Diretoria Técnico Científica, 2016c.

_____. Presidência da República. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Estratégia Nacional de Inteligência.* Brasília: Abin, 2017a. Disponível em: http://www.abin.gov.br/conteudo/uploads/2015/05/ENINT.pdf. Acesso em: 01 maio 2019.

_____. Decreto n° 9.209, de 27 de novembro de 2017. Altera o Decreto n º 4.376, de 13 de setembro de 2002, que dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei n º 9.883, de 7 de dezembro de 1999. *Diário Oficial da União:* seção 1, Brasília, DF, 28 nov. 2017b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Lei/L11182.htm. Acesso em: 12 maio 2019.

BOEING. *Boeing Statement On Ethiopian Airlines Flight 302 Investigation Preliminary Re*port. Chicago: 2019. Disponível em: https://boeing.mediaroom.com/2019-04-04-Boeing-Statement-On-Ethiopian-Airlines-Flight-302-Investigation-Preliminary-Report. Acesso em: 15 jul. 2019.

BRUZZEGUEZ, Gustavo A.; NEUMANN, Clóvis; SOUZA, João Carlos F. O hardware comprometido: uma importante ameaça a ser considerada pela atividade de inteligência. *Revista Brasileira de Inteligência*, Brasília: Abin, v. 13, p. 113-127, 2018.

CHEREM, João Carlos dos Santos. *Infraestrutura de transportes e o preparo da mobilização nacional.* Rio de Janeiro: ESG, 2011.

European Union Agency for Cybersecurity. *NCSS good practice guide: designing and implementing national cyber security strategies.* ENISA: 2016. Disponível em: https://www.enisa.europa.eu/publications/ncss-good-practice-guide. Acesso em 18 jul. 2019.

ESTADOS UNIDOS DA AMÉRICA. The President of United States. *Report of the President's Commission on Aviation Security and Terrorism.* Washington, D.C.: 1990. Disponível em: http://www.policyfutures.com/PCAST/PCASTreport.pdf. Acesso em: 11 maio 2019.

_____. National commission on terrorist attacks upon the United States - public law 107-306. *The 9/11 commission report.* National commission on terrorist attacks upon the

United States, 2004. Disponível em: https://9-11commission.gov/report/911Report.pdf. Acesso em: 11 maio 2019.

_____. Department of Defense. *Instruction number 3115*.14. United States Department of Defense, 29 jul. 2011a. Disponível em: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/311514p.pdf. Acesso em: 12 jul. 2019.

_____. Federal Communications Commission. *GPS, Wi-Fi, and Cell Phone Jammers:* frequently asked questions (FAQs). Federal Communications Commission, 2011b. Disponível em: https://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf. Acesso em: 20 jul. 2019.

_____. United States Government Accountability Office. *Air traffic control* – FAA needs a more comprehensive approach to address cybersecurity as agency transitions to NextGen (report to congressional requesters). United States Government Accountability Office, 2015. Disponível em: https://www.gao.gov/assets/670/669627.pdf. Acesso em: 20 jul. 2019.

_____. United States Departament of Transportation. *MSCI Alert: 2017-005A-Black Sea-GPS Interference*. United States Departament of Transportation. Maritime Administration (MARAD), 2017. Disponível em: https://www.maritime.dot.gov/content/2017-005a-black-sea-gps-interference. Acesso em: 20 jul. 2019.

_____. The President of United States. *National Strategy for Aviation Security of the United States of America*. Washington, D.C.: 2018a. Disponível em: https://www.whitehouse.gov/wp-content/uploads/2019/02/NSAS-Signed.pdf. Acesso em 18 maio 2019.

_____. Department of Justice. Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies. *Justice News*. Washington, D.C, 10 oct. 2018b. Disponível em: https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading. Acesso em 15 jul. 2019.

GOWARD, Dana A. GPS spoofing incident points to fragility of navigation satellites – "National Defense". Resilient Navigation and Timing Foundation, 23 aug. 2017. Disponível em: https://rntfnd.org/2017/08/23/gps-spoofing-incident-points-to-fragility-of-navigation-satellites-national-defense/. Acesso em: 20 jul. 2019.

HERMAN, Michael. *Intelligence power in peace and war*. Cambridge, UK: Cambridge University Press, 1999.

HEUER, Richards J. Jr; PHERSON, Randolph H. *Structured analytic techniques for intelligence*

analysis. CQ Press, 2016. Kindle edition. Paginação irregular.

HANKS, Douglas; TORRES, Nora Gámez. *Report:* Cuban spy documents target security at Miami's airport. MIA says no breach. Miami Herald, 2019. Disponível em: https://www.miamiherald.com/news/local/community/miami-dade/article231133238.html. Acesso em: 20 jul. 2019.

MCLAUGHLIN, Jenna. US Reaper drone data leaked on dark web, researchers say. *CNN politics,* 10 jul. 2018. Disponível em: https://edition.cnn.com/2018/07/10/politics/us-reaper-drone-materials-hacker-theft/index.html. Acesso em: 10 jul. 2019.

OLIVEIRA, Marcos A. Guedes, et al. *Guia de Defesa Cibernética na América do Sul.* Recife: Ed. UFPE, 2017. Disponível em: https://pandia.defesa.gov.br/images/acervodigital/GuiaDefesaCiberneticaAmericaSul.pdf. Acesso em: 21 jul. 2019.

SILVA, Mateus Vidal Alves. *Ações de inteligência na produção de conhecimentos da autoridade de aviação civil.* 2017. Trabalho de Conclusão do Curso (Especialização em Inteligência de Estado e Inteligência de Segurança Pública – INASIS 2016-2017) – Associação Internacional para Estudos de Segurança e Inteligência, Faculdades Milton Campos, Nova Lima, 2017.

SINGER, Peter Warren; FRIEDMAN, Allan. *Segurança e guerra cibernéticas:* o que todos precisam saber. Rio de Janeiro: Biblioteca do Exército, 2017.

SHULSKY, Abram N.; SCHMITT, Gary J. *Silent warfare:* understanding the world of intelligence. 3. ed. Washington, DC: Potomac Books, 2002. Kindle edition. Paginação irregular.