ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO AVANÇADO DE COMANDO E ESTADO-MAIOR

JEFFERSON **CASTELANO** TAVARES, Maj Av

Guerra cibernética e guerra centrada em rede: uma visão teórica da influência cibernética nas ações de Força Aérea

Rio de Janeiro
2022

ESCOLA DE COMANDO E ESTADO-MAIOR DA AERONÁUTICA
COORDENADORIA ACADÊMICA
CURSO AVANÇADO DE COMANDO E ESTADO-MAIOR

JEFFERSON **CASTELANO** TAVARES, Maj Av

Guerra cibernética e guerra centrada em rede: uma visão teórica da influência cibernética nas ações de Força Aérea

Trabalho de conclusão de curso apresentado, como requisito parcial para aprovação, no Curso Avançado de Comando e Estado-Maior.
Linha de Pesquisa: Poder Aeroespacial.
Orientador: Heráclito Moreira de Souza

.

Rio de Janeiro
2022

AGRADECIMENTOS

Agradeço primeiramente ao Grande Arquiteto do Universo por conceder-me a oportunidade de lapidar a pedra bruta dos meus conhecimentos, aos meus pais e familiares que tiveram paciência em meus dias ausentes, ao meu orientador pela eficácia na correção e auxílio da formatação desta pesquisa e, em especial, ao Ten Cel Av Tiago Josue Diedrich que dispôs de seu tempo, em grande parte nos finais de semana e feriados, para auxiliar-me na busca de linhas de ação em prol de materializar os conceitos e entendimentos no conteúdo desta pesquisa.

RESUMO

Essa pesquisa busca analisar em que medida a guerra cibernética exerce influência em uma rede teórica de ações de Força Aérea em 2022 à luz da teoria da guerra centrada em rede. Inicialmente são descritos os conceitos da guerra cibernética. Para, em seguida, reconhecer a relação existente entre a guerra cibernética e as ações de Força Aérea à luz da guerra centrada em rede. E, por fim, processar os dados coletados e analisar a influência das ações cibernéticas em uma rede teórica de ações de Força Aérea em 2022. Após a análise dos dados, verificou-se que, em uma escala de 1 a 5, a guerra cibernética alcançou um valor de aderência de 3,6 em relação à guerra centrada em rede. Além de ser identificada uma correlação de 34,66%, 82,18% e 85,60% das ações de ataque, proteção e exploração cibernética, respectivamente, com a rede teórica. Conclui-se, portanto, que a permeabilidade das ações de Força Aérea ao domínio cibernético, apesar de ser positiva, está distante do seu potencial máximo, evidenciando a lacuna que pode ser explorada por parte do inimigo para se obter uma posição de vantagem, o que está alinhado à teoria da guerra centrada em rede e ao entendimento doutrinário de que o domínio cibernético pode potencializar o uso de uma rede ou degradá-la. Por derradeiro, esta pesquisa descritiva faz uso do método indutivo, correlacionando as ideias e teorias de autores em busca de conclusões mais amplas.

Palavras-chave: ações cibernéticas; ações de Força Aérea; guerra centrada em rede; guerra cibernética.

ABSTRACT

This research analyzes how cyber warfare influences a theoretical network of Air Force actions in 2022 based on network-centric warfare theory. Initially, the concepts of cybernetics warfare are described. Next, the relationship between cyber warfare and Air Force actions in the light of network-centric warfare is recognized. Finally, the collected data are analyzed to verify the influence of cyber actions on a theoretical network of Air Force actions in 2022. After analyzing the data, it was found that, on a scale of 1 to 5, cyber warfare achieved an adherence value of 3.6 relative to the proposed network-centric warfare. In addition, a correlation of 34.66%, 82.18% and 85.60% of cyberspace attack, cyberspace protection and cyberspace exploitation, respectively, with the theoretical network was identified. It is concluded, therefore, that the permeability of Air Force actions to the cyber domain, despite being positive, is far from its maximum potential, evidencing the gap that can be exploited by the enemy to obtain a position of advantage, being aligned with the network-centric warfare theory and with the doctrinal understanding that the cyber domain can enhance the use of a network or degrade it. Finally, this descriptive research makes use of the inductive method, correlating the ideas and theories of authors looking for broader conclusions.
Keywords*: Air Force actions; cyber actions; cyber warfare; network-centric warfare.*

LISTA DE ILUSTRAÇÕES

Figura 1 – Representação ilustrativa do potencial de uma rede de 3 Nós (3 x 2 = 6) 15
Figura 2 – Representação ilustrativa de uma infiltração cibernética em um F-22 24

Quadro 1 – Quadro de correlação das denominações segundo a DMDC 20

LISTA DE TABELAS

Tabela 1 – Amostra das respostas ao questionário 28
Tabela 2 – Ações de Força Aérea dentro da faixa de concordância 29
Tabela 3 – Valor potencial das ações cibernéticas em relação à GCR teórica 29
Tabela 4 – Amostra da soma das ações cibernéticas para cada ação de Força Aérea 30
Tabela 5 – Respostas ao questionário. 62
Tabela 6 – Soma das ações cibernéticas para cada ação de Força Aérea. 66
Tabela 7 – Ações de Força Aérea 68

LISTA DE ABREVIATURAS E SIGLAS

AFA	Ação de Força Aérea
C4ISR	Comando, Controle, Comunicações e Computadores, Informações, Vigilância e Reconhecimento
CCA-BR	Centro de Computação da Aeronáutica de Brasília
ComDCiber	Comando de Defesa Cibernética
DBFAB	Doutrina Básica da Força Aérea Brasileira
DMDC	Doutrina Militar de Defesa Cibernética
DP	Desvio Padrão
END	Estratégia Nacional de Defesa
ESP	Especialista
FAB	Força Aérea Brasileira
GCR	Guerra Centrada em Rede
NuCDCAER	Núcleo do Centro de Defesa Cibernética da Aeronáutica
PEMAER	Plano Estratégico Militar da Aeronáutica
SCTIC2	Sistemas de Comunicações e Tecnologia da Informação para Comando e Controle
SISDABRA	Sistema de Defesa Aeroespacial Brasileiro
SMDC	Sistema Militar de Defesa Cibernética
STIC2	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
TIC	Tecnologia da Informação e Comunicações

SUMÁRIO

1 INTRODUÇÃO 9
1.1 Problema 10
1.2 Objetivos geral e específico 10
1.3 Justificativa do estudo 11
2 METODOLOGIA 11
3 REFERENCIAL TEÓRICO 14
3.1 Guerra centrada em rede 14
3.2 Cibernética 17
4 APRESENTAÇÃO DOS DADOS E ANÁLISE DOS RESULTADOS 20
4.1 Guerra cibernética 20
4.2 Vulnerabilidades cibernéticas 22
4.3 Aeronaves 24
4.4 Correlação doutrinária das ações 25
4.5 Resultados gerais 28
5 CONCLUSÃO 31
REFERÊNCIAS 33
APÊNDICE A – Questionário 36
APÊNDICE B – Respostas ao questionário 62
APÊNDICE C – Soma das ações cibernéticas para cada ação de Força Aérea 66
ANEXO A – Ações de Força Aérea 68

1 INTRODUÇÃO

O desenvolvimento de tecnologias de guerra é uma condição básica para qualquer país se colocar de forma persuasiva no contexto militar internacional, isso pode ser observado como uma forma a auferir vantagem dissuasória e garantir a própria soberania.

Nesse sentido, a área cibernética tem se mostrado um significativo campo de atuação para a guerra moderna e, apesar do termo ter sido levado a conhecimento acadêmico na década de 1940, tomou seu local de relevância na atualidade com a evolução da computação, ao passo que, para o leigo, é facilmente associado aos *hackers*. Porém, esse assunto vem se tornando pauta relevante para as potências bélicas e a especialização das Forças Armadas no campo da cibernética vem se tornando um fator de primeira necessidade.

Decorrente disso, as operações militares internalizaram os avanços e as vantagens da tecnologia, mudando sua concepção de guerra convencional, onde os atores no teatro de operações possuíam baixa consciência situacional das evoluções do combate e levavam muito tempo para se ajustarem às mudanças e evoluções, para uma visão de um ecossistema em rede no qual a contínua adaptação traria vantagens táticas e operacionais. A essa abordagem de guerra onde diversos atores estão interconectados foi dado o nome de guerra centrada em rede (GCR) do inglês *Network Centric Warfare* (CEBROWSKI; GARSTKA, 1998).

A inter-relação das duas teorias fica evidente quando tratamos da troca de informação. Por um lado, a guerra centrada em rede objetiva em grande parte obter vantagem no teatro de guerra aumentando os pontos de conexão da rede, por outro lado, existe a cibernética com sua capacidade de interagir com esse ambiente, às vezes potencializado seu uso outras vezes expondo sua fragilidade.

Em 2000 o Tenente Coronel Lionel Alford publicou um artigo intitulado *Cyber Warfare: Protecting Military Systems* levantando pontos de atenção sobre as vulnerabilidades das aeronaves que possuíam programas como um elemento chave de fluxo de informação, afirmando que o desempenho e capacidade das aeronaves dependiam, e dependerão, cada vez mais de sistemas integrados para o controle automatizado da informação, abrindo caminho para a cibernética dentro do poder aéreo (ALFORD, 2000).

Levando em consideração as perspectivas de Cebrowski e Garstka (1998), sobre a GCR, e Alford (2000) sobre a cibernética, podemos observar dois pontos relevantes para discussão.

Primeiro, a Força Aérea Brasileira (FAB) não está distante da compreensão da magnitude dessas afirmações, pois o Plano Estratégico Militar da Aeronáutica (PEMAER) destaca a importância do desenvolvimento do Projeto LINK-BR2, que consiste no

desenvolvimento de um protocolo que permite interconectar diferentes tipos de meios de combate por intermédio de enlace de dados em rede trocando informações entre si, sejam eles aéreos, terrestres ou marítimos (BRASIL, 2018).

Segundo, que políticas foram trabalhadas para que o Ministério da Defesa se alinhasse com os fundamentos elencados na Estratégia Nacional de Defesa (END), no sentido de direcionar recursos para setores tecnológicos essenciais para a Defesa Nacional, como é o caso do cibernético (BRASIL, 2018). Assim, foi criando o Sistema Militar de Defesa Cibernética (SMDC), tendo como órgão central o Comando de Defesa Cibernética (ComDCiber), comando operacional composto por militares do Exército, Marinha e Aeronáutica. Não obstante a isso, a FAB aprovou em 2020 a diretriz que dispõe sobre a implantação do Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER) no Centro de Computação da Aeronáutica de Brasília (CCA-BR) para tratar de assuntos afetos a essa temática.

Baseado nessa perspectiva, esse trabalho buscou explorar o estado atual da cibernética na FAB, levando em conta sua relação com a teoria da GCR e as ações de Força Aérea, tudo isso balizado pelos conceitos de ambas as teorias e pela doutrina atual.

1.1 Problema

Nesse contexto, fazendo um paralelo das ideias apresentadas anteriormente com às diretrizes elencadas para as Forças Armadas Brasileiras na END, surgiu a inquietação nesse pesquisador a respeito da FAB e seus meios de combate operando em um ambiente conectado e de interesse para o domínio cibernético, de modo que possibilitou a formulação da seguinte pergunta de pesquisa: em que medida a guerra cibernética exerce influência em uma rede teórica de ações de Força Aérea, em 2022, à luz da teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da doutrina básica da Força Aérea?

1.2 Objetivos geral e específico

Diante da relevância que o assunto possui para o desenvolvimento tecnológico das Forças Armadas, foi imperativa uma investigação bibliográfica para coletar as informações em busca de respostas que atendessem, com critérios científicos, o questionamento apresentado, sendo necessário direcionar este trabalho para atingir o seu objetivo geral de analisar em que medida a guerra cibernética exerce influência em uma rede teórica de ações de Força Aérea,

em 2022, à luz da teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da doutrina básica da Força Aérea.

Assim, a investigação segue o objetivo específico inicial de descrever os conceitos da guerra cibernética. Para, em seguida, reconhecer a relação entre a guerra cibernética e as ações de Força Aérea à luz da teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da doutrina básica da Força Aérea. E, finalmente, analisar a influência das ações cibernéticas em uma rede teórica de ações de Força Aérea em 2022.

1.3 Justificativa do estudo

O assunto é dotado de relevância pois trata de um panorama atual da guerra moderna que é o domínio cibernético. Além disso, a necessidade de constante aprimoramento tecnológico leva em conta que a exploração dos sistemas de informação computadorizados podem prover uma superioridade no campo de batalha, onde a balança da força pende a favor de quem mantém seu desenvolvimento tecnológico em constante atualização.

Outro ponto relevante é que as pesquisas acadêmicas, voltadas para a cibernética e associada ao combate, têm se tornado relevantes para o entendimento dos conflitos modernos, fazendo com que estudos nessa área sejam promissores para o desenvolvimento de conhecimentos que possam balizar as doutrinas militares.

2 METODOLOGIA

O trabalho descreve a teoria da guerra centrada em rede segundo Alberts, Garstka e Stein (2000) e da cibernética de Wiener (1970), relacionando-as ao emprego do poder aeroespacial.

O advento da cibernética se deu impulsionado pela relevância do poder aéreo na segunda guerra mundial, pois o termo cibernética, cunhado por Norbert Wiener em 1948 em seu livro intitulado cibernética, foi usado para tratar do desenvolvimento de mecanismos destinados a regular automaticamente canhões de artilharia, na tentativa de abater aeronaves de forma mais eficiente e automatizada. Assim, a palavra cibernética, derivada da palavra grega *kubernetes*, ou piloto, mesma palavra grega que deriva a palavra governador, foi empregada por Wiener para descrever sistemas que usam aparatos mecânicos ou eletrônicos para substituir o controle humano (WIENER, 1970).

O termo *Network Cenrtric Warfare* aparece a primeira vez alguns anos depois, em 1997 no artigo DOD *lays groundwork for network-centric warfare* de Bob Brewin, falando sobre a gestão de redes de informação das forças armadas americanas. Porém, tomou relevância em 1998 com o artigo intitulado *Network-Centric Warfare: Its Origin and Future* de autoria do Vice-Almirante Arthur Cebrowski e de John Garstka (EUGÉNIO, 2008).

A base para a descrição do uso da cibernética no ambiente aéreo foi o artigo de Alford (2000) publicado na *Acquisition Review Quarterly*, *Spring 2000*, e o relatório GAO-19-128 do *United States Government Accountability Office* (GAO) ao *Committee on Armed Services, U.S. Senate*, de 2018. Tanto o artigo quanto o relatório apresentam as preocupações a respeito das possíveis ameaças cibernéticas às aeronaves de combate.

Já a correlação teórica da GCR foi baseada no livro de David S. Alberts, John J. Garstka e Frederick P. Stein, intitulado *Network centric warfare: developing and leveraging information superiority*, publicado em 1999 tendo sua segunda edição revisada em 2000.

A apresentação dos dados está estruturada com base em seus objetivos específicos, seguindo uma sequência de ideias concatenadas de modo a encontrar resposta para o problema de pesquisa proposto.

Primeiramente, são descritos os conceitos da guerra cibernética, trazendo à consciência os conhecimentos relativos às ações cibernéticas constantes na doutrina básica da Força Aérea Brasileira e doutrina militar de defesa cibernética que permeiam as teorias trabalhadas nessa pesquisa, de forma a promover o entendimento inicial e posterior compreensão específica do problema abordado.

Essa revisão de literatura também engloba a doutrina básica da Força Aérea Brasileira (DBFAB), doutrina militar de defesa cibernética (DMDC), artigos científicos publicados com temas voltados à cibernética e guerra cibernética, e a doutrina norte-americana atual, bem como conteúdo de livros e artigos científicos publicados em periódicos na internet utilizando as seguintes palavras-chaves: guerra cibernética; ações cibernéticas; vulnerabilidade cibernética; e guerra centrada em rede.

Em seguida, é feita uma breve revisão bibliográfica sobre as vulnerabilidades cibernéticas associadas às aeronaves, bem como dos conceitos doutrinários das tarefas e ações de Força Aérea, de forma a estruturar o conhecimento de maneira lógica para reconhecer a relação entre a guerra cibernética e as ações de Força Aérea à luz da teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da doutrina básica da Força Aérea.

Posteriormente, é analisada a influência das ações cibernéticas em uma rede teórica de ações de Força Aérea em 2022, realizando uma avaliação dos dados e resultados extraídos das literaturas e das respostas ao questionário enviado a especialistas em cibernética.

Nessa análise, a pesquisa propõe uma abordagem do ponto de vista teórico das capacidades percebidas pelos especialistas em cibernética, levando em consideração a aplicabilidade das ações cibernéticas em cada ação de Força Aérea (AFA). Assim, é verificada a interação do domínio cibernético na GCR, em termos teóricos, no que tange às ações cibernéticas e ações de Força Aérea descritas na DBFAB e DMDC, respectivamente.

Além disso, das 55 ações de Força Aérea, constantes na DBFAB, foram elencadas 54 excetuando-se a ação de defesa cibernética que é abordada do ponto de vista da guerra cibernética.

Os valores numéricos foram obtidos a partir de um questionário enviado a especialistas na área de cibernética com dois anos ou mais de experiência e aos integrantes do NuCDCAER, de modo a ser possível correlacionar as ações cibernéticas e sua aplicabilidade em uma rede teórica de ações de Força Aérea.

O questionário abrangeu sete especialistas em cibernética e contou com 54 perguntas contendo três questões a respeito das ações cibernéticas, gerando uma coleta de dados contendo 1134 respostas.

As perguntas visaram à percepção sobre a aplicação de cada ação cibernética nas ações de Força Aérea (cada AFA está listada no Anexo A com seu respectivo designativo e numerada de 1 a 54). Essa percepção foi graduada de 1 a 5, onde 1 equivale a discordar totalmente e 5 concordar totalmente. Dessa forma, foi possível mensurar o grau de concordância na aplicação da guerra cibernética em todo o leque doutrinário das ações de Força Aérea.

Para cada ação de Força Aérea havia uma descrição, conforme DBFAB, seguida das ações cibernéticas (ataque, proteção e exploração) com as respectivas opções de seleção dentro do espectro de 1 a 5, sendo possível selecionar apenas um desses valores.

O valor 3 foi considerado como sendo o ponto de corte para analisar os graus de concordância. As avaliações abaixo desse valor foram interpretadas como discordância e avaliações igual ou acima disso como concordância. Isso também foi levado em consideração para interpretar as médias das avaliações.

Por fim, o último passo é a conclusão, que apresenta de forma sucinta todas as etapas deste estudo, juntamente com seus resultados.

Vale pontuar que o trabalho apresenta três limitações. A primeira é associada às capacidades cibernéticas para uma GCR. A FAB se encontra na fase inicial de criação de um

Centro de Defesa Cibernética e ainda não possui as capacidades reais que possam ser medidas, devido a isso foi necessária a aplicação do questionário para gerar os valores de análise. Outra questão é relativa ao tamanho da população envolvida, que se baseou na resposta de apenas sete pessoas. Acredita-se que, com o passar dos anos, o número de especialistas em cibernética no âmbito da FAB cresça, o que pode propiciar uma coleta de dados mais robusta para trabalhos futuros. A última, e não menos importante, é a ausência de estudos conjugando a guerra centrada em rede e a guerra cibernética no âmbito da Defesa Nacional.

3 REFERENCIAL TEÓRICO

Este capítulo discorre sobre as teorias da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da cibernética de Wiener (1970), teorias que estão intimamente ligadas quando tratamos da troca de informação. Primeiramente é apresentada a teoria cibernética com sua capacidade de interagir com o ambiente conectado.

3.1 Guerra centrada em rede

A revolução da informação juntamente com as mudanças econômicas tornou possível as organizações evoluírem e se tornarem dominantes em suas respectivas áreas de atuação, baseando-se na dinâmica competitiva focada em rede e na visão de um ecossistema em contínua adaptação. Consequentemente, o domínio da guerra também acompanhou essas evoluções (ALBERTS; GARSTKA; STEIN, 2000).

Baseado nessa percepção, Alberts, Garstka e Stein (2000) teorizaram o conceito de guerra centrada em rede propondo a evolução da guerra convencional para uma que englobasse a conexão dos atores envolvidos por meio da troca de informação de forma rápida, permitindo uma mudança na maneira de fazer o combate para algo mais fácil e eficaz. Assim, a GCR veio para potencializar a adaptação às mudanças, garantindo vantagens para quem explora a superioridade da informação.

Segundo Alberts, Garstka e Stein (2000) a GCR se concentra nos benefícios potenciais de conectar em rede os atores do espaço de batalha para obter efeitos sinérgicos.

Esses benefícios são descritos em quatro princípios que ratificam seu uso em combate (USA, 2005):

a) uma força em rede robusta[1] melhora o compartilhamento de informações;

[1] Uma rede robusta é uma rede capaz de suportar falhas e perturbações

b) o compartilhamento de informações aumenta a qualidade das informações e a consciência situacional compartilhada;

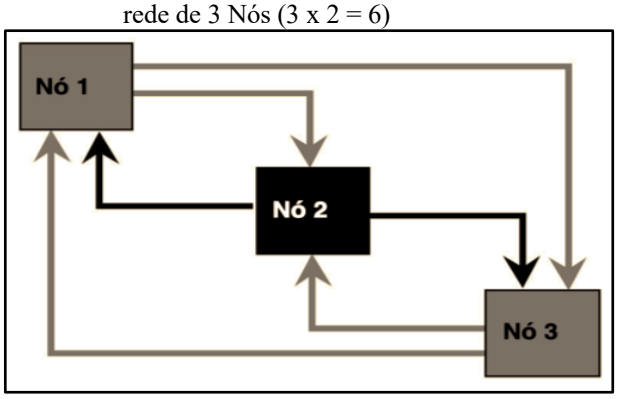
c) a consciência situacional compartilhada permite a colaboração sincronizada, e aumenta a sustentabilidade[2] e a velocidade de comando; e

d) a sustentabilidade e a velocidade de comando aumentam drasticamente a eficácia da missão.

Outro ponto forte da guerra centrada em rede é seu potencial de compensar uma desvantagem em número, tecnologia ou posição. Em outras palavras, a tecnologia sozinha não garante maior probabilidade de sucesso militar sem uma efetiva troca de informação entre os agentes envolvidos. Essa efetiva troca de informação pode ser expressa como ganho valor e vantagem competitiva (ALBERTS; GARSTKA; STEIN 2000; EUHUS, 2018)

Nessa perspectiva, a era da informação veio para criar valor de forma inovadora, pois anteriormente não havia como mensurar o valor potencial de uma rede. Alberts, Garstka e Stein (2000) vieram para reformular essa percepção e fizeram uso da "Lei de Metcalfe" para fundamentar a teoria da GCR e medir esse valor. Esse postulado recebeu o nome de Robert Metcalfe, inventor da topologia da Ethernet, onde ele afirma que o valor potencial de uma rede é "n" multiplicado por "n-1" (Figura 1), sendo "n" o número de nós na rede (ALBERTS; GARSTKA; STEIN, 2000).

Figura 1 – Representação ilustrativa do potencial de uma rede de 3 Nós (3 x 2 = 6)



Fonte: Alberts, Garstka e Stein (2000, p. 33, tradução nossa)

Com base nessa premissa, é possível medir o potencial de uma rede considerando o seu número de nós "n" e a interação entre eles "n-1". Em outras palavras, o valor encontrado quando se multiplica "n" por "n-1" representa o número de caminhos diretos por onde são tramitados os dados e informações entre os integrantes de uma rede (Figura 1).

[2] Capacidade de sustentar, ou habilidade de manter um sistema ou processo em um certo nível.

Sendo assim, pode-se dizer que a existência de uma rede potencializa o uso da informação por meio de seus nós de conexão de forma não linear, atingindo seu máximo valor ao chegar próximo dos 100 por cento das interações possíveis (ALBERTS; GARSTKA; STEIN, 2000).

Alberts, Garstka e Stein (2000, p. 34, tradução nossa) são taxativos em afirmar que a "superioridade da informação é um estado que é alcançado quando uma vantagem competitiva é derivada da capacidade de explorar uma posição de informação superior".

Nessa perspectiva, a combinação de estratégias, táticas, técnicas e procedimentos de uma força conectada, pode ser empregada para criar uma vantagem decisiva ao explorar o uso da rede (USA, 2005).

Na FAB, o conceito de GCR está alinhado com o entendimento de que a "conectividade das redes contribui para obtenção da superioridade da informação e da iniciativa, aumenta a mobilidade e a coordenação entre os combatentes" (BRASIL, 2010, p. 8). Desse modo, a visão de conectividade está focada no aumento do valor potencial da rede para manter uma vantagem relativa durante as ações de combate.

Podemos citar como exemplo da exploração dessas capacidades o sistema de enlace de dados LINK 16 americano, o LINK-BR2 da Força Aérea Brasileiro e o Sistema de Defesa Aeroespacial Brasileiro (SISDABRA), que possuem equipamentos eletrônicos capazes de estabelecer conexão entre os integrantes de uma cadeia de comando e controle (BRASIL, 2021).

Segundo Alberts, Garstka e Stein (2000) a superioridade no domínio informacional é um conceito comparativo ou relativo, tendo seu valor proveniente dos resultados militares que possam ser alcançados. Ele faz uma clara comparação que esse valor é análogo à superioridade aérea ou ao controle do ambiente marítimo. Sendo assim, seu grande potencial é inerente à capacidade de tornar mais eficaz as ações de combate, sejam elas defensivas ou ofensivas. Esse potencial é flexível à medida que o uso das capacidades da rede é viabilizado ou não no combate, podendo antecipar ou anular as ações do adversário.

Nessa perspectiva, Alberts, Garstka e Stein (2000) acrescentam que, para interromper ou degradar um ativo de defesa aérea inimiga, o combate tradicional pode envolver o uso de novas armas e uma variedade de ataques cibernéticos, sejam a um roteador de comunicações, um banco de dados ou a um sistema de auxílio à decisão.

Desse modo, apesar das vantagens apresentadas na GCR inerentes à tecnologia e automação das informações em combate, existem pontos a serem observados e que são enxergados como fragilidades de um ecossistema interconectado, seja por rede física ou por

meio do espectro eletromagnético, que são as vulnerabilidades a ataques cibernéticos (USA, 2018a).

3.2 Cibernética

Wiener (1970) afirma que podemos compreender a sociedade por meio do estudo da comunicação e das mensagens. Ele entendeu que, além da teoria de transmissão de mensagens da engenharia elétrica, a cibernética era uma abordagem mais ampla, que tornaria possível o estudo das mensagens, não só como meios de dirigir a maquinaria e a sociedade, mas também de desenvolver autômatos (máquinas, computadores etc.), podendo ser compreendida como uma ciência que aborda a comunicação e o controle das informações independente do meio de transmissão.

Para ele, o meio e os estágios por onde passam a mensagem não possuem relevância para a comunicação desta entre dois agentes (WIENER, 1970). Sua preocupação estava focada nas manifestações relacionadas com o controle da comunicação. Essa premissa nos remete ao exercício do "telefone sem fio", onde a mensagem chega ao final da cadeia de comunicação totalmente modificada. A cibernética se molda a esse contexto de forma a diminuir o ruído, controlando sistematicamente a informação para que ela chegue ao destino em sua forma original.

Máquinas, portas automáticas, elevadores, carros, aeronaves, mísseis etc., se comunicam com o mundo exterior por meio de sensores e estamos acostumados com esse convívio a algum tempo. Wiener (1970) afirma que nossa maneira de interagir com o meio e de aprender a nos ajustarmos a ele é análogo ao da automação, que por meio da retroalimentação é capaz de ajustar a ação futura em função das informações recebidas.

> "A realimentação é um método de controle de um sistema pela reintrodução, nele, dos resultados de seu desempenho pretérito. Se esses resultados forem usados apenas como dados numéricos para a crítica e regulagem do sistema, teremos a realimentação simples dos técnicos de controle. Se, todavia, a informação que remonta do desempenho for capaz de mudar o método e o padrão geral de desempenho, então teremos um processo a que poderemos denominar aprendizagem" (WIENER, 1970, p. 61).

Neto (2020, p. 34) complementa que "a obra de Wiener acerca da cibernética vai muito além de questões ligadas a mecanismos e a autômatos", e que seríamos capazes de compreender qualquer organismo e seu funcionamento ao analisarmos seus mecanismos de comunicação e retroalimentação.

Já para as Forças Armadas Brasileiras, o entendimento do que é cibernética segue a seguinte definição segundo a DMDC:

> "termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. No campo da Defesa Nacional, inclui os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle (SISMC2), os sistemas de armas e vigilância, e os sistemas administrativos que possam afetar as atividades operacionais" (BRASIL, 2014, p. 18).

Para Neto (2020, p. 25), uma percepção importante é que a cibernética deve ser tratada também como um "espaço" e um "recurso" capazes de unificar as dimensões geográficas tradicionais, contribuindo para levantar a percepção da criação de uma suposta quarta Força, para agir no domínio do território cibernético aos moldes das já tradicionais Forças que operam nos domínios territoriais aéreo, marítimo e terrestre.

Por outro lado, ao compararmos o ciberespaço a outros domínios, observa-se uma certa carência de identidade, não sendo possível considerá-lo como um lugar físico, pois desafia sua medição em qualquer direção (LANZENDORFER; SPANGLER, 2015).

Já a doutrina conjunta americana visualiza o ciberespaço em três camadas interdependentes que podem interagir entre si atingindo uma ou mais delas (USA, 2018b):

a) camada de rede física, que consiste nos equipamentos de tecnologia da informação constantes no domínio físico, capazes de transportar, armazenar e processar as informações no espaço cibernético;
b) camada de rede lógica, que é a camada abstrata, baseada em códigos e capaz de transportar o dado de informação. Os nós da camada física podem usar a camada lógica para procurar o melhor caminho de comunicação em vez do caminho físico mais curto; e
c) camada de cyber-persona, que é uma identidade, criada no espaço cibernético pela abstração da camada lógica. Desse modo, um agente pode possuir várias cyber-persona espalhadas no Ciberespaço.

Já Kuehl (2009), define o espaço cibernético, ou ciberespaço, da seguinte maneira:

> "o ciberespaço é um domínio global dentro do ambiente de informação cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando tecnologias de comunicação de informação" (KUEHL, 2009, p. 27, tradução nossa).

Além dessas definições para o ciberespaço existem outras possíveis, todas elas convergindo para o mesmo entendimento. Desse modo, este trabalho toma a definição conforme a DMDC para um melhor delineamento do conceito, considerando o ciberespaço como um "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas" (BRASIL, 2014, p. 18).

É importante também o entendimento de que o espaço cibernético é um dos cinco domínios operacionais, assim como o aéreo, o marítimo, o terrestre e o espacial, e que sua liberdade de ação dentro dos outros domínios proporciona uma alavancagem de suas capacidades gerando efeitos decisivos (BRASIL, 2014).

Com o advento dos avanços tecnológicos, grandes potências como China e Estados Unidos estão direcionando o interesse para esse novo domínio, pois a cibernética aliada à tecnologia pode vir a alterar a balança de poder político e econômico no âmbito internacional (NETO, 2020).

O objetivo aí é ocupar espaço nesse ambiente, expandindo um poder que extrapola as fronteiras territoriais. Essa visão é importante, em grande parte por considerar que "o ciberespaço já se perfaz um território, para alguns atores, e que é disposto de forma transversal e com acesso a todas as outras dimensões espaciais" (NETO, 2020, p. 30).

Segundo Commons (2018), para se obter superioridade no ciberespaço é preciso monitorar o tráfego de informação digital na área de operação e ser capaz de obter livre acesso tanto das redes de comunicação amigas, para defender-se de interferência adversária, quanto da rede adversária, para usá-la a seu favor. Pois ser incapaz de navegar pelo terreno da informação é não poder obter informações relevantes do campo de batalha para auxílio à tomada de decisão.

Outro ponto importante é colocado por Kuehl (2009) sobre a relevância dada às tecnologias que exploram o espaço cibernético, pois ele considera que a criação, armazenamento, modificação e exploração da informação só está sendo feita no ciberespaço devido ao uso da eletrônica ou da energia eletromagnética.

Isso remete à percepção de que a obtenção de vantagens no ambiente cibernético exige também capacidades tecnológicas em consonância com a demanda do conflito, e ser capaz de operar no campo de batalha cibernético e espectro eletromagnético como fogo não letal proporciona janelas cronológicas de vantagem (USA, 2017).

Corroborando essa percepção, Commons (2018) também entende que a inter-relação entre o domínio cibernético e o espectro eletromagnético é relevante e vem surgindo para moldar as ações em outros domínios.

Atualmente, as forças de combate, principalmente as aéreas, dependem muito do uso do espectro eletromagnético para comando e controle, consciência situacional e direcionamento das ordens de comando. Dentro dessa perspectiva, a doutrina norte americana contempla o espaço cibernético como sendo um dos cinco domínios da guerra e que seu uso concomitante com o espectro eletromagnético traz benefícios para as operações unificadas em uma força

conjunta, limitando as ações do inimigo e diminuindo sua capacidade de comando e controle, de maneira que sua liberdade de agir nos outros domínios seja degradada (USA, 2021).

A FAB também contempla essa visão na sua doutrina em uma de suas ações designada "sinergia eletrônica cibernética" que consiste em

> "atividades de defesa cibernética de sinergia, integradas com as atividades de guerra eletrônica, que consistem em aumentar esforços para empregar meios de Força Aérea, a fim de: criar bibliotecas de alvos cibernético-eletrônicos; criar dispositivos para comunicação operacional segura em celular ou integrados à telefonia; pesquisar e desenvolver interferência cibernético-eletrônica mediante despistamento e *jamming*; além de gerenciar atividades de guerra centrada em rede, criptografia, *datalink*, furtividade, detecção antecipada, comando descentralizado e uso de armas inteligentes" (BRASIL, 2020b, p. 12).

Após discorrer sobre os conceitos, que formam a base para o conhecimento e entendimento da teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da cibernética de Wiener (1970), serão apresentadas a seguir a coleta de dados e a análise dos resultados.

4 APRESENTAÇÃO DOS DADOS E ANÁLISE DOS RESULTADOS

Este capítulo é divido em cinco partes. A primeira apresenta os conceitos da guerra cibernética, bem como das ações cibernéticas. O segundo e o terceiro, discorrem sobre as vulnerabilidades cibernéticas associadas às aeronaves. O quarto, traz os conceitos doutrinários das tarefas e ações de Força Aérea, correlacionando a guerra cibernética com as ações de Força Aérea. O último, traz uma análise dos dados e resultados para se avaliar a influência das ações cibernéticas na rede proposta.

4.1 Guerra cibernética

Quando se fala em cibernética no contexto da Defesa Nacional, são abordados os conceitos e responsabilidades segundo seus respectivos níveis de decisão na DMDC. Estas responsabilidades foram colocadas no Quadro 1 para melhor entendimento:

Quadro 1 – Quadro de correlação das denominações segundo a DMDC

NÍVEL	DENOMINAÇÃO	RESPONSABILIDADE
Político	Segurança Cibernética	Presidência da República
Estratégico	Defesa Cibernética	Ministério da Defesa
Operacional	Guerra Cibernética	Forças Armadas
Tático		

Fonte: Adaptado de Brasil (2014)

Assim sendo, a abordagem cibernética no campo militar possui a denominação doutrinária de "guerra cibernética", sendo de responsabilidade das Forças Armadas a atuação nos níveis tático e operacional.

É importante ressaltar que a denominação "defesa cibernética" quando usada nessa pesquisa fará referência ao nível estratégico de decisão e a denominação guerra cibernética fará referência ao nível operacional ou tático.

Sendo assim, a defesa cibernética é descrita na DMDC como sendo 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, 2014, p. 18).

Já a guerra cibernética em sua descrição doutrinária

> "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)[3] 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, 2014, p. 18, grifo nosso).

Em termos práticos, tanto no nível estratégico, operacional ou tático, ocorrem as atividades correspondentes às ações cibernéticas, que são o emprego de uma ou mais capacidades relacionadas às atividades de defesa cibernética e guerra cibernética. São ações no espaço cibernético que buscam produzir efeitos que se traduzam em vantagem política, estratégica, operacional ou tática, ou seja, são a materialização do emprego cibernético, seja na obtenção de dados, informações, conhecimentos de interesse, ou contra as estruturas computacionais e de comunicações (BRASIL, 2020c), sendo divididas em três tipos na DMDC:

a) ataque cibernético,

> "compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente" (BRASIL, 2014, p. 23);

b) proteção cibernética,

> "abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de segurança, defesa e guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente" (BRASIL, 2014, p. 23); e

[3] O termo foi atualizado pela DBFAB em 2020, passando a ser denominado Sistemas de Comunicações e Tecnologia da Informação para Comando e Controle (SCTIC2).

c) exploração cibernética,

> "consiste em ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas" (BRASIL, 2014, p. 23).

A doutrina norte americana também divide as ações do ciberespaço em três categorias denominadas proteção do ciberespaço, exploração do ciberespaço e ataque do ciberespaço, com significados análogos à doutrina brasileira, mas divide a proteção cibernética em duas, sendo segurança do ciberespaço e defesa do ciberespaço. Essa divisão se dá por efeitos práticos, enquanto a segurança do ciberespaço procura impedir o acesso, a defesa do ciberespaço trata das ameaças que violaram a segurança (USA, 2018b).

Esses conhecimentos são a base para o entendimento da aplicação cibernética no ambiente de combate, que consiste em atacar, proteger e explorar as vulnerabilidades das camadas física, lógica e *cyber-persona* de um sistema.

4.2 Vulnerabilidades cibernéticas

A premissa básica para o início de um ataque com grande potencial de sucesso é a infiltração. Após ela ocorrer, pode-se manipular a camada de rede lógica, os sistemas de controle de voo, danificar equipamentos, extrair dados de interesse, impedir ou rastrear comunicação, diminuir níveis de saturação de oxigênio da cabine, impedir que componentes funcionem ou funcionem de maneira inadequada, podendo até assumir totalmente o controle de uma aeronave, como no caso de uma aeronave remotamente pilotada (ALFORD, 2000). Assim, um ataque cibernético pode gerar efeito em todo o espaço cibernético de atuação, sendo capaz de causar destruição também no espaço físico (USA, 2021).

Alford (2000, p. 106, tradução nossa) afirma que "fundamentalmente, os sistemas cibernéticos podem ser infiltrados de duas maneiras, por entradas físicas ou de sinal". A infiltração física pode ser realizada por meio da camada de rede física conectada ao próprio sistema (cartão de memória, dispositivos USB, computador de manutenção, controles do painel, controles de voo etc.). E a infiltração de sinal pode ocorrer por meio de conexões diretas ou indiretas dos sistemas (rede local provida pelo roteador, *wireless*, dispositivos infravermelhos, conexões de rádio frequência etc.). Em outras palavras, todo sistema possui uma porta de entrada para dados e informação, e essa entrada pode ser explorada e de modo a abrir caminho para um ataque cibernético.

Segundo Yasar, N., Yasar, F. e Topcu (2012) os ataques cibernéticos também podem ser divididos em duas categorias, ataques à camada de rede lógica e ataques à camada de rede física. Ambos têm como objetivo interagir com o sistema alvo por meio de uma rede, seja ela com ou sem fio.

Exemplos de ataques à camada de rede lógica:

a) *malware*, são programas maliciosos desenvolvidos para danificar, monitorar (*spyware*), restringir acesso (*ransomware*), dissimular (*spoofing*), criar entrada de acesso (*trojan*), replicar-se para outros sistemas (*worm*), controlar ou desabilitar computadores (YASAR, N; YASAR, F; TOPCU, 2012); e

b) bombas-relógio, bomba lógica ou de gatilho, são códigos que poder ser acionados baseado em uma condição específica, quando ela é atendida o código que causa dano entra em ação (CLARKE; KNAKE, 2015).

Exemplo de ataques à camada de rede física:

a) circuitos integrados que possuem funcionalidades extras escondidas, sendo que essas funcionalidades podem ser acionadas a critério do agente, inclusive por meio de radiofrequência. (YASAR, N; YASAR, F; TOPCU, 2012); e

b) *e-bombs*, são bombas de pulso eletromagnético capazes de danificar ou deixar inoperante equipamentos eletrônicos (YASAR, N; YASAR, F; TOPCU, 2012).

Não há uma taxonomia comum dos ataques cibernéticos, o que mais se encontra nos artigos acadêmicos é a diferenciação por tipo, descrevendo a finalidade do ataque. Alguns dos mais comuns ataques são os seguintes:

a) negação de serviço, inunda o sistema com dados esgotando recursos, impedindo ou prejudica o uso da rede ou sistema para um computador (USA, 2018a);

b) *man-in-the middle*, uma forma de espionagem ativa, o invasor intercepta e modifica a comunicações de dados se passando por outro agente (USA, 2018a);

c) *pass-the-hash*, intercepta a criptografia de um nome de usuário e senha para se autenticar na rede de interesse (USA, 2018a);

d) *spoofing*, bloqueio de um sinal ou substituição dele por outro falso. No caso de uma falsificação de sinais ADS-B por exemplo, pode-se assumir o controle de um drone (ALTAWY; YOUSSEF, 2016);

e) *port scanning attack*, método para achar pontos de entrada nos computadores alvo (SILVA, 2022);

f) *zero-day,* "trata-se de uma vulnerabilidade de segurança ainda desconhecida [...] o fabricante possui exatamente "zero dias" para desenvolver uma atualização e

disponibilizá-la [...] antes que algum *hacker* tente explorar essa brecha" (SILVA, 2022, p. 27); e

g) ataque de força bruta, tentativas de adivinhar a senha de acesso de um sistema e/ou serviço de rede (SILVA, 2022).

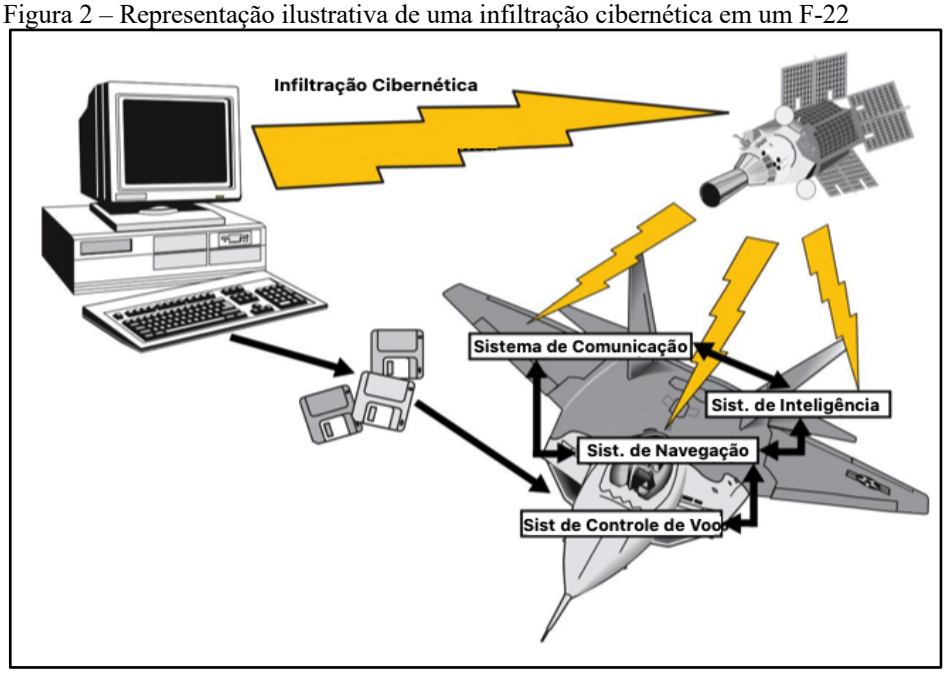
As variedades, tipos e quantidades de ataques elevou a preocupação dos EUA, a ponto de sua doutrina de guerra passar a se preocupar com essa vulnerabilidade também em suas aeronaves de combate, partindo do entendimento que qualquer sistema militar controlado por *software* é vulnerável a ataques cibernéticos (ALFORD, 2000).

4.3 Aeronaves

Nos dias atuais as aeronaves estão cada vez mais ganhando capacidades com o auxílio da tecnologia, e o uso delas no combate vem se tornando dependente dessa evolução. O Tenente Coronel Lionel D. Alford Jr. em 1999 já havia identificado que nas aeronaves mais avançadas o desempenho e as capacidades dependiam de mais de 75% dos programas de computador embarcados, o que por sua vez aumentou a vulnerabilidade a ataques cibernéticos (ALFORD, 2009).

Um exemplo é o caça F-22, representado na Figura 2, que possui sistemas de comunicação, inteligência, controle de voo, armamento etc., todos controlados por *software* e considerados como sistemas abertos, pois necessitam de conexões externas para atualizar as informações, tornando-se suscetíveis a serem atacados (ALFORD, 2000).

Figura 2 – Representação ilustrativa de uma infiltração cibernética em um F-22



Fonte: Alford (2000, p. 104, tradução nossa)

Um ataque cibernético pode ter como alvo qualquer sistema de uma aeronave como o controle de voo, de propulsão, radar, alerta de emergência, de dados de voo, inclusive o subsistema de armas de combate, ou seja, tudo que dependa de *software*, podendo tornar impraticável o cumprimento de uma missão militar, ou até mesmo a perda de vidas (USA, 2018a).

Um exemplo é a entrada por meio de dados constantemente atualizados no Sistema de Posicionamento Global (GPS), podendo não só diminuir a consciência situacional do piloto, inserindo erros na navegação, como também degradar a precisão do armamento, devido aos dados inconsistentes enviados ao sistema de emprego da aeronave (ALFORD, 2000).

Um caso que ilustra essa preocupação é o da frota de aeronaves Rafale francês que parou em janeiro de 2009 devido a um *worm* criado para o Microsoft Windows. O vírus havia infectado alguns dos sistemas de suporte terrestre impossibilitando a decolagem das aeronaves (YASAR, N; YASAR, F; TOPCU, 2012).

Um ponto que levantou extrema preocupação dos EUA é que os sistemas de armas são bastantes vulneráveis a ataques, pois possuem entradas para potenciais ataques via de radiofrequência e receptores radar, sendo possível um invasor entrar no sistema por vias de acesso que estão conectadas a outros domínios, como por exemplo o invasor saltar de um sistema terrestre para um espacial e buscar caminho até ter acesso aos sistemas da aeronave mesmo que indiretamente (USA, 2018a).

Entre 2012 e 2017, vários testes foram realizados pelo departamento de defesa americano buscando vulnerabilidades nos sistemas críticos das aeronaves. Os especialistas que realizaram os testes constataram que foi relativamente simples entrar sem serem detectados e assumir o controle dos sistemas, impossibilitando uma defesa efetiva aos ataques cibernéticos (USA, 2018a).

Foi nesse contexto que os EUA reformularam sua doutrina, política de defesa e leis fiscais, exigindo que a Secretaria de Defesa avaliasse as vulnerabilidades dos sistemas de armas até o final de 2019 e desenvolvesse estratégias para mitigar esses riscos considerados elevados (USA, 2018a).

4.4 Correlação doutrinária das ações

Em um esclarecimento inicial, se faz necessário o entendimento do termo doutrina como o "conjunto de princípios, conceitos, normas e procedimentos, fundamentado principalmente na experiência, destinado a estabelecer linhas de pensamentos e a orientar ações, exposto de

forma integrada e harmônica" (BRASIL, 2015, p. 94). Além disso, no âmbito da FAB, a doutrina militar aeroespacial está relacionada ao "emprego do Poder Militar Aeroespacial em tempos de paz, crise ou guerra, e divide-se em três níveis: estratégico, operacional e tático" (BRASIL, 2020a, p. 13).

No nível estratégico, a doutrina "abrange os princípios e os conceitos que orientam o preparo e o emprego da FAB" (BRASIL, 2020a, p. 13).

No nível operacional, ela "define os conceitos, [...] das ações de Força Aérea" (BRASIL, 2020a, p. 13).

No nível tático, ela "define as normas e os procedimentos a serem seguidos na execução das ações de Força Aérea que sustentam o emprego do Poder Militar Aeroespacial" (BRASIL, 2020a, p. 13).

Na prática, os objetivos mais abrangentes de uma campanha ou operação militar são definidos pelas tarefas de Força Aérea em uma análise estratégica e operacional, ou seja, se referem aos efeitos que podem ser produzidos com os meios de Força Aérea (BRASIL, 2020a).

Apesar de haver pouca referência a respeito da cibernética na descrição das tarefas, todas se relacionam com o ambiente cibernético em certa medida. Dentre as sete tarefas descritas na DBFAB, observa-se a interação com o ciberespaço de acordo com a descrição contida nela e com o entendimento da DMDC da seguinte forma (BRASIL, 2014, 2020a):

a) controle aeroespacial, com ações cibernéticas ofensivas e defensivas, fornecendo às forças amigas a liberdade de ação;
b) interdição, afetando por meio de ataques cibernéticos, cinéticos ou não-cinéticos, a organização e o funcionamento das forças de superfície inimigas;
c) inteligência, vigilância e reconhecimento, garantindo a segurança e confiabilidade dos dados;
d) sustentação ao combate, sendo capaz de potencializar características como alcance, mobilidade, penetração e pronta-resposta, ampliando o poder de combate dos meios de Força Aérea e das forças armadas amigas;
e) comando, controle, comunicação e sistemas de informação, para a manutenção da confidencialidade, integridade e disponibilidade das informações em níveis estratégicos, operacionais e táticos;
f) proteção da força, provendo uma proteção cibernética ao ambiente operacional, tornando-o seguro ao emprego da Força Aérea; e
g) apoio às ações de Estado, mantendo a integridade de infraestruturas sensíveis e essenciais à operação no local de atuação.

Já as ações de Força Aérea, consistem no emprego de meios aeroespaciais[4] e meios de Força Aérea[5] para consecução dos objetivos e alcance do efeito final desejado, sendo descrito na DBFAB como o

> "ato de empregar, no nível tático, meios aeroespaciais e de Força Aérea para causar um ou mais efeitos desejados em uma campanha ou operação militar. Envolve ações letais e não letais de emprego do poder aeroespacial, bem como ações especializadas destinadas a suportar e a complementar a capacidade operacional da Força Aérea" (BRASIL, 2020a, p. 9).

Desse modo, as ações de Força Aérea são executadas de forma combinada objetivando o alcance dos efeitos desejados utilizando-se dos meios existentes e disponíveis para emprego. Ou seja, sua execução se dá no nível tático, mas visa atingir objetivos de qualquer nível, seja estratégico, operacional ou tático (BRASIL, 2020b).

Conforme abordado anteriormente, as tarefas de Força Aérea compreendem a uma perspectiva operacional mais abrangente e, em certa medida, a cibernética permeia todas as tarefas elencadas na doutrina. Como forma de avaliar a rede dos elementos que compõem as tarefas de Força Aérea, é necessário fazer o uso das ações de Força Aérea que, no nível tático, representam sua aplicabilidade.

Essa visão é corroborada por Cebrowski e Garstka (1998), no entendimento de que a guerra centrada em rede também é aplicável a todos os níveis da guerra, contribuindo para a coalescência de estratégia, operações e táticas. Nessa perspectiva, uma rede complexa de dados e informação perfaz pela atuação de diversos atores, sejam unidades de artilharia, brigadas de combate, esquadrilhas de aeronaves, satélites ou até mesmo um elemento de forças especiais no terreno com um rádio portátil ou celular. Toda essa teia de conexões pode ser representada pela troca de informações entre os nós das ramificações em um ambiente de GCR que, em uma abordagem doutrinária, se materializa no nível operacional no conjunto das 55 ações de Força Aérea expressas na DBFAB em 2022.

Essa visão enseja na inter-relação da guerra cibernética com esse ambiente, de modo a fortalecer a interação entre as ações de Força Aérea interrompendo, degradando, corrompendo, ou negando o emprego por parte do oponente. Desse modo, a efetividade do ciberespaço no volume de interesse das tarefas de Força Aérea se torna possível pela atuação das ações cibernéticas na malha de trâmite de informação da GCR, sendo possível em teoria avaliar seu potencial no nível operacional à luz da lei de Metcalfe proposta na teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000).

---

[4] Elementos aéreos da FAB ou adjudicados a ela.
[5] Elementos terrestres da FAB ou adjudicados a ela.

4.5 Resultados gerais

A GCR demonstra que o tamanho da rede, representado por seu valor potencial, pode ser mensurável de acordo com a lei de Metcalfe. Essa premissa leva ao entendimento de que a capacidade máxima da rede se traduz em seu valor com todos os nós da rede interligados.

Nesse contexto, a cibernética torna essa rede robusta à medida que interage com todos os integrantes, protegendo a troca e o controle das informações. Assim, a correlação existente entre a guerra cibernética e a GCR torna evidente a vulnerabilidade do ambiente conectado quando qualquer um dos elos está sujeito à infiltração cibernética. Por outro lado, a capacidade de proteger essas ligações expressa a resiliência e a robustez do sistema.

Com base nessa premissa, e considerando a rede teórica composta por 54 nós, que correspondem às ações de Força Aérea, encontramos o potencial máximo "n x (n – 1)" de 2862 interações possíveis (valor potencial da rede teórica a ser considerado como sendo 100%).

Já o levantamento estatístico foi feito com base nos dados coletados junto a especialistas em cibernética com dois anos ou mais de experiência de atuação na área. No total, foram coletadas 1134 respostas de sete especialistas.

O questionário foi elaborado visando a percepção sobre a aplicação de cada ação cibernética nas ações de Força Aérea, sendo possível mensurar o grau de concordância na aplicação da guerra cibernética em todo o leque doutrinário das ações de Força Aérea.

As médias das ações cibernéticas para cada ação de Força Aérea (valores compilados no Apêndice B) variaram de 2,00 a 4,71 (Tabela 1), sendo que nenhuma delas obteve todos os graus abaixo de 3, o que está de acordo com a percepção doutrinária de que as ações de Força Aérea se relacionam com o ambiente cibernético em certa medida.

Tabela 1 – Amostra das respostas ao questionário

Ação de Força Aérea	Ação cibernética	Avaliação do especialista (ESP)							Soma e média	
		ESP 1	ESP 2	ESP 3	ESP 4	ESP 5	ESP 6	ESP 7	Soma	**Média**
AFA54	Exploração	4	5	5	5	5	5	4	33	**4,71**
AFA02	Ataque	4	5	5	4	5	5	4	32	4,57
[...][6]	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]	[...]
AFA48	Ataque	2	5	1	3	1	1	1	14	**2,00**
	Média	3,10	4,80	2,76	4,28	3,95	3,66	2,67	25,21	3,60

Fonte: O autor

Ao se calcular a média de todas as avaliações, que em uma visão holística expressa a grandeza numérica do domínio cibernético e, consequentemente, da guerra cibernética nessa GCR teórica, chegou-se ao valor 3,6 (Tabela 1) que se encontra na faixa de concordância. Isso

[6] Os demais valores estão tabulados no Apêndice B.

corrobora a percepção de que o ciberespaço interage em certa medida positivamente com as tarefas de Força Aérea, assim como se constata no entendimento da DMDC.

Por outro lado, levando em consideração a média das avaliações em cada ação de Força Aérea (Tabela 2), constatou-se que: apenas 59,26% das ações de Força Aérea (equivalente a 32 ações) ficaram na faixa de concordância no que tange à ação de ataque cibernético; 90,74% (equivalente a 49 ações) na ação de proteção cibernética; e 92,59% (equivalente a 50 ações) na ação de exploração cibernética.

Tabela 2 – Ações de Força Aérea dentro da faixa de concordância

Ações cibernéticas	Quantidade de ações de Força Aérea	Porcentagem em relação às 54 ações de Força Aérea
Ataque cibernético	32	59,26%
Proteção cibernética	49	90,74%
Exploração cibernética	50	92,59%

Fonte: O autor

Assim, ao retomarmos a teoria da GCR de Alberts, Garstka e Stein (2000) e sua correlação existente com a guerra cibernética, contatou-se que a vulnerabilidade do ambiente conectado pode ser expressa na capacidade de proteger suas ligações ao mensurarmos a permeabilidade da cibernética nessa GCR teórica.

Desse modo, chegou-se aos seguintes valores potenciais da rede (Tabela 3) em termos de guerra cibernética: 992 conexões (32 nós) em relação à ação de ataque cibernético; 2352 conexões (49 nós) em relação à ação de proteção cibernética e 2450 conexões (50 nós) em relação à ação de exploração cibernética.

Essa permeabilidade da guerra cibernética nas ações de Força Aérea também pode ser expressa em termos de porcentagem do potencial máximo da rede, resultando em uma correlação de 34,66%, 82,18% e 85,60% das ações de ataque, proteção e exploração cibernética, respectivamente, em relação à GCR teórica.

Tabela 3 – Valor potencial das ações cibernéticas em relação à GCR teórica

Ações cibernéticas	Nós	Potencial da rede	Correlação com a GCR
GCR teórica	54	2862	100,00%
Ataque cibernético	32	992	34,66%
Proteção cibernética	49	2352	82,18%
Exploração cibernética	50	2450	85,60%

Fonte: O autor

Da análise das médias (valores compilados no Apêndice C), agora considerando a grandeza numérica do domínio cibernético e da guerra cibernética em cada ação de Força Aérea, também foi possível identificar que a ação de varredura (AFA52 na Tabela 4) obteve a maior avaliação na aplicação da guerra cibernética (4,38).

Por outro lado, a ação de reabastecimento em voo (AFA42 na Tabela 4) recebeu uma das menores pontuação (2,71).

Com isso, ao retomar a teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) afirmando que, para garantir vantagens e explorar a superioridade da informação, é necessário buscar atingir o máximo valor potencial de uma rede, chegando próximo de 100% das interações possíveis entre seus nós de conexão, podemos inferir que: os valores apresentados nas Tabelas 3 e 4, relacionados às ações cibernéticas e à GCR teórica, demonstram o que Alford (2009) havia identificado sobre a vulnerabilidade intrínseca de uma rede.

Tabela 4 – Amostra da soma das ações cibernéticas para cada ação de Força Aérea

Ação De Força Aérea	Ataque cibernético (soma)	Proteção cibernética (soma)	Exploração cibernética (soma)	Total (soma)	Média[7]
AFA52	30	30	32	92	**4,38**
[...][8]	[...]	[...]	[...]	[...]	[...]
AFA42	17	20	20	57	**2,71**
AFA48	14	23	18	55	2,62
AFA50	16	18	18	52	2,48
MÉDIA	22,20	25,96	27,46	75,63	3,60

Fonte: O autor

Para ilustrar essa perspectiva, pode-se exemplificar a ação de Força Aérea que obteve a maior aceitação de influência da guerra cibernética que foi a ação de varredura. Esta ação em grande parte é realizada na FAB dentro de cenário de emprego de uma missão aérea composta, mais conhecida como missão de pacote, onde várias aeronaves adentram em uma região de interesse com efeito sinérgico, maximizando o compartilhamento de informações, consciência situacional compartilhada, velocidade de comando, enfim, aumentando a eficácia da missão.

Nesse contexto, a primeira ação executada é a de varredura com aeronaves de caça, sendo necessário que elas perdurem mais tempo que as demais para garantir a proteção do pacote. Porém, como característica peculiar, as aeronaves de caça possuem autonomia bastante restrita, o que impacta diretamente no tempo de permanência em combate e consequentemente na proteção das demais aeronaves. Dessa forma, a única maneira de aumentar esse tempo é provendo a ação de reabastecimento em voo para a missão de pacote.

Assim, ao serem exploradas as vulnerabilidades cibernéticas de uma aeronave reabastecedora nessa GCR, pode-se inviabilizar a missão de pacote ou até mesmo colocar em risco todas as demais aeronaves ao restringir o tempo de atuação da ação de varredura.

[7] A média para cada ação de Força Aérea é calculada somando-se todas as respectivas avaliações dos especialistas em cada ação cibernética e dividindo-as por 21 (7 avaliações para cada uma das 3 Ações Cibernética, o que totaliza 21).
[8] Os demais valores estão tabulados no Apêndice C.

Este é um exemplo que pode representar uma grande vulnerabilidade para uma GCR em que a guerra cibernética se encontra atuante. Em outras palavras, o uso restrito do domínio cibernético por parte da tropa amiga, pode tornar menos resiliente a rede em que se encontram todos os atores em constante troca de informações, gerando elevado risco para outras ações de Força Aérea, o que impacta diretamente no propósito operacional das tarefas de Força Aérea podendo gerar vantagens decisivas para um inimigo em um conflito.

5 CONCLUSÃO

Esse trabalho foi iniciado a partir da inquietação do autor em descobrir de que maneira a Força Aérea e seus meios de combate operam em um ambiente conectado e de interesse para o domínio cibernético.

Essa inquietação gerou um questionamento que foi traduzido no objetivo geral da pesquisa de forma a analisar em que medida a guerra cibernética exerce influência em uma rede teórica de ações de Força Aérea, em 2022, à luz da teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da doutrina básica da Força Aérea.

Desse modo, para alcançar o objetivo geral proposto, foram planejados três objetivos específicos. O primeiro, pretendeu descrever os conceitos da guerra cibernética. O segundo, buscou reconhecer a relação entre a guerra cibernética e as ações de Força Aérea à luz da teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da doutrina básica da Força Aérea. Já o terceiro, visou analisar a influência das ações cibernéticas em uma rede teórica de ações de Força Aérea em 2022.

O primeiro e o segundo objetivos específicos foram alcançados descrevendo os conceitos da guerra cibernética e reconhecendo a relação entre a guerra cibernética e as ações de Força Aérea à luz da teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da doutrina básica da Força Aérea.

Para a consecução do terceiro objetivo, as respostas ao questionário encaminhado aos especialistas em cibernética foram tabuladas de modo a ser possível analisar a influência da guerra cibernética em uma rede teórica de ações de Força Aérea em 2022.

Dessa forma, respondendo à questão problema do presente trabalho que teve como objetivo geral analisar em que medida a guerra cibernética exerce influência em uma rede teórica de ações de Força Aérea, em 2022, à luz da teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000) e da doutrina básica da Força Aérea, foram apontados os valores potenciais de cada ação cibernética na GCR teórica, constatando-se uma correlação de 34,66%,

82,18% e 85,60% das ações de ataque, proteção e exploração cibernética, respectivamente, com a GCR teórica das ações de Força Aérea. Além de ser identificado que a aderência da guerra cibernética alcançou o valor 3,6 em relação à GCR teórica na percepção geral dos especialistas, levando à inferência de que o ciberespaço interage em certa medida positivamente com as tarefas de Força Aérea, assim como se constata no entendimento da DMDC.

Com isso, ao retomar a teoria da guerra centrada em rede de Alberts, Garstka e Stein (2000, p. 34, tradução nossa) afirmando que a "superioridade da informação é um estado que é alcançado quando uma vantagem competitiva é derivada da capacidade de explorar uma posição de informação superior", conclui-se que a permeabilidade das ações de Força Aérea ao domínio cibernético, expressa na guerra cibernética e suas ações cibernéticas, quando se encontra longe de seu potencial máximo, demonstra a fragilidade encontrada em um ecossistema interconectado. Pois, partindo da premissa básica de que um ataque cibernético ocorre a partir de uma infiltração bem-sucedida (ALFORD, 2000), ao se lograr uma permeabilidade, por parte do inimigo, acima das identificadas pelos especialistas, pode-se explorar uma posição de vantagem em uma GCR onde o domínio cibernético é atuante.

Assim sendo, mesmo que as vulnerabilidades sejam abordadas apenas de forma teórica pelos autores e pelas doutrinas, tudo nos leva à percepção de que é imperativo o uso do domínio cibernético para obter vantagens competitivas em combate. Em outras palavras, o domínio cibernético pode potencializar o uso de uma rede ou degradá-la, de modo que uma posição de vantagem em uma GCR está diretamente atrelada às capacidades cibernéticas que sustentam essa rede (BRASIL, 2014).

Com relação às limitações dos resultados da pesquisa, o quantitativo de especialistas na área cibernética que participaram do questionário pode ser considerado baixo (sete), apesar do volume total de itens respondidos ter sido expressivo (1134). Outro ponto a se considerar é que os valores identificados são apenas balizadores quantitativos para avaliação das relações e influências existentes entre as variáveis, não sendo possível levá-los em consideração como índices provenientes de capacidades cibernéticas existentes.

Por fim, como sugestão de pesquisa futura, propõe-se estudos focados nas capacidades da aeronave de combate F-39, recém adquirida pela FAB, no intuito de correlacioná-las às vulnerabilidades percebidas dentro do domínio cibernético, tanto no campo teórico como no experimental, de forma a expandir os conceitos doutrinários relativos ao emprego dos meios aeroespaciais no campo da guerra cibernética.

REFERÊNCIAS

ALBERTS, David S.; GARSTKA, John J.; STEIN, Frederick P. ***Network Centric Warfare:*** *Developing and Leveraging Information Superiority. Assistant Secretary of Defense (C3I/Command Control Research Program).* Washington DC, 2000.

ALFORD, Lionel D. ***CYBER WARFARE:*** *PROTECTING MILITARY SYSTEMS. Air Force Materiel Command Wright-Patterson* AFB. OH, 2000.

ALFORD, Lionel D. *Cyber Warfare: The Threat to Weapon Systems*. **WSTIAC Q**, v. 9, n. 4, 2009.

ALTAWY, Riham; YOUSSEF, Amr M. *Security, Privacy, and Safety Aspects of Civilian Drones: A Survey.* **ACM *TRANSACTIONS ON CYBER-PHYSICAL SYSTEMS***, v. 1, n. 2, p. 1-25, 2016.

BRASIL. Comando da Aeronáutica. Comando de Preparo. Portaria COMPREP nº 630/SPOG-33, de 9 de dezembro de 2021. Aprova a edição do MCA 55-91 "Manual de Guerra Centrada em Redes". **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 228, f. 18338, 14 dez. 2021.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria nº 1.224/GC3, de 10 de novembro de 2020. Aprova a reedição da Doutrina Básica da Força Aérea Brasileira - Volume 1. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 205, f. 14971, 12 nov. 2020a.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria nº 1.225/GC3, de 10 de novembro de 2020. Aprova a edição da Doutrina Básica da Força Aérea Brasileira - Volume 2. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 205, f. 14971, 12 nov. 2020b.

BRASIL. Comando da Aeronáutica. Gabinete do Comandante da Aeronáutica. Portaria nº 2.102/GC3, de 18 de dezembro de 2018. Aprova a reedição do Plano Estratégico Militar da Aeronáutica. **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 222, f. 14766, 20 dez. 2018.

BRASIL. Congresso Nacional. Decreto Legislativo nº 179, de 2018. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem (CN) nº 2 de 2017 (Mensagem nº 616, de 18 de novembro de 2016, na origem). **Diário Oficial da União**, Brasília, DF, n. 241, Seção 1, p. 4, 17 dez. 2018.

BRASIL. Ministério da Defesa. Portaria Normativa nº 9/GAP/MD, de 13 de janeiro de 2016. Aprova o Glossário das Forças Armadas - MD35-G-01 (5ª Edição/2015). **Diário Oficial da União**, Brasília, DF, n. 14, Seção 1, p. 8, 21 jan. 2016.

BRASIL. Ministério da Defesa. Portaria Normativa nº 84/GM-MD, de 15 de setembro de 2020. Aprova a Doutrina de Operações Conjuntas MD30-M-01/Volumes 1 e 2 (2ª Edição/2020). **Diário Oficial da União**, Brasília, DF, n. 178, Seção 1, p. 250, 15 set. 2020c.

BRASIL. Ministério da Defesa. Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014. Aprova a Doutrina Militar de Defesa Cibernética. **Diário Oficial da União**, Brasília, DF, n. 224, Seção 1, p. 9, 19 nov. 2014.

CEBROWSKI, Arthur K.; GARSTKA, John J. *Network-Centric Warfare: Its Origin and Future. In*: **US *NAVAL INSTITUTE PROCEEDINGS***. 1998. p. 28-35. Disponível em: https://www.usni.org/magazines/proceedings/1998/january. Acesso em: 2 fev. 2022.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Brasport, 2015.

COMMONS, Austin G. A Cibernética é o Novo Domínio Aéreo: A Superioridade nos Domínios em Megacidades. ***MILITARY REVIEW***: Revista profissional do exército dos EUA. n. 2, t. 73, p. 66-77. Segundo trimestre 2018. Edição Brasileira. Disponível em: https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Arquivos/Segundo-Trimestre-2018/. Acesso em: 2 fev. 2022.

EUGÉNIO, António L. B. A Guerra Centrada em Rede: um breve balanço, dez anos depois. **REVISTA MILITAR**, n. 2481, 2008. Disponível em: https://www.revistamilitar.pt/artigo/330. Acesso em: 2 mar. 2022.

EUHUS, Brandon T. *A Clausewitzian Response to "Hyperwarfare". **The US Army War College Quarterly: PARAMETERS***, v. 48, n. 3, p. 65-76, 2018. Disponível em: https://press.armywarcollege.edu/parameters/vol48/iss3/9/. Acesso em: 24 fev. 2022.

KUEHL, Daniel T. *From Cyberspace to Cyberpower: Defining the Problem. **Cyberpower and national security**,* 2009. Disponível em: https://ndupress.ndu.edu/Media/News/Article/1216674/cyberpower-and-national-security/. Acesso em: 22 fev. 2022.

LANZENDORFER, Quinn E.; SPANGLER, Scott C. *INNOVATING KNOWLEDGE MANAGEMENT IN CYBER WARFARE. **ISSUES IN INFORMATION SYSTEMS***, v. 16, n. 2, p. 246-254, 2015. Disponível em: https://doi.org/10.48009/2_iis_2015_246-254. Acesso em: 19 fev. 2022.

NETO, Walfredo B. F. **UMA ESTRATÉGIA NACIONAL DE DEFESA PARA ALÉM DA GUERRA**: GEOPOLÍTICA CIBERNÉTICA E SEU TRANSBORDAMENTO ECONÔMICO-TECNOLÓGICO NO BRASIL (2008-2018). 2020. Tese (Doutorado em Economia Política Internacional) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2020.

SILVA, Flávia H. da. **Estudo de técnicas de ataque e defesa em equipamentos da indústria 4.0**. 2022. Trabalho de Conclusão de Curso (Bacharel em Engenharia da Computação) – Universidade Federal de Ouro Preto, João Monlevade, 2022.

USA. *Department of the Army*. **FM 3-12:** *CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE. Washington*, DC: *Army Publishing Directorate*, 2021.

USA. *Department of the Army. **Multi-Domain Battle:** Evolution of Combined Arms for the 21st Century* 2025-2040. Virginia: TRADOC, 2017.

USA. *Government Accountability Office.* ***WEAPON SYSTEMS CYBER SECURITY****:* DOD *Just Beginning to Grapple with Scale of Vulnerabilities.* Washington, DC: GAO, 2018a.

USA. *Joint Chiefs of Staff.* ***Joint Publication*** **3-12:** *Cyberspace Operations*. Washington, DC: JCS, 2018b.

USA. *Office of Force Transformation*. ***The Implementation of Network-Centric Warfare***. Washington, DC: *Office of the Secretary of Defense*, 2005.

WIENER, Norbert. **CIBERNÉTICA E SOCIEDADE:** O uso humano de seres humanos. Tradução: José Paulo Paes. 2. ed. São Paulo: Cultrix, 1970. Título original: *The human use of human beings: Cybernetics and society*.

YASAR, Nurgul; YASAR, Fatih M.; TOPCU, Yucel. *Operational Advantages Of Using Cyber Electronic Warfare (*CEW) *In The Battlefield*. *In*: ***Cyber Sensing*** **2012**. SPIE, 2012. p. 151-159.

APÊNDICE A – Questionário

Ações Cibernéticas e Ações de Força Aérea

1) Este questionário faz parte de uma coleta de dados para artigo acadêmico da Escola de Comando e Estado-Maior da Aeronáutica (ECEMAR). O objetivo será correlacionar, em termos teóricos, as "AÇÕES CIBERNÉTICAS" (Ataque, Proteção e Exploração) e as "AÇÕES DE FORÇA AÉREA" (54) descritas nas Doutrinas (Doutrina Militar de Defesa Cibernética MD31-M-07 e Doutrina Básica da FAB DCA 1-1).
2)As Ações de Força Aérea são executadas pela combinação adequada de "Meios de Força Aérea" (pessoal, aeronaves, plataformas espaciais, veículos terrestres, embarcações, armamentos, instalações, equipamentos e sistemas) com o objetivo de alcançar os efeitos desejados.

*Obrigatório

1. Trabalha a quantos tempo na área de Cibernética *

Marcar apenas uma oval.

- ◯ 1 ano
- ◯ 2 anos
- ◯ 3 anos
- ◯ 4 anos
- ◯ 5 anos ou mais

1 a 10/54

APÊNDICE A – Questionário (continuação)

As perguntas a seguir são relativas ao contexto de cada ação de Força Aérea (a descrição de cada ação foi extraída na integra da Doutrina Básica da FAB DCA 1-1), e terão uma escala de concordância que variam de 1 a 5, onde 1 equivale a discordar totalmente e 5 concorda totalmente. Desse modo, para cada ação de Força Aérea, marque na sua opinião se as ações cibernéticas (ataque, proteção e exploração) podem ser aplicadas a ela?

Discordo Totalmente	1	2	3	4	5	Concordo Totalmente

2. 1) Ação Cívico-Social (ACISO) é a ação que consiste em empregar Meios de Força Aérea para atuar no campo psicossocial da população, através de atividades educacionais, cívicas, prestando serviços médico-hospitalares, de confecção de documentos ou sanitários para aumentar o bem-estar da população. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

3. 2) Ação Direta (Aç Dir) é a Ação que consiste em empregar Meios de Força Aérea para neutralizar alvos oponentes de valor estratégico ou operacional, em áreas hostis ou sob controle do oponente, produzindo efeitos específicos sobre o Poder Aeroespacial oponente. Caracteriza-se pelo emprego de meios cinéticos contra alvos fixos e estacionários, utilizando-se técnicas de infiltração e exfiltração, ações terrestres curtas e específicas no objetivo, com engajamento mínimo, podendo contar com apoio de fogo aéreo ou naval. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

4. 3) Alerta em Voo (ALEVOO) é a Ação que consiste em empregar Meios Aeroespaciais para prover proteção à determinada Área de Interesse ou Ponto Sensível, seja operando a partir de uma Área de Responsabilidade de Caça (ARCA) ou ponto préestabelecido para a Patrulha Aérea de Combate (PAC), utilizando-se de meios cinéticos para neutralizar aeronaves inimigas. Quando em contexto de operação internacional, emprega-se a terminologia em inglês Fighter Area of Responsibility (FAOR) para representar a ARCA e Combat Air Patrol (CAP) para representar a PAC. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

5. 4) Alerta na Base (ALEBAS) é a Ação que consiste em empregar Meios Aeroespaciais a partir de determinada base de apoio e/ou desdobramento, mediante acionamento em face às ameaças na Área de Interesse e utilizando-se de meios cinéticos para neutralizar aeronaves inimigas. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

6. 5) Antissubmarino (AS) é a Ação que consiste em empregar Meios Aeroespaciais para buscar, detectar, identificar, acompanhar e neutralizar ou destruir submarinos inimigos, a fim de prover a defesa de linhas de comunicações marítimas, de áreas de interesse das operações navais e de outras áreas relevantes. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

7. 6) Apoio Aéreo Aproximado (Ap AA) é a Ação que consiste em empregar Meios Aeroespaciais, utilizando-se de meios cinéticos contra alvos fixos, estacionários e móveis na superfície, para detectar, identificar e neutralizar forças oponentes que estejam em contato direto com forças amigas. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

8. 7) Assalto Aeroterrestre (Ass Aet) é a Ação que consiste em empregar Meios Aeroespaciais para introduzir forças paraquedistas e seus equipamentos, prioritariamente por lançamento e eventualmente por meio de pouso, em áreas de interesse no TO. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

9. 8) Assuntos Civis (As Civ) é a Atividade que consiste em empregar Meios de Força Aérea para viabilizar a coordenação e cooperação, em apoio à missão, entre o Comandante da Força Aérea e das Unidades subordinadas e adjudicadas e os atores civis, incluindo-se a população civil local e as suas autoridades representativas, assim como as organizações governamentais e não governamentais, nacionais e internacionais. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

10. 9) Ataque (Atq) é a Ação que consiste em empregar Meios Aeroespaciais utilizando-se de meios cinéticos para neutralizar ou destruir alvos oponentes fixos, estacionários e móveis na superfície, previamente localizados e identificados. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

11. 10) Autodefesa de Superfície (ADS) é a Ação que consiste em empregar Meios de Força Aérea para detectar, identificar e neutralizar ataques realizados por forças terrestres, aeroterrestres, aeromóveis ou anfíbias oponentes às Áreas Sensíveis (A Sen) e aos Pontos Sensíveis (P Sen) de interesse da Força Aérea, por meio do emprego de meios cinéticos contra alvos móveis de superfície. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

11 a 20/54

12. 11) Busca e Salvamento (Search and Rescue - SAR) é a Ação que consiste em empregar Meios Aeroespaciais e de Força Aérea para buscar, localizar e salvar pessoas desaparecidas e/ou em perigo, geralmente envolvendo aeronaves ou embarcações, em virtude das restrições dos órgãos privados e de Segurança Pública de meios adequados para acesso rápido aos locais que se encontram as vítimas *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

13. 12) Busca e Salvamento em Combate (Combat Search and Rescue - CSAR) é a Ação que consiste em empregar Meios Aeroespaciais e de Força Aérea para buscar, localizar, identificar e salvar militares ou civis de interesse que se encontrem em TERRITÓRIO HOSTIL, especialmente tripulantes abatidos ou acidentados. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

14. 13) Combate a Incêndio em Voo (CI Voo) é a Ação que consiste em empregar Meios Aeroespaciais para combater incêndios, a partir de plataformas aéreas, especificamente equipadas para essa finalidade. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

15. 14) A Comunicação Social (Com Soc) é a Ação que consiste em empregar Meios de Força Aérea para manter a opinião pública favorável às ações militares amigas. A Com Soc envolve as funções de Relações Públicas (RP) e de Informação Pública (Info Pub). *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

16. 15) Contraterrorismo (C Trr) é a Ação que consiste em empregar Meios de Força Aérea para neutralizar a ação de grupos terroristas, em um contexto de Garantia da Lei e da Ordem ou de Defesa da Pátria, em áreas de interesse da Força Aérea, agindo no combate a ataques de forças oponentes. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

17. 16) Controle Aéreo Avançado (CAA) é a Ação que consiste em empregar Meios Aeroespaciais para coordenar o Ataque ou o Apoio Aéreo Aproximado contra alvos oponentes, previamente localizados e identificados, a fim de neutralizá-los ou destruí-los. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

18. 17) Controle e Alarme em Voo (CAV) é a Ação que consiste em empregar Meios Aeroespaciais para controlar aeronaves amigas e para detectar, identificar e proporcionar alarme antecipado de incursões aéreas oponentes. *

Marcar apenas uma oval por linha.

	1	2	4	5
Ataque	◯	◯	◯	◯
Proteção	◯	◯	◯	◯
Exploração	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

19. 18) Controle Satelital (CS) das plataformas espaciais no espaço exterior, de forma coordenada com as atividades de C2, defesa do espaço aéreo e com as entidades internacionais, independentemente da natureza “dual” (civil-militar) do sistema. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

20. 19) Defesa Antiaérea (DAAe) é a Ação que consiste em empregar Meios de Força Aérea, a partir da superfície, para detectar, identificar e neutralizar vetores aéreos oponentes que ameacem forças amigas e Áreas (A Sen)ou Pontos Sensíveis (P Sen)de interesse da Força Aérea, por meio do emprego de meios cinéticos contra alvos aéreos. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

21. 20) Defesa Biológica, Nuclear, Química e Radiológica (DBNQR) é a Ação que consiste em empregar Meios de Força Aérea para reconhecer, identificar e descontaminar pessoal, material, viaturas e aeronaves necessários ao emprego da Força Aérea, agindo na prevenção contra ameaças de origem biológica, nuclear, química ou radiológica. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

21 a 30/54

22. 21) Demonstração Aérea (Dem Ae) é a Ação que consiste em empregar Meios Aeroespaciais por unidade especializada em demonstrações de desempenho de tripulações e de aeronaves, a fim de difundir a imagem da FAB para os públicos interno e externo. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

23. 22) Ensaio em Voo (Eso Voo) é a Ação que consiste em empregar Meios Aeroespaciais com o propósito de obter conhecimentos referentes às qualidades de voo e ao desempenho das aeronaves, bem como os relacionados ao desempenho e características de sistemas em geral. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

24. 23) Escolta (Esct) é a Ação que consiste em empregar Meios Aeroespaciais para prover proteção dedicada às surtidas amigas ou proteção às aeronaves de alto valor. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

25. 24) Evacuação Aeromédica (EVAM) é a Ação que consiste em empregar Meios Aeroespaciais para remover pessoas feridas ou doentes, geralmente com prestação de assistência médica especializada a bordo, de um local onde tenham recebido assistência inicial para locais onde possam receber tratamento médico adequado. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

26. 25) Exfiltração Aérea (Exfl Ae) é a Ação que consiste em empregar Meios Aeroespaciais para retirar, de uma determinada região, tropas terrestres ou forças paraquedistas e seus equipamentos e colocá-los em local seguro ou o de origem, após a realização de um Assalto Aeroterrestre ou de uma Infiltração Aérea. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

27. 26) Gerenciamento da Navegação Aérea (GNA) é a Ação que consiste em empregar Meios de Força Aérea para, por intermédio da prestação dos serviços de navegação aérea, prover o gerenciamento do fluxo dos movimentos aéreos, bem como promover a segurança da navegação aérea no espaço aéreo brasileiro. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

28. 27) Gerenciamento e Vigilância do Tráfego Espacial (GVTE) é a Ação que consiste em empregar Meios Aeroespaciais e de Força Aérea para detectar, identificar e acompanhar plataformas espaciais acima da Linha Kármán (limite convencionado que fica a uma altitude de 100 km acima do nível do mar, usado para definir o limite entre a atmosfera terrestre e o espaço exterior). *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

29. 28) Guiamento Aéreo Avançado (GAA) é a Ação que consiste em empregar Meios de Força Aérea para coordenar, A PARTIR DO SOLO, o ataque de aeronaves contra alvos oponentes. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

30. 29) Infiltração Aérea (Infl Ae) é a Ação que consiste em empregar Meios Aeroespaciais para infiltrar Forças Especiais no território inimigo, a fim de realizar ações específicas ou visando a facilitar ou apoiar o emprego futuro e maciço das Forças de combate. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

31. 30) Inspeção em Voo (Insp V) é a Ação que consiste em empregar Meios Aeroespaciais para executar atividades necessárias à aferição e correção de equipamentos empregados pelo Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB), com o objetivo de efetuar correções e verificar a sua eficiência, com o foco na melhoria contínua de seu desempenho técnico-operacional. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

32. 31) Instrução Aérea (Instr Ae) é a Ação que consiste em empregar Meios Aeroespaciais para formar ou adestrar tripulantes para o cumprimento das diversas Ações de Força Aérea. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

33. 32) Inteligência (Intlg) é a atividade que consiste em empregar Meios de Força Aérea para coletar, processar, analisar, produzir e difundir conhecimento sobre o oponente e para salvaguardar o conhecimento sensível das forças amigas. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

34. 33) Interferência Eletrônica (Interf Elt) é a Ação que consiste em empregar Meios de Força Aérea para reduzir ou impedir o uso do espectro eletromagnético pelo oponente. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

35. 34) Lançamento de Cargas Úteis ao Espaço Exterior (LCEE) é a ação de preparar, lançar e rastrear cargas úteis acima da Linha Kármán com propósitos variados, desde atividades relacionadas a voos suborbitais, orbitais ou para o espaço profundo. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

36. 35) Logística (Log) é a Ação que consiste em empregar Meios Aeroespaciais e de Força Aérea para prever, prover e manter recursos e serviços de interesse para as operações militares ou ações governamentais. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

37. 36) Minagem Aérea (Min Ae) é a Ação que consiste em empregar Meios Aeroespaciais para obstrução de tráfego e para destruição de embarcações de superfície e submarinas inimigas por intermédio de lançamento aéreo de minas marítimas, com vistas a preservar áreas marítimas e costeiras de interesse estratégico. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

38. 37) Operações Psicológicas (Op Psc) são as Ações que consistem em empregar Meios de Força Aérea em tempos de paz, crise ou guerra, direcionadas a um público-alvo inimigo, amigo ou neutro para influenciar comportamentos, atitudes, sentimentos, emoções e opiniões, de maneira a facilitar a conquista dos objetivos, sejam eles políticos, estratégicos, operacionais ou táticos estabelecidos no planejamento. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

39. 38) Patrulha Marítima (PATMAR) é a Ação que consiste em empregar Meios Aeroespaciais para detectar, localizar, identificar, acompanhar, limitar o movimento ou neutralizar embarcações oponentes, sejam meios de superfície, em águas interiores e espaços marítimos de interesse das operações navais. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

40. 39) Polícia da Aeronáutica (PA) é a Ação que consiste em empregar Meios de Força Aérea para manter a lei e a ordem no interior de instalações militares ou em áreas de interesse da Força Aérea. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

41. 40) Policiamento do Espaço Aéreo (PEA) é a Ação que consiste em empregar Meios Aeroespaciais e de Força Aérea para detectar, identificar, acompanhar e neutralizar tráfegos aéreos ilícitos, que ingressem ou utilizem o espaço aéreo de interesse em tempo de paz. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

41 a 50/54

APÊNDICE A – Questionário (continuação)

42. 41) Posto de Comunicação Aeroespacial (P Com-Aepc) é a Ação que consiste em empregar Meios Aeroespaciais para assegurar o fluxo de informações entre forças amigas no TO. A Ação tem seu uso principal nos enlaces entre os Órgãos de Controle de Operações Aéreas Militares (OCOAM) e as aeronaves cumprindo diversos tipos de missões aéreas, normalmente, à baixa altura, em regiões onde houver falhas ou inexistência de equipamentos terrestres. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

43. 42) Reabastecimento em Voo (REVO) é a Ação que consiste em empregar Meios Aeroespaciais para ampliar a autonomia e o alcance das aeronaves amigas, por meio da transferência de combustível entre aeronaves em voo. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

44. 43) Reconhecimento Aeroespacial (Rec Aepc) é a ação que consiste em empregar Meios Aeroespaciais para detectar, identificar, coletar e difundir dados específicos sobre forças oponentes e áreas de interesse. A Ação de Reconhecimento Aeroespacial constitui importante instrumento para a elaboração de planejamentos e a tomada de decisões em diversos níveis. Basicamente, o Reconhecimento Aeroespacial é parte integrante da IVR e, por meio dele, busca-se obter dados, protegidos ou não, do inimigo e outros de interesse governamental. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

45. 44) Reconhecimento Armado (Rec A) é a Ação que consiste em empregar Meios Aeroespaciais para detectar, identificar, neutralizar ou destruir alvos oponentes fixos, estacionários ou móveis, na superfície, em uma área ou rota previamente selecionada. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

46. 45) Reconhecimento Especial (Rec Esp) é a Ação que consiste em empregar Meios de Força Aérea, em ambientes longínquos, hostis ou sob controle do inimigo, para obter ou confirmar, a partir do solo, conhecimentos específicos sobre o Poder Aeroespacial oponente. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

47. 46) Ressuprimento Aéreo (Resup Ae) é a Ação que consiste em empregar Meios Aeroespaciais para entregar equipamentos e suprimentos necessários às ações de combate das Forças amigas, por meio de lançamento de cargas, visando manter ou ampliar a sua capacidade de combate. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

48. 47) Segurança das Instalações (Seg Inst) é a Ação que consiste em empregar Meios de Força Aérea para assegurar, em caráter rotineiro, a integridade do patrimônio e das instalações de interesse da Força Aérea. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

49. 48) Socorro em Voo (Scr V) é a Ação que consiste em empregar Meios Aeroespaciais para prestar apoio, a partir de uma aeronave em voo, a aeronaves em emergência, interceptando-as, assistindo-as e, eventualmente, orientando-as para o pouso. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

50. 49) Supressão de Defesa Antiaérea Inimiga (SDAI) é a Ação que consiste em empregar Meios Aeroespaciais para destruir, neutralizar ou degradar a capacidade de defesa antiaérea e de C2 do inimigo, em determinada área e por um período de tempo, usando energia eletromagnética ou armamento cinético. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

51. 50) Transporte Aéreo Logístico (TAL) é a Ação que consiste em empregar Meios Aeroespaciais para deslocar pessoal e material, a fim de atender a necessidades logísticas e de ligação, de interesse para as operações militares ou ações governamentais por meio de pouso, carga e descarga das aeronaves. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

51 a 55/54

52. 51) Transporte Especial (Trnp Esp) é a Ação que consiste em empregar Meios Aeroespaciais para transportar autoridades nacionais ou estrangeiras, quando determinado pela autoridade competente. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

53. 52) Varredura (Var) é a Ação que consiste em empregar Meios Aeroespaciais para detectar e neutralizar aeronaves inimigas e alvos de oportunidade, a fim de dominar uma porção específica do espaço aéreo de interesse e por período limitado. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

54. 53) Vigilância Aérea (Vig Ae) é a ação que consiste em empregar Meios Aeroespaciais e de Força Aérea para detectar, identificar, acompanhar, coletar e difundir informações de área de interesse, por meio da coleta de sinais e imagens de um alvo específico ou não, em tempo real. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE A – Questionário (continuação)

55. 54) Vigilância e Controle do Espaço Aéreo (VCEA) é a Ação que consiste em empregar, da superfície, Meios de Força Aérea para detectar, identificar, acompanhar e controlar AERONAVES em espaço aéreo de interesse, a fim de contribuir para a preservação da soberania no espaço aéreo brasileiro e assegurar máxima segurança ao tráfego aéreo em geral. A VCEA feita do ar denomina-se Controle e Alarme em Voo. *

Marcar apenas uma oval por linha.

	1	2	3	4	5
Ataque	◯	◯	◯	◯	◯
Proteção	◯	◯	◯	◯	◯
Exploração	◯	◯	◯	◯	◯

APÊNDICE B – Respostas ao questionário

Tabela 5 – Respostas ao questionário.

(continua)

Ação de Força Aérea	Ação cibernética	Avaliação do especialista							Soma, média e desvio padrão (DP)		
		ESP 1	ESP 2	ESP 3	ESP 4	ESP 5	ESP 6	ESP 7	Soma	Média	DP
AFA02	Ataque	4	5	5	4	5	5	4	32	4,57	0,53
AFA09	Ataque	4	5	5	4	5	5	4	32	4,57	0,53
AFA33	Ataque	4	5	4	5	5	5	4	32	4,57	0,53
AFA49	Ataque	4	5	5	4	5	5	4	32	4,57	0,53
AFA15	Ataque	4	5	3	4	5	5	4	30	4,29	0,76
AFA29	Ataque	4	5	3	4	5	5	4	30	4,29	0,76
AFA52	Ataque	4	5	3	4	5	5	4	30	4,29	0,76
AFA19	Ataque	4	5	4	4	4	3	4	28	4,00	0,58
AFA37	Ataque	4	5	1	5	4	5	4	28	4,00	1,41
AFA06	Ataque	3	5	2	4	5	5	3	27	3,86	1,21
AFA03	Ataque	3	5	3	4	4	5	2	26	3,71	1,11
AFA05	Ataque	3	5	3	4	4	5	2	26	3,71	1,11
AFA16	Ataque	1	5	5	4	3	5	3	26	3,71	1,50
AFA28	Ataque	4	5	2	4	5	5	1	26	3,71	1,60
AFA07	Ataque	4	5	2	4	5	1	4	25	3,57	1,51
AFA32	Ataque	3	5	2	5	2	4	4	25	3,57	1,27
AFA34	Ataque	5	5	1	4	3	5	1	24	3,43	1,81
AFA36	Ataque	4	4	4	4	2	5	1	24	3,43	1,40
AFA38	Ataque	4	5	1	4	4	5	1	24	3,43	1,72
AFA41	Ataque	4	5	3	4	3	3	2	24	3,43	0,98
AFA44	Ataque	4	5	1	4	5	1	4	24	3,43	1,72
AFA18	Ataque	3	5	1	5	2	3	4	23	3,29	1,50
AFA40	Ataque	5	5	1	5	5	1	1	23	3,29	2,14
AFA45	Ataque	4	4	2	3	5	1	4	23	3,29	1,38
AFA53	Ataque	4	5	2	4	4	3	1	23	3,29	1,38
AFA04	Ataque	3	5	2	4	4	2	2	22	3,14	1,21
AFA54	Ataque	4	5	2	4	3	3	1	22	3,14	1,35
AFA08	Ataque	4	5	1	5	2	3	1	21	3,00	1,73
AFA10	Ataque	2	5	2	4	3	3	2	21	3,00	1,15
AFA12	Ataque	4	5	2	4	2	3	1	21	3,00	1,41
AFA17	Ataque	5	5	1	4	4	1	1	21	3,00	1,91
AFA25	Ataque	2	5	1	4	4	1	4	21	3,00	1,63
AFA13	Ataque	4	5	1	5	1	3	1	20	2,86	1,86
AFA23	Ataque	3	5	1	4	4	1	2	20	2,86	1,57
AFA39	Ataque	4	4	1	5	4	1	1	20	2,86	1,77
AFA43	Ataque	4	5	1	4	2	3	1	20	2,86	1,57
AFA11	Ataque	4	5	1	5	2	1	1	19	2,71	1,89
AFA20	Ataque	1	5	1	4	2	3	3	19	2,71	1,50
AFA27	Ataque	4	5	2	4	2	1	1	19	2,71	1,60
AFA26	Ataque	4	5	1	4	2	1	1	18	2,57	1,72
AFA30	Ataque	4	5	1	3	2	1	2	18	2,57	1,51
AFA46	Ataque	4	5	1	4	2	1	1	18	2,57	1,72

(continuação)

Ação de Força Aérea	Ação cibernética	Avaliação do especialista							Soma, média e desvio padrão (DP)		
		ESP 1	ESP 2	ESP 3	ESP 4	ESP 5	ESP 6	ESP 7	Soma	Média	DP
AFA14	Ataque	4	3	1	5	2	1	1	17	2,43	1,62
AFA22	Ataque	3	5	1	3	1	3	1	17	2,43	1,51
AFA31	Ataque	4	5	1	3	1	1	2	17	2,43	1,62
AFA35	Ataque	4	4	1	5	1	1	1	17	2,43	1,81
AFA42	Ataque	4	4	1	4	2	1	1	17	2,43	1,51
AFA47	Ataque	4	5	1	4	1	1	1	17	2,43	1,81
AFA50	Ataque	4	3	1	4	2	1	1	16	2,29	1,38
AFA51	Ataque	4	4	1	4	1	1	1	16	2,29	1,60
AFA21	Ataque	1	4	1	3	2	3	1	15	2,14	1,21
AFA24	Ataque	3	5	1	3	1	1	1	15	2,14	1,57
AFA01	Ataque	4	5	1	1	1	1	1	14	2,00	1,73
AFA48	Ataque	2	5	1	3	1	1	1	14	2,00	1,53
AFA54	Exploração	4	5	5	5	5	5	4	33	4,71	0,49
AFA02	Exploração	3	5	5	5	5	5	4	32	4,57	0,79
AFA10	Exploração	4	5	5	5	5	4	4	32	4,57	0,53
AFA15	Exploração	3	5	5	5	5	5	4	32	4,57	0,79
AFA20	Exploração	4	5	5	5	4	5	4	32	4,57	0,53
AFA28	Exploração	3	5	5	5	5	5	4	32	4,57	0,79
AFA32	Exploração	3	5	5	5	5	5	4	32	4,57	0,79
AFA43	Exploração	3	5	5	5	5	5	4	32	4,57	0,79
AFA52	Exploração	3	5	5	5	5	5	4	32	4,57	0,79
AFA53	Exploração	3	5	5	5	5	5	4	32	4,57	0,79
AFA04	Exploração	2	5	5	5	5	5	4	31	4,43	1,13
AFA09	Exploração	2	5	5	5	5	5	4	31	4,43	1,13
AFA41	Exploração	4	5	4	5	4	5	4	31	4,43	0,53
AFA49	Exploração	3	5	4	5	5	5	4	31	4,43	0,79
AFA06	Exploração	3	5	5	5	4	5	3	30	4,29	0,95
AFA07	Exploração	2	5	5	5	4	5	4	30	4,29	1,11
AFA12	Exploração	4	5	5	5	3	5	3	30	4,29	0,95
AFA26	Exploração	3	5	3	5	5	5	4	30	4,29	0,95
AFA03	Exploração	3	5	5	5	4	3	4	29	4,14	0,90
AFA05	Exploração	3	5	4	5	5	5	2	29	4,14	1,21
AFA16	Exploração	3	5	2	5	5	5	4	29	4,14	1,21
AFA17	Exploração	1	5	4	5	5	5	4	29	4,14	1,46
AFA18	Exploração	4	5	2	5	4	5	4	29	4,14	1,07
AFA25	Exploração	3	5	5	5	4	3	4	29	4,14	0,90
AFA29	Exploração	2	5	4	5	4	5	4	29	4,14	1,07
AFA33	Exploração	3	5	3	5	4	5	4	29	4,14	0,90
AFA37	Exploração	3	5	4	5	3	5	4	29	4,14	0,90
AFA38	Exploração	3	5	4	5	4	5	3	29	4,14	0,90
AFA44	Exploração	3	5	3	5	4	5	4	29	4,14	0,90
AFA45	Exploração	3	4	4	5	4	5	4	29	4,14	0,69
AFA08	Exploração	3	5	1	5	5	5	4	28	4,00	1,53
AFA19	Exploração	2	5	3	5	4	5	4	28	4,00	1,15
AFA23	Exploração	3	5	1	5	5	5	4	28	4,00	1,53
AFA27	Exploração	3	5	3	4	4	5	4	28	4,00	0,82

(continuação)

Ação de Força Aérea	Ação cibernética	Avaliação do especialista							Soma, média e desvio padrão (DP)		
		ESP 1	ESP 2	ESP 3	ESP 4	ESP 5	ESP 6	ESP 7	Soma	Média	DP
AFA30	Exploração	4	5	1	5	4	5	4	28	4,00	1,41
AFA14	Exploração	3	3	5	5	3	5	3	27	3,86	1,07
AFA34	Exploração	3	5	3	5	5	5	1	27	3,86	1,57
AFA40	Exploração	4	5	3	5	4	5	1	27	3,86	1,46
AFA47	Exploração	4	5	3	5	4	1	4	26	3,71	1,38
AFA36	Exploração	3	4	3	5	4	5	1	25	3,57	1,40
AFA39	Exploração	3	4	3	5	4	5	1	25	3,57	1,40
AFA01	Exploração	4	5	1	5	3	4	1	23	3,29	1,70
AFA11	Exploração	2	5	1	5	2	5	3	23	3,29	1,70
AFA51	Exploração	4	4	1	5	3	5	1	23	3,29	1,70
AFA13	Exploração	3	5	1	5	4	3	1	22	3,14	1,68
AFA21	Exploração	2	4	3	3	4	5	1	22	3,14	1,35
AFA31	Exploração	4	5	1	4	3	1	4	22	3,14	1,57
AFA22	Exploração	1	5	2	3	4	5	1	21	3,00	1,73
AFA35	Exploração	2	4	4	5	3	1	2	21	3,00	1,41
AFA46	Exploração	3	5	2	5	4	1	1	21	3,00	1,73
AFA42	Exploração	3	4	2	5	4	1	1	20	2,86	1,57
AFA24	Exploração	2	5	2	4	4	1	1	19	2,71	1,60
AFA48	Exploração	2	5	1	5	3	1	1	18	2,57	1,81
AFA50	Exploração	3	3	1	5	4	1	1	18	2,57	1,62
AFA17	Proteção	4	5	5	4	5	5	4	32	4,57	0,53
AFA54	Proteção	4	5	4	4	5	5	4	31	4,43	0,53
AFA01	Proteção	4	5	4	5	5	5	2	30	4,29	1,11
AFA04	Proteção	3	5	4	4	5	5	4	30	4,29	0,76
AFA19	Proteção	2	5	5	4	5	5	4	30	4,29	1,11
AFA23	Proteção	2	5	5	4	5	5	4	30	4,29	1,11
AFA25	Proteção	3	5	4	4	5	5	4	30	4,29	0,76
AFA26	Proteção	2	5	5	4	5	5	4	30	4,29	1,11
AFA34	Proteção	4	5	3	4	5	5	4	30	4,29	0,76
AFA41	Proteção	4	5	4	4	5	4	4	30	4,29	0,49
AFA52	Proteção	3	5	4	4	5	5	4	30	4,29	0,76
AFA03	Proteção	2	5	4	4	5	5	4	29	4,14	1,07
AFA10	Proteção	2	5	4	4	5	5	4	29	4,14	1,07
AFA14	Proteção	4	3	5	4	5	5	3	29	4,14	0,90
AFA18	Proteção	2	5	4	4	5	5	4	29	4,14	1,07
AFA27	Proteção	2	5	4	4	5	5	4	29	4,14	1,07
AFA51	Proteção	4	4	3	4	5	5	4	29	4,14	0,69
AFA07	Proteção	4	5	4	4	4	5	2	28	4,00	1,00
AFA08	Proteção	3	5	5	4	2	5	4	28	4,00	1,15
AFA20	Proteção	2	5	3	4	5	5	4	28	4,00	1,15
AFA31	Proteção	3	5	3	3	5	5	4	28	4,00	1,00
AFA32	Proteção	3	5	4	4	3	5	4	28	4,00	0,82
AFA33	Proteção	3	5	2	4	5	5	4	28	4,00	1,15
AFA40	Proteção	5	5	3	4	5	5	1	28	4,00	1,53
AFA06	Proteção	4	5	3	4	4	5	2	27	3,86	1,07
AFA30	Proteção	3	5	1	4	5	5	4	27	3,86	1,46
AFA28	Proteção	4	5	2	4	4	5	4	28	4,00	1,00

(conclusão)

Ação de Força Aérea	Ação cibernética	Avaliação do especialista							Soma, média e desvio padrão (DP)		
		ESP 1	ESP 2	ESP 3	ESP 4	ESP 5	ESP 6	ESP 7	Soma	Média	DP
AFA53	Proteção	2	5	3	4	4	5	4	27	3,86	1,07
AFA22	Proteção	2	5	5	3	5	5	1	26	3,71	1,70
AFA46	Proteção	3	5	3	4	5	5	1	26	3,71	1,50
AFA47	Proteção	2	5	5	4	5	1	4	26	3,71	1,60
AFA02	Proteção	2	5	1	4	5	5	3	25	3,57	1,62
AFA15	Proteção	3	5	1	4	4	5	3	25	3,57	1,40
AFA35	Proteção	3	4	4	4	5	1	4	25	3,57	1,27
AFA05	Proteção	2	5	1	4	3	5	4	24	3,43	1,51
AFA16	Proteção	2	5	1	4	5	3	4	24	3,43	1,51
AFA21	Proteção	2	4	4	3	5	5	1	24	3,43	1,51
AFA24	Proteção	1	5	3	4	5	5	1	24	3,43	1,81
AFA38	Proteção	4	5	2	4	5	3	1	24	3,43	1,51
AFA12	Proteção	1	5	5	4	4	3	1	23	3,29	1,70
AFA43	Proteção	2	5	3	4	5	3	1	23	3,29	1,50
AFA48	Proteção	2	5	1	4	5	5	1	23	3,29	1,89
AFA49	Proteção	3	5	2	4	4	1	4	23	3,29	1,38
AFA29	Proteção	2	5	1	4	5	1	4	22	3,14	1,77
AFA39	Proteção	1	4	2	4	5	5	1	22	3,14	1,77
AFA09	Proteção	1	5	1	4	4	3	3	21	3,00	1,53
AFA11	Proteção	3	5	1	4	4	3	1	21	3,00	1,53
AFA36	Proteção	4	4	2	4	5	1	1	21	3,00	1,63
AFA45	Proteção	4	4	3	3	5	1	1	21	3,00	1,53
AFA37	Proteção	2	5	2	4	4	1	2	20	2,86	1,46
AFA42	Proteção	3	4	2	4	5	1	1	20	2,86	1,57
AFA44	Proteção	2	5	2	4	5	1	1	20	2,86	1,77
AFA13	Proteção	2	5	1	4	2	3	2	19	2,71	1,38
AFA50	Proteção	2	3	2	4	5	1	1	18	2,57	1,51
Média		3,10	4,80	2,76	4,28	3,95	3,66	2,67	25,21	3,60	1,28

Fonte: O autor

APÊNDICE C – Soma das ações cibernéticas para cada ação de Força Aérea

Tabela 6 – Soma das ações cibernéticas para cada ação de Força Aérea.

(continua)

Ação de força aérea	Ataque cibernético (soma)	Proteção cibernética (soma)	Exploração cibernética (soma)	Total (soma)	Média[9]
AFA52	30	30	32	92	4,38
AFA02	32	25	32	89	4,24
AFA33	32	28	29	89	4,24
AFA15	30	25	32	87	4,14
AFA19	28	30	28	86	4,10
AFA28	26	28	32	86	4,10
AFA49	32	23	31	86	4,10
AFA54	22	31	33	86	4,10
AFA32	25	28	32	85	4,05
AFA41	24	30	31	85	4,05
AFA03	26	29	29	84	4,00
AFA06	27	27	30	84	4,00
AFA09	32	21	31	84	4,00
AFA04	22	30	31	83	3,95
AFA07	25	28	30	83	3,95
AFA10	21	29	32	82	3,90
AFA17	21	32	29	82	3,90
AFA53	23	27	32	82	3,90
AFA18	23	29	29	81	3,86
AFA29	30	22	29	81	3,86
AFA34	24	30	27	81	3,86
AFA25	21	30	29	80	3,81
AFA05	26	24	29	79	3,76
AFA16	26	24	29	79	3,76
AFA20	19	28	32	79	3,76
AFA23	20	30	28	78	3,71
AFA26	18	30	30	78	3,71
AFA40	23	28	27	78	3,71
AFA08	21	28	28	77	3,67
AFA37	28	20	29	77	3,67
AFA38	24	24	29	77	3,67
AFA27	19	29	28	76	3,62
AFA43	20	23	32	75	3,57
AFA12	21	23	30	74	3,52
AFA14	17	29	27	73	3,48
AFA30	18	27	28	73	3,48
AFA44	24	20	29	73	3,48
AFA45	23	21	29	73	3,48
AFA36	24	21	25	70	3,33
AFA47	17	26	26	69	3,29
AFA51	16	29	23	68	3,24
AFA01	14	30	23	67	3,19

[9] A média de concordância para cada ação de Força Aérea é calculada somando-se todas as respectivas avaliações dos especialistas em cada ação Cibernética e dividindo por 21 (7 avaliações para cada ação Cibernética, o que totaliza 21).

(conclusão)

Ação de força aérea	Ataque cibernético (soma)	Proteção cibernética (soma)	Exploração cibernética (soma)	Total (soma)	Média
AFA31	17	28	22	67	3,19
AFA39	20	22	25	67	3,19
AFA46	18	26	21	65	3,10
AFA22	17	26	21	64	3,05
AFA11	19	21	23	63	3,00
AFA35	17	25	21	63	3,00
AFA13	20	19	22	61	2,90
AFA21	15	24	22	61	2,90
AFA24	15	24	19	58	2,76
AFA42	17	20	20	57	2,71
AFA48	14	23	18	55	2,62
AFA50	16	18	18	52	2,48
MÉDIA	22,20	25,96	27,46	75,63	3,60

Fonte: O autor

ANEXO A – Ações de Força Aérea

Tabela 7 – Ações de Força Aérea

AÇÕES DE FORÇA AÉREA	
AFA01. Ação Cívico-Social	AFA28. Guiamento Aéreo Avançado
AFA02. Ação Direta	AFA29. Infiltração Aérea
AFA03. Alerta em Voo	AFA30. Inspeção em Voo
AFA04. Alerta na Base	AFA31. Instrução Aérea
AFA05. Antissubmarino	AFA32. Inteligência
AFA06. Apoio Aéreo Aproximado	AFA33. Interferência Eletrônica
AFA07. Assalto Aeroterrestre	AFA34. Lanç. de Cargas Úteis ao Espaço
AFA08. Assuntos Civis	AFA35. Logística
AFA09. Ataque	AFA36. Minagem Aérea
AFA10. Autodefesa de Superfície	AFA37. Operações Psicológicas
AFA11. Busca e Salvamento	AFA38. Patrulha Marítima
AFA12. Busca e Salvamento em Combate	AFA39. Polícia da Aeronáutica
AFA13. Combate a Incêndio em Voo	AFA40. Policiamento do Espaço Aéreo
AFA14. Comunicação Social	AFA41. Posto de Comunicação Aeroespacial
AFA15. Contraterrorismo	AFA42. Reabastecimento em Voo
AFA16. Controle Aéreo Avançado	AFA43. Reconhecimento Aeroespacial
AFA17. Controle e Alarme em Voo	AFA44. Reconhecimento Armado
AFA18. Controle Satelital	AFA45. Reconhecimento Especial
AFA19. Defesa Antiaérea	AFA46. Ressuprimento Aéreo
Sem Numeração. Defesa Cibernética	AFA47. Segurança das Instalações
AFA20. Defesa Biológica, Nuclear, Química e Radiológica	AFA48. Socorro em Voo
AFA21. Demonstração Aérea	AFA49. Supressão de Defesa Antiaérea Inimiga
AFA22. Ensaio em Voo	AFA50. Transporte Aéreo Logístico
AFA23. Escolta	AFA51. Transporte Especial
AFA24. Evacuação Aeromédica	AFA52. Varredura
AFA25. Exfiltração Aérea	AFA53. Vigilância Aérea
AFA26. Gerenciamento da Navegação Aérea	AFA54. Vigilância e Controle do Espaço Aéreo
AFA27. Gerenciamento e Vigilância do Tráfego Espacial	

Fonte: Brasil (2020b, p. 47)