CIBERGUERRA E CAPACITAÇÃO MILITAR: UMA ANÁLISE COMPARATIVA ENTRE O CURSO DE FORMAÇÃO DE OFICIAIS DE INFANTARIA DA AFA E DA USAFA EM RELAÇÃO ÀS AMEAÇAS ATUAIS[1]

CYBER WARFARE AND MILITARY TRAINING*: A COMPARATIVE ANALYSIS BETWEEN THE AFA AND USAFA INFANTRY OFFICER TRAINING COURSES IN RELATION TO CURRENT THREATS*

Gustavo Corrêa[2]
André Jorge Dias de Moura Júnior[3]

RESUMO

A rápida evolução tecnológica e a popularização da internet proporcionaram o surgimento de um novo domínio, o ciberespaço. Esse domínio potencializou a criação de ameaças à defesa nacional e apresentou-se como um novo domínio de combate no teatro de operações, exigindo a capacitação de profissionais militares especializados nessa área. No Brasil, a Estratégia Nacional de Defesa (END) reconhece o meio cibernético como um dos setores estratégicos e o Ministério da Defesa (MD) incentiva a capacitação dos militares nessa área. Assim, o MD acionou um Grupo de Trabalho (GT) para definir um currículo único de ensino de cibernética para as escolas militares. Para tal, as academias militares de formação estão adaptando seus métodos de ensino para atender às demandas do domínio do ciberespaço. Nesse sentido, este trabalho possui o objetivo geral de analisar a grade curricular do Curso de Formação de Oficiais de Infantaria da Aeronáutica, com o foco na área de cibernética, a fim de que se reflita sobre as competências desenvolvidas pelo cadete nessa temática. Para alcançá-lo, possui os seguintes objetivos específicos: explicar o domínio do ciberespaço junto aos conceitos básicos de segurança cibernética, ciberguerra e ciberataque; identificar as ameaças cibernéticas mais relevantes na contemporaneidade; e comparar a grade curricular na área de cibernética dos cadetes de Infantaria da AFA com a dos cadetes da USAFA e com as atuais ameaças cibernéticas. A pesquisa adota uma abordagem qualitativa, dividida em análise documental e revisão bibliográfica. Para isso, foram examinados documentos oficiais e currículos da Academia da Força Aérea (AFA) e da *United States Air Force Academy* (USAFA). Os resultados indicam que a AFA incorporou disciplinas específicas no seu currículo, contemplando fundamentos de segurança e guerra cibernética, embora com um escopo mais restrito em comparação à formação oferecida pela USAFA, e que o currículo brasileiro abrange parcialmente as atuais ameaças cibernéticas. Conclui-se também que, apesar de a formação dos cadetes de Infantaria da Aeronáutica estar avançando na integração do domínio cibernético, ainda há espaço para ampliar o treinamento prático e as competências operacionais. O estudo destaca ainda a necessidade de aprofundar a formação cibernética para fortalecer a capacidade defensiva da Força Aérea Brasileira (FAB).

Palavras-chave: Segurança cibernética; Ciberespaço; Academia da Força Aérea; *United States Air Force Academy;* Guerra cibernética

---

[1] Artigo de Conclusão de Curso apresentado ao Curso de Formação de Oficiais de Infantaria (CFOInf) da Academia da Força Aérea (AFA).

[2] Cadete de Infantaria do 4º Esquadrão (Turma *Ártemis*, 2025).

[3] Capitão Intendente formado pela AFA no ano de 2016. Especialista e mestre em Relações Internacionais pela Universidade de Brasília (UnB). E-mail: andrediasajdmj@fab.mil.br.

ABSTRACT

Rapid technological evolution and the popularization of the internet have led to the emergence of a new domain, cyberspace. This domain has potentially created threats to national defence and has presented itself as a new combat front in the theater of operations, requiring the training of military professionals specialized in this area. In Brazil, the National Defense Strategy (END) recognizes the cyber environment as one of the strategic sectors and the Ministry of Defense (MD) encourages military training in this area. The MD therefore set up a Working Group (WG) to define a single cyber teaching curriculum for military schools. To this end, the military training academies are adapting their teaching methods to meet the demands of the cyberspace domain. With this in mind, this work has the general objective of analyzing the curriculum of the Air Force Infantry Officer Training Course, focusing on the area of cybernetics, in order to reflect on the skills developed by the cadet in this area. To achieve this, it has the following specific objectives: to explain the domain of cyberspace together with the basic concepts of cyber security, cyber warfare and cyber attack; to identify the most relevant cyber threats in contemporary times; and to compare the cyber curriculum of AFA infantry cadets with that of USAFA cadets and with current cyber threats. The research adopts a qualitative approach, divided into documentary analysis and a literature review. Official documents and curricula from the Air Force Academy (AFA) and the United States Air Force Academy (USAFA) were examined. The results indicate that the AFA has incorporated specific subjects into its curriculum, covering the fundamentals of security and cyber warfare, albeit with a narrower scope compared to the training offered by the USAFA, and that the Brazilian curriculum partially covers current cyber threats. It also concludes that, although the training of Air Force infantry cadets is making progress in integrating the cyber domain, there is still room to expand practical training and operational skills. The study also highlights the need to deepen cyber training in order to strengthen the defensive capacity of the Brazilian Air Force (FAB).

Keywords: Cybersecurity; Cyberspace; Brazilian Air Force Academy; United States Air Force Academy; Cyber warfare

INTRODUÇÃO

O ciberespaço, outrora um ambiente nebuloso e pouco explorado, transformou-se em um ambiente estratégico de disputa, no qual nações e seus exércitos passaram a atuar ativamente. Esse ambiente é foco constante de investimentos e desenvolvimento contínuo, tanto por parte dos governos quanto das empresas privadas. A exemplo disso, nota-se que o Departamento do Exército dos Estados Unidos está avançando com o seu projeto de Proteção Cibernética de Infraestrutura Crítica do Exército (ACICP), a fim de proteger infraestruturas críticas contra possíveis ataques cibernéticos, destinando, para esse fim, cerca de meio bilhão de dólares (Obis, 2023).

Com a criação da *Advanced Research Projects Agency Network* (ARPANET) – a primeira

rede de computadores desenvolvida pelo Departamento de Defesa dos Estados Unidos, em 1969 –, as redes passaram a conter informações valiosas, despertando o interesse por invasões e roubo de dados (Hauben, 2007). Diante disso, a evolução das Forças Armadas (FFAA) deve contemplar a formação de seus militares para o enfrentamento das ameaças no domínio cibernético. Com o decorrer dos anos, a evolução da tecnologia inovou também o ambiente de atuação das FA. Desse modo, o meio cibernético passou a integrar os domínios operacionais reconhecidos pelas Forças Armadas, como o ambiente naval, aéreo, espacial e terrestre. Assim, faz-se necessário reconhecer o ciberespaço como mais um domínio operacional.

Nesse sentido, é interessante citar a Rússia devido aos seus embates com os Estados Unidos e aos seus ataques recentes à Ucrânia. Sabe-se que a cibernética russa não é tratada como um campo separado, mas, sim, uma vertente do campo informacional (Connell; Vogler, 2017). Esse conceito, utilizado pelos teóricos militares russos, abrange operações na internet e atividades de espionagem, sendo a cibernética apenas um dos meios de conduzir o combate (Connell; Vogler, 2017). Já no Brasil, existe o Comando de Defesa Cibernética (Com D Ciber) que é um comando conjunto em que há a interoperabilidade entre as Forças Armadas brasileiras e cuja missão envolve o uso do espaço cibernético de forma a planejar e executar atividades em prol aos interesses nacionais, além de restringir o ciberespaço àqueles que são contra os interesses do país (Brasil, 2023).

Para elucidar a temática, pode-se citar o ataque ao telefone via satélite Inmarsat instalado no avião presidencial – o *airbus* VC-1A, pertencente à FAB –, com o qual a presidente Dilma Rousseff se comunicava com o mundo (EUA..., 2015). Conforme publicado pelo Portal de Notícias G1 (2015), no mesmo ataque cibernético foram grampeados 29 telefones do governo, os quais foram espionados pela Agência Nacional de Segurança dos Estados Unidos (National Security Agency – NSA). Além desse episódio, em 2021, o Brasil enfrentou mais de 88,5 bilhões de tentativas de ciberataques (Fortinet, 2022).

Diante desse contexto, a Estratégia Nacional de Defesa (END), instituída em 2008 e com a versão de 2024 aprovada pelo Congresso Nacional, reconhece a dimensão cibernética como um dos setores estratégicos, além dos setores nuclear e espacial. Em consonância com essa diretriz, o Ministério da Defesa (MD) brasileiro incentiva a capacitação de militares na área cibernética. Em maio de 2021, foi realizado o seminário *A Defesa Cibernética e a Guerra do Futuro*, que reuniu docentes das escolas de formação e aperfeiçoamento das FA, visando integrar o ensino da cibernética nos currículos militares (Brasil, 2021a). Outrossim, o MD criou um Grupo de Trabalho (GT) com a finalidade de definir um currículo único de ensino de cibernética nas escolas vinculadas às Forças

Armadas (Brasil, 2021b).

Considerando a importância já apresentada da dimensão cibernética na guerra contemporânea, é imprescindível capacitar os militares nesta área. Optou-se, assim, o autor do presente trabalho por colaborar na formação dos cadetes de Infantaria da Academia da Força Aérea, a partir da análise de seus currículos e processos formativos, no tocante à cibernética.

Como opção metodológica, a escolha da grade curricular da USAFA como objeto de comparação com a grade curricular do Curso de Formação de Oficiais de Infantaria da Aeronáutica justifica-se pelo fato de essa academia norte-americana ser referência nacional e mundial na educação. Essa academia foi ranqueada em 6° lugar pela Forbes - revista de negócios e economia mais conceituada do país - na área de *STEAM Education*, ou seja, instituições de ensino que oferecem programas nos campos de ciências, tecnologia, engenharia e matemática (USAFA, 2025a). Cabe ressaltar que os Estados Unidos da América (EUA) é uma potência militar reconhecida mundialmente, cujo preparo e poder de suas FA são referências para as demais nações. Por esse motivo, é importante entender o desenvolvimento e a capacitação de seus militares para as novas ameaças à segurança do país.

Ainda no que tange à metodologia, este trabalho utiliza a pesquisa qualitativa de cunho descritivo, cujo foco é analisar e interpretar literaturas e documentos referentes ao tema, e faz revisões bibliográficas na área de guerra cibernética (Marconi; Lakatos, 2017). Os artigos e documentos utilizados no referencial teórico foram encontrados nas bases de dados do Google Acadêmico, da SciELO, da Diretoria de Ensino (DIRENS) da FAB e do site oficial da USAFA. Além disso, foi realizada uma análise comparativa entre a grade curricular dos cadetes de Infantaria da AFA e dos cadetes que optam por cursar a disciplina de cibernética na USAFA, cabe ressaltar que não são todos os cadetes norte-americanos que cursam a graduação na área de cibernética.

Sendo assim, parte-se da seguinte problematização: em que medida as competências previstas na grade curricular dos cadetes de Infantaria da Aeronáutica abrangem as atuais ameaças cibernéticas?

Este artigo justifica-se pelo surgimento de um teatro de operações incerto e com consequências para o mundo real, como o caso do Stuxnet – um vírus utilizado para controlar as centrífugas de enriquecimento de urânio do Irã –, em 2010, que destruiu as estruturas de enriquecimento de urânio daquele país. A inquietação deste autor também decorre da aparente carência de disciplinas que abordam o tema em sua formação, o que pode dificultar a capacitação dos novos oficiais de Infantaria para enfrentar os desafios no campo cibernético, um domínio cada vez

mais relevante no conflito entre nações. Vale ressaltar que o foco do artigo no quadro de Infantaria da Aeronáutica se dá pelo fato de os militares pertencentes a esse quadro atuarem nas Ações de Segurança das Instalações e terem por atribuição, segundo a DCA 205-4: Segurança e Defesa no Comando da Aeronáutica, "a condução de ações ofensivas e defensivas em prol da proteção dos meios de Força Aérea, contribuindo para a preservação do poder de combate da FAB" (Ministério da Defesa, 2020).

Nesse contexto, observa-se a relevância do conhecimento em cibernética nas escolas militares de formação. Assim, investiga-se como o tema é apresentado na formação militar dos cadetes da Aeronáutica, com o foco para o Quadro de Infantaria, visto que, na palestra dada por Juliano Cortinhas, professor da Universidade de Brasília (UnB), atualmente a sociedade está inserida em um contexto de guerra de quinta geração (Possiede, 2020). Isto é, há o emprego massivo de ciberataques.

Portanto, o objetivo geral deste trabalho é analisar a grade curricular do Curso de Formação de Oficiais de Infantaria da Aeronáutica, com o foco na área de cibernética, frente às atuais ameaças. Como mencionado, o Brasil é alvo frequente de ataques cibernéticos, o que ressalta a exposição do país a invasões nesse ambiente e a demanda de profissionais qualificados para atuar nessas situações. Trata-se, então, de uma pesquisa descritiva sobre a forma em que a AFA está proporcionando aos cadetes esse conhecimento específico necessário.

Com base no exposto, foram delineados os seguintes objetivos específicos:

a) Explicar o domínio do ciberespaço junto aos conceitos básicos de segurança cibernética, ciberguerra e ciberataque;
b) Identificar as ameaças cibernéticas mais relevantes na contemporaneidade; e
c) Comparar a grade curricular na área de cibernética dos cadetes de Infantaria da AFA com a dos cadetes da USAFA e com as atuais ameaças cibernéticas.

Para alcançá-los, a pesquisa se inicia explicando a origem do termo "ciberespaço" e conceituando-o. Em um segundo momento, abordam-se conceitos de segurança cibernética, ciberguerra e ciberataque. Em seguida, será realizada uma explicação das ameaças cibernéticas mais relevantes na contemporaneidade. Por fim, analisa-se a grade curricular da AFA e da USAFA com o foco voltado para a área de cibernética.

1 REFERENCIAL TEÓRICO E REVISÃO BIBLIOGRÁFICA

1.1 O CIBERESPAÇO

A ideia de ciberespaço originou-se nos Estados Unidos com o desenvolvimento da ARPANET, a primeira rede de internet criada no mundo (Hauben, 2007). E, utilizando-se dos mesmos protocolos, foi criada a internet, como é conhecida atualmente (Hauben, 2007).

Após o surgimento dessa primeira rede, surgiu o termo "ciberespaço", que foi citado pela primeira vez em 1984 no livro *Neuromancer*, escrito por William Gibson. De maneira mais abstrata, o autor o define como um lugar idealizado pelo operador, caracterizado como uma representação gráfica de dados de todas as máquinas (Gibson, 2008). Nesse sentido, é possível dizer que esse domínio é um espaço não físico no qual todos os computadores estão conectados em rede e suas informações estão disponíveis (Gibson, 2008). Os sistemas de comunicação também estão presentes nesse ambiente, podendo ser acessados por qualquer indivíduo que tenha ou que force o acesso por meio de um ciberataque (Gibson, 2008).

Consequentemente, o conceito de ciberespaço passa a ser crucial no âmbito militar, pois, como apontado pelos autores supracitados, esse ambiente contém informações e dados que podem ser do interesse de cada país, podendo ser utilizado como um teatro de operações, além de alvo de ações militares. Nesse contexto, por exemplo, os governos autoritários restringem o livre acesso à informação de suas populações, desse modo, o domínio sobre a internet torna-se uma ferramenta de poder, permitindo a manipulação das informações (Boas, 2006). Nesse sentido, o ciberespaço se tornou também uma área operacional, pois a atuação nesse domínio é caracterizada como de baixo custo para o Estado e de grande fluidez (Sheldon, 2011). Trata-se ainda de um lugar no qual a cibernética converte os crimes virtuais em consequências para o mundo real, manipula e coleta as informações contidas nesse meio, transformando-as em efeito estratégico (Sheldon, 2011).

Por conseguinte, o *Livro Branco de Defesa Nacional – LBDN* (Brasil, 2020) e a *Estratégia Nacional de Defesa – END* (Brasil, 2016) – documentos brasileiros sobre as atividades de defesa do país – destacam uma especial atenção para a segurança do ciberespaço, cujo setor é essencial para garantir o fluxo informacional e a comunicação do país. Nesse sentido, a seção seguinte abordará o conceito de segurança cibernética.

1.2 SEGURANÇA CIBERNÉTICA

Em 1988, Robert Morris tentou estimar o tamanho da internet. Para isso, desenvolveu um programa capaz de se propagar pelas redes de computadores e que, devido a uma falha no sistema, poderia se replicar indefinidamente (Jajoo, 2021). O programa, conhecido como *Minhoca de Morris*, acabou causando um efeito oposto ao esperado, sobrecarregando a internet e derrubando-a (Jajoo, 2021). Diante desse fato, Morris acidentalmente se tornou pioneiro ao realizar com sucesso um ciberataque e, consequentemente, alertou a sociedade sobre a necessidade de um sistema de proteção digital (Jajoo, 2021). Em resposta, foi criado o *Computer Emergency Response Team (CERT)*, um centro de pesquisas destinado a solucionar problemas que pudessem comprometer a internet (Jajoo, 2021). Esse evento marcou o início do desenvolvimento da doutrina que hoje é conhecida como segurança cibernética.

Segundo o *Department of Homeland Security* (DHS), a segurança cibernética tem o objetivo de prevenir os ciberataques, gerenciando os danos causados pelo acesso não autorizado a informações digitais e a sistemas de comunicação (Cybersecurity, 2009). Ela visa, também, restaurar os dados e esses sistemas no caso de um ataque (Cybersecurity, 2009). Dessa forma, observa-se que essa área tem a finalidade de garantir a confidencialidade e a integridade das informações (Cybersecurity, 2009).

O Livro Verde de Segurança Cibernética no Brasil - uma publicação governamental que detalha situações específicas - define: “a segurança cibernética é a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas” (Brasil, 2010, p. 19). Tendo em vista essa definição, é necessário diferenciá-la do conceito de defesa cibernética. A defesa cibernética, de acordo com a Doutrina Militar de Defesa Cibernética (2023), refere-se a “ações realizadas no espaço cibernético, [...], com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente” (Brasil, 2023, p. 17). Já a segurança cibernética, refere-se à proteção e à prevenção, visto que se pretende garantir a segura utilização da internet – tanto da população civil quanto do meio militar –, assegurando que as informações e os dados não sejam violados por outras entidades. Assim, compreende-se que “defesa” é um termo bélico, com forte abordagem de cunho militar, com o intuito de obter informações e prejudicar o oponente.

Nesse contexto, a importância do conhecimento dessa área é evidenciada nos Estados

Unidos, potência militar reconhecida mundialmente, já que o país investe na sua academia de formação de oficiais, a *United States Air Force Academy* (USAFA), fornecendo a área de segurança cibernética (*Cyber Defense*) como matéria de estudo aos cadetes americanos.

> A disciplina de Defesa Cibernética de uma sequência fundamental de três semanas para alunos de graduação em Ciência Cibernética se concentra nos fundamentos da defesa de rede e forense digital. Os tópicos incluem modelos de segurança, análise de vulnerabilidade, mecanismos de defesa, design e gerenciamento de rede, resposta a incidentes, estruturas de sistema de arquivos, análise de memória não volátil, análise de memória volátil, análise de tráfego de rede, integridade de arquivo, cadeia de custódia e ética (USAFA, 2024, p. 326, tradução nossa).

Logo, as competências para as quais o curso de cibernética americano capacita os oficiais que optaram por cursar essa disciplina são vitais para o combate moderno, sendo igualmente relevantes para os oficiais brasileiros, uma vez que o militar em formação desenvolve estratégias para proteger redes e realizar operações cibernéticas ofensivas, quando necessário, identificar e avaliar potenciais ameaças e conhecer as leis e os regulamentos globais que regem a segurança cibernética.

Nesse sentido, para ilustrar o tema, convém ressaltar que a vigilância do domínio aéreo brasileiro é realizada por uma rede de radares distribuídos pelo país, a qual também controla o tráfego de aeronaves civis. A proteção do espaço aéreo é feita mediante a interceptação de voos ilegais ou de ameaças terroristas. Isso acontece, por exemplo, a partir de estações de controle como a Estação Radar de vigilância aérea em Ponta Porã (MS), com o objetivo de aumentar a eficiência no trabalho de combate a atividades ilícitas na fronteira Oeste do Brasil. Outrossim, o Grupo de Segurança e Defesa de Canoas (BACO) possui a capacidade de monitoramento rápido e em tempo real por meio de Aeronaves Remotamente Pilotadas (ARP), integrando o sistema de vigilância eletrônica da base, sendo assim, uma vulnerabilidade também para um ataque cibernético. Dessa forma, esses dois fatos demonstram vulnerabilidades de ataque, caso não exista uma segurança cibernética bem consolidada, corroborando a necessidade de profissionais capacitados na área em questão.

1.3 CIBERGUERRA E CIBERATAQUE

O manual *Doutrina Militar de Defesa Cibernética*, de 2014, conceitua o termo “ciberguerra” ou “guerra cibernética” da seguinte forma:

> "[...] corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C2 do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC" (Brasil, 2014, p. 19).

Clarke e Knake (2010) definem a guerra cibernética como ações do Estado-nação para interromper ou causar danos a outras nações, por meio de ataques a computadores ou redes sociais. Já Teixeira Júnior, Lopes e Freitas (2017) explicam esse termo como "um estado de coisas em que o poder militar utiliza meios, estratégias e ferramentas no ciberespaço para alcançar seus objetivos". Além disso, a ciberguerra tem como objetivo adquirir informações restritas e destruir ou prejudicar as infraestruturas críticas do Estado (Teixeira Júnior; Lopes; Freitas, 2017), como no caso Stuxnet, em 2010, no qual um *malware* foi capaz de destruir as centrífugas de enriquecimento de urânio iranianas (Lopes; Oliveira, 2014).

Diante desse cenário, é interessante citar o pensamento de Cavelty (2010) sobre ciberguerra. Ele propõe que o termo seja apenas uma vertente dos tipos de conflitos cibernéticos e que, sob a ótica militar, essa guerra seja considerada parte da guerra de informação (Cavelty, 2010). Ademais, o autor afirma que é um tipo de conflito de baixo custo e "limpo" (sem conflitos sangrentos), se comparado a outras formas de conflitos armados (Cavelty, 2010). Cavelty (2010) ainda prevê que no futuro não haverá apenas uma corrida armamentista no ciberespaço, mas também uma corrida para o aprimoramento de estratégias da ciberguerra.

Convém ressaltar que, para realizar um ciberataque, um Estado precisa ser minimamente desenvolvido em termos de tecnologia, o que implica em uma dependência tecnológica, visto que a utilização do ciberespaço acaba se tornando uma porta aberta, ou seja, a infraestrutura da nação atacante também se torna vulnerável a ataques virtuais (Cavelty, 2010). Desse modo, o desenvolvimento de capacidades é bastante custoso para o país (Cavelty, 2010), assertiva que fortalece o interesse do trabalho no modo como a AFA capacita os cadetes no tema em questão.

Ainda no contexto da ciberguerra, com o decorrer dos anos, o avanço da tecnologia digital transformou o ciberespaço em uma zona de combate estratégica. A crescente dependência da internet para operações governamentais e militares e as ameaças cibernéticas evoluíram de forma significativa, tornando-se preocupações globais. Métodos de ciberataque têm sido amplamente

utilizados para roubar informações sensíveis ou prejudicar as infraestruturas críticas do país.

Segundo o Ministério da Defesa (Brasil, 2023), o ciberataque é definido como uma ação dirigida a equipamentos, redes de computadores e sistemas de comunicação do adversário, com o objetivo de prejudicar ou destruir as infraestruturas que favorecem sua operação. Isso inclui: "degradar a capacidade de operação do oponente, reduzindo a eficácia de funcionamento dos seus sistemas"; "destruir ou degradar equipamentos e sistemas [...]"; e "negar o acesso do oponente a sistemas de interesse do TO/A Op" (Brasil, 2023, p. 24). "O ataque cibernético constitui um elemento da operação militar, pois consiste em impactar os sistemas de rede e tecnológicos do oponente, afetando, consequentemente, sua eficiência de operar. Ademais, o ciberataque deve ser coordenado e sincronizado com os ataques físicos" (Brasil, 2023, p. 24).

Já Schmitt (2017) define um ciberataque como uma operação que, sendo ofensiva ou defensiva, espera afetar as pessoas e causar dano ou destruição a infraestruturas. Nesse sentido, a próxima seção aborda sobre as ameaças na contemporaneidade.

1.4 AMEAÇAS CIBERNÉTICAS ATUAIS

A pandemia do novo coronavírus marcou o aumento e a sofisticação de ataques cibernéticos (Lodh e Dalave, 2022). Nesse sentido, a empresa CrowdStrike (2025), perita em segurança cibernética e da informação, elaborou um relatório sobre o cenário das ameaças cibernéticas na América Latina, em 2025, sendo que o autor do presente artigo extraiu apenas as informações referentes ao Brasil.

Nesse contexto, o Brasil foi o país com o maior número de credenciais vazadas (CrowdStrike, 2025). Destacando que, dessas credenciais, quase 300 milhões são provenientes do governo brasileiro (CrowdStrike, 2025). Cabe frisar a constatação pela empresa *CrowdStrike* dos grupos de crime cibernético (e-crime) que estão atualizando os *malwares* para obterem mais eficiência nos ataques, o que corrobora com a necessidade do constante aprendizado e capacitação de profissionais nessa área (CrowdStrike, 2025). Além disso, essa empresa identificou seis grupos de e-crime, dentre os quais o *Odyssey Spider*, o *Plump Spider* e o *Samba Spider* atuam diretamente no Brasil (CrowdStrike, 2025). Somado a isso, foram identificados grupos de *hackers* com atuação também na América Latina ligados a países como a Rússia, China e Coreia do Norte (CrowdStrike, 2025). A *CrowdStrike* (2025) também identificou o crescente surgimento de movimentos *hacktivistas*, atividades as quais são utilizados ciberataques com o

foco em ações políticas, seja para confrontar governos ou para instaurar a desordem social. Para tal, é importante que se tenha um conhecimento geopolítico geral sobre os interesses das nações, sendo capaz de conhecer os motivos históricos, culturais e os métodos de ataque do inimigo (CrowdStrike, 2025).

Dessa forma, as medidas de prevenção e proteção da tecnologia e dos usuários precisam avançar na mesma velocidade dos ciberataques. Para elucidar a temática, este artigo listou, de maneira não exaustiva, ameaças cibernéticas na contemporaneidade, de acordo com Lodh e Dalave (2022) e Ahmed e Tushar (2020):

a) *Phishing*: é um crime que consiste no roubo de informações pessoais. O agente age por meio de mensagens ou *e-mails* convincentes, os quais contém *links* maliciosos que permitem que ele acesse o seu sistema (Lodh e Dalave, 2022). Outro método é a criação de páginas na *internet* similares a de companhias reais, enganando o indivíduo a inserir seus dados pessoais, como dados bancários. Esse tipo de ataque é muito utilizado no Brasil para roubar informações de conta bancária e para levar a vítima a baixar ferramentas de controle remoto (CrowdStrike, 2025). Como forma de prevenção, faz-se necessário instalar um *firewall* – barreira virtual (Lodh e Dalave, 2022). Além disso, uma boa educação sobre cibernética, incluindo os tipos de crimes virtuais, é uma boa prática de se evitar esses golpes, ensinando sobre o Sistema de Nomes de Domínio (DNS) – sistema que transforma nomes de domínio para enderenço IP numérico –, pois ao identificar a veracidade do DNS, pode-se inferir se a página na *internet* é falsa ou oficial (Chen e Guo, 2006).
b) *Ransomware*: é um tipo de malware que infecta o computador e rapidamente se espalha pelo sistema, bloqueando os arquivos ou a própria máquina (Tailor e Patel, 2017). Essa infecção ataca os arquivos e dados essenciais no sistema do computador do usuário e os criptografa (Ahmed e Tushar, 2020). O Brasil foi o país da América Latina mais afetado em 2024 de acordo com o relatório de inteligência da *CrowdStrike*. De modo a prevenir esse tipo de ataque, recomenda-se manter o *firewall* ativo e o *software* do seu sistema atualizado, utilizar anti-virus e, como boa prática, fazer *back up* dos documentos (Lodh e Dalave, 2022). Além disso, é importante entender as técnicas, táticas e procedimentos de um *broker* de acesso, pois é essa entidade maliciosa que vai identificar o alvo mais vulnerável e facilitar a entrada do *ransomware* no sistema (CrowdStrike, 2025).
c) *Malware*: utilizado por agentes maliciosos, permite o livre acesso aos arquivos do sistema

infectado, sendo muito usado para roubar senhas e credenciais dos usuários (Lodh e Dalave, 2022). *Malware* é constituído por códigos de programação e por um *software* capaz, também, de destruir sistemas operacionais e programas computacionais (Faruk *et al.*, 2021). Um ataque frequente ao Brasil é por meio de um *trojan – malware* que se disfarça por um *software* legítimo – com o objetivo de capturar dados específicos (CrowdStrike, 2025). Um método eficaz de prevenção é a criptografia dos arquivos e a utilização de anti-virus e *firewall* (Lodh e Dalave, 2022).

d) *Spoofing*: esse método de ciberataque é utilizado para falsificar o sinal recebido pelo *Global Positioning System (GPS)*, alterando a posição, a velocidade e o tempo desse sistema (Van Der Merwe *et al.*, 2018). O atacante envia sinais falsos para o receptor do *GPS*, manipulando a navegação legítima do sistema, além disso, esse método se enquadra em um ataque de guerra eletrônica e guerra de informação, visto que há a invasão do *hardware* do receptor de sinal (Van Der Merwe *et al.*, 2018). Como forma de prevenção sugere-se a implementação da criptografia do sinal de *GPS* como forma de autenticação para se evitar sinais ilícitos e falsos, sendo esse método considerado o mais eficaz pelos autores Van Der Merwe *et al*. (2018).

1.5 EDUCAÇÃO NA CIBERNÉTICA

Mountrouidou *et al.* (2019) realizaram um estudo demonstrando o custo, em bilhões, associado aos efeitos dos ciberataques, em 2019, nos Estados Unidos. Nesse estudo, eles apontaram a urgente necessidade de profissionais qualificados em segurança cibernética e o que a falta desses profissionais acarreta para o país. Outrossim, os autores defendem a participação de núcleos de estudos sobre cibersegurança, dando foco ao incentivo nas escolas e universidades.

Já Pencheva *et al.* (2020) realizaram um estudo pela Universidade de Bristol, Reino Unido, sobre a inserção da segurança cibernética no ensino. Nesse estudo, os pesquisadores indicaram a relevância do currículo interdisciplinar, abrangendo, junto à cibernética, matérias como a língua inglesa, a computação e a ciência, além de seguir, também, as diretrizes oficiais do governo (Pencheva *et al.*, 2020). Além disso, os pesquisadores ressaltam a importância de inserir os alunos em métodos ativos como atividades práticas, simulações e estudos de casos (Pencheva *et al.*, 2020).

Dessa forma, sua pesquisa demonstra a seriedade do tema e a importância de investir nele no âmbito da educação, visto que, para os pesquisadores, a segurança cibernética é definida como

uma ciência que abrange temas dinâmicos, dada a evolução global das ameaças e dos ataques de Estado-nação, além de crimes organizados. Em acordo com esses pensamentos, o Ministério da Defesa brasileiro confeccionou um relatório, referente ao Grupo de Trabalho (GT), de alinhamento do ensino de defesa cibernética nas Forças Armadas (Brasil, 2021b).

1.6 FORMAÇÃO DO OFICIAL DA AERONÁUTICA

As FA são instituições nacionais e permanentes essenciais para a soberania do Brasil. Compostas de Exército, Marinha e Aeronáutica, são empregadas na defesa da pátria e asseguram os poderes constitucionais, a lei e a ordem. Além disso, as FA atuam em missões humanitárias, de paz e segurança de infraestruturas críticas.

> [A] Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) define infraestrutura crítica como: "instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade" (Brasil, 2018)

A FAB, sob a missão de "manter a soberania do espaço aéreo e integrar o território nacional, com vistas à defesa da pátria", atua para impedir o uso do espaço aéreo brasileiro e do espaço exterior para prática de atos hostis ou contrários aos interesses nacionais (Ministério da Defesa, 2018, p. 20). E tem como principal instituição de ensino e formação militar de seus oficiais de carreira, a Academia da Força Aérea (AFA).

Diante disso, a AFA tem como missão formar oficiais de carreira da Aeronáutica dos Quadros de Oficiais Aviadores, Intendentes e de Infantaria. Para atingir esse objetivo, a parte acadêmica dessa instituição é norteada pela Instrução do Comando da Aeronáutica (ICA), que contempla o Projeto Pedagógico para o Curso de Oficiais Aviadores, de Oficiais Intendentes e de Oficiais de Infantaria. Neste artigo, foi analisado o documento e *ICA 37-901/2024*, voltado para a formação dos cadetes de Infantaria. Cabe frisar que a grade curricular da AFA, que aborda sobre a área de cibernética, foi elaborada pelo Ministério da Defesa, por meio de um Grupo de Trabalho (GT) (Brasil, 2021b).

O documento *ICA 37-901*, Projeto Pedagógico de Curso – PPC para o Curso de Formação de Oficiais de Infantaria – CFOInf (Ministério da Defesa, 2024a), é uma instrução normativa que define como será a formação dos futuros Oficiais de Infantaria da Aeronáutica. Ele serve como guia

para planejamento, organização e execução do curso, conforme as diretrizes do Comando da Aeronáutica. Esse documento é fundamentado pelo modelo de Gestão por Competências incorporado pelo Comando da Aeronáutica (COMAER) com a finalidade de "identificar e gerir perfis profissionais que proporcionem um maior retorno institucional, identificando os pontos de excelência do Profissional Militar e as oportunidades de melhoria, suprindo lacunas e agregando conhecimento" (Ministério da Defesa, 2024b, p. 16).

Ainda no escopo da Força Aérea Brasileira (FAB), o PCA 11-405 define competência como "a capacidade de desempenhar as atividades dentro de uma função ou área ocupacional, com os níveis de desempenho esperados" (Ministério da Defesa, 2024b, p. 17). Já Perrenoud (1999), ao defender o ensino por competências, afirma que esse método incorpora técnicas de aprendizagem para que os alunos se desviem da esfera tradicional do estudo, que é a memorização de conteúdos, para a integração do conhecimento, habilidade e prática. Assim, eles serão capazes de atuarem em atividades de suas vidas profissionais e de agirem com autonomia para resolverem problemas reais (Perrenoud, 1999).

Nesse sentido, o curso tem como um dos objetivos gerais proporcionar ao cadete de Infantaria conhecimentos, habilidades e atitudes que permitirão ser proficiente em "[...] identificar os preceitos básicos da doutrina de Guerra Cibernética no COMAER [Comando da Aeronáutica]" (Ministério da Defesa, 2024a, p. 26). No capítulo 3, serão analisadas as matérias e as competências previstas na formação do cadete de Infantaria e que estão relacionadas ao tema da pesquisa.

1.7 FORMAÇÃO DO OFICIAL DA USAF

A *United States Air Force Academy* - instituição militar de ensino norte-americano - tem como missão forjar líderes de caráter, motivados a servir à nação e desenvolver a liderança necessária para conduzir a Força Aérea e a Força Espacial para a vitória (USAFA, 2025a). Além disso, essa academia é fundamentada em valores morais que são disseminados por toda a *United States Air Force*, são eles: *Integrity First, Service Before Self* e *Excellence In All We Do* (USAFA, 2025b).

Cabe frisar que a USAFA é uma universidade pública que se preocupa com o desenvolvimento e com a inovação nos campos aéreo, espacial e no ciberespaço (USAFA, 2025a). Nesse sentido, dentre os diversos cursos oferecidos por essa academia, esta pesquisa analisou o departamento de *Cyber Science*, da Divisão de Engenharia.

Convém ressaltar também que o ensino acadêmico norte-americano é norteado pelo *Course of Instruction Handbook*, semelhante à ICA. Esse documento contempla os cursos, programas e especializações ofertados pela academia. Neste artigo, foram analisados o *Course of Instruction Book* 2023-2024 e 2024-2025, com o foco nos programas *Cyber Science e Cyber.*

2 METODOLOGIA

Para alcançar os objetivos geral e específico desta pesquisa, foi utilizado o método qualitativo, pois o autor elaborou uma escala (não abrange ou abrange parcialmente/totalmente) para verificar se as competências contidas na grade curricular do cadete de Infantaria da Aeronáutica abrangem as capacidades necessárias para enfrentar as atuais ameaças cibernéticas. Entende-se por "não abrange", caso seja constatado que o currículo dos cadetes de Infantaria da Aeronáutica não aborde nenhuma ameaça ou método de prevenção que foram listados. E, entende-se como "abrange parcialmente/totalmente", caso seja constatado que essa grade curricular englobe algumas das ameaças ou todas elas. A abordagem qualitativa de cunho descritivo se justifica, também, por se tratar de um estudo interpretativo, utilizando técnicas como observação e análise de conteúdo para absorver dados e informações (Severino, 2013).

Segundo Minayo (2001), a pesquisa qualitativa é apropriada e útil para estudar e entender os métodos de ensino utilizados pelas instituições acadêmicas. Neste caso, estuda-se a Academia da Força Aérea (AFA), o ensino por competências empregado por essa instituição e a *United States Air Force Academy* (USAFA). Já o caráter descritivo justifica-se pela análise comparativa e pela interpretação das grades curriculares da AFA e da USAFA, visto que o tema é de uma crescente relevância mundial – no caso deste trabalho, a inserção da cibernética na formação acadêmica (Rodrigues *et al*., 2007). Cabe frisar que a escolha da *United States Air Force Academy*, como objeto de comparação, justifica-se pela classificação em 6° lugar entre as universidades *STEAM* que a academia norte-americana obteve, segundo a *Forbes* – mencionada na introdução deste artigo –, pela 3° colocação entre as escolas públicas dos EUA e, também, pelo 1° lugar entre as *Funded Undergraduated Research University* – instituições que oferecem oportunidades de pesquisa para os seus alunos (USAFA, 2025a). Cabe ressaltar que foi realizada uma comparação com as atuais ameaças cibernéticas e seus métodos de prevenção com as unidades didáticas e as competências das matérias ministradas pela AFA na área de cibernética (*Cibernética*, *Doutrina Militar de Defesa Cibernética* e *Introdução à Computação*).

Para o levantamento documental e para a revisão bibliográfica, foram analisados documentos oficiais como o *Livro Branco de Defesa Nacional* (Brasil, 2020), a *Estratégia Nacional de Defesa* (Brasil, 2016), o *Livro Verde de Segurança Cibernética no Brasil* (Brasil, 2010), a *ICA 37-901/2024* e as diretrizes do Ministério da Defesa relacionadas à formação militar e à capacitação em segurança cibernética, sendo fundamentais para o escopo da pesquisa. Segundo Lakatos e Marconi (2017), essa metodologia é utilizada para que os materiais escolhidos recebam um tratamento analítico apropriado, permitindo ao pesquisador obter informações originais. Além disso, foram utilizados artigos científicos e publicações institucionais disponíveis em *sites* oficiais, como o da FAB, o do Ministério da Defesa e o da USAFA, que abordam o tema em questão.

Cabe destacar ainda a análise do livro *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, de Schmitt (2017), o qual foi elaborado por um grupo internacional de especialistas jurídicos que analisa como o direito internacional se aplica a operações no ciberespaço.

Portanto, a metodologia utilizada permite oferecer ao leitor uma consciência sobre o panorama da capacitação e do preparo dos cadetes de Infantaria da AFA, no tocante às atuais ameaças cibernéticas.

3 RESULTADOS E DISCUSSÕES

A pesquisa teve como objetivo analisar o preparo acadêmico dos cadetes de Infantaria da AFA em relação às atuais ameaças cibernéticas. Para isso, foi feita uma análise comparativa com a *United States Air Force Academy* (USAFA) e com as ameaças cibernéticas atuais.

3.1 PREPARO DOS CADETES DA USAFA

Como mencionado na seção 1.7, o *Course of Instruction Book*, da USAFA, é um manual norte-americano que contém informações gerais relativas aos cursos oferecidos pela instituição. A área de cibernética tem uma carga horária de 145 horas (incluindo as disciplinas interdisciplinares) é tratada da seguinte maneira:

a) *Cyber*: esse curso acadêmico engloba a matéria *Basic Cyber Operations* (*Cyber 256*), no qual os cadetes têm a oportunidade de participar de um programa de sete dias sobre operações cibernéticas, motivando-os a seguir a carreira na *United States Air Force Academy*

(USAFA, 2024). Os cadetes também exploram a área de missões cibernéticas conjuntas durante o curso, com ênfase nos fundamentos de ataque, defesa e operações em computadores e redes (USAFA, 2024). Ademais, é oferecido o curso *Senior Cyber Instructor Training*, que prepara os cadetes para se tornarem instrutores do *Cyber 256*. Esse curso explora o planejamento de missões e seus desafios éticos, legais e operacionais por meio do ciberespaço (USAFA, 2024). Assim, os cadetes aprendem técnicas de instrução e habilidades para operar de maneira segura no ciberespaço (USAFA, 2024).

b) *Cyber Science*: esse curso acadêmico prepara os cadetes para estabelecer, operar, manter e defender os sistemas computacionais e os de comunicação, capacitando-os para contribuir em uma variedade de missões cibernéticas (USAFA, 2024). Também é oferecida a matéria de *Cyber Warfare* sobre segurança cibernética, que estuda os fundamentos de vulnerabilidade cibernética de maneira teórica e prática (USAFA, 2024). A matéria contempla os fundamentos de defesa de rede, incluindo análises de vulnerabilidade e mecanismos de defesa (USAFA, 2024). Além disso, a academia americana ministra a matéria de *Cyber Operations*, que permite aos cadetes planejarem e executarem missões realísticas (USAFA, 2024). Ela engloba planejamento de missão, métodos de ciberataque, avaliação de risco e as preocupações legais, éticas e estratégicas relevantes (USAFA, 2024). A matéria aplica conceitos e técnicas para análise, concessão, implementação e manutenção de ciberciência de grande escala (USAFA, 2024).

Outrossim, a disciplina *Data Science Major*, é um curso interdisciplinar com o curso *Cyber Science*, ou seja, ela integra os conhecimentos da área do saber que, neste caso, são: *Computer, Management, Cyber Science e Mathematical Science* (USAFA, 2024). Assim, paralelamente ao estudo realizado na Universidade de Bristol, Reino Unido, a área de cibernética é abrangida pela USAFA junto a outras disciplinas, potencializando o aprendizado, as técnicas, as táticas e o nível operacional no qual os cadetes poderão atuar.

Nesse sentido, essas matérias ministradas proporcionam ao cadete um pensamento analítico e habilidades de programação, sendo assim, um recurso poderoso para o futuro oficial utilizar em missões de gestão de recursos e em operações logísticas, visto que a matéria de gestão (*Management*) é interdisciplinar com a cibernética.

O militar torna-se, também, capaz de desenvolver tecnologias para suprir alguma carência da Força e de atuar em prol dos objetivos e interesses nacionais. Por exemplo, tal capacidade é ilustrada pelo ataque cibernético do exército de "*hackers*" norte-coreano, contido no relatório da

Organização das Nações Unidas (ONU), cujo objetivo foi o roubo de criptomoedas para financiar a compra de armas nucleares (Roth e Berlinger, 2021).

Além disso, em consonância com Mountrouidou *et al.* (2019), a *United States Air Force Academy* investiu na educação cibernética inaugurando o *The Madera Cyber Innovation Center*, que pertence ao departamento de *Cyber Science* e contém 14 laboratórios e salas de aula (USAFA, 2025c). Dessa forma, esse centro potencializa o aprendizado de técnicas e de habilidades voltadas para a segurança cibernética, promovendo, também, a imersão dos militares em treinamentos realísticos, colaborando com as metodologias ativas, as simulações e os estudos de caso que a pesquisa de Pencheva *et al.* (2020) prevê.

Portanto, dada a complexidade das ações de uma operação cibernética, nota-se que a USAFA investe na educação e prepara seus cadetes para identificar as vulnerabilidades dos sistemas militares, incentivando-os durante missões cibernéticas realísticas nas quais eles podem identificar os tipos de ciberataques e aplicar os fundamentos de segurança cibernética, a fim de mitigar ciberataques como o da Coreia do Norte.

3.2 PREPARO DOS CADETES DE INFANTARIA DA AFA

Como citado anteriormente, o Ministério da Defesa (MD) elaborou a grade curricular das academias de formação militar, por meio de um Grupo de Trabalho, e o Comando de Defesa Cibernética fomenta a pesquisa e o desenvolvimento de capacidades na área de cibernética. Nesse contexto, a Academia da Força Aérea está se preparando para que os cadetes também possuam um conhecimento nessa área. Sendo assim, a *ICA 37-901/2024*, que teve como base o relatório do MD sobre a educação de defesa cibernética nas escolas militares, prevê que as disciplinas “Cibernética” e “Doutrina Militar de Defesa Cibernética” serão cursadas pelos cadetes de Infantaria para a integralização curricular do CFOInf para as turmas matriculadas a partir de 2024 (Ministério da Defesa, 2024a).

A *Cibernética* é uma disciplina que pertence ao Campo de Formação Geral. Com carga horária de 36 horas, é ministrada no 3º ano da formação. A partir dela, o cadete será capaz de:

> “[...] identificar os preceitos de segurança e defesa cibernética; aplicar as principais tecnologias e ferramentas para garantir a segurança da informação; identificar as vulnerabilidades dos sistemas informatizados; identificar como as vulnerabilidades dos sistemas informatizados da Organização podem expor os dados e afetar a

> segurança da informação; e identificar as normas de segurança da informação do COMAER" (Ministério da Defesa, 2024a, p. 25-26).

Nesse sentido, o futuro oficial de Infantaria é capacitado a prevenir e a proteger os sistemas de rede de sua Organização Militar (OM), visto que a segurança cibernética é a área cujo objetivo é garantir a segura utilização da internet e, no caso de um ciberataque, seja é capaz de restaurar os dados do sistema. Desse modo, o militar, com a formação na disciplina de *Cibernética*, mitiga a possibilidade de as informações da OM serem violadas.

Assim, essa matéria visa preparar o cadete para compreender e atuar em um ambiente operacional marcado pela tecnologia e pelo domínio digital.

> "Campo de Formação Geral: é composto pelo campo de formação básica, que é comum ao bacharelado de Ciências Militares e de Administração. É relacionado com o embasamento teórico no campo jurídico, filosófico, psicológico, geopolítico, econômico, administrativo e outros que se mostram pertinentes na formação do oficial" (Ministério da Defesa, 2024a, p. 29).

Já a disciplina *Doutrina Militar de Defesa Cibernética*, pertencente ao Campo de Formação Militar, relacionado à singularidade da profissão, tem carga horária de 24 horas e é ministrada no 4º ano da formação. A partir dela, o cadete de Infantaria será capaz de "[...] descrever os fundamentos de Defesa e Guerra Cibernética; compreender atividades de Guerra Cibernética; compreender o Sistema Militar de Defesa Cibernética; e analisar a Guerra Cibernética nas Operações Militares" (Ministério da Defesa, 2024a, p. 230).

Nesse contexto, a formação do cadete o capacita a participar de operações que exijam conhecimento técnico na dimensão cibernética, visto que essa disciplina abarca o conceito de ciberguerra conceituado pelo Ministério da Defesa, conforme citado na seção 1.3. Isto é, o militar possui conhecimento para usar, de forma ofensiva ou defensiva, dados e informações para atingir o Comando e Controle do oponente, visto que é ministrada ao cadete a unidade didática de "Defesa e Guerra Cibernética nas Operações Militares".

Ademais, a disciplina de *Cibernética* tem como pré-requisito a disciplina de *Introdução à computação* (Ministério da Defesa, 2024a). Nessa última, o cadete será capaz de: "aplicar os preceitos básicos de Inteligência e Contrainteligência [...]"; "aplicar medidas de segurança [...], da Tecnologia da Informação [...]"; e "identificar os preceitos básicos da doutrina de Guerra Cibernética no COMAER" (competências gerais) (Ministério da Defesa, 2024a, p. 148). Dessa forma, a AFA, de

maneira mais simples, apresenta um currículo interdisciplinar, integrando as áreas de conhecimento de cibernética e de computação, como prevê o estudo de Pencheva *et al.* (2020).

Logo, ao abordar os fundamentos de guerra cibernética no âmbito da FAB, o cadete torna-se capacitado para reconhecer os riscos e as vulnerabilidades dos sistemas computadorizados e dos sistemas de rede, bem como para conhecer os princípios da segurança cibernética para a proteção de dados no ambiente cibernético.

3.3 ANÁLISE COMPARATIVA ENTRE AS GRADES CURRICULARES

A partir dos dados apresentados acima, o Quadro 1 sintetiza a análise comparativa quanto à formação sobre cibernética oferecida na AFA e na USAFA:

Quadro 1 Comparativo entre a formação cibernética na USAFA e na AFA

Aspecto	United States Air Force Academy (USAFA)	Academia da Força Aérea (AFA)
Disciplinas principais	*Cyber Operations* *Cyber Science* *Cyber Warfare*	*Cibernética* *Doutrina Militar de Defesa Cibernética*
Ênfase	Defesa e ataque cibernético; missões simuladas; análise forense digital	Conceitos básicos de segurança e guerra cibernética
Carga horária	145h (*Cyber* + *Cyber Science* + matérias interdisciplinares)	36h (*Cibernética*) + 24h (*Doutrina Militar de Defesa Cibernética*) + 25h (Introdução à Computação)
Treinamento prático	Simulações realísticas de missões cibernéticas (*The Madera Cyber Innovation Center*)	Conteúdo teórico e aplicação básica de ferramentas
Integração interdisciplinar	Alta (ética, direito, tecnologia, operações – *Computer, Cyber Science, Management* e *Mathematical Sciences*)	Moderada (fundamentos técnicos e doutrinários – Cibernética e Introdução a Computação)
Objetivo	Formação de especialistas em operações cibernéticas	Formação básica para identificação de ameaças e defesa da informação

Fonte: elaboração própria.

Com o objetivo de analisar como a AFA capacita seus cadetes de Infantaria no campo da cibernética, considerando o crescente impacto do ciberespaço como novo domínio operacional, este trabalho demonstrou que a referida academia reconhece a importância da formação cibernética ao incluir disciplinas específicas como *Cibernética* e *Doutrina Militar de Defesa Cibernética* no

currículo dos cadetes, ao seguir as diretrizes propostas pelo MD, consolidando a preparação básica para os desafios contemporâneos de defesa.

A análise comparativa entre a AFA e a USAFA evidenciou que, enquanto a formação brasileira incorpora conceitos fundamentais de segurança cibernética e guerra cibernética, o currículo norte-americano é mais abrangente, incluindo treinamento prático em missões realísticas de ciberoperação, análise forense e estratégias ofensivas e defensivas. Essa comparação revela uma oportunidade para o aprimoramento contínuo do currículo nacional, especialmente no tocante à prática operacional e à integração de cenários simulados. Além disso, a disciplina *Doutrina Militar de Defesa Cibernética* provê o arcabouço necessário à inserção do militar nas operações no contexto da guerra cibernética.

Vale ressaltar que, considerando a crescente ameaça cibernética e a dependência tecnológica das operações militares, a capacitação contínua e aprofundada em cibernética mostra-se essencial para a garantia da soberania e da segurança nacional.

3.4 ANÁLISE COMPARATIVA ENTRE A GRADE CURRICULAR DA AFA E AS ATUAIS AMEAÇAS CIBERNÉTICAS

A partir dos dados apresentados nos tópicos 1.4 e 3.2, o Quadro 2 sintetiza o preparo dos cadetes em relação às atuais ameaças:

Quadro 2 Relação entre os tipos de ciberataque e a educação cibernética na AFA

Ameaças	Unidades Didáticas	Competências
Phishing	**Cibernética**: Segurança na *internet*; Fundamentos de Segurança Cibernética; Tipos de ataques; Ameaças cibernéticas; Atuação de *Hackers* (Ataques Cibernéticos). **Introdução à Computação**: Fundamentos de redes (endereçamento).	Aplicar as principais tecnologias e ferramentas para garantir a segurança da informação; Identificar as vulnerabilidades dos sistemas informatizados. Identificar as funcionalidades da Internet e da Web
Ransomware	**Cibernética**: Fundamentos de Segurança da Informação; Segurança na *internet*; Fundamentos de Segurança Cibernética; Tipos de ataques; Ameaças cibernéticas; Criptografia aplicada. **Introdução à Computação**: Fundamentos de *Hardware* (barramento); Fundamentos de *Software.*	Aplicar as principais tecnologias e ferramentas para garantir a segurança da informação. Identificar as vulnerabilidades dos sistemas informatizados.

Malware	**Cibernética**: Segurança na *internet*; Códigos maliciosos (*malware*); Criptografia aplicada; Tipos de ataques; Ameaças cibernéticas.	Aplicar as principais tecnologias e ferramentas para garantir a segurança da informação. Identificar as vulnerabilidades dos sistemas informatizados
Spoofing	**Cibernética:** Atuação de *Hackers* (Ataques cibernéticos); Tipos de ataques; Criptografia aplicada; Ameaças cibernéticas. **Introdução à Computação**: Fundamentos de *Hardware*: barramentos.	Aplicar as principais tecnologias e ferramentas para garantir a segurança da informação.

Fonte: elaboração própria.

Com o objetivo de analisar a capacitação dos militares em relação às ameaças cibernéticas, o Quadro 2 apresenta as Unidades Didáticas das disciplinas que abordam sobre os tipos de ataques e os métodos de prevenção a eles. Além disso, como explicado na seção 1.6, o ensino por competências tem por finalidade capacitar o profissional a aplicar os conhecimentos e as habilidades adquiridas em situações reais. Sendo assim, no primeiro momento, o militar alcançará os níveis de competência apresentados pelo Quadro 2 que são necessários para mitigar as ameaças cibernéticas, de acordo com o preconizado na seção 1.4 pelos autores Lodh e Dalave (2022), Van Der Merwe *et al.* (2018) e Ahmed e Tushar (2020).

Cabe frisar que, conforme o relatório da CrowdStrike, há três grupos de e-crime instalados na América Latina com atuação direta no Brasil e grupos com atuação em toda a América Latina conectados a interesses políticos de países como a Rússia, China e Coreia do Norte. Destacando que há um aumento do número de *hacktivismo* influenciado pelo contexto histórico, cultural e político das nações. No entanto, na análise da *ICA37-901/2024*, que trata sobre a grade curricular dos futuros oficiais de Infantaria da Aeronáutica, foi constatada uma lacuna nesse âmbito, ou seja, as matérias da área de cibernética não são administradas interdisciplinarmente com alguma matéria que aborde a geopolítica internacional. Dessa forma, o militar, não possuindo um conhecimento sobre a motivação e os interesses da nação inimiga, não será capaz de realizar um estudo prévio sobre os métodos de ciberataque do inimigo, sendo a diferença entre a contenção e a catástrofe daquele ataque.

Portanto, a síntese comparativa demonstra que as unidades didáticas e as competências das disciplinas *Cibernética*, *Doutrina Militar de Defesa Cibernética* e *Introdução à Computação* abrangem parcialmente as capacidades necessárias para o futuro oficial de Infantaria da Aeronáutica enfrentar as atuais ameaças cibernéticas, tendo em vista os tipos de ataques listados na seção 1.4, suas respectivas medidas de prevenção, e o contexto e os interesses dos grupos de crime cibernéticos.

Respondendo, assim, a problematização: “em que medida as competências previstas na grade curricular dos cadetes de Infantaria da Aeronáutica abrangem as atuais ameaças cibernéticas?”.

4 CONCLUSÃO

O avanço tecnológico inovou a área de atuação das Forças Armadas, consolidando o ciberespaço como novo domínio operacional, onde há a atuação tanto de governos, quanto de entidades não-estatais, impondo, assim, a necessidade da formação de militares especializados para atuar nesse ambiente. Este trabalho teve como objetivo geral analisar a grade curricular do Curso de Formação de Oficiais de Infantaria da Aeronáutica, com o foco na área de cibernética, a fim de responder a seguinte problematização: “em que medida as competências previstas na grade curricular dos cadetes de Infantaria da Aeronáutica abrangem as atuais ameaças cibernéticas?”. Para que tal objetivo fosse atingido, fez-se necessária a divisão em três objetivos específicos, a fim de delimitar o tema e organizar as fases de execução da pesquisa. Esse detalhamento resultou em: explicar o domínio do ciberespaço junto aos conceitos de segurança cibernética, ciberguerra e ciberataque; identificar as ameaças cibernéticas mais relevantes na contemporaneidade; e comparar a grade curricular na área de cibernética dos cadetes de Infantaria da AFA com a dos cadetes da USAFA e com as atuais ameaças cibernéticas.

A pesquisa, de natureza qualitativa de cunho descritivo, baseou-se em análise documental e levantamento bibliográfico para atingir o primeiro objetivo específico. Já para atingir os demais objetivos, foi realizada uma análise comparativa do currículo na área de cibernética do Curso de Formação de Oficiais de Infantaria com a grade curricular dos cadetes da USAFA e com as atuais ameaças cibernéticas.

A investigação evidenciou que a AFA incorporou disciplinas voltadas para a segurança e a guerra cibernética, como *Cibernética* e *Doutrina Militar de Defesa Cibernética*, embora com carga horária reduzida e com escopo mais restrito que a formação norte-americana, além de ser uma matéria interdisciplinar apenas com *Introdução à Computação*. A USAFA, por sua vez, ministra a temática de maneira interdisciplinar mais abrangente – *Computer, Management* e *Mathematical Science* – e promove intensa formação prática, com missões simuladas, análise forense digital, treinamento ofensivo e defensivo no ciberespaço.

Já no tocante às atuais ameaças cibernéticas, a dificuldade em acompanhar a rápida evolução dos ciberataques é uma questão presente no mundo todo. Em resposta, o Ministério da Defesa, como

foi citado ao longo do artigo, elaborou um currículo único de ensino de cibernética para as escolas militares vinculadas às Forças Armadas. Sendo assim, o currículo analisado, em específico o da Infantaria da Aeronáutica, mostrou-se eficaz na prevenção aos ataques do tipo: *phishing*, *ransomware*, *malware* e *spoofing*. Porém, não aborda sobre as questões geopolíticas internacionais ligadas a grupos de e-crime ou a nações inimigas.

Portanto, a formação dos cadetes de Infantaria da Aeronáutica pode ser aprimorada, com o aumento da carga horária prática e com a inserção de simulações operacionais em segurança cibernética e de matérias que potencializam o aprendizado na área de cibernética. As conclusões apontam que os ensino por competências na AFA abrange parcialmente o escopo das ameaças cibernéticas contemporâneas listadas no corpo da pesquisa. Assim, o trabalho reforça a importância estratégica de fortalecimento da formação cibernética no contexto da defesa nacional, visando a proteção de infraestruturas críticas e a manutenção da soberania frente às novas ameaças.

Para estudos futuros, recomenda-se investigar, através de entrevistas e questionários, a efetividade da formação cibernética ministrada na AFA e propor estratégias para o fortalecimento das competências operacionais dos futuros oficiais, como a implementação de uma disciplina que aborde sobre a geopolítica internacional ligada aos atuais ciberataques.

REFERÊNCIAS

AHMED, Jabber; TUSHAR, Quddus. COVID-19 pandemic: A new era of cyber security threat and holistic approach to overcome. **2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)**. 2020.

BOAS, Taylor. **Weaving the Authoritarian Web:** The Control of Internet Use in Nondemocratic Regimes. Berkeley: University of California, 2006.

BRASIL. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações **Livro Verde: segurança cibernética no Brasil**. Brasília, 2010.

BRASIL. Lei nº 12.464, de 4 de agosto de 2011. Dispõe sobre o ensino na Aeronáutica; e revoga o Decreto-Lei nº 8.437, de 24 de dezembro de 1945, e as Leis nºs 1.601, de 12 de maio de 1952, e 7.549, de 11 de dezembro de 1986. **Diário Oficial da União**, Brasília, 2011.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Doutrina Militar de Defesa Cibernética**. Brasília, 2014.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**, 2016.

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Dispõe sobre a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional. **Diário Oficial da União**: seção 1, Brasília, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9573.htm. Acesso em: 5 maio 2025.

BRASIL. Ministério da Defesa. Congresso Nacional. **Livro Branco de Defesa Nacional**. Brasília, 2020.

BRASIL. Ministério da Defesa. Defesa incentiva formação de militares em cibernética. **Ministério da Defesa**, 21 maio 2021a. Disponível em: https://www.gov.br/defesa/pt-br/centrais-de-conteudo/noticias/defesa-incentiva-formacao-de-militares-em-cibernetica?utm_source=chatgpt.com. Acesso em: 30 abr. 2025.

BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Defesa Cibernética. Escola Nacional de Defesa Cibernética. **Relatório GT-ENaDCiber**. Brasília, 2021b.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Doutrina Militar de Defesa Cibernética**. 2. ed. Brasília. p. 17-24, 2023.

CAVELTY, Myriam. Cyberwar: concept, status quo, and limitations. **CSS**, v. 71, p. 1-3, 2010. Disponível em: https://www.files.ethz.ch/isn/114442/CSS_Analysis_71.pdf. Acesso em: 30 abr. 2025.

CHEN, Juan; GUO, Chuanxiong. Online detection and prevention of phishing attacks. **First International Conference on Communications and Networking in China**. 2006.

CLARKE, Richard; KNAKE, Robert. **Guerra Cibernética**: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2010.

CONNELL, Michael; VOGLER, Sarah. Russia's Approach to Cyber Warfare. **CNA**, 2017. Disponível em: https://www.cna.org/reports/2017/russias-approach-to-cyber-warfare#:~:text=Russia%20views%20cyber%20very%20differently%20than. Acesso em: 30 abr. 2025.

CROWDSTRIKE. Relatório sobre o cenário de ameaças na América Latina 2025. **CrowdStrike**, 2025. Disponível em: https://www.crowdstrike.com/pt-br/resources/reports/crowdstrike-2025-latin-america-threat-landscape-report/. Acesso em: 30 jun. 2025.

CYBERSECURITY. **Homeland Security**, 2009. Disponível em: https://www.dhs.gov/topics/cybersecurity#:~:text=The%20Department%20of%20Homeland%20Security%20and. Acesso em: 30 abr. 2025.

EUA grampearam Dilma, ex-ministros e avião presidencial, revela WikiLeaks. **G1**, 4 jul. 2015. Disponível em: https://g1.globo.com/politica/noticia/2015/07/lista-revela-29-integrantes-do-governo-dilma-espionados-pelos-eua.html. Acesso em: 30 abr. 2025.

FARUK, Jobair *et al.* Malware detection and prevention using artificial intelligence techniques. **International Conference on Big Data**. 2021.

FORTINET. BRASIL sofreu mais de 88,5 bilhões de tentativas de ataques cibernéticos em 2021. **Fortinet**, 8 fev. 2022. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021#:~:text=O%20Brasil%20sofreu%20mais%20de,e%20automatizadas%20de%20seguran%C3%A7a%20cibern%C3%A9tica. Acesso em: 30 abr. 2025.

GIBSON, William. **Neuromancer**. Tradução de Fábio Fernandes. São Paulo: Aleph, 2008.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

HAUBEN, Michael. History of ARPANET. **Site de I'Instituto Superior de Engenharia do Porto**, v. 17, p. 1-20, 2007.

JAJOO, Akshay. **A study on the Morris Worm**. Indiana: Purdue University, 2021.

LODH, Anushka; DALAVE, Chetan. A study on types of cyber crimes and cyber attacks today. **International Journal For Research In Applied Science and Engineering Technology**, v. 10, n. 2, p. 220-225, 2022.

LOPES, Gills; OLIVEIRA, Carolina de. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. **Revista Brasileira de Estudos de Defesa**, v. 1, n. 1, p. 55-69, 2014. Disponível em: https://rbed.abedef.org/rbed/article/view/39457. Acesso em: 30 abr. 2025.

MARCONI, Marina; LAKATOS, Eva. **Fundamentos de metodologia científica**. 8. ed. São Paulo: Atlas, 2017.

MINAYO, Maria Cecília de Souza. **O desafio do conhecimento**: pesquisa qualitativa em saúde. 7. ed. São Paulo: Hucitec, 2001.

MINISTÉRIO DA DEFESA. Força Aérea Brasileira. Comando da Aeronáutica. **Concepção Estratégica – Força Aérea 100 (DCA 11-45)**. Brasília, 2018.

MINISTÉRIO DA DEFESA. Força Aérea Brasileira. Comando da Aeronáutica. **Segurança e Defesa no Comando da Aeronáutica (DCA 205-4)**. Brasília, 2020.

MINISTÉRIO DA DEFESA. Força Aérea Brasileira. Comando da Aeronáutica. **Projeto Pedagógico de Curso para o Curso de Formação de Oficiais de Infantaria – 2024 (ICA 37-901)**. Pirassununga. p. 148, 2024a.

MINISTÉRIO DA DEFESA. Força Aérea Brasileira. Comando da Aeronáutica. **Plano de Ensino da Aeronáutica: PCA 11-405**. Brasília, 2024b.

MOUNTROUIDOU, Xenia *et al*. Securing the human: a review of literature on broadening diversity in cybersecurity education. *In*: ITICSE WORKING GROUP REPORTS, 19., 2019, New York. **Anais** [...]. New York: ACM. p. 157-169, 2019

OBIS, Anastasia. Army to Invest Half a Billion Dollars in Critical Infrastructure. **GovCio MEDIA & RESEARCH**, 1º dez. 2023. Disponível em: https://govciomedia.com/army-to-invest-half-a-billion-dollars-in-critical-infrastructure. Acesso em: 30 abr. 2025.

PENCHEVA, Denny *et al*. Bringing cyber to school: Integrating cybersecurity into secundar school education. **IEEE Security E Privacy**, v. 18, n° 2, p. 68-74, 2020.

PERRENOUD, Philippe. L'école saisie par les compétences. **Quel avenir pour les compétences**, p. 21-41, 2000.

POSSIEDE, Bárbara. As guerras de hoje são de quinta geração. O Brasil está preparado? **Central de Notícias Uninter**, 27 jul. 2020. Disponível em: https://www.uninter.com/noticias/as-guerras-de-hoje-sao-de-quinta-geracao-o-brasil-esta-preparado#:~:text=%E2%80%9CAs%20guerras%20hoje%20em%20dia%20s%C3%A3o%20guerras%20de,essenciais%2C%20conceitos%20d. Acesso em: 30 abr. 2025.

RODRIGUES, William Costa. **Metodologia Científica**. Faetec/IST. Paracambi, v. 2, 2007.

ROTH, Richard; BERLINGER, Joshua. ONU: Hackers norte-coreanos roubaram quase R$ 1,7 bi para pagar armas nucleares. **CNN Brasil**, 9 fev. 2021. Disponível em: ONU: Hackers norte-coreanos roubaram quase R$ 1,7 bi para pagar armas nucleares | CNN Brasil. Acesso em: 10 maio 2025.

SCHMITT, Michael (ed.). **Tallinn Manual 2.0 on the International Law Applicable to Cyber**

Operations. Cambridge: Cambridge University Press, 2017.

SEVERINO, Antônio. **Metodologia do trabalho científico**. 1. ed. São Paulo: Cortez, 2013.

SHELDON, John. Deciphering cyberpower strategic purpose in peace and war. **Strategic Studies Quarterly**, p. 95-112, 2011. Disponível em: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf. Acesso em: 30 abr. 2025.

TAILOR, Jinal; PATEL, Ashish. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. **International Journal of Research and Scientific Innovation**, v. 4, n. 15, p. 116-121, 2017.

TEIXEIRA JÚNIOR, Augusto Wagner Menezes; LOPES, Gills Villar; FREITAS, Marco Túlio Delgobbo. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. **Carta Internacional**, Belo Horizonte, v. 12, n. 3, p. 30-53, 2017. Disponível em: https://cartainternacional.abri.org.br/Carta/article/view/620. Acesso em: 30 abr. 2025.

UNITED STATES AIR FORCE ACADEMY – USAFA. **Course of Instruction Handbook**. Colorado: DFVRC, 2024. Disponível em: https://www.usafa.edu/app/uploads/COI.pdf. Acesso em: 30 abr. 2025.

UNITED STATES AIR FORCE ACADEMY – USAFA. Core Curriculum. **United States Air Force Academy**, 2025a. Disponível em: https://www.usafa.edu/academics/core-curriculum/ . Acesso em: 29 maio 2025.

UNITED STATES AIR FORCE ACADEMY – USAFA. Computer and Cyber Science. **United States Air Force Academy**, 2025b. Disponível em: https://www.usafa.edu/department/computer-science/ . Acesso em: 31 maio 2025.

UNITED STATES AIR FORCE ACADEMY – USAFA. Madera Cyber Innovation Center opens with ribbon-cutting ceremony. **United States Air Force Academy**, 25 abr. 2025c. Disponível em: https://www.usafa.edu/madera-cyber-innovation-center-opens-with-ribbon-cutting-ceremony/?fbclid=PAQ0xDSwKUqz9leHRuA2FlbQIxMQABp0THCeESK1WchULi42ePJtfJocZBAyKHKEBnrrEg2I49vRHO7RPqjied3Jpy_aem_SFk9U5lf3fFahbR4gqPa3A. Acesso em: 12 maio 2025.

VAN DER MERWE, Rossouw *et al.* Classification of spoofing attack types. **European Navigation Conference (ENC)**. p. 91-99, 2018.

WANNACRY ransomware used in widespread attacks all over the world. **Kaspersky**, 12 maio 2017. Disponível em: https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/. Acesso em: 30 abr. 2025.