HOPLOS
VOL. 06 Nº 10/2022

Otoniel Fontana Silva

Doutorando e Mestre (2019) em Educação pela Universidade Luterana do Brasil (ULBRA). Militar da Força Aérea Brasileira. Possui graduação em Administração e Especialização em Docência pela ULBRA; Especialização em Gestão da Educação pela UFF/RJ e MBA em Recursos Humanos pela UNINTER.

Ricardo Willy Rieth

Doutor (1992) e Pós-Doutor (2000) em História pelo Instituto de Estudos em História da Baixa Idade Média da Universität Leipzig, Alemanha. Possui graduação em Ciências Sociais (Bacharelado) pela UNISINOS (1988) e MBA em Gestão Empresarial pela FGV (2019). É professor no PPGEDU da ULBRA e de agosto de 2018 a dezembro de 2019 foi Reitor da mesma instituição.

EDUCAÇÃO CORPORATIVA MILITAR: ESTRATÉGIA PARA A SEGURANÇA E DEFESA CIBERNÉTICA NA FORÇA AÉREA BRASILEIRA

CORPORATE MILITARY EDUCATION: STRATEGY FOR CYBER SECURITY AND DEFENSE IN THE BRAZILIAN AIR FORCE

RESUMO: O artigo aborda um tema de grande relevância para a Segurança e Defesa Nacional na atualidade. Observa-se que foi acrescentado às quatro dimensões de batalha convencionais da guerra (terrestre, naval, aérea e espacial) o espaço cibernético. Por este motivo, o objetivo é analisar a Educação Corporativa Militar, desenvolvida pela Força Aérea Brasileira (FAB), voltada para a segurança e defesa cibernética. Para tanto, questiona-se de que forma este processo de capacitação pode contribuir estrategicamente no campo da cibernética. No primeiro tópico, serão apresentados embasamentos teóricos e conceitos relacionados ao tema, tendo em vista a ampliação dos recursos tecnológicos e as mudanças recentes nas estruturas de segurança e defesa. Já no segundo tópico, será analisado como a Educação Corporativa Militar contribui com a segurança e defesa cibernética, buscando também compreender seu alinhamento com o Livro Branco de Defesa Nacional. A metodologia empregada é de cunho qualitativo, por meio de pesquisa bibliográfica e documental. O estudo possibilitou compreender como as Forças Armadas estão atuando frente aos desafios no âmbito da cibernética, principalmente na profissionalização e na formação continuada de seus recursos humanos no território nacional brasileiro. Em consequência, observou-se a relevância da Educação Corporativa Militar na Força Aérea Brasileira (FAB) como uma estratégia para a segurança e defesa cibernética.

Palavras-chave: Educação Corporativa Militar; Segurança Cibernética; Defesa Cibernética.

ABSTRACT: The article proposes to address a topic of great relevance for National Security and Defense in contemporary times. To the four dimensions of war: terrestrial, naval, air and space, was added the dimension of cyberspace. For this reason, the aim is to analyze Corporate Military Education, developed by the Brazilian Air Force (FAB), focused on cybersecurity and defense. Therefore, it is questioned how this educational process can contribute strategically in the field of cybernetics. In the first topic, theoretical foundations and concepts related to this topic will be presented, with special attention to technological resources and recent changes in structures of security and defense. In the second topic, it will be analyzed how Military Corporate Education contributes to cybersecurity and defense, searching for its alignment with the White Paper on National Defense. The methodology used is qualitative, through bibliographic and documentary research. It was possible to understand how the Armed Forces are acting in the face of challenges in the field of cybernetics, especially in the professionalization and continuous training of their human resources in the Brazilian national territory. As a result, the relevance of Military Corporate Education in the Brazilian Air Force (FAB) was observed as a strategy for cyber security and defense.

Keywords: Military Corporate Education; Cybernetics Security; Cybernetics Defense.

1 Introdução[1]

O campo de batalha no século XXI passou por diversas mudanças. O conflito de guerra, que anteriormente ocorria de forma simétrica entre duas ou mais nações, ou seja, no enfrentamento direto, não é mais o único existente. O combate possuía quatro dimensões convencionais de guerra: terrestre, naval, aérea e espacial. Atualmente, foi incorporado o espaço cibernético (DE PAULA, 2016), tema que imprime grandes desafios aos países que estão sofrendo com ataques nesta área.

Com o estabelecimento do Setor Cibernético, decorrente da aprovação da Estratégia Nacional de Defesa (END)[2], a situação evoluiu e dois campos distintos passaram a ser reconhecidos: a) a Segurança Cibernética, a cargo da Presidência da República (PR), por meio do Gabinete de Segurança Institucional (GSI); e, b) a Defesa Cibernética, centrada no Ministério da Defesa, que conta ainda com Estado-Maior Conjunto das Forças Armadas e centros de defesa cibernética de cada uma das Forças (BRASIL, 2008).

Neste sentido, destaca-se a segurança e defesa cibernética como uma necessidade essencial a todo país que deseja manter a soberania de seu espaço aéreo, territorial e marítimo. Para isso, torna-se imprescindível que sejam estruturadas, mantidas e, permanentemente, verificadas as estratégias de segurança e defesa que estão sendo empregadas, pois requerem atenção especial para que possam garantir, de maneira eficiente, o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional.

Torna-se importante destacar a diferenciação entre segurança cibernética e defesa cibernética, sob a perspectiva de Souza (2013). O autor infere que a segurança cibernética está voltada ao combate e à prevenção de crimes cibernéticos na esfera da segurança pública, sendo uma questão de investigação policial. Já a defesa cibernética diz respeito aos aspectos operacionais e táticos das Forças Armadas, no sentido de prevenir ou contra-atacar, por exemplo, numa situação de guerra cibernética (SOUZA, 2013).

O Brasil possui três documentos de grande relevância na área de Defesa: a Política Nacional de Defesa (PND), a Estratégia Nacional de Defesa (END) e o Livro Branco de Defesa Nacional (LBDN). Segundo o portal do Ministério da Defesa, a Política Nacional de Defesa (PND) é o principal documento de planejamento da defesa do País, o qual estabelece objetivos e diretrizes para o preparo e emprego da capacitação nacional, com o envolvimento dos setores

[1] O conteúdo do artigo apoia-se em resultados da pesquisa que originou a dissertação de mestrado de Otoniel Fontana Silva: "Educação Corporativa Militar: a construção de identidades e representações a partir da análise dos cursos de formação da Força Aérea Brasileira".

[2] Sua primeira edição foi em 2008.

militar e civil, em todas as esferas de poder. A Estratégia Nacional de Defesa (END), por sua vez, pretende definir como fazer o que está determinado na PND. Já o Livro Branco de Defesa Nacional (LBDN) apresenta uma visão geral da defesa e das Forças Armadas, tendo como principal propósito permitir transparência e promover a confiança entre os países (BRASIL, 2020a).

Além desses documentos mencionados, têm-se aqueles voltados à defesa cibernética: Política Cibernética de Defesa e a Doutrina Militar de Defesa Cibernética; e à segurança cibernética: Livro Verde de Segurança Cibernética e Estratégia Nacional de Segurança Cibernética (E-Ciber), que orienta a sociedade brasileira sobre as principais ações do governo federal, em termos nacionais e internacionais, na área da segurança cibernética.

O professor Scott D. Tollefson, da *National Defense University* (NDU - Washington D.C./EUA), afirma que nas últimas três décadas, este campo de estudo no Brasil tem se acentuado de modo surpreendente (ARTURI; MACHADO, 2014). Svartman (2014) destaca também que "o primeiro documento a anunciar abertamente a política de defesa brasileira desde a promulgação da Constituição de 1988 foi a Política de Defesa Nacional (PDN) de 1996".

O Livro Branco de Defesa Nacional (BRASIL, 2020a) infere que o Brasil deve ter um cuidado especial com a sua defesa, procurando manter-se compatível com seu porte político-estratégico. Além disso, esclarece também que uma das mais importantes atribuições do Estado é prover a segurança e a defesa necessárias para que a sociedade possa se desenvolver e alcançar seus objetivos.

A formulação de estratégias e o planejamento de ações direcionadas à segurança e defesa têm tomado proporções consideráveis, pois se trata de uma necessidade essencial ao país. Por esta razão, a PND é estabelecida como o conjunto de medidas e ações do Estado, no campo militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças externas, potenciais ou manifestas. Alinhada a isso está a Força Aérea Brasileira, que tem como missão "manter a soberania do espaço aéreo e integrar o território nacional, com vistas à defesa da pátria" (BRASIL, 2018, p. 20).

A Estratégia Nacional de Defesa (END) elencou três setores como estratégicos: o nuclear, o cibernético e o espacial. A Diretriz Ministerial do MD nº 14/2009 determinou que o setor nuclear ficasse sob a coordenação da Marinha, o cibernético com o Exército e o setor espacial com a Força Aérea. Nos três setores, a prioridade é elevar a capacitação científica e tecnológica do País e preparar recursos humanos para atuarem, sempre que exigido, no limite do conhecimento. Embora o setor cibernético esteja sob a coordenação do Exército, o presente

artigo dirige sua atenção primordialmente a análises da Educação Corporativa Militar, desenvolvida pela Força Aérea Brasileira (FAB), voltada para a segurança e defesa cibernética. Para tanto, questiona-se de que forma este processo de capacitação pode contribuir estrategicamente com o campo da cibernética.

A metodologia empregada é de cunho qualitativo, por meio de pesquisa bibliográfica, que, segundo Gil (2002, p. 44), "é desenvolvida a partir de material já elaborado, constituído, principalmente, de livros e artigos científicos ligados à temática pesquisada". No primeiro tópico, são apresentados conceitos relacionados à segurança e defesa cibernética e apresentam-se documentos e legislações oficiais que tratam desse tema. Posteriormente, no segundo tópico, o objetivo foi identificar aspectos voltados à Educação Corporativa na FAB e como ela direciona seus recursos humanos para alcançarem as competências profissiográficas necessárias aos desafios contemporâneos no âmbito da cibernética. Para tanto, foi realizado um levantamento dos últimos 5 (cinco) anos (2017 - 2021), no portal da Força Aérea Brasileira, de assuntos que tratem das estratégias aplicadas em formação e aperfeiçoamento de temas relacionados à segurança e defesa cibernética.

2 Educação Corporativa Militar

As Forças Armadas possuem demandas específicas na formação de seus recursos humanos que dificilmente poderiam ser desenvolvidas ou produzidas por uma instituição de ensino civil. Por este motivo, mantêm suas próprias escolas de formação e aperfeiçoamento, cujas características se enquadram no conceito de educação corporativa, tendo em vista que a aprendizagem de seu pessoal ocorre, justamente, no interior e por intermédio de sua corporação. Nesse sentido, o termo Educação Corporativa Militar[3] torna-se pertinente a este modelo de ensino, que pode ser caracterizado como intrainstitucional.

Desta forma, seguindo este entendimento, a PND infere que

> O Brasil deve estar em condições de ampliar rapidamente seus recursos humanos e meios materiais disponíveis em prol da Defesa Nacional, tendo em vista que os investimentos em capacitação são pressupostos essenciais para a obtenção de recursos humanos qualificados" (BRASIL, 2020a, p. 34).

[3] "Educação Corporativa Militar": expressão criada pelo Pesquisador Militar Otoniel Fontana Silva, em seu trabalho de mestrado intitulado "Educação Corporativa Militar: a construção de identidades e representações a partir da análise de currículos dos cursos de formação da Força Aérea Brasileira".

A Educação Corporativa apresenta-se como um reflexo das estratégias e das novas propostas para a defesa. Os processos de formação e capacitação são consequências das demandas provenientes das estratégias de inovação tecnológica no âmbito da Defesa. Sendo assim, este tema se torna importante para a compreensão de como ocorre a capacitação dos membros das Forças Armadas, ou seja, como são aperfeiçoados os recursos humanos militares.

A Educação Corporativa representa, portanto, uma nova dimensão para o treinamento e desenvolvimento de recursos humanos. "Seu foco reside na organização que aprende, que estimula o aprendizado, principalmente, no que se refere às competências essenciais da organização" (BAYMA, 2004, p. 25). Daí surge o papel das universidades corporativas, que visam garantir a educação continuada interna, fazendo a ligação entre os objetivos da instituição, o seu planejamento estratégico e a busca de recursos e conhecimentos.

Na perspectiva de Eboli (2004), uma organização que aprende é uma organização capacitada em criar, adquirir e transferir conhecimentos e em modificar seus comportamentos para refletir estes novos conhecimentos e *insights*. Sob a perspectiva de Tarapanoff e Alvares (2012), o que tornaria a educação corporativa verdadeiramente corporativa é a sua ligação com a estratégia institucional.

A Diretriz de Comando da Aeronáutica DCA 11-45/2016 trata da Concepção Estratégica "Força Aérea 100", que tem por finalidade estabelecer a visão para a Força Aérea Brasileira (FAB) ao completar 100 anos de sua criação. O documento serve de orientação para o Planejamento Estratégico Militar da Aeronáutica (PEMAER) e as demais fases do planejamento institucional. Ao tratar dos aspectos voltados à Gestão de Recursos Humanos, afirma que o fator humano permanece no centro das prioridades da FAB.

Conforme o documento, a gestão dos recursos humanos aperfeiçoará os processos de recrutamento e seleção, enfocando a formação e a especialização com vistas ao cumprimento da missão constitucional da Aeronáutica, considerando tanto o preparo e emprego da FAB, quanto o aprimoramento técnico-profissional, visando à elevação dos conhecimentos que contemplam os níveis intelectual, cultural e analítico de seus integrantes (BRASIL, 2016).

Com isso, a dinâmica de recrutamento deve estar focada na estruturação de uma força de trabalho mista, com profissionais de carreira e temporários, que devem ser preparados para a incorporação de novos sistemas de armas e conceitos nas diversas áreas. Além disso, o plano é reduzir a quantidade de pessoal na área de apoio e ampliar os recursos humanos voltados para a atividade fim. A formação do militar da FAB "deve estar pautada em um modelo de ensino que permita ao ativo mais valioso da organização interagir, de modo sinérgico, com atores de

outras Forças e agências, sejam elas nacionais ou internacionais" (BRASIL, 2016, p. 32). De maneira que, "a FAB deve ser capaz de modernizar suas técnicas de formação, especialização, preservando as normas e disciplina necessárias para alcançar a eficácia identificada na sua visão para o futuro" (Ibid.).

Em 2017, a Força Aérea Brasileira publicou um Plano de Modernização. Este documento oficial preconiza alguns pontos que devem ser alterados na estrutura da FAB. O documento trata da reestruturação, aperfeiçoamento e modernização de seu sistema de ensino, com foco em diversas áreas estratégicas, entre elas o desenvolvimento de recursos humanos capacitados a atuarem em diversas frentes, como, por exemplo, na defesa cibernética.

A proposta da Diretoria de Ensino (DIRENS) para uma Força Aérea moderna e eficaz elencou três grandes aspectos para a modernização: aspectos gerenciais, pedagógicos e de infraestrutura. A referida subdivisão, de acordo com o documento, propõe uma visão didática e aponta as ações práticas que respaldam efetivamente as mudanças preconizadas. Cada segmento apresenta, sob seu escopo, metas definidas a curto, médio e longo prazos (BRASIL, 2017d).

Interessa a esta pesquisa, de modo especial, a proposta de modernização sob os aspectos tecnológicos voltados ao ciberespaço, tendo em vista que grande parte dos processos de aprendizagem têm se desenvolvido neste espaço. Segundo o documento analisado,

> Com o advento da modernização, o DEPENS [Departamento de Ensino][4], com foco no aperfeiçoamento do ensino da Força Aérea e na melhoria dos processos educativos, está comprometido em reestruturar e estabelecer normas e diretrizes de forma a dinamizar o ensino na nova concepção pedagógica proposta" (BRASIL, 2017d, p. 45).

De acordo ainda com o documento, esta nova concepção pedagógica está associada à modificação do ensino baseado em conteúdos e graus de aprendizagem para o desenvolvimento de uma metodologia de ensino que relacione teoria e prática.

Nesse contexto de modernização, merece destaque a recente inclusão do campo da Defesa como área de saber científico, pela CAPES, que, segundo reportagem no site da FAB, de julho de 2017, "traz novas perspectivas para o ensino da pós-graduação na Universidade da Força Aérea (UNIFA), contribuindo como atrativo para pesquisadores civis na academia". Com a atual criação do doutorado profissional no País, surgem novas perspectivas para o desenvolvimento de pesquisas avançadas no campo da Defesa brasileira.

[4] O Departamento de Ensino teve sua nomenclatura alterada para Diretoria de Ensino (DIRENS) em 17 de abril de 2017.

São mudanças que trarão benefícios ao Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA), em termos de parcerias, crescimento e internacionalização (BRASIL 2017a). O site da FAB cita uma entrevista realizada sobre o assunto com o Vice-Reitor Acadêmico da UNIFA, Brigadeiro Intendente Luiz Tirrê Freire, o qual afirmou que:

> O segmento da Defesa é um assunto antigo, que possui concepções iniciadas com a criação de documentos, como a Estratégia Nacional de Defesa e o Livro Branco de Defesa. Essa decisão vai fazer com que os processos da Defesa sejam melhor recebidos, agora com roupagem civil no segmento acadêmico, promovendo uma integração do ambiente militar com a sociedade como parte do processo (BRASIL, 2017a, s. p.).

A referência acima traz uma compreensão importante no que se refere à integração entre as Forças Armadas e a sociedade, que pode se tornar parte nesse processo. Para o Pró-Reitor de Pós-Graduação e Pesquisa da UNIFA, Coronel Aviador Hudson Ávila Diniz,

> A novidade vai trazer integração entre pesquisadores civis com as temáticas militares. A medida vai nos levar a ter pesquisadores para pensar especificamente no poder aeroespacial, mais sensíveis aos temas de defesa e segurança nacionais, sejam militares ou civis, o que irá contribuir estrategicamente para a abertura de vagas para pensadores na área de segurança do País, para pessoas capacitadas a preencher vagas no Ministério da Defesa (BRASIL, 2017a, s. p.).

Verifica-se, conforme palavras do Pró-Reitor da UNIFA, uma integração entre o meio militar e pesquisadores civis sobre temáticas no âmbito da defesa. Observa-se uma cooperação civil-militar harmoniosa, que pode ser verificada pela troca de experiências, de modo que nos eventos militares são convidados professores civis e nos seminários acadêmicos externos são convidados pesquisadores militares.

Como exemplos dessa integração, cita-se o XXI Ciclo de Estudos Estratégicos, que ocorreu na Escola de Comando e Estado-Maior do Exército (ECEME), em julho de 2019; e o 2º Ciclo de Estudos Estratégicos de Defesa, que ocorreu em maio de 2020 na Escola Superior de Guerra. Segundo publicação no Portal da FAB, este último evento contou com a participação simultânea de 240 pessoas em um ambiente virtual, reunindo executivos e industriais. Foram debatidas formas de interação e cooperação para o desenvolvimento de tecnologias inovadoras à Defesa, com aplicabilidade no meio militar e civil (BRASIL, 2020c).

Em dezembro de 2017, a Universidade da Força Aérea (UNIFA) promoveu o I Seminário de Segurança e Defesa Cibernética. O evento contou com a participação do corpo docente e discente da UNIFA, totalizando 290 inscritos, entre militares das Forças Armadas, representantes de instituições de ensino superior, pesquisadores, professores, convidados e interessados nos riscos e nas inovações tecnológicas das estruturas críticas do cenário

cibernético (BRASIL, 2017c). Neste seminário, o Coronel Paulo Sergio Porto, do Comando de Defesa Cibernética, destacou que "para se opor a possíveis ataques cibernéticos é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação" (BRASIL, 2017c). Tais aspectos demonstram, entre outras coisas, o desenvolvimento e a progressão tanto da FAB como das Forças Armadas na busca por realizar estas aproximações.

Outra reportagem sobre a Reestruturação do Ensino na FAB foi publicada no dia 8 de agosto de 2017 e ressalta as principais transformações estratégicas de gestão de ensino, que estão a cargo da Diretoria de Ensino da Aeronáutica (DIRENS). Segundo a matéria, as transformações são frutos das estratégias de modernização, que, de acordo com o plano, consiste num processo que deveria ser finalizado em 2021 (BRASIL, 2017b).

O processo denominado pela FAB como Plano de Modernização, caracteriza-se, de forma geral, pela reformulação na estrutura educacional e tecnológica, tendo por objetivo adequar o militar às exigências dos novos tempos, que impõem o preparo de um profissional competente, hábil, ativo, com habilidades práticas de trabalho, e não apenas teóricas, mas que seja coerente com os novos pensamentos de pronta resposta operacional, contribuindo para a segurança e defesa do Brasil.

Observa-se que o Plano de Modernização está alinhado à Política de Defesa Nacional (BRASIL, 2005), que segundo Visentini e Pereira (2014, p. 94)

> é inovadora no sentido de buscar promover o desenvolvimento e o reaparelhamento de nossas Forças Armadas, baseando-se no princípio de independência tecnológica e superação de entraves de desenvolvimento científico e tecnológico.

Uma das estratégias utilizadas para o aprimoramento dos recursos humanos elencadas no Plano de Modernização, no sentido de preparar operacionalmente com conhecimentos sobre técnicas de ataque e defesa cibernética, está o amplo investimento na Educação a Distância (EAD). Na atualidade, poucas são as organizações de ensino e Instituições de Ensino Superior (IES) no Brasil que ainda não empreenderam nesta modalidade. Observa-se, entretanto, que além dos aspectos positivos, existem questões negativas que podem ser melhoradas.

Como prova deste investimento, a EAD se reflete nas estratégias e nas novas propostas para o Plano de Modernização da FAB. De modo que as estratégias de modernização estão voltadas para o alcance dos objetivos da Educação Corporativa Militar, a qual tem como foco proporcionar a formação, o aperfeiçoamento e a especialização dos profissionais militares, de acordo com os quadros e níveis hierárquicos. Entretanto, dentre as diretrizes preconizadas no documento, têm-se estabelecido transformações de natureza tecnológica, observadas também

pelo investimento em plataformas virtuais de aprendizagem para a ampliação da Educação a Distância.

A Educação a Distância pode ser vista, assim, como uma grande aliada na Educação Corporativa Militar. Além disso, apresenta-se como uma estratégia eficiente para as organizações de ensino cumprirem sua missão, como também para o aprimoramento de seus recursos humanos, com vistas à segurança e defesa nacional. Torna-se pertinente destacar uma das falas do Comandante do Centro de Instrução Especializada da Aeronáutica, Luiz Gomes Jardim que, ao tratar sobre a EAD na FAB, diz:

> A educação a distância tem sido efetivamente benéfica para o processo de capacitação e atualização dos profissionais de toda a Força. [...] Nesse sentido, as possibilidades de acesso ao conhecimento que a EaD apresenta, principalmente àqueles que atuam em localidades isoladas, como a região amazônica, por exemplo, são estratégicas para proporcionar, em tempo hábil, a educação corporativa (JARDIM, 2007, p. 7).

A questão da educação a distância na FAB é visualizada, assim, como uma forma estratégica do uso da tecnologia, além de algumas mudanças no contexto educacional. Os cursos descentralizados nas unidades militares, conforme relatado, visam à redução de custo, maior acesso por parte de militares afastados dos centros de formação e celeridade no processo formativo. Observa-se também que, além dos novos cursos criados nesta modalidade, cursos presenciais foram transformados para a modalidade EAD ou ainda se tornaram híbridos, isto é, uma parte presencial, outra a distância.

Como forma de investigar o esforço da Força Aérea no envolvimento com a capacitação de seus recursos humanos, torna-se relevante analisar os cursos de formação oriundos da Academia da Força Aérea (AFA) e os eventos de capacitação voltados para esta temática. O currículo do Curso de Formação do Oficial Aviador, Oficial Intendente e Oficial de Infantaria traz, em suas ementas, conteúdos que tratam sobre segurança e defesa cibernética. Dentre os assuntos elencados no currículo, cita-se: a) legislações relacionadas com a atividade cibernética no Brasil; b) medidas de proteção no Espaço Cibernético; c) eventos para o conhecimento cibernético no mundo e no COMAER[5]; d) inteligência Cibernética; e) doutrina Cibernética e conduta no espaço Cibernético; f) fundamentos da Doutrina militar de Defesa Cibernética; e, g) estrutura e organização do Sistema de Segurança e Defesa do COMAER (BRASIL, 2019a).

De especial importância para a presente investigação foi a realização de análises no Portal Institucional da FAB[6], a fim de reunir informações acerca de publicações de eventos,

[5] COMAER: Comando da Aeronáutica.
[6] (www.fab.mil.br), busca na ferramenta de pesquisa por: “cibernética”.

seminários e workshops que estivessem voltados à capacitação e profissionalização no sentido das demandas requeridas para uma eficiente Segurança e Defesa Cibernética no país. Os eventos analisados são tanto aqueles promovidos pela FAB, quanto aqueles em que a FAB participou.

Para tanto, foram investigadas as publicações dos últimos cinco anos (2017 - 2021). Estas informações são apresentadas abaixo, no quadro onde estão descritos: nome e objetivo; quem promoveu o evento e data de sua realização.

Quadro 1 – Eventos voltados à Segurança e Defesa Cibernética

Nome e objetivo do evento	*Quem promoveu o evento e data*
O **Guardião Cibernético 3.0** é considerado o maior evento da área no Hemisfério Sul. É um exercício simulado de atividades práticas de proteção cibernética, com a participação de líderes e especialistas em tecnologia da informação. A atividade tem o propósito de incrementar a proteção do espaço cibernético no âmbito da Defesa, por meio da atuação colaborativa junto a infraestruturas críticas de vários setores.	**Coordenado pelo Comando de Defesa Cibernética (ComDCiber)**, localizado em Brasília (DF), o evento ocorreu de 5 a 7 de outubro/2021 e reuniu 65 organizações e 350 especialistas em tecnologia da informação dos setores estratégicos do Brasil, entre civis e militares.
O Núcleo do Centro de Defesa Cibernética da Aeronáutica participa do **Locked Shields 2021**. É considerado o maior e o mais complexo exercício cibernético internacional. Simulando um cenário de apoio a um país fictício, as equipes são enviadas na defesa e na restauração dos sistemas atacados: defesa aérea, água, financeiro e espacial. Além disso, são apresentados incidentes cibernéticos nos níveis decisórios para verificação dos níveis de maturidade dos países em relação a assuntos de segurança cibernética e de proteção de dados.	Neste ano, o evento ocorreu entre os dias 13 e 16 de abril de 2021, em Tallinn, na Estônia, e reuniu mais de 2 mil especialistas de 23 países. Participaram, também, militares integrantes do Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER), além de especialistas do Comando de Operações Aeroespaciais (COMAE). O evento, que acontece anualmente, é organizado pelo **Centro de Excelência de Defesa Cibernética Cooperativa (CCDCOE) da OTAN.**
II Seminário de Segurança e Defesa Cibernética, com foco nos desafios da Defesa Cibernética na Projeção Espacial Brasileira. O principal objetivo do encontro é apresentar o cenário atual e perspectivas futuras de assuntos como quinto domínio de guerra, vulnerabilidade da internet das coisas, guerra cibernética nas olimpíadas e paralimpíadas e outros temas relacionados à segurança da informação.	O seminário ocorreu em novembro de 2020, realizado pela **Universidade da Força Aérea (UNIFA) em parceria com a Fundação Getúlio Vargas (FGV).**
O Instituto Tecnológico de Aeronáutica (ITA) conquistou a primeira colocação na 6ª edição da **Competição Cibernética do tipo Capture the Flag** (Captura de Bandeira) das Forças Armadas, mais conhecida como **Mandabyte**. O evento tem como objetivo a descoberta de novos talentos na área de Tecnologia da Informação (TI), a promoção e difusão da cultura de segurança e defesa cibernética, além do incentivo e aperfeiçoamento dos militares.	A sexta edição do Mandabyte, realizada em 13 de novembro de 2019, contou com a participação de 176 militares de todo o Brasil. A disputa ocorreu com desafios do tipo Capture the Flag, em seis áreas de conhecimento cibernético: Criptografia, Pentest Profissional, Pentest em Aplicações Web, Engenharia de Código, Forense Computacional e Miscelâneas. As atividades foram coordenadas pela **Escola Nacional de Defesa Cibernética (ENaDCiber), com o suporte técnico do Centro de Defesa Cibernética (CDCiber)**.

Exercício Guardião Cibernético 2.0. O Exercício é voltado para a proteção cibernética por meio da atuação colaborativa envolvendo as três Forças Armadas, órgãos públicos e entidades privadas dos setores elétrico, financeiro, nuclear e de telecomunicações. A atividade utilizou o programa Simulador de Operações Cibernéticas (SIMOC), reproduzindo sistemas computacionais. A simulação envolveu gabinetes de crise das áreas de tecnologia da informação, comunicação social, jurídica e alta administração de eventos cibernéticos com impacto nas organizações.	A Força Aérea Brasileira (FAB) participou, entre os dias 2 e 4 de junho de 2019, em Brasília (DF), do Exercício Guardião Cibernético 2.0 – um treinamento simulado de proteção a ataques cibernéticos, promovido pelo **Comando de Defesa Cibernética (ComDCiber)**. No total, 214 participantes e 40 empresas e organizações públicas participaram, de forma colaborativa e integrada.
Reunião de Integração do Centro de Defesa Cibernética. O Evento busca a integração das Forças Armadas e discussões de assuntos técnicos na área cibernética. O objetivo do GTT é debater soluções tecnológicas para o Sistema Militar de Defesa Cibernética (SMDC), principalmente na área de consciência situacional cibernética. Também foram deliberados assuntos relacionados ao nível de alerta cibernético.	O **Centro de Defesa Cibernética (CDCiber)**, sob a coordenação da 3ª Subchefia do Estado-Maior da Aeronáutica (3SC EMAER) e do Centro de Computação da Aeronáutica de Brasília (CCA-BR), promoveu, nesta quarta e quinta-feira (12 e 13/06/2019), a Reunião do Grupo de Trabalho Técnico (GTT) Integração na FAB.
Exercício Guardião Cibernético – um treinamento simulado de proteção a ataques cibernéticos, voltado aos setores financeiro e nuclear. O exercício utilizou o programa Simulador de Operações Cibernéticas (SIMOC). Um dos resultados do exercício foi a identificação de premissas básicas para a elaboração de um Plano Nacional de Tratamento e Resposta a Eventos de Segurança Cibernética nos setores nuclear e financeiro.	A atividade, que aconteceu entre os dias 3 e 6 de julho/2018 em Brasília (DF) e foi coordenada pelo **Comando de Defesa Cibernética (ComDCiber)**, contou com a participação de militares das três Forças e outros órgãos governamentais, além de empresas do setor nuclear, bancos e comunidade acadêmica.
A UNIFA promoveu **I Seminário de Segurança e Defesa Cibernética**. O evento contou com a participação do corpo docente e discente da UNIFA, totalizando 290 inscritos, entre militares das Forças Armadas, integrantes de entidades de ensino superior, doutores, professores, convidados e interessados nos riscos e nas inovações tecnológicas das estruturas críticas do cenário cibernético.	A Universidade da Força Aérea (UNIFA), no Rio de Janeiro (RJ), promoveu, nos dias 13 e 14 de novembro/2017, o I Seminário de Segurança e Defesa Cibernética. Aberto ao público, em especial aos estudiosos do tema e ao universo acadêmico, o seminário foi organizado pelo **Centro de Estudos Estratégicos (CEE) da UNIFA**, em contribuição ao seu Programa de Pós-Graduação em Ciências Aeroespaciais (PPG-CA).

Fonte: Elaborado pelo autor com dados do Portal da FAB.

A partir das análises realizadas, observa-se que a Educação Corporativa Militar contribui com a segurança e defesa cibernética, tendo em vista a estratégia direcionada à profissionalização de militares e à formação continuada de recursos humanos, com foco no conhecimento sobre segurança e defesa cibernética. Constatou-se em uma matéria publicada pelo NOTAER[7], a FAB ratificando sua posição quanto às estratégias direcionadas a esta perspectiva, o Tenente-Brigadeiro do Ar Carlos de Almeida Baptista Júnior, atual Comandante

[7] O jornal NOTAER é uma publicação mensal do Centro de Comunicação Social da Aeronáutica (CECOMSAER).

da Aeronáutica, afirma o seguinte: “trataremos com afinco a valorização dos nossos recursos humanos para que, cada vez mais, sejam capazes de lidar com sistemas de alto nível tecnológico. Daremos continuidade aos nossos processos de formação e aperfeiçoamento” (BRASIL, 2021). Observou-se, também, que desde a formação na Academia da Força Aérea (AFA) até os eventos desenvolvidos, as estratégias aplicadas pela FAB estão conectadas ao que está preconizado no Livro Branco de Defesa Nacional, referente à preparação e capacitação do pessoal.

3 Considerações Finais

Este artigo buscou compreender o quanto a Educação Corporativa Militar, desenvolvida pela Força Aérea Brasileira (FAB), contribui para a segurança e defesa cibernética, com base na capacitação de seus profissionais militares para atuarem estrategicamente frente aos crescentes desafios contemporâneos deste campo da ciência.

As políticas de segurança e defesa cibernética desenvolvidas no Brasil, com destaque para a Força Aérea Brasileira, estão sendo direcionadas a olhar de modo especial às estratégias de capacitação de seus recursos humanos, alinhadas ao que preconiza o Livro Branco de Defesa Nacional (LBDN), principalmente no que diz respeito ao fomento da profissionalização de militares.

Em razão disso, no primeiro tópico deste trabalho, foram apresentados embasamentos teóricos e conceitos relacionados à segurança e defesa cibernética, tendo em vista a ampliação de recursos tecnológicos e as mudanças recentes nas estruturas de defesa. Tomando por referência a Estratégia Nacional de Defesa (END), a defesa cibernética necessita ainda de muitos investimentos para que o país tenha capacidade de reduzir a vulnerabilidade de seus sistemas cibernéticos. Por este motivo, as parcerias e as cooperações são fundamentais para que as Forças Armadas permaneçam com poder de reação e defesa.

Já no segundo tópico, foram abordados conceitos e análises referentes à Educação Corporativa Militar, que se apresenta como um reflexo das estratégias e das novas propostas de modernização para a segurança e defesa no âmbito das Forças Armadas, especialmente na FAB. Os processos de formação, aperfeiçoamento e capacitação dos recursos humanos são consequências das demandas provenientes do campo da Defesa. Sendo assim, a Concepção Estratégica “Força Aérea 100”, ao tratar dos aspectos voltados à gestão de recursos humanos, infere que o fator humano permanece no centro das prioridades da FAB, de modo que mantém

instituições e processos que estão promovendo continuamente cursos focados na formação de competências essenciais para esta abordagem.

Ao analisar os aspectos do Plano de Modernização da FAB foi possível verificar estratégias de modernização voltadas ao ciberespaço. A integração de pesquisadores civis e militares, com o objetivo de interagirem de forma estratégica nas temáticas mais sensíveis de segurança e defesa nacional, também indica um alinhamento à Política de Defesa Nacional, pois busca promover o desenvolvimento e o reaparelhamento das Forças Armadas, com independência tecnológica e superação de entraves de desenvolvimento científico e tecnológico.

Foram também abordadas as estratégias da FAB na ampliação da Educação a Distância, que se apresenta como um reflexo do Plano de Modernização do Ensino e que contribui estrategicamente com a formação de pessoal qualificado para atuar na área de segurança e defesa cibernética. A introdução de tecnologias adequadas para suporte à modalidade EAD demonstra um crescente desenvolvimento da Educação Corporativa Militar. Observou-se, ainda, que as questões voltadas à execução das políticas e estratégias de modernização, de desenvolvimento de recursos humanos, bem como de atenção à defesa cibernética, procuram seguir um planejamento preestabelecido.

Assim, após as análises realizadas, foi possível compreender que a Educação Corporativa Militar, desenvolvida pela Força Aérea Brasileira (FAB), contribui para a segurança e defesa cibernética.

4 Referências

ARTURI, Carlos Schmidt; MACHADO, Felipe. Políticas de Defesa, Inteligência e Segurança. *In*: ARTURI, Carlos (Org.). *Políticas de Defesa, Inteligência e Segurança*. Porto Alegre: UFRGS/CEGOV, 2014. 188 p. Disponível em: https://www.ufrgs.br/cegov/files/pub_38.pdf. Acesso em: jul. 2020.

BARKER, Ken. Cyber attack: what goes around comes around. *The School of Public Policy Publications - SPP Briefing Paper*, v. 12, n. 17, 2019. Disponível em: https://www.cgai.ca/cyberattack_what_goes_around_comes_around. Acesso em: abr. 2022.

BAYMA, Fátima. Educação a Distância e Educação Corporativa. *In*: BAYMA, Fátima (Org.). *Educação Corporativa: desenvolvendo e gerenciando competências*. São Paulo: Pearson Prentice Hall, 2004.

BRUSTOLIN, Vitelio. Comparative Analysis of Regulations for Cybersecurity and Cyber Defence in the United States and Brazil. *Revista Brasileira de Estudos de Defesa*, v. 6, n. 2, p. 93–123, jul./dez. 2019. Disponível em: https://rbed.abedef.org/rbed/article/view/75149. Acesso em: abr. 2022.

BRASIL. *Decreto nº 5.384, de 30 de junho de 2005*. Aprova a Política de Defesa Nacional e dá outras providências. Brasília/DF: Presidência da República, 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm. Acesso em: abr. 2022.

BRASIL. *Decreto nº 6.703, de 18 de dezembro de 2008*. Aprova a Estratégia Nacional de Defesa e dá outras providências. Brasília/DF: Presidência da República, 2008. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Exército Brasileiro. *Portal do Instituto Militar de Engenharia*. 2010a. Disponível em: http://www.defesacibernetica.ime.eb.br/.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. CANONGIA, Claudia; MANDARINO, Raphael (Orgs.). *Livro verde: segurança cibernética no Brasil*. Brasília: GSIPR/SE/DSIC, 2010b. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. *Doutrina Militar de Defesa Cibernética*. 2014. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_07a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. *Diretriz do Comando da Aeronáutica DCA 11-45/2016*. 2016. Disponível em: https://www.fab.mil.br/Download/arquivos/prestacaodecontas/DCA_11_45_2016_FAB_100.pdf. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Força Aérea Brasileira. Inserção da Defesa como área científica traz perspectivas para o mestrado na FAB. *Portal da FAB*, 28 jul. 2017. 2017a. Disponível em: https://www.fab.mil.br/noticias/mostra/30641/REESTRUTURA%C3%87%C3%83O%20-%20Inser%C3%A7%C3%A3o%20da%20Defesa%20como%20%C3%A1rea%20cient%C3%ADfica%20traz%20perspectivas%20para%20o%20mestrado%20na%20FAB. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Força Aérea Brasileira. Diretoria de Ensino da Aeronáutica divulga mudanças na área da educação. *Portal da FAB*, 8 ago. 2017. 2017b. Disponível em:

https://www.fab.mil.br/noticias/mostra/30681/REESTRUTURA%C3%87%C3%83O%20-%20Diretoria%20de%20Ensino%20da%20Aeron%C3%A1utica%20divulga%20mudan%C3%A7as%20na%20%C3%A1rea%20da%20educa%C3%A7%C3%A3o. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Força Aérea Brasileira. UNIFA promove I Seminário de Segurança e Defesa Cibernética. *Portal da FAB*, 20 nov. 2017c. Disponível em: https://www.fab.mil.br/noticias/mostra/31293/EVENTO%20-%20UNIFA%20promove%20I%20Semin%C3%A1rio%20de%20Seguran%C3%A7a%20e%20Defesa%20Cibern%C3%A9tica. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Força Aérea Brasileira. *PCA 37-11 Plano de Modernização do Ensino da Aeronáutica*. 2017d. Disponível em: https://www.fab.mil.br/cabine/anexos/_pca_37-11.pdf. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. *Diretriz do Comando da Aeronáutica DCA 11-45/2018*. 2018. Disponível em: https://www.fab.mil.br/Download/arquivos/prestacaodecontas/DCA_11_45_2018_FAB_100.pdf. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Força Aérea Brasileira. Sistema de Legislação da Aeronáutica. *Currículo Mínimo do Curso de Formação de Oficiais Aviadores*. 2019a. Disponível em: https://www.sislaer.fab.mil.br/terminalcendoc/Acervo/Detalhe/4886?a=1&guid=1604793608531. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Exército Brasileiro. Com foco na cooperação mútua, 4º Estágio Internacional de Defesa Cibernética reúne militares de 10 países. *Portal do EB*, 15 mai. 2019. 2019b. Disponível em: https://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/znUQcGfQ6N3x/content/id/9894663. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. *Livro Branco de Defesa Nacional*. 2020a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. *Política Nacional de Defesa e Estratégia Nacional de Defesa*. 2020b. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Força Aérea Brasileira. FAB participa do 2º Ciclo de Estudos Estratégicos de Defesa. *Portal da FAB*, 3 jun. 2020c. Disponível em: https://www.fab.mil.br/noticias/mostra/35813/EVENTO%20-%20FAB%20participa%20do%202%C2%BA%20Ciclo%20de%20Estudos%20Estrat%C3%A9gicos%20de%20Defesa. Acesso em: abr. 2022.

BRASIL. *Decreto nº 10.222, de 5 de fevereiro de 2020*. Aprova a Estratégia Nacional de Segurança Cibernética. 2020d. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: abr. 2022.

BRASIL. Ministério da Defesa. Força Aérea Brasileira. *NOTAER - O Jornal da Força Aérea*, a. XLV, n. 5, mai. 2021. Disponível em: https://issuu.com/portalfab/docs/notaer_maio_2021?fr=sMDYyYjM0NzA1MTk. Acesso em: abr. 2022.

DE PAULA, Eduardo Rodrigues. *Guerra Cibernética:* Perspectivas para a consolidação de uma Estratégia cibernética para o Estado brasileiro. 2016. Monografia (Curso de Estado-Maior para Oficiais Superiores) – Escola de Guerra Naval, Rio de Janeiro, 2016. Disponível em: https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/CEMOS%20077%20MONO%20CC%20EDUARDO%20RODRIGUES.pdf. Acesso em: mai. 2022.

EBOLI, Marisa. Educação Corporativa: princípios de sucesso e melhores práticas. *In*: BAYMA, Fátima (Org.). *Educação Corporativa: desenvolvendo e gerenciando competências*. São Paulo: Pearson Prentice Hall, 2004.

FERREIRA, Ricardo Férre Lacerda. *USASEC: um método para integração de requisitos de usabilidade e segurança para proteção cibernética em aplicações WEB*. 2017. Dissertação (Mestrado em Informática) – Instituto Tecnológico de Aeronáutica, São José dos Campos, 2017. Disponível em: http://www.bdita.bibl.ita.br/tesesdigitais/73381.pdf. Acesso em: abr. 2022.

GIL, A. C. *Como elaborar projetos de pesquisa. São Paulo,* SP: Atlas, 2002.

HUNKER, Jeffrey. US international policy for cybersecurity: five issues that won't go away. *Journal of National Security Law & Policy*, v. 4, n. 1, p. 197-216, 2010. Disponível em: https://jnslp.com/2010/09/29/u-s-international-policy-for-cybersecurity-five-issues-that-won%E2%80%99t-go-away/. Acesso em: abr. 2022.

HUREL, Louise Marie. *Cibersegurança no Brasil*: uma análise da estratégia nacional. Artigo Estratégico 54, Instituto Igarapé, Rio de Janeiro, abr. 2021. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: abr. 2022.

JARDIM, Luiz Gomes. Força Aérea Brasileira (FAB). Galáxia da Educação a Distância. *Boletim da ABED*, ano X, ed. 29, jul./ago. 2007.

LOOSE, Júlia; PAGLIARI, Graciela de Conti. Israel e defesa cibernética: estudo da vinculação Estado, setor privado e academia. *Revista Brasileira de Estudos de Defesa*, v. 7, n. 2, p. 81-101, jul./dez. 2020. Disponível em: https://rbed.abedef.org/rbed/article/view/75206/42132. Acesso em: abr. 2022.

MANDARINO JR., Raphael. *Segurança e Defesa do Espaço Cibernético Brasileiro*. Brasília: CUBZAC, 2010.

MONTEIRO, Tânia. Segurança cibernética será reforçada. *O Estado de São Paulo*, São Paulo, 9 mar. 2020. Disponível em: https://acervo.estadao.com.br/pagina/#!/20200309-46164-nac-7-pol-a7-not. Acesso em: abr. 2022.

PINTO, Danielle Jacon Ayres; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. *Revista Brasileira de Estudos da Defesa*, v. 7, n. 2, p. 103-131, jul./dez. 2020. Disponível em: https://rbed.abedef.org/rbed/article/view/75178/42133 Acesso em: abr. 2022.

SOUZA, Gills Lopes Macêdo. *Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá*. 2013. Dissertação (Mestrado em Ciência Política) – Centro de Filosofia e Ciências Humanas, Universidade Federal de Pernambuco, Recife, 2013. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/12489/1/Disserta%C3%A7ao%20gills-lopes.pdf. Acesso em: abr. 2022.

SOUZA JUNIOR, Alcyon Ferreira de. *Segurança cibernética: política brasileira e a experiência internacional*. 2013. Dissertação (Mestrado em Gestão do Conhecimento e Tecnologia da Informação) – Universidade Católica de Brasília, Brasília, 2013. 120f. Disponível em: https://bdtd.ucb.br:8443/jspui/bitstream/123456789/1417/1/Alcyon%20Ferreira%20de%20Souza%20Junior.pdf. Acesso em: abr. 2022.

SILVA, Otoniel Fontana. *Educação Corporativa Militar*: a construção de identidades e representações a partir da análise dos cursos de formação da Força Aérea Brasileira. 2018. Dissertação (Mestrado em Educação) – Programa de Pós-Graduação em Educação, Universidade Luterana do Brasil, Canoas/RS, 2018. Disponível em: https://servicos.ulbra.br/BIBLIO/PPGEDUM270.pdf. Acesso em: abr. 2022.

SVARTMAN, Eduardo Munhoz. A Agenda de Defesa do Brasil para a América do Sul. *In*: ARTURI, Carlos Schmidt (Org.). *Políticas de Defesa, Inteligência e Segurança*. Porto Alegre: UFRGS/CEGOV, 2014. 188 p. Disponível em: https://www.ufrgs.br/cegov/files/pub_38.pdf. Acesso em: abr. 2022.

TARAPANOFF, Kira; ALVARES, Lillian. Educação Corporativa. *In*: TARAPANOFF, Kira (Org.). *Aprendizado Organizacional*: contexto e propostas. Vol. 2. Curitiba: Intersaberes, 2012.

THEOHARY, Catherine A.; ROLLINS, John W. Cyberwarfare and Cyberterrorism: In Brief. *Congressional Research Service*, March 27, 2015. Disponível em: https://nsarchive.gwu.edu/document/26888-document-034-congressional-research-service-catherine-theohary-and-john-w-rollins. Acesso em: abr. 2022.

VENTRE. Daniel. *Ciberguerra*. *In*: XIX Curso Internacional de Defensa: Seguridad global y potências emergentes em um mundo multipolar, 2011, Universidad Zaragoza, Jaca, Espanha. 2011, p. 31-46. Disponível em: https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF48.pdf. Acesso em: abr. 2022.

VISENTINI, Paulo Fagundes; PEREIRA, Analúcia Danilevicz. O Atlântico Sul como espaço estratégico para o Brasil: política externa e de defesa. *In*: ARTURI, Carlos Schmidt (Org.). *Políticas de Defesa, Inteligência e Segurança*. Porto Alegre: UFRGS/CEGOV, 2014. 188 p. Disponível em: https://www.ufrgs.br/cegov/files/pub_38.pdf. Acesso em: abr. 2022.

Recebido em 15 de maio de 2022.
Aceito para publicação em 24 de julho de 2022.