TENENTE-CORONEL JERÔNIMO
Instrutor da Academia de Guerra do Exército do Chile e Oficial de Ligação de Doutrina.

A CAPACIDADE CIBERNÉTICA NO EXÉRCITO DO CHILE

O ciberespaço ganha cada vez mais relevância no complexo cenário mundial. A globalização e o exponencial progresso tecnológico proporcionaram um avanço na era digital nunca experimentado.

Com esse avanço, iniciaram-se também as atividades ilícitas, criminosas e ofensivas no espaço cibernético, consubstanciando-se em uma nova ameaça para os estados-nação e demais organizações, afetando setores vitais dos países e, por consequência, atingindo também os cidadãos comuns.

A obra *La ciberguerra: sus impactos y desafíos*, publicada em 2018 pelo Centro de Estudos Estratégicos da Academia de Guerra (CEEAG) do Exército chileno, afirma que, em nível regional, os países que se destacaram como alvos de ciberataques, na América Latina, foram Brasil, Argentina, Colômbia, México e Chile. O acesso ou roubo de informações de um computador infectado predomina na região. Como exemplo, o autor cita uma família de códigos maliciosos – *Dorkbot* – que, em meados de 2016, gerou mais de 80.000 ações contra sistemas virtuais, concentrados no Chile (44%), Peru (15%) e Argentina (11%).

Assim, evidencia-se que a América Latina se configura como palco de inúmeros ataques cibernéticos, demonstrando ser uma região instável e insegura quanto à proteção de ativos no domínio cibernético.

Como consequência, o quinto domínio das operações militares – o ciberespaço – tem imprimido uma mudança no rol de atribuições das forças armadas, reorientando esforços e recursos para geração de novas capacidades para se contraporem às novas ameaças no ciberespaço, somado aos conceitos de zona cinza dos conflitos armados e guerra híbrida, com predominância de atores não estatais e ameaças difusas.

O Exército do Chile, visando gerar capacidades em face das necessidades atuais, projetou sua nova estrutura superior. Essas mudanças respondem aos novos cenários já mencionados, abarcando diferentes capacidades militares, otimizando recursos e sincronizando os respectivos atuadores.

Dentre essas mudanças, destaca-se o Comando de Operações Especiais (COPE), no final de 2020. O COPE está organizado com três brigadas operativas: Brigada de Operações Especiais (BOE), Brigada de Aviação do Exército (BAVE) e Brigada de Inteligência (BINTE). Trata-se de uma solução *sui generis*, pois reúne sob o mesmo comando as capacidades relacionadas às operações especiais, montanha, aviação, inteligência, guerra eletrônica e cibernética – sendo essas unidades preexistentes, mas que sob a égide de um comando único tem a expectativa de gerar uma sinergia e aumento dessas capacidades.

Cabe relembrar que se entende por capacidade como a aptidão requerida a uma força ou organização militar para cumprir determinada missão ou atividade. Essa aptidão é exercida sob condições e padrões determinados, pela combinação de meios para desempenhar uma gama de tarefas.

Ademais, a capacidade é obtida a partir de um conjunto de sete fatores determinantes, interrelacionados e indissociáveis: Doutrina, Organização (e/ou processos), Adestramento, Material, Educação, Pessoal e Infraestrutura – que formam o acrônimo DOAMEPI (Brasil, 2019).

Dessa forma, o objetivo do presente artigo é apresentar a atual situação da capacidade cibernética do Exército do Chile, segundo os fatores DOAMEPI.

> **Em nível regional, os países que se destacaram como alvos de ciberataques, na América Latina, foram Brasil, Argentina, Colômbia, México e Chile.**

O SETOR CIBERNÉTICO NO EXÉRCITO DO CHILE

O Chile adota um modelo, de forma similar à doutrina brasileira, onde a segurança cibernética representa um conceito mais amplo e abrangente, englobando as ações de defesa cibernética, de forma análoga à conhecida relação entre segurança e defesa nacional.

A defesa cibernética é a vertente do sistema segurança cibernética, a nível nacional, que reúne as capacidades das Forças Armadas para executar operações no ciberespaço. Assim, está focada na defesa e sobrevivência dos sistemas militares, bem como daqueles que são vitais para o bom funcionamento de diferentes órgãos estatais.

Outra importante observação é que suas

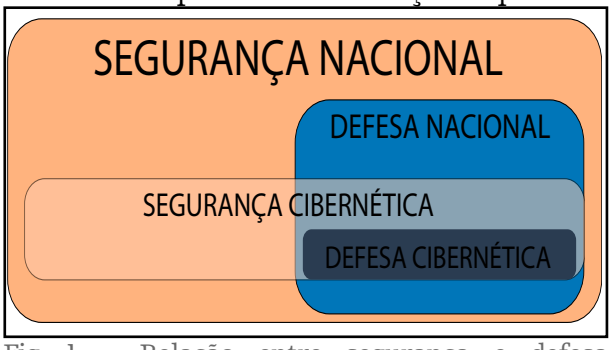

Fig 1 – Relação entre segurança e defesa cibernética. Fonte: o autor – adaptado de apresentação do Batalhão de Defesa Cibernética.

ações são respaldadas do ponto de vista jurídico, com base no princípio de legítima defesa, que permite o uso de capacidades militares de defesa cibernética ativa para lidar com ataques cibernéticos contra o Estado (MIRANDA, 2021).

Além disso, o Exército do Chile optou por subordinar a cibernética à função de combate inteligência, conforme o manual de defesa cibernética:

> As unidades e organizações de "Defesa Cibernética" constituem a parte dos meios institucionais de inteligência que são dedicados ao desenvolvimento de tarefas destinadas a proporcionar a devida segurança e proteção das informações institucionais que são armazenadas, processadas ou transmitidas pelos sistemas de informação do Exército, a fim de garantir disponibilidade, confidencialidade e integridade. (Regulamento RDI 20008 – Defesa Cibernética, 2016, p. 65)

Dessa maneira, a Diretoria de Planejamento de Informação do Exército (DIPLINE) representa o órgão de direção setorial de inteligência, contrainteligência, operações de informação e cibernética, sendo o escalão de mais alto nível do setor cibernético no exército. Cabe à DIPLINE aconselhar o Chefe do Estado-Maior no controle e coordenação das atividades executivas que, sob a autoridade da Brigada de Inteligência do Exército (órgão executivo), são realizadas pelas unidades de inteligência do Exército. (Ministério da Defesa Nacional, Decreto 305, 2021). Por sua vez, a BINTE é subordinada ao Comando de Operações Especiais.

Do exposto, infere-se que as atividades do setor cibernético estão concentradas na Brigada de Inteligência do Exército, subordinada ao Comando de Operações Especiais. Ou seja, não existe um órgão, no nível direção ou execução, que seja exclusivo para as atividades cibernéticas. Como efeito, pode-se gerar uma limitação da atuação e abrangência do setor cibernético, que em teoria deveria atuar de forma transversal com outras diretorias e órgãos, principalmente no tocante às ações de proteção cibernética, onde o usuário final também se torna protagonista do processo, representando o elo mais frágil ante uma tentativa hostil contra os sistemas próprios.

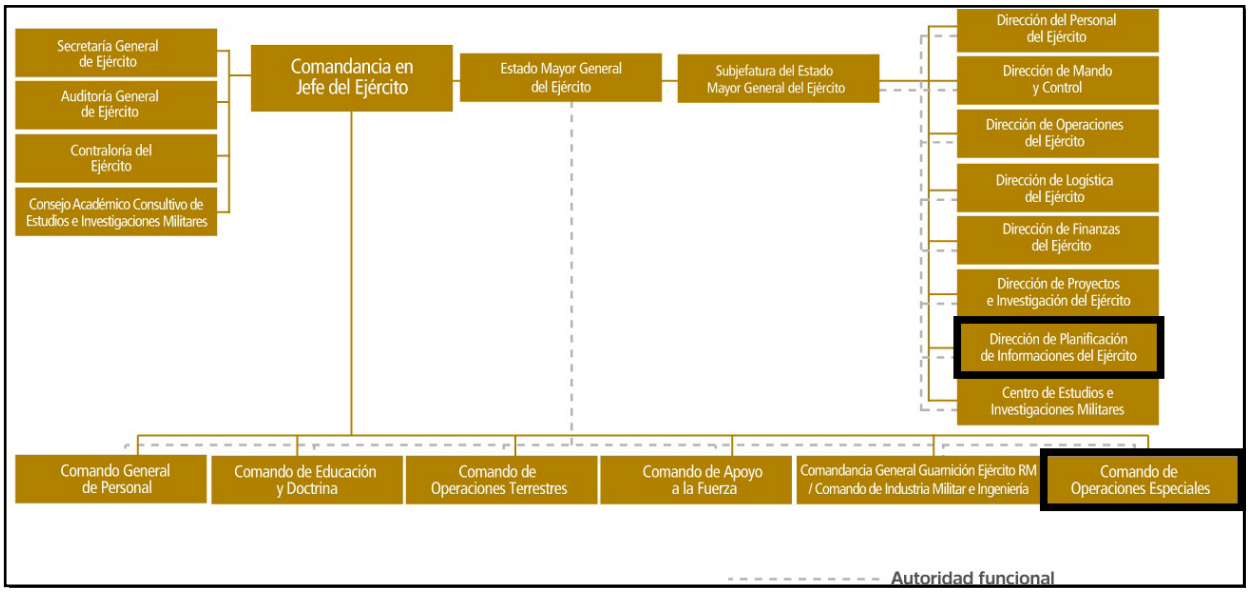

Fig 2 – Organização do Exército do Chile, com destaque para a DIPLINE e o COPE.
Fonte: Exército do Chile https://www.ejercito.cl/estructura-y-organizacion.

Outro fator importante é a fonte de recursos, que pode ter uma limitação em virtude da possível concorrência com outras áreas, como é o caso específico da inteligência, que está – pelo menos sob a ótica da organização – abrangendo a atividade cibernética.

Além disso, as Forças Armadas do Chile têm expressivo desenvolvimento das atividades conjuntas, sendo o Estado-Maior Conjunto (EMCO) o responsável pelo emprego das capacidades geradas pelas forças singulares. Entretanto, a capacidade cibernética, a nível conjunto, está em fase preliminar de implantação, não tendo uma estrutura organizada.

FATORES DOAMEPI - DOUTRINA

Segundo o manual Doutrina Militar Terrestre do Brasil, a doutrina é base para os demais fatores, estando materializado nos produtos doutrinários. Desse modo, a geração de capacidades de uma unidade ou força inicia-se com a formulação de sua base doutrinária, que considera a gama de missões (traduzida nas capacidades operativas), atividades e tarefas que essa unidade cumpre em operações.

A defesa cibernética, em nível institucional, tem sua base doutrinária no regulamento RDI - 20008 Defesa Cibernética, definindo a estrutura para a defesa cibernética no Exército do Chile.

Esse marco legal aborda os conceitos e definições próprios da cibernética, estipula o quadro jurídico sob o qual as ações relacionadas à defesa cibernética são enquadradas, estabelece a infraestrutura crítica a ser protegida e estipula os órgãos de ciberdefesa do exército. Além disso, relaciona a defesa cibernética com as funções primárias, enquadra a defesa cibernética no processo de planejamento militar e estabelece as tarefas a serem realizadas pela instituição em matéria de defesa cibernética.

Esse manual assegura a realização de operações cibernéticas ofensivas, contra pessoas, redes de computadores e sistemas C4I [1] adversário. Segundo Plum (2020), a previsão doutrinária de ataque cibernético outorga liberdade de ação à força, impactando positivamente na sua capacidade. Soma-se a isso, o emprego sistêmico previsto na doutrina em voga, que vislumbra tarefas para a capacidade cibernética em todas as operações – relacionando-as com as demais funções de combate e enquadrando-as dentro do contexto das operações de informação.

Observa-se que a doutrina abrange o nível mais alto da instituição, contudo existe uma lacuna para as ações táticas da Força Terrestre, com manuais e regulamentos voltados para as ações defensivas, que

abrange os usuários e sistemas empregados pela força e, também, ações ofensivas, para normatizar e orientar tais ações, visando o público alvo especializado.

ORGANIZAÇÃO E/OU PROCESSOS

Esse fator é materializado por intermédio da estrutura organizacional dos elementos de emprego da Força Terrestre (F Ter). Algumas capacidades são obtidas por processos, com vistas a evitar competências redundantes, quando essas já tenham sido contempladas em outras estruturas (Brasil, 2019).

Como mencionado, a Brigada de Inteligência é o órgão executivo do setor cibernético. Essa Grande Unidade de Inteligência possui dois regimentos de inteligência, sendo que o Regimento de Inteligência Nº 2 "Llaitún" reúne as capacidades cibernética e guerra eletrônica, materializadas pelo Batalhão de Defesa Cibernética (Figura 3) e o Batalhão de Guerra Eletrônica.

missão executar operações militares no ciberespaço, com o propósito de garantir o livre uso do domínio cibernético de interesse militar e manter a proteção das infraestruturas críticas institucionais, bem como obter informações relevantes para o sistema de inteligência do exército.

A Companhia de Operações Cibernéticas Defensivas cumpre um rol duplo de atribuições, pois além de ser uma estrutura voltada para a guerra, também desempenha o papel de centro de tratamento de incidentes de rede ou CSIRT - Computer Security Incident Response Team (CSIRT, na sigla em inglês), sendo uma estrutura permanentemente ativada.

O setor cibernético, no Exército do Chile, a nível de direção, está organizado com uma estrutura não vocacionada especificamente para atividade no domínio cibernético. Porém, no nível tático, o Batalhão de Defesa Cibernética se destaca de maneira positiva.

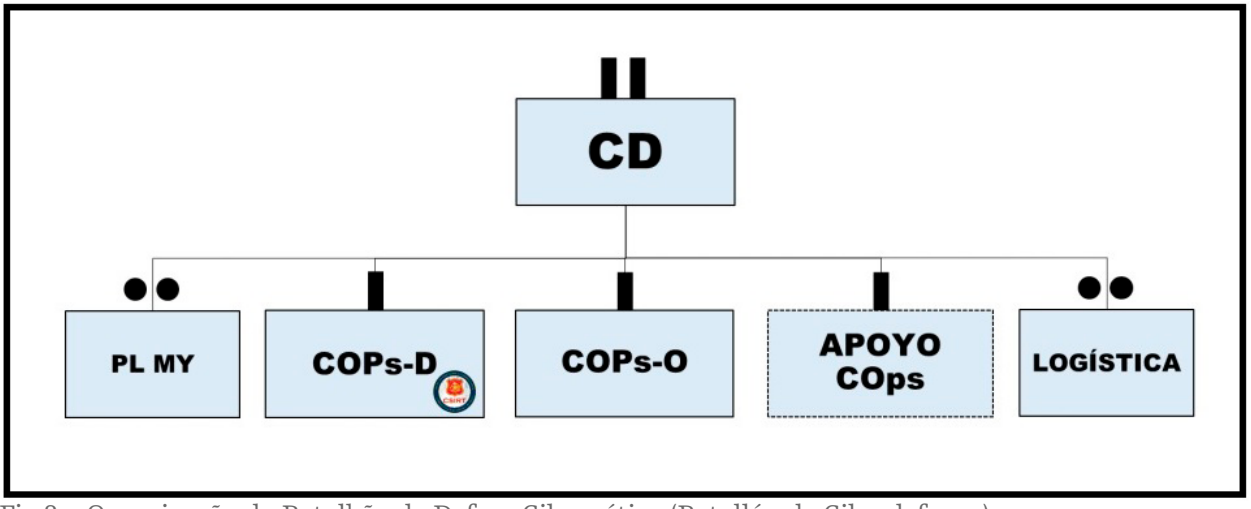

Fig 3 – Organização do Batalhão de Defesa Cibernética (Batallón de Ciberdefensa).
Fonte: Batalhão de Defesa Cibernética – palestra institucional.

O Batalhão de Defesa Cibernética está organizado a uma companhia de operações cibernéticas defensiva (COPs-D), uma companhia de operações cibernéticas ofensiva (COPs-O), uma companhia de apoio às operações cibernéticas (Apoyo COps), uma seção de estado-maior e uma seção logística. Essa OM Ciber tem como

ADESTRAMENTO

Compreende as atividades de preparo, obedecendo a programas e ciclos específicos, incluindo a utilização de simulação em todas as suas modalidades: virtual, construtiva e viva.

O adestramento das subunidades do Batalhão de Defesa Cibernética chileno

é realizado, principalmente, por meio da participação de suas subunidades em exercícios militares. O ciclo de adestramento é uma das áreas que se encontra em fase inicial de desenvolvimento, não se observando programas padrão de adestramento como em outras capacidades.

Além disso, a Companhia de Operações Cibernética Defensiva participa do Exercício de Simulação de Gestão de Segurança Cibernética para Funcionários Públicos, organizado pelo CSIRT governamental, realizado em parceria com a empresa de segurança cibernética Kaspersky e aberto aos funcionários do Estado e empresas membros do Sistema de Empresas Públicas (CHILE, 2022). Trata-se de uma simulação realista de um incidente de cibersegurança, guardando semelhanças com o Exercício Guardião Cibernético, realizado pelo Comando de Defesa Cibernética (ComDCiber), do Exército Brasileiro.

MATERIAL

A Doutrina Militar Terrestre (2019) preconiza que o fator material compreende todos os materiais e sistemas para uso na F Ter, acompanhando a evolução de tecnologias de emprego militar e com base na prospecção tecnológica. É expresso pelo quadro de distribuição de material dos elementos de emprego e inclui as necessidades decorrentes da permanência e sustentação das funcionalidades desses materiais e sistemas durante todo o seu ciclo de vida.

Segundo Miranda (2021), o Batalhão de Defesa Cibernética aumentou sua capacidade em termos do material implementado para realizar suas funções – hardware e principalmente softwares, porém, sua principal dificuldade é representada pela obsolescência tecnológica em parte da infraestrutura crítica a ser salvaguardada, definida pela instituição. Tudo isso porque existem diferentes organizações encarregadas dos dados de pessoal, planejamento de operações militares e administração dos recursos que, como resultado dessa obsolescência, não conseguiram migrar para plataformas mais modernas e seguras. E isso se traduz em uma maior exposição às ameaças cibernéticas.

Por outro lado, em relação aos recursos financeiros destinados à aquisição de materiais e outros investimentos e custeio do setor cibernético, existe um Plano de Desenvolvimento Estratégico do Exército que priorizou a capacidade cibernética, garantindo um fluxo contínuo de recursos.

EDUCAÇÃO

Compreende todas as atividades continuadas de capacitação e habilitação, formais e não formais, destinadas ao desenvolvimento do integrante da Força Terrestre quanto à sua competência individual requerida. Essa competência deve ser entendida como a capacidade de mobilizar, ao mesmo tempo e de maneira interrelacionada, conhecimentos, habilidades, atitudes, valores e experiências para decidir e atuar em situações diversas.

No Exército do Chile, a vertente educação é de responsabilidade setorial do Comando de Educação e Doutrina (CEDOC), que tem, por um lado, a responsabilidade pela geração de doutrina por meio da Divisão de Doutrina (DIVDOC) e, por outro, é responsável pelo sistema de educação militar através da Divisão de Educação (DIVEDUC).

Contribuindo com o setor cibernético, a Academia Politécnica Militar (ACAPOMIL) ministra o Curso Técnico Avançado de Defesa Cibernética, fornecendo pessoal permanente com competências necessárias para atuar como administradores da rede de defesa cibernética, bem como no Batalhão de Defesa Cibernética. O curso é destinado a engenheiros militares, com conhecimentos avançados na área e constitui um nível superior de educação militar sobre o assunto.

O Exército do Chile estabeleceu uma linha de carreira para os cabos profissionais [2], na linha de ensino militar bélico, na área de defesa cibernética, que inclui cursos ministrados tanto pela Escola de Telecomunicações (ESCTEL) como pela Escola de Inteligência (ESCINT). A ESCTEL está vocacionada para as atividades de proteção cibernética, visando preservar os

ativos próprios do Exército do Chile. Assim, essa instituição de ensino possui um centro de treinamento em telecomunicações, que inclui em suas instalações o Centro de Treinamento CISCO e o Laboratório de ensino e treinamento de rede – onde são ministrados cursos de treinamento e especialização. Como exemplo, cita-se os cursos CISCO CCNA [3], que são orientados para a entrega de habilidades para desenvolver redes seguras, reconhecer ameaças e vulnerabilidades de rede e mitigá-las, mantendo a integridade, confidencialidade e disponibilidade de dados e serviços. Ao mesmo tempo, esse pessoal tem especialização secundária em guerra eletrônica e, uma vez que tenham recebido ambos os treinamentos, estão prontos para serem treinados pela Escola de Inteligência.

Após concluir os treinamentos específicos de cibernética e guerra eletrônica, os militares seguem para ESCINT, onde frequentam o curso básico de inteligência militar, que será uma especialização orientada para os conhecimentos preconcebidos na área de cibernética e guerra eletrônica. Dessa forma, o ciclo de educação está completo e os militares estão aptos para aplicar os conhecimentos adquiridos. Com o treinamento fornecido em ambas as escolas, a instituição recebe um cabo da arma de Telecomunicações, especialista em guerra eletrônica e inteligência, que desenvolveu as habilidades técnico-profissionais para trabalhar em redes e sistemas de defesa cibernética.

Infere-se que o Exército do Chile desenvolveu uma adequada solução para o aperfeiçoamento técnico-profissional das praças, gerando uma linha de carreira para os sargentos da instituição no campo da defesa cibernética. Porém, não há medidas similares com relação à especialização de oficiais.

PESSOAL

Abrange todas as atividades relacionadas aos integrantes da força, nas funcionalidades: plano de carreira, movimentação, dotação e preenchimento de cargos, serviço militar, higidez física, avaliação, valorização profissional e moral. É uma abordagem sistêmica voltada para a geração de capacidades, que considera todas as ações relacionadas com o planejamento, a organização, a direção, o controle e a coordenação das competências necessárias à dimensão humana da Força.

No âmbito do fator pessoal, o Exército do Chile conta com um plano de carreira para os cabos profissionais, como descrito no fator educação, que visa ao preenchimento de cargos no setor cibernético, principalmente na área de proteção cibernética. Da mesma forma, a ACAPOMIL desenvolve um programa com o Curso Técnico Avançado de Defesa Cibernética, que permite habilitar pessoal em um nível mais avançado para atividades no setor cibernético.

Contudo, no Exército do Chile não existe a previsão para uma carreira de oficiais dedicados ao domínio cibernético. Assim, o fluxo de pessoal na direção e controle, que é desempenhado pelos oficiais, não apresenta uma sistemática ou padronização.

INFRAESTRUTURA

Engloba todos os elementos estruturais (instalações físicas, equipamentos e serviços necessários) que dão suporte ao preparo e ao emprego dos elementos da F Ter, de acordo com a especificidade de cada um e o atendimento aos requisitos do exercício funcional.

Cabe ressaltar que a infraestrutura de proteção cibernética é mais ampla e transversal a todo exército. De modo contrário, a infraestrutura relacionada às ações ofensivas são mais específicas e restritas a unidades militares de cibernética.

A implementação da infraestrutura física relativa ao setor cibernético tem sido gradual, de acordo com o Plano de Desenvolvimento Estratégico já mencionado. Tudo isso, refletiu-se em um aumento considerável no número de instalações do Batalhão de Defesa Cibernética, desde sua criação. Miranda

(2021) afirma que a infraestrutura é um dos pontos fortes da unidade, devido ao fato de que a instituição tem feito um esforço significativo para melhorar as condições da unidade, materializados pela construção dos pavilhões das companhias de operações cibernéticas.

CONSIDERAÇÕES FINAIS

Em síntese, ao término da análise dos fatores DOAMEPI, é possível consolidar os principais fatores positivos e negativos, evidenciados no presente artigo, relativos à capacidade cibernética no Exército do Chile, sintetizada por uma matriz SWOT [4].

Exército do Chile adotou, subordinando o setor cibernético ao sistema de inteligência. A implantação de uma área estratégica sob a direção da DIPLINE e execução do COPE é sublinhada com ressalvas, pois a especificidade do setor cibernético certamente exigirá uma estrutura com maior vocação para essa atividade. Soma-se a isso a falta de um curso de especialização para oficiais no aspecto educação e pessoal.

Sob a óptica dos fatores externos, ressalta-se como fator positivo o marco legal, representado pela Política Nacional de Defesa Cibernética e o conteúdo do Plano de Desenvolvimento do Exército, que estão impulsionando a capacidade

	FATORES POSITIVOS	FATORES NEGATIVOS
Fatores Internos	**STRENGTHS (Fortalezas)** - Cursos de especialização para sargentos; e - Recursos de forma sistêmica: materializados na infraestrutura em ampliação e material.	**WEAKNESSES (Debilidades)** - Organização: não conta com um órgão de direção ou gestão dedicado à cibernética; e - Falta de um plano de carreira para os oficiais.
Fatores Externos	**OPORTUNITIES (Oportunidades)** - Marco legal sólido.	**THREATS (Ameaças)** - Falta de capacidade conjunta.

Tabela 1 – Principais fatores relativos à capacidade cibernética no Exército do Chile.

Considerando os fatores internos, há força no fator educação, representada pela sólida formação das praças, que passam pelo curso de guerra eletrônica, cibernética e inteligência. Deduz-se que a educação tem uma forte relevância ao fornecer profissionais qualificados para o desempenho de tarefas no setor cibernético. Além disso, os aspectos de infraestrutura e material demonstram fortalezas, principalmente pelo fluxo contínuo de recursos financeiros para essas áreas.

Por outro lado, como debilidade, destaca-se a peculiar estrutura que o

cibernética. Como ameaça, elenca-se a falta de capacidade no nível conjunto.

Por fim, conclui-se que a capacidade cibernética no Exército do Chile está em fase de implantação, sendo sua maturação compatível com a realidade regional. Além disso, o Exército Brasileiro tem demonstrado interesse em contribuir com o setor cibernético do Chile, uma vez que as Conferências Bilaterais entre Estados-Maiores (CBEM) de 2020 e 2022, realizado entre ambos os exércitos, expressaram vários entendimentos no setor – fato esse que contribuirá para o aumento da segurança cibernética no cone sul.

REFERÊNCIAS

BRASIL. Ministério da Defesa. Exército Brasileiro. **Doutrina Militar Terrestre.** 2ª. ed. Brasília, 2019.
BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. Brasília, 2014.
CARNEIRO, João M. E. **A Guerra Cibernética**: **uma proposta de elementos para formulação doutrinária do Exército Brasileiro**. 2012. 204 f. Tese (Doutorado em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.
CHILE. *Política de Ciberdefensa.* Santiago, Región Metropolitana, Chile: Diario Oficial de la República de Chile, 8 de Marzo de 2018.
CHILE. Exército do Chile. **Regulamento RDI 20008 - Defesa Cibernética**. Santiago, Región Metropolitana, Chile: División Doctrina. 2016.
CHILE. Ministério da Defesa Nacional. **Doctrina de Ciberdefensa Conjunta DNC 2-11**. Santiago, Región Metropolitana, Chile: Estado Mayor Conjunto. 2018.
CHILE. Ministério da Defesa Nacional. **Decreto 305 – Extingue a Direção de Inteligência e cria a Direção de Planejamento de Informações do Exército**. Santiago, Chile: MINDEF 2021.
CHILE. Ministério do Interior e Segurança Pública. **Política de Segurança Cibernética**. Santiago, 2020.
CHILE. MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA DE CHILE**. Segundo exercício de simulação em gestão da segurança cibernética.** Disponível em: https://www.ciberseguridad.gob.cl/noticias/segundo-ejercicio-de-simulacion-en-gestion-de-ciberseguridad-para-funcionarios-publicos-reune-mas-de-380-participantes/. Acessado em: 10 de set. 22.
CORREA FILHO, Ivan de Souza. **A segurança cibernética no Brasil – uma análise da situação atual.** Trabalho de Conclusão de Curso. Escola Superior de Guerra. Brasília, 2016.
MIRANDA, Cristian Aguilera. **Estrategia de Ciberdefensa Institucional.** Memória para obtenção do título de Oficial de Estado-Maior. Academia de Guerra do Exército do Chile. Santiago, 2021.
ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE. **NATO Cyber Defence**. Bruxelas: *Public Diplomacy Division*. 2019.
PLUM, Thiago Itamar. **Proposta de metodologia para avaliação da capacidade cibernética de Estados-Nação**. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2020.
VALENZUELA, Gonzalo Burgos. *La Política Nacional y su relación con el ciberespacio***.** Memória para obtenção do título de Oficial de Estado-Maior. Academia de Guerra do Exército do Chile. Santiago, 2021.

NOTAS

[1] Sistemas C4I: Sistemas de Comando, Controle, Comunicações, Computadores e Inteligência.
[2] Cabos profissionais: início da carreira das praças - equivalente ao 3º Sargento no Exército brasileiro
[3] A certificação **CCNA** (**Cisco Certified Network Associate**) é uma prova da **CISCO** SYSTEMS, uma companhia sediada em San Jose, na Califórnia, cuja principal atividade é oferecer soluções para redes e comunicações, fabricando roteadores e switches, além da prestação de serviços de manutenção através de empresas parceiras.
[4] O termo SWOT é um acrônimo para *Strengths, Weaknesses, Opportunities and Threats* (Forças, Fraquezas, Oportunidades e Ameaças). A análise SWOT é uma ferramenta de diagnóstico estratégico para empresas, governos ou entidades em um determinado ambiente. A técnica é atribuída a Albert Humphrey, que foi um líder de pesquisa na Universidade de Stanford nos anos 60 e 70.

SOBRE O AUTOR

O Tenente-Coronel de Comunicações Lúcio Jerônimo é instrutor da Academia de Guerra do Exército do Chile e Oficial de Ligação de Doutrina junto à Divisão de Doutrina do Exército do Chile. Foi declarado Aspirante a Oficial pela Academia Militar das Agulhas Negras (AMAN) em 2002. É mestre em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO/2010). Concluiu o curso de Comando e Estado-Maior (ECEME) em 2019. Comandou a 20ª Companhia de Comunicações Páraquedista, no Rio de Janeiro, no biênio 2016-2017. Desempenhou a função de instrutor do Centro de Instrução de Guerra Eletrônica (CIGE). Possui especialização em Análise do Ambiente Eletromagnético pelo Instituto Tecnológico de Aeronáutica (ITA). Realizou os seguintes cursos: Básico de Guerra Eletrônica, Intermediário de Guerra Eletrônica, Doutrinário de Guerra Eletrônica (FAB), Expedito de Guerra Eletrônica (MB), Básico de Paraquedista, Mestre de Salto, Operações na Selva Cat "B", Avançado de Comunicações (EUA) e Regular de Estado-Maior (Chile) (jeronimo.lucio@eb.mil.br).