ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

Maj Com **WAGNER** DE MATOS SALUSTRIANO

Capacitação de Cadetes da Academia Militar das Agulhas Negras (AMAN) em Cibernética: a descoberta de novos talentos para o setor

Rio de Janeiro

2020

S181c Salustriano, Wagner de Matos

Capacitação de Cadetes da Academia Militar das Agulhas Negras (AMAN) em Cibernética: a descoberta de novos talentos para o setor. / Wagner de Matos Salustriano. —2020.
63 f. : il. ; 30 cm.

Orientação: Valdecir Gregory.

Trabalho de Conclusão de Curso (Especialização em Ciências Militares) — Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2020.

Bibliografia: f. 61-63.

1. CAPACITAÇÃO 2. AMAN 3. CIBERNÉTICA. 4. NOVOS TALENTOS I. Título.

CDD 355.5

Maj Com **WAGNER** DE MATOS SALUSTRIANO

Capacitação de Cadetes da Academia Militar das Agulhas Negras (AMAN) em Cibernética: a descoberta de novos talentos para o setor

Trabalho de Conclusão de Curso apresentado Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Orientador: TC Com Valdecir Gregory

Rio de Janeiro

2020

Maj Com **WAGNER** DE MATOS SALUSTRIANO

Capacitação de Cadetes da Academia Militar das Agulhas Negras (AMAN) em Cibernética: a descoberta de novos talentos para o setor

Trabalho de Conclusão de Curso apresentado Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Aprovado em ___ outubro de 2020

COMISSÃO AVALIADORA

_____

VALDECIR **GREGORY** – TC Com QEMA – Me. - Presidente
Escola de Comando e Estado-Maior do Exército

_____

ENIO CORRÊA DE SOUZA **–** TC Com QEMA – Membro
Escola de Comando e Estado-Maior do Exército

_____

CLEBER HENRIQUE BERNARDES SIMÕES – Maj Cav QEMA – Membro
Escola de Comando e Estado-Maior do Exército

“Tenho observado, hoje, nas empresas, que elas olham muito pra fora em busca de novos talentos e esquecem que, na maioria das vezes, o talento está dentro da própria empresa não sendo utilizado, geralmente”
(Guilherme Machado)

AGRADECIMENTOS

A Deus, por permitir nossa existência e a quem primeiro nos apegamos nos momentos de dificuldades.

A minha esposa Aline e meu filho Arthur, pelo apoio, incentivo e compreensão nos momentos de ausência.

Aos meus pais, pelo esforço em proporcionar a melhor educação aos seus filhos, pelo exemplo, carinho e apoio em todos os projetos da minha vida.

Aos amigos, pelo apoio na realização deste trabalho.

Ao meu orientador, TC Gregory, pelas sábias sugestões na condução deste trabalho, pelo incentivo e tranquilidade com que conduziu as diversas fases deste trabalho.

Ao TC Joselito, Comandante do Curso de Comunicações da Academia Militar das Agulhas Negras, no fornecimento das informações e materiais do ensino de cibernética na AMAN, fundamentais neste trabalho.

Ao Cel Paulo Sérgio, Comandante da Escola Nacional de Defesa Cibernética, que contribuiu com relatórios e documentações doutrinárias relativas à capacitação de recursos humanos para o setor cibernético.

RESUMO

Em um mundo altamente conectado, onde os meios de Tecnologia da Informação (TI) estão presentes no dia a dia das pessoas, das instituições e das empresas, verifica-se que junto com a solução de diversos problemas como a diminuição das distâncias e a conectividade, tais meios também trouxeram novos problemas e desafios. Neste contexto, as atividades militares tiveram que adaptar-se ao novo ambiente operacional caracterizado pela incerteza, pela informatização e pela rapidez no fluxo de informações onde não se sabe quem é o inimigo e sua capacidade em comprometer estruturas estratégicas, governos e a vida das pessoas. Dessa forma, o conhecimento do termo cibernética anteriormente empregado de forma mais restrita, tem se tornado comum tanto no ambiente militar quanto no civil. No meio militar, os conflitos bélicos das últimas décadas têm mostrado a necessidade de sistemas de comando e controle que permitam uma maior consciência situacional a fim de facilitar o processo decisório, entretanto que sejam confiáveis e seguros. Ainda, cabe destacar que a cibernética é uma área sensível e de uma grande exigência técnica onde seus operadores precisam do máximo de dedicação, empenho e pendor para esta atividade, sendo fundamental a constante capacitação. Assim, a descoberta de novos talentos torna-se vital, imprescindível e deve ser buscada o mais cedo possível a fim de aproveitar esta competência o maior tempo possível e desenvolvê-la.

Palavras-chave: TI, incerteza, cibernética, exigência técnica, capacitação, novos talentos

ABSTRACT

In a highly connected world, where the Information Technology (IT) tools are present in daily lives of people, institutions and companies, it seems that along with the solution of several problems such as the reduction of distances and connectivity, these means also brought new problems and challenges. Therefore, military activities had to adapt to a new operational environment characterized by uncertainty, computerization and the rapid flow of information where the enemy is unknown as well as his ability to compromise strategic structures, governments and people's lives. Thus, knowledge of the term cybernetics previously used in a more restricted way, has become common in both the military and civilian environments. From the military perspective, the conflicts of the last decades have shown the need for reliable and safe command and control systems that allow a greater situational awareness in order to facilitate the decision-making process. Still, it´s worth noting that cybernetics is a sensitive area that requires constant training and great technical expertise in which the operators need the maximum dedication, commitment and compromise. Therefore, the discovery of new talents becomes vital, essential and must be pursued as soon as possible in order to take advantage of this competence in a long term and to develop new capabilities.

Key-words: IT, uncertainty, cybernetics, technical requirements, training, new talents

LISTA DE ILUSTRAÇÕES

FIGURAS

TABELAS

GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

Segundo a Escola Superior de Guerra (ESG), os Objetivos Nacionais Permanentes, ou Objetivos Fundamentais (OF) de uma nação são aqueles “identificados mediante exame dos valores, aspirações e interesses nacionais, possuem ânimo de permanência, isto é, embora não sejam eternos, são assim considerados. (ESG, 2010).

No caso do Brasil, esses OF estão insculpidos na Constituição Federal de 1988, no Título I - Dos Princípios Fundamentais - sendo: a Democracia, a Integração Nacional, a Integridade do Patrimônio Nacional, a Paz Social, o Progresso e a Soberania. Devido ao tamanho do seu território, população, economia e outros fatores o país é considerado uma potência regional no âmbito da América do Sul.

Nesse contexto, a fim de garantir seus interesses e sua soberania, deve possuir Forças Armadas bem estruturadas, equipadas com modernos equipamentos e com militares capacitados para que possam estar em condições de cumprir seu papel constitucional previsto no Art 142 da Constituição Federal, conforme descrito abaixo:

> Art. 142. As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem.

Nesse contexto, a criação do Ministério da Defesa (MD), no ano de 1999, foi fundamental para que o assunto Defesa pudesse ser discutido de forma ampla perante a população brasileira e não só no âmbito dos militares como era de praxe. Diante de incertezas em relação aos cenários futuros, faz-se necessário a expansão deste assunto, por entender que a Defesa não é algo pertencente somente à Expressão Militar e sim depende de uma Estratégia Nacional que permeie todas as Expressões do Poder Nacional (Político, Econômico, Psicossocial, Militar e Científico-Tecnológico).

Assim, a sociedade brasileira como um todo deve tratar com uma maior frequência e importância o tema Defesa como forma de atingir seus Objetivos Nacionais e afirmar sua incondicional soberania sobre seu território, em função da existência de grandes reservas minerais, da maior biodiversidade e reserva de água doce do planeta, além de diversas outras riquezas que atiçam a cobiça de outros atores internacionais.

Em um mundo atualmente conectado, cabe destacar que tem-se observado o aumento dos meios de Tecnologia da Informação que estão presentes no dia a dia das pessoas, onde pode até não haver um consenso na sua utilização, mas ao analisar a conjuntura atual verifica-se o quanto as pessoas são dependentes e necessitam dos meios tecnológicos em suas vidas. Neste ponto, as atividades cibernéticas no comprometimento de estruturas, meios e na condução dos países são cada vez mais frequentes.

Desta forma, a Estratégia Nacional de Defesa, lançada em 2008 e revisada em 2012, instituiu como estratégicos para a Defesa Nacional os setores espacial, nuclear e cibernético, ficando sob incumbência do Exército Brasileiro o desenvolvimento do setor cibernético. Assim, em 2012, ocorreu a publicação da Política Cibernética de Defesa com o intuito de orientar, no âmbito do Ministério da Defesa (MD), as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos.

Além disso, outras providências foram tomadas, como a criação do Centro de Defesa Cibernética (CDCiber), em 2010, com a finalidade de implantar o setor cibernético no âmbito do Exército Brasileiro e na defesa do país e em 2015, o Comando de Defesa Cibernética (ComDCiber), com o objetivo de planejar, orientar, coordenar, integrar e executar atividades relacionadas ao desenvolvimento e aplicação das capacidades cibernéticas, agindo como órgão central do Sistema Militar de Defesa Cibernética. Com a criação do ComDCiber, o CDCiber passou a estar subordinado ao mesmo, marcando o estabelecimento de estruturas voltadas aos níveis operacional e tático, mas que podem gerar reflexos no nível estratégico.

Com isso, diversos desafios foram impostos ao Exército Brasileiro na gestão de seus Recursos Humanos voltados para a área cibernética podendo afirmar que a capacitação é um dos maiores desafios.

De acordo com Ferreira (2017) capacitação é um processo contínuo, permanente e deliberado de aprendizagem, com o propósito de contribuir para a construção de competências organizacionais, por meio do desenvolvimento de competências individuais e coletivas. Consequentemente, além de buscar fornecer as aptidões necessárias ao desempenho funcional, visa valorizar e motivar o profissional.

Desta maneira, com o intuito de capacitar recursos humanos das Forças Armadas, foi criado o curso de Guerra Cibernética no Centro de Instrução de Guerra Eletrônica (CIGE), em 2012. Em 2019, além da criação da Escola Nacional de Defesa Cibernética (ENaDCiber), foi inserida a disciplina cibernética nos principais estabelecimentos de ensino do Exército, como é o caso da Academia Militar das Agulhas Negras (AMAN), dentre outras ações.

1.1 PROBLEMA

Diante do que foi apresentado, a participação do vetor cibernético é uma realidade cada vez mais presente no âmbito nacional e com tendência cada vez maior de utilização em Operações Militares.

Assim, a capacitação de pessoal em cibernética ganha destaque, uma vez que os meios tecnológicos evoluem com extrema rapidez, exigindo que esta capacitação seja contínua e dinâmica, o que implica numa constante seleção de recursos humanos com perfil adequado para o setor. Desta forma, este trabalho irá procurar se debruçar sobre os seguintes problemas:

Como contribuir com a capacitação de recursos humanos para o setor cibernético através da descoberta de novos talentos na AMAN?

1.2 OBJETIVOS

1.2.1 Objetivo geral

Estudar como ocorre a capacitação dos cadetes da AMAN em cibernética com destaque para a descoberta de novos talentos.

1.2.2 Objetivos específicos

a. Apresentar de forma sucinta a implantação do setor cibernético no Exército Brasileiro.

b. Apresentar as considerações gerais sobre a capacitação de militares, as áreas de atuação e as trilhas do conhecimento no contexto cibernético.

c. Estudar a disciplina cibernética na AMAN.

d. Identificar como é o ensino de cibernética na Academia Militar do Exército Americano (*West Point*).

e. Propor sugestões para a identificação e seleção de talentos em cibernética no Curso de Formação da AMAN.

1.3 DELIMITAÇÃO DO ESTUDO

O presente estudo estará limitado apenas na capacitação em cibernética na AMAN. O Estudo também tem como meta propor medidas para a descoberta e condução de talentos neste setor.

1.4 RELEVÂNCIA DO ESTUDO

O avanço tecnológico vivido pela sociedade nos últimos anos, particularmente nos meios de Tecnologia da Informação e Comunicações (TIC), transformou o cotidiano das pessoas, empresas, governos e nações. No Brasil essa realidade também não é diferente e as Forças Armadas e em particular o Exército como instituição de Estado têm acompanhado esta evolução, onde como todo processo evolutivo vem carregado de desafios.

Neste ambiente atual caracterizado pela incerteza, pela informatização e pela rapidez no fluxo de informações, cresce de importância a preocupação com as atividades cibernéticas. Nesse sentido, é de fundamental importância que os quadros estejam constantemente capacitados, que se mantenham na atividade e trabalhem na área o maior tempo possível, tendo vista a complexidade deste setor, o dinamismo de suas ações e as consequências que acarretam.

Ainda cabe destacar que pelas características já descritas, a cibernética é uma área sensível e de uma grande exigência técnica que exige de seus operadores o

máximo de dedicação, empenho e pendor para esta atividade. Assim, a descoberta de novos talentos torna-se vital, imprescindível e deve ser buscada o mais cedo possível a fim de aproveitar esta competência o maior tempo possível e desenvolvê-la.

Neste sentido, a AMAN como instituição de ensino superior responsável pela formação dos oficiais da linha bélica combatente de carreira do Exército Brasileiro, é a que possui o primeiro contato com o jovem que se tornará oficial. E por ser um Curso de quatro anos é a que possui as melhores condições na possível descoberta de militares para o setor cibernético.

Desse modo, a relevância do trabalho fica evidenciada diante de tudo o que foi apresentado, constituindo-se um objeto para melhor compreender como é a capacitação em cibernética na AMAN e se nesta capacitação ocorre descoberta de novos talentos.

2 METODOLOGIA

Nessa seção, é apresentada a metodologia que será utilizada para desenvolver o trabalho, evidenciando-se os seguintes tópicos: tipo de pesquisa, universo e amostra, coleta de dados, tratamento de dados e limitações do método.

2.1 TIPO DE PESQUISA

Tomando por base os conceitos teóricos apresentados no Manual de Elaboração de Projetos de Pesquisa da Escola de Comando e Estado Maior do Exército (ECEME), a metodologia que será empregada na confecção do trabalho científico será conforme o descrito a seguir. Seguindo a taxionomia de Vergara (2009), essa pesquisa será qualitativa, explicativa, bibliográfica e documental. Qualitativa, pois privilegiará análises de documentos, relatos, entrevistas e questionários para entender os benefícios por meio da atuação de militares de uma forma mais profunda. Explicativa porque o autor buscará tornar o assunto o menos complexo possível. Bibliográfica porque terá sua fundamentação teórico-metodológica na investigação dos assuntos abordados e na criação do conhecimento disponíveis em livros, manuais, artigos e redes eletrônicas de acesso livre ao público em geral. Documental porque se utilizará de documentos de trabalhos, relatórios, ofícios e memorandos não disponíveis para consultas públicas.

2.2 UNIVERSO E AMOSTRA

O universo do presente estudo são os cadetes da Academia Militar das Agulhas Negras. As amostras que serão utilizadas são os Cadetes do terceiro e quarto ano do Curso de Comunicações da AMAN por possuírem uma maior experiência no ensino de cibernética na AMAN.

2.3 COLETA DE DADOS

A coleta de dados do presente trabalho de conclusão de curso dar-se-á por meio da coleta na literatura, pesquisa documental e questionários podendo incluir

entrevistas, se for possível. Nessa oportunidade, serão levantadas as fundamentações teóricas para a comprovação ou não da hipótese levantada.

Essa pesquisa iniciar-se-á com uma pesquisa bibliográfica na literatura (livros, manuais, revistas especializadas, jornais, artigos, anais de congressos, internet, teses e dissertações) com dados pertinentes ao assunto. Nessa oportunidade, serão levantados assuntos sobre a capacitação no setor cibernético.

Em prosseguimento, utilizar-se-á a pesquisa documental no material de ensino da AMAN (Plano de Disciplina, Currículo e outros) com a finalidade de verificar o que está sendo ministrado em relação a cibernética.

Finalmente, será realizado um questionário com os cadetes do curso de comunicações da AMAN para verificar como ocorre as instruções de cibernética, a descoberta de novos talentos e se for o caso as oportunidades de melhoria, assim consolidando os dados do trabalho.

2.4 TRATAMENTO DOS DADOS

O método de tratamento de dados que será utilizado no presente estudo será a análise de conteúdo e a Delphi no qual serão realizados estudo de textos e documentos, analisando os significados da mensagem e procurando obter o consenso de opiniões dos cadetes que estão cursando o curso sobre o que está se investigando por intermédio do questionário aplicado.

2.5 LIMITAÇÕES DO MÉTODO

A metodologia em questão possui limitações, particularmente, quanto à profundida do estudo a ser realizado, pois não contempla, dentre outros aspectos, o estudo de campo e a entrevista com mais pessoas diretamente ligadas aos processos em estudo. Porém, devido ao fato de se tratar de um trabalho de término de curso, a ser realizado em pouco tempo, os métodos escolhidos estão adequados e possibilitará o alcance dos objetivos propostos.

3 O SETOR CIBERNÉTICO NO EXÉRCITO BRASILEIRO

Esta seção promove um debate sobre os principais termos que servem de base conceitual para a consecução da presente pesquisa, apresentando: conceitos básicos da cibernética, a implantação do setor cibernético no Exército Brasileiro e a capacitação de militares para o setor cibernético.

3.1 CONCEITOS BÁSICOS

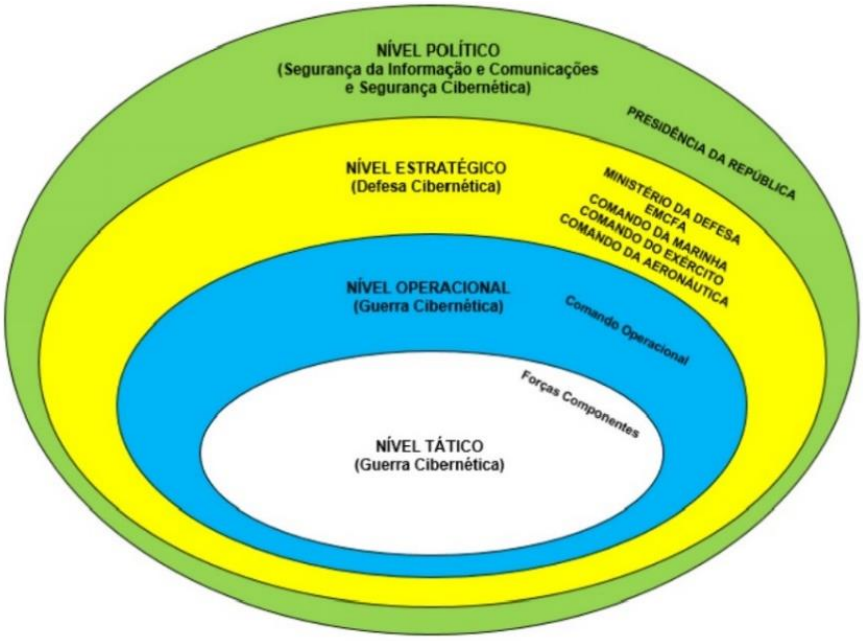
De acordo com o Manual de Guerra Cibernética (2019), Defesa Cibernética é um conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa (MD), com as finalidades de proteger os sistemas de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponente

Depois dessa definição, ressalta-se que as ações no espaço cibernético são denominadas, de acordo com o nível de decisão, conforme apresentado na figura 1 abaixo, onde no nível Político as ações são intituladas como Segurança da Informação e Comunicações (SIC) e Segurança Cibernética, sendo coordenadas pela Presidência da República e abrangendo a Administração Pública Federal (APF), bem como as infraestruturas críticas nacionais.

Já no nível Estratégico, recebem a denominação de Defesa Cibernética, definida anteriormente e a cargo do MD, Estado-Maior Conjunto das Forças Armadas (EMCFA) e comandos das Forças Armadas (FA), mas sempre interagindo com a Presidência da República e a APF.

Finalmente, nos níveis Operacional e Tático, que são os níveis mais afetos às FA, estas ações são chamadas de Guerra Cibernética, denominação essa restrita ao âmbito interno dessas Forças. Assim, de acordo com o Manual de Guerra Cibernética, essa denominação corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de Comando e Controle ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar.

Figura 1: Níveis de decisão e as ações cibernéticas correspondentes



Fonte: EB70-MC-10.232 Manual de Guerra Cibernética

Dentro do Exército Brasileiro foi instituído o Sistema de Guerra Cibernética do Exército (SGCEx) que visa à proteção cibernética do Sistema de Comando e Controle do Exército, assegurando a capacidade de atuar em rede com segurança, bem como a coordenar e a integrar a proteção das infraestruturas críticas da informação sob responsabilidade do Exército.

Assim, outro conceito que deve ser explorado é o de Capacidades Operativas (CO) do SGCEx, no qual a definição está conectada às aptidões que uma Força deve possuir a fim de cumprir uma missão. Desta forma, segundo previsto no manual de Guerra Cibernética, as CO estão divididas em três, a saber: Proteção Cibernética, Ataque Cibernético e Exploração Cibernética conforme a tabela 1 abaixo:

Tabela 1: Capacidades Operativas do SGCEx

CAPACIDADE OPERATIVA	**DESCRIÇÃO**
Proteção Cibernética	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.

Defesa Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

Fonte: EB70-MC-10.232 Manual de Guerra Cibernética

Ainda, é necessário entender o “quem faz o que” de acordo com essas CO em uma situação de conflito no âmbito de uma Força Terrestre Componente (FTC). Para tal, a tabela 2, a seguir, relaciona as estruturas ou Organizações Militares (OM) com as suas CO e suas responsabilidades.

Tabela 2: Estruturas operativas de Guerra Cibernética, suas CO e responsabilidades

Estrutura	**Atq**	**Expl**	**Prot**	**Responsabilidades**
Batalhão de Guerra Eletrônica (BGE)	X	X	X	Realiza a exploração e o ataque cibernéticos em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. O Cmt do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética e de ataque cibernético em prol da FTC.
Batalhão de Comunicações (BCom)	-	-	X	Realiza a proteção cibernética dos sistemas de informação do grande comando apoiado. O Cmt do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética da FTC.
Batalhão de Comunicações e Guerra Eletrônica (BCom GE)	-	X	X	Realiza a proteção cibernética dos sistemas de informação da FTC apoiada, bem como a exploração cibernética (com limitações) em proveito deste escalão. O Cmt do batalhão é responsável pelo planejamento e assessoramento relacionado às ações de proteção cibernética e de exploração cibernética da FTC, quando o BGE não estiver presente.
Batalhão de Inteligência Militar (BIM)	-	X	X	Realiza a exploração cibernética em proveito da FTC apoiada. Conduz ações de proteção cibernética dos sistemas de informação da própria unidade. Seu Cmt será responsável pelo planejamento e assessoramento relacionado às ações de exploração cibernética de interesse para as operações de inteligência conduzidas em proveito da manobra da FTC e para a produção do conhecimento de inteligência.
Companhia de Comando e Controle (Cia C2)	-	-	X	Realiza a proteção cibernética dos postos de comando da Força Terrestre Componente

Companhia de Comunicações (Cia Com)	-	-	X	Realiza a proteção cibernética dos sistemas de informação de uma grande unidade.
OM integrantes da FTC	-	-	X	Realizam a proteção cibernética (somente preventiva) dos sistemas de informação da OM

Fonte: EB70-MC-10.232 Manual de Guerra Cibernética

Estes conceitos foram apresentados com o intuito de divulgar uma nomenclatura básica sobre o tema e difundir as estruturas da FTC com capacidade de realizar a Guerra Cibernética, tendo vista que estas Organizações Militares serão o destino dos futuros Oficiais formados na AMAN, em particular os de Comunicações. Dessa maneira, procurou-se dar o embasamento teórico para o entendimento do próximo capítulo desta seção.

3.2 A IMPLANTAÇÃO DO SETOR CIBERNÉTICO NO EXÉRCITO BRASILEIRO

A Estratégia Nacional de Defesa (END) definiu três setores estratégicos prioritários para a Defesa Nacional: o nuclear, o cibernético e o espacial. Onde coube ao Exército Brasileiro (EB) a condução do setor cibernético.

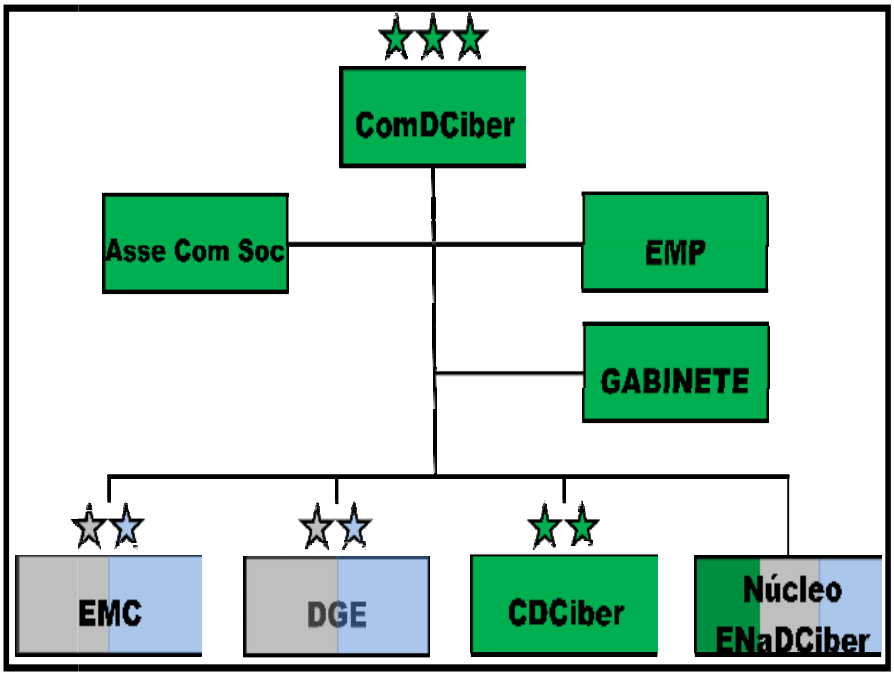
Dessa forma, no ano de 2009, o Comandante do Exército, em Portaria n° 03- Reservada, de 29 de junho de 2009, instituiu o setor cibernético no âmbito do (EB), determinando que o mesmo fosse implantado por meio de um projeto, no qual passou a ser denominado de Projeto Estratégico Defesa Cibernética (PEDCiber), tendo o Estado-Maior do Exército (EME) como órgão de coordenação e o Departamento de Ciência e Tecnologia (DCT) como elaborador da proposta relativa ao Setor. Já no ano de 2010, foi criado pelo Comandante do Exército, o Centro de Defesa Cibernética (CDCiber). E a contar de 2 de agosto daquele ano foi ativado seu núcleo (Nu CDCiber), ficando subordinado ao DCT.

Dois anos mais tarde foi publicado o Decreto Presidencial n° 7.809, a 20 de setembro de 2012, o qual entre outras medidas, incluía, na Estrutura Regimental do Comando do Exército, o Centro de Defesa Cibernética. Ainda neste ano, o Ministério da Defesa (MD), por intermédio da Portaria n° 3.405, de 21 de dezembro de 2012, atribuiu ao CDCiber a responsabilidade pela coordenação e pela integração das atividades de Defesa Cibernética, no âmbito do MD.

Depois disso, já em 2014, foi criado pelo MD o Programa da Defesa Cibernética na Defesa Nacional (PDCDN), que entre outras situações, determinava a criação do Comando de Defesa Cibernética (ComDCiber), onde deveria ser um Comando Operacional Conjunto, ou seja, com a participação de militares das três Forças Armadas, além da ordem para que fosse concebido a Escola Nacional de Defesa Cibernética (ENaDCiber) objetivando a capacitação de Recursos Humanos sejam eles civis ou militares. Além disso, em 18 de novembro de 2014, visando garantir maior consistência jurídica ao setor e nortear os planejamentos, foi publicada a Portaria Normativa n° 3.010, que aprovou a Doutrina Militar de Defesa Cibernética.

Destarte, outro marco importante foi a efetiva criação em 2015 do ComDCiber e ENaDCiber pelo Comandante do Exército, ativando seus Núcleos, a contar de 1° de janeiro daquele ano. Então, no ano de 2016, foi aprovada a Diretriz de implantação do Comando de Defesa Cibernética, na qual em abril de 2016 passou a possuir a seguinte estrutura organizacional (figura 2):

Figura 2: Organograma do Comando de Defesa Cibernética



Fonte: palestra institucional do ComDCiber

- Uma assessoria de Comunicações Social (Asse Com Soc);
- Estado-Maior Pessoal (EMP);

- Estado Maior Conjunto (EMC), onde a chefia é por revezamento entre um Contra-Almirante da Marinha do Brasil e um Brigadeiro da FAB;
- Departamento de Gestão e Ensino (DGE) nos mesmos moldes que o EMC;
- Centro de Defesa Cibernética (CDCiber), onde o chefe sempre será um General de Brigada do EB;
- Escola Nacional de Defesa Cibernética (ENaDCiber), onde a chefia é de um Coronel do EB.

Diante do exposto, percebe-se que o processo de implantação do setor cibernético está ocorrendo de maneira organizada, de forma sistêmica, porém sem perder a oportunidade. Em menos de dez anos, partiu-se de estruturas inexistentes, onde se contava apenas, de forma independente, com as próprias Organizações Militares de cada Força Armada, para uma estrutura integradora e de grande sinergia, com capacidade de atuar no espaço cibernético, a fim de assegurar os objetivos nacionais.

3.3 CAPACITAÇÃO DE MILITARES PARA O SETOR CIBERNÉTICO

Atualmente, observa-se o crescente interesse por pesquisas em relações internacionais sobre o ciberespaço, especialmente em seu aspecto securitário (PORTELA, 2016, p. 108). A afirmação anterior demonstra a evolução do setor cibernético, onde novas ferramentas e processos impactam a arte da guerra. Instrumentos, como as chamadas armas cibernéticas, proporcionam aquisição de informação necessária para o campo de batalha.

Assim, a informação tornou-se mais do que nunca um produto importante, afinal, com informação precisa, um comandante desdobra suas forças, lança seus contingentes contra os pontos vulneráveis do inimigo e muito provavelmente alcança a vitória. Para o tomador de decisão nos níveis mais elevados, a informação é igualmente vital, pois, com ela, planeja melhor os objetivos para alcançar os fins políticos. A informação, portanto, tem o potencial de mudar o comportamento dos atores, violentamente ou não. Eis aí a essência dos que defendem a guerra cibernética como novo domínio de operações militares.

Segundo Richard A. Clarke, em seu livro Guerra Cibernética “A percepção de que o ciberespaço é um "domínio" onde a luta ocorre e que os EUA devem "dominar", permeia o pensamento militar americano sobre o tema da guerra cibernética.” Neste contexto, alguns países e organizações passaram a considerar o ciberespaço como um domínio combatente, produzindo, assim, mudanças institucionais, estratégicas e doutrinárias. Como exemplo dessa inclinação de pensamento estratégico-militar, foi criado o U.S. Cyber Command (USCYBERCOM), em 2009.

Dessa maneira, observa-se uma clara tendência dos países no aperfeiçoamento de suas estruturas cibernéticas. Entretanto, é no ramo pessoal que estão os maiores desafios, pois são as pessoas que fazem a guerra cibernética ocorrer. Assim, ao tratar de capacitação de militares em cibernética este assunto desafia as instituições de ensino na área militar, por considerar tópicos e métodos diferentes do que tradicionalmente se utiliza na educação regular de ensino de defesa.

No Brasil, o Setor Cibernético no âmbito da Defesa abrange um grande número de áreas de atuação, destacando-se a capacitação de pessoal, a inteligência cibernética, a pesquisa científica, o arcabouço legal doutrinário, o preparo e o emprego operacional, a proteção de seus próprios ativos, a gestão de pessoal, a interação com os poderes Legislativo, Executivo e Judiciário e com instituições civis empresariais e acadêmicas.

Em relação a Capacitação, o Ministério da Defesa determina em sua Estratégia Setorial de Defesa (2020-2031), concebida em 2019, a Ação Setorial de Defesa 7.2.5 “Capacitar recursos humanos para atuar no setor cibernético”, ratificando a importância da capacitação dos recursos humanos como o centro de um processo destinado a permitir a atuação com liberdade de ação no espaço cibernético.

Nas diretrizes do Comandante do Exército (EXÉRCITO, 2019), quando abordada a premissa de Capacitação Técnica, descreve que os recursos humanos do EB devem ser capazes de enfrentar os desafios da Guerra Atual e do Futuro, para a qual muitas tecnologias ainda estão em processo de concepção, demandando do militar do século XXI alto grau de flexibilidade e capacidade de autoaperfeiçoamento. Para tal, em relação ao setor cibernético, tem-se a diretriz número trinta e dois que diz: “Ampliar a atuação do Exército Brasileiro no setor

cibernético, tanto no vetor de capacitação, quanto na integração com as demais Forças no âmbito do Ministério da Defesa", demonstrando a importância dada pelo comando da Força a capacitação de militares em cibernética.

Para tanto, a fim de cumprir estas determinações, o ComDCiber estabeleceu procedimentos para padronização da capacitação dos militares envolvidos no sistema cibernético, a fim de proporcionar o nivelamento e conhecimento adequados de acordo com as diversas áreas de atuação preparando para as funções e cargos inerentes ao emprego no setor cibernético para o cenário atual.

Para cada área de atuação, há uma trilha de cursos e treinamentos correspondentes e divididos em três categorias: a básica, a intermediária e a avançada. Na trilha básica serão realizados cursos EAD em instituições de ensino civis, contratadas por meio de processos licitatórios internos ou por meio de convênios, com custos ou sem custos para a Administração Militar.

Na trilha intermediária o foco está voltado para a realização de cursos presenciais nacionais e EAD internacionais; no tocante à trilha de conhecimento no nível avançado, os cursos de especialização podem ser de curta ou de longa duração, realizados no exterior. Cabe destacar que o militar capacitado deve replicar o conhecimento e assim diminuir custos futuros.

A seguir, serão apresentados os quadros das áreas de atuação e as respectivas divisões nas trilhas de conhecimento específicas da cibernética (atividade fim), havendo também para as atividades meio, que não serão abordadas nesse trabalho:

Tabela 3: Trilha da área de conhecimento defesa cibernética

ÁREA DE CONHECIMENTO DEFESA CIBERNÉTICA		
TRILHA BÁSICA	TRILHA INTERMEDIÁRIA	TRILHA AVANÇADA
Redes de computadores	Segurança de redes	Desenvolvimento de *exploits*
Programação	Segurança de aplicações *web*	Segurança avançada em aplicações *web*
Sistemas operacionais	Segurança de aplicações	Segurança avançada de redes
Banco de dados	Análise forense	Levantamento de informações
Criptografia	Teste de invasão	Engenharia reversa de código malicioso
-	Redes computadores	Segurança de redes
-	Programação	Segurança de aplicações web

-	Sistemas operacionais	Segurança de aplicações
-	Banco de dados	Análise forense
-	Criptografia	Teste de invasão
-	Segurança de redes sem fio	Mineração de dados
-	Gerenciamento sistemas Linux	*Big Data*
-	Gerenciamento sistemas Windows	-
-	Desenvolvimento seguro	-
-	*Business Intelligence*	-

Fonte: Plano de Capacitação Cibernética 2016-2017, do ComDCiber.

Tabela 4: Trilha da área de conhecimento Gestão Cibernética

ÁREA DE CONHECIMENTO GESTÃO CIBERNÉTICA		
TRILHA BÁSICA	TRILHA INTERMEDIÁRIA	TRILHA AVANÇADA
Planejamento e gestão estratégica de TI	Gestão da Segurança da Informação NBR 27001 e NBR 27002	Curso de cibernética nos EUA
Fundamentos de governança de TI	Gestão de riscos de TI - NBR 31000 e NBR 27005	Curso de cibernética na Alemanha
Fundamentos do COBIT 5	-	Pós-graduação em gestão
Políticas de Segurança da Informação	-	Mestrado em Defesa Cibernética na Espanha
Treinamento para Certificação CISSP	-	-
Estágio de adaptação cibernética	-	-

Fonte: Plano de Capacitação Cibernética 2016-2017, do ComDCiber

Além disso, o Centro de Instrução de Guerra Eletrônica (CIGE) recebeu a missão, em 2012, de habilitar militares, oficiais e sargentos das Forças Armadas, para ocupar cargos e desempenhar funções de segurança, defesa e guerra cibernética, sendo criado assim o Curso de Guerra Cibernética. Anos mais tarde, com a adaptação das instalações, meios e pessoal, o CIGE passou a conduzir diversos estágios para diversos públicos, como por exemplo o Estágio de Cibernética para Cadetes da AMAN.

Outra medida importante na capacitação foi a inclusão pelo Departamento de Educação e Cultura do Exército (DECEx) da matéria cibernética nas diversas escolas do Exército Brasileiro, como é o caso da AMAN que será tratado no próximo capítulo.

4 A DISCIPLINA CIBERNÉTICA NA AMAN

Nesta seção, pretende-se realizar uma abordagem um pouco mais aprofundada do ensino da disciplina cibernética na AMAN, com o objetivo de proporcionar um melhor entendimento de como foi implementada esta disciplina e como ela é tratada na atualidade, proporcionando ao leitor uma melhor noção das atividades pedagógicas conduzidas naquele estabelecimento de ensino voltadas ao setor cibernético.

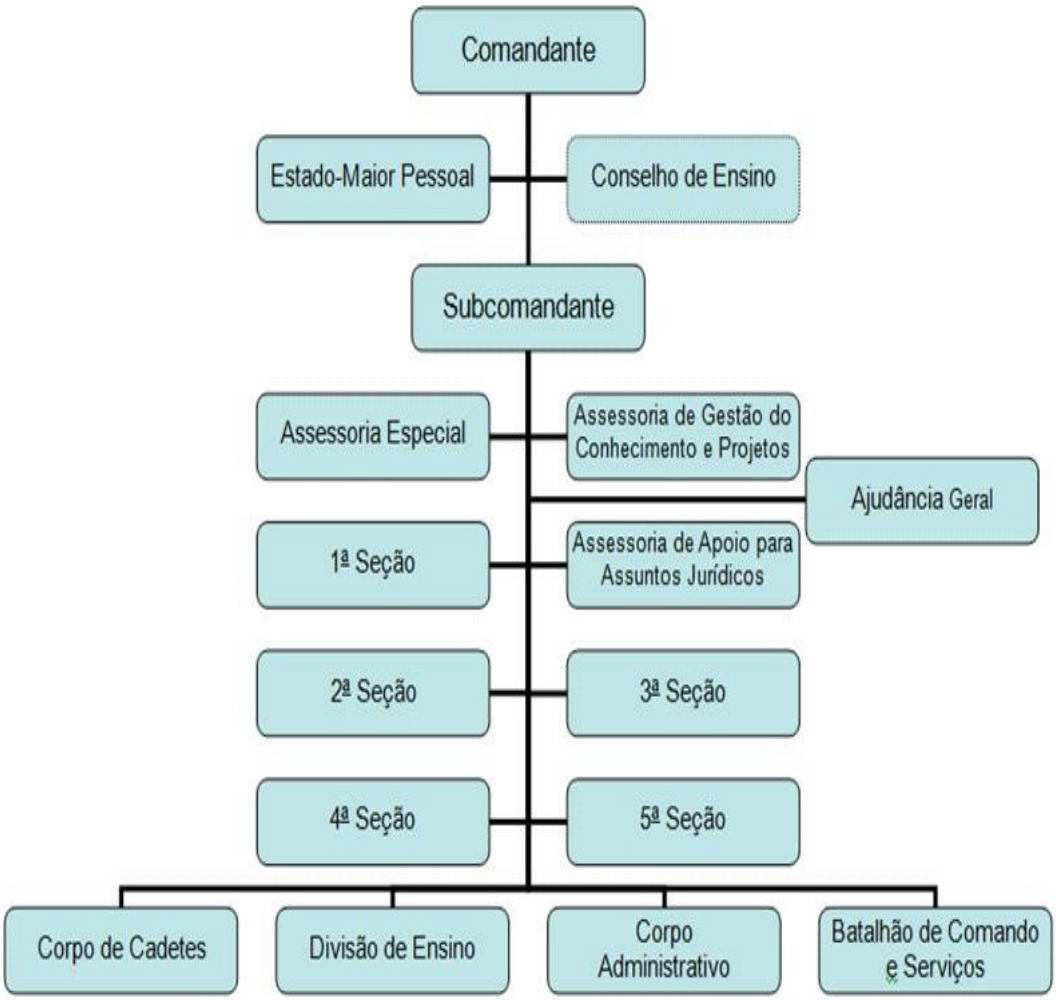
4.1 HISTORICO DA IMPLANTAÇÃO DA DISCIPLINA CIBERNÉTICA NA AMAN

Complementando as informações anteriores e finalizando este capítulo, será apresentada uma visão geral da implantação da disciplina cibernética na AMAN.

Instituição de ensino superior responsável pela formação dos oficiais combatentes de carreira do Exército Brasileiro, a AMAN tem sua história com início em 1810, com a criação da Academia Real Militar pelo Príncipe Regente D. João, sendo, inicialmente, instalada na Casa do Trem, no Rio de Janeiro, hoje Museu Histórico Nacional. Ao longo dos seus mais de duzentos anos de existência, a Academia Militar ocupou seis sedes, até que, em 1944, chegou à Resende, interior do estado do Rio de Janeiro às margens da Rodovia Presidente Dutra.

O curso de formação de oficiais combatentes possui cinco anos de duração, tendo o seu primeiro ano na Escola Preparatória de Cadetes do Exército (EsPCEx), na cidade de Campinas-SP e os demais em Resende-RJ na AMAN. Ao seu final do curso, o concludente é declarado Aspirante a Oficial e recebe o grau de Bacharel em Ciências Militares, após ter cumprido uma grade curricular que inclui disciplinas ligadas às ciências humanas, exatas, sociais e militares inerentes às diversas especialidades que integram a Linha de Ensino Militar Bélica do Exército (Infantaria, Cavalaria, Artilharia, Engenharia, Intendência, Comunicações e Material Bélico). Atualmente, para cumprir esta missão a AMAN possui a seguinte estrutura organizacional:

Figura 3: Organograma da Academia Militar das Agulhas Negras



Fonte: Regulamento da Academia Militar das Agulhas Negras (EB10-R-05.004)

Das estruturas da figura 3, a Divisão de Ensino (DE) e o Corpo de Cadetes (CC) destacam-se no aprendizado do cadete. A DE é o setor responsável pelo planejamento, controle e coordenação do ensino na AMAN. Sua missão é integrar as diversas disciplinas dos cursos e conduzir as atividades de ensino acadêmico, de forma a permitir o desenvolvimento progressivo e harmônico dos quatro anos de formação acadêmica do cadete, trazendo aos bancos acadêmicos as mais modernas técnicas de ensino, buscando entregar ao Exército Brasileiro um oficial atualizado, com o pensamento voltado para os conflitos contemporâneos, com aguçado senso crítico e com olhar voltado para o futuro.

Já o Corpo de Cadetes é o responsável pela formação militar do futuro oficial e para tal é constituído por seu comandante, subcomandante, Estado-Maior, pelos Cursos e Seções, conforme apresentado na figura 4. Aos cursos, cabe formar os

futuros oficiais nas diversas Armas, Serviço de Intendência e Quadro de Material Bélico e as seções por complementar a formação militar do cadete, atuando no desenvolvimento de atributos das áreas cognitiva, psicomotora e afetiva.

Figura 4: Organograma do Corpo de Cadetes da AMAN

Fonte: palestra institucional do Corpo de Cadetes

Assim, no 1º ano da Academia Militar, Curso Básico, ocorre a Formação Básica do futuro oficial cujo objetivos visam ajustar a personalidade do cadete aos princípios que regem a vida militar, assegurar os conhecimentos que o habilitem ao prosseguimento de sua formação de oficial, fortalecer o caráter militar, preparar o combatente básico, obtendo reflexos na execução de técnicas e táticas individuais de combate, obter capacitação física e desenvolver habilidades técnicas.

Nos 2º, 3º e 4º anos, a formação é direcionada para as sete especialidades do Exército Brasileiro, que constituem a linha de Ensino Militar Bélico. Essa qualificação tem por objetivo principal a capacitação ao exercício do comando de pequenas frações, pelotão e de subunidades de sua respectiva Arma, Quadro ou Serviço. Ainda, consolidam-se o aperfeiçoamento das técnicas individuais do combatente, o elevado padrão de ordem unida e o contínuo desenvolvimento da capacidade física.

Hoje, o ensino na Academia Militar é baseado em conceitos metodológicos modernos, buscando o desenvolvimento de competências indispensáveis para os “Líderes da Era do Conhecimento”. As metodologias de aprendizagem e a mobilização e integração de saberes para a resolução de problemas são as realidades pedagógicas da AMAN.

Neste sentido, com o advento da cibernética no Exército Brasileiro, viu-se a necessidade de incluir este assunto no currículo do cadete da AMAN. Com isso, em 2012, iniciou-se um projeto que teve como escopo a readequação da infraestrutura elétrica, aquisição de equipamentos de Tecnologia da Informação (TI), instalação de cabeamento para rede de dados, aquisição de mobiliário e outros.

Posteriormente, em 2014 e no início de 2015, um novo projeto executado pela recém criada Cadeira de Cibernética, pertencente a Divisão de Ensino, teve como objetivo a instalação e configuração dos equipamentos de TI adquiridos. No ano de 2016, a Cadeira de Cibernética deu início ao Projeto de Reestruturação de Ensino de Cibernética na AMAN, junto com o Curso de Comunicações, iniciando os trabalhos de atualização do material didático e de sua infraestrutura física. Tais ações continuam em constante aperfeiçoamento, a fim de cumprir as diretrizes do Comando do EB, conforme figura 5:

Figura 5: Diretriz para adequação cibernética nos estabelecimentos de ensino

4.2 Implantação do Setor Cibernético no Exército	**4.2.1 Implantar a estrutura de defesa e guerra cibernética.**	4.2.1.1 Estruturar(1) o órgão central do Sistema de Defesa Cibernética do Exército Brasileiro. (2020-2023)	**CIBERNÉTICA**	**Defesa Cibernética**	**EME DCT DEC COTER DGP DECEx SEF COLOG C Mil A CIE**
		4.2.1.2 Estruturar(1) o componente operacional de Defesa e Guerra Cibernética. (2020-2023)			
		4.2.1.3 Adequar(1) a estrutura de preparo e emprego de Defesa e Guerra Cibernética. (2020-2023)			
		4.2.1.4 Adequar(1) a estrutura de ensino de Defesa e Guerra Cibernética. (2020-2023)			
		4.2.1.5 Adequar(1) a estrutura de proteção cibernética das redes e sistemas corporativos do Exército. (2020-2023)			
		4.2.1.6 Adequar(1) a estrutura de apoio à produção do conhecimento oriundo da fonte cibernética. (2020-2023)			
		4.2.1.7 Adequar(1) a estrutura de apoio tecnológico e desenvolvimento de sistemas para o setor cibernético do Exército. (2020-2023)			
		4.2.1.8 Adequar(1) a estrutura de apoio às atividades de pesquisa científica, tecnológica e de inovação para o setor cibernético do Exército. (2020-2023)			

Observação: (1) Atividades já iniciadas.

Fonte: Plano Estratégico do Exército (2020-2023)

A Cadeira de Cibernética ministra, atualmente, a disciplina de Cibernética II que, além de focalizar as competências do Oficial de Informática previstas no RISG, aborda ações cibernéticas defensivas e possui uma infraestrutura física com quatro laboratórios e três salas de aula, além de uma sala onde estão os servidores que hospedam serviços que permitem ministrar aulas práticas aos Cadetes. Cabe destacar que a disciplina Cibernética I é vista pelos alunos da EsPCEx com uma carga horário de 60 horas, cuja finalidade é de fazer com que o Aluno seja iniciado nas atividades ligadas à gerência de redes e atuar como Oficial de Informática de uma Organização Militar (figura 6).

Figura 6: Alunos da EsPCEx planejando uma rede de computadores

Fonte: http://www.espcex.eb.mil.br/index.php/eventos/305-alunos-realizam-prova-pratica-de-cibernetica-i

As instruções de cibernética na AMAN são comuns para todos os cadetes do primeiro ano da AMAN, com a disciplina Cibernética II, que complementa a matéria de Cibernética I, vista na EsPCEx, e possui uma carga horária de 60 horas. Contudo, a partir do segundo ano, somente o cadete da arma de comunicações passa a ter contato com esta matéria, trabalhando com a mesma no segundo, terceiro e quarto anos sob responsabilidade do Curso de Comunicações (C Com), que está subordinado ao Corpo de Cadetes, como mostrado na figura 4.

Figura 7: Estágio de Defesa Cibernética para cadetes das Forças Armadas

Fonte: Centro de Instrução de Guerra Eletrônica

Ainda, como forma de complementar os conhecimentos, é realizado o Estágio de Defesa Cibernética para Cadetes das Forças Armadas (Figura 7), de forma presencial, no Centro de Instrução de Guerra Eletrônica, em Brasília-DF, aonde somente alguns Cadetes do 4º Ano do C Com participam.

Por fim, será apresentada na seção quatro como ocorre o ensino de cibernética na AMAN tanto para os cadetes do 1º ano ou Curso Básico quanto para os cadetes do CCom com maior profundidade, possibilitando maiores subsídios para análise do problema proposto neste trabalho.

4.2 O ENSINO DE CIBERNÉTICA NO CURSO BÁSICO DA AMAN

O Curso da AMAN é divido em fases, conforme previsto no artigo 34 do Regulamento daquele estabelecimento de ensino (EB10-R-05.004) e descrito abaixo:

> Art. 34. O Curso de Formação e Graduação de Oficiais de Carreira da Linha de Ensino Militar Bélico é estruturado em três fases distintas:
> I - a 1ª fase, correspondendo ao ano da EsPCEx, a 2ª fase ao 1º ano da AMAN, ambas com o objetivo de iniciar a formação do cadete, com a aquisição de conhecimentos comuns a todos os cursos, habilitando-o ao prosseguimento nos 2º, 3º e 4º anos da AMAN; e
> II - a 3ª fase, correspondendo aos 2º, 3º e 4º anos da AMAN, tem por objetivos:
> a) complementar a formação dada ao cadete nas 1ª e 2ª fases, habilitando-o para o desempenho de cargos de tenente e capitão não-aperfeiçoado das Armas, do Serviço de Intendência e do Quadro de Material Bélico; e
> b) orientar o futuro oficial quanto ao prosseguimento dos estudos necessários para os cargos de capitão aperfeiçoado e para os de postos mais elevados.

Diante desta descrição, pode-se perceber que o Curso Básico ou 1º ano da AMAN está na 2ª fase onde o principal objetivo é a aquisição de conhecimentos comuns a todos os cursos, ou seja, trata-se dos ensinamentos fundamentais e básicos ao futuro Oficial do Exército Brasileiro. Assim, pode-se inferir parcialmente que o conteúdo da Disciplina Cibernética II deve ser aquele que todos os oficiais combatentes devem possuir.

Isso ocorre pela constante necessidade de utilizar os meios tecnológicos de forma segura e eficaz, corroborada com as palavras do Chefe do Departamento de Educação e Cultura do Exército (DECEx), General Tomás, durante a aula inaugural ministrada em 14 de fevereiro do corrente ano para o corpo docente e para os Cadetes

da AMAN, onde evidenciou a necessidade da capacitação técnica dos recursos humanos de maneira alinhada com as novas tecnologias.

Neste sentido, basta verificar a quantidade de dispositivos adquiridos pelo Exército Brasileiro, que exige de seus operadores, independente da arma, quadro ou serviço, este tipo de conhecimento comum. Exemplo disso, é programa estratégico Sistema Integrado de Monitoramento de Fronteiras (SISFRON) que distribuiu e ainda vem distribuindo equipamentos a serem operados pela tropa, como é o caso do 11º RC Mec, localizado em Ponta Porã-MS, como mostra a figura 8.

Figura 8: Militares do 11º RC Mec operando o radar SENTIR-M20

Fonte: https://www.defesaaereanaval.com.br/defesa/savis-bradar-apresentou-linha-de-radares-na-4a-bid-brasil

Feitas estas considerações iniciais, ao se analisar o Plano de Disciplina (PlaDis) de Cibernética II, alguns pontos se destacam, entre eles a Unidade de Competência que diz “Atuar como Oficial de Informática e utilizar, de forma segura, dispositivos conectados à rede de computadores”. Ou seja, o futuro oficial do EB deverá ser capaz de operar equipamentos com desenvoltura e segurança.

Além disso, ao examinar as Unidades Didáticas e principalmente seus objetivos, presentes na tabela 5 abaixo, verifica-se a utilização em sua maioria de verbos factuais, ou seja, focado somente nos fatos, mas sem procurar compreendê-los e/ou interpretá-los. Desta forma, demonstrando se tratar de conhecimentos básicos, mas que são de grande relevância para as atividades que estes militares irão executar no futuro.

Tabela 5: Objetivos de cada Unidade Didática da Disciplina Cibernética II

Unidade Didática	Objetivos
I – Apresentação da Disciplina	- Conscientizar para a importância da disciplina. - Ambientar o discente com o laboratório. - Verificar o nível de conhecimento de TIC.
II – Gestão da Segurança da Informação	- Compreender e aplicar a gestão da segurança da Informação a fim de assessorar o comando em suas decisões.
III - Legislação	- Apresentar uma reflexão sobre as principais legislações aplicadas à Cibernética, bem como apresentar os documentos de referência do Comando de Defesa Cibernética e manuais do Exército a fim de que o cadete se mantenha atualizado.
IV – Segurança Criptográfica	- Apresentar os principais conceitos referentes ao tema criptografia digital visando aplicação prática na tropa.
V – Segurança de Redes de Computadores	- Apresentar, sumariamente, o funcionamento de uma rede de computadores, como pré-requisito aos assuntos relativos à segurança cibernética. - Apresentar, sumariamente, alguns protocolos (serviços básicos de rede), bem como algumas ferramentas de segurança, auditoria e tolerância a falhas que, direta ou indiretamente, estão relacionadas à segurança cibernética.
VI – Segurança para Internet	- Apresentar os principais golpes, ataques e códigos maliciosos em redes de computadores, bem como aspectos de segurança relativo ao uso de redes de computadores em face destas ameaças virtuais com vistas ao emprego de proteções aos ativos particulares e de sua OM.
VII – Exercício Prático Geral	- Consolidar, através de situações-problema, os assuntos abordados na disciplina, visando ao emprego prático dos conteúdos apresentados em sala de aula e em laboratório.

Fonte: Plano de Disciplina de Cibernética II do ano de 2019

Cabe ressaltar, conforme já mencionado no capítulo 2.3, que a cadeira de cibernética possui apenas 60 horas para transmitir estes conhecimentos. Exigindo que os instrutores sejam sucintos e objetivos em suas abordagens e que os cadetes tenham que se esforçar mais para assimilar as informações passadas e estar em condições de praticá-las.

Ainda, como visto na tabela 2 do capítulo 4.1, as Organizações Militares (OM) integrantes da FTC deverão estar em condições de realizar sua própria proteção cibernética, mas de maneira preventiva. Que exige dos integrantes daquelas OM uma certa compreensão das atividades cibernéticas visando a execução desta tarefa

e para auxiliar nos planejamentos como interpretação das possibilidades de um inimigo que tenha capacidades cibernéticas.

Em relação a identificação e registro de talentos do 1º ano em cibernética, não foi encontrado nada que tratasse desse assunto, sendo a observação feita somente através de Fatos Observados lançados no Sistema de Observação do Cadete (SOC), onde o objetivo maior do sistema não é a busca por talentos e sim de gerar os chamados Fatos Observados Positivos e Negativos que trata da parte de justiça e disciplina gerando possíveis recompensas aos militares que se destacam em uma determinada tarefa ou instrução e punições aqueles que comentem alguma transgressão disciplinar, sendo portanto comportamental ou atitudinal e não algo ligado as habilidades cognitivas.

Por fim, chega-se a uma conclusão parcial de que seria interessante o aumento da carga horária da disciplina pela relevância do assunto, bem como uma melhor forma de registro dos militares que se destacam na matéria favorecendo a execução de um banco de dados de pessoal que permitisse o melhor emprego dos recursos humanos.

4.3 O ENSINO DE CIBERNÉTICA NO CURSO DE COMUNICAÇÕES DA AMAN

Neste capítulo, será abordado como funciona o ensino de cibernética para os cadetes do segundo, terceiro e quarto anos do Curso de Comunicações (CCom) da AMAN. Salienta-se que este grupo de cadetes corresponde à 3ª fase, cujo objetivo é complementar a formação dada ao cadete nas 1ª e 2ª fases, habilitando-o para o desempenho de cargos de tenente e capitão não-aperfeiçoado conforme previsto no regulamento da AMAN, visto no capítulo anterior.

Feita esta consideração, é fundamental entender que o CCom tem por missão principal capacitar os cadetes de Comunicações para exercer os cargos de Oficial Subalterno e Intermediário não-aperfeiçoado, nas Organizações Militares de Comunicações. Assim, pode-se compreender melhor o motivo da Unidade de Competência dos PlaDis (EXÉRCITO, 2020) do CCom durante todo o curso ser basicamente o mesmo, a saber: “Planejar e conduzir o emprego da fração em operações convencionais, comandando os pelotões de comunicações orgânicos da Cia Com/Bda e Btl Com/DE”.

Neste sentido, pode-se afirmar que nesta fase o cadete irá receber um conhecimento mais específico, tendo vista as funções que irá exercer. Conforme, será apresentado as tabelas 6, 7 e 8 abaixo, que correspondem respectivamente, as disciplinas: Cibernética III voltada ao 2º ano, Cibernética IV ao 3º ano e Cibernética V ao 4º ano, com o propósito de mostrar as diferenças de objetivos em relação ao visto pelos cadetes do 1º ano e posteriormente servir de subsídio para as continuação dos estudos deste capítulo.

Tabela 6: Objetivos de cada Unidade Didática da Disciplina Cibernética III

Unidade Didática	**Objetivos**
I – *Cisco Certified Network Associate* I (CCNA I)	- Compreender a importância das redes de computadores no nosso cotidiano. - Descrever as características das arquiteturas de rede: tolerância a falhas; escalabilidade; qualidade do serviço; segurança. - Compreender a estrutura de rede conforme os modelos OSI e TCP/IP e as suas camadas. - Compreender o funcionamento do protocolo IPV4 e a respectiva divisão de IPs. - Compreender a divisão de redes e sub-redes. - Compreender os conceitos e funcionamento na rede das conexões *unicast, multicast* e *broadcast.* - Realizar a instalação, configuração e conhecer as ferramentas do *Packet Tracer***.**
II - *Cisco Certified Network Associate* II (CCNA II)	- Compreender qual o papel do *switch* no funcionamento de uma rede. - Compreender o que é um *switch* e identificá-lo. - Realizar as configurações básicas de um *switch*. - Compreender o funcionamento da tabela MAC. - Identificar uma tabela MAC. - Realizar as configurações de um *switch* necessárias desde o terminal até a integração com o roteador, abordando as configurações de interface e porta. - Compreender qual o papel do roteador no funcionamento de uma rede. - Identificar um roteador. - Definir o que é um roteador - Realizar as configurações básicas de um roteador. - Compreender o funcionamento da tabela de roteamento. - Identificar uma tabela de roteamento. - Compreender como funcionam os protocolos de roteamento. - Realizar as configurações necessárias para a integração terminal *switch*-roteador de forma a deixar uma LAN funcional utilizando-se do roteamento estático. - Realizar as configurações necessárias para a integração *switch*-roteador de forma a construir uma LAN.

	- Compreender o funcionamento da Camada OSI e os respectivos protocolos. - Executar os padrões de *hardware* correspondentes a camada física do modelo OSI. - Elaborar um diagrama que mostre, no modo simulação, a aplicação dos protocolos da camada de Enlace do modelo OSI. - Elaborar um diagrama que mostre, no modo simulação, a aplicação dos protocolos da camada de Rede do modelo OSI. - Elaborar um diagrama que mostre, no modo simulação, a aplicação dos protocolos da camada de Transporte (TCP, UDP) do modelo OSI.
III – Infraestrutura de rede	- Identificar os tipos de cabo de par trançado (UTP e STP) e suas categorias. - Distinguir os tipos conexões do cabo de par trançado (direta e *crossover*). - Identificar as características de um cabo de par trançado num *datasheet***.** - Definir e identificar os tipos de emenda de cabo de par trançado. - Realizar a crimpagem de cabo UTP para formar cabo *straight**, through*** ou *crossover***.** - Operar corretamente o testador de cabo de par traçado para verificar a qualidade da conexão.

Fonte: Plano de Disciplina de Cibernética III para o ano de 2021

Tabela 7: Objetivos de cada Unidade Didática da Disciplina Cibernética IV

Unidade Didática	**Objetivos**
I – Gerenciamento de Máquinas Virtuais	- Compreender conceitos básicos de virtualização de sistemas operacionais. - Realizar o *download* e instalação do *VirtualBox*. - Instalar o pacote de extensões. - Compreender os parâmetros de configuração disponíveis na interface do *Oracle VirtualBox*. - Criar uma máquina virtual. - Executar o *Snapshot* de uma máquina virtual. - Compreender os tipos de iniciação e desligamento de uma máquina virtual. - Gerenciar mídias virtuais. - Realizar a clonagem de máquinas virtuais. - Compreender os tipos de adaptadores de rede existentes. - Configurar o adaptador de uma máquina virtual a partir de um contexto específico. - Instalar o *VBox Guest Adittions*. - Configurar área de transferência compartilhada. - Configurar pasta compartilhada com o *host***.** - Configurar o acesso de dispositivos USB à máquina virtual.

	- Realizar operações de máquinas virtuais em interface de linha de comando.
II – Serviços de Rede	- Compreender a arquitetura do servidor *Apache*. - Instalar o *Apache***.** - Compreender os principais comandos do servidor *Apache* - Configurar uma aplicação *Web* no *Apache*. - Configurar o módulo PHP no *Apache*. - Executar a configuração de *logs*. - Sanar erros comuns em serviços *Web*. - Configurar o monitoramento do serviço. - Realizar boas práticas de segurança de serviços *Web*. - Executar a encriptação de dados com *Apache.* - Compreender a arquitetura e o funcionamento do DHCP. - Executar a instalação do *isc-dhcp-server*. - Executar a configuração inicial do servidor DHCP. - Executar a configuração de interfaces de rede do serviço. - Executar a declaração de sub-redes utilizadas. - Configurar *hosts* de endereço IP fixo. - Iniciar, encerrar e reiniciar o serviço DHCP - Compreender a arquitetura e o funcionamento do DNS. - Executar a instalação do pacote *bind9*. - Executar a configuração do servidor DNS para operação nos modos IPv4 e IPv6. - Executar a configuração do arquivo de opções para funcionamento do servidor DNS primário. - Configurar as zonas de DNS. - Configurar as zonas de encaminhamento. - Configurar o servidor DNS secundário. - Configurar os clientes DNS. - Compreender a arquitetura e o funcionamento do FTP. - Executar a instalação do pacote *proftpd*. - Executar a configuração inicial do servidor FTP. - Criar grupos e adicionar usuários ao serviço. - Compreender a arquitetura e o funcionamento do NTP. - Compreender as características do NTP.br. - Configurar uma máquina para operação no modo servidor.
III - Firewall	- Compreender a arquitetura e o funcionamento de um *firewall.* - Compreender as características e a compatibilidade do *PFSense*. - Realizar a instalação do *PFSense*. - Executar a configuração inicial do *PFSense*. - Criar *aliases***.** - Configurar regras de *firewall*. - Configurar regras de redirecionamento. - Executar o monitoramento da rede com *PFSense***.**

Fonte: Plano de Disciplina de Cibernética IV para o ano de 2021

Tabela 8: Objetivos de cada Unidade Didática da Disciplina Cibernética V

Unidade Didática	Objetivos
I – *Proxy*	- Compreender a arquitetura e o funcionamento de um servidor *proxy.* - Compreender as características e a compatibilidade do *Squid.* - Executar a instalação do *Squid.* - Executar a configuração inicial do *Squid.* - Configurar listas de controle de acesso (ACL). - Configurar autenticação de acesso - Configurar a geração de relatórios - Executar o *backup* do servidor e configurar o processo para execução automática.
II - *Hardening*	- Identificar os princípios de *hardening.* - Recuperar senha de *root.* - Executar a proteção do gerenciador de *boot* (GRUB). - Executar a segurança do particionamento de disco. - Executar a limitação do uso de recursos do sistema de arquivos por usuário. - Executar o controle granular das permissões de acesso a arquivos e diretórios.
III – *Cybersecurity Essentials*	- Compreender as fases de um ataque cibernético conforme o modelo *Lockheed Martin*, identificando, em cada uma, o que pode ser feito para evitar ou interromper a ação de um atacante. - Compreender como cada tipo de *malware* e ataque cibernético funciona, elencando medidas que o usuário ou o administrador de redes deve tomar para garantir a segurança do perímetro cibernético sob sua responsabilidade.

Fonte: Plano de Disciplina de Cibernética V para o ano de 2021

Tendo apresentado as Unidades Didáticas (UD) e seus respectivos objetivos nas tabelas 6, 7 e 8, percebe-se uma mudança profunda para os do 1º ano mostrado na tabela 5. A iniciar pelas próprias UD onde verifica-se uma maior complexidade e os objetivos cujos verbos exigem uma maior habilidade do discente, aliando sempre a teoria com a prática.

Isso justifica-se, pois a missão básica de uma OM de Comunicações sempre é de Instalar, Explorar, Manter e Proteger os Sistemas de Comunicações de sua Brigada (Bda) ou Divisão de Exército (DE) enquadrante. Dito isto, com a evolução tecnológica do espaço de batalha, os meios de Tecnologia da Informação e Comunicações (TIC) exigem cada vez mais um conhecimento aprofundado do assunto, ocasionando uma maior necessidade de capacitação dos recursos humanos, como pode ser observado na figura 9 abaixo.

Figura 9: Cadete do CCom durante instrução de manutenção de computadores

Fonte: Curso de Comunicações da AMAN (2020)

Neste sentido, o Curso de Comunicações destina uma carga horária (CH) maior em relação ao Curso Básico para esta disciplina. Para o segundo ano, a CH de Cibernética III é de 104 horas de instrução, no terceiro ano, Cibernética IV possui 64 horas e no quarto ano, a Cibernética V tem 60 horas, totalizando 228 horas de instrução de Cibernética. Entretanto, pela gama de assuntos e sua complexidade e constante atualização, exigirá do futuro oficial da arma de comunicações a busca pelo autoaperfeiçoamento e especialização.

Outro aspecto que se deduz da análise das tabelas 6, 7 e 8 é que as matérias visam a operações dos meios de TIC e a proteção cibernética, não sendo abordadas as atividades de ataque Cibernético e exploração cibernética, constantes da tabela 1 vista anteriormente. Isto ocorre, pois ao final do curso, conforme previsto no Perfil Profissiográfico do concludente do CCom da AMAN, estes novos oficiais estarão aptos a “planejar e conduzir o emprego de fração em operações convencionais comandando os pelotões de comunicações orgânicos das Companhias e Batalhões de Comunicações”. Assim conforme tabela 4 apresentada, as capacidades operativas cibernéticas exigidas se resumem apenas a Proteção Cibernética.

Em relação a identificação e registro de talentos em cibernética, da mesma forma que no Curso Básico, apenas verificou-se o lançamento de Fatos Observados no Sistema de Observação do Cadete (SOC), que, conforme já tratado, não tem foco na descoberta de talentos. Existe também o Projeto de Acompanhamento e Avaliação da Área Atitudinal, comumente conhecido pelo acrônimo P4A. Segundo Teixeira Junior e Moreira (2017), idealizadores e implementadores do instrumento, o P4A é uma ferramenta que sistematiza a observação e avaliação do campo atitudinal dos cadetes, permitindo o acompanhamento do processo pedagógico do desenvolvimento de atitudes, porém sem realizar registros de habilidades.

Por fim, infere-se parcialmente que seria interessante um aumento da carga horária, particularmente para o 3º ano, devido à dificuldade dos assuntos tratados e a necessidade de uma maior prática, bem como a execução de um banco de dados de pessoal, que permitisse o acesso a estas informações, para a seleção de militares para o Curso de Guerra Cibernética, por exemplo. Estes aspectos serão tratados mais à frente nas seções 6 e 7.

5 CIBERNÉTICA NA ACADEMIA MILITAR DOS ESTADOS UNIDOS DA AMÉRICA

Esta seção tem por finalidade abordar como funciona o ensino de cibernética na Academia Militar dos Estados Unidos da América (EUA), apresentando seus objetivos e realizando uma comparação com o ensino desta matéria na AMAN que foi abordado na seção anterior. Foi escolhido os EUA para realizar esta comparação tendo vista possuir o Exército mais poderoso do mundo e consequentemente ser alvos de estudos pelos demais exércitos.

Porém, antes de iniciar o escopo desta seção, é necessário realizar uma pequena abordagem sobre a cibernética naquele país. Pois, em um mundo onde a TIC possibilita um maior acesso a novos conhecimentos, negócios e serviços e ainda sustentam a superioridade militar dos EUA, ao permitir que suas forças militares obtenham vantagem.

Assim, o governo estadunidense nos últimos anos passou a verificar que sua prosperidade, liberdade e segurança depende do acesso confiável à informação. Afinal, atualmente os EUA estão envolvidos em uma competição estratégica com a China e a Rússia, que expandiram essa competição para ações no ciberespaço, representando riscos estratégicos aos interesses americanos.

De acordo com a reportagem da *BBC NEWS,* de 25 de novembro de 2018, a República Popular da China vem ameaçando a supremacia militar e principalmente a vitalidade econômica dos EUA nos últimos anos.

Neste sentido, esta reportagem aborda que de acordo com diversos especialistas, o acesso ilegal a informações confidenciais das instituições públicas e privadas americanas são um dos motivos dessa ameaça chinesa, exemplificada de forma mais recente, por hackers chineses (figura 10) que estão sendo acusados pelo Departamento de Justiça dos EUA, por realizar ações contra empresas americanas que estão trabalhando no desenvolvimento de vacina para a COVID-19.

Também, de acordo com a reportagem, outra ameaça é a Rússia que tem utilizado de operações de informação baseadas em atividades cibernéticas para influenciar a população e interferir nos processos democráticos como se suspeita que tenha ocorrido nas eleições americanas de 2016. Por último, existem outros atores, como a Coréia do Norte e o Irã, que também empregam atividades cibernéticas para atacar os EUA e ameaçar seus interesses e que são vistas como potenciais ameaças.

Figura 10: Hackers chineses acusados pelo Departamento de Justiça dos EUA

Fonte: https://www.defcon-lab.org/apt-china-e-eua-guerra-cibernetica-nos-tribunais/

Dessa maneira, já em 2009, o Departamento de Defesa norte-americano estabeleceu seu Comando Cibernético (CYBERCOM), localizado em *Fort Meade* no estado de *Maryland*, como um quartel-general conjunto para coordenar os esforços no ciberespaço, onde integrantes de todas as Forças Singulares se unem dentro do CYBERCOM (figura 11) para agir contra as ameaças cibernéticas.

Figura 11: Comando Cibernético dos EUA

Fonte: Artigo do Maj Matt Graham, Exército dos EUA publicado na *Military Review* do terceiro trimestre de 2016 (p.72 a 80)

Em 2017, o presidente dos EUA, Donald Trump, elevou o status do CYBERCOM à mesma categoria das divisões do Pentágono dedicadas no combate aos ataques cibernéticos, dando uma maior autonomia para agir por conta própria ao detectar ameaças virtuais (figura 12). Atualmente, possui a missão de direcionar, sincronizar e coordenar o planejamento e operações do ciberespaço para defender e incrementar os interesses norte-americanos em colaboração com seus parceiros internos e internacionais.

Figura 12: Equipe de Operações Cibernéticas analisando dados de ameaças

Fonte: Artigo do Ten Cel David M. Beskow, Exército dos EUA e Kathleen M. Carley, Ph.D publicado na *Military Review* do terceiro trimestre de 2019 (p.25 a 35)

Um exemplo recente das atividades do CYBERCOM, publicado pela revista VEJA em 23 de junho de 2019, ocorreu em 2019 quando foram realizados ataques cibernéticos, contra sistemas de computadores do Irã usados para controlar lançamentos de mísseis e foguetes, tal medida também ocorreu em meio ao temor dos Estados Unidos de que o Irã tentasse realizar ataques cibernéticos aos aliados de Washington no Oriente Médio

Depois destas considerações iniciais, será abordado a seguir o ensino de cibernética na Academia Militar dos EUA (figura 13) conhecida também como

Academia de *West Point*, justamente por estar localizada em *West Point*, Nova Iorque. Criada oficialmente em 1802 pelo congresso americano é o berço da formação dos oficiais de carreira do Exército dos EUA, homóloga à Academia Militar das Agulhas Negras no Brasil.

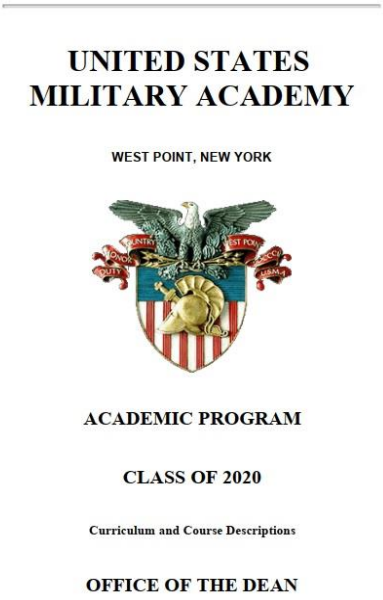
Sua missão, de acordo com seu sítio na *internet,* é "educar, treinar e inspirar o Corpo de Cadetes para que cada graduado seja um líder de caráter comissionado comprometido nos valores de Dever, Honra, País além de estar preparado para uma carreira de excelência profissional e serviço à Nação como oficial do Exército dos Estados Unidos ".

Figura 13: Vista Aérea da Academia Militar Norte-americana

Fonte: https://www.westpoint.edu/

Possui um período de formação de quatro anos e um objetivo acadêmico principal de fazer com que os graduados integrem conhecimentos e habilidades das várias disciplinas visando antecipar e responder adequadamente às oportunidades e desafios em um mundo em constante mudança. Para atingir esse objetivo é seguido um programa acadêmico chamado *Redbook* (Figura 14) projetado para fornecer as informações necessárias das capacidades de todos os cursos, por departamento de ensino, oferecidos em cada ano e período acadêmico. Cabe destacar que esta foi a principal bibliografia utilizada na confecção desta seção.

Figura 14: Programa Acadêmico da Academia Militar dos EUA (*Redbook*) 2020



UNITED STATES
MILITARY ACADEMY

WEST POINT, NEW YORK

ACADEMIC PROGRAM

CLASS OF 2020

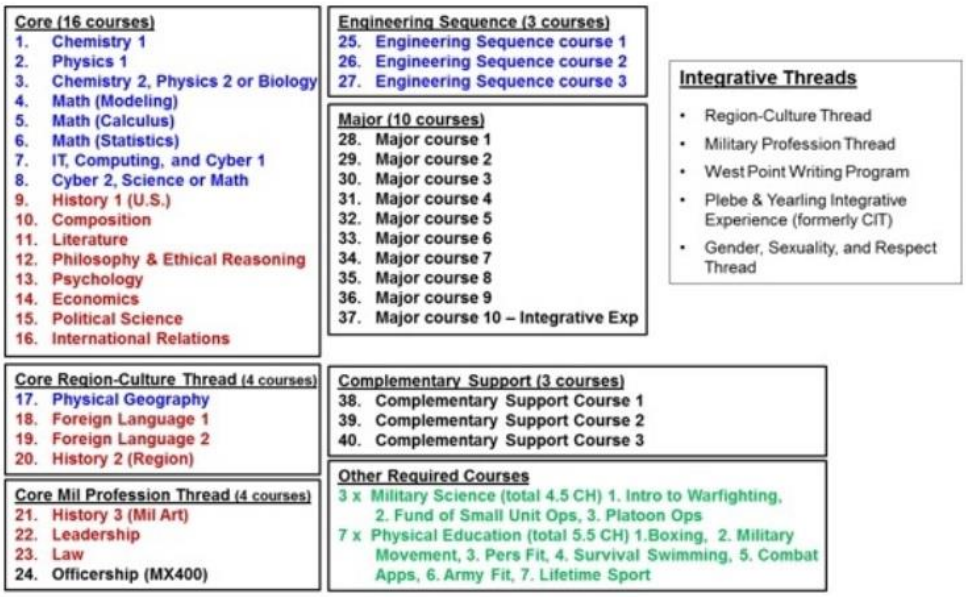
Curriculum and Course Descriptions

OFFICE OF THE DEAN

Fonte: https://courses.westpoint.edu/static/index.htm

O currículo da Academia Militar possui duas características significativas (figura 15). O primeiro é um núcleo sólido de vinte e quatro cursos que a Academia considera essenciais para a ampla base de conhecimento necessária para todos os graduados e uma sequência de engenharia básica de três cursos para os cadetes que não escolhem se especializar em engenharia.

Figura 15: Visão Geral do Programa Acadêmico de *West Point*



Fonte: https://courses.westpoint.edu/static/index.htm

Esse currículo básico, quando combinado com a educação física e a ciência militar, constitui o "*major professional*" da Academia Militar. A segunda característica é a oportunidade de se especializar e explorar uma área em profundidade através da seleção de um curso acadêmico composto por pelo menos treze cursos obrigatórios ou eletivos.

Assim, conforme descrito no programa acadêmico, o currículo básico também inclui uma sequência de tecnologia da informação/cibernética (TI/CIBER) projetada para garantir que todos os graduados da academia estejam confortáveis e capazes de usar os meios de TIC em um exército que deve lutar e vencer em um domínio cibernético abrangente.

As habilidades em TI/CIBER são desenvolvidas por meio de um curso introdutório no primeiro ano e pela integração de aplicativos de computador e cibernética em todo o currículo principal e, particularmente, no requisito de TI/CIBER no terceiro ou quarto anos. O requisito de TI/CIBER pode ser cumprido com o curso principal, CY305, *Cyber Foundations* ou com a cobertura existente do curso de tópicos cibernéticos, em especial de especialização ou de aprofundamento como é chamado naquele estabelecimento de ensino.

Ainda, cabe destacar que no início do segundo ano o cadete de West Point poderá optar por uma das Engenharias principais para prosseguir em seus estudos, são elas: Engenharia Cibernética, Engenharia Elétrica, Engenharia Ambiental, Engenharia de Infraestrutura, Engenharia Nuclear e Engenharia de Sistemas.

Destarte, ao analisar o programa acadêmico percebe-se uma grande presença de matérias exatas no seu currículo, onde a vocação de West Point está focada na formação de engenheiros. Essa condição acaba por facilitar o entendimento e absorção do conhecimento em Cibernética, uma vez que programas de computador trabalham essencialmente com dados matemáticos.

Outra característica é a parte prática dos assuntos ministrados, onde os cadetes são instigados desde de cedo a trabalhar com criatividade e a criar novas soluções tecnológicas para as atividades militares, como pode ser observado na figura 16 abaixo, onde cadetes estão realizando uma demonstração ao comandante do exército americano, General de Exército Mark Milley, da utilização de um fuzil com capacidades cibernéticas para abater Veículo Aéreo Não Tripulado (VANT).

Figura 16: Demonstração de cadetes de *West Point* ao Comandante do Exército

(Sgt Chuck Burden, Exército dos EUA)

O Comandante do Exército, Gen Ex Mark Milley, observa oficiais do Instituto Cibernético do Exército na Academia Militar dos EUA, em West Point, Nova York, demonstrar o abatimento de um veículo aéreo não tripulado (VANT) utilizando-se de um fuzil com capacidades cibernéticas.

Fonte: Artigo do Maj Matt Graham, Exército dos EUA publicado na *Military Review* do terceiro trimestre de 2016 (p.72 a 80)

Realizando a comparação entre o ensino da AMAN e de *West Point*, pode-se verificar que existem várias diferenças, principalmente curriculares e nos objetivos pedagógicos. Enquanto, a AMAN possui uma maior preocupação com o ensino das artes essencialmente militares, a Academia dos EUA possui um foco maior nas disciplinas técnico-científico e de humanas, justificada pelo fato de que diferente da AMAN nem todos os formandos permanecerão no Exército.

Outra diferença está na base curricular, onde West Point tem sua essência nas ciências exatas, voltadas principalmente aos estudos dos diversos cursos de engenharia voltando assim na criatividade para resolução dos problemas militares com base em tecnologia.

Diferentemente, na AMAN o cerne está nas disciplinas humanas, onde o centro são as relações interpessoais, o que pode ser exemplificado com as matérias de psicologia, filosofia, relações internacionais, política e estratégia, dentre outros, com uma carga horária significativa se compararmos com a academia americana.

Estas diferenças são fundamentais ao tratar do ensino de cibernética, pois pode-se concluir que a Academia Militar dos EUA está em vantagem, uma vez que os meios cibernéticos têm como base as ciências exatas para o seu desenvolvimento e

execução. A característica prática e exclusiva do ensino de cibernética em West Point permite a formação de recursos humanos com maior capacidade cognitiva para atuar neste setor tão sensível.

Finalmente, não foi possível nesta seção tratar de como ocorre a busca por talentos na Academia Militar dos EUA por ser um assunto classificado por aquele país não permitindo realizar uma comparação nesta área. Entretanto, visualiza-se que não houve prejuízos a consecução deste trabalho, tendo vista o material reunido na AMAN aliado a experiência adquirida pelo questionário realizado com os cadetes do Curso de Comunicações cujo resultados serão discutidos na seção a seguir.

6 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS DE QUESTIONÁRIO

Nesta seção serão apresentados os resultados de um questionário, composto de nove perguntas de múltipla escolha, realizado com os cadetes do segundo, terceiro e quarto anos do Curso de Comunicações da AMAN. Como já tratado na seção dois, esse universo foi escolhido por ter um maior contato com a disciplina e desta forma possuir melhores condições de contribuir com este trabalho.

Participaram do questionário um total de 110 cadetes, sendo 32 (trinta e dois) do 2º ano, 40 (quarenta) do 3º ano e 38 (trinta e oito) do 4º ano. Assim, a primeira pergunta tinha justamente a finalidade de verificar a participação dos cadetes sem, no entanto, pedir sua identificação a fim de evitar desvios de respostas.

A segunda questão foi a respeito da carga horária da disciplina Cibernética II, ministrada no 1º ano. O resultado obtido foi que 55,5% dos cadetes acreditaram ser suficiente, contra 44,5% que julgaram a carga insuficiente, demonstrando assim a falta de experiência dos cadetes nesse assunto, uma vez que os cadetes não participam de exercícios reais onde a cibernética assume papel protagonista nas operações.

Outrossim, os resultados da terceira pergunta, que tratava da relação entre as instruções do Curso Básico com o despertar do interesse no setor cibernético foram os mesmos, representando uma oportunidade de melhoria no despertar de interesse no setor cibernético.

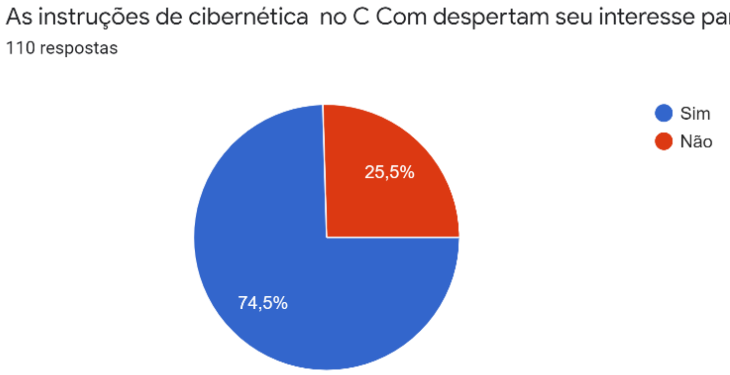
Já a quarta questão tratou da busca de destaques na disciplina Cibernética II, obtendo o seguinte resultado: 28,4% responderam que sim, 36,4% que parcialmente e 35,5% que não. Com essas respostas pode-se verificar que a busca por talentos cibernéticos é praticamente nenhuma, limitando-se somente a elogios e recompensas, não realizando a separação destes recursos.

Destarte, os gráficos 1 e 2 abaixo dizem respeito a quinta e sexta perguntas, respectivamente, as quais tinham por objetivo verificar qual a influência do fato de o Curso de Comunicações continuar a ministrar a disciplina cibernética para a escolha pela arma de comunicações e para o interesse no setor. Dessa forma, verifica-se que os resultados comprovam a importância que o cadete de comunicações atribui para a área cibernética, bem como seu entusiasmo.

Gráfico 1: Relação entre instruções de cibernética e a escolha da Arma de Comunicações

Fonte: O autor

Gráfico 2: Relação entre instruções de cibernética e o interesse no setor



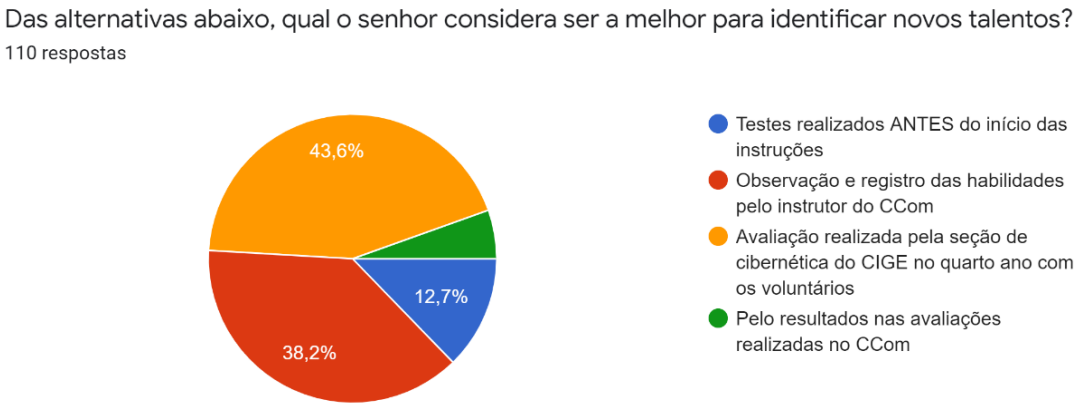
Fonte: O autor

Em relação ao próximo quesito, foi perguntado sobre o número de cadetes que realmente se destacam nas disciplinas de Cibernética III, IV e V, onde constatou-se que os destaques são poucos, variando de 1 a 5 cadetes, corroborando a dificuldade em encontrar militares para atuar neste espectro e na necessidade de haver métodos eficazes para buscar, reter e dar o tratamento necessário a estes novos talentos.

Em consonância com a questão anterior, foi perguntado, no item 8, sobre o grau de importância dado pelos cadetes a identificação e registro de talentos para o setor cibernético, onde 70,9% consideram MUITO IMPORTANTE e 27,3% IMPORTANTE, totalizando em 98,2% que compreendem a relevância de ações na busca por novos talentos.

A última questão tratou de perguntar aos cadetes, dentre alternativas apresentadas, qual era a mais adequada na identificação de novos talentos para o setor cibernético, externando os resultados constantes do gráfico 3.

Gráfico 3: Melhor alternativa na identificação de talentos



Fonte: O autor

Ao analisar o resultado obtido no gráfico 3 pode-se constatar que, para a maioria, o método mais eficiente de identificar talentos para o setor cibernético na AMAN é através de avaliações realizadas por um órgão externo, neste caso, a seção de Cibernética do Centro de Instrução de Guerra Eletrônica (CIGE), a fim de obter uma lisura no processo. Além disso, foi dado destaque para a observação e registro pelo instrutor da disciplina.

Por fim, pelos resultados obtidos pelo questionário realizado, sugere-se a criação de um sistema de banco de dados unificado no Sistema de Educação e Cultura do Exército, que abarque não somente a cibernética mais outras habilidades que incrementam as capacidades do Exército Brasileiro a fim de permitir o registro dessas habilidades dos inúmeros recursos humanos nos diversos estabelecimento de ensino do EB como é o caso da Academia Militar das Agulhas Negras.

7 SUGESTÕES PARA A IDENTIFICAÇÃO E SELEÇÃO DE TALENTOS EM CIBERNÉTICA NA AMAN

Neste capítulo, serão apresentadas algumas sugestões para a seleção de talentos na AMAN, focada para o setor cibernético, mas que com as devidas alterações podem ser utilizadas para outras especialidades. Contudo, antes serão realizadas algumas considerações sobre a definição de talento, as necessidades humanas e suas relações com a identificação, registro e gerenciamento do pessoal de carreira do EB.

Assim, no meio empresarial talentos são potenciais para desempenho de acordo com o conceito de cada empresa, ou seja, profissionais criativos e dinâmicos que trazem novas ideias e fazem a diferença nas suas empresas. Trazendo para o meio militar pode-se afirmar que talentos são aqueles militares com grande capacidade de trabalho, comprometidos com a Instituição e com alto domínio naquilo que executam.

Neste sentido, vale ressaltar que o EB se destaca em possuir recursos humanos comprometidos com os valores da Força e que altos graus de capacitação e/ou especialização, como é o caso do setor cibernético, exigem tempo e experiência na função. Nesse aspecto, um dos grandes desafios ao tratar de militares especialistas é a retenção destes na instituição, pois anualmente ocorre de alguns pedirem demissão, atraídos por empregos na iniciativa privada e em outros locais do setor público.

Nesse cenário, o gerenciamento de recursos humanos é algo extremamente complexo, principalmente numa Instituição como o EB possuidora de grande efetivo e que dispõe de presença nacional e disponibilidade permanente. Ao mesmo tempo em que além do risco de perder esses militares outro é de estes saírem após uma capacitação, por exemplo, o que traz prejuízos financeiros enormes e causa muitas vezes a descontinuidade de uma determinada tarefa específica.

Com a finalidade de buscar entender a causa dessa evasão, será apresentado e feita uma breve análise do conceito criado pelo psicólogo norte-americano Abraham Maslow, conhecida por pirâmide de Maslow (figura 17), que determina as necessidades fundamentais e as condições necessárias para que cada ser humano sobreviva e atinja a sua satisfação pessoal e profissional.

Figura 17: Pirâmide de Maslow

Fonte: Raimundo e Neto (2017) apud Eugênio (2016)

Feita a mostra da pirâmide de Maslow e confrontando com as principais causas da evasão em geral, uma se destaca, a desmotivação com a carreira. E, nesse aspecto, alguns fatos que podem contribuir para essa desmotivação no EB são de o militar estar trabalhando em uma área que não gosta ou que não crê possuir as capacidades necessárias ao desempenho da função, a falta de oportunidade de crescimento profissional e a de perspectiva para com o futuro

Nessa perspectiva, cabe destacar que elementos especializados em cibernética são raros tanto no meio civil quanto no militar e que para formar um combatente cibernético requer tempo e dinheiro. Por isso, é fundamental a busca de ações que motivem e façam esse profissional prosseguir na carreira e permanecer na Força.

Corroborando com este ponto de vista, a Política Cibernética de Defesa de 2012, traz dentre outras diretrizes, as atinentes ao Objetivo Nr II (capacitar e gerir talentos humanos necessários à condução das atividades do setor Cibernético no âmbito do MD), que estão expostos a seguir:

> a) definir os perfis do pessoal necessário para a condução das atividades do Setor Cibernético;
> b) criar cargos e funções específicos e mobiliá-los com pessoal especializado para atender às necessidades do Setor Cibernético;
> c) estabelecer critérios e controlar a mobilização e desmobilização de pessoal para a atividade de Defesa Cibernética;

> d) identificar, cadastrar e selecionar o pessoal com competências ou habilidades, existente nos ambientes interno e externo das FA, para integrar o SMDC;
> e) capacitar, de forma continuada, pessoal para atuar no Setor Cibernético, sob a orientação do órgão central do SMDC, aproveitando estruturas existentes;
> f) viabilizar a participação de pessoal envolvido com o Setor Cibernético em cursos, estágios, congressos, seminários, simpósios e outras atividades similares relacionadas no Brasil e no exterior;
> g) realizar, periodicamente, eventos que possibilitem a apresentação e discussão de temas relevantes em áreas de interesse do Setor Cibernético, a serem organizados e conduzidos pelo órgão central do SMDC, para nivelamento e atualização do conhecimento;
> h) criar instrumentos para viabilizar e motivar a permanência do pessoal especializado nas atividades do Setor Cibernético, permitindo a continuidade da atividade;
> i) realizar parcerias estratégicas e intercâmbio entre as FA e instituições de interesse; e
> j) incluir o conteúdo Defesa Cibernética nos currículos dos cursos, em todos os níveis, no que couber, dos estabelecimentos de ensino do MD.

Assim, infere-se que existe uma preocupação não só no âmbito do Exército Brasileiro, mas do Ministério da Defesa com a capacitação e a gestão de talentos do setor cibernético, escopo deste estudo. Desta feita, a execução de um banco de talentos desde a entrada na Força torna-se imprescindível.

Para tal, ciente desta necessidade no final de 2018, foi aprovada a Diretriz para Implementação do Sistema de Gestão de Talentos (SISGESTA) do Departamento de Educação e Cultura do Exército (DECEx) onde um dos objetivos, dentre outros, é “Implementar, utilizar e manter em constante atualização um Banco de Talentos com informações detalhadas sobre a capacitação real de cada um dos concluintes dos seus cursos e estágios e dos demais integrantes do Sistema de Educação e Cultura do Exército (SECEx)”.

Contudo, o SISGESTA ainda se encontra em fase de implementação não estando ativa nos estabelecimentos de ensino. Além disso, o sistema prevê que a qualquer momento a pessoa inserida possa solicitar sua retirada do banco de talentos e ainda a portaria não trata como seria a implantação desses talentos, ou seja, quais critérios serão utilizados, particularmente nos cursos de formação, onde de acordo com o currículo escolar todos daquela Arma, Quadro ou Serviço terão as mesma informações.

Dessa maneira, feitas estas considerações e a fim de contribuir com a descoberta e gestão de talentos em cibernética na AMAN, abaixo estão algumas sugestões, porém cabe destacar que são ideias e opiniões deste autor e que carecem de maiores estudos a fim de verificar sua viabilidade.

✓ Criação de um banco de dados de cibernética, que permita a inserção dos cadetes destaques especificando motivos, qualidades e qual a área da cibernética aquele militar tem maior afinidade.

✓ Aumentar a carga horária de cibernética II, relativa ao Curso Básico da AMAN, de forma a possibilitar uma melhor observação de possíveis talentos.

✓ Elevar a carga horária de Cibernética IV, voltada ao 3º ano do CCom.

✓ Realização de uma avaliação pelo setor de cibernética do CIGE, a fim de manter a isenção, com os militares destaques e voluntários.

✓ Possibilidade dos cadetes do Curso de Comunicações que se destacaram e que sejam voluntários realizarem o curso de Guerra Cibernética no CIGE durante o 4º ano da AMAN no mesmo período que o Curso de Guerra na Selva.

✓ Realização de palestras na área de pessoal sabidamente especialista no setor;

✓ Realização de estágios de cibernética para os cadetes das outras Armas, Quadro de Material Bélico e Serviço de Intendência de forma a levantar possíveis cadetes com pendor e gosto pela atividade.

✓ Divulgar com maior intensidade as atividades realizadas pelo setor cibernético com o intuito de estimular os cadetes.

✓ Realizar campeonatos de cibernética na AMAN com o intuito de incrementar as capacidades e estimular o interesse pelo assunto e consequentemente aparecimento de talentos.

✓ Fazer com que os cadetes participem de competições nacionais e internacionais na modalidade *capture the flag* (CTF), nome dado a competição entre *hackers* desafiados a desvendar problemas sobre Segurança da Informação.

✓ Fomentar as atividades do grêmio de cibernética da AMAN com a disponibilização de recursos para a realização de maiores atividades.

✓ Constituir uma equipe de cadetes para participar da competição cibernética das Forças Armadas, conhecida por "Manda Byte", estimulando a criatividade e a continuidade na atividade.

✓ Efetivar o ranqueamento dos cadetes dentro das especialidades da cibernética de forma a fornecer dados seguros de seu desempenho.

8 CONCLUSÃO

Do estudo realizado neste trabalho, foi possível chegar a um conjunto de conclusões a respeito de como ocorre a capacitação em cibernética na AMAN e se durante esta atividade ocorre a descoberta de novos talentos para o setor.

Cabe recordar que o trabalho foi dividido em capítulos que tiveram a finalidade de conduzir o leitor a uma possível resposta ao problema formulado, qual seja: “Como contribuir com a capacitação de recursos humanos para o setor cibernético através da descoberta de novos talentos na AMAN?”.

Assim, no capítulo 4 foi estudado com um pouco mais de aprofundamento como se desenrola o ensino da disciplina cibernética na AMAN, aclimatando o leitor as peculiaridades do estabelecimento de ensino, a complexidade do tema, apresentando os dados reais da forma que é realizada a transmissão de conhecimentos e seus objetivos.

Para tal, inicialmente foi apresentado uma nomenclatura básica sobre o tema, bem como as estruturas das Organizações Militares da FTC e suas respectivas capacidades de realizar a Guerra Cibernética, tendo vista que estas OM serão o destino dos futuros Oficiais formados na AMAN.

Na sequência, foi estudado o ensino de Cibernética no Curso Básico verificando que seria necessário um aumento de carga horária, uma vez que esta disciplina só é vista por todos os cadetes de maneira geral no primeiro ano e possui apenas 60 horas/aula dificultando a consecução do objetivo previsto nesta matéria que é de habilitar o futuro oficial a “Atuar como Oficial de Informática e utilizar, de forma segura, dispositivos conectados à rede de computadores”, uma vez que TODOS os Oficiais integrantes da linha bélica atuarão com meios de TI e devem ser capazes de realizar sua Defesa Cibernética minimizando riscos e vulnerabilidades.

Ainda no capítulo 4, foi visto o ensino de Cibernética no Curso de Comunicações e apurou-se que também seria interessante um aumento da carga horária, particularmente para o terceiro ano pela dificuldade dos assuntos tratados e a necessidade de uma maior prática.

Destarte, no Capítulo 5 foi exposto o ensino de Cibernética na Academia Militar dos EUA ou *West Point* de forma detalhada com o propósito de realizar uma comparação, tendo vista aquele país possuir notadamente o Exército mais poderoso

do mundo e consequentemente ser alvo de reprodução de seu modelo de ensino por outros exércitos.

Neste ponto, demonstrou-se que existem várias diferenças entre o ensino da AMAN onde o cerne é o ensino das artes essencialmente militares e o de *West Point* que possui um foco maior nas disciplinas técnico-científicas e de humanas, justificada pelo fato de que diferente da AMAN nem todos os formandos permanecerão naquele Exército.

Dessa maneira, foi mostrado que a Academia Militar dos EUA tem sua essência nas ciências exatas voltadas principalmente nos estudos dos diversos cursos de engenharia voltando assim na criatividade para resolução dos problemas militares com base em tecnologia, facilitando o ensino de cibernética, uma vez que os meios cibernéticos têm como base as ciências exatas para o seu desenvolvimento e execução.

Além disso, a característica prática e exclusiva do ensino de cibernética em West Point permite a formação de recursos humanos com maior capacidade cognitiva para atuar neste setor tão sensível. Portanto, podendo servir de modelo para a AMAN, logicamente respeitando-se suas peculiaridades.

Na sequência, o Capítulo 6 retratou os resultados de um questionário, composto de nove perguntas de múltipla escolha, realizado com os cadetes do segundo, terceiro e quarto anos do Curso de Comunicações da AMAN. Participaram do questionário um total de 110 cadetes, sendo 32 (trinta e dois) do 2º ano, 40 (quarenta) do 3º ano e 38 (trinta e oito) do 4º ano, sendo esse universo escolhido por ter um maior contato com a disciplina ao longo dos quatro anos de formação e desta forma contribuindo de maneira mais efetiva com este trabalho.

Logo, quando realizou-se a análise dos resultados obtidos pelo questionário foi verificado que grande parte dos cadetes reconhecem a importância do setor cibernético e que isto influencia diretamente a escolha pela arma de comunicações, também ratificou-se a necessidade de um aumento da carga horária da disciplina principalmente para os cadetes das demais Armas, Quadro e Serviço.

Ademais, reiterou-se a necessidade de meios que permitam a descoberta, seleção e acompanhamento de talentos no setor cibernética, como por exemplo, um sistema de banco de dados unificado no Sistema de Educação e Cultura do Exército que abarque não somente a cibernética mais outras habilidades permitindo o registro

dessas habilidades dos inúmeros recursos humanos e nos diversos estabelecimentos de ensino do EB como é o caso da Academia Militar das Agulhas Negras.

Por fim no capítulo 7, foram apresentadas algumas sugestões para a seleção de talentos na AMAN, focadas para o setor cibernético, com o objetivo de buscar um aperfeiçoamento do processo, contudo entendendo que algumas das mudanças sugeridas são de difícil implementação e necessitam maiores estudos. Cabe destacar ainda que é notório a preocupação não só no âmbito do Exército Brasileiro, mas do Ministério da Defesa com a capacitação e a gestão de talentos do setor cibernético, demonstrando a importância deste e de futuros estudos sobre este assunto.

Respondendo ao problema formulado verificou-se, ao longo da pesquisa realizada, que **praticamente não existe descoberta de talentos** para o setor cibernético. Comprovada pelo questionário realizado e pelas pesquisas realizadas, gerando grandes oportunidades de melhoria na implementação de atividades que possam dirimir esta dificuldade.

Por fim, pode-se concluir que a capacitação de pessoal tem um papel fundamental na construção do poder cibernético militar e nacional que, aliada a uma estrutura nacional e militar tecnológica pujante e a uma política nacional ampla e eficiente proporcionarão as condições indispensáveis para o fortalecimento da soberania e para a concretização dos interesses do País no cenário interno e no campo político internacional

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil (1988)**. 35. ed. Brasília,

_____. **Política Nacional de Defesa.** 2016.

_____. **Estratégia Nacional de Defesa**. 2016

_____. Ministério da Defesa. **Política de Cibernética Defesa**. Brasília, DF, 2012.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde: segurança cibernética no Brasil/** Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. Brasília, DF, 2014

_____. Ministério da Defesa. **Política de Segurança da Informação para o Sistema Militar de Comando e Controle**. Brasília, DF, 2014.

_____. Ministério da Defesa. **Concepção Operacional do Sistema Militar de Defesa Cibernética**. Brasília, DF, 2015.

_____. Ministério da Defesa. Secretaria de Política, Estratégia e Assuntos Internacionais. **MD51-M-04: Doutrina Militar de Defesa**. 2. ed. Brasília, DF, 2007a.

_____. Ministério da Defesa. **MD31-M-08: Doutrina Militar de Defesa Cibernética**. Brasília, DF, 2014.

_____. Ministério da Defesa. Exército Brasileiro. **EB20-MF-10.102: Doutrina Militar Terrestre.** 1. ed. Brasília, DF, 2014.

_____. Ministério da Defesa. Exército Brasileiro. **EB10-R-05.004: Regulamento da Academia Militar das Agulhas Negras.** Brasília, DF, 2014.

_____. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **Diretriz de Iniciação do Programa da Defesa Cibernética na Defesa Nacional, a cargo do Exército Brasileiro.** Brasília. 2015.

_____. Ministério da Defesa. Secretaria de Coordenação e Organização Institucional – SEORI. Portaria Normativa Nº 2.624/MD, de 7 de dezembro de 2015. **Política Setorial de Defesa.** Brasília. 2015.

_____. Exército. ECEME. **Formatação de trabalhos acadêmicos**. 2. ed. Rio de Janeiro, 2007.

_____. **Port Res Nº 03 Cmt EB, 29 Jun 09**. Institui o Setor Cibernético no EB. Gabinete do Comandante do Exército. Brasília, 2009.

_____. **Port N º 666 Cmt EB, 04 Ago 2010**. Cria o Centro de Defesa Cibernética. Gabinente do Comandante do Exército. Brasília, 2010a.

_____. **Port N º 667 Cmt EB, 04 Ago 2010**. Ativa o Núcleo do Centro de Defesa Cibernética. Gabinente do Comandante do Exército. Brasília, 2010b.

_____. Exército. ECEME. **Elaboração de Projetos de Pesquisa na ECEME.** Rio de Janeiro, 2012.

_____. Exército. AMAN. **Plano de Disciplina Cibernética II.** Resende, 2019.

_____. Exército. AMAN. **Plano de Disciplina Cibernética III.** Resende, 2020.

_____. Exército. AMAN. **Plano de Disciplina Cibernética IV.** Resende, 2020

_____. Exército. AMAN. **Plano de Disciplina Cibernética V.** Resende, 2020

BRASIL. Ministério da Defesa. MD30-M-01: **Doutrina de Operações Conjuntas 1º Volume**. 1. Ed. Brasília, DF, 2011.

BRASIL. Ministério da Defesa. MD35-G-01. **Glossário das Forças Armadas**. 5. Ed. Brasília-DF, 2015.

BRASIL. **INSTRUÇÃO NORMATIVA N º 11-MD/SC-1/EMCFA, DE 17 DE OUTUBRO DE 2013.** Estado-Maior Conjunto das Forças Armadas. Brasília-DF, 2013.

BRASIL. Presidência da República. **Lei Complementar Nº 97**. Brasília, DF, 1999.

BESKOW, David M. KARLEY, Kathleen M. **Segurança Cibernética Social – Um requisito emergente de Segurança Nacional**, Julho-Setembro 2019. *Military Review*.

CARNEIRO, A. S. L. **Capacitação de Recursos Humanos no Exército Brasileiro para a Segurança Cibernética**: desenvolvimento de competências para a atuação em uma Equipe de Tratamento de Incidentes de Rede. Tese (Doutorado em Ciências Militares) –Escola de Comando e Estado-Maior do Exército. Rio de Janeiro, 2012.

CLARKE, Richard A; KNAKE, Robert K. **Cyber War The Next Threat to National Security and What to Do About It.** HarperCollins e-books. Trial version. Disponível em:<http://www.processtext.com/abcepub.html>Acesso em 21Mai.17.

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

FERREIRA, Carlos Alberto de Azeredo. **A Capacitação de Pessoal para o setor cibernético no âmbito da Defesa.** Trabalho de Conclusão de Curso (Especialização em Política, Estratégia e Alta Administração Militar) –Escola de Comando e Estado-Maior do Exército. Rio de Janeiro, 2017.

GRAHAM, Matt. **A Força Cibernética dos EUA – Prevendo a próxima Guerra**, Julho-Setembro 2016. *Military Review*.

USA. USCYBERCOMMAND. U.S. Cyber Command: Mission and Vision. Maryland. Disponível em: <https://www.cybercom.mil/About/Mission-and-Vision/> . Acesso em: 14/07/2020.