ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

Maj Com **ANDRÉ** KOHLER DAMIÃO

A formação curricular do guerreiro cibernético: Análise sobre o perfil profissiográfico do guerreiro cibernético da formação à especialização no Exército Brasileiro

Rio de Janeiro

2021

Maj Com **ANDRÉ** KOHLER DAMIÃO

A formação curricular do guerreiro cibernético:

Análise sobre o perfil profissiográfico do guerreiro cibernético: da formação à especialização no Exército Brasileiro

Trabalho de Conclusão de Curso apresentado à 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: Ten Cel Com ENIO CORRÊA DE SOUZA

Rio de Janeiro

2021

S111a Damião, André Kohler

A formação curricular do guerreiro cibernético:
Análise sobre o perfil profissiográfico do guerreiro cibernético: da formação à especialização no Exército Brasileiro. / André Kohler Damião. – 2021.
60 f. : il. ; 30 cm.

Orientação: ENIO CORRÊA DE SOUZA.
Trabalho de Conclusão de Curso (Especialização em Ciências Militares) — Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2021.
Bibliografia: f. 51-53.

1. PROJETOS ESTRATÉGICOS DO EXÉRCITO. 2. PROJETO GUARANI. 3.GESTAO. I. Título.

CDD 355.4

Maj Com **ANDRÉ** KOHLER DAMIÃO

A formação curricular do guerreiro cibernético:
Análise sobre o perfil profissiográfico do guerreiro cibernético da formação a especialização no Exército Brasileiro

Trabalho de Conclusão de Curso apresentado à 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.

Aprovado em 21 de novembro de 2021.

COMISSÃO AVALIADORA

_____
Enio Corrêa de Souza – Ten Cel Com - Presidente
Escola de Comando e Estado-Maior do Exército

_____
Carlos Otávio Macedo de Sousa– Cel Inf - Membro
Escola de Comando e Estado-Maior do Exército

_____
Marco Antônio Barbosa – Ten Cel Inf - Membro
Escola de Comando e Estado-Maior do Exército

À minha esposa, meus filhos, meus familiares e companheiros do CCEM 1, fontes de inspiração e exemplo.

AGRADECIMENTOS

Primeiramente à Deus, Senhor dos Exércitos, pelo dom da vida, pela esperança nas turbulências, pela paz e saúde que tem me permitido seguir em frente a cada dia que passa.

À minha esposa Juliana pelo incentivo e apoio incondicional, não apenas nesse trabalho, mas em todos os projetos de nossas vidas.

Aos meus filhos Matheus e Luca Gabriel pelo carinho e compreensão nas horas de ausência.

Ao meu orientador, TC Ênio, pelas orientações e correções precisas e, principalmente, pela confiança e incentivo que dispensou a melhorar esse trabalho científico.

RESUMO

A partir do Início do século XXI, com o compartilhamento da internet a nível mundial, o mundo se tornou altamente incerto, volátil e interligado, a Tecnologia da Informação (TI) cada vez mais impulsiona o desenvolvimento, em quase todas as áreas a TI se torna fundamental para o avanço. Porém, o progresso gerado pela conectividade também trouxe problemas inéditos, o espaço cibernético passou a ser disputado como as terras em séculos passados. O termo Guerra Cibernético, antes visto apenas em filmes, já se mostra a tônica para as próximas guerras, junto a ele surgiu outros termos, como “Crime Cibernético”. Assim, os principais países do mundo estão buscando desenvolver essa capacidade, países como Estados Unidos, Rússia, China e Reino Unido estão em estágio avançado de desenvolvimento O Brasil, da mesma forma, caminha para se tornar um dos principais players nesse cenário, desde a Política Nacional de Defesa de 2008, o Brasil tem buscado o avanço no assunto. Portanto, é fundamental a sinergia dos principais atores responsáveis pelo desenvolvimento dessa capacidade estratégica, o Ministério da Defesa e o Exército Brasileiro estão a frente dessa importante missão. O principal local para descoberta de novos talentos é nas escolas de formação, que possuem os tempos dos Planos de Disciplina limitado, por isso, o correto alinhamento do perfil profissiográfico das escolas de formação com a especialização em Guerra Cibernética irá aumentar a velocidade da capacitação nessa área. Esse alinhamento formativo irá maximizar o progresso da capacidade operativa em Proteção, Exploração e Ataque Cibernético.

Palavras-chave: Tecnologia da Informação; Cibernética; Plano de Disciplina; Perfil Profissiográfico.

ABSTRACT

From the beginning of the 21st century, with the huge internet propagation, the world has become highly uncertain, volatile and interconnected. The Information Technology (IT) drives global development more and more and becomes fundamental in almost every area of life. However, the progress generated by connectivity also brought unprecedented problems: cyberspace began to be disputed like land was in past centuries, or worst. The term Cyber War, previously seen only in movies, is already the key for the next wars, other terms also emerged, such as “Cyber Crime”. Thus, the main countries in the world are seeking to develop this capacity, like United States, Russia, China and the United Kingdom are at an advanced stage of development. Brazil, likewise, is on the way to become one of the main players in this scenario. Since the National Defense Policy of 2008, Brazil has sought to advance in the matter. Therefore, the synergy of the main actors responsible for the development of this strategic capacity is essential, the Ministry of Defense and the Brazilian Army are at the forefront of this important mission. The main place for discovering new talents is at the schools, which have limited times of Discipline Plans, so the correct alignment of the professional profile of training schools with the specialization in Cyber Warfare will increase the speed of training in this area. This alignment will maximize the operative capability progress in Cyber Protection, Exploration and Attack.

Keywords: Information Technology; Cybernetics; Discipline Plan; Professional Profile.

LISTA DE ABREVIATURAS

AMAN	Academia Militar das Agulhas Negras
AFA	Academia da Força Aérea
CComGEx	Comunicações e Guerra Eletrônica do Exército
CIGE	Centro de Instrução de Guerra Eletrônica
CDCiber	Centro de Defesa Cibernético
Com D Ciber	Comando de Defesa Cibernética
EB	Exército Brasileiro
EN	Escola Naval
END	Estratégia Nacional de Defesa
ESA	Escola de Sargentos das Armas
EsAO	Escola de Aperfeiçoamento de Oficiais
ENaDCiber	Escola Nacional de Defesa Cibernética
FAB	Força Aérea Brasileira
MD	Ministério da Defesa
MB	Marinha do Brasil
PND	Política Nacional de Defesa
SGCEx	Sistema de Guerra Cibernética do Exército

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

2021

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho tem por finalidade analisar a formação curricular do guerreiro cibernético no Exército Brasileiro (EB), especificamente o perfil profissiográfico do guerreiro cibernético: na formação acadêmica e na especialização no Curso de Guerra Cibernética.

Desde a evolução dos meios de comunicações, a versatilidade do campo de batalha vem se moldando aos avanços tecnológicos. Originada na utopia de filmes e livros da segunda metade do século XX, a dimensão cibernética teve seu ápice no temor apocalítico do possível colapso dos sistemas de comunicação na virada do século, o bug Y2K (o "bug do milênio").

Dessa forma, diversos países buscaram desenvolver essa nova capacidade em seus exércitos. Como exemplo, a Rússia, um dos atuais expoentes na capacidade cibernética, foi acusada em 2007 pelos ataques cibernéticos sofridos pela Estônia. O uso em guerra declarada, teve como principal utilizador novamente a Rússia, que, em 2008, realizou a negação de vários serviços da Geórgia, isolando o sistema informacional georgiano, o que conduziu à vitória russa no conflito.

Outros países, como Estados Unidos da América (EUA), Rússia e China já enxergam a cibernética como uma vertente nova dentro das Forças Armadas. Segundo Pinheiro (2008), no Brasil fica cada vez mais evidente que as atividades de Guerra Cibernética e Segurança da Informação são parcelas relevantes da defesa dos interesses vitais do Estado Nacional Brasileiro. Nesse contexto, foi aprovado em 18 de dezembro de 2018, pelo Decreto nº 6.703, a Estratégia Nacional de Defesa (END), a qual estabeleceu os setores estratégicos e as diretrizes para atuação da Marinha, Aeronáutica e Exército, estabelecendo para o Exército Brasileiro o desenvolvimento do Setor Cibernético.

Em 2010, o Centro de Instrução de Guerra Eletrônica (CIGE) sediou o I Seminário de Defesa Cibernética das Forças Armadas, visando iniciar a coordenação conjunta de implantação da Cibernética no âmbito do Ministério da Defesa. Dessa maneira, foi formada em 2012, no CIGE os primeiros Guerreiros Cibernéticos. Desde então, a cada ano, militares das três Forças aumentam o poder de combate na Guerra Cibernética. Poucos anos mais tarde, a Academia Militar das Agulhas Negras (AMAN) também se atualizou, inserindo na carga horária da formação do Oficial Combatente

a matéria de Cibernética, atualizando, em todos os anos de formação, independente da Arma, Quadro ou Serviço, o Plano Disciplinar (Pladis) com os novos assuntos.

Nesse ínterim, o Ministério da Defesa inaugurou o Centro de Defesa Cibernética (CDCiber) em 2012 e o Exército Brasileiro criou o Comando de Defesa Cibernética (ComDCiber), ambos sediados no Comando de Comunicações e Guerra Eletrônica do Exército (CComGEx), em Brasília-DF. Posteriormente foi criada a Escola Nacional de Defesa Cibernética (ENaDCiber).

Atualmente, a matéria de Cibernética, seja na formação ou no Curso de Guerra Cibernética ainda está sendo moldada, devido, principalmente, à novidade do assunto e à constante mutação das formas de ataque e defesa nesse incógnito ambiente. O perfil profissiográfico do Guerreiro Cibernético começa a ser desenvolvido na formação acadêmica, quando o então cadete recebe uma carga horária pesada de cibernética durante os cinco anos de formação.

Outrossim, mais tarde alguns militares mais vocacionados realizam o Curso de Guerra Cibernética. Aliado a outros, como o de Inteligência Cibernética e o de Proteção Cibernética (em fase de implantação), os cursos se destinam a especializar oficiais e praças das três Forças Armadas. Alguns trabalhos tem sido feito em conjunto, como a Manobra Escolar na AMAN, quando os oficiais alunos do Curso de Guerra Cibernética interagem com os cadetes, realizando ataques e planejando a defesa cibernética em um ambiente simulado operacional. A vigente necessidade exige a coordenação da matéria, principalmente entre as escolas de formação e o CIGE, aperfeiçoando o perfil profissiográfico dos profissionais da área.

Nessa visão, por se tratar de importante vertente, a análise do perfil profissiográfico, da formação à especialização, faz-se necessária para aprimorar as capacidades criadas em ambas as escolas.

A responsabilidade sobre o setor cibernético na Defesa Nacional paira sobre a gerência castrense. Ademais, cada vez mais o cenário internacional exige a habilidade nessa dimensão. Portanto, essa área vem recebendo demanda das três Forças Armadas, dos órgãos públicos e das empresas civis. Assim sendo, cresce de importância a busca que a especialização dos militares do Exército Brasileiro seja feita com o melhor aproveitamento possível, para que possa ter a eficácia requerida pela END.

Nesse contexto, as escolas de formação vêm ensinando desde o primeiro ano de formação a matéria de cibernética. Independente do curso, a cibernética ganha

relevância nos Planos de Disciplinas, guardando o enfoque necessário a cada arma, quadro e serviço.

A questão central e o objeto principal do presente trabalho é a análise do perfil profissiográfico do guerreiro cibernético, por meio de uma pesquisa dos diferentes Pladis, desde a formação até o fim da especialização, considerando também o Curso de Aperfeiçoamento de Oficiais na Escola de Aperfeiçoamento de Oficiais (EsAO), local que fará parte do currículo dos oficiais que se habilitarem a realizar a especialização em Guerra Cibernética.

O problema visualizado é que alguns assuntos podem estar duplicados nos Pladis, outros podem estar sendo ensinados sem a praticidade, que será futuramente necessária, e, ainda, é possível que a base curricular esteja fora de ordem lógica ou faltando algum assunto.

Cabe destacar que, nos últimos anos os diversos Pladis foram atualizados, na tentativa de correlatar os assuntos ministrados, tanto para a melhor performance do guerreiro cibernético, quanto para os militares que não seguirão essa ramificação.

Pontua-se que é importante considerar que o tempo de formação e especialização são limitados por diversas restrições, desde orçamentárias, operacionais e curriculares. Dessa forma, a distribuição mais eficiente dos assuntos, principalmente na formação acadêmica, possibilitará o aumento do desempenho e eficácia do perfil profissiográfico do guerreiro cibernético.

Assim, o presente trabalho de conclusão de curso será desenvolvido em torno do seguinte problema: se os Pladis, de formação e especialização, estão eficientemente alinhados para fornecer a melhor estrutura disciplinar possível ao guerreiro cibernético. Para responder ao problema, será analisado o atual alinhamento do perfil profissiográfico do guerreiro cibernético, desde a matéria de cibernética nas escolas de formação até o curso de especialização no CIGE, propondo, se for o caso, mudanças nos planos de disciplinas das supracitadas escolas.

Para alcançar o objetivo traçado, será seguido um roteiro em que se pretende apresentar um breve histórico da relevância da cibernética no cenário nacional e internacional, apresentar o Pladis, no tocante a cibernética, da escola de formação do guerreiro cibernético e apresentar o Pladis do Curso de Guerra Cibernética. Por último será necessário correlacionar os Pladis, verificando interseções ou lacunas, com o perfil profissiográfico demandando pelo Ministério da Defesa.

2 METODOLOGIA

O presente estudo será realizado, principalmente, por meio de uma pesquisa qualitativa. Segundo a taxionomia de Vergara (2009), esse trabalho será descritivo, pois pretende analisar e descrever a forma como se desenvolve, atualmente, o ensino de cibernética nas diferentes escolas de formação e no curso de especialização. Explicativo, porque visa esclarecer sobre os conceitos básicos em cibernética e o ensino curricular do Guerreiro Cibernético. Por último, será bibliográfico e documental, pois sua fundamentação teórico-metodológico resultará na criação de conhecimento a partir de documentos existentes aberto ao público em geral e alguns documentos de acesso reservado.

Os principais meios de pesquisa serão por meio de questionário aplicado em militares que possuam o curso de Guerra Cibernética, questionário aplicado a militares que ainda não realizaram a especialização e consulta a rede mundial de computadores, manuais, regulamentos, Normas Gerais de Ação, Pladis e Perfil Profissiográfico. A fundamentação teórico-metodológica será baseada na investigação sobre os assuntos relacionados com a base curricular do Guerreiro Cibernético.

A limitação metodológica para o desenvolvimento desse trabalho refere-se ao aos aspectos qualitativos, que se pressupõe uma interpretação dos fenômenos, para só então chegar a uma conclusão. Dessa forma, alguns dos dados serão coletados por meio de entrevista com militares envolvidos na formação e especialização do guerreiro cibernético.

O presente estudo estará limitado ao perfil profissiográfico do guerreiro cibernético no Exército Brasileiro, tendo como linha mestre os Pladis das escolas de formação e de especialização do especialista, considerando, também, os assuntos de cibernética ministrados durante o seu aperfeiçoamento.

Outra importante condicionante é o tempo exíguo de formação e especialização. A eficiência na escolha da carga horária de cada assunto pode resultar na melhor formação ou especialização, melhorando as habilidades e capacidades do militar inclusive em outras áreas, exploradas principalmente durante a formação.

Dessa forma, a boa gestão da carga horária, com a eficiente distribuição no Pladis, tanto na escola de formação, quanto na escola de especialização, trará benefícios não só ao militar, mas principalmente ao Ministério da Defesa.

A seguir, considerando a formação curricular do guerreiro cibernético, será analisado o perfil profissiográfico desse da formação à especialização no EB.

3. A CIBERNÉTICA

Esta seção promove um certame sobre a base conceitual necessária ao entendimento do trabalho. Alguns dos principais termos, conceitos e processos em andamento e finalizados servirão para ambientar o leitor acerca do assunto Cibernética, das atuais aplicações e atual estágio no Brasil e, principalmente, no Exército Brasileiro.

3.1 INTRODUÇÃO A CIBERNÉTICA

"O termo Cibernética foi cunhado por Norbert Wiener, um importante matemático estadunidense que ficou conhecido mundialmente pela publicação do seu livro, em 1948" (CHAVES, 2015). Na segunda edição de seu livro, 13 anos mais tarde, logo no prefácio, Wiener (1961) trata a cibernética, não mais como um programa futurístico, mas como uma ciência.

Um dos conceitos para cibernética, alinhado com o criador do termo Wiener, foi definido por Grenz e Smith:

> A ciência do controle e da comunicação do modo como se relaciona com os mecanismos, indivíduos e sociedades. A cibernética inclui os vários tipos de processos que dependem da troca e do fluxo de informações. Um recurso cibernético é um mecanismo ou sistema que processa informações, tais como um computador ou o sistema de telecomunicações (GRENZ e SMITH, 2005, p. 35)

Inicialmente, a cibernética teve pouco uso prático, a falta de interligação entre os sistemas limitava o espectro que lhe era necessário. Mesmo assim, na década seguinte a Wiener, causou notado impacto, principalmente nas potências mundiais da época União das Repúblicas Socialistas Soviéticas (URSS) e Estados Unidos da América (EUA). MASARO, aborda em seu trabalho científico, os primeiros passos da cibernética como ciência. Aborda, em sua pesquisa, o neurofisiologista Ralph Gerard, que na década de 1950, reafirmava sua surpresa a seus colegas cibernéticos, principalmente alertando sobre o rápido interesse externo (ao seu ambiente de estudo), comparando a uma febre nacional.

Entretanto, foi apenas na década seguinte, com a segunda e terceira geração dos computadores que a cibernética ganhou impulso no cenário internacional. Uma série de exposições, convenções e conferências inseria a cibernética no mundo bi polarizado da Guerra Fria. Em 1965, em *Stuttgart*, a exposição *Computer-Graphik* e a

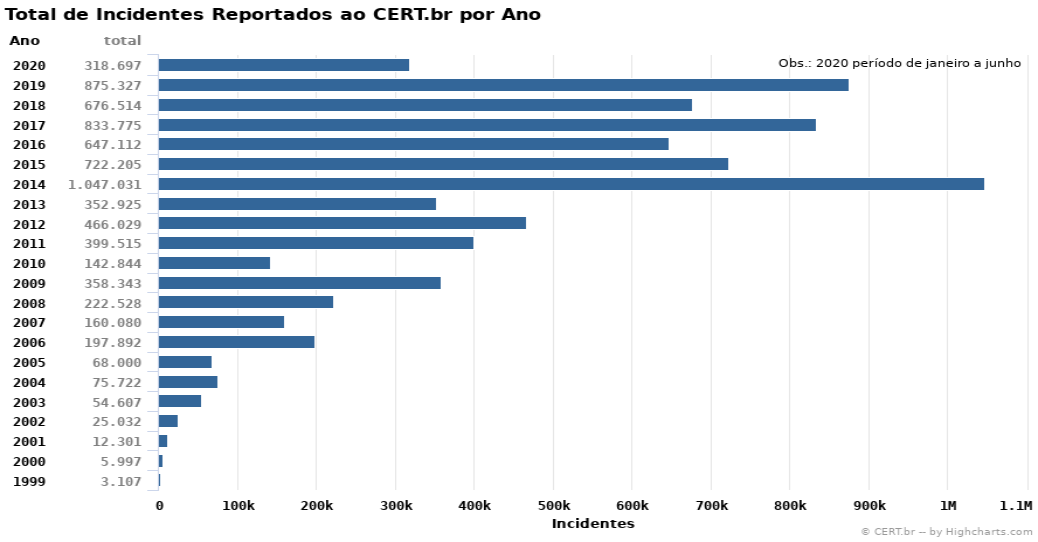
amostra *Cybernetic Serendipity* no Instituto de Arte Contemporânea de Londres em 1968 são exemplos do surgimento da nova ciência, conceituada por Wiener.

A cibernética caminhou praticamente junto com o crescimento da *World Wide Internet*, à medida que esta se desenvolvia, aquela surgia com novas aplicações e usos. O uso da cibernética como meio bélico, fogos não cinéticos, ou como simples hostilidade teve, inicialmente, origem utópica em livros e nas produções cinematográficas do final do século XX. A novela Neuromancer que Willian Gibson publicou em 1984, popularizou a palavra cyber e um mundo utópico e fictício. Filmes como Wargames de John Badham em 1983 e Sneakers de Phil Aden Robinson em 1992 são exemplos da “febre nacional” mencionada por Gerard na década de 1950.

“O ciberespaço está presente em todas as redes de computadores do mundo e em cada coisa a elas conectada, ou por elas controlada. Não é apenas a Internet” (CLARKE, KNAKE, 2015, 64). No capítulo 3 de seu livro, CLARKE e KNAKE relatam a importância da cibernética no campo de batalha. Diversos especialistas elencam a dimensão cibernética com uma das principais, ou até mesmo a única, dentre as que serão utilizadas nas próximas guerras. “É uma zona de guerra, onde muitas das batalhas decisivas do século XXI vão ocorrer” (CLARKE, KNAKE, 2015, 63).

O início do século XXI revelou significativos ataques por meio da utilização da dimensão cibernética. A figura 1 mostra um gráfico que relata a crescente dos ataques cibernéticos reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERTBR). Por meio dessa figura é possível notar o aumento gradativo do uso nocivo da cibernética durante o início do século XX.

FIGURA 1 – Estatísticas dos Incidentes Reportados ao CERT.br de 1999 a 2020



Fonte: CERT.br, 2021

Em meu trabalho científico de conclusão do Curso de Aperfeiçoamento de Oficiais, em 2018, GUERRA CIBERNÉTICA: PROTEÇÃO CIBERNÉTICA - Monitoramento de redes e sistemas e levantamentos de vulnerabilidades - apresentei alguns dos principais ataques do início do século XXI. Em 2007 a Rússia, apesar de negar, utilizou as técnicas *Defacement* e Distributed Denial of Service (DDoS) contra a Estônia. Durante a guerra com a Geórgia em 2008, o “cyber-cerco ao cyberspace georgiano” contribuiu para a vitória russa. Outros como o *Stuxnet* no Irã e o *Wannacry* ficaram mundialmente conhecidos, aumentando a preocupação com a segurança em todos os governos.

3.2 A CIBERNÉTICA NA ATUALIDADE

Atualmente, a cibernética está entre as principais preocupações dos exércitos, exercendo especial pressão sobre os governos em todo o mundo. Alguns criaram um Força Singular separada apenas para a cibernética, outros a incluíram dentro do Exército ou Força Aérea. Independente da forma como a cibernética tem sido utilizada, é importante frisar que é de comum acordo entre os principais especialistas que a cibernética, como fogos não cinéticos, será fundamental para o sucesso em qualquer guerra futura.

Quanto a principal potência militar da atualidade, o Estados Unidos da América criou a “Air Forces Cyber” como vertente militar, devido a importância dada ao assunto. Conforme site oficial da força americana. “Deve oferecer opções soberanas para a defesa dos Estados Unidos da América e seus interesses globais – voar e lutar no ar, no espaço e no ciberespaço” (AFCYBER, 2021). Parte do potencial americano foi descoberto no famoso vazamento efetuado por Edward Snowden “na prática, os documentos de Edward Snowden, juntamente com o que se sabe sobre esses códigos, revelam uma capacidade de espionagem poderosa” (ROHR, 2014).

Outros países, ainda mais avançados as capacidades dessa dimensão, Rússia e China possuem os chamados Exército de Hackers. “Uma das indústrias atacadas pelos hackers seria a aeroespacial, e sites especializados em aviação e defesa levantaram a suspeita de plágio da China para o desenvolvimento dos aviões J-20” (ROHR, 2014). As reais capacidades chinesas permanecem ocultas ao cenário internacional, onde diversas acusações são feitas rotineiramente, principalmente pelo ex presidente americano Donald Trump.

Talvez o principal país, considerando a capacidade cibernética, seja a Rússia. Acusada até mesmo de fraudar eleições americanas, a invasão à Ucrânia mostrou boa parte do potencial russo nessa dimensão. “Forças de segurança da Ucrânia acusaram o Exército da Rússia de ter bloqueado comunicações de telefone celular do país” (BBC, 2014).

Na penúltima eleição americana, na espionagem a agentes britânicos, no monitoramento americano de diversos chefes de governo, inclusive brasileiro, e em muitas outras ocasiões, a dimensão cibernética vem sendo cada vez mais utilizada. Não apenas em vantagens empresariais ou políticas, o espectro foi utilizado em diversos conflitos nos últimos anos, inclusive na atual guerra da Rússia com a Ucrânia, nos quais essa habilidade vem se mostrando fundamental para condução ao êxito.

3.3 A CIBERNÉTICA NO BRASIL

Mandarino e Canongia citam em seu livro a importância da cibernética no contexto internacional e brasileiro:

> “A Segurança Cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria informação, dentre outras. Diante de tais desafios, as Nações vêm se preparando, urgentemente, para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação de governo, bem como de todos os demais segmentos da sociedade. Dessa forma, o entendimento sobre a importância da segurança cibernética caracteriza-se cada vez mais como condição sine qua non de desenvolvimento” (MANDARINO, CANONGIA, 2010, P.13)

Desde que foi elencada como setor estratégico pelo Ministério na Defesa, a cibernética no Brasil tem crescido rapidamente, ganhando proeminência no contexto sul americano e destaque no cenário internacional. De acordo com o site da *Kapersky*, o Brasil é o segundo país que mais recebe ataques cibernéticos.

No dia 05 de julho de 2021 foi publicado no site oficial do governo brasileiro a atualização da União Internacional de Telecomunicações (UIT) – agência especializada em tecnologias de informação e comunicação da Organização das Nações Unidas (ONU), referente a segurança em cibernética relativa ao ano de 2020. O Brasil subiu 53 posições, passou do 71º para o 18º lugar no Índice Global de Segurança Cibernética. Nos países da América, o Brasil ficou atrás apenas dos EUA e Canadá.

De acordo com o do Ministério da Economia, Caio Mario Paes de Andrade:

> “A posição conquistada pelo nosso país demonstra o compromisso crescente do Governo Brasileiro para enfrentar e reduzir as ameaças à segurança cibernética, mesmo diante dos desafios enfrentados com a Covid-19, que exigiram a rápida adaptação das atividades cotidianas e dos serviços socioeconômicos para a esfera digital. O avanço da transformação digital deve vir acompanhado da proteção aos usuários, e nós temos assegurado essa proteção” (ANDRADE, 2021)

A segurança cibernética faz parte do eixo de Governo Confiável, da Estratégia de Governo Digital 2020-2022, o que mostra a importância do assunto para o atual governo. Algumas medidas recentes contribuíram para que o Brasil conseguisse atingir esse destaque no índice, a Lei Geral de Proteção de Dados, em vigor desde 2020, já possui previsão, a partir de agosto de 2021, para aplicar multas sob a chancela da Autoridade Nacional de Proteção de Dados (ANPD), também os decretos nº 9.573, versando sobre a Política Nacional de Segurança de Infraestruturas Críticas e o decreto nº 9.637, que aborda a Política Nacional de Segurança da Informação.

Em no primeiro semestre 2021 o Brasil teve um aumento de 220% na quantidade de ataques cibernéticos. As empresas de energia elétrica foram os principais alvos desses ataques. Em entrevista a CNN, o analista de dados e fundador da startup Business Intelligence e Analytics, Claudio Bonel, relatou que “Os ataques às empresas aumentaram bastante em tempos de pandemia, período em que o trabalho home-office foi implementado em grande escala. Com isso, nós temos um volume maior de acesso remoto”.

Um emblemático ataque cibernético, sofrido pelo Brasil, aconteceu em maio de 2021, a tentativa de invasão ao site do STF causou transtornos administrativos e políticos. Para evitar que o site fosse invadido, os técnicos tiveram que “derrubar” o site, evitando uma escalada do problema. Esses ataques evidenciam a necessidade desse assunto estar contido na PND e END. O Exército Brasileiro tem papel primordial nesse caminho,

3.4 A CIBERNÉTICA NAS FORÇAS ARMADAS

Desde 2008 as Forças Armadas tem estado na vanguarda da implementação da segurança cibernética, não apenas na área de Defesa, mas também sendo pivô de diversas medidas para aumento da segurança em cibernética no Brasil. A criação do CDCiber, ComDCiber e ENaDCiber, dentro do planejamento estratégico do

governo brasileiro, levou as Forças Armadas a estimular a discussão referente ao assunto no âmbito dos órgãos públicos e instituições civis.

Mais voltado para área da Defesa, em 2020 foi criado o Sistema Militar de Defesa Cibernética (SMDC), em cumprimento à Política Cibernética de Defesa, aprovada pela Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012. Elencado como órgão central do sistema o ComDCiber. O SMDC tem por objetivo realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses.

Na figura 2, apresentada pelo manual, encontra-se a divisão dos níveis de decisão, sendo o nível Político as ações são de Segurança Cibernética, Segurança da Informação e Comunicações (SIC). Essas de responsabilidade da Presidência da República e abrangem todo o escopo cibernético no país.

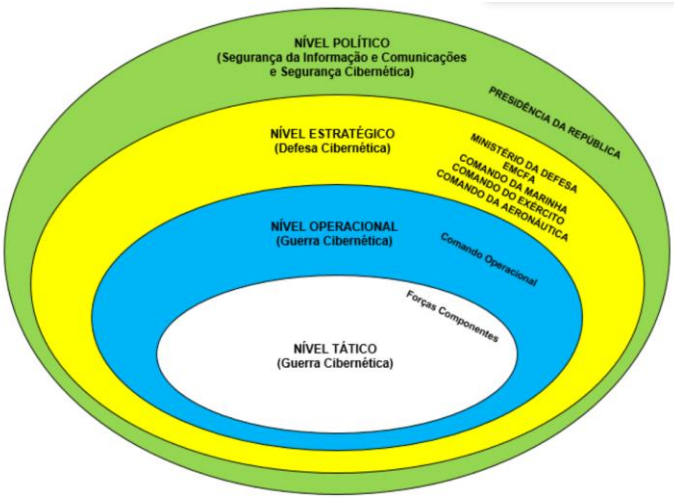


FIGURA 2 – Níveis de decisão em cibernética no Brasil

Fonte: EB70-MC-10.232 - Manual de Guerra Cibernética, 2019

No nível estratégico, coordenado pelo MD e seus entes subordinados, o assunto Defesa Cibernética é inserido, principalmente voltado para capacidade de Proteção Cibernética. Nos níveis Operacional e Tático, a capacidade Guerra Cibernética é inserida como a principal capacidade, sob a responsabilidade do Comando Operacional e Forças Componentes.

O Manual de Guerra Cibernética (2019), define Defesa Cibernética como o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa (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.

Âmbito Ministério da Defesa, foram elencadas as principais capacidades e tarefas a serem desenvolvidas e aperfeiçoadas, visando o preparo e a dissuasão. O EB20-C-07.001 Catálogo de capacidades, dentro da Capacidade Militar Terrestre – 09 – Cibernética, foi definido as 03 (três) Capacidades Operativas da CMT 09: CO35 Exploração Cibernética, CO36 Proteção Cibernética e CO37 Ataque Cibernético. De igual forma, as capacidades foram elencadas no Sistema de Guerra Cibernética do Exército. A descrição das capacidades está no QUADRO 01 abaixo extraído do Catálogo de Capacidades do EB:

QUADRO 1 – Capacidades em cibernética

CAPACIDADE	DEFINIÇÃO
CMT 09 - Cibernética	ser capaz de realizar ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para superar os Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC3) do oponente e defender os próprios. Abrange, essencialmente, as ações de ataque, exploração e proteção cibernética. Essa capacidade mantém estreita ligação com a CO31 Segurança das Informações e Comunicações e com a CMT 08 Operações de Informação.
CO35 - Exploração Cibernética	ser capaz de conduzir ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas.
CO36 - Proteção Cibernética	ser capaz de conduzir ações para garantir o funcionamento dos nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética para neutralizar ataques e exploração cibernética em nossos meios. É uma atividade de caráter permanente.
CO37 - 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, contribuindo para o sucesso das operações.

Fonte – Catálogo de Capacidades do Exército, 2015-2025

Atualmente as três Forças desenvolvem em sinergia a capacidade em cibernética âmbito ComDCiber, que tem 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.

4 A BASE CURRICULAR DA FORMAÇÃO NO EB

O EB conseguiu em pouco mais de dez anos desenvolver uma estrutura, inexistente até o início da década passada, organizada e sistêmica, que permitiu a sinergia do ensino e aplicação. Desde a implantação como setor de defesa, em 2009, o EB, juntamente com as demais Forças, evolui para atingir a capacidade de atuar no espaço cibernético. A principal ferramenta adotada foi o ensino, o início da disciplina nas escolas de formação e os diversos estágios, eletivas e cursos na área fizeram com que o Guerreiro Cibernético tivesse condições adequadas para desenvolver suas habilidades.

O Exército Brasileiro possui duas principais escolas para formação de militares combatentes, a ESA para sargentos e a AMAN para os oficiais. Essas duas são respeitadas instituições escolares, em ambas as escolas o currículo está em constante atualização. A cibernética é uma dessas mudanças, tanto a AMAN, desde a década passada, quanto a ESA, mais recentemente, em 2020. Essas escolas têm buscado moldar seus Planos de Disciplina e Perfis Profissiográfico para se adaptar as diretrizes políticas e estratégicas, a fim de desenvolver a Capacidade Militar em Cibernética.

4.1 A CIBERNÉTICA NA ESA

Na ESA, a implementação da matéria cibernética foi introduzida em 2020, conforme a tabela abaixo, o Pladis do Curso de Comunicações possui 1024 horas destinada às matérias curriculares. A matéria de cibernética possui uma elevada participação percentual na formação do Sargento de Comunicações, mais de 10% do tempo previsto está destinado a matéria específica de Cibernética, conforme o QUADRO 2.

QUADRO 2 - Extrato do PLADIS do Curso de Comunicações da ESA

DISCIPLINA	**Cg H (D+N)**	**Cg H por Disciplina**
OUTRAS	918	918
CIBERNÉTICA	106	106
Cg H atividades de ensino disciplinares	1024	1024

Fonte: PLADIS 2021/CCom ESA.

O atual comandante do CCom/ESA, 2021, o Cap Com Caetano, da turma da AMAN de 2008, em entrevista, relatou que em 2020 a implementação feita pela Cap Com Junqueira, da turma da AMAN de 2007, foi iniciada a matéria para adequar a ESA as novas exigências do campo de batalha. Mesmo que muito recente, por ser 2021 o primeiro ano de efetivo início das instruções, o currículo já foi elogiado pelo atual comandante da EsCom, Cel Com Sandro Silva Cordeiro. Nas palavras do comandante do CCom/ESA, a matéria visa introduzir o futuro sargento de comunicações à cibernética, como assuntos de introdução a redes e proteção, baseado principalmente nos cursos ofertados pela empresa CISCO em parceria com a EsCom.

Incrementando o assunto cibernética, diversas outras matérias possuem como elementos de competência básica – atuar em um ambiente de Guerra Cibernética. Outras matérias, como na disciplina de Emprego das Comunicações, na Unidade Didática (UD) VIII - Sistemas Militares de Comunicações, abordam como um assunto o Sistema de Defesa Cibernético. Diversos outros assuntos permeiam os fundamentos e princípios da cibernética, aumentando consideravelmente o peso do assunto, quando somados, considerando todo o Pladis. Portanto quando somado essas horas extras a carga horária específica, a cibernética passa dos 15% da carga horária efetiva total.

Na disciplina de Cibernética, as 106 horas destinadas são distribuídas conforme as UD do QUADRO 3.

QUADRO 3: Distribuição das UD na Disciplina de Cibernética na ESA.

UNIDADE DIDÁTICA	**NOME**	**Cg H (106h)**
UD I	Introdução a redes	31
UD II	Enlaces de rede	7
UD III	GNU / Linux	24
UD IV	Servidores Linux	32

Fonte: PLADIS 2021 CCom/ESA

Os assuntos ministrados, nas palavras do comandante do CCom/ESA, têm o intuito de introduzir o assunto aos futuros sargentos de comunicações, esses visam principalmente o assunto de proteção cibernética. As capacidades de Ataque e Exploração Cibernético são vistos de maneira mais superficial, na própria matéria e nas eletivas na EsCom e CIGE, divido em três estágios e um curso da CISCO. São eles:

- Estágio de proteção Cibernética na EsCom como matéria optativa;

- Estágio de Guerra Cibernética no CComGEx como matéria optativa.

- Curso da CISCO NETACAD CCNA 2 na EsCom na modalidade EAD ou presencial na ESCOM; e

- Estágio Cybersecurity Essentials na modalidade EAD no Instituto Rondon de Capacitação Continuada.

A intenção atual do Curso de Comunicações da ESA é transformar essas eletivas em Estágios Setoriais de Área.

A competência principal que a disciplina de cibernética se destina na ESA é habilitar o futuro sargento a comandar pequenas frações em Operações de Guerra no amplo espectro (convencional e assimétrica), integrado às Funções de Combate. Nesse escopo mais amplo, alguns elementos foram elencados para compor essa competência, são eles: empregar as Comunicações nas operações militares; instalar e Operar uma Rede de Computadores; Instalar e manter a rede de transmissão de dados; gerenciar a rede de transmissão de dados; e atuar em um ambiente de Guerra Cibernética.

Quanto ao Perfil Profissiográfico do Sargento de Comunicações, dentre as diversas competências, os QUADROS 4 e 5 tiveram por objetivo extrair do perfil as competências atinentes à cibernética.

a. Parte Comum:

QUADRO 4: Parte comum do Perfil profissiográfico do Sargento de Comunicações.

COMPETÊNCIAS PRINCIPAIS	UNIDADES DE COMPETÊNCIA	ELEMENTOS DE COMPETÊNCIA
Realizar atividades cotidianas e administrativas nas Organizações Militares.	Planejar o emprego e comandar pequenas frações em operações no amplo espectro, em situação de guerra e de não guerra.	Atuar em ambiente de guerra cibernética.

Fonte: Perfil Profissiográfico do Sargento de Comunicações da ESA.,

b. Parte específica:

QUADRO 5: Parte específica (extrato) do Perfil profissiográfico do Sargento de Com.

COMPETÊNCIAS PRINCIPAIS	UNIDADES DE COMPETÊNCIA	ELEMENTOS DE COMPETÊNCIA
Comandar pequenas frações em operações no amplo espectro em situações de Guerra e de Não Guerra, integrando às funções de combate	Atuar como chefe do grupo de Centro de Controle de Sistema, em uma Seção do Centro de Comunicações.	Atuar em um ambiente de guerra cibernética
		Realizar a Proteção Cibernética das redes do escalão considerado.

Fonte: Perfil Profissiográfico do Sargento de Comunicações da ESA.

Como conclusão parcial, nota-se a preocupação da ESA em se atualizar quanto a cibernética. A implementação da nova disciplina atende as diretrizes governamentais estratégicas, principalmente na área de Defesa. Devido ao menor tempo de formação, o Sargento de Comunicações tem seu PLADIS voltado para introdução e proteção cibernética, principalmente quanto ao assunto de redes e sistemas operacionais.

4.2 A CIBERNÉTICA NA AMAN

A formação do oficial de carreira combatente dura cinco anos, tem como propósito de formar os oficiais da Linha Bélica nas Armas de Infantaria, Cavalaria, Artilharia, Engenharia e Comunicações, no Serviço de Intendência ou no Quadro de Material Bélico. Em todas as Armas/ Cursos ocorre sólida formação humanística, científica e tecnológica, aspectos considerados essenciais para o prosseguimento na carreira militar (Almeida, 2019).

O primeiro ano na EsPCEx, que serve como uma ambientação do meio militar, o cadete irá ter as primeiras instruções militares, aliadas ao estudo acadêmico. que visa “propiciar ao aluno o conhecimento militar comum a todos os cursos” (Almeida, 2019). Por último, três anos dentro das Armas, Quadro e Serviço (Infantaria, Cavalaria, Artilharia, Engenharia, Intendência, Comunicações e Material Bélico).. A grade curricular acadêmica, além da matéria militar, a Linha de Ensino Militar Bélica, inclui também as matérias comuns nas áreas de exatas, sociais e humanas.

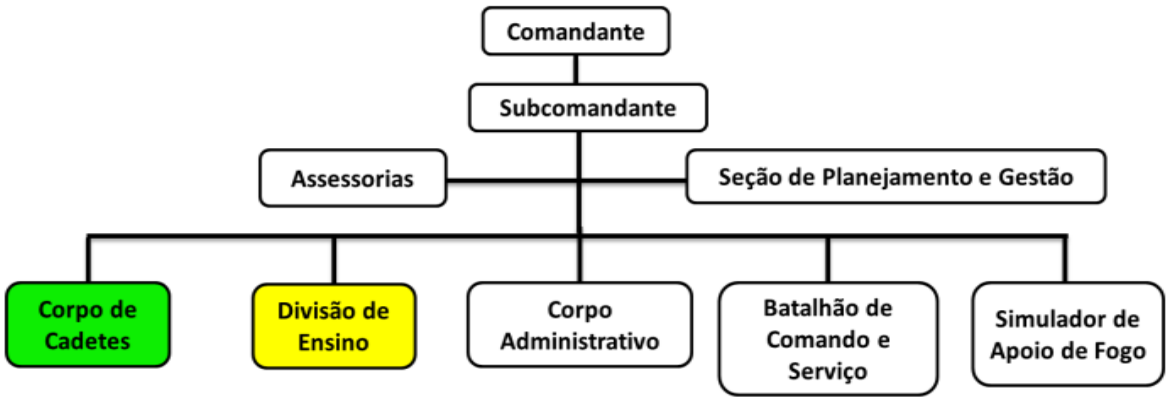
A divisão das três fases da formação do oficial combatente está previsto no Regulamento Interno da AMAN:

> 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 nãoaperfeiçoado 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. (EB10-R-05.004, 2014)

Para entender como a cibernética na AMAN se desenvolve, é importante entender a organização interna, a FIGURAS 3, mostra o organograma da AMAN.

FIGURA 3 – Organograma da AMAN

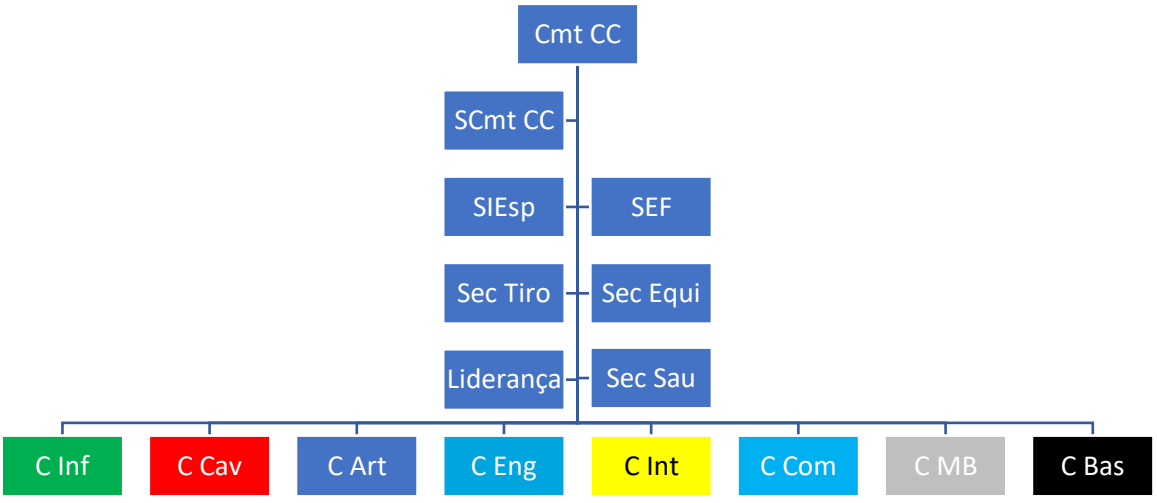


Fonte: Almeida, 2019

Para efeitos desta pesquisa, será utilizado a subdivisão das seções Corpo de Cadetes de Divisão de Ensino. O Corpo de Cadetes é responsável pela formação atitudinal e militar dos futuros oficiais combatentes. Algumas matérias são ministradas pelos instrutores do Corpo de Cadetes, como Liderança, Equitação, Treinamento Físico e as matérias bélicas, visando o desenvolvimento das áreas cognitiva, psicomotora e afetiva. As instruções a cargo do Corpo de Cadetes é "orientar o futuro oficial quanto ao prosseguimento dos estudos necessários para os cargos de Capitão aperfeiçoado e para os de postos mais elevados" (Almeida, 2019).

Na FIGURA 4 podemos ver a subdivisão do Corpo de Cadetes.

FIGURA 4 – Organograma do Corpo de Cadetes.



Fonte: Autor.

A área acadêmica comum fica sob a responsabilidade da Divisão de Ensino, algumas matérias da parte comum são: Direito, Psicologia, Sociologia, Idiomas, História Militar Geral e do Brasil, Metodologia do Ensino Superior, Iniciação à Pesquisa Científica, Direito Penal Militar, Direito Administrativo, Relações Internacionais, Geopolítica, Administração, entre outras.

Em 2011 a cibernética foi inserida no Plano de Disciplina da AMAN, iniciando os trabalhos em 2012. Inicialmente foi subdividida em Cibernética I, II, III, IV e V, uma para cada ano de formação, as primeiras instruções foram ministradas por militares não especializados, da própria escola, principalmente do Curso de Comunicações. Aos poucos o Pladis foi sendo moldado e, atualmente, a AMAN conta com militares possuidores do curso de Guerra Cibernética, uma cadeira própria e salas dotadas de equipamentos de última geração.

Atualmente a cibernética está inserida tanto nas instruções comuns da Divisão de Ensino, com a disciplina Cibernética II, que juntamente com a Cibernética I, ministrada na EsPCEx, destina-se a todos os cadetes, independente do curso. A partir do da entrada nas Armas, Quadro ou Serviço, a Linha Bélica de Ensino, apenas o Curso de Comunicações continua com a matéria, com as Cibernéticas III, IV e V, respectivamente nos 2º, 3º e 4º ano. A FIGURA 5 mostra a divisão das matérias, dentro de cada Seção de Ensino, incluindo a cibernética na Seção D de Ensino.

FIGURA 5 – Organograma Divisão de Ensino

Fonte: Almeida, 2019.

A evolução do ensino em cibernética na AMAN, seguiu as diretrizes do Cmt do EB, conforme o Plano Estratégico do Exército 2020-2023, visando o aperfeiçoamento nesta capacidade, o Objetivo Estratégico do Exército OEE 4 – tem por meta atuar no espaço cibernético com liberdade de ação. Para alcançar esse OEE, foi elencado duas ações estratégicas, 4.1.1 - Implantar o Sistema Militar de Defesa Cibernética (SMDC) e 4.2.1 - Implantar a estrutura de defesa e guerra cibernética. Conforme FIGURA 6, que consta as atividades necessárias para atingir as ações estratégicas definidas da Capacidade Cibernética, sob a égide do MD, juntamente com outros órgãos políticos e setoriais.

FIGURA 6 - OEE 4 - ATUAR NO ESPAÇO CIBERNÉTICO COM LIBERDADE DE AÇÃO

OEE 4 - ATUAR NO ESPAÇO CIBERNÉTICO COM LIBERDADE DE AÇÃO					
Estratégia	**Ação Estratégica**	**Atividades**	**Capacidade Militar Terrestre**	**Prg/Pjt**	**Rspnl/ Intrs**
4.1 Implantação do Setor Cibernético na Defesa	**4.1.1 Implantar o Sistema Militar de Defesa Cibernética (SMDC).**	4.1.1.1 Estruturar(1) o Sistema Militar de Defesa Cibernética (SMDC). (2020-2023)	**CIBERNÉTICA**	**Defesa Cibernética na Defesa Nacional**	**MD EME DCT DEC DECEx COTER DGP SEF COLOG Gab Cmt Ex**
		4.1.1.2 Implantar(1) o Comando de Defesa Cibernética. (2020-2023)			
		4.1.1.3 Implantar(1) a Escola Nacional de Defesa Cibernética. (2020-2023)			
		4.1.1.4 Aumentar a capacidade cibernética nacional de interesse da Defesa. (2020-2023)			
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.

Conforme mostra a figura, a maioria das atividades já iniciaram, desde 2012, na AMAN a cibernética vem se moldando para aumentar a capacidade cibernética nacional de interesse da Defesa (Atividade 4.1.1.3):

> “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” (SALUSTRIANO, 2020)

O ensino durante a formação do oficial está divido entre duas escolas. Na Escola Preparatória de Cadetes do Exército (EsPCEx) a Cibernética I (“Introdução à Computação”) visa a formulação da base e fundamentos para a matéria. Atualmente, estuda-se retirar do Pladis da EsPCEx a referida matéria e fundir com os assuntos ministrados no primeiro ano da AMAN. O QUADRO 6 apresenta um extrato do Pladis da EsPCEx e a respectiva carga horária.

QUADRO 6 – Extrato do Pladis da EsPCEx

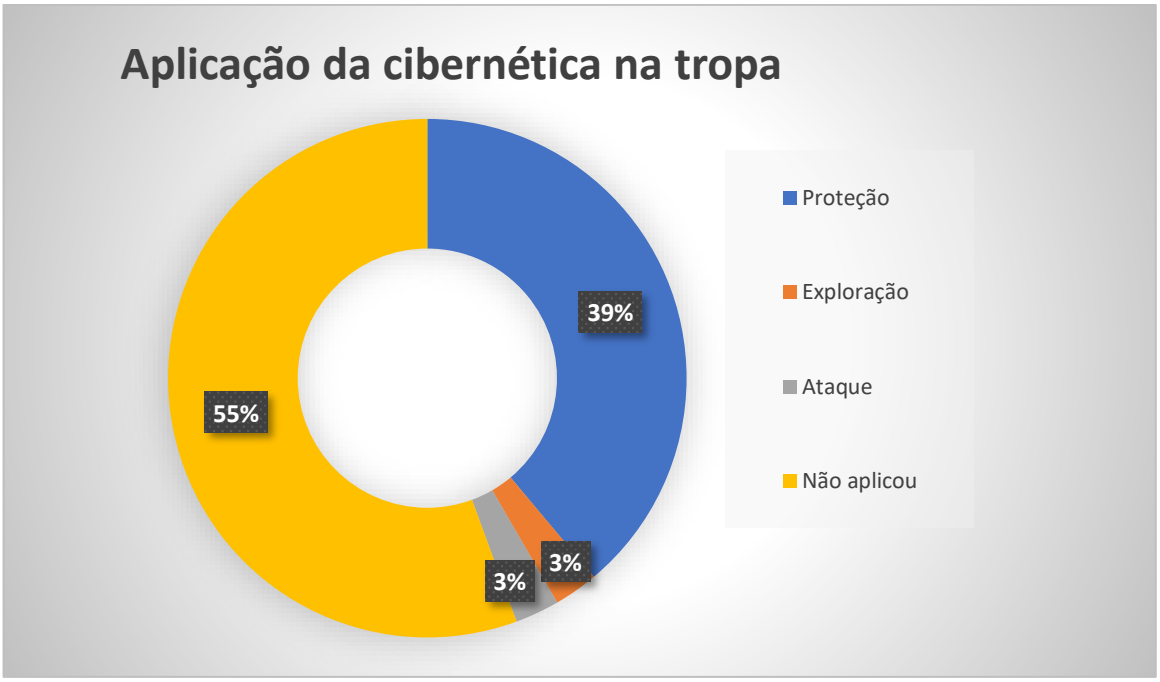
DISCIPLINA: INTRODUÇÃO À COMPUTAÇÃO		**Cg H Total**: 60 h
UNIDADE DE COMPETÊNCIA: Atuar como Oficial de Informática		
ELEMENTOS DE COMPETÊNCIA: Aplicar a segurança da informação. Orientar as atividades ligadas à gerência de redes		
UD	**ASSUNTO**	**OBJETIVO**
UD I: Raciocínio Lógico	a. Proposições e Conectivos: conceito de proposição; valores lógicos das proposições; proposições simples e proposições compostas; conectivos; tabela-verdade; notação.	- Descrever proposições e conectivos; - Determinar os valores lógicos das proposições; - Compreender o significado de tabela-verdade.
	b. Operações Lógicas sobre Proposições: negação; conjunção; disjunção; disjunção exclusiva; condicional; bicondicional.	- Compreender as operações lógicas sobre proposições; - Realizar as operações lógicas sobre proposições.
	c. Construção de tabelas-verdade: tabela-verdade de uma proposição composta; número de linhas de uma tabela-verdade;. construção da tabela-verdade de uma proposição composta; valor lógico de uma proposição composta; uso de parêntesis	- Construir a tabela-verdade de uma proposição composta.
	d. Tautologias, Contradições e Contingências.	- Definir tautologias, contradições e contingências.
	e. Implicação Lógica: definição; propriedades; tautologias e implicação lógica.	- Definir implicação lógica; - Descrever as propriedades da implicação lógica.
	f. Equivalência Lógica: definição; propriedades; tautologias e equivalência lógica.	- Definir equivalência lógica; - Descrever as propriedades da equivalência lógica.
	g. Argumentos e Regras de Inferência: definição de argumento; validade de um argumento; critério de validade de um argumento; condicional associada a um argumento; regras de inferência.	- Definir argumentos ; - Citar as regras de inferência; - Descrever a validade de um argumento e seus critérios; - Empregar as regras de inferência.
	h.Validade de Argumentos: validade mediante tabelas-verdade; validade mediante regras de inferência	- Examinar a validade de um argumento.
	i. Quantificadores: quantificador universal; quantificador existencial.	- Descrever quantificadores.

UD II: Algoritmo	a. Introdução a Algoritmo: conceito de algoritmo; algoritmos e a lógica de programação; tipos de algoritmos	- Conceituar algoritmo; - Descrever as relações entre algoritmos e a lógica de programação; - Compreender os tipos de algoritmos.
	b. Variáveis, Constantes e Tipos de Dados:	- Definir variáveis e constantes; - Citar os tipos de dados.
	c. Operadores: operadores aritméticos; operadores relacionais; operadores lógicos	- Reconhecer operadores aritméticos, relacionais e lógicos; - Identificar a precedência entre os operadores; - Compreender a aplicação dos operadores na construção de algoritmos.
	d. Entrada e Saída: comandos ou funções de entrada e saída.	- Compreender a aplicação dos comandos/funções de entrada e saída na lógica de programação
	e. Condicionais: condicional simples; condicional composta	- Identificar os tipos de condicionais ; - Compreender a aplicação de condicionais na construção de algoritmos
	f. Introdução à Iteração: estruturas de repetição.	- Descrever iteração; - Compreender a aplicação da iteração na construção de algoritmos
	g. Controle de Fluxo de Instruções: conceito de controle de fluxo de instruções; tipos de controle de fluxo de instruções.	- Conceituar controle de fluxo de instruções; - Citar os tipos de controle de fluxo; - Compreender o controle de fluxo na construção de algoritmos e na lógica de programação
	h. Funções e Procedimentos: definição de funções; definição de procedimentos; aplicação de funções e procedimentos; benefícios da modularização de um programa.	- Definir funções e procedimentos. - Aplicar os conceitos de funções e procedimentos na elaboração de algoritmos (modularização)
	i. Desenvolvimento de Algoritmos: construção de algoritmos; implementação de algoritmos (construção de programas de computador).	- Desenvolver algoritmos, empregando os conceitos apreendidos; - Implementar algoritmos em uma linguagem de programação (construção de programas de computador)

Fonte: Pladis EsPCEx, 2020.

Outrossim, no primeiro ano da AMAN, Curso Básico, é ministrado a Cibernética II pela cadeira de Cibernética, sendo que está matéria está prevista uma mudança para em 2023 virar Cibernética I (mesclando os assuntos da atual Cibernética I e II). Atualmente, tem por objetivos preparar o futuro Oficial para utilizar de forma segura dispositivos de TIC (notebook, desktops, smartphones, tablets, etc.) conectados, ou não, a redes de computadores e preparar o futuro Oficial para a função de Oficial de Informática das OM do corpo de tropa. A principal capacidade a ser desenvolvida nessa fase da formação é a Proteção Cibernética, o que conforme pesquisa aplicada, no questionário B, GRÁFICO 1, é a principal capacidade aplicada pelos oficiais na tropa, inclusive pelos que fizeram o Curso de Guerra Cibernética.

GRÁFICO 1 – Aplicação da cibernética na tropa.



Fonte: Questionário B, Autor.

No QUADRO 7, está lançado os assuntos ministrados na Cibernética II.

QUADRO 7 – Extrato Pladis 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: Salustriano, 2020

A carga horária destinada a Cibernética II é de 60 horas, juntamente com a Cibernética I são as únicas que todos os cadetes realizam, independente da arma, quadro ou serviço. Após esse conhecimento básico no assunto, basicamente assuntos sobre segurança e legislação, apenas os cadetes de comunicações irão participar das próximas matérias Cibernética III, IV e V.

Quando ingressam no segundo ano da AMAN, na arma de Comunicações, os cadetes iniciam a Cibernética III. Essa capacita o futuro oficial a estruturar, do rascunho à instalação, a estrutura física e lógica de uma rede de computadores (até a camada 4 do modelo TCP/IP), enquadrado em um cenário tático, onde, a partir do qual, deve solucionar situações-problema, o QUADRO 8 demonstra a importância da matéria, passando de um terço das matérias militares do Plano de Disciplina do cadete do 2º ano.

QUADRO 8 – Carga Horária Pladis do 2º ano do Curso de Comunicações da AMAN

DISCIPLINA	**Cg H por Disciplina**	**Porcentagem**
OUTRAS	233	66%
CIBERNÉTICA	120	34%
Cg H atividades de ensino militar	353	100%

Fonte: PLADIS 2021/CCom AMAN.

A Cibernética III possui 120 horas-aula, 34,09% das 353 horas destinadas para as disciplinas militares da formação do cadete do 2º ano de Comunicações.

Possui por competência, os elementos:

- Planejar e coordenar um sistema de gerenciamento eletrônico de mensagens e de uma rede de dados com enlace físico e sem fio (Pel C Com)

- Planejar e gerenciar o emprego de um Módulo de Telemática Op (MTO).

No QUADRO 9 estão as três Unidades Didáticas da Cibernética II e a distribuição das 120 horas.

QUADRO 9 – Extrato do Pladis do 3º ano do Curso de Comunicações da AMAN.

UD I: Cisco Certified Network Associate I (CCNA I)	**Cg H: 40**		**OBJETIVOS DA APRENDIZAGEM / EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. O impacto das redes de computadores em nossas vidas	04	01	- Compreender a importância das redes de computadores no nosso cotidiano. (CONCEITUAL)
b. Características da arquitetura de rede	06	01	- Descrever as características das arquiteturas de rede: tolerância a falhas; escalabilidade; qualidade do serviço; segurança. (FACTUAL)

c. Estrutura de rede modelo OSI e TCP/IP	06	02	- Compreender a estrutura de rede conforme os modelos OSI e TCP/IP e as suas camadas. (CONCEITUAL) - Compreender o funcionamento da Camada OSI e os respectivos protocolos. (CONCEITUAL)
d. IPV4	06	02	- Compreender o funcionamento do protocolo IPV4 e a respectiva divisão de IPs. (CONCEITUAL)
e. Endereçamento IP, redes e sub-redes	06	02	- Compreender a divisão de redes e sub-redes. (CONCEITUAL)
f. *Unicast, multicast e Broadcast*	06	01	- Compreender os conceitos e funcionamento na rede das conexões unicast, multicast e broadcast. (CONCEITUAL)
g. Ferramenta de emulação/simulação de rede	06	01	- Realizar a instalação, configuração e conhecer as ferramentas de emulação/simulação de rede. (PROCEDIMENTAL). **ET – DEDICAÇÃO**
UD II: Cisco Certified Network Associate II (CCNA II)	**Cg H: 64**		**OBJETIVOS DA APRENDIZAGEM / EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. Funcionamento de *switches*	06	-	- Compreender qual o papel do switch no funcionamento de uma rede. (CONCEITUAL) - Compreender o que é um switch e identificá-lo. (CONCEITUAL)
b. Gerenciamento de *switches*	06	-	- Realizar as configurações básicas de um switch. (PROCEDIMENTAL)
c. Tabela MAC	04	-	- Compreender o funcionamento da tabela MAC. (CONCEITUAL) - Identificar uma tabela MAC. (FACTUAL)
d. Gerenciamento avançado de switch	06	-	- Realizar as configurações de um switch necessárias desde o terminal até a integração com o roteador, abordando as configurações de interface e porta. (PROCEDIMENTAL)
e. Funcionamento de roteadores	04	-	- Compreender qual o papel do roteador no funcionamento de uma rede. (CONCEITUAL) - Identificar um roteador. (FACTUAL) - Definir o que é um roteador (CONCEITUAL)
f. Gerenciamento de roteadores	04	-	- Realizar as configurações básicas de um roteador. (PROCEDIMENTAL)
g. Tabela de roteamento	06	-	- Compreender o funcionamento da tabela de roteamento. (CONCEITUAL) - Identificar uma tabela de roteamento. (FACTUAL)
h. LAN, WAN e MAN	04	-	- Compreender as diferenças entre LAN, WAN e MAN (CONCEITUAL) - Realizar as configurações necessárias para a integração switch-roteador de forma a construir uma LAN funcional. (PROCEDIMENTAL)
i. Roteamento estático	06	-	- Compreender como funcionam os protocolos de roteamento. (CONCEITUAL) - Realizar as configurações necessárias para a integração terminal-*switch*-roteador de forma a deixar uma WAN funcional utilizando-se do roteamento estático. (PROCEDIMENTAL)
j. Roteamento dinâmico (RIP/OSPF)	06	-	- Realizar as configurações necessárias para a integração terminal-*switch*-roteador de forma a deixar uma WAN funcional utilizando-se do roteamento dinâmico. (PROCEDIMENTAL)
k. Wrapping-Up	12	16	- Elaborar um diagrama que mostre, no modo simulação, a aplicação dos protocolos da camada de Enlace do modelo OSI. (PROCEDIMENTAL)

			- Elaborar um diagrama que mostre, no modo simulação, a aplicação dos protocolos da camada de Rede do modelo OSI. (PROCEDIMENTAL) - Elaborar um diagrama que mostre, no modo simulação, a aplicação dos protocolos da camada de Transporte (TCP, UDP) do modelo OSI. (PROCEDIMENTAL) **ET – DECISÃO**
UD III: Infraestrutura de Rede	**Cg H: 10**		**OBJETIVOS DA APRENDIZAGEM/EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. Infraestrutura de rede	10	04	- Identificar os tipos de cabo de par trançado (UTP e STP) e suas categorias; (FACTUAL) - Distinguir os tipos conexões do cabo de par trançado (direta e crossover); (CONCEITUAL) - Identificar as características de um cabo de par trançado num *datasheet*; (FACTUAL) - Definir e identificar os tipos de emenda de cabo de par trançado; (CONCEITUAL e FACTUAL) - Realizar a crimpagem de cabo UTP para formar cabo *straight*, *through* ou *crossover*; (PROCEDIMENTAL) - Operar corretamente o testador de cabo de par traçado para verificar a qualidade da conexão. (PROCEDIMENTAL) **ET – INICIATIVA**

Fonte: PLADIS 2021/CCom AMAN.

A diferença entre os objetivos da Cibernética I e II com a Cibernética III ficam claras quando observamos os verbos dos objetivos, no lugar de definir, identificar ou conhecer, surgem os verbos compreender, realizar, elaborar e distinguir. Os assuntos estão intrinsecamente ligados com a introdução no assunto de Proteção Cibernética de Redes a ser aperfeiçoa na Cibernética III, uma capacidade que certamente será utilizada pelos futuros oficiais de comunicações, principalmente na missão doutrinária, Instalar, Explorar, Manter e Proteger os Sistemas de Comunicações do comando enquadrante.

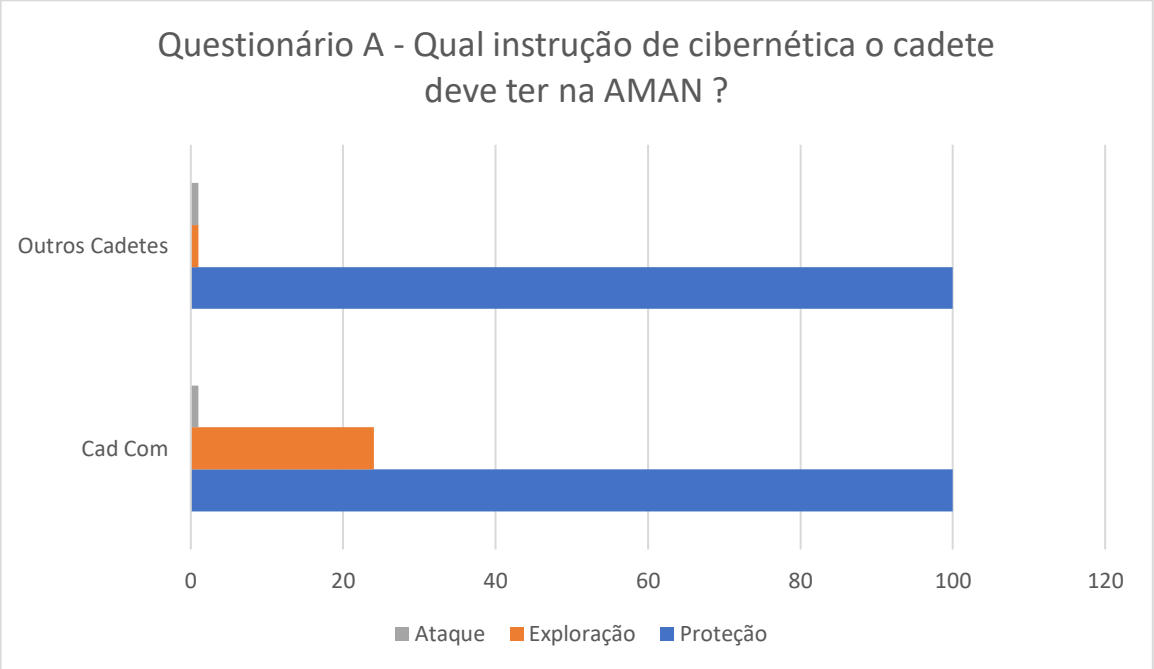
No terceiro ano da AMAN, o cadete de comunicações mais amadurecido ingressa na Cibernética IV. Nesse estágio, a matéria de cibernética ganha maior complexidade. o futuro oficial tem que aprender a operar com virtualizadores (economia de recursos), levantar os serviços fundamentais para o funcionamento pleno de uma rede (DHCP, DNS, Web, FTP e NTP) e, por fim, a proteção sumária da mesma a partir da configuração de um firewall local dada uma situação-problema.

No Pladis da Cibernética IV, fica evidente o aumento do grau de complexidade. A competência principal fica semelhante, nesse caso, comandar frações em situação de guerra, integrado às funções de combate. A Unidade de competência e Elementos de competência modificam para:

> **“UNIDADES DE COMPETÊNCIA:**
> - Planejar e conduzir o emprego da fração em operações convencionais, comandando os pelotões de comunicações orgânicos da Cia Com/Bda e Btl Com/DE;
> **-** Planejar e conduzir o emprego da fração em operações não convencionais, comandando um pelotão de comunicações em operações de resistência e integrando força expedicionária;
> **ELEMENTOS DE COMPETÊNCIA:**
> - Planejar e coordenar um sistema de gerenciamento eletrônico de mensagens e de uma rede de dados com enlace físico e sem fio (Pel C Com)
> - Gerenciar um sistema de comando e controle em apoio às operações integrando força expedicionária.” (AMAN, 2021)

No Questionário A, aplicado aos oficiais que já possuem o Curso de Guerra Cibernética, fica claro a importância dada a proteção cibernética. Como visto no GRÁFICO 2, todos que preencheram a pesquisa deram importância para a matéria ministrada e praticada em Cibernética III e IV.

GRÁFICO 2 – Instruções que o cadete deve ter na AMAN



Fonte: Questionário A, autor.

No QUADRO 10, na matéria de cibernética IV, o principal verbo é o “executar”, os assuntos aprendidos das matérias anteriores servem de base para a prática no assunto, juntamente com as novas matérias. Nessa fase da formação, a Proteção Cibernética de redes ganha importância, tornando-se fundamental para aprendizagem e aplicação futura.

QUADRO 10 – Extrato Pladis 3º ano CCom/AMAN

UD I: Gerenciamento de Máquinas Virtuais	**Cg H: 4**		**OBJETIVOS DA APRENDIZAGEM / EIXO TRANSVERSAL**
ASS	**D**	**N**	
a. Máquinas virtuais	04	-	- Compreender conceitos básicos de virtualização de sistemas operacionais. (CONCEITUAL) - Realizar o *download* e instalação de um virtualizador. (PROCEDIMENTAL) - Realizar a instalação do pacote de extensões. (PROCEDIMENTAL) - Compreender os parâmetros de configuração disponíveis na interface de um virtualizador. (CONCEITUAL) - Executar procedimentos para a criação de uma máquina virtual. (PROCEDIMENTAL) - Executar o *Snapshot* de uma máquina virtual. (PROCEDIMENTAL) - Compreender os tipos de inicialização e desligamento de uma máquina virtual. (CONCEITUAL) - Executar o gerenciamento de mídias virtuais. (PROCEDIMENTAL) - Realizar a clonagem de máquinas virtuais. (PROCEDIMENTAL) - Compreender os tipos de adaptadores de rede existentes. (CONCEITUAL) - Realizar a configuração do adaptador de uma máquina virtual a partir de um contexto específico. (PROCEDIMENTAL) - Executar a instalação dos adicionais de visitante. (PROCEDIMENTAL) - Realizar a configuração da área de transferência compartilhada. (PROCEDIMENTAL) - Realizar a configuração da pasta compartilhada com o *host.* (PROCEDIMENTAL) - Realizar a configuração do acesso de dispositivos USB à máquina virtual. (PROCEDIMENTAL) - Realizar operações de máquinas virtuais em interface de linha de comando. (PROCEDIMENTAL) **ET – OBJETIVIDADE**
UD II: Administração de Sistemas Linux	**Cg H: 10**		**OBJETIVOS DA APRENDIZAGEM / EIXO TRANSVERSAL**
ASS	**D**	**N**	
a. Instalação do Sistema Linux	01	-	- Executar a instalação de um sistema operacional Linux. (PROCEDIMENTAL) - Executar a configuração do gerenciador de repositório de pacotes no Linux. (PROCEDIMENTAL) - Executar a verificação e a atualização das aplicações do sistema. (PROCEDIMENTAL)
b. Sistema de Arquivos do Linux	01	-	- Compreender a arquitetura do *Filesystem Hierarchy Standard* (FHS). (CONCEITUAL) - Compreender a utilização dos comandos e suas respectivas ajudas no sistema. (CONCEITUAL) - Compreender o funcionamento das permissões de arquivos. (CONCEITUAL) - Executar a manipulação de permissões de arquivos. (PROCEDIMENTAL) - Executar o redirecionamento de entrada e saída. (PROCEDIMENTAL) - Executar a criação de diretórios. (PROCEDIMENTAL) - Executar a cópia de arquivos e diretórios. (PROCEDIMENTAL)

			- Executar a movimentação e a remoção de arquivos e diretórios. (PROCEDIMENTAL) - Executar a listagem e a busca de arquivos e diretórios. (PROCEDIMENTAL)
c. Editores de Texto	01	-	- Compreender o emprego de editores de texto no sistema operacional Linux. (CONCEITUAL) - Executar a operação do editor de texto *nano*. (PROCEDIMENTAL) - Executar a operação do editor de texto vi. (PROCEDIMENTAL)
d. Configuração de Rede	02	-	- Compreender os arquivos de configuração de redes do sistema operacional Linux. (CONCEITUAL) - Executar a configuração de rede do sistema operacional Linux a partir da edição dos arquivos de configuração. (PROCEDIMENTAL) - Empregar as ferramentas *ping, nslookup, route, netstat* e *traceroute* para o diagnóstico da rede. (PROCEDIMENTAL)
e. Gerenciamento de Usuários e Grupos	02	-	- Compreender a função dos arquivos */etc/passwd*, */etc/shadow* e */etc/group* no gerenciamento de usuários. (CONCEITUAL) - Executar a criação e remoção de usuários a partir de parâmetros estabelecidos. (PROCEDIMENTAL) - Executar a criação e remoção de grupos a partir de parâmetros específicos. (PROCEDIMENTAL) - Empregar o comando *passwd* no gerenciamento de senhas. (PROCEDIMENTAL) - Compreender o protocolo de serviço de acesso remoto seguro no controle de acesso remoto a *hosts*. (CONCEITUAL) - Empregar o protocolo de serviço de acesso remoto seguro no gerenciamento remoto de servidores. (PROCEDIMENTAL)
f. Gerenciamento de *Backup*	01	-	- Compreender a importância do emprego de *backup* no contexto da segurança da informação. (CONCEITUAL) - Compreender os tipos de *backup* existentes. (CONCEITUAL) - Executar o *backup* de informações utilizando comandos internos do Linux.
g. Registro de Eventos	02	-	- Compreender a importância do emprego de *logs* no contexto da segurança da informação. (CONCEITUAL) - Executar o controle de *logs* no monitoramento do sistema operacional Linux. (PROCEDIMENTAL) - Empregar o registro de *logs* na solução de problemas de sistema. (PROCEDIMENTAL) **ET - METICULOSIDADE**
UD III: Serviços de rede	**Cg H: 40**		**OBJETIVOS DA APRENDIZAGEM / EIXO TRANSVERSAL**
ASS	**D**	**N**	
a. Serviço *Web*	10	-	- Compreender a arquitetura de um servidor *Web*. (CONCEITUAL) - Realizar a instalação de um servidor *Web*. (PROCEDIMENTAL) - Compreender os principais comandos de um servidor *Web*. (CONCEITUAL) - Realizar a configuração de uma aplicação *Web* no servidor. (PROCEDIMENTAL) - Realizar a configuração do módulo PHP no servidor *Web*. (PROCEDIMENTAL) - Executar a configuração de *logs*. (PROCEDIMENTAL) - Identificar erros comuns em serviços *Web*. (FACTUAL) - Apresentar uma solução para corrigir os erros comuns em serviços *Web* - Realizar a configuração do monitoramento do serviço. (PROCEDIMENTAL) - Realizar boas práticas de segurança de serviços *Web*. (FACTUAL)

			- Executar a encriptação de dados com um servidor *Web*. (PROCEDIMENTAL)
b. *Dynamic Host Configuration Protocol* (DHCP)	10	-	- Compreender a arquitetura e o funcionamento do serviço DHCP. (CONCEITUAL) - Executar a instalação de um servidor DHCP. (PROCEDIMENTAL) - Executar a configuração inicial do servidor DHCP. (PROCEDIMENTAL) - Executar a configuração de interfaces de rede para o serviço. (PROCEDIMENTAL) - Executar a declaração de sub-redes utilizadas. (PROCEDIMENTAL) - Executar a declaração de *hosts* com endereçamento fixo. (PROCEDIMENTAL) - Realizar a configuração de *hosts* de endereço IP fixo. (PROCEDIMENTAL) - Realizar os procedimentos de inicialização, encerramento e reinício do serviço DHCP. (PROCEDIMENTAL)
c. *Domain Name System* (DNS)	10	-	- Compreender a arquitetura e o funcionamento do serviço DNS. - Executar a instalação de um servidor DNS. (PROCEDIMENTAL) - Executar a configuração do servidor DNS para operação nos modos IPv4 e IPv6. (PROCEDIMENTAL) - Executar a configuração do arquivo de opções para funcionamento do servidor DNS primário. (PROCEDIMENTAL) - Realizar a configuração das zonas de DNS. (PROCEDIMENTAL) - Realizar a configuração das zonas de encaminhamento. (PROCEDIMENTAL) - Realizar a configuração do servidor DNS secundário. (PROCEDIMENTAL) - Realizar a configuração dos clientes DNS. (PROCEDIMENTAL)
d. *File Transfer Protocol* (FTP)	06	-	- Compreender a arquitetura e o funcionamento do serviço FTP. - Executar a instalação de um servidor FTP. (PROCEDIMENTAL) - Executar a configuração inicial do servidor FTP. (PROCEDIMENTAL) - Executar a configuração completa de um servidor FTP a partir de uma situação dada. (PROCEDIMENTAL)
e. *Network Time Protocol* (NTP)	04	-	- Compreender a arquitetura e o funcionamento do serviço NTP. - Compreender as características do NTP.br (CONCEITUAL) - Realizar a configuração de uma máquina para operação no modo servidor. (PROCEDIMENTAL) **ET – PERSISTÊNCIA**
UD IV: *Firewall*	**Cg H: 16**		**OBJETIVOS DA APRENDIZAGEM / EIXO TRANSVERSAL**
ASS	**D**	**N**	
Firewall de Rede	16	-	- Compreender a arquitetura e o funcionamento de um *firewall*. (CONCEITUAL) - Compreender as características e a compatibilidade de um servidor *firewall*. (CONCEITUAL) - Realizar a instalação de um servidor *firewall*. (PROCEDIMENTAL) -Executar a configuração inicial de um servidor *firewall*. - Realizar a criação de *aliases.* (PROCEDIMENTAL) - Realizar a configuração de regras de *firewall*. (PROCEDIMENTAL) - Realizar a configuração de regras de redirecionamento. - Executar o monitoramento da rede com um servidor *firewall.* (PROCEDIMENTAL) **ET – CRIATIVIDADE**

Fonte: Pladis 3º ano CCom/AMAN

A carga horária destinada para a Cibernética do 3º ano do CCom/AMAN é 16,39% da carga horária total, pois o foco dessa fase da formação são as Técnicas

Militares que demandam mais da metade da carga horária das matérias militares de comunicações, conforme QUADRO 11.

QUADRO 11 – Carga Horária do 3º Ano CCom/AMAN

DISCIPLINA	Cg H por Disciplina	Porcentagem
OUTRAS	408	84%
CIBERNÉTICA IV	80	16%
Cg H atividades de ensino militar	488	100%

Fonte: Pladis 3º ano CCOM/AMAN

No último ano da AMAN, o objetivo é capacitar o futuro oficial a desenvolver as habilidades e capacidades de um Oficial Combatente de Comunicações, nessa fase da formação o cadete enfrenta uma complexidade maior, Entre os objetivos do perfil profissiográfico o cadete devera estabelecer a rede e seus sistemas, implementar controles de acesso e proteger ativamente sua infraestrutura, a partir de ferramentas de software e de conscientização quanto a vetores de ataque, como na Engenharia Social.

A competência principal é igual ao 3º ano, enquanto que as Unidade e Elemento da competência são as que seguem:

> "**UNIDADE DE COMPETÊNCIA**:
> - Planejar e conduzir o emprego da fração em operações convencionais, comandando os pelotões de comunicações orgânicos da Cia Com/Bda e Btl Com/DE.
>
> **ELEMENTO DE COMPETÊNCIA**:
> - Planejar e gerenciar o emprego de um Módulo de Telemática Operacional (MTO). (AMAN, 2021)

No quadro 12, podemos ver que a carga horária destinada a Cibernética V é quase um quarto da carga horária total das matérias militares de comunicações.

QUADRO 12 – Carga Horária 4º ano CCOM/AMAN

DISCIPLINA	Cg H por Disciplina	Porcentagem
OUTRAS	283	79%
CIBERNÉTICA V	77	21%
Cg H atividades de ensino militar	360	100%

Fonte: Pladis 4º ano CCom/AMAN, 2021

No 4º ano de Comunicações, o cadete aprende um pouco mais sobre os níveis operacional e estratégico das operações. No ano do aspirantado, os cadetes aprendem uma cibernética voltada para exploração e ataque. Assuntos como

engenharia social, modelo Lockheed Martin e os princípios de hardening, nesse aspecto principalmente que entra o problema do trabalho proposto. A necessidade versus o exíguo tempo de formação destinado para assunto. No QUADRO 13 está listado o extrato da matéria de cibernética do 4º ano do CCom/AMAN.

QUADRO 13 – Extrato Pladis 4º ano CCOM/AMAN

UD I: Guerra Cibernética (G Ciber)	**Cg H: 2**		**OBJETIVOS DA APRENDIZAGEM/EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. G Ciber	2	-	- Compreender os níveis de decisão da G Ciber. (CONCEITUAL) - Compreender os fundamentos da G Ciber. (CONCEITUAL) - Compreender as estruturas operativas de G Ciber, suas atividades cibernéticas e responsabilidades. (CONCEITUAL) - Compreender as capacidades operativas da G Ciber (CONCEITUAL) - Compreender a G Ciber no contexto das funções de combate. (CONCEITUAL) - Compreender a G Ciber nas Op terrestres. (CONCEITUAL)
UD II: *Proxy*	**Cg H: 20**		**OBJETIVOS DA APRENDIZAGEM/EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. Servidor *Proxy*	20	-	- Compreender a arquitetura e o funcionamento de um servidor *proxy*. (CONCEITUAL) - Compreender as características e a compatibilidade de um servidor *proxy*. (CONCEITUAL) - Executar a instalação de um servidor *proxy*. (PROCEDIMENTAL) - Executar a configuração inicial de um servidor *proxy*. (PROCEDIMENTAL) - Realizar a configuração de listas de controle de acesso (ACL). (PROCEDIMENTAL) - Realizar a configuração de autenticação de acesso (PROCEDIMENTAL) - Realizar a geração de relatórios (PROCEDIMENTAL) - Executar o *backup* do servidor e configurar o processo para execução automática. (PROCEDIMENTAL) **ET – DEDICAÇÃO**
UD III: *Hardening*	**Cg H: 10**		**OBJETIVOS DA APRENDIZAGEM/EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. *Hardening*	02	-	- Identificar os princípios de *hardening*. (FACTUAL)
b. Acesso ao Sistema Operacional GNU/Linux	02	-	- Realizar a recuperação de senha de *root*. (PROCEDIMENTAL) - Executar a proteção do gerenciador de *boot* (GRUB). (PROCEDIMENTAL)
c. Particionamento	02	-	- Executar a segurança do particionamento de disco. (PROCEDIMENTAL)
d. Quotas de disco	02	-	- Executar a limitação do uso de recursos do sistema de arquivos por usuário (PROCEDIMENTAL)
e. Lista de Controle de Acesso	02	-	- Executar o controle granular das permissões de acesso a arquivos e diretórios. (PROCEDIMENTAL) **ET – ORGANIZAÇÃO**

UD IV: *CyberSecurity Essentials*	**Cg H: 37**		**OBJETIVOS DA APRENDIZAGEM/EIXO TRANSVERSAL**
ASSUNTOS	**D**	**N**	
a. *Cyber Kill Chain*	10	-	- 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. (CONCEITUAL)
b. *Malwares* e Ataques Cibernéticos	15	-	- 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. (CONCEITUAL)
c. Engenharia Social	08	-	- Compreender como funcionam as técnicas de engenharia social utilizadas por atacantes cibernéticos, enquadrando, em cada uma, as táticas utilizadas. (CONCEITUAL) - Compreender como atuar contra as técnicas e táticas de engenharia social. (CONCEITUAL) - Compreender a importância do trabalho de orientação de subordinados e assessoramento de superiores quando estiver em função de responsável pela proteção cibernética de uma rede de computadores, tanto na vida vegetativa de uma OM, quanto em campanha. (CONCEITUAL)
d. Controle de Acesso	04	-	- Compreender os tipos de controladores de acesso e entender como podem ser utilizados em prol da segurança cibernética no meio militar. (CONCEITUAL) - Executar os diversos tipos de controle de acesso em campanha, a fim de impedir ataques à rede de computadores de exercício. (PROCEDIMENTAL) **ET – RESPONSABILIDADE**

Fonte: Pladis 4º ano CCom/AMAN, 2021

Além dos três anos de matéria de cibernética, o cadete de comunicações pode participar de eletivas ou estágios setoriais de área em cibernética, os principais são:

- Estágio de Atividades Cibernéticas no CIGE;
- Estágio de Comando e Controle na EsCom; e
- Proteção Cibernética na EsCom

Infere-se, parcialmente, que a AMAN se encontra com a organização em matéria de cibernética estruturada A implementação das disciplinas já sofreram atualizações, e estão de acordo com as diretrizes governamentais estratégicas, principalmente na área de Defesa. Devido ao maior tempo de formação, cinco anos, o oficial de Comunicações tem seu PLADIS voltado não apenas para proteção cibernética, mas também para matéria inicial de exploração e ataque cibernético, gerando o problema desta pesquisa.

5. A ESPECIALIZAÇÃO EM CIBERNÉTICA

A especialização tem como principal curso o Guerra Cibernética. Criado em 2010 o curso visa a realização de ações de segurança, proteção e guerra cibernética em redes de computadores e sistemas de informação. Outros cursos complementam a especialização em cibernética, como o mais recente curso criado de Proteção Cibernética, além de estágios e cursos da CISCO.

5.1 O CURSO DE GUERRA CIBERNÉTICA

O Curso de Guerra Cibernética (G Ciber) está em atualização. Atualmente, o G Ciber ministra todas as atividades de Guerra Cibernética, porém, para o próximo ano a Escola de Comunicações deve assumir o curso de Proteção Cibernética, deixando o primeiro apenas com a parte de exploração e ataque cibernético. Este curso tem a classificação restrita, portanto o Pladis e Perfil Profissiográfico será referenciado de maneira resumida, sem comprometer a segurança dos dados curriculares do curso.

Atualmente a especialização tem o objetivo de preparar os oficiais e sargentos para ocuparem cargos e desempenharem funções, que exijam conhecimentos e práticas especializadas de defesa e guerra cibernética, no Sistema de Guerra Cibernética do Exército. Os cursos disponibilizados pelo CIGE fornecem o ensino nas atividades de proteção e segurança, exploração e ataque cibernético à rede de computadores ou ativos.

Devido ao caráter reservado do Pladis do curso, os quadros serão apenas tópicos, que não prejudicarão o entendimento desse trabalho. A competência principal do curso é “Realizar ações de segurança, proteção e guerra cibernética em redes de computadores e sistemas de informação, Desempenhar funções que exijam conhecimentos e práticas especializadas dos Sistemas de Guerra Eletrônica do Exército (SIGELEx)” (CIGE,2021).

Conforme o QUADRO 14, esses são os principais assuntos ministrados no curso.

QUADRO 14 – Extrato Pladis G Ciber

DISCIPLINA	Carga Horária
FUNDAMENTOS DE GUERRA CIBERNÉTICA	**66**
METODOLOGIA DA PESQUISA CIENTÍFICA	34
PROTEÇÃO CIBERNÉTICA	101
EXPLORAÇÃO CIBERNÉTICA	311
ATAQUE CIBERNÉTICO	92
SETOR CIBERNÉTICO	9
INGLÊS	35

Fonte: Pladis G Ciber, 2021

Nesse contexto, o perfil profissiográfico do guerreiro cibernético prevê o assessoramento no planejamento e possibilidade de atuação. Habilita os sargentos e oficiais a comporem os módulos de defesa cibernética na formação das Forças Tarefas Componentes, contribuindo para liberdade de ação no espaço cibernético, como traçado pelo objetivo estratégico número 4 do Exército, previsto no Plano Estratégico do Exército 2020-2023.

A finalidade do curso é:

> "Habilitar os tenentes e os capitães de carreira das Armas, do Quadro de Material Bélico, do Serviço de Intendência e, em caráter excepcional, do Quadro de Engenheiros Militares (especialidades de Engenharia da Computação, Engenharia de Comunicações e Engenharia Eletrônica) e do Quadro Complementar de Oficiais (especialidade de Informática), para ocuparem cargos e desempenharem funções que exijam conhecimentos e práticas especializadas de defesa e guerra cibernética no Sistema de Guerra Cibernética do Exército." (EME, 2017)

O QUADRO 15 mostras as Unidades de Competência e Elementos de Competência elencados na Portaria Nº117-EME:

QUADRO 15 – Extrato perfil profissiográfico do guerreiro cibernético

COMPETÊNCIAS PRINCIPAIS	UNIDADES DE COMPETÊNCIAS	ELEMENTOS DE COMPETÊNCIAS
Realizar ações de segurança, proteção e guerra cibernética em redes de computadores e sistemas de informação	Executar atividades de Proteção e Segurança em uma rede de computadores e seus ativos.	Executar atividades de *hardening* de servidores.
		Aplicar o conceito de defesa em profundidade.
	Executar atividades de Exploração Cibernética em uma rede de computadores e seus ativos.	Coletar informações dos sistemas de interesse.
		Identificar vulnerabilidades em aplicações Web.
		Executar atividades de forense computacional.

	Executar atividades de Ataque Cibernético em uma rede de computadores e seus ativos.	Atacar redes sem fio.
		Atacar redes cabeadas.
		Atacar a serviços de rede e aplicações.
	Assessorar no planejamento e execução de ações cibernética.	Assessorar na definição das limitações e possibilidades de uma fração cibernética
		Compreender as características técnicas e desdobramentos operacionais de uma ação cibernética
		Assessorar na condução de uma ação cibernética
	Assessorar quanto a atuação no espaço cibernético	Definir as limitações e possibilidades de uma fração cibernética
		Compreender as características técnicas e desdobramentos operacionais de uma ação cibernética

Fonte – Portaria Nº 117- EME, 2017

A especialização divide-se em Curso de Cibernética para Oficiais e Curso de Cibernética para Sargentos. Apesar da diferenciação do curso, a carga horária distribuída do Pladis é a mesma, o que enfatiza a importância a matéria básica a ser ministrada na ESA, diminuindo o hiato de conhecimento do oficial e do sargento na formação, quanto à cibernética.

O Curso de Guerra Cibernética também recebe militares de outras Forças Armadas. Por determinação na PND e END, como supracitado, a missão de adquirir a capacidade em Cibernética é do Ministério da Defesa, com responsabilidade do Exército Brasileiro. Assim, é importante que todas as forças incluam em suas escolas de formação a matéria de Cibernética e atualizem seus perfis profissiográficos.

Dessa forma, nota-se que o Exército vem alinhando a matéria de cibernética nas escolas de formação e criando cursos na área, em específico o Curso de Guerra Cibernética que já formou mais de dez turmas de oficiais. Outros cursos foram criados na área, como o Curso de Proteção Cibernética, em março de 2021, e o Estágio Geral de Proteção Cibernética para oficiais, que são ministrados pela Escola de Comunicações. Assim, o EB tem buscado executar as diretrizes ministeriais e presidencial para aperfeiçoar a capacidade em cibernética.

6. CONCLUSÃO

O presente trabalho se baseou na problemática do melhor alinhamento entre as matérias de cibernética das escolas de formação, principalmente a AMAN e o curso de Guerra Cibernética. O principal problema se situou em torno das capacidades Exploração Cibernética e Ataque Cibernético. No âmbito da pesquisa ficou evidente o desenvolvimento avançado da estrutura de ensino de ambas as escolas, porém essas carecem de um alinhamento estratégico.

Vale relembrar que o trabalho foi divido em capítulos que tiveram a finalidade de levar a uma possível resposta acerca da interseção ou alinhamentos dos Plano de Disciplina, entre as escolas, por consequência do Perfil Profissiográfico do Guerreiro Cibernético. Assim, responder ao problema proposto.

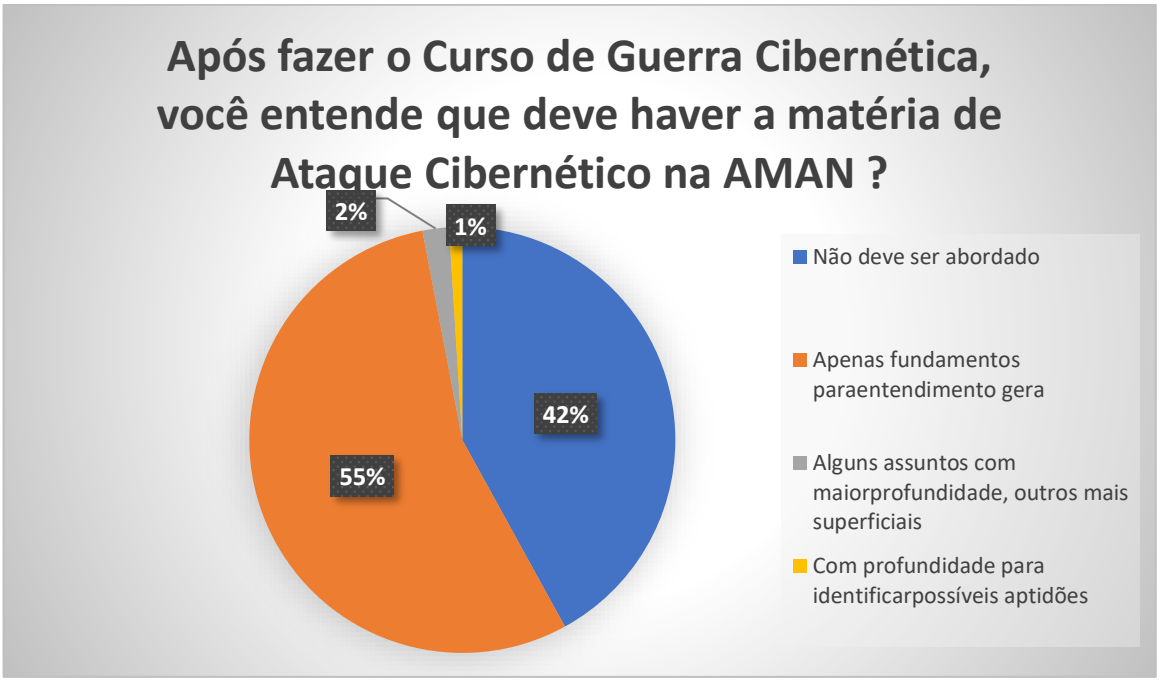
O foco do trabalho se deteve nos capítulos 4 e 5, esse sobre a especialização no Curso de Guerra Cibernética e aquele versando sobre o desenvolvimento da cibernética na AMAN. Na análise dos dois Pladis e Perfil Profissiográfico algumas conclusões podem ser subtraídas.

Em síntese, ambas escolas possuem o Pladis pronto, a evolução e atualização acontecerá devido a volatilidade do assunto. Porém fica notório o avanço da AMAN no assunto, por vezes “invadindo” as matérias ministradas no curso de especialização, surgindo a necessidade de atualização conforme o alinhamento necessário para melhor aproveitamento do tempo destinado para ambos os cursos.

Alguns assuntos tornaram-se comuns entre as escolas, a exemplo os princípios de *hardening*, as fases do ataque cibernético, a engenharia social entre outros. Como sugestão, sob coordenação do CComGEx ou do CDCiber as escolas poderiam se reunir anualmente para estabelecer os alinhamentos dos Pladis.

Como forma de fundamentar o trabalho, foi realizado uma pesquisa com os militares que concluíram o curso de Guerra Cibernética, o GRÁFICO 3 demonstra o posicionamento desses militares sobre o assunto. Em resumo, mais de 97% dos militares que preencheram a pesquisa acreditam que a matéria de Ataque e Exploração Cibernética deveria ser ministrada de maneira superficial ou apenas fundamentos básicos.

GRÁFICO 3 – Instruções de Ataque e Exploração Cibernética na AMAN



Fonte: Questionário A, autor.

Em uma das pesquisas respondidas, foi sugerido que o curso de Guerra Cibernética foca mais em técnicas mais ofensivas de acordo com as experiências e demandas de operações/exercícios, enquanto os cadetes da AMAN deveriam ter mais profundidade, apenas, na parte de proteção para que tenham base, quando voluntários para fazer o curso de Guerra Cibernética., então desenvolveram as habilidades de Ataque e Exploração. Esses possuem conteúdos e técnicas que exigem muita responsabilidade, um dos motivos pela qual a seleção dos alunos para o curso passa inclusive por análise do pessoal do Centro de Inteligência do Exército.

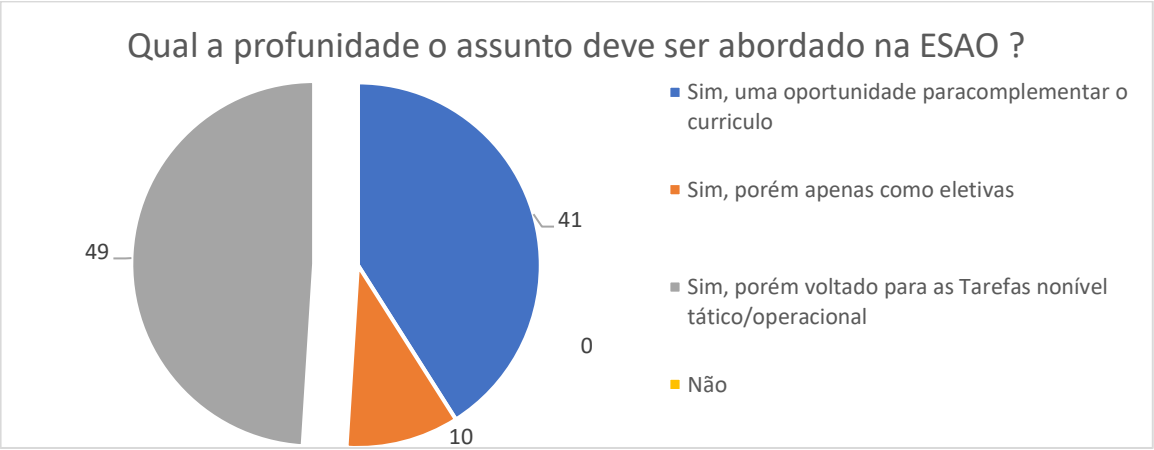
Um interessante paralelo pode ser traçado com o Curso de Inteligência Militar, até por efeitos de comparação, um curso pode complementar o outro, ambos, em teoria, fazem proteção, exploração e ataque de ativos. Resumindo, todos os cadetes aprendem noções de inteligência e contra inteligência, mas nem todos são aptos para exercer a inteligência militar propriamente dita, por isso os processos dentro da inteligência são passados apenas para quem realizar o curso na área.

Outrossim, a A Proteção Cibernética é uma área do conhecimento que é aplicada por praticamente qualquer oficial de comunicações, inclusive por qualquer militar, seja de comunicações ou de outra arma, quadro ou serviço, com

a tecnologia de hoje a proteção cibernética é necessária em todos os níveis. Por isso, outra sugestão para a AMAN seria incluir no Pladis dos outros cursos as medidas de Proteção Cibernética, para que todos, dentro da sua área de atuação possam defender os ativos que estão sob sua responsabilidade.

A pesquisa também questionou o papel da ESAO na formação e aperfeiçoamento do guerreiro cibernético e do oficial de comunicações, o GRÁFICO 4 demonstra a visão dos militares possuidores do Curso de Guerra Cibernética.

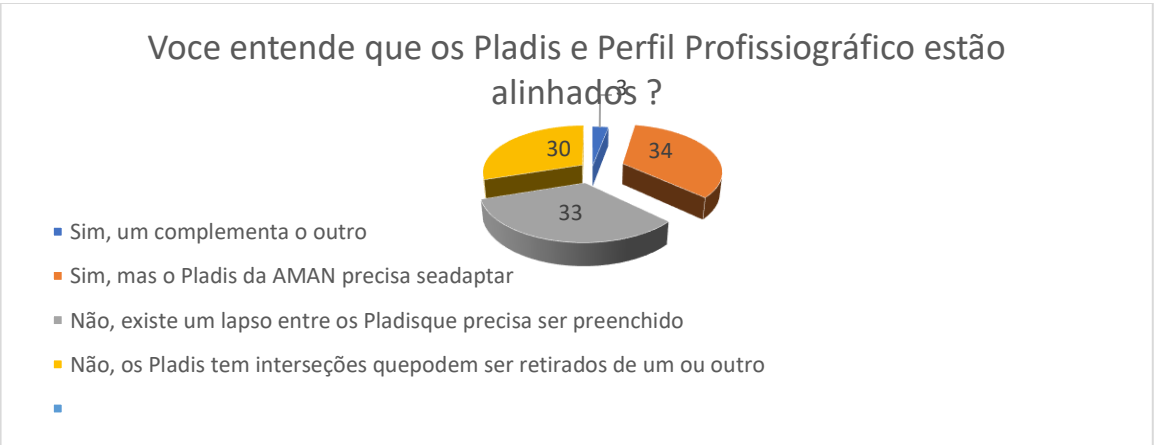
GRÁFICO 4 – Instruções de cibernética na ESAO



Fonte: Questionário A, autor.

Outra pergunta se destinou a necessidade de atualização dos Pladis, inicialmente a problemática do trabalho, conforme o GRÁFICO 4, quase 70% dos entrevistados acreditam que os Pladis necessitam ser atualizados para que aconteça o alinhamento entre a necessidade dos diferentes perfil profissiográfico e Planos de Disciplina.

GRÁFICO 5 – Necessidade de alinhamento dos Pladis e Perfil Profissiográfico



Fonte: Questionário A, autor.

Por fim, após análise realizada, pode-se concluir que apesar do elevado avanço da cibernética no ensino acadêmico e de especialização, ainda existem arestas a aparar para alinha ambos Pladis e Perfis Profissiográfico. A construção da capacidade cibernética esta diretamente ligada ao preparo da tropa e capacidade de dissuasão no cenário internacional, o que torna imprescindível o avanço nessa área, para então alcançar plenamente os objetivos políticos traçados.

REFERÊNCIAS

AMAN. **Perfil Profissiográfico:** Curso de Comunicações. Resende: Acadêmica, 2021.

AMAN. **Plano de Disciplina:** Curso de Comunicações. Resende: Acadêmica, 2021.

ALMEIDA, Anderson Magno de. **DESENVOLVIMENTO PROFISSIONAL DOCENTE**: perspectivas de professores da Academia Militar das Agulhas Negras. Taubaté, SP: 2018.

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

BBC. Rússia e Ucrânia travam 'duelo cibernético'. **G1**, 2014. Disponível em: <http://g1.globo.com/mundo/noticia/2014/03/russia-e-ucrania-travam-duelo-cibernetico.html>. Acesso em: 10 abr. 2021.

BRASIL. Departamento de Educação e Cultura do Exército. **Instruções reguladoras da organização e da execução dos cursos de graduação, de especialização-profissional, de extensão e de pós-graduação, no âmbito do DEP (IR 60-37).** Portaria Nº 135 – DEP, de 31 de outubro de 2006. Rio de Janeiro: DEP, 2006.

BRASIL. Estado Maior do Exército. **Criação do Curso de Guerra Cibernética**. Portaria N º 117-EME, de 3 de abril, de 2017, Brasília: EME, 2017

ESA. **Perfil Profissiográfico:** Curso de Comunicações. Três Corações: ESA, 2021.

ESA. **Plano de Disciplina:** Curso de Comunicações. Três Corações: ESA, 2021.

_____. Escola De Comando e Estado-Maior Do Exército. A **Guerra Cibernética**: uma proposta de elementos para formulação doutrinária no Exército Brasileiro. Rio de Janeiro: BIBLIEx, 2012.

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

CIGE. **Perfil Profissiográfico**. Brasília: CIGE, 2021.

CIGE. **Plano de Disciplina**. Brasília: CIGE, 2021.

CLARKE, Richard A. e KNAKE, Robert K. **Guerra Cibernética**: A Próxima Ameaça À Segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015.

ESTADOS UNIDOS DA AMÉRICA. US Air Force. History of HQ Twenty-Fourth Air Force and 624th Operations Center. **AFCYBER**, 2014. Disponível em: https://www.16af.af.mil/About-Us/Fact-Sheets/Display/Article/1957318/sixteenth-air-force-air-forces-cyber/. Acesso em: 10 abr. 2021.

EXÉRCITO, Escola de Comando e Estado-Maior. **Formatação de Trabalhos Científicos / Departamento de Pesquisa e Pós-graduação**. Rio de Janeiro: ECEME, 2017.

GONÇALVES, Elisa Pereira. **Iniciação à pesquisa científica**. São Paulo: Alínea, 2003.

MANDARINO JR, R; CANONGIA, C. **Livro Verde**: Segurança Cibernética no Brasil. Brasília, GSI/PR: 2010. 63 p.

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

_____. Ministério da Defesa. **EB20-C-07.001 Catálogo de capacidades,** Brasília 2020.

_____. Ministério da Defesa. **EB70-MC-10.332 – Guerra Cibernética**. Brasília,2017.

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

_____. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, 2008

_____. Ministério da Defesa. **MD31-M-07 – Doutrina Militar de Defesa Cibernética**. Brasília, 2014.

OLIVEIRA, Maria Marly de. **Como fazer pesquisa qualitativa**. Petrópolis: Vozes, 2007.

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

PORTO, André de Jesus. **Segurança e proteção cibernética na formação do sargento combatente de comunicações**. Rio de Janeiro: EsAO, 2020.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. – Novo Hamburgo: Feevale, 2013.

ROHR, Altieres. Conheça as capacidades dos hackers militares da China e dos EUA. **G1**, 2014. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/conheca-capacidades-dos-hackers-militares-da-china-e-dos-eua.html>. Acesso em: 07 abr. 2021.

SALUSTRIANO, Wagner de Matos. **Capacitação de Cadetes da Academia Militar das Agulhas Negras (AMAN) em Cibernética: a descoberta de novos talentos para o setor.** Rio de Janeiro, 2020.

SETOR CIBERNÉTICO. **Governo Federal**, 2014. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/ciencia-e-tecnologia/setores-estrategicos/setor-cibernetico>. Acesso em: 05 abr. 2021.

SETORES ESTRATÉGICOS PARA A DEFESA. **Governo Federal**, 2020. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/ciencia-e-tecnologia/setores-estrategicos>. Acesso em: 05 abr. 2021.

____. **Sistema Militar de Defesa Cibernética (SMDC),** em cumprimento à Política Cibernética de Defesa, Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012. Brasília, DF: 2012

SHELDON, J. B. **Deciphering cyberpower: strategic purpose in peace and war**. Strategic Studies, v. 5, issue 2, 2011. Disponível em: < https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf>. Acesso em: 18 maio 2018.

VERGARA, Sylvia Constant. **Métodos de pesquisa em administração**. 3. ed. São Paulo: Atlas, 2008. 287 p., il. Bibliografia: p. 269-287. ISBN: 978-85-224-4999-6.

WIENER, N. **Cybernetics:** or control and communication in the animal and the machine. Cambridge, Massachusetts: M.I.T. Press, 1961

ANEXO A

QUESTIONÁRIO A

- Qual ano você se formou na AMAN?
- Na AMAN voce teve instrução de Guerra Cibernética?
- Marque as opções que você acha que o cadete de Comunicações deve ter na AMAN
    - Proteção Cibernética
    - Exploração Cibernética
    - Ataque Cibernético
- Marque as opções que você acha que os cadetes dos outros cursos devem ter na AMA:
    - Proteção Cibernética
    - Exploração Cibernética
    - Ataque Cibernético
- Sobre as instruções na AMAN, especificamente sobre a matéria Ataque Cibernético, como você entende que deve ser abordado na AMAN:
    - Não deve ser abordado
    - Apenas fundamentos para entendimento geral
    - Alguns assuntos com maior profundidade, outros mais superficiais
    - Com profundidade para identificar possíveis aptidões
- Na EsAO, voce entende que deve ser abordado o assunto?
- Você entende que os atuais Pladis da AMAN e da especialização cibernética estão alinhados?
- Você aplicou o Curso de Guerra Cibernética?
- Observação

ANEXO B

QUESTIONÁRIO B

- Qual ano você se formou na AMAN?
- Você teve instruções de cibernética na AMAN?
- Você pretende realizar o curso de Guerra Cibernética?
- Quais assuntos você aplicou na tropa ?
    - Proteção Cibernética
    - Exploração Cibernética
    - Ataque Cibernético
- Você entende que as instruções de cibernética na AMAN estão coerentes com o tempo destinado para formação?
- Observação