ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

TC Inf JONAS **MOLZ**

A importância dos cursos de formação e especialização do Exército Brasileiro para uma preparação mais adequada de recursos humanos voltada para a Guerra Cibernética.

Rio de Janeiro

2022

TC Inf JONAS **MOLZ**

A importância dos cursos de formação e especialização do Exército Brasileiro para uma preparação mais adequada de recursos humanos voltada para a Guerra Cibernética.

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: Maj Com Samuel Bombassaro Neto

Rio de Janeiro
2022

M731i Molz, Jonas.

A importância dos cursos de formação e especialização do Exército Brasileiro para uma preparação mais adequada de recursos humanos voltada para a Guerra Cibernética. / Jonas Molz.—2022.
78 f. : il. ; 30 cm.

Orientação: Samuel Bombassaro Neto.
Trabalho de Conclusão de Curso (Especialização em Ciências Militares)—Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2022.
Bibliografia: f. 69-72

1. Guerra Cibernética. 2. Formação de Recursos Humanos. I. Título.

CDD 355

TC Inf JONAS **MOLZ**

A importância dos cursos de formação e especialização do Exército Brasileiro para uma preparação mais adequada de recursos humanos voltada para a Guerra Cibernética.

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.

Aprovado em de de 2022.

COMISSÃO AVALIADORA

_____
Samuel Bombassaro Neto – Maj Com QEMA – Presidente
Escola de Comando e Estado-Maior do Exército

_____
Hermes Leonardo Morais Faiolo Silva – Maj Eng QEMA – Membro
Escola de Comando e Estado-Maior do Exército

_____
Paulo Comunale – Maj Int QEMA – Membro
Escola de Comando e Estado-Maior do Exército

AGRADECIMENTOS

À minha família que apoiou e incentivou todas as etapas desta pesquisa, auxiliando, cooperando e entendendo as várias horas dedicadas até a conclusão do Trabalho de Conclusão de Curso.

Ao Major Samuel Bombassaro Neto pelas orientações seguras e precisas, o qual sempre buscou entender as limitações de seu orientando, atuando com grande profissionalismo durante as fases do estudo realizado.

Ao Coronel Veterano Norton Luis Silva da Costa, pelo apoio prestado, especialmente no início dos trabalhos, na busca por fontes de pesquisa atinentes ao tema, contribuindo sobremaneira para os resultados galgados.

RESUMO

A Guerra Cibernética, vertente que busca o uso de informações e de sistemas de informações, é um dos temas de maior relevância no âmbito das Forças Armadas. Nesse contexto, uma formação mais adequada de recursos humanos tende a disponibilizar importantes capacidades e incrementar poder de combate à Força Terrestre do País, além do evidente efeito dissuasório no continente Sul-Americano. Particularmente para o Exército Brasileiro, o assunto é de especial importância, por sua responsabilidade no setor cibernético, determinada pela Estratégia Nacional de Defesa. Assim, é crescente o uso da Guerra Cibernética em operações e, também, situações diversas, principalmente envolvendo altos escalões, como o de uma Força Tarefa Componente ou os Grandes Comandos Militares de Área. Inúmeros autores, além dos próprios documentos e manuais militares, são taxativos ao elencar benefícios advindos da utilização da Guerra e da Proteção Cibernética. Ademais, estudos visando o aprimoramento e possíveis diferenciações nos cursos de Guerra e Proteção Cibernética, no curso para planejadores do emprego e na base conceitual transmitida nas escolas de formação, notadamente voltados para oficiais e sargentos, se fazem necessários, haja vista que os mesmos são cada vez mais demandados no assunto e, após formados e/ ou especializados, muitas vezes executarão funções bastante distintas e complexas.

Palavras-chave: Guerra e Proteção Cibernética, Formação de Recursos Humanos, Aprimoramento na Formação e na Especialização, Complexidade.

ABSTRACT

Cyber Warfare, the use of cyber attacks against an enemy state, is one of the most relevant topics within the Armed Forces. Therefore, adequate training of human resources is essential to provide these important capabilities and increase combat power in the Nation's Land Force, and will have a deterrent effect on the South American continent. Particularly for the Brazilian Army, the matter is of special importance, due to its responsibility in the cybernetic sector, determined by the National Defense Strategy. Thus, the use of Cyber Warfare in operations and also in different situations is increasing, mainly involving high levels, such as a Component Task Force or Large Military Area Commands. In addition to military documents and manuals, many authors emphasize the benefits of War and Cybernetic Protection. Moreover, studies focused on the improvement and possible differences in the courses of War and Cybernetic Protection, the planners course and in the conceptual basis conveyed in the training schools, notably aimed at officers and sergeants, are necessary, given that they are increasingly demanded in the subject and, after training and/ or specialized, they will often perform quite different and complex functions.

Keywords: War and Cybernetic Protection, Human Resources Training, Improvement in Training and Specialization, Complexity.

SUMÁRIO

1 INTRODUÇÃO

A presente pesquisa busca correlacionar a formação e a especialização de recursos humanos em Cibernética (Ciber), tema de extrema relevância, detalhando como ela pode ser aperfeiçoada e contribuir para o poder de combate da Força Terrestre. Acerca do conceito de Guerra Cibernética (G Ciber), conforme o manual de GUERRA CIBERNÉTICA (2017), pode ser definida como o uso ofensivo e defensivo de informações e de sistemas de informações que produzam efeitos nas capacidades de Comando e Controle (C^2) do adversário, tais como exploração ou negação de dados. O mesmo Manual, em seu prefácio faz as seguintes considerações:

> A revolução tecnológica elevou o espaço cibernético a uma nova condição nos assuntos relacionados à defesa e segurança. Tal espaço é um domínio global dentro da dimensão informacional do ambiente operacional que consiste em uma rede interdependente de infraestruturas de Tecnologia da Informação e Comunicações (TIC) e de dados, incluindo a internet, redes de telecomunicações, sistemas de computador, processadores embarcados e controladores.
>
> O Exército Brasileiro (EB) tem acompanhado essa revolução tecnológica e seus impactos doutrinários. Com esse foco e de forma coerente com a Doutrina Militar de Defesa Cibernética, buscou-se formular a doutrina sobre Guerra Cibernética do EB, de forma a contribuir para o desenvolvimento de capacidades nesse domínio. (BRASIL, 2017a).

Corroborando com as citações do prefácio acima transcrito, pode-se destacar que as concepções de guerra moderna se encontram envoltas ao uso massivo de novas tecnologias. Entre elas, merece destaque a Guerra Cibernética, a qual encontra-se inserida em praticamente todos os combates modernos, seja nos armamentos de ponta, por meio de interferências nas operações, no comando e controle, na pontaria e no guiamento de armamentos inteligentes, entre outras funções. Tal fato ressalta a importância de uma mentalidade de proteção a ser criada e desenvolvida desde os bancos escolares.

Portanto, é necessário concentrar esforços para analisar a importância dos Cursos de Formação e Especialização para uma preparação mais adequada de recursos humanos voltada para a Guerra Cibernética, especialmente pelo crescente uso de armamentos e equipamentos dependentes de meios de Tecnologia da Informação (TI), especialmente nas principais escolas de formação e especialização que abordam o tema no Exército Brasileiro.

Desde os primórdios dos estudos da “Arte da Guerra”, Sun Tzu (1999) ressaltou a importância da qualidade do treinamento dos oficiais e da tropa, o que reforça a

relevância de uma formação e especialização adequada. Destarte, a necessidade de aperfeiçoar os cursos de formação e especialização em Cibernética (Proteção e Guerra Ciber), ministrada aos oficiais e sargentos do Exército Brasileiro, insere-se nesse contexto.

A Guerra Cibernética, vertente que atua sobre sistemas em rede, é um dos temas de maior relevância no âmbito das Forças Armadas, pois pode interceder no uso de armamentos e equipamentos dependentes de meios de TI. Assim, tende a agregar grande poder de combate a Força Terrestre Componente (FTC), além do evidente efeito dissuasório de seu domínio, especialmente no Continente Sul-Americano.

Particularmente para o Exército Brasileiro, o assunto é de especial relevância, por sua responsabilidade no setor cibernético, determinada pela Estratégia Nacional de Defesa. Assim, é latente a necessidade de coordenar e adotar medidas que visem a Proteção Cibernética dos sistemas empregados e operados no País, assim como deve-se ter a expertise de saber empregar ações de exploração e ataque cibernético caso seja necessário.

Inúmeros autores, além dos próprios documentos e manuais militares, são taxativos ao elencar benefícios advindos da utilização da Guerra Cibernética, além da evidente necessidade de medidas de proteção em todos os escalões. Ademais, estudos visando incrementar e aperfeiçoar a matéria nas escolas de formação e especialização, assim como uma possível diferenciação nos cursos de cibernética para oficiais e praças podem ser úteis para a Força Terrestre.

1.1 PROBLEMA

Nesse contexto, foi formulado o seguinte problema: como a formação e a especialização de recursos humanos do Exército Brasileiro, em Guerra e Proteção Cibernética pode ser aperfeiçoada, considerando os seguintes bancos escolares: Academia Militar das Agulhas Negras (AMAN), Escola de Sargentos das Armas (ESA), Escola de Comunicações (EsCom) e Centro de Instrução de Guerra Eletrônica (CIGE).

1.2 OBJETIVOS

1.2.1 **Objetivo geral**

Apresentar formas de aprimorar a formação e a especialização de recursos humanos do Exército Brasileiro em Guerra e Proteção Cibernética.

1.2.2 **Objetivos específicos**

Para atingir o objetivo geral citado acima, especialmente voltado para a formação e a especialização de oficiais e sargentos da Força Terrestre, foram traçados os seguintes objetivos específicos:

- Identificar o conceito, a metodologia empregada, os óbices e possíveis sugestões de aprimoramento na formação de oficiais e sargentos do Exército Brasileiro em cibernética, especificamente aplicada na Academia Militar das Agulhas Negras (AMAN) e na Escola de Sargentos das Armas (ESA).

- Identificar o conceito, a metodologia empregada, os óbices e possíveis sugestões de aprimoramento na especialização dos Oficiais e Sargentos do Exército Brasileiro em Proteção e Guerra Cibernética, especificamente aplicada na Escola de Comunicações (EsCom) e no Centro de Instrução de Guerra Eletrônica (CIGE).

1.3 DELIMITAÇÃO DO ESTUDO

Por definição do Catálogo de Capacidades do Exército, a Guerra Cibernética corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C^2 do adversário. Podem ocorrer no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle ($STIC^2$) do oponente e defender os próprios $STIC^2$. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2015).

Diante disso, este estudo está delimitado nos Cursos de Formação e Especialização para uma preparação mais adequada de recursos humanos voltada para a Cibernética, considerando que uso de armamentos e equipamentos dependentes de meios de TI. Nesse contexto, o uso de equipamentos e armamentos em rede, uma tendência global, tende a tornar tal especialização cada vez mais importante. Ademais, o desenvolvimento de uma mentalidade de proteção deve ser buscada desde os bancos escolares e aperfeiçoado nos cursos de especialização.

1.4 RELEVÂNCIA DO ESTUDO

Conforme o manual de Guerra Cibernética (2017), a oportunidade para o emprego dessas ações (Ciber) ou a sua efetiva utilização será proporcional à dependência do oponente em relação às Tecnologias de Informação e Comunicações (TIC). Nesse contexto, a relevância do presente estudo fica evidenciada quando se verifica na prática, a incontável utilização de meios dependentes de TIC nas guerras da era da informação, todos possíveis alvos da Guerra Cibernética, seja de forma direta ou indireta, como na atual Guerra da Ucrânia (2022), exemplificada em sistemas de Armas, Sistemas de Aeronaves Remotamente Pilotadas (SARP), radares, sensores, atuação sobre sistemas de Comando e Controle, entre outros sistemas e meios de ataque e defesa cibernética.

Além disso, o mesmo manual de Guerra Cibernética (2017), acerca da atual conjuntura mundial, cita que a sociedade brasileira, em particular a expressão militar do Poder Nacional, deverá estar permanentemente preparada, considerando os atuais e futuros contenciosos internacionais. Para tal, medidas deverão ser adotadas de modo a capacitá-la a responder oportuna e adequadamente, com proatividade, antecipando-se em face dos possíveis cenários adversos à defesa nacional (2017a, p13). Dessa forma, deve-se estimular o debate acadêmico acerca do assunto e os necessários recursos humanos para sua mais adequada utilização, fomentando o incremento na profissionalização e melhorias nos processos de formação e especialização.

No tocante às Ciências Militares, este trabalho se justifica ao buscar propor sugestões de aprimoramento em cursos de formação e de especialização de oficiais e sargentos do Exército Brasileiro em Cibernética. Visando esse aperfeiçoamento, além de reforçar o assunto nas escolas de formação, poder-se-á surgir uma possível

diferenciação na formação de oficiais e praças, tudo com a finalidade de melhorar a qualificação profissional dos militares da área, direcionado as funções que serão desempenhadas por cada operador e ou planejador de operações cibernéticas ao longo de suas carreiras.

2 METODOLOGIA

2.1 TIPO DE PESQUISA

A presente pesquisa, quanto a abordagem, foi do tipo quali-quantitativa, na qual se buscou valorizar tanto os aspectos subjetivos quanto os aspectos numéricos na análise dos dados coletados. Foram selecionadas fontes de pesquisa baseadas em publicações militares que abordem as temáticas de Doutrina Cibernética, Doutrina de Operações Militares e outros manuais afetos ao tema, bem como periódicos militares, instruções provisórias, instruções gerais, instruções reguladoras, portarias normativas e diretrizes. Além dessas, foram buscados trabalhos acadêmicos, como artigos científicos e livros, relacionados ao emprego da Ciber.

Por fim, foram enviados questionários para militares que atuam ou atuaram na formação em Cibernética da Academia Militar das Agulhas Negras (AMAN) e da Escola de Sargentos das Armas (ESA), e na especialização por meio de Cursos, para a Escola de Comunicações (EsCom) e para o Centro de Instrução de Guerra Eletrônica (CIGE), visando levantar dados e possíveis soluções para os problemas levantados. Além destes, mais um questionário foi distribuído, destinado a oficiais e sargentos com algum curso na área ou com experiência em cibernética, com a mesma finalidade já citada.

Por fim, o tipo de pesquisa científica empregado quanto aos procedimentos, foi de uma pesquisa do tipo *survey*, pois se buscou informações diretamente com um grupo de interesse a respeito dos dados que se desejava obter, no caso, instrutores e monitores dos Estabelecimentos de Ensino (Estb Ens) citados e outros militares com especialização ou experiência no tema.

2.2 DELIMITAÇÃO DA PESQUISA

Nas pesquisas em bases de dados eletrônicas, foram designados os seguintes termos de descrição para a pesquisa: “guerra cibernética, defesa cibernética, meios de tecnologia da informação, formação em cibernética, emprego de armamentos e equipamentos dependentes de TI, guerra do futuro, formação em escolas militares do Exército, Cursos de Especialização em Cibernética, AMAN, ESA, EsCom, CIGE”, observando as particularidades de cada base de dados.

2.3 TRATAMENTO DE DADOS

Após a busca e a seleção de todos os conceitos que fazem parte do problema, foi executada uma análise dos dados coletados, com uma revisão bibliográfica dos diversos manuais, regulamentos, decretos, periódicos e demais documentos que tratam sobre o assunto, além do cabedal de conhecimentos recebidos nos diversos questionários propostos. A pesquisa foi desenvolvida buscando apresentar os diversos fundamentos da formação e especialização de recursos humanos em Ciber, particularizando a AMAN, a ESA, a EsCom e o CIGE.

2.4 LIMITAÇÕES DO MÉTODO

O presente trabalho é limitado ao nível de profundidade, sobretudo, pelo tempo disponível para a desenvolvimento da pesquisa do Trabalho de Conclusão de Curso (TCC) e as dificuldades de afastamentos longos para colher dados presenciais em centros de referência no assunto. Ainda assim, o estado final desejado deste estudo é que se alcance os objetivos propostos e, fruto da análise dos dados levantados, criem-se concepções e possíveis contribuições relevantes na formação de recursos humanos da Força Terrestre em cibernética.

3 REFERENCIAL TEÓRICO

3.1 FUNDAMENTOS DA GUERRA CIBERNÉTICA

A Guerra Cibernética tem se mostrado uma opção importante no rol de ações não cinéticas das operações militares. Isto foi motivado pela velocidade da revolução tecnológica recente que culminou na elevação do espaço cibernético à condição de domínio operacional. (US ARMY, 2010; USA, 2018). Tal fato destaca a importância do assunto para uma Força Terrestre, o que motiva o Exército Brasileiro a manter em seus quadros militares capacitados e prontos para atuarem nesse domínio.

A transversalidade da G Ciber aos demais domínios (marítimo, terrestre, aéreo e espacial), permite-lhe criar efeitos militares decisivos, produzindo vantagens e influenciando eventos em todos os ambientes operacionais. Entretanto, em um contexto de Operações no Amplo Espectro e à medida que surgem um número maior de atores no ambiente operacional, bem como aspectos relacionados às dimensões humana e informacional, verifica-se que a complexidade dos problemas enfrentados pelas forças militares aumenta. Para mitigar as consequências deste novo domínio na Defesa Nacional e contrapor os novos desafios apresentados às Forças Armadas na condução das operações militares contemporâneas, em 2008, o Ministério da Defesa incumbiu o Exército Brasileiro das tarefas de coordenar e de integrar as ações de Defesa Cibernética no país. (BRASIL, 2014d).

Contudo, com as peculiaridades do domínio cibernético e o fato do conceito de Guerra Cibernética ser uma concepção recente, a doutrina de emprego de suas ações ofensivas ainda carecem de amadurecimento. (Vasquez, 2020).

Nesse contexto, ao referenciarmos a grande responsabilidade que o Exército Brasileiro possui na defesa do país e, também, no domínio do espaço cibernético, torna-se impreterível a relevância da constante atualização e uma adequada formação/ especialização de seu capital humano.

3.1.1 **O espaço cibernético e a Guerra Cibernética**

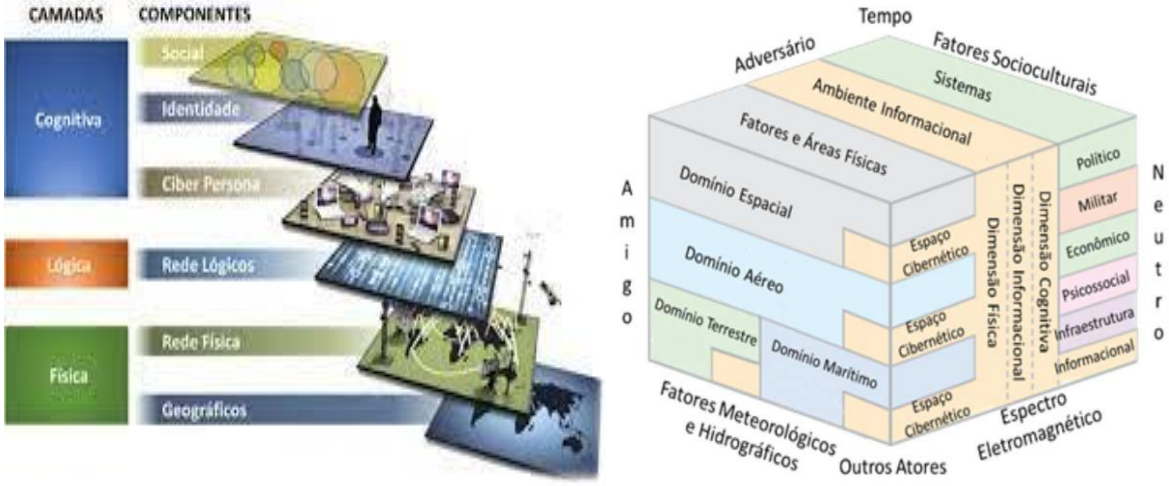
O espaço cibernético é um ambiente complexo que vai além dos limites organizacionais e das fronteiras nacionais. (BRANDÃO; IZYCKI, 2019). Ele é resultante da interação de pessoas, softwares e serviços disponíveis na Internet por

meio de dispositivos e redes de telecomunicações conectados a ela. (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2012).

Na doutrina militar brasileira, o espaço cibernético é caracterizado por ser um ambiente virtual composto por dispositivos computacionais, conectados em redes ou não, onde as informações digitais transitam e são processadas ou armazenadas. Tais atributos criam um espaço operativo comum, integrando as dimensões física, informacional e humana no que se refere a sua dependência aos meios de tecnologia da informação e comunicações. (BRASIL, 2014d; BRASIL, 2017a; USA, 2018).

A complexidade desse ambiente pode ser minimizada por sua descrição segundo três perspectivas da dimensão informacional, na qual o espaço cibernético está inserido, conforme representado na figura 1 (inter-relação dessas camadas):

Figura 1 - Camadas do Espaço Cibernético e sua visão holística



Fonte: US Army (2010); United Kingdom (2016), adaptado por Vasquez, 2020

A camada física é caracterizada pelo hardware e pela infraestrutura computacional responsáveis pelo armazenamento, transporte e processamento de informações, distribuídos em um espaço geográfico. Seus componentes exigem medidas de segurança física, que podem ser aproveitados para a obtenção do acesso lógico. Ela também define a localização geográfica e a estrutura legal apropriada a ser aplicada nas operações militares, considerando que existem questões de propriedade e soberania ligadas aos domínios físicos e as fronteiras geopolíticas são facilmente ultrapassadas no ciberespaço. (UNITED KINGDOM, 2016; USA, 2018).

A segunda camada refere-se à rede lógica. Essa é uma abstração da camada física e consiste no código de programação, nos protocolos e nos dados que acionam os componentes de rede. Ela restringe o engajamento de seus alvos por meios inerentes ao espaço cibernético, ou seja, um dispositivo ou aplicação projetada para

criar um efeito no ciberespaço ou através dele. (UNITED KINGDOM, 2016; USA, 2018).

A última camada é a cognitiva. Ela é responsável por conectar as pessoas ou grupos à sua forma de apresentação no espaço cibernético (*ciberpersona*). Ela reflete seus aspectos humanos e sociais, incluindo as contas de usuários (humanas ou automatizadas) e de grupos, bem como seus dados e relacionamentos. (UNITED KINGDOM, 2016; USA, 2018).

Essa gama de entidades que interagem nesse domínio para trocarem informações, faz com que ele seja determinante no planejamento operacional (US ARMY, 2019). Deste modo, é fundamental compreender as condições, circunstâncias e fatores que influenciam o ambiente operacional cibernético pois, por meio dele, é possível criar efeitos únicos e decisivos em todos os demais domínios. (BRASIL, 2014d; USA, 2018).

3.1.2 **Os princípios e características da Guerra Cibernética**

Para alcançar tais objetivos, o vetor militar a ser utilizado é a Guerra Cibernética. Ela é definida pelas ações no espaço cibernético que amplificam as ações cinéticas e garantem liberdade de ação da força empregada, potencializando seus efeitos no Teatro de Operações. (BRASIL, 2012; BRASIL, 2017a).

O termo Guerra Cibernética refere-se, ainda, ao planejamento e à execução das atividades cibernéticas nos níveis operacional e tático de uma operação militar. Ela corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de comando e controle (C^2) do adversário. (BRASIL, 2014d).

O seu emprego é pautado em quatro princípios relevantes: o efeito, a dissimulação, a rastreabilidade e a adaptabilidade. Os dois primeiros dizem respeito diretamente às ações ofensivas, enquanto os últimos às defensivas. O princípio do efeito remete à produção de impactos no espaço cibernético. Esses devem produzir vantagem em todos os níveis de decisão, afetando o mundo real, mesmo que não sejam cinéticos. A dissimulação trata das medidas a serem adotadas a fim de mascarar a autoria e o ponto de origem das ações ofensivas. A rastreabilidade, por sua vez, está relacionada à detecção das ações cibernéticas do oponente. E, por fim, o princípio da adaptabilidade consiste na capacidade da Guerra Cibernética em

adaptar-se e manter a proatividade mesmo diante de mudanças súbitas e imprevisíveis no combate. (BRASIL, 2014d).

Uma das principais características da Guerra Cibernética é a insegurança latente dos sistemas computacionais, que parte da premissa de que não há sistemas completamente seguros e que suas vulnerabilidades poderão ser exploradas. Assim, a Guerra Cibernética aproveita-se da ausência das amarras das limitações físicas de distância e espaço e ignora as fronteiras geográficas para conduzir suas ações em qualquer parte do globo. (BRASIL, 2017a).

Também há de se observar que o desenvolvimento de armas cibernéticas possui um ciclo mais curto se comparado às tradicionais. Desta maneira, seu custo é inferior aos armamentos cinéticos convencionais. Isto proporciona um desbalanceamento de forças, em que Estados, organizações ou agentes com recursos financeiros limitados são capazes de perpetrar danos tão severos quanto os cometidos por entidades com maiores condições econômicas. (BRANDÃO; IZYCKI, 2019; BRASIL, 2017a).

Outro aspecto interessante a ser constatado é a dualidade das ferramentas que podem ser usadas por atacantes e administradores de sistemas com finalidades distintas. Um software de identificação de vulnerabilidades tanto pode ser empregado para identificar falhas em um sistema para a adoção de medidas de proteção, quanto para apresentar oportunidades de ataque. (BRASIL, 2017a).

Por este cenário, nota-se que uma operação cibernética pode empregar vários tipos de ataques, disseminados por diferentes vetores, que exijam níveis de acesso distintos, tudo de forma combinada, sequencial ou simultânea, inclusive conjugar recursos cibernéticos e físicos. (BERNIER, 2013).

Desta forma, pode-se dizer que o sucesso das ações ofensivas cibernéticas depende do domínio de todo o ciclo de vida do ataque: reconhecimento, preparação, entrega do artefato, exploração, instalação, comando e controle e ações nos objetivos. (BRANDÃO; IZYCKI, 2019; HUTCHINS; CLOPPERT; AMIN, 2011).

Entretanto, é importante destacar que a Guerra Cibernética não tem um fim em si mesma. Ela é tipicamente empregada no contexto de uma Operação Militar, apoiando a condução de outros tipos de operação e contribuindo para a obtenção de um efeito desejado. Todavia, suas ações podem não gerar os resultados esperados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados. Devido a esta incerteza, cada operação deve ser planejada e

acompanhada minuciosamente, considerando as particularidades do ciberespaço. (BRASIL, 2017a).

3.1.3 **A Guerra Cibernética como meio não cinético de apoio ao combate**

Para fins de aplicação do poder de combate, estão definidas três capacidades operativas: proteção, exploração e ataque. A atividade de proteção cibernética é de caráter permanente e refere-se à condução de tarefas para neutralizar as ações ofensivas do oponente sobre os ativos computacionais, redes de computadores e de comunicações. A de exploração tem o objetivo de preparar os alvos cibernéticos para ações futuras. Isso se dá por meio do mapeamento dos sistemas e dos ativos de informação presentes no espaço cibernético de interesse, bem como da identificação e exploração de suas vulnerabilidades. Por sua vez o ataque é caracterizado pela interrupção, negação, degradação, corrupção ou destruição de informações, de sistemas, de dispositivos ou de redes computacionais ou de comunicações do oponente, conforme ilustrado na tabela abaixo.

Tabela 1 – Capacidades do SGCEx

Capacidade Operativa	Descrição
Proteção Cibernética	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
Exploração Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

Fonte: Manual de Guerra Cibernética (BRASIL, 2017a)

Das três capacidades operativas descritas acima, as ações de exploração e de ataque cibernético configuram a atuação não cinética da Guerra Cibernética. Seu emprego provoca efeitos no ambiente físico, podendo ser executados simultaneamente às ações cinéticas para causar resultados complementares sobre um mesmo alvo, sem o emprego do fogo cinético. (BRANDÃO; IZYCKI, 2019; BRASIL, 2015; BRASIL 2017a).

Em geral, estas ações afetam as propriedades básicas da segurança da informação: confidencialidade, integridade e disponibilidade. Desta forma, é imprescindível que a análise e o planejamento de Guerra Cibernética sejam orientados por estes elementos, permitindo seu emprego de maneira seletiva e pontual, engajando objetivos elencados pelos diversos níveis (estratégico, operacional e tático). (Vasquez, 2020).

Destaca-se, ainda, a possibilidade de se considerar outros atributos complementares, tais como: autenticidade, confiabilidade, conformidade, legalidade, não repúdio (irretratabilidade) e responsabilidade. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013; BRASIL, 2017a; BRASIL, 2017b).

Com a capacidade de causar danos ou baixas nas estruturas físicas, nos centros de C^2, nas redes de computadores, nos centros de comunicações, afetar o moral das tropas adversárias ou, ainda, reduzir a possibilidade do inimigo de explorar o ambiente operativo, é pelas ações de exploração e de ataque que a Guerra Cibernética se integra à função de combate Fogos (BRASIL, 2015), cuja definição é: [...] um conjunto de atividades, tarefas e sistemas integrados, [que] permitem a aplicação e o controle de fogos, orgânicos ou não, integrados pelos processos de planejamento e coordenação. [...] Para isso, os sistemas de fogos devem estar integrados, considerando os meios conjuntos e incorporando a defesa antiaérea e a capacidade de realizar ações eletrônicas e cibernéticas. (BRASIL, 2015, p. 1-1).

A responsabilidade da integração dos fogos com os atuadores não cinéticos é da célula de Coordenação de Fogos. Para tanto, ela conta com uma equipe multidisciplinar e especializada incumbida de avaliar todas as possibilidades e limitações dos meios disponíveis, buscando a eficácia do apoio de fogo. A tarefa de sincronização desses meios de intervenção no combate é encargo do Grupo Integrado de Seleção e Priorização de Alvos (GISPA). Dentre os elementos que podem integrar esse grupo, o Oficial de Ligação de Guerra Cibernética é responsável pelo assessoramento quanto às possibilidades dos atuadores dessa capacidade. (BRASIL, 2017b).

Em relação aos elementos de Guerra Cibernética com capacidade ofensiva no nível tático, quando for ativada a Estrutura Militar de Defesa, esses poderão englobar uma Força Conjunta de Guerra Cibernética, como Força Componente, para executar as operações cibernéticas em proveito do Teatro de Operações ou da Área de Operações (TO/AO), bem como estruturas de Guerra Cibernética de cada uma das

demais Forças Componentes. Na Força Terrestre Componente (FTC), o planejamento e o assessoramento atinentes às ações cibernéticas ofensivas é encargo do comandante do Batalhão de Guerra Eletrônica, enquanto o comandante do Batalhão de Inteligência Militar é responsável pelas ações de Inteligência Cibernética. (BRASIL, 2011; BRASIL, 2017a).

As principais tarefas atinentes a atividade de proteção cibernética são a gestão de riscos, a consciência situacional, a defesa ativa, a pronta resposta, o forense digital, o teste de artefatos cibernéticos, a conformidade de Segurança da Informação e Comunicações (SIC), a gestão de incidentes de redes, o controle de acesso, a proteção das comunicações, o emprego da criptografia, a implementação de controles de segurança, a segurança física e a gestam da continuidade da missão e recuperação de desastres.

No tocante a atividade de ataque cibernético, as principais tarefas são o reconhecimento, o escaneamento, a manutenção do acesso e a cobertura de rastros.

A atividade de exploração cibernética executa a tarefa de inteligência cibernética, ou seja, realiza ações de busca e de coleta de dados no espaço cibernético, para a produção do conhecimento de inteligência.

Referente às citadas atividades de proteção, ataque e exploração da guerra cibernética, a tabela abaixo, extraída do manual de Guerra Cibernética, detalha as principais tarefas atinentes a cada atividade.

Tabela 2 - As atividades e tarefas da Guerra Cibernética

Atividade	Tarefa
Proteção Cibernética	**Gestão de Riscos** Gerenciar as relações entre ativos de informação, patrimônio digital, ameaças, vulnerabilidades, impactos, probabilidade de ocorrência de incidentes de segurança da informação e riscos. Estabelece o nível de alerta cibernético correspondente e executa o tratamento, a comunicação e a monitoração contínua desses riscos.
	Consciência Situacional Monitorar sistematicamente o espaço cibernético de interesse do EB no tocante à possibilidade de concretização de ameaça, de modo a estar em condições de decidir e aplicar as ações requeridas conforme as condições do espaço cibernético.
	Defesa Ativa Detectar, identificar, avaliar e neutralizar vulnerabilidades nas redes de computadores e sistemas de informação em uso pelo EB, antes que elas sejam exploradas. Mediante ordem, desencadear ações ofensivas contra a fonte da ameaça, mesmo que localizada fora do espaço cibernético defendido.
	Pronta Resposta Reagir prontamente às ameaças identificadas, observando os diferentes níveis de alerta cibernético (grau de risco).

(continua)

(continuação)
Tabela 2 - As atividades e tarefas da Guerra Cibernética

Atividade	Tarefa
Proteção Cibernética	**Teste de Artefatos Cibernéticos** Testar, simular, analisar, avaliar e homologar artefatos e sistemas cibernéticos.
	Conformidade de SIC Verificar a observância de aspectos legais, normativos e procedimentais de SIC no âmbito do SGCEx.
	Gestão de Incidentes de Redes Coordenar o tratamento de incidentes nas redes de interesse, acompanhar a solução e acionar procedimentos.
	Controle de Acesso Permitir que os administradores e gerentes determinem o que os indivíduos podem acessar, de acordo com sua credenciais de segurança, após a autorização, a autenticação, o controle e a monitoração dessas atividades.
	Proteção das comunicações Examinar os sistemas de comunicações internos, externos, públicos e privados; estruturas de rede; dispositivos; protocolos; acesso remoto e administração.
	Emprego de Criptografia Empregar técnicas, abordagens e tecnologias de criptografia.
	Implementação de controles de segurança Controlar atividades de pessoal e procedimentos de segurança, na utilização dos sistemas necessários às atividades na área cibernética.
	Segurança Física Autorizar a entrada e estabelecer os procedimentos de segurança do ambiente operativo, a fim de proteger instalações, equipamentos, dados, mídias e pessoal contra ameaças físicas aos ativos de informação.
	Gestão da Continuidade da Missão e Recuperação de Desastres Preservar as atividades operativas por ocasião da ocorrência de interrupções ou de catástrofes.
Ataque Cibernético	**Reconhecimento** Investigar em fontes abertas para obter informações sobre o alvo.
	Escaneamento (*Scanning*) Encontrar falhas na proteção cibernética do alvo.
	Exploração da Vulnerabilidade Realizar ações como: obter acesso, degradar uma aplicação ou negar acesso para outros usuários.
	Manutenção do acesso Manipular *software* instalado no sistema alvo com objetivo de disponibilizar um *backdoor* para acesso futuro.
	Cobertura de rastros Ocultar as ações realizadas no sistema alvo com objetivo de impedir ou dificultar que usuários e/ou administradores identifiquem as ações de um atacante.
Exploração Cibernética	**Inteligência Cibernética** Realizar ações de busca e de coleta de dados no espaço cibernético, para a produção do conhecimento de Inteligência.

Fonte: Manual de Guerra Cibernética (BRASIL, 2017a)

O entendimento destes conceitos basilares de cada atividade da guerra cibernética torna-se fundamental para o restante da pesquisa, pois servirá de base para os assuntos a serem trabalhados nos próximos capítulos.

3.2 O CRESCENTE USO DE ARMAMENTOS E EQUIPAMENTOS DEPENDENTES DE MEIOS DE TI

Conforme Eduardo Arthur Izycki, analista no Gabinete de Segurança Institucional, dedicado à proteção de infraestruturas críticas, verificam-se, abaixo, conceitos recentes e atuais de exemplos de emprego de meios dependentes de redes

vulneráveis a ataques cibernéticos, além de ressaltar a importância da cibernética nos embates do futuro:

> Nos conflitos do futuro, bits e bytes serão tão comuns quanto balas e bombas. Essa relevância se dá em dois sentidos. Primeiramente, o controle da cibernética será essencial para quaisquer ações conflituosas nos espaços físicos (terra, mar, ar e espaço), pois dela dependem as comunicações, a visualização de alvos, a guiagem de mísseis e o exercício de comando e controle, entre outras. Segundo, a cibernética passou a ser um novo domínio no qual Estados rivalizam, somando-se à terra, mar, ar e espaço, mas diferindo deles porque têm geografia mutável. A cibernética passa a ser, assim, não somente meio que possibilita a realização de agressões físicas, mas também novo ambiente em que conflitos são travados. (IZYCKI, 2019).

Nesse sentido, verifica-se a tendência ao uso crescente de armamentos e equipamentos em combate, dependentes de tecnologias de informação e comunicações (TIC) em rede, como sistemas de armas remotamente controlados, SARP, radares, sensores, sistemas de comando e controle, além de sistemas e meios de ataque e interferência cibernética.

Na atual concepção de não-Guerra, a doutrina de Guerra Cibernética do Brasil está vocacionada para a Defesa Cibernética, exemplificada pela criação de mecanismos de proteção e defesa, como o Comando de Defesa Cibernética, composto por militares da Marinha, do Exército e da Força Aérea. Sua consolidação como Comando Operacional Conjunto, acabou integrando a estrutura regimental do Exército Brasileiro, objetivando manter um bom nível de operacionalidade e possuir capacidade de atuar de várias formas no cenário cibernético.

Já em outra realidade, como na Guerra da Rússia contra a Ucrânia, diversos meios de comunicação publicaram notas nas quais o governo Norte Americano acusou a Rússia de ter realizado ataques cibernéticos à Ucrânia. (BBC NEWS, 2022).

A multinacional Microsoft confirmou os ataques Russos a várias plataformas digitais ucranianas, conforme a transcrição abaixo:

> Rússia coordena ataques cibernéticos e militares na Ucrânia, diz Microsoft
> O relatório assinala que, na primeira semana da invasão, hackers russos atacaram uma importante emissora ucraniana “no mesmo dia em que o exército russo anunciou sua intenção de destruir os alvos de ‘desinformação’ ucranianos e dirigiu um ataque com mísseis contra uma torre de televisão em Kiev”. A corporação americana ressaltou que o objetivo desses ataques coordenados era “atrapalhar ou degradar as funções militares e governamentais da Ucrânia e solapar a confiança do público nessas mesmas instituições”. Além disso, a Microsoft detalhou que havia detectado quase 40 ataques cibernéticos destrutivos, voltados contra centenas de sistemas, um terço dos quais foram direcionados contra organizações governamentais ucranianas em todos os níveis, desde o nacional até o local, enquanto outros 40% tinham como alvo a infraestrutura crítica do país. (JOVEN PAN NEWS, 2022).

Já o professor de Direito e Coordenador do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (FGV), LUCA BELLI, fez as seguintes colocações em reportagem a CNN:

> “A guerra que estamos presenciando acontece de forma híbrida. Junto com a invasão militar mais clássica, com tanques, temos agora uma invasão cibernética. Além da inutilização de sites, é bem provável que os sistemas de energia, telecomunicações e redes de internet sejam severamente interrompidos na Ucrânia para criar caos durante a invasão. A população sem eletricidade, acesso à televisão e à internet, não consegue se organizar. E isso facilita muito a invasão russa. Os russos dispõem de tecnologia de ponta e vão utilizar tudo o que for possível para vencer a guerra”, afirma o Coordenador do Centro de Tecnologia e Sociedade da FGV. (BELLI, 2022).

Nessa conjuntura, os meios de Guerra Cibernética do Brasil, embora vocacionados para a Defesa em tempos de paz, devem adquirir e manter capacidades de ataque em caso de guerra, além de estar em condições de aumentar suas ações de segurança cibernética para proteger os sistemas em rede do Estado e de defesa. Dessa forma, além do evidente efeito dissuasório da capacidade citada, o País elevará seu poder de combate na medida que agregará capacidades operativas aos sistemas de comando e controle e, em um futuro próximo, aos sistemas de armas de altíssima tecnologia dependentes de redes de TI.

Ainda nesse cenário, merecem destaque as medidas de proteção cibernética em todos os tipos de tropa, visando dificultar a atuação da Guerra Cibernética Inimiga sobre os sistemas de comando e controle da Força Terrestre. Conforme o Manual MD30-M-01 – Doutrina de Operações Conjuntas 2º Volume, verificam-se as seguintes características da Guerra Cibernética e dos sistemas e equipamentos:

> 2.2.2.4. Características dos sistemas e equipamentos: listar os sistemas e equipamentos de comunicações, de guerra eletrônica e guerra cibernética que possam influenciar as ações de comando e controle, vinculados às forças com suas características conhecidas, bem como mencionar sucintamente os procedimentos operacionais conhecidos ou supostos relacionados com as atividades de comando e controle.
> 2.3.9 Guerra cibernética**:** descrição sucinta e ampla sobre a capacidade de ataque, exploração e defesa cibernética em prol dos sistemas de C² da operação. Os aspectos aqui descritos devem ser coordenados com a célula de cibernética e evitar que dados lançados nesse campo sejam redundantes. (BRASIL, 2020a).

A citação acima descreve algumas ações que podem ser desenvolvidas pela Guerra Cibernética sobre os sistemas de C² de uma operação. Com isso, reforça a responsabilidade de todos os níveis de comando para com medidas de proteção e defesa cibernética, sempre em coordenação com a célula de cibernética do Grande Comando Operacional enquadrante.

4 A FORMAÇÃO DE OFICIAIS E PRAÇAS

4.1 ASPECTOS DA FORMAÇÃO DE RECURSOS HUMANOS

O Ensino Profissional no Exército é realizado por meio de dois sistemas distintos, porém integrados: o Sistema de Ensino Militar e o Sistema de Instrução Militar do Exército Brasileiro (SIMEB). (BRASIL, 2018).

O Sistema de Instrução Militar do Exército Brasileiro (SIMEB) é voltado para o adestramento da Força Terrestre como instrumento de combate, para a formação das praças temporárias e para a adaptação de técnicos civis à vida militar. Esse sistema é coordenado pelo Comando de Operações Terrestres (COTER). (BRASIL, 2018).

Já o Sistema de Ensino do Exército abarca a formação de Oficiais e Sargentos em escolas militares próprias, das quais pode-se destacar a Academia Militar das Agulhas Negras (AMAN) como principal formadora de oficiais do Exército, e a Escola de Sargentos das Armas (ESA), como principal instituição de ensino militar formadora de sargentos da Força Terrestre, as quais foram o foco de estudo da formação inicial básica em Cibernética desta pesquisa.

Da mesma forma, a Marinha e a Força Aérea possuem escolas congêneres formadoras de oficiais e praças, como a Escola Naval (EN) e a Academia da Força Aérea (AFA), formadores de oficiais das respectivas forças, as quais não foram objetos de estudo neste trabalho.

Além disso, a especialização em Proteção e Guerra Cibernética é realizada em Estabelecimentos de Ensino subordinados ao Comando de Comunicações e Guerra Eletrônica do Exército e vinculados à Diretoria de Educação Técnica Militar, para fins de orientação técnico-pedagógica. Nesse contexto, a EsCom e o CIGE oferecem cursos de extensão e de especialização para oficiais e praças nas áreas das comunicações, eletrônica e informática e, ainda, contribuem para a formulação da doutrina militar específica.

Acerca da inserção do assunto cibernética nos Planos de Disciplina das referidas escolas, verifica-se que todas vêm implementando melhorias na formação e especialização de seus alunos, especialmente no tocante a Proteção Cibernética.

Como já mencionado, especificamente sobre a AMAN, a ESA, a EsCom e o CIGE, alguns aspectos envoltos a matéria serão trabalhados a seguir, iniciando-se pela análise de respostas à perguntas comuns que se enquadram a todas as Escolas

participantes do questionário remetido ao comando dos estabelecimentos de ensino citados, respondido por seus instrutores e monitores, e um destinado a militares com cursos ou que trabalham na área da cibernética (especialistas).

Qual a necessidade/ frequência de atualização de conhecimento/ cursos na área para manter-se em dia com as novidades e tecnologias disruptivas?

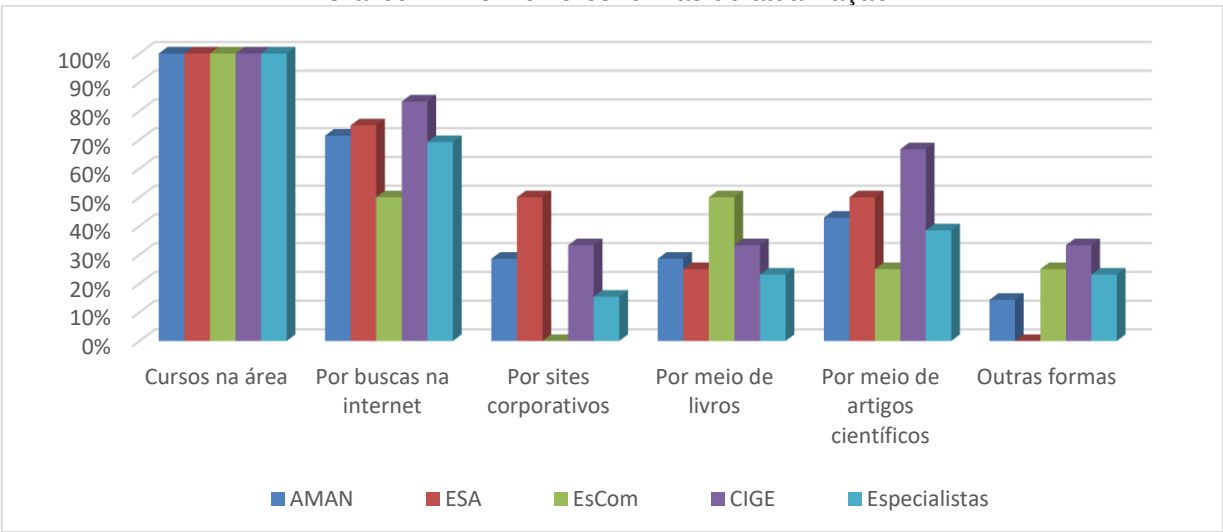
Gráfico 1 – A necessidade de atualização de conhecimento

Fonte: o autor

Conforme o gráfico acima, a maioria considerou que a necessidade/ frequência de atualização de conhecimento/ cursos na área, para manter-se em dia com as novidades e tecnologias disruptivas, deve ser constante e com periodicidade diária ou semanal.

Qual(ais) a(s) melhor(es) forma de atualização?

Gráfico 2 – As melhores formas de atualização



Fonte: o autor

Conforme o gráfico acima, a maioria considerou que as melhores formas de atualização são por meio de cursos na área e por buscas na internet. Além disso, foram elencadas outras formas de manter-se atualizado, como por meio da participação em congressos e competições, do Instituto Rondon de Capacitação Continuada (IRCC), da Escola Nacional de Defesa Cibernética, de intercâmbios com

outras instituições, como universidades e forças policiais, por meio de fóruns e Chats no Discord e no Telegram, em Workshops e outros eventos colaborativos entre as Forças e empresas relevantes do setor. Ainda, citou-se a atualização por meio de atividades reais, na qual se aprende executando, sem soluções publicadas em fóruns.

Cabe destacar que o universo cibernético é muito extenso e algumas áreas se atualizam muito mais do que outras. Geralmente, os assuntos ensinados aos alunos em escolas de formação, como na AMAN e na ESA, apresentam uma evolução em ritmo menos veloz, dado que focam mais em conceitos basilares, especialmente ligados a proteção cibernética.

Existe alguma plataforma corporativa que permita, apoie ou facilite essa atualização?

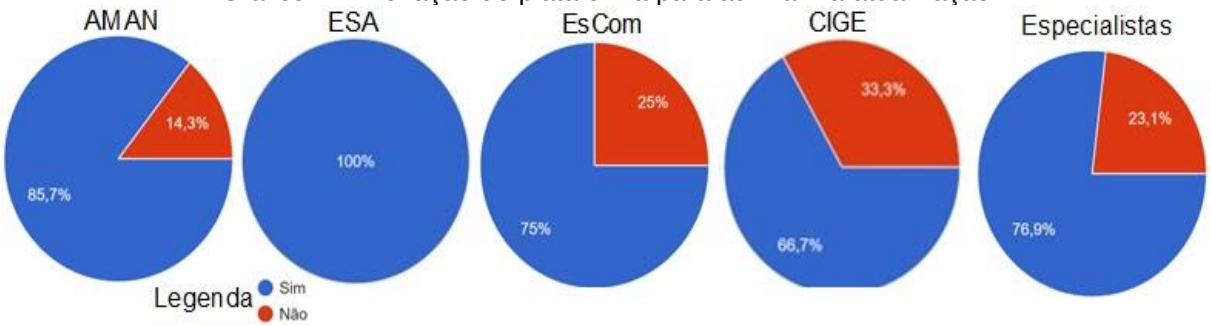
Gráfico 3 – A existência de alguma plataforma corporativa

Fonte: o autor

Conforme o gráfico acima, a maioria considerou não existir ou desconhecer uma plataforma corporativa para atualização.

Seria interessante a criação de uma plataforma que permitisse essa constante atualização, que trouxesse as novidades e inovações aos interessados, além de realizar constante reciclagem nos especialistas na área?

Gráfico 4 – A criação de plataforma para auxiliar na atualização

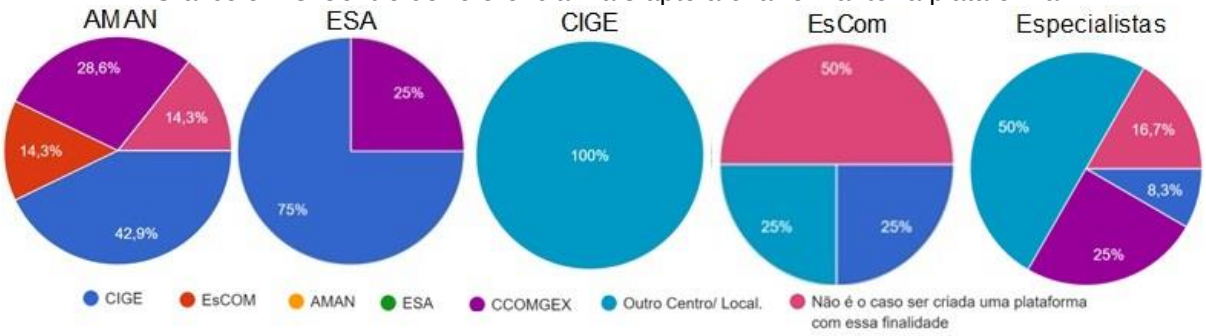


Fonte: o autor

Conforme o gráfico acima, a grande maioria considerou que seria interessante a criação de uma plataforma que permitisse e facilitasse essa constante atualização.

Qual seria o Centro de referência mais apto a criar e manter uma plataforma que atendesse a essa necessidade?

Gráfico 5 – O Centro de referência mais apto a criar e manter a plataforma

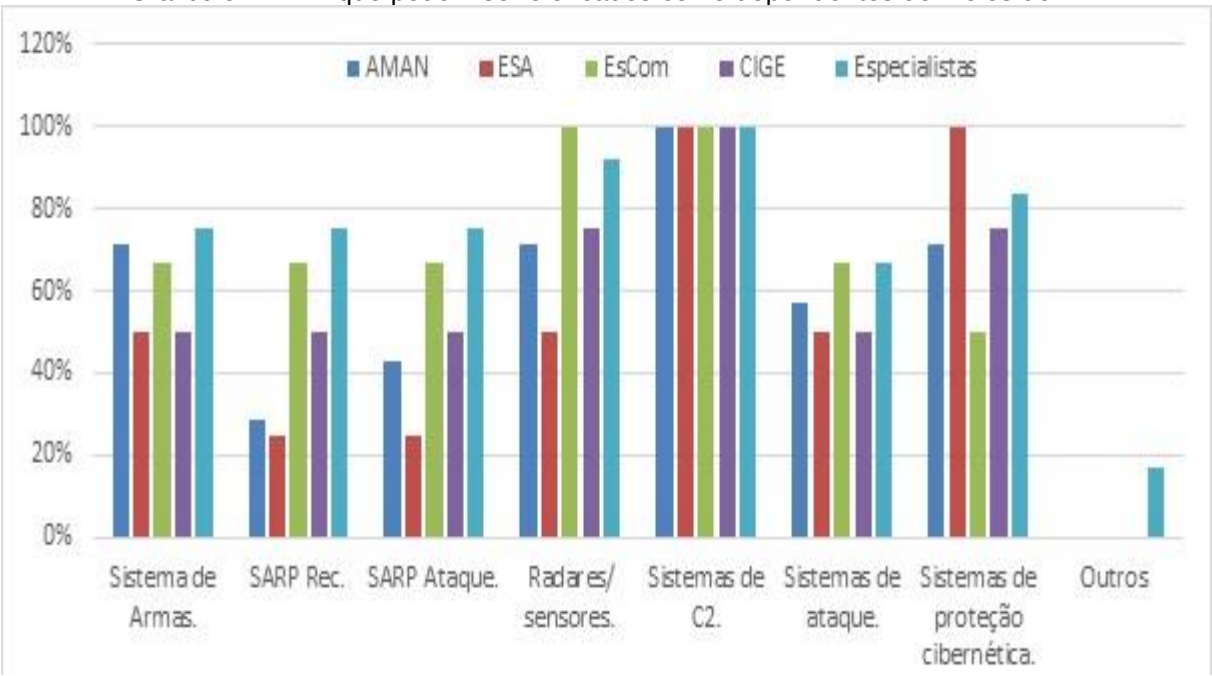


Fonte: o autor

Conforme o gráfico acima, grande parcela da AMAN e da ESA considerou que o CIGE seria o Centro de referência mais apto para criar e manter uma plataforma que atendesse a necessidade em pauta. Já nas demais escolas e para os especialistas, outros locais foram considerados como ideais, como o Comando de Defesa Cibernética (Com D Ciber), a Escola Nacional de Defesa Cibernética (ENaDCiber) e até mesmo um local específico para o desenvolvimento dessa ferramenta, uma vez que não é a atividade fim das Organizações Militares relacionadas.

Quais Meios de Emprego Militar (MEM) podem ser elencados como dependentes de meios de TI, como armamentos e/ ou equipamentos, e que são ou que poderiam ser destacados como vulneráveis a atuação da G Ciber?

Gráfico 6 – MEM que podem ser elencados como dependentes de meios de TI



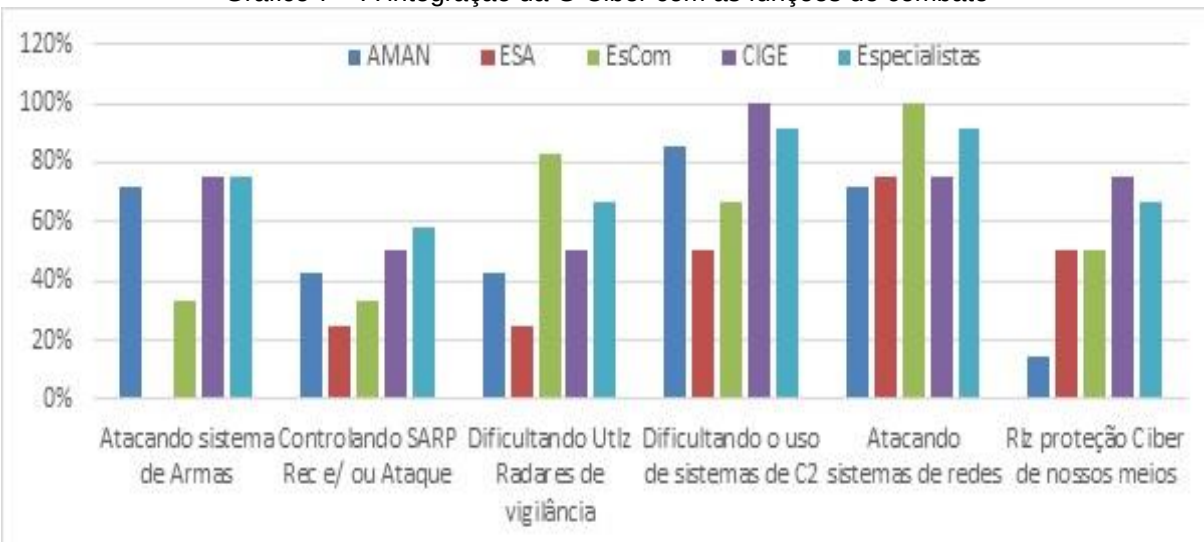
Fonte: o autor

Conforme o gráfico acima, todos os MEM dependentes de meios de TI podem ser elencados como vulneráveis a atuação da G Ciber, com destaque para os sistemas de C^2, de proteção cibernética e os radares e sensores.

Ademais, foram citados alguns outros exemplos que podem sofrer interferências cibernéticas, como os sistemas de um Centro de Comunicações Informatizado (C^2 em Combate, VOIp, Terminais de Satélite, Videoconferência, SPED, ZIMBRA, SPED Operacional), quaisquer rádios que funcionem baseados em IP, servidores, equipamentos de rede, computadores, celulares e sistemas de arma que dependam de meios de TI, Bateria Astros e até o Caça Gripen (no momento da atualização de seus sistemas). Os SARP são mais suscetíveis a ação da GE para serem derrubados do que da G Ciber, porém é possível atacá-los. Ainda, outros exemplos de alvos são o Sistema de Controle de Pessoal (SICAPEX), o CPEx (Centro de Pagamento do Exército), o Sistema Pacificador (com localização de tropas em operações reais), Firewalls, roteadores e câmeras IP de monitoramento. Em suma, todos os MEM que estão conectados podem sofrer interferências cibernéticas.

De que maneira a G Ciber pode ser integrada as Funções de Combate (Movimento e Manobra, Inteligência, Fogos, Comando e Controle, Proteção e Logística), potencializando os efeitos dessas no combate?

Gráfico 7 – A integração da G Ciber com as funções de combate



Fonte: o autor

Conforme o gráfico acima, todas as maneiras e formas citadas podem integrar a G Ciber às Funções de Combate e potencializar seus efeitos, com destaque para o ataque à sistemas de redes e a ação de dificultar o uso de sistemas de C^2.

Ademais, foram realizadas outras considerações e detalhamentos acerca dessa integração, como por meio da exploração de todos os ativos que utilizam meios computacionais, o uso de “dashboards” para visualizar todos os dados de log e criação de alertas dos perímetros. Além disso, deve-se ter em mente que o emprego da G

Ciber deve ser contínuo e ininterrupto, pois é um grande erro pensar que a G Ciber será empregada apenas no contexto de um Teatro de Operações.

Em um teatro de operações, no desdobramento de uma brigada, existe uma dependência de enlaces de micro-ondas para fornecer os links de rede. Se a Guerra Eletrônica (GE) inimiga for capaz de interferir neste sinal, haverá uma perda de comunicação por meios de TI (comando e controle/ Logística). Se a G Ciber puder aproveitar essa interferência para capturar pacotes, toda a informação que ali trafegar pode ser capturada (inteligência). Da mesma forma, é possível realizar um ataque man-in-the-middle (forma de ataque em que os dados trocados entre duas partes são de alguma forma interceptados, registrados e, possivelmente, alterados pelo atacante sem que as vítimas se apercebam) (comando e controle/ inteligência). Porém, o principal vetor de acesso será o celular/ computador do militar conectado à internet através desses links da brigada, que pode ser alvo de phishing ou receber um arquivo malicioso e dar acesso à rede interna. Se o oponente conseguir escalar privilégio nessa rede, pode roubar dados ou interromper o funcionamento dos sistemas (inteligência e C^2), pode atacar o SARP e, se conseguir escalar privilégio no sistema de controle das aeronaves, pode tomar o controle dele (fogos, inteligência). Se atacar um radar, pode projetar uma leitura falsa e provocar gastos de munição ou então desabilitá-lo (fogos). A proteção cibernética pode ser feita isolando a rede da internet, impedindo o uso de dispositivos pessoais nesta rede e tendo um controle de emissões consciente. A ação de proteção deve ser realizada, principalmente, para evitar deixar meios de acesso ao oponente e monitorar com regras, extremamente restritivas, aqueles que forem imprescindíveis.

Sobre as formas gerais de ataques cibernéticos, podem ser realizados por meio de uma boa engenharia social, força bruta, DoS, Envenenamento de MAC e formas de Injeção de SQL, o que poderá inviabilizar o bom funcionamento dos meios atacados. Nesse contexto, os ataques cibernéticos poderiam apoiar a função de combate fogos e movimento e manobra, realizando ataques não cinéticos ao inimigo.

Como exemplos de ataques Ciber, em um sistema de armas poderia impedir o lançamento de uma bateria astros; sobre um SARP poderia ser realizado um ataque anterior a utilização do SARP e configurado uma função nova ou modificar uma função pré-definida; em radares, se os mesmos estiverem linkados em rede com um centro de comando, este pode ser atacado e perder a eficiência; sobre meios de C^2, ao identificar os protocolos utilizados, pode-se negar os serviços dos meios de comande

e controle. Em suma, qualquer sistema de MEM que transmita ou receba informações está vulnerável, a exemplo do sistema de armas da Viatura Guarani, que possui rádios integrados em rede e pode ser atacado, sendo o rádio a porta de entrada para os sistemas do carro.

Na exploração, as informações capturadas podem apoiar a função de combate inteligência. As ações de coleta e busca de dados em redes de dados inimigas, por meio da exploração cibernética, podem ser fontes importantes de obtenção, levantando informações de interesse para a inteligência por meio de corrupção das redes inimigas.

Por fim, na prevenção de ataques cibernéticos, uma boa medida é a capacitação de pessoal e equipamentos e o uso aperfeiçoado do sistema MTO (produção sob encomenda), na qual os sistemas são restritos e controlados para mitigar as vulnerabilidades. Nesse sentido, em apoio a função de combate proteção, seriam realizadas ações de neutralização a ataques e exploração inimigas, por meio da proteção cibernética. Uma das formas de verificação dos níveis de vulnerabilidade é com a realização de teste de penetração em nossas redes, para assegurar que os sistemas estão com um resiliência desejável.

4.2 A FORMAÇÃO DE OFICIAIS

A Academia Militar das Agulhas Negras (AMAN) é a instituição de ensino superior referência na formação dos oficiais de carreira combatentes do Exército Brasileiro. Conforme extraído abaixo de seu site, verifica-se o compromentimento da Escola com a formação dos futuros líderes da Força Terrestre.

> A Academia Militar das Agulhas Negras (AMAN) é a instituição de ensino superior responsável pela formação dos oficiais combatentes de carreira do Exército Brasileiro.
>
> Sua história tem início em 1810, com a criação da Academia Real Militar pelo Príncipe Regente D. João, sendo, inicialmente, instalada na Casa do Trem, no Rio de Janeiro, hoje Museu Histórico Nacional.
>
> Hoje, o ensino na Academia Militar é baseado em conceitos metodológicos modernos, buscando o desenvolvimento de competências indispensáveis para os “Líderes da Era do Conhecimento”. As metodologias atividades de aprendizagem e a mobilização e integração de saberes para a resolução de problemas são as realidades pedagógicas da AMAN.
>
> Com conhecimentos, habilidades e atitudes forjados por valores cívicos e morais e pelas raízes históricas e tradições do Exército Brasileiro, é na AMAN que o futuro oficial desenvolve suas virtudes militares, tornando-se um profissional identificado com os mais nobres sentimentos de “servir” à Nação Brasileira, comprometido com o Exército e capaz de participar da defesa da Pátria (AMAN, 2019).

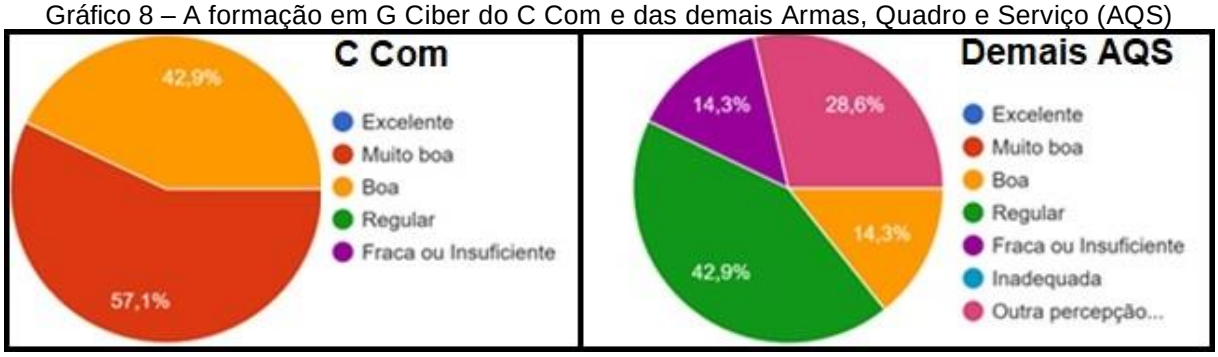
Nesse contexto, a AMAN criou a partir de 2012, a cadeira de cibernética, com a finalidade de ministrar o assunto a todos os Cadetes lá formados, e não somente o Curso de Comunicações, conforme ocorria anteriormente. Abaixo, segue a descrição do site do Estabelecimento de Ensino acerca da referida cadeira.

> A Cadeira de Cibernética da Divisão de Ensino da AMAN ministra, atualmente, a disciplina de Cibernética II que, além de focalizar as competências do Oficial de Informática previstas no RISG, aborda ações cibernéticas defensivas e possui uma infraestrutura física com 04 (quatro) laboratórios (cada um com 45 computadores) e 03 (três) salas de aula, além de uma sala onde estão os servidores que hospedam serviços que permitem ministrar aulas práticas aos Cadetes.
>
> A estrutura atual se originou de um projeto iniciado em 2012 que teve como escopo a readequação da infraestrutura elétrica, aquisição de equipamentos de TI (computadores, servidores, switches, nobreaks, etc), instalação de cabeamento para rede de dados, aquisição de mobiliário (bancadas e cadeiras). Posteriormente, em 2014 e no início de 2015, um novo projeto executado pelo próprio pessoal da Cadeira, teve como objetivo a instalação e configuração dos equipamentos de TI adquiridos para a Cadeira de Cibernética. No ano de 2016, a Cadeira de Cibernética deu início ao Projeto de Reestruturação de Ensino de Cibernética na AMAN, juntando com o Curso de Comunicações, iniciando os trabalhos de atualização do material didático e de sua infraestrutura física (AMAN, 2017).

Conforme descrito acima, a matéria vem sendo reestruturada desde 2016, buscando aperfeiçoar e atualizar o material didático e sua infraestrutura, fato que corrobora com a relevância da presente pesquisa. Destarte, a seguir passar-se-a a analisar as respostas aos questionários respondidos pelos instrutores e monitores da referida Cadeira e do C Com da AMAN.

Qual a sua análise sobre a formação em G Ciber do Curso de Comunicações e das demais Armas, Quadro e Serviço (AQS) da AMAN?

Gráfico 8 – A formação em G Ciber do C Com e das demais Armas, Quadro e Serviço (AQS)



Fonte: o autor

Conforme o gráfico acima, a formação dos cadetes do C Com é muito superior aos das demais Armas, Quadro e Serviço (AQS). Além disso, merecem destaque algumas considerações, como a necessidade de uma inclusão mais efetiva de cibernética nas demais AQS, pois atualmente o cadete tem contato com cibernética no 1º ano e se for para o Curso de Comunicações. Dessa forma, as demais AQS

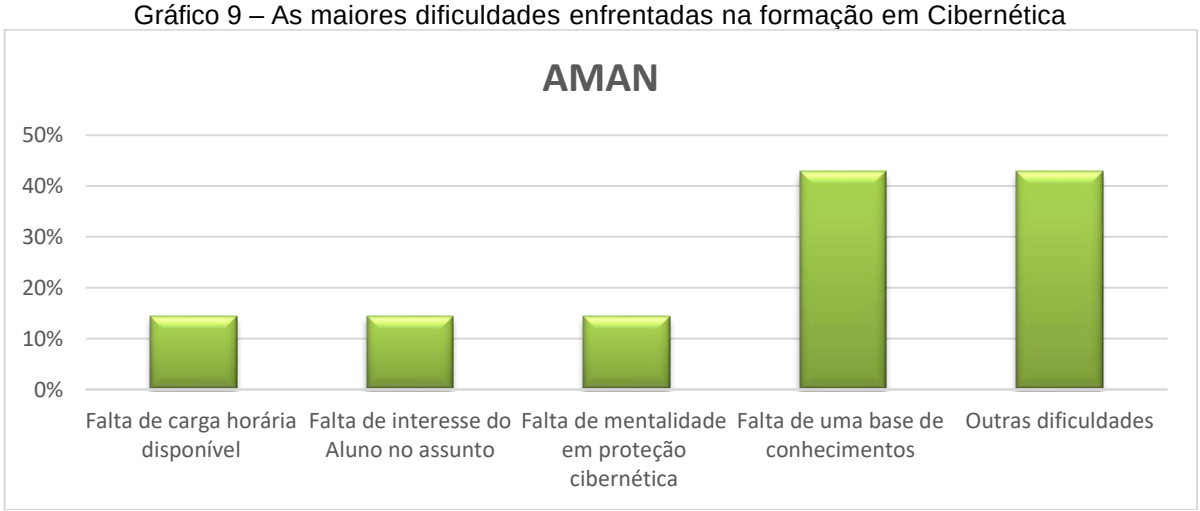
acabam não compreendendo adequadamente o papel da cibernética e, principalmente, da guerra cibernética, até pela conjunção de termos, uma vez que a cibernética e a guerra cibernética são termos semelhantes e, muitas vezes, utilizados de forma intercambiável.

Nesse sentido, pode-se esclarecer que a cibernética que o Cadete de Comunicações aprende é voltada para o fornecimento de ferramentas de TI, para o exercício do Comando e Controle. O militar capaz de realizar guerra cibernética é vocacionado ao ataque e exploração, ou seja, utilizar-se das infraestruturas de TI para atingir quaisquer alvos e objetivos no "espaço cibernético". Porém, na realidade, a percepção das demais AQS é que todos são a mesma coisa e, por vezes, querem que o Cadete seja capaz de realizar ataques, bem como um guerreiro cibernético seja capaz de fornecer meios de TI, o que foge de suas finalidades. Assim, as demais AQS devem ser formadas para conhecerem essa diferença e, principalmente, para serem capazes de acessar os sistemas fornecidos pelas comunicações, bem como agir individualmente pela segurança da informação na ponta da linha.

Para traçar um paralelo: O comunicante tem que saber atirar com seu fuzil, progredir e manobrar a sua tropa para não depender da infantaria para se defender de fustigações e escaramuças. Da mesma forma, o infante tem que saber proceder com o seu computador, celular e demais meios de TI para usar os sistemas sem sobrecarregar o comunicante e não ser vítima de um ataque cibernético simples, como um “phishing”, engenharia social ou até mesmo deixar informação sensível por um uso irresponsável dos sistemas.

Quais são as maiores dificuldades enfrentadas durante a formação do Cadete em Cibernética?

Gráfico 9 – As maiores dificuldades enfrentadas na formação em Cibernética

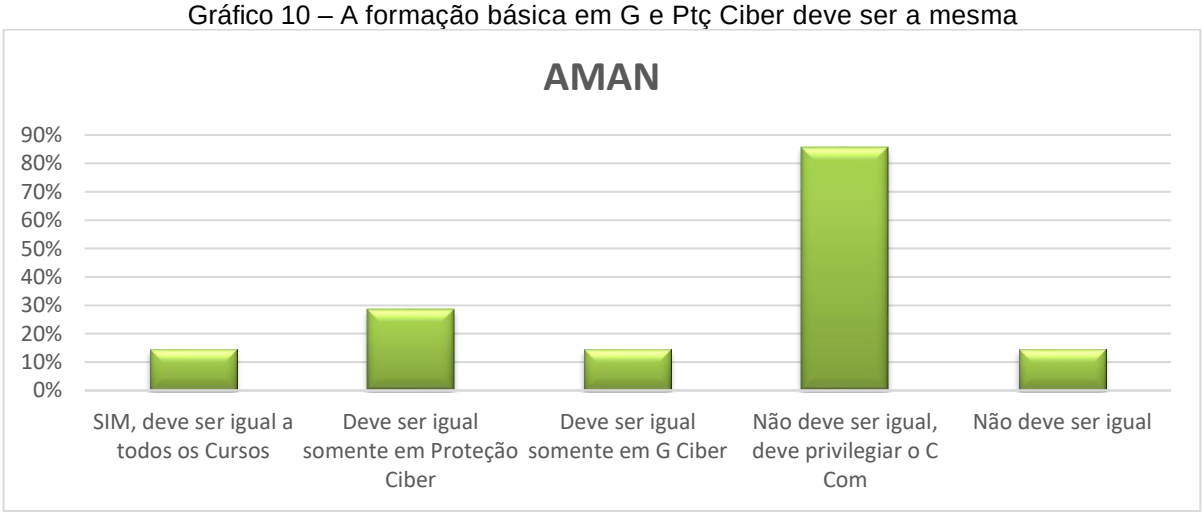


Fonte: o autor

Conforme o gráfico 10 acima, a maior dificuldade enfrentada durante a formação do Cadete em Cibernética é a falta de uma base de conhecimentos, a exemplo da transmitida a militares da Arma de Com, para que o assunto seja mais aprofundado para militares de outros cursos. Outras dificuldades foram elencadas, como deficiência em infraestrutura, falta de tempo e recursos para o instrutor se aperfeiçoar na atividade, uma vez que o instrutor acaba se envolvendo com a administração. Ademais, invariavelmente, o Cadete que não deseja ir para as comunicações terá uma aversão pelo tema, mas é necessário ensinar-lhe o básico para acessar os sistemas fornecidos pelas comunicações, entender os procedimentos e ferramentas de segurança e, principalmente, ser adestrado em procedimentos individuais de segurança da informação, no nível do usuário, sob risco de comprometer a necessária proteção cibernética de nossas tropas.

Em sua opinião, a formação básica em Guerra e Proteção Cibernética deve ser a mesma para todas as Armas, Quadros e Serviço?

Gráfico 10 – A formação básica em G e Ptç Ciber deve ser a mesma



Fonte: o autor

Conforme o gráfico acima, a maioria considerou que a formação básica em Guerra e Proteção Cibernética não deve ser a mesma para todas as Armas, Quadro e Serviço. Como justificativas, pode-se destacar que a formação deve manter-se mais aprofundada na arma de comunicações, uma vez que seus cadetes passam 03 anos recebendo instruções sobre o tema.

No tocante a formação para ataque cibernético, exige-se um conhecimento prévio de TI, Redes, Sistemas e Linux, entre outros. Se incluirmos tudo isso em todas as AQS seria impraticável dada a carga horária necessária. Cabe salientar que as matérias de cibernética do Curso de Com somam mais de 300h/aula anuais, e o cadete ainda sai com um entendimento básico da maioria dos temas, sendo

necessário estudo e dedicação pessoal daquele que aspira ser um guerreiro cibernético.

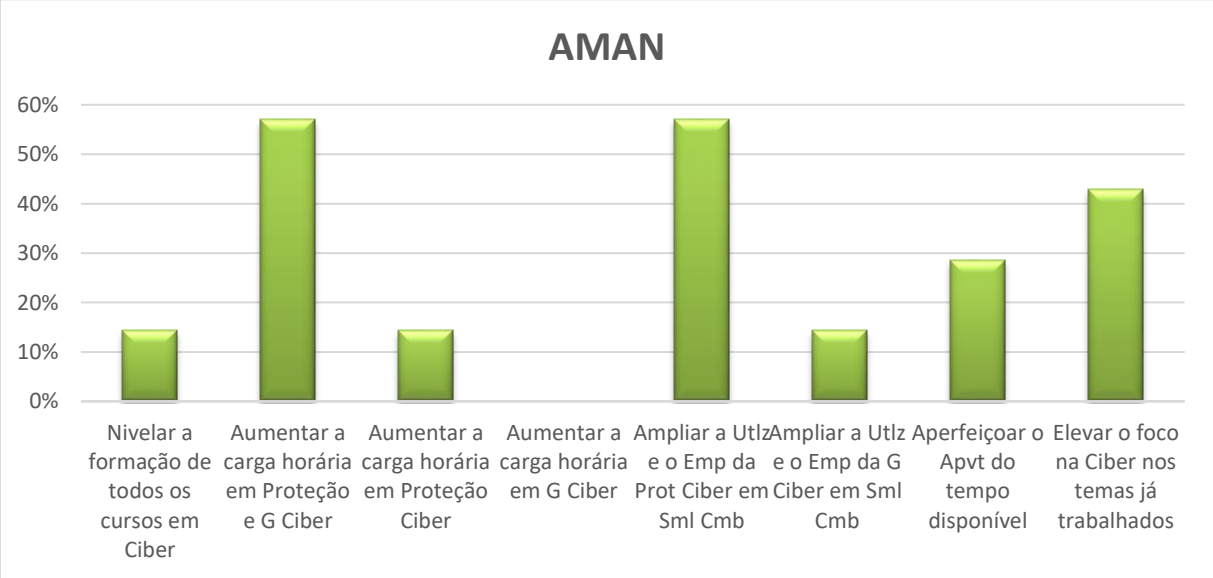
Atinente a proteção e a defesa cibernética, as demais AQS devem ser encaradas como usuárias dos sistemas, e o comunicante como administrador deles. Portanto, a cada um deve ser ensinado conforme a sua responsabilidade no uso e gestão dos meios de TI. O usuário deve ser capaz de identificar possíveis ações cibernéticas e agir individualmente para não ser vítima delas, bem como informar aos administradores. Já o administrador deve saber implementar ferramentas de segurança, implementar políticas de segurança da informação e realizar a proteção e a busca ativa de ameaças em seu sistema.

Nesse contexto, embora a mentalidade de Proteção Cibernética seja de responsabilidade de todas as Armas, Quadro e Serviço, o Comunicante trabalha diariamente com sistemas que devem ser protegidos e possui uma carga horária de instruções muito maior. Assim, torna-se muito difícil aumentar as instruções de Cibernética nas outras Armas, em detrimento de instruções específicas e peculiares de cada curso.

Por fim, os cadetes de comunicações, de fato, irão realizar atividades de proteção cibernética na tropa, ao contrário dos demais cadetes, aos quais um conhecimento básico acerca das possibilidades e limitações da G Ciber é suficiente para cumprirem suas missões.

Quais medidas o Sr. visualiza que poderiam ser incrementadas na formação em Cibernética do Cadete, especialmente com foco na proteção?

Gráfico 11 – As medidas a serem incrementadas na formação em Cibernética



Fonte: o autor

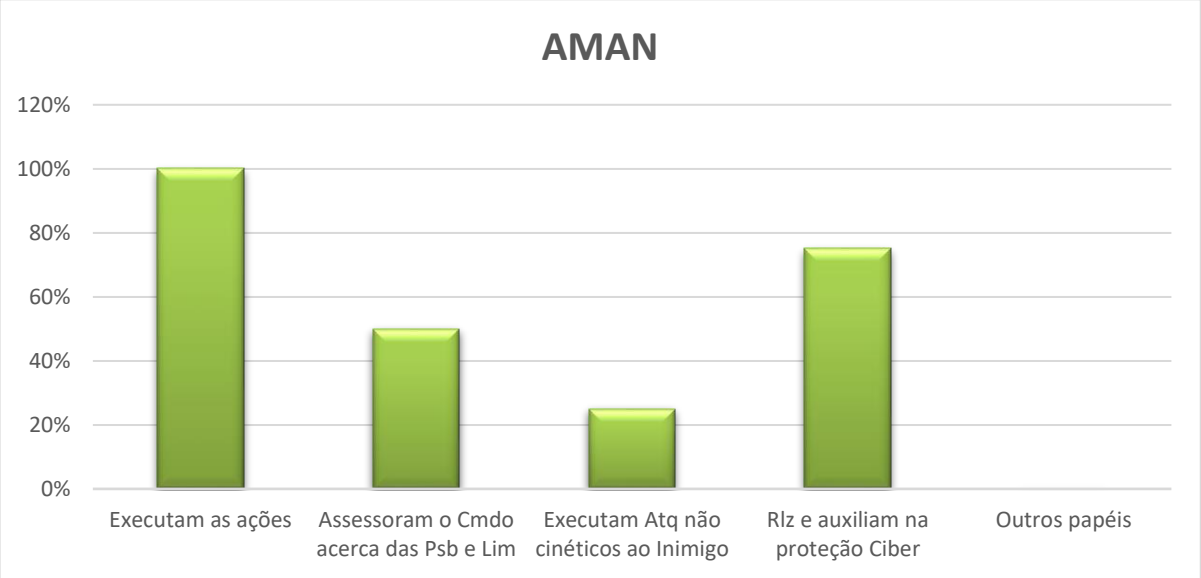
Conforme o gráfico acima, a maioria considerou a formação em Cibernética pode ser aprimorada com a ampliação da carga horária e da utilização e do emprego da Guerra Cibernética em simulações virtuais, construtivas e reais de combate, elevando o foco do assunto nos temas já trabalhados na escola.

Acerca do questionamento se seria possível uniformizar o PLADIS de todos os cursos no assunto, a maioria considerou que a uniformização do PLADIS de todos os cursos em cibernética não seria viável. Como justificativas, verifica-se que a gama de conhecimento para trabalhar na área é muito grande, envolvendo programação, sistemas operacionais, protocolos de comunicação e criptografia, entre outros, o que exigiria um conjunto de pré-requisitos maior que não podem ser passados a todos os cursos de formação, devido às limitações de carga horária. Além disso, cada arma tem sua missão, como no caso das comunicações, que é instalar, explorar, manter e proteger os meios de comando e controle que, atualmente, envolvem a TI e, por conseguinte, a cibernética. Já as demais AQS devem focar na mentalidade de formar um usuário consciente na utilização de todos os sistemas de redes instalados, visando mitigar o risco do fator humano no comprometimento da proteção cibernética.

Acerca do questionamento se o estudo mais aprofundado das possíveis ameaças aos sistemas, dependentes de meios de TI, aperfeiçoaria a formação do futuro oficial no assunto em tela, todos consideraram que o referido estudo aperfeiçoaria a formação do cadete em G Ciber.

E qual o papel e a importância dos operadores nas formas de integração da Cibernética (Atq e Def) com as funções de Combate?

Gráfico 12 – Os operadores na integração da cibernética com as F Cmb



Fonte: o autor

Conforme o gráfico acima, todas as ações apresentadas expressam o papel e a importância dos operadores nessa integração, com destaque para a execução das ações e para o auxílio na proteção dos nossos meios.

Acerca do questionamento se a integração da cibernética com as funções de combate (F Cmb) é ensinada aos Cadetes de todos os Cursos, todos consideraram que essa integração não é ensinada aos alunos de todos os cursos.

Em resumo, a cibernética na Academia Militar das Agulhas Negras (AMAN) busca criar uma maior mentalidade e consciência de cibersegurança nos Cadetes. Além da capacitação técnica, busca gerar a consciência no futuro oficial, de que a defesa cibernética dos sistemas utilizados pela Força é um aspecto que deve possuir prioridade em seus afazeres.

As instruções visam especificamente a proteção cibernética, com a finalidade de proteger os ativos disponíveis. Em geral, visam proporcionar conhecimentos básicos de cibernética e programação. Aos Cadetes de comunicações, o objetivo é ter condições de planejar a proteção cibernética básica da rede da sua futura Organização Militar (OM).

Acerca das instruções para as Armas, Quadro e Serviço (AQS), verifica-se que as mesmas devem entender a diferença entre cibernética e guerra cibernética. Seria interessante, inclusive, desvincular o nome cibernética da gestão de TI e da segurança da informação feita pelos comunicantes, visando deixar mais clara a diferença entre o operador de guerra cibernética, que ataca e explora o inimigo, e o comunicante, que instala, explora, mantém e protege os meios de TI fornecidos às demais AQS para o exercício do comando e controle. Além disso, deve-se desenvolver a mentalidade de segurança de informação para não serem vetores de acesso à nossa rede para a guerra cibernética inimiga, possuindo ao menos um conhecimento básico de uso de meios de TI. Dessa forma, o comunicante poderá focar em fornecer e proteger as redes e sistemas, e não resolver panes simples de usuário, como dificuldade em habilitar o uso do proxy no navegador.

Já o principal objetivo para o Curso de Com é passar uma base sólida em Redes de Computadores, pois todos os equipamentos que o futuro Oficial de Comunicações irá ter contato são conectados e funcionam em rede, tendo como ênfase, também, a Proteção Cibernética dos ativos dessa rede. Nesse contexto, a AMAN habilita o oficial de Com a planejar, montar e gerenciar uma rede de computadores e seus sistemas, com a finalidade de fornecer meios de comando e

controle ao escalão apoiado, seja uma Brigada, uma Divisão de Exército ou Corpo de Exército, bem como proteger, com limitações, esses meios de ataques cibernéticos. Nesse sentido, são ensinadas boas práticas de segurança da informação e ferramentas básicas de proteção, como lista de controle de acesso, proxy, firewall e outras ferramentas, como o módulo de proteção cibernética que está sendo desenvolvido pelo CIGE. Cabe destacar que não se pretende ensinar guerra cibernética na AMAN, pois essa é uma especialização que exige, além de técnicas e equipamentos específicos, uma seleção de recursos humanos apurada.

Assim, verifica-se que o objetivo do ensino de Cibernética visa aumentar a consciência para o assunto e passar técnicas, táticas e procedimentos para proteger nossos sistemas. Nesse contexto, o PLADIS é composto por uma trilha de conhecimento que busca atingir o objetivo acima proposto. No 2º ano o cadete aprende a planejar, montar e gerenciar uma rede de computadores utilizando-se de switching, VLANs, roteamento estático e dinâmico através de roteadores. No 3º ano, o cadete a planejar o uso, instalar e gerenciar os sistemas e serviços de rede baseado em servidores linux, utilizando máquinas virtuais. Finalmente no 4º ano, o cadete tem contato com gestão de segurança da informação, bem como aprende a implementar ferramentas de proteção de rede como firewall e proxy. O PLADIS do CCom/ AMAN foi apresentado para o CCOMGEX, com a participação de diversas Escolas em Nivelamento de GE e Ciber promovido pelo DECEX, nos anos de 2021 e 2022. Dessa forma, o Plano de Disciplinas está seguindo orientações técnicas do itinerário formativo coordenado pelo CCOMGEX.

Por fim, pela carga horária do curso, não é possível o aprofundamento teórico e técnico, tendo como foco maior a prática (procedimental). Há uma preocupação maior em como fazer do que o por que fazer. Os Cadetes que possuem maior interesse no assunto, tem como opção participar do Grêmio de Cibernética.

4.3 A FORMAÇÃO DE PRAÇAS

Ao se abordar a formação de praças do Exército Brasileiro, a Escola de Sargentos das Armas (ESA) torna-se, naturalmente, o foco principal de qualquer estudo ou pesquisa. Abaixo, verifica-se a descrição de sua finalidade e subordinação, conforme a página oficial da Escola na internet:

> A Escola de Sargentos das Armas (ESA) é o Estabelecimento de Ensino de Nível Superior (Tecnólogo) do Exército Brasileiro, responsável pela formação de Sargentos Combatentes de Carreira das Armas de: Infantaria, Cavalaria, Artilharia, Engenharia e Comunicações.
>
> A ESA é diretamente subordinada à Diretoria de Educação Técnica Militar (DETMil) a qual, em observância às diretrizes emanadas do Departamento de Educação e Cultura do Exército (DECEx), orienta e fiscaliza as atividades de ensino da Escola (ESA, 2022).

Nesse contexto, as principais missões da escola são formar o sargento de carreira, controlar o ensino técnico-pedagógico durante o Primeiro Ano em outras Unidades destinada para esse fim, conduzir o concurso de admissão a nível nacional e contribuir para o aperfeiçoamento da doutrina, especialmente no emprego de pequenas frações. Tais missões estão detalhadas abaixo, conforme o site oficial da Escola.

> Formar sargentos, habilitando-os para exercício dos cargos das graduações de Terceiro-Sargento e Segundo-Sargento não aperfeiçoados, estabelecidos nos quadros de organização (QC), em tempo de guerra ou de paz, diplomando-os a partir de 2020, inclusive, com o grau acadêmico superior de tecnologia;
>
> Exercer o controle técnico-pedagógico do Primeiro Ano do CFGS realizado em Unidades Escolares Tecnológicas do Exército (UETE);
>
> Conduzir o concurso de admissão aos cursos de formação e graduação de sargentos (CFGS) de carreira, em conformidade com as instruções reguladoras específicas fixadas pelo Departamento de Educação e Cultura do Exército (DECEx); e
>
> Contribuir para o aprimoramento da doutrina militar na área de sua competência (ESA, 2022).

Ainda, a ESA tem como visão de futuro ser referencial de excelência, pela qualidade da Formação do sargento combatente de carreira no âmbito das Forças Armadas brasileiras e estrangeiras.

A formação do aluno da ESA é dividida em dois períodos: Primeiro Ano e Segundo Ano do Curso de Formação e Graduação de Sargentos Combatentes de Carreira das Armas (CFGS). O Primeiro Ano do CFGS é realizado em 13 (treze) Unidades Escolares Tecnológicas do Exército (UETE), supervisionadas pela ESA, sendo estas o 20º Regimento de Cavalaria Blindado - (Campo Grande/MS), o 12º GAC (Jundiaí/SP), o 1º GAAAe (Rio de Janeiro/RJ), o 41º BIMtz (Jataí/GO), o 14º GAC (Pouso Alegre/MG), o 23º BC (Fortaleza/CE), o 6º RCB (Alegrete/RS), o 23º BI (Blumenau/SC), o 10º BI (Juiz de Fora/MG), o 4º GAC (Juiz de Fora/MG), o 13° R C Mec (Pirassununga/SP), o 16º B I Mtz (Natal/RN) e o 4º BE Cmb (Itajubá/MG). Este período tem duração de 44 (quarenta e quatro) semanas e prepara o aluno para o período de qualificação.

Após a conclusão do primeiro ano, o aluno escolhe sua qualificação militar de Sargentos, conforme mérito intelectual. O segundo ano tem a duração de 44 semanas. No que diz respeito às Armas, o segundo ano é conduzido integralmente, na ESA. No que tange a logística, o segundo ano é realizado na Escola de Sargentos de Logística (EsSLog), no Rio de Janeiro/RJ e no que se refere ao segundo ano de Aviação do Exército, esta é realizada no Centro de Instrução de Aviação do Exército, em Taubaté/SP (CIAVEx), conforme dados extraídos do site da ESA.

No segundo ano do CFGS, o aluno recebe instruções específicas das armas de Infantaria, Cavalaria, Artilharia, Engenharia e Comunicações, oportunidade em que o espírito de corpo da arma desenvolvido e consolidado.

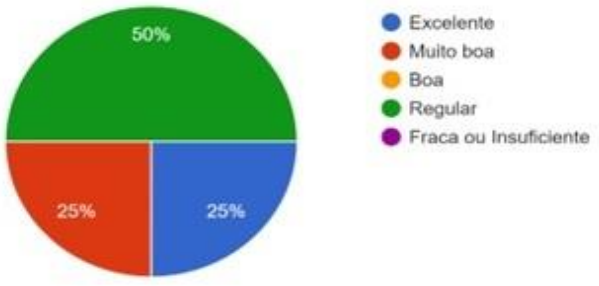
A formação profissional do Sargento Combatente de Exército é a razão de ser da Escola. Ao final do curso, o concludente é declarado 3º Sargento de Carreira Combatente do Exército Brasileiro e ocupará os cargos previstos nos Quadro de Organização da Força Terrestre.

A seguir, passar-se-a a analisar algumas das respostas ao questionário acerca de cibernética confeccionado pelo autor desta pesquisa e respondido pelos instrutores e monitores do C Com da ESA.

Acerca dos principais objetivos da Cibernética ou da Instrução de Ciber na ESA, pode-se destacar a busca por capacitar o aluno a compreender as funcionalidades básicas da rede, assim como executar configurações básicas de rede e de equipamentos de TIC. Além disso, ensinar o futuro sargento as habilidades técnicas necessárias para que atue na tropa como um profissional capacitado na área, além de despertar o interesse pela busca do conhecimento em cibernética.

Qual a sua análise sobre a formação em G Ciber do Curso de Comunicações da ESA?

Gráfico 13 – A análise sobre a formação em G Ciber do Curso de Comunicações



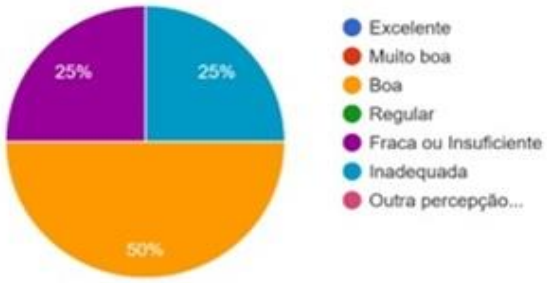
Fonte: o autor

Conforme o gráfico acima, a formação em G Cibernética do C Com da ESA foi considerada regular por 50% do público que respondeu ao questionário. Como

justificativas, salienta-se a problemática da carga horária que acaba sendo pequena, mesmo diante da crescente importância da cibernética e seu uso para fins bélicos. Além disso, faltam instrutores/ monitores com cursos na área.

Qual a sua análise sobre a formação em G Ciber das demais Armas, Quadro e Serviço (AQS) da ESA?

Gráfico 14 – A análise sobre a formação em G Ciber das demais AQS

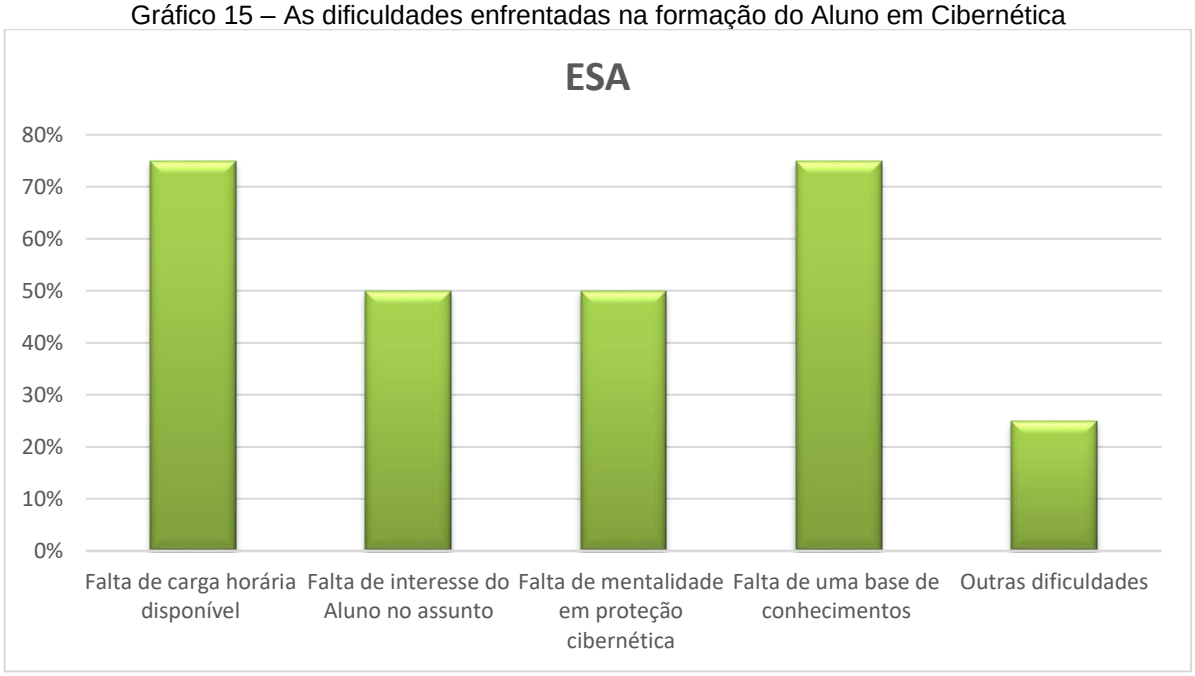


Fonte: o autor

Conforme o gráfico acima, a formação em G Cibernética dos demais Cursos da ESA foi considerada fraca ou inadequada por 50% dos instrutores e monitores.

Quais são as maiores dificuldades enfrentadas durante a formação do Aluno em Cibernética?

Gráfico 15 – As dificuldades enfrentadas na formação do Aluno em Cibernética

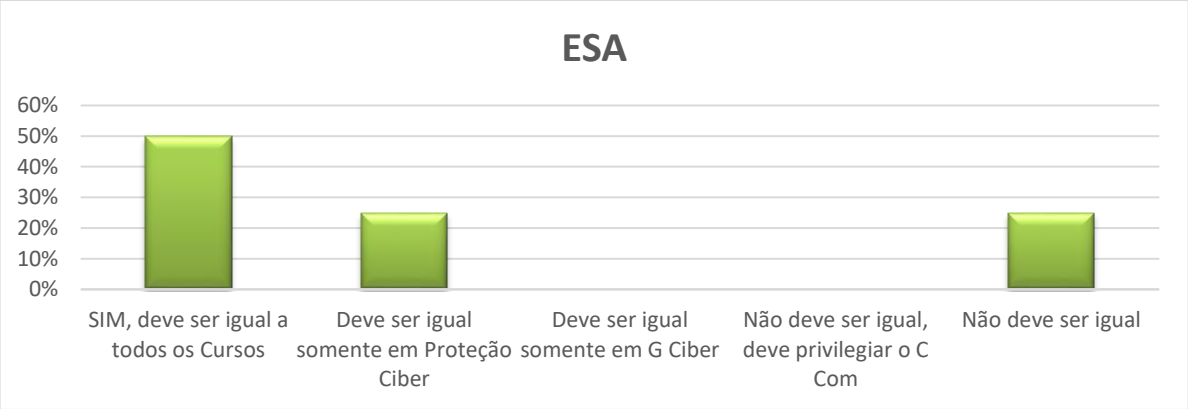


Fonte: o autor

Conforme o gráfico acima, a maioria considerou que as maiores dificuldades enfrentadas durante a formação do Aluno em Cibernética foram a falta de carga horária disponível e de uma base de conhecimentos, a exemplo da transmitida a militares da Arma de Com, para que o assunto seja mais aprofundado para militares de outros cursos.

Em sua opinião, a formação básica em Guerra e Proteção Cibernética deve ser a mesma para todas as Armas, Quadros e Serviço?

Gráfico 16 – A formação em G e Ptç Ciber deve ser a mesma para todas as AQS

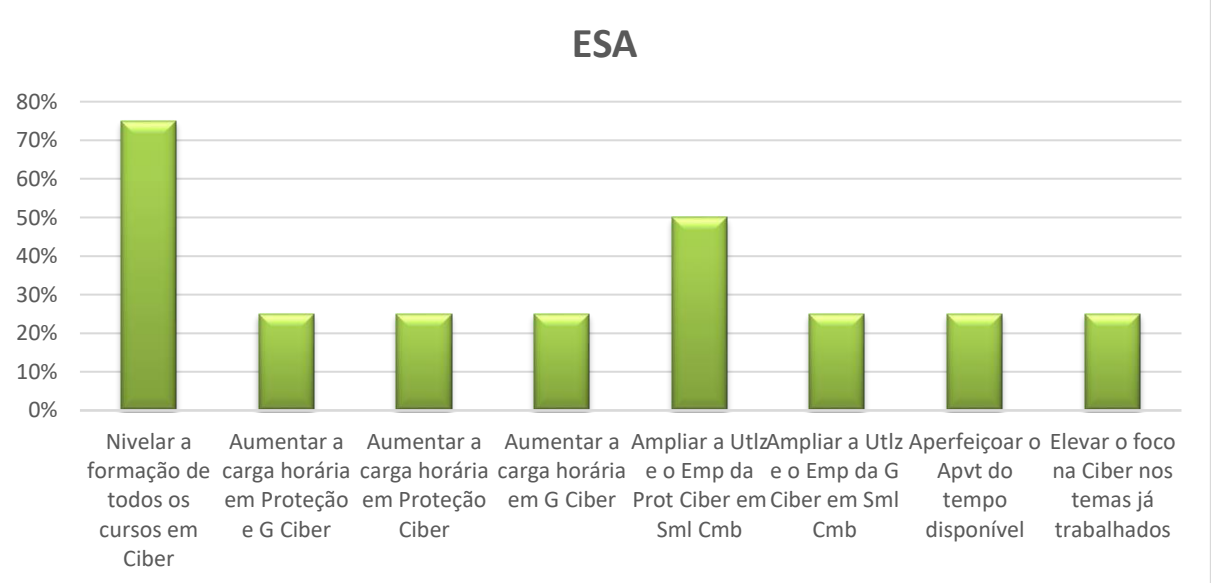


Fonte: o autor

Conforme o gráfico acima, a maioria considerou que a formação básica em Guerra e Proteção Cibernética deveria ser a mesma em todos os cursos, pois considera-se o assunto de vital importância no mundo atual. Nesse sentido, deve-se criar uma mentalidade de proteção cibernética, na qual todos deveriam ter conhecimentos básicos do assunto para fins de segurança durante as operações. Ademais, esse entendimento não é somente para a guerra, pois foca em defesa e proteção cibernética de todos os sistemas de TI operados no País, os quais dependem de boas práticas mescladas com contrainteligência para operar com segurança e mitigar os possíveis efeitos de ataques cibernéticos.

Quais medidas o Sr. visualiza que poderiam ser incrementadas na formação em Cibernética do Aluno, especialmente com foco na defesa/ proteção?

Gráfico 17 – As medidas para incrementar a formação em Cibernética do Aluno



Fonte: o autor

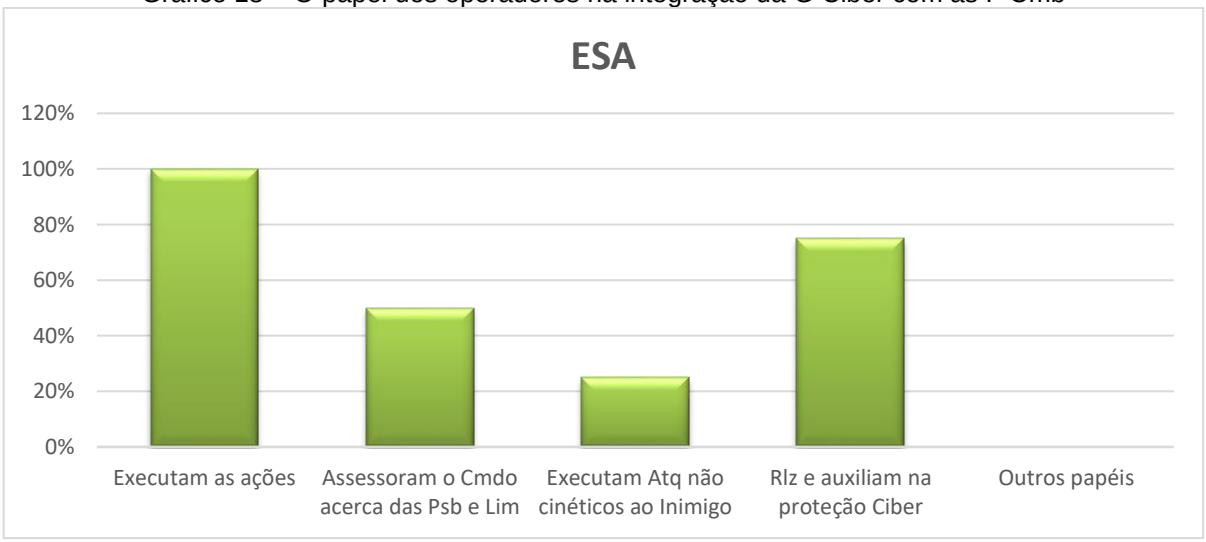
Conforme o gráfico acima, a maioria considerou que as seguintes medidas poderiam ser incrementadas para aprimorar a formação em Cibernética: nivelar a formação de todos os cursos no assunto e ampliar a utilização e o emprego da Guerra Cibernética em simulações virtuais, construtivas e reais de combate. Acerca da referida instrução na ESA, cabe destacar que é composta somente de conhecimentos basilares e que não existem assuntos específicos voltados para o ataque e a proteção cibernética, o que poderia ser implementado no Curso de Comunicações.

Acerca da possibilidade de uniformizar o PLADIS de todos os cursos em cibernética, a maioria considerou que essa uniformização dependeria de vários fatores. Nesse sentido, considera-se que a gama de conhecimento para trabalhar na área seja muito grande, como programação, sistemas operacionais, protocolos de comunicação e criptografia, o que exigiria um conjunto de pré-requisitos maior que não podem ser passados em todos os cursos de formação pela falta de carga horária do assunto.

Acerca do questionamento se o estudo mais aprofundado das possíveis ameaças aos sistemas, dependentes de meios de TI, aperfeiçoaria a formação do futuro sargento no assunto em tela, todos consideraram que o referido estudo aperfeiçoaria a formação do aluno em G Ciber.

E qual o papel e a importância dos operadores na integração da G Ciber com as funções de combate (F Cmb Mov e Man, Intlg, fogos não cinéticos, etc)?

Gráfico 18 – O papel dos operadores na integração da G Ciber com as F Cmb



Fonte: o autor

Conforme o gráfico acima, todas as ações apresentadas expressam o papel e a importância dos operadores nessa integração, com destaque para a execução das ações e para o auxílio na proteção dos nossos meios.

Acerca do questionamento se a integração da cibernética com as F Cmb é ensinada a todos os Alunos, houve unanimidade de que ela não é ensinada em todos os Cursos.

Acerca de outros pontos a destacar, no que tange à contribuição para uma formação mais adequada em G Ciber na ESA, merece destaque a falta de qualificação de instrutores e monitores, além de estarem limitados apenas a comunicantes. Nesse contexto, poder-se-ia disponibilizar mais oportunidades para o instrutor e o monitor da ESA se capacitar, com a disponibilização de vagas para a realização de cursos de Proteção e Guerra Cibernética.

Em análise sumária das respostas acima, verifica- se que a ESA não aborda diretamente os assuntos de Guerra e Proteção Cibernética com seus Alunos, ou seja, não ensina como realizar ataque ou proteção no currículo. O PLADIS da Escola não contempla nem a teoria desses assuntos. Mas a Escola de Sargentos das Armas possui a matéria Cibernética em sua carga horária, composta por fundamentos, redes e Linux basicamente.

Nesse contexto, são ministradas bases técnicas essenciais para a continuação da formação do Guerreiro Cibernético, mais aprofundado para os Sargentos da Arma de Comunicações, independente da linha de especialização que seguirão.

Excluindo-se os Alunos de Comunicações, os demais Alunos tem uma carga horária mínima no 1º ano. Porém, como a matéria é ministrada no 1º Ano, ou seja, nas Unidades Escolares Tecnológicas do Exército (UETE), não é ministrada por especialistas, salvo se aquela determinada OM tiver um em seus quadros, o que didaticamente não se configura como a melhor situação.

A inserção de uma carga horária no 2º Ano da formação, a ser ministrada na Escola e a disponibilização de vagas para instrutores e monitores da ESA nos cursos de Cibernética poderiam conbtribuir com uma melhor formação.

Outra medida que poderia impactar positivamente no desenvolvimento das instruções de proteção cibernética seria a exploração do tema em Exercícios de Simulação virtual, viva e mista.

Nesse contexto, baseado no ensino por competências, no qual todos os conceitos devem ser trabalhados em conjunto, pode-se elevar o foco da cibernética em temas já trabalhados na escola, além de nivelar o conhecimento, especialmente em Proteção, de todos os alunos, independente do Curso que escolheram. Dessa

forma, poder-se-á integrar a cibernética às demais funções de combate, contribuindo para a criação de uma mentalidade de proteção cibernética na Força Terrestre.

5 OS CURSOS DE ESPECIALIZAÇÃO DE OFICIAIS E PRAÇAS

Acerca dos cursos de especialização para Oficiais e Sargentos na área de cibernética, verfica-se que alguns centros oferecem oportunidades de Ensino, alguns inclusive à Distância, como a Escola Nacional de Defesa Cibernética (EnaDCiber) e a Escola de Comunicações. Já a Escola de Inteligência Militar do Exército (EsIMEx) ministra o Curso de Inteligência Cibernética, destina para oficiais que busquem aperfeiçoamento no assunto, mais direcionado, porém, a área de inteligência, a qual não será alvo desta pesquisa.

Referente ao Sistema de Ensino do Exército, duas escolas militares próprias oferecem cursos de especialização em Cibernética, a Escola de Comunicações (EsCom) e o Centro de Instrução de Guerra Eletrônica (CIGE). A primeira oferece o Curso de Proteção Cibernética e a segunda o Curso de Guerra Cibernética. Ambas as instituições realizam trabalhos úteis ao setor no País e podem ser destacadas como principais instituições de especialização e extensão em Cibernética da Força Terrestre. Alguns aspectos dos referidos cursos e da cibernética trabalhada nestes Centros de referência serão discutidos a seguir.

5.1 O CENTRO DE INSTRUÇÃO DE GUERRA ELETRÔNICA (CIGE)

O Centro de Instrução de Guerra Eletrônica (CIGE) foi o primeiro centro de treinamento de Guerra Eletrônica da América Latina, criado em 1984, e matareializado em 1985, a partir de um núcleo de implantação. Os trabalhos de formulação da doutrina e capacitação de recursos humanos foram pautados, inicialmente, na realização de cursos no exterior por militares brasileiros, visando a qualificação e a busca de conhecimentos na área da cibernética, conforme descrito na Página eletrônica do Centro.

> O Centro de Instrução de Guerra eletrônica (CIGE), primeiro centro de treinamento de Guerra Eletrônica da América Latina, foi criado pelo Decreto Presidencial n° 89445, de 19 de março de 1984.
>
> O CIGE ganhou vida com a ativação do Núcleo de Implantação do Centro de Instrução de Guerra Eletrônica (NICIGE), criado pela Portaria do EME n°

07, de 11 de fevereiro de 1985, cujo primeiro Chefe foi o Cel Com QEMA HUMBERTO JOSÉ CORRÊA DE OLIVEIRA.

Para viabilizar a implantação do CIGE, foram priorizadas as ações relacionadas à formulação de doutrina e à capacitação de Recursos Humanos. Dentre as atividades realizadas pelo NICIGE, destacam-se:

- Realização de cursos no exterior (ALEMANHA, FRANÇA, INGLATERRA e EUA), com vistas à formação de um núcleo de instrutores no CIGE;
- Aquisição de um Módulo Básico Experimental de Guerra Eletrônica (MBEGE) para atender às necessidades de qualificação de militares na atividade de Guerra Eletrônica;
- Visitas às instalações fabris e militares no exterior, com o objetivo de colher informações técnicas e doutrinárias;
- A formulação da doutrina de Guerra Eletrônica do Exército Brasileiro (CIGE, 2022).

O Centro de Instrução de Guerra Eletrônica (CIGE) é o pioniero no assunto Guerra Cibernética e vem evoluindo constantemente, conforme descrito abaixo.

Além das atividades de Guerra Eletrônica, o CIGE é a OM pioneira no Exército no assunto Guerra Cibernética. Com o advento da Estratégia Nacional de Defesa, o CIGE sediou, em 2010, o I Seminário de Defesa Cibernética das Forças Armadas, evento esse que marcou as primeiras discussões doutrinárias e estruturantes do Setor Cibernético no Ministério da Defesa e nas Forças Armadas. Recentemente, as instalações e o QCP do CIGE foram reformulados para contemplar o corpo docente e operacional da Guerra Cibernética. Dando prosseguimento à vocação no ensino, desde 2012, o CIGE realiza, anualmente, o Curso de Guerra Cibernética, destinado a oficiais e praças das três Forças Armadas, com a participação de diversos palestrantes do meio acadêmico, empresarial e militar.

Ainda no ano de 2012, o CIGE foi pioneiro ao realizar uma inovação no sistema de ensino do Exército Brasileiro. O Curso Intermediário de Guerra Eletrônica foi rebatizado como: Curso de Inteligência do Sinal. Além da mudança de nome, o curso foi reestruturado e passou a ser realizado em parceria com a EsIMEx (Escola de Inteligência Militar do Exército), de forma que o curso continua sendo do CIGE, porém, com um mês a cargo da EsIMEx.

O ano de 2016 foi marcado por dois grandes eventos que vêm se repetindo desde então: A participação do CIGE na Manobra Escolar da AMAN e a realização anual do Estágio Internacional de Defesa Cibernética.

A Manobra Escolar é realizada anualmente na AMAN e, com a participação do CIGE, os alunos das diversas escolas têm a oportunidade de travar contato com a Guerra Eletrônica e a Guerra Cibernética. Durante os quinze dias de manobra, o CIGE leva instrutores e alunos para operarem e explorarem os ambientes cibernéticos e eletrônicos, ambientados no exercício.

O Estágio Internacional de Defesa Cibernética, também com a duração de duas semanas, reúne no CIGE, desde 2016, oficiais de diversas nações amigas para uma grande troca de conhecimentos sobre o tema.

Com o objetivo de capacitar em Guerra Eletrônica militares de todas as Armas, Quadro e Serviço do Exército Brasileiro, o curso de Segurança do Sinal foi retomado em 2018 com nova carga horária e assuntos atualizados. O curso é realizado desde então nos anos pares.

Em 2019, com a evolução do Curso de Planejamento de Guerra Eletrônica, o CIGE iniciou o Curso de Planejamento de Guerra Eletrônica e Guerra Cibernética em Apoio às Operações ocorrendo, atualmente, durante os anos pares.

Neste mesmo ano, o CIGE promoveu um Estágio de Atividades Cibernéticas para Cadetes das três Forças Armadas e também um Estágio de Proteção eletrônica para Cadetes da AMAN. Ambos com periodicidade anual.

> Em 2020, o CIGE concluirá a ampliação das suas instalações, visando uma melhor infraestrutura para o cumprimento de suas missões.
>
> Ao longo de mais de três décadas, a Atividade de Guerra Eletrônica vem se reinventando e ganhando força e vigor em seu Centro de Instrução, herdeiro e guardião das tradições da Guerra Eletrônica e orgulho das várias gerações de Guerreiros Eletrônicos que o construíram e o mantêm pujante e em constante modernização (CIGE, 2022).

A seguir, passar-se-a a analisar as respostas aos questionário respondido pelos instrutores e monitores do CIGE.

Acerca dos principais objetivos da Cibernética ou da Instrução de Ciber no CIGE, pode-se destacar a busca por habilitar militares, no anoto de suas demais habilitações, a ocupar cargos e funções que utilizem técnicas cibernética. O centro é a principal fonte de recursos humanos especializados para a força. Além disso, o Centro busca dar ao aluno uma base generalista para que ele possa se especializar em uma determinada área futuramente, visto a gama de assuntos que são abordados no curso, além de formar recursos humanos com a capacidade de realizar ataques cibernético.

Qual a sua análise sobre a formação em G Ciber do CIGE?

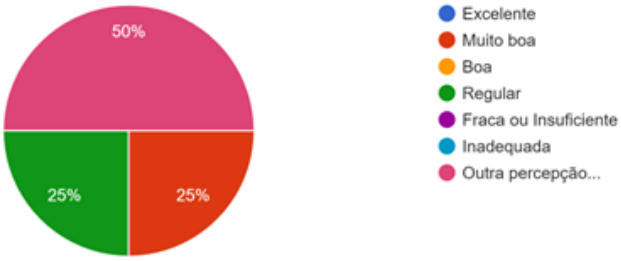
Gráfico 19 - A análise sobre a formação em G Ciber do CIGE

Fonte: o autor

Conforme o gráfico acima, a formação em G Ciber do CIGE é excelente ou muito boa para todos os participantes do presente questionário.

Qual a sua análise sobre a formação de planejadores de G Ciber do CIGE?

Gráfico 20 - A análise sobre a formação de planejadores de G Ciber

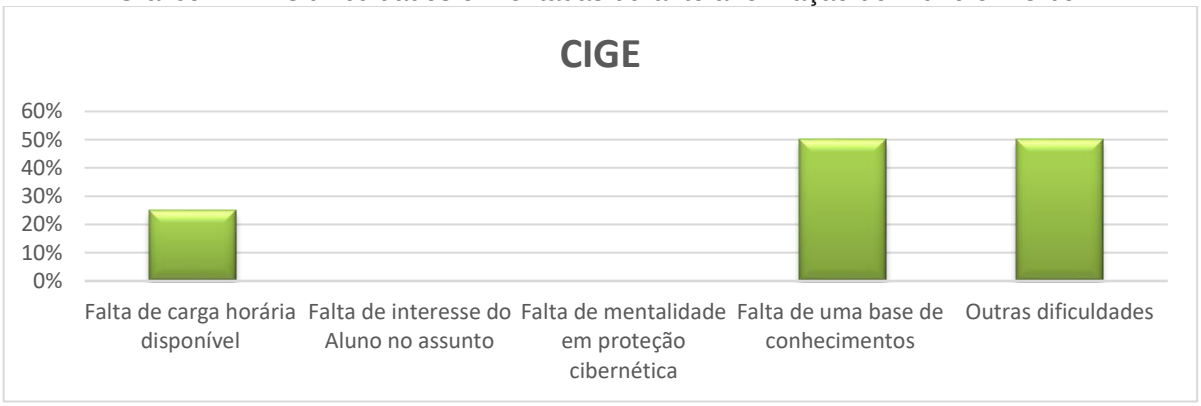


Fonte: o autor

Conforme o gráfico acima e as respostas complementares acerca do item "outra percepção", há o entendimento de que o planejamento deva ser ensinado na ESAO e na ECEME, não havendo curso de planejamento de G Ciber no CIGE.

Quais são as maiores dificuldades enfrentadas durante a formação do Aluno em Cibernética?

Gráfico 21 – As dificuldades enfrentadas durante a formação do Aluno em Ciber



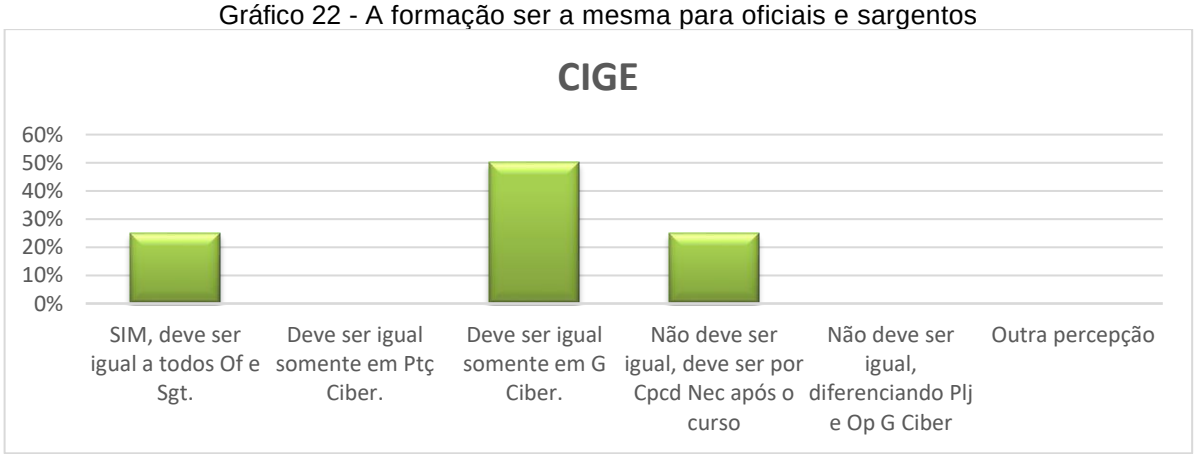
Fonte: o autor

Conforme o gráfico acima, a maioria considerou que as maiores dificuldades enfrentadas durante a formação do Aluno em Cibernética foram a falta uma base maior de conhecimentos e carga horária, além de outras dificuldades.

Acerca do questionamento se o PLADIS do curso de G Ciber para oficiais e sargentos é o mesmo, não houve consenso nas respostas apresentadas.

Em sua opinião, a formação deve ser a mesma para oficiais e sargentos?

Gráfico 22 - A formação ser a mesma para oficiais e sargentos

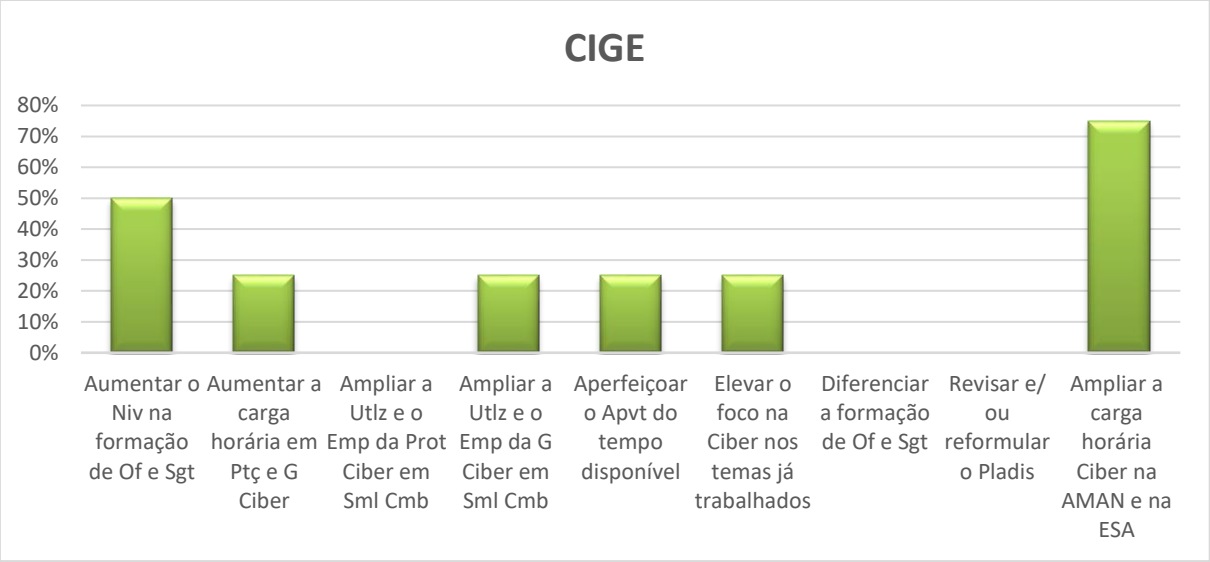


Fonte: o autor

Conforme o gráfico acima, a maioria considerou que a formação deve igual somente em G Ciber. Ademais, considera-se que o curso deve levar em conta as capacidades que serão requeridas de cada militar após o curso, o que tende a diferenciar as necessidades de oficiais e sargentos. Acerca das justificativas da resposta, destaca-se que em cibernética, ambos devem saber executar as tarefas técnicas, designadas, pois, muitas vezes, leva-se muitos anos para ter um especialista em determinado assunto. Ademais, o assunto é muito amplo e as capacidades individuais não devem ser deixadas de lado por conta de posto ou graduação.

Quais medidas o Sr. visualiza que poderiam ser incrementadas para aprimorar a formação em Cibernética do Aluno?

Gráfico 23 – As medidas para aprimorar a formação em Cibernética



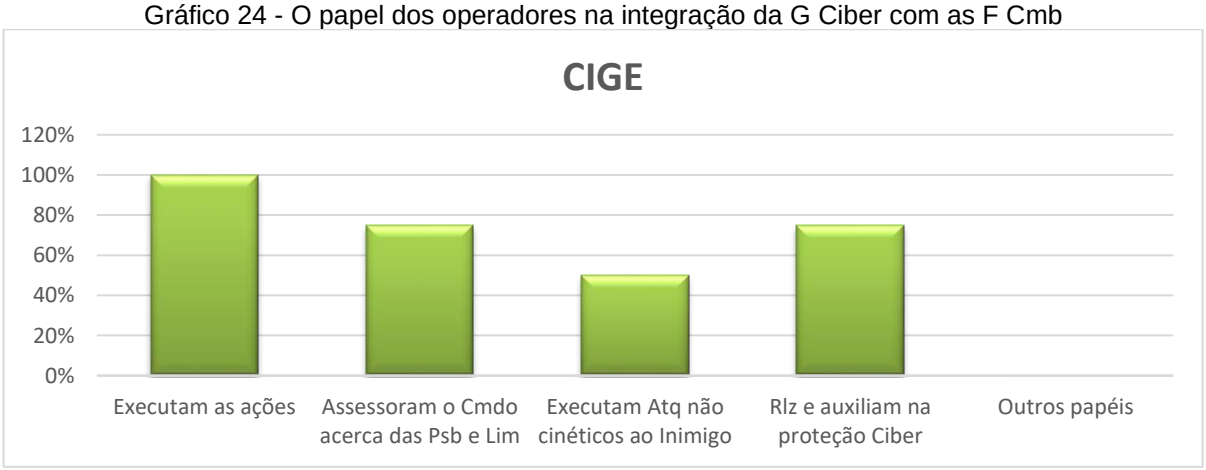
Fonte: o autor

Conforme o gráfico acima, a maioria considerou que a formação pode ser aprimorada com a ampliação da carga horária nas escolas de formação (AMAN e ESA), pois, dessa forma, o militar chegaria para o curso mais bem capacitado em conhecimentos basilares. Ademais, um aumento no nivelamento, antes do curso, também contribuirá para essa base necessária ao bom desenvolvimento da formação.

Acerca do questionamento se um estudo mais aprofundado de possíveis ameaças aos sistemas dependentes de meios de TI, aperfeiçoaria a formação do aluno, não houve maioria entre os participantes, com a metade considerando que aperfeiçoaria e a outra metade que não aperfeiçoaria a formação.

E qual o papel e a importância dos operadores na integração da G Ciber com a funções de combate (Mov e Man, Intlg, fogos não cinéticos, etc)?

Gráfico 24 - O papel dos operadores na integração da G Ciber com as F Cmb

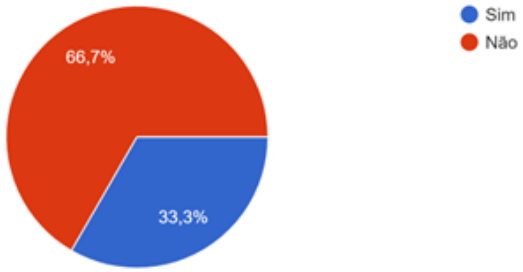


Fonte: o autor

Conforme o gráfico acima, todas as ações apresentadas expressam o papel e a importância dos operadores nessa integração, com destaque para a execução das ações.

A integração das Funções de Combate (F Cmb) com a cibernética é ensinada aos Alunos de todos os cursos?

Gráfico 25 - A integração das F Cmb com a Ciber ensinada aos Alunos de todos os cursos



Fonte: o autor

Conforme o gráfico acima, a maioria considerou que essa integração não é ensinada ao Aluno de todos os cursos.

Em uma análise das respostas, acerca das maiores dificuldades na formação em G Ciber pode-se destacar que a falta de uma base mais sólida de conhecimento dos alunos, normalmente em níveis distintos de domínio cognitivo, atrapalha o andamento do curso e, em consequência, a qualidade da especialização realizada.

Uma medida que poderia aperfeiçoar a formação, com algum incremento de carga horária, seria a divisão do Curso de Guerra Cibernética em Básico e Avançado. Cabe destacar que a formação do combatente cibernético não finaliza ao final do curso de especialização, pois demanda um esforço pessoal para desenvolver capacidades de forma contínua, em uma incessante busca por manter-se atualizado as novas tecnologias que surgem a cada dia.

5.2 A ESCOLA DE COMUNICAÇÕES

As origens da Escola de Comunicações (EsCom) remontam ao pós- 1ª Guerra Mundial, com a criação do Centro de Instrução de Transmissões em 1921. Ao longo dos anos, este tradcional Estabelecimento de Ensino do Exército passou por diversas reformulações e aperfeiçoamentos, conforme descrito a seguir.

> A Escola de Comunicações teve suas origens no período pós 1ª Guerra Mundial, com a criação do Centro de Instrução de Transmissões, a 1º de julho de 1921. Naquela oportunidade, ocupou as instalações do 1º Batalhão de Engenharia, atual aquartelamento do Batalhão Escola de Comunicações (BEsCom). Seu primeiro comandante, o 1º Ten Paulo Maccord, não

> imaginaria que aquele pioneirismo em preparar telefonistas, radiotelegrafistas e sinaleiros se tornaria o berço para o surgimento da Arma de Comunicações.
>
> Em 1926, desvinculou-se do Batalhão de Engenharia e passou a operar anexa à Escola das Armas, atual Escola de Aperfeiçoamento de Oficiais (EsAO). Em 1º de abril de 1935, recebeu a sua sede própria, na Avenida Duque de Caxias nº 325. A 29 de fevereiro de 1936, passou a denominar-se Curso Especial de Transmissões e, a 17 de abril de 1940, Escola de Transmissões.
>
> A deflagração da 2ª Guerra Mundial e a entrada do Brasil naquele conflito acarretaram profundas modificações na Escola. O material então existente foi substituído por outro mais moderno e o quadro de instrutores adaptado às novas condições do ensino, preparando os militares que se tornariam imprescindíveis à coordenação e ao controle das ações vitoriosas da 1ª Divisão de Infantaria Expedicionária, nos campos de batalha da Itália.
>
> Finalmente, a 1º de julho de 1953, por ato do Poder Executivo, foi instituída a denominação de Escola de Comunicações (EsCom). Em 1956, em reconhecimento à sua competência e destacada participação junto ao Exército e à sociedade brasileira, teve sua Bandeira Nacional agraciada com a Ordem do Mérito Militar, honrosamente recebida pelas mãos do então Presidente Juscelino Kubitscheck de Oliveira. Em cinco de maio de 1975, o estandarte teve a honra de ser incorporado ao patrimônio histórico-cultural.
>
> Até 1979, a EsCom foi também responsável pela formação do Sargento Combatente de Comunicações, quando o curso foi transferido para a Escola de Sargentos das Armas (ESA). Permaneceu com a missão de formar e aperfeiçoar Sargentos de Manutenção de Comunicações, oferecendo cursos de extensão e especialização para oficiais e praças nas áreas das Comunicações, Eletrônica e Informática e, ainda, contribuir para a formulação da doutrina militar específica.
>
> Em 19 de maio de 2006, foi concedida, por meio da Portaria Nº 254, de 12 de maio de 2006, do Comandante do Exército, a denominação histórica "Escola Coronel Hygino Corsetti", uma justa homenagem à pessoa que tanto influenciou o desenvolvimento da Arma de Comunicações e das telecomunicações brasileiras.
>
> Em 10 de março de 2010, com a publicação da Portaria do Comandante do Exército n° 125, foi aprovada a transferência da Escola de Comunicações para Brasília-DF, nas instalações do Centro de Comunicações e Guerra Eletrônica do Exército. Após a necessária adaptação das instalações, com a implantação de novos e modernos laboratórios, em 21 de janeiro de 2011, foi realizada sua reinauguração, agora na nova sede no Planalto Central (EsCom, 2022).

Na atualidade, a Escola oferece cursos de extensão e especialização para Oficiais e Sargentos, além de contribuir para a doutrina militar nas áreas de comunicações, eletrônica e informática. Destarte, está também ligada a Cibernética, que permeia todas as áreas de atuação deste Estabelecimento de Ensino. Segue abaixo a descrição atual da EsCom.

> Atualmente, este Estabelecimento de Ensino está subordinado ao Comando de Comunicações e Guerra Eletrônica do Exército e vinculado à Diretoria de Educação Técnica Militar, para fins de orientação técnico-pedagógica. A EsCom oferece cursos de extensão e de especialização para oficiais e praças nas áreas das comunicações, eletrônica e informática e, ainda, contribui para a formulação da doutrina militar específica. A Escola mantém ritmo contínuo de realizações, acompanhando de perto a evolução das Comunicações no Exército e no resto do mundo. Além da preocupação de estar sempre integrada com o avanço da tecnologia, a EsCom cultiva e

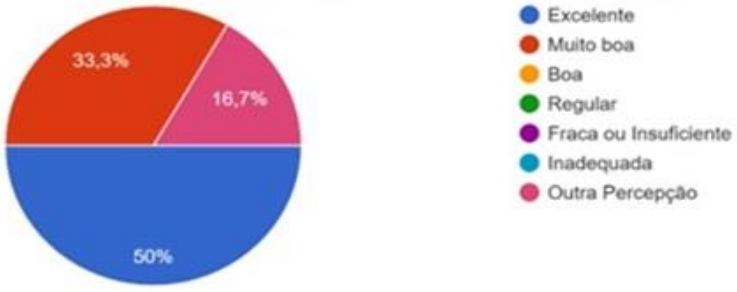
> mantém sempre viva a história do Marechal Cândido Mariano da Silva Rondon, patrono da Arma de Comunicações (EsCom, 2022).

A seguir, passar-se-a a analisar as respostas ao questionário respondido pelos instrutores e monitores da EsCom.

Acerca dos principais objetivos da Cibernética ou da Instrução de Ciber na EsCom, observando as publicações de Comunicações (EB70-MC-10.241) e de C² do Exército Brasileiro, pode-se destacar que prioriza a formação de Oficiais e Praças para desempenhar atividades de Proteção Cibernética nas redes do Sistema de Comando e Controle do Exército (SC²Ex), passa noções de segurança em geral, detecção, resposta e prevenção a incidentes cibernéticos, capacitando os militares para que exerçam, no âmbito do Exército Brasileiro (EB), atividades relacionadas à Proteção Cibernética. Além disso, visa fomentar a mentalidade de que a consciência de segurança e a capacidade técnica em proteção cibernética são fatores essenciais a todos os componentes do EB, assim como a capacitação de pessoal para proteger os sistemas de informação no nível tático e operacional.

Qual a sua análise sobre a formação em Proteção Cibernética da EsCom?

Gráfico 26 - A análise sobre a formação em Proteção Cibernética da EsCom

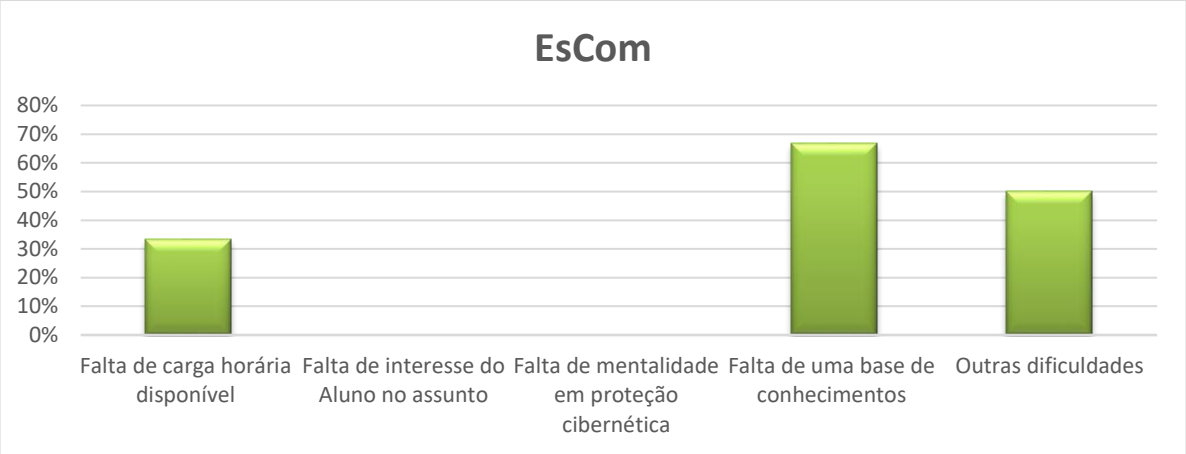


Fonte: o autor

Conforme o gráfico acima, a formação em Proteção Cibernética da EsCom foi considerada excelente ou muito boa pela maioria do público que respondeu ao questionário. Corroborando com a análise do gráfico acima, merece destaque que a referida formação pode ser considerada excelente porque se baseia nos principais frameworks internacionais, como NIST e SANS, possui um PLADIS dinâmico, permitindo ajustes de até 30% de seu conteúdo ao ano e o corpo docente é extremamente técnico, de forma que os cursos são atuais e relevantes, dentro do que se propõe.

Quais são as maiores dificuldades enfrentadas durante a formação do Aluno em Cibernética?

Gráfico 27 - As dificuldades enfrentadas na formação do Aluno em Cibernética

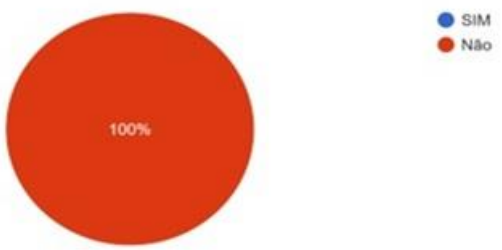


Fonte: o autor

Conforme o gráfico acima, a maioria considerou que a maior dificuldade enfrentada durante a especialização do aluno em proteção cibernética foi a falta de uma base de conhecimentos, o que exige grande carga horária para nivelamento dos instruendos. Acerca das "Outras dificuldades" elencadas, pode-se destacar a manutenção de um corpo docente especializado e a falta de um laboratório (cluster de servidores) semelhante ao CIGE, para montar vários cenários de defesa cibernética, o que atualmente não existe por uma limitação de hardware. A limitação de pessoal é outra dificuldade, visto a grande carga de trabalho dos instrutores. Como sugestão, existe a possibilidade de se iniciar a capacitação na Modalidade EAD, antes do aluno se apresentar na Escola. Apesar de já estar acontecendo, são necessários mais investimento e apoio de legislação para que o militar tenha tempo de estudo na OM de origem antes da fase presencial, assim como já ocorre em outros cursos da Força. Dessa forma, se desenvolve uma mentalidade de capacitação mais ampla.

O PLADIS do curso de Proteção Ciber para oficiais e sargentos é o mesmo?

Gráfico 28 – A equidade do PLADIS para oficiais e sargentos

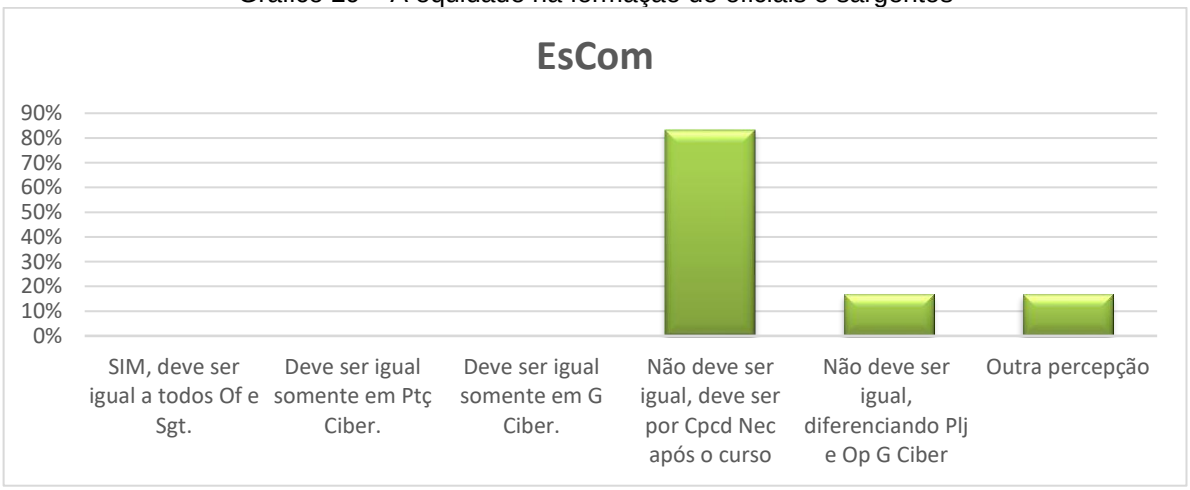


Fonte: o autor

Conforme o gráfico acima, o PLADIS do curso de Proteção Cibernética para oficiais e sargentos não é o mesmo.

Em sua opinião, a formação deve ser a mesma para oficiais e sargentos?

Gráfico 29 – A equidade na formação de oficiais e sargentos



Fonte: o autor

Conforme o gráfico acima, a maioria considerou que a formação não deve ser a mesma para oficiais e sargentos, pois deve diferenciar as formações conforme capacitações que serão necessárias após o curso.

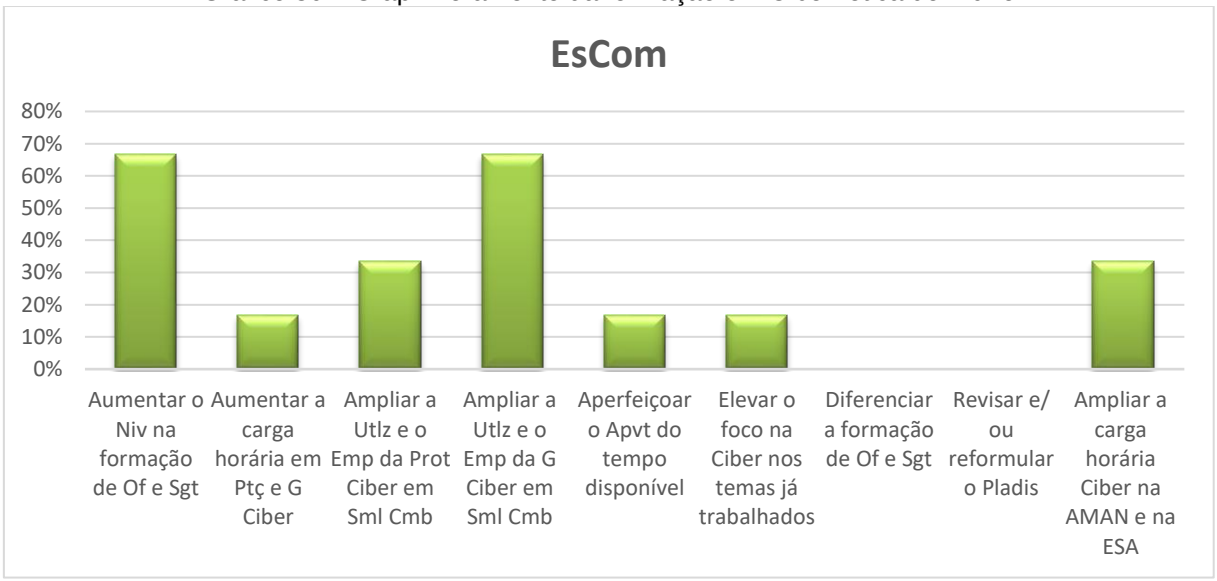
No entanto, assim como ocorre no exército americano, a formação básica deve sim ser a mesma, embora o oficial deva receber ainda a capacitação sobre planejamento e gestão. Assim, inicialmente deveria aprender a fazer, para que tenha a capacidade de avaliação das complexibilidades, limitações e riscos existentes e, em uma fase posterior, deveria ser capacitado a realizar planejamentos e gestões de emprego de G Ciber, de forma a agir com maior eficácia, tempestividade e previsão perante as ameaças que possam surgir.

Já no nível do subtenente e sargento, a atuação é focada na execução das atividades de proteção cibernética. Apesar do citado foco em gestão maior para os oficiais, em uma 1ª fase os pré-requisitos técnicos, especialmente da parte EAD, devem ser os mesmos para Of e Sgt e, para isto, seria interessante um laboratório virtual para os alunos treinarem a distância, antes de virem para a Escom na fase presencial. Dos conhecimentos basilares necessários, a base de informática em redes deve ser prioridade dos alunos.

Como após a conclusão do curso os militares irão desempenhar diferentes funções, no que concerne à proteção cibernética, seria mais interessante que os enfoques de uma possível 2ª fase fossem direcionados às capacidades que serão mais demandadas em cada função, seja de oficiais ou de praça. O ideal seria que as atividades dos dois cursos se conectassem e se complementassem em atividades conjuntas, o que é inviabilizado pelo fato de acontecerem em semestres diferentes.

Quais medidas o Sr. visualiza que poderiam ser incrementadas para aprimorar a formação em Cibernética do Aluno?

Gráfico 30 – O aprimoramento da formação em Cibernética do Aluno



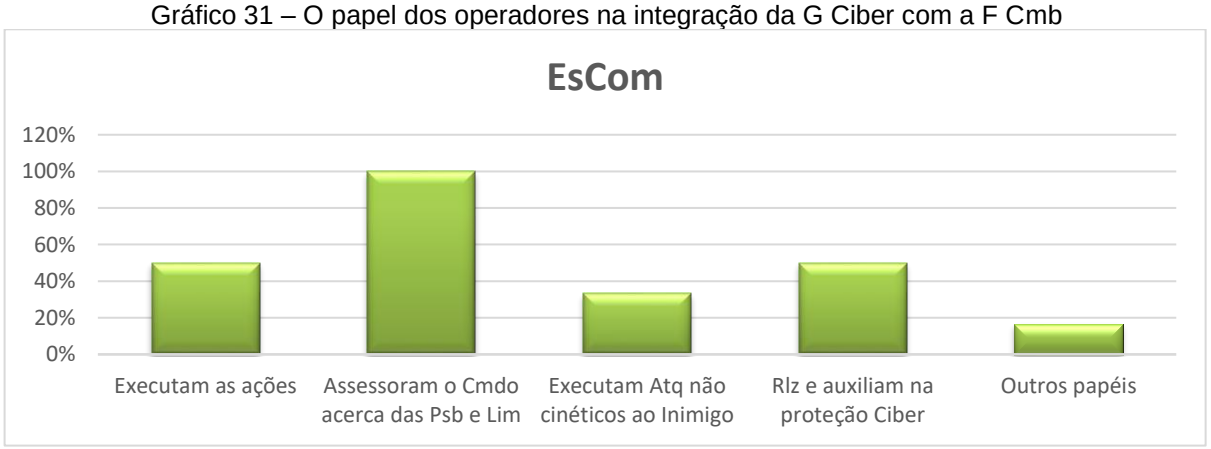
Fonte: o autor

Conforme o gráfico acima, as principais medidas elencadas para aprimorar a formação em Cibernética foram aumentar o nivelamento na formação de oficiais e sargentos de todos os cursos; ampliar a utilização e o emprego da Guerra Cibernética em simulações virtuais, construtivas e reais de combate; e ampliar a carga horária de cibernética nas escolas de formação (AMAN, ESA, etc).

Acerca do questionamento se um estudo mais aprofundado de possíveis ameaças aos sistemas dependentes de meios de TI, aperfeiçoaria a formação no assunto, todos consideraram que o referido estudo aperfeiçoaria a formação do aluno em G Ciber.

Qual o papel e a importância dos operadores na integração da G Ciber com a funções de combate (Mov e Man, Intlg, fogos não cinéticos, etc)?

Gráfico 31 – O papel dos operadores na integração da G Ciber com a F Cmb

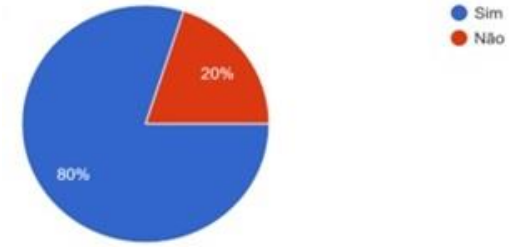


Fonte: o autor

Conforme o gráfico acima, todas as ações apresentadas expressam o papel e a importância dos operadores nessa integração, com destaque para o assessoramento ao comando acerca das possiblidades e limitações da G Ciber. Acerca de outros papéis, pode-se destacar o de adquirir conhecimento agregando valor a capacidade humana do Exército Brasileiro.

A integração da Ciber com as F Cmb é ensinada aos Alunos?

Gráfico 32 – A integração da G Ciber com as F Cmb ensinada ao Aluno



Fonte: o autor

Conforme o gráfico acima, a maioria considerou que essa integração não é ensinada aos alunos.

Acerca de outras contribuições para uma formação mais adequada em Cibernética, merece destaque o fato de haver uma grande evasão de pessoal qualificado da Força Terrestre, sobretudo para a iniciativa privada. São pontuais os militares com capacidades específicas em Cibernética, mas não há uma política de retenção ou valorização deste pessoal, o que tem resultado em grande evasão ou desinteresse em permanecer na área. Muitas vezes, os que persistem, o fazem em detrimento da carreira.

Em uma análise das respostas e do estudo acerca da especialização realizadas na EsCom, verifica-se que existe a necessidade de manutenção de um corpo docente especializado, a criação de um laboratório (cluster de servidores) semelhante ao CIGE, para montar vários cenários de defesa cibernética, o que não ocorre atualmente por limitação de hardware; incrementar o início da capacitação na Modalidade EAD, antes do aluno se apresentar na Escola, pois apesar de já estar acontecendo, são necessários mais investimentos e apoio de legislação para que o militar tenha tempo de estudo antes do curso, assim como ocorre no CAS, CHQAO, CGAEM e ECEME.

Outra medida que poderia ser implementada, seria a criação de um curso básico de cibernética para o militar identificar sua maior área de afinidade, para depois realizar uma formação mais especializada, como em OSSINT, Web, Linux, Windows, MAC, Android, Wifi, IoT, Sistemas Críticos, Forense, Anl Malware, Direito digital e inúmeros outros.

Uma política mais clara e específica de valorização de militares com capacidades cibernéticas pode evitar a evasão ou o desinteresse em permanecer na atividade, contribuindo para a manutenção das capacidades na área.

Por fim, o desenvolvimento de uma mentalidade de capacitação mais ampla em toda a Força Terrestre se faz necessária, visando a manutenção da segurança dos diversos sistemas operados, seja em tempos de paz ou de guerra.

5.3. A CONTRIBUIÇÃO DE ESPECIALISTAS

Ainda no escopo da especialização e extensão, aplicou-se semelhante questionário a militares que realizaram cursos na área e/ou trabalharam com cibernética. A seguir, passar-se-a a analisar as respostas ao respectivo questionário.

Acerca dos principais objetivos da Cibernética ou da Instrução de Ciber, pode-se destacar a qualificação de recursos humanos para o desempenho das atividades e das capacidades operativas de ataque, exploração e proteção cibernética em proveito do Sistema de Guerra Cibernética do Exército.

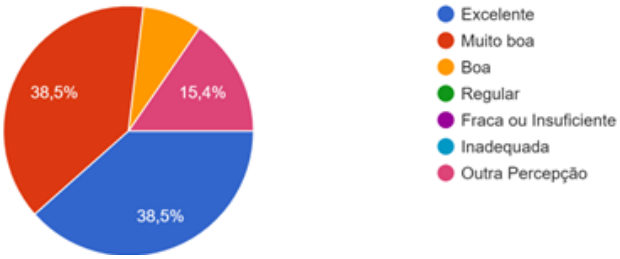
Nesse contexto, a capacitação do usuário comum deve privilegiar noções de proteção cibernética e do planejador deve ensinar como empregar as capacidades cibernéticas de exploração e ataque, além de como prever, planejar e coordenar as medidas necessárias para a proteção cibernética das redes e sistemas empregados. Em suma, a instrução deve preparar o militar para ser empregado em situações reais, tanto em situação de guerra ou de paz.

Além disso, deve apresentar o novo domínio de batalha, de forma a conscientizar a todos que o conflito pode ser influenciado e até decidido pelas possibilidades que podem surgir dos avanços tecnológicos e equipamentos militares ligados em redes e sistemas de TI, todos suscetíveis a G Ciber. Portanto, deve-se estar em condições de atuar no espaço cibernético para nossa proteção e defesa ativa, assim como dominar as ferramentas de exploração e ataque para empregar se necessário for.

Ademais, a cibernética funciona como uma importante ferramenta dentro das disciplinas de inteligência, para aquisição de dados relevantes que vão auxiliar os demais sensores. Ainda, possui a significativa função de preservar os meios cibernéticos da instituição e contribuir com a consciência situacional do comando.

Qual a sua análise sobre a formação em G Ciber do CIGE?

Gráfico 33 – A análise sobre a formação em G Ciber do CIGE



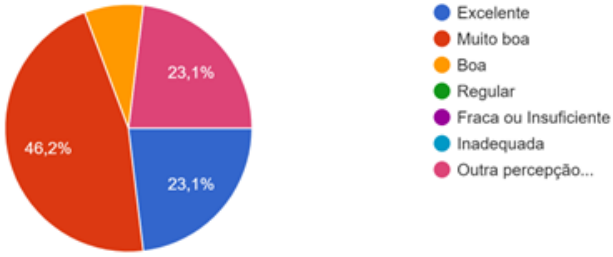
Fonte: o autor

Conforme o gráfico acima, a formação em G Ciber do CIGE é excelente ou muito boa para a maioria dos participantes do presente questionário. Corroborando com a análise do gráfico acima, destaca-se que o CIGE ensina excelentes técnicas de ataque e exploração ciber, alicerçada nas principais técnicas, cursos e atividades que existem no mundo. A seção de G Ciber procura manter o estado da arte e, para tal, há o custo de preparação dos instrutores com certificações e afins. No entanto, o curso não ensina o planejamento para o emprego da capacidade em apoio às Op F Ter.

Nesse contexto, pode-se afirmar que o Centro prepara excepcionalmente o militar para o ambiente de guerra cibernética. Porém, o processo de seleção e o sistema de reprovação de militares que não alcançam padrões mínimos, muitas vezes, comprometem a qualidade do curso. Ademais, a qualidade e o nível de capacitação esbaram na capacidade individual relacionada, principalmente, com a falta de conhecimento prévio dos alunos, para que possam aprender as ferramentas de exploração e ataque cibernético mais avançadas. Outra oportunidade de melhoria seria a ampliação do número de vagas pelo EME, para atender à demanda de pessoal capacitado para ocupar os claros de Ciber no EB e nas demais forças.

Qual a sua análise sobre a formação em proteção Cibernética na EsCom?

Gráfico 34 – A análise sobre a formação em Proteção Ciber na EsCom

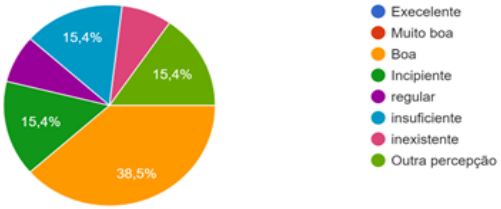


Fonte: o autor

Conforme o gráfico acima, a formação em Proteção Cibernética da EsCom foi considerada muito boa ou excelente pela maioria do público que respondeu ao questionário.

Qual a sua análise sobre a formação em Cibernética na AMAN e na ESA?

Gráfico 35 – A análise sobre a formação em Ciber na AMAN e na ESA



Fonte: o autor

Conforme o gráfico acima, a formação em Cibernética na AMAN e na ESA não teve uma conceituação excelente ou muito boa por nenhum dos especialistas consultados, sendo considerada boa ou incipiente para maioria. Como justificativas, pode-se destacar que a instrução de cibernética ministrada até o 1º ano da AMAN é boa, porém muito limitada ao conhecimento de redes basicamente, o que já é um conhecimento inicial. Porém a instrução somente prossegue nos demais anos de formação para os Cadetes do Curso de Comunicações. Entre o 2º e o 4º ano, o Cadete de Comunicações é capacitado para Proteção Cibernética de sistemas de Comando e Controle. Os demais cadetes não recebem mais instrução de cibernética a partir do 2º ano.

Uma oportunidade de melhoria seria que todos os cadetes prosseguissem nas instruções de cibernética, sem necessariamente chegar ao nível de profundidade do Curso de Comunicações, mas aprofundando os conhecimentos de redes, programação e TI, que são fundamentais para proteção cibernética e para a futura formação do Guerreiro Cibernético. Alguns cadetes se capacitam em Guerra Cibernética como eletiva ou Curso no último ano de formação, adquirindo importante capacitação para a Força Terrestre.

Quais são as maiores dificuldades enfrentadas durante a formação do Aluno em Cibernética?

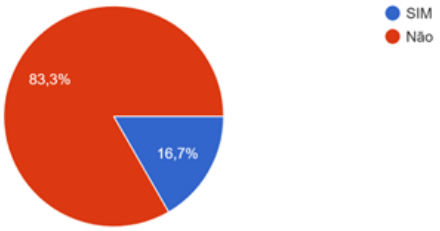
Gráfico 36 – As dificuldades enfrentadas durante a formação em Cibernética

Fonte: o autor

Conforme o gráfico acima, a maior dificuldade enfrentada durante a formação do aluno em Cibernética é a falta de uma base de conhecimentos, para que o assunto seja mais aprofundado. Outras dificuldades foram elencadas, como a falta de uma mentalidade em Proteção Cibernética, pois a maior superfície de ataque cibernético é o usuário e todos devem estar comprometidos. Ainda, deve-se desprender a cibernética da Arma de Comunicações, pois relacionar a essa arma faz com que as demais deem pouca atenção ao assunto, por julgar que seja atribuição dos comunicantes. Assim, a cibernética deve estar inserida na formação de todos os militares e reprovar os alunos que não atingirem padrões mínimos, inicialmente forçando a preocupação com esse relevante assunto.

O PLADIS do curso de G Ciber para oficiais e sargentos é o mesmo?

Gráfico 37 – A equidade do PLADIS do curso de G Ciber para Of e Sgt

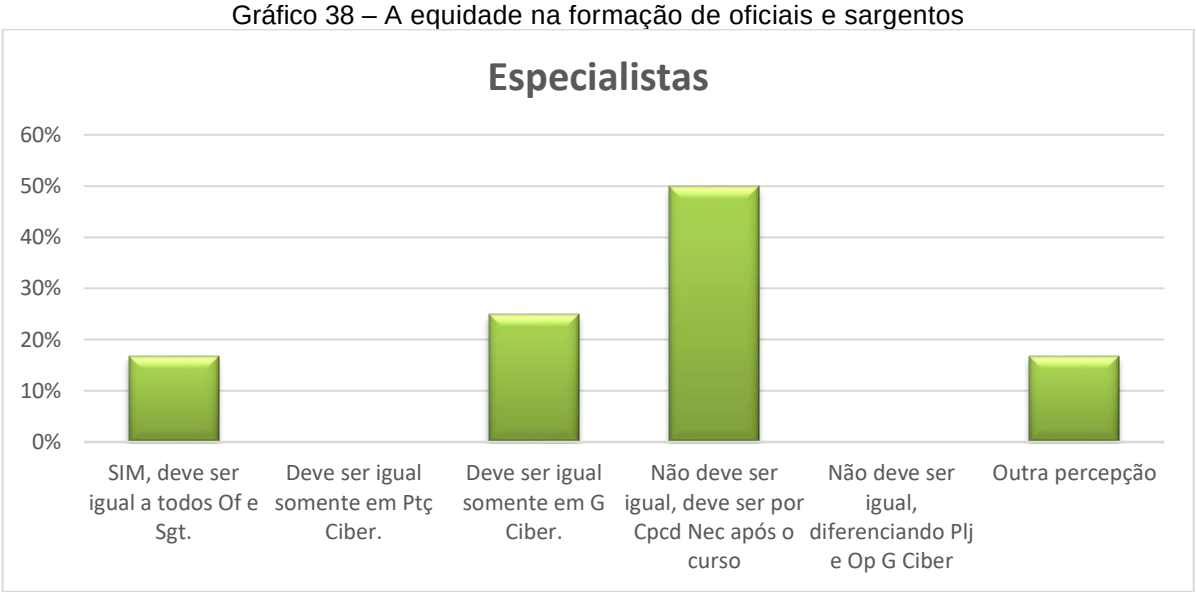


Fonte: o autor

Conforme o gráfico acima, O PLADIS do curso de G Ciber não é o mesmo para oficiais e sargentos.

Em sua opinião, a formação deve ser a mesma para oficiais e sargentos?

Gráfico 38 – A equidade na formação de oficiais e sargentos



Fonte: o autor

Conforme o gráfico acima, a maioria considerou que a formação não deve igual, pois deve ser pelas capacidades necessárias para a Força Terrestre após o curso. Ademais, considera-se que o Sgt acaba ficando mais tempo na parte operacional e os

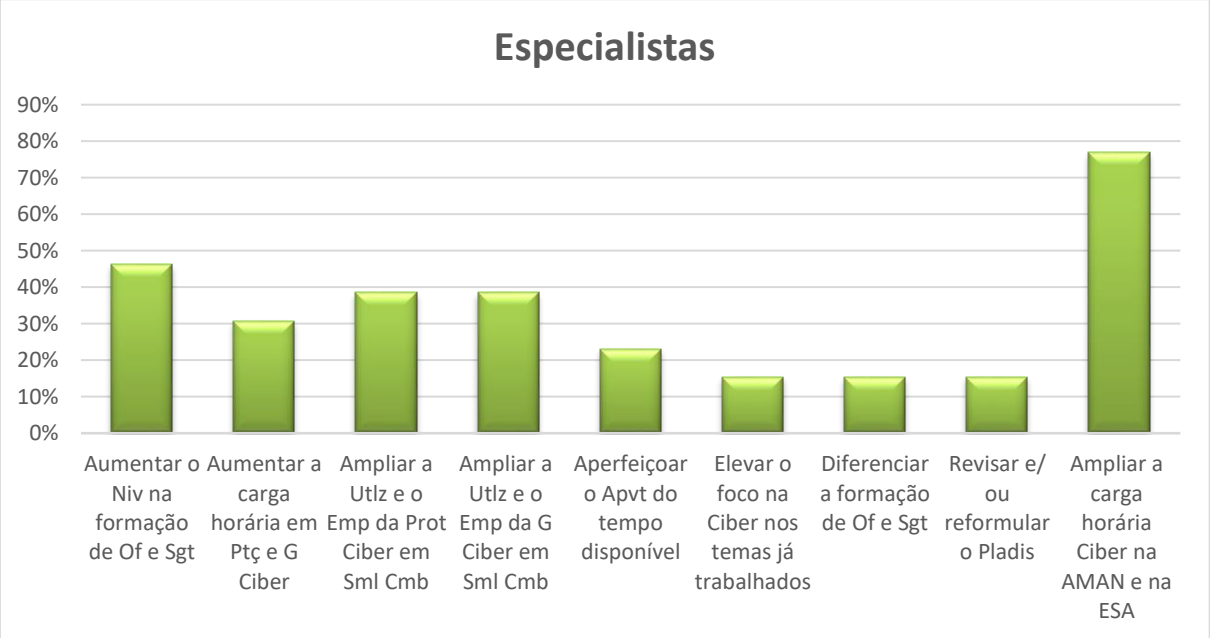
oficiais, conforme vão subindo de posto, acabam tendo que focar mais no planejamento ou até em níveis estratégicos. Ou seja, as capacidades devem ser ensinadas de acordo com a necessidade de emprego de cada público-alvo.

Assim, do ponto de vista operativo há muitas semelhanças, porém o oficial deve ser capaz de planejar e conduzir operações no espaço cibernético. Essa diferença por si já justifica um currículo diferente. Pode ser considerada, ainda, uma diferença entre a fase da carreira do oficial, por exemplo, o tenente seria mais vocacionado para operar e conduzir destacamentos, enquanto os capitães seriam capacitados, em fase posterior (um Curso intermediário, por exemplo), para planejarem e conduzirem operações mais complexas de exploração e ataque.

Como oportunidade de melhoria, poderia separar em um curso básico de G Ciber (operador) que deveria ter o PLADIS igual para of e sgt e em um curso avançado de G Ciber (planejamento de operações Ciber) que deveria ter um PLADIS diferente para Of e Sgt. Merece destaque que está em estudo a criação de um curso avançado para contemplar a necessidade de planejamento de operações Ciber.

Quais medidas o Sr. visualiza que poderiam ser incrementadas para aprimorar a formação em cibernética do Aluno?

Gráfico 39 – As medidas para aprimorar a formação em cibernética do Aluno



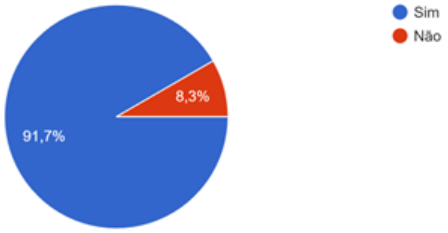
Fonte: o autor

Conforme o gráfico acima, a maioria considerou que a formação pode ser aprimorada com a ampliação da carga horária nas escolas de formação (AMAN e ESA), pois, dessa forma, o militar chegaria para o curso mais bem capacitado em conhecimentos basilares, além de despertar mais cedo para a importância do tema.

Ademais, outras medidas poderiam aprimorar a referida formação, como a reprovação de alunos que não obtenham padrões mínimos, a realização de uma formação continuada após o militar entrar no sistema para manter-se atualizado, a adoção de um ensino mais seletivo nas escolas de formação, focando naqueles que tenham conhecimento e interesse pela área, a fim de se identificar e aperfeiçoar talentos.

O estudo mais aprofundado das possíveis ameaças a estes sistemas aperfeiçoaria a formação em G Ciber?

Gráfico 40 – O estudo das ameaças e o aperfeiçoamento na formação em G Ciber

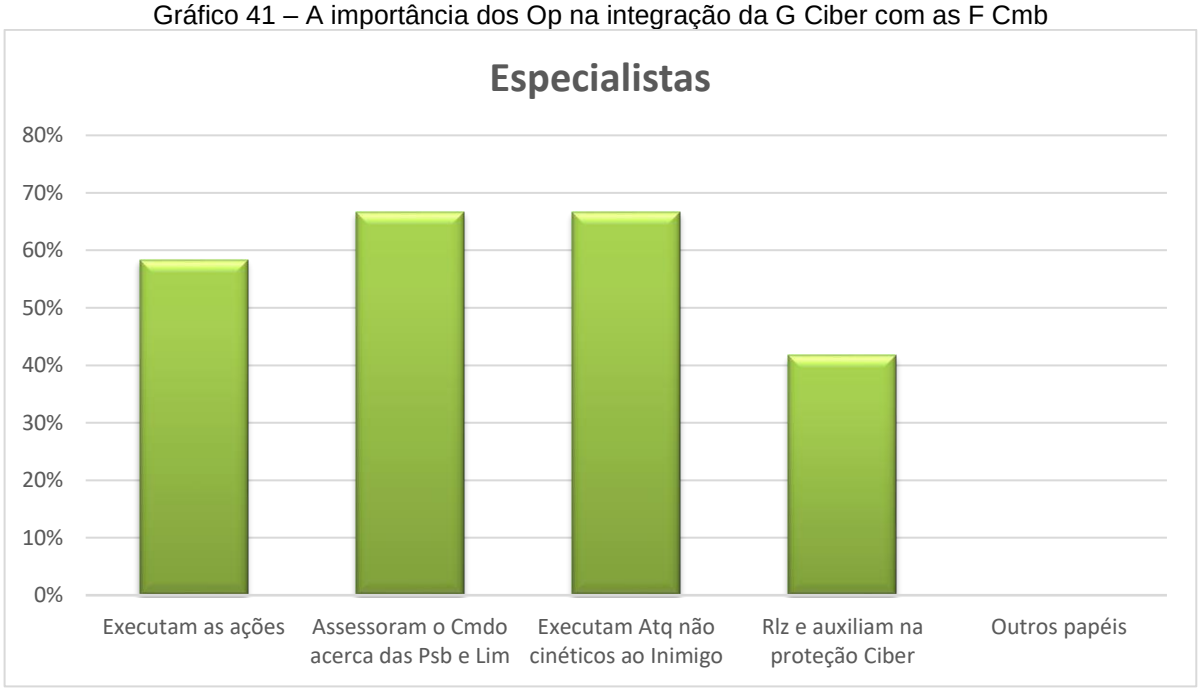


Fonte: o autor

Conforme o gráfico acima, a maioria dos participantes considerou que um estudo mais aprofundado de possíveis ameaças aos sistemas dependentes de meios de TI poderia aperfeiçoar a formação do aluno.

E qual o papel e a importância dos operadores na integração da G Ciber com as funções de combate (Mov e Man, Intlg, fogos não cinéticos, etc.)?

Gráfico 41 – A importância dos Op na integração da G Ciber com as F Cmb



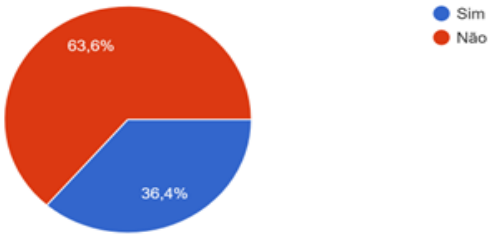
Fonte: o autor

Conforme o gráfico acima, todas as ações apresentadas expressam o papel e a importância dos operadores nessa integração, com destaque para a execução de

ataques não cinéticos ao inimigo e ao assessoramento do comando acerca das possibilidades e limitações da Guerra Cibernética.

A integração da G Ciber com as F Cmb é ensinada ao Alunos nos cursos?

Gráfico 42 – A integração ensinada aos Alunos



Fonte: o autor

Conforme o gráfico acima, a maioria dos participantes considerou a integração da G Ciber com as funções de combate não é ensinada aos alunos.

Acerca de outras contribuições para uma formação mais adequada em cibernética, merecem destaque as seguintes observações: como a proteção deve ser aplicada em todos os níveis e escalões, deve ser enfatizada nos cursos de formação (AMAN e ESA, por exemplo) podendo ser aprofundada em cursos de extensão (na EsCom, por exemplo). As ações de exploração e ataque podem ser aprendidas nos cursos de especialização do CIGE, nos moldes atuais, porém com mais vagas ou turnos.

Os cursos de Guerra e de Proteção Cibernética devem, além de realizar a referida especialização, servir para nivelar conhecimentos e procedimentos, além de criar uma mentalidade de Ciber e acerca da necessidade de manter-se atualizado, com a realização de cursos e capacitações nacionais e internacionais na área (como SANS, Offensive Security, etc).

A criação de um sistema de gestão e manutenção de militares na área de cibernética poderia favorecer o emprego prioritário na área, tal qual acontece na aviação, nas forças especiais e na inteligência, pois a capacitação é longa e continuada. Um curto período fora da atividade já pode comprometer a capacidade do militar, pela velocidade do avanço das tecnologias disruptivas.

Em função do desconhecimento das reais capacidades da G Ciber pelos grandes escalões como Brigada, Divisão de Exército e Corpo de Exército/ Comando Militar de Área, seria interessante haver uma capacitação específica de oficiais do QEMA na área.

A vaga de Oficial de Doutrina do CIGE deveria ser ocupada por um oficial do QEMA, assim como é previsto em QCP, visando realizar um avanço significativo no tocante ao planejamento destas ações nos cursos do Centro.

Por fim, a execução de Projetos interdisciplinares poderia contribuir para a consolidação dos conhecimentos e sua aplicação junto a outros cursos, como o operador e o gestor de C^2.

6 CONCLUSÃO

A presente pesquisa atendeu ao seguinte problema: como a formação e a especialização de recursos humanos do Exército Brasileiro, em Guerra e Proteção Cibernética pode ser aperfeiçoada, considerando os seguintes bancos escolares: Academia Militar das Agulhas Negras (AMAN), Escola de Sargentos das Armas (ESA), Escola de Comunicações (EsCom) e Centro de Instrução de Guerra Eletrônica (CIGE).

O objetivo geral foi apresentar formas de aprimorar a formação e a especialização de recursos humanos do Exército Brasileiro em Guerra e Proteção Cibernética, o qual foi atingido. Da mesma forma, os objetivos específicos de identificar o conceito, a metodologia empregada, os óbices e possíveis sugestões de aprimoramento na formação de oficiais e sargentos do Exército Brasileiro em cibernética, especificamente aplicada na Academia Militar das Agulhas Negras (AMAN) e na Escola de Sargentos das Armas (ESA); e de identificar o conceito, a metodologia empregada, os óbices e possíveis sugestões de aprimoramento na especialização dos Oficiais e Sargentos do Exército Brasileiro em Proteção e Guerra Cibernética, especificamente aplicada na Escola de Comunicações (EsCom) e no Centro de Instrução de Guerra Eletrônica (CIGE), também foram alcançados.

Acerca da metodologia adotada, inicialmente o presente estudo apresentou a relevância da Guerra e da Proteção Cibernética na atualidade, a qual foi embasada em pesquisas bibliográficas e comprovada por meio de exemplificação de emprego na Guerra da Ucrânia e na proteção de sistemas/ estruturas críticas de TI. Posteriormente, realizou-se uma pesquisa de campo, por meio de questionário enviado as principais escolas de formação e especialização do Exército Brasileiro, na qual coletou-se diversos dados que foram analisados e serviram de base para as considerações finais elencadas abaixo. Nesse contexto, destacou-se a importância dos cursos de formação e especialização para uma preparação mais adequada de recursos humanos no Exército Brasileiro, apresentando medidas a serem analisadas e, possivelmente, implementadas nos estabelecimentos de ensino estudados para refinar o ensino do assunto.

Assim, após o estudo realizado, verifica-se que apesar do ensino de G Ciber estar sendo bem conduzido, existem oportunidades de aperfeiçoamento que foram divididas em 03 (três) categorias: a primeira voltada para ambos os cursos (de

formação e de especialização), uma segunda voltada para os cursos de fomação (AMAN e ESA) e, finalmente, uma terceira destinada a apresentar sugestões aos cursos de especialização (EsCom e CIGE). Nesse sentido, seguem abaixo as propostas de aprimoramento na formação e na especialização em cibernética levantadas:

a. Ampliação da carga horária e da utilização e do emprego da Guerra Cibernética em simulações virtuais, construtivas e vivas de combate, elevando o foco do assunto nos temas já trabalhados nas escolas;

b. Implementar um estudo mais aprofundado das possíveis ameaças aos sistemas dependentes de meios de TI;

c. Aumentar o rigor na cobrança de resultados, com a reprovação de alunos que não obtenham padrões mínimos;

d. Implementar uma sistemática de formação continuada após o militar entrar no sistema, por meio de um programa de ensino a distância e, sempre que possível, presencial para aperfeiçoamento e atualização constante, especialmente com a evolução de novas tecnologias disruptivas;

e. A adoção de um ensino mais seletivo nas escolas de formação, focando naqueles que tenham conhecimento e interesse pela área, a fim de se identificar e aperfeiçoar talentos;

f. Em todos os Estb Ens de Ciber, deve-se buscar a manutenção de um corpo docente especializado em G/ Ptç Ciber, evitando que o assunto seja ministrado por militares com pouca ou nenhuma especialização;

g. Criação de um curso básico de cibernética para o militar identificar sua maior área de afinidade, para depois realizar uma formação mais especializada, como em OSSINT, Web, Linux, Windows, MAC, Android, Wifi, IoT, Sistemas Críticos, Forense, Anl Malware, Direito digital e inúmeros outros;

h. Criar uma política mais clara e específica de valorização de militares com capacidades cibernéticas, com um plano de carreira específico e vantajoso, cargos privativos e adicional de especialização, visando evitar a evasão ou o desinteresse em permanecer na atividade e a manutenção das capacidades operativas da Força;

i. Buscar o desenvolvimento de uma mentalidade de Guerra e Proteção Cibernética mais ampla em toda a Força Terrestre, visando a manutenção da segurança dos diversos sistemas operados, seja em tempos de paz ou de guerra, a fim de conscientizar que um conflito pode ser influenciado e até decidido pelas

possibilidades que podem surgir dos avanços tecnológicos e equipamentos militares ligados em redes e sistemas de TI, todos suscetíveis a G Ciber. Portanto, deve-se estar em condições de atuar no espaço cibernético para nossa proteção e defesa ativa, assim como dominar as ferramentas de exploração e ataque para empregar se necessário for;

j. Aumentar a integração e o uso da cibernética como uma importante ferramenta dentro das disciplinas de inteligência, para aquisição de dados relevantes que vão auxiliar os demais sensores;

k. Implementar um currículo diferente para oficiais e sargentos, pois do ponto de vista operativo há muitas semelhanças, porém o oficial deve ser capaz de planejar e conduzir operações no espaço cibernético;

l. Estabelecer, ainda, diferenças no currículo de cada fase da carreira do oficial, pois como exemplo, um tenente poderia ser mais vocacionado para operar e conduzir destacamentos, enquanto os capitães poderiam ser capacitados, em fase posterior (um Curso intermediário, por exemplo), para planejarem e conduzirem operações mais complexas de exploração e ataque;

m. Implementar medidas para mitigar os óbices pela falta de tempo e recursos para o instrutor se aperfeiçoar na atividade, priorizando sua indicação para cursos e atualização, além de evitar o desvio para outras atividades e buscar manter o instrutor na atividade; e

n. Superar deficiências em infraestrutura, como a falta de laboratório de G Ciber em estabelecimentos de ensino para praticar a teoria ensinada.

Ademais, seguem sugestões de melhorias na formação, especialmente voltadas para a AMAN e para a ESA:

a. Embora a maioria dos instrutores e monitores tenha considerado que a uniformização do PLADIS de todos os cursos em cibernética não seria viável, uma maior uniformização traria ganhos para a criação de uma mentalidade em cibernética. Como justificativas para a inviabilidade, verifica-se que a gama de conhecimento para trabalhar na área é muito grande, envolvendo programação, sistemas operacionais, protocolos de comunicação e criptografia, entre outros, o que exigiria um conjunto de pré-requisitos maior que não podem ser passados a todos os cursos de formação, devido às limitações de carga horária. Nesse contexto, como uniformização mínima, todos os cursos devem focar na mentalidade de formar um

usuário consciente na utilização de todos os sistemas de redes instalados, visando mitigar o risco do fator humano no comprometimento da proteção cibernética; e

b. Implementar uma sistemática de prosseguimento nas instruções de cibernética, sem necessariamente chegar ao nível de profundidade do Curso de Comunicações, mas aprofundando os conhecimentos de redes, programação e TI, que são fundamentais para proteção cibernética e para a futura formação do Guerreiro Cibernético. Como exemplo, alguns cadetes se capacitam em Guerra Cibernética como eletiva ou Curso no último ano de formação, adquirindo importante capacitação para a Força Terrestre.

Por fim, abaixo estão listadas as observações de possíveis aprimoramentos na especialização em Guerra e Proteção Cibernética:

a. Iniciar a capacitação na Modalidade EAD, antes do aluno se apresentar na Escola. Apesar de já estar acontecendo, são necessários mais investimento e apoio de legislação para que o militar tenha tempo de estudo na OM de origem antes da fase presencial, assim como ocorre em outros cursos, como no Curso de Aperfeiçoamento de Sargentos (CAS) e no Curso de Gestão e Assessoramento de Estado-Maior (CGAEM). Nesse contexto, a qualidade e o nível de capacitação esbaram na capacidade individual relacionada, principalmente, com a falta de conhecimento prévio dos alunos, para que possam aprender as ferramentas de exploração e ataque cibernético mais avançadas;

b. Nesse contexto, um acréscimo de tempo e das exigências de conhecimentos basilares para a execução dos cursos, especialmente na fase de nivelamento não presencial, também contribuirá para essa base necessária ao bom desenvolvimento da especialização e possibilitará aprofundar capacidades;

c. A criação de laboratórios na EsCom (cluster de servidores) semelhante ao CIGE, para montar vários cenários de defesa cibernética, o que não ocorre atualmente por limitação de hardware;

d. Aperfeiçoar o processo de seleção e o sistema de reprovação de militares que não alcançam padrões mínimos, para não comprometer a qualidade do curso;

e. Ampliação do número de vagas pelo EME, para atender à demanda de pessoal capacitado para ocupar os claros de Ciber no EB e nas demais forças;

f. Realização de especialização em duas fases. Inicialmente em um curso básico de G Ciber (operador), que deveria ter o PLADIS igual para oficiais e sargentos. Uma segunda fase poderia abarcar um curso avançado de G Ciber (planejamento de

operações Ciber), o qual deveria ter um PLADIS diferente para oficiais e sargentos. Merece destaque que está em estudo a criação de um curso avançado para contemplar a necessidade de planejamento de operações Ciber;

g. Enfatizar que os cursos de Guerra e de Proteção Cibernética devem, além de realizar a referida especialização e nivelar conhecimentos e procedimentos, buscar criar uma mentalidade de Guerra Cibernética e de constante atualização no assunto, com a realização de cursos e capacitações nacionais e internacionais (como SANS, Offensive Security, etc);

h. Criar um sistema de gestão e manutenção de militares na área de cibernética para favorecer o emprego prioritário na área, tal qual acontece na aviação, nas forças especiais e na inteligência, pois a capacitação é longa e continuada. Um curto período fora da atividade já pode comprometer a capacidade do militar, pela velocidade do avanço das tecnologias disruptivas;

i. Implementar uma capacitação específica de oficiais do QEMA na área, em função do desconhecimento das reais capacidades da G Ciber pelos grandes escalões como Brigada, Divisão de Exército e Corpo de Exército/ Comando Militar de Área;

j. Preencher a vaga de Oficial de Doutrina do CIGE com um oficial do QEMA, como previsto em QCP, visando possibilitar avanços mais significativos no tocante ao planejamento destas ações nos cursos do Centro;

k. Implementar a execução de projetos interdisciplinares visando contribuir para a consolidação dos conhecimentos e sua aplicação junto a outros cursos, como o operador e o gestor de C^2; e

l. Estimular a realização de palestras e simpósios, principalmente no CIGE, EsCom, ECEME e ESAO, com a participação de autoridades e convidados civis e militares, visando estimular o debate, a produção de conhecimento e notas complementares, assim como contribuir para a necessária criação de uma mentalidade de Proteção e Guerra Cibernética no País.

Finalmente, como recomendações para pesquisas futuras, verifica-se que a vastidão do assunto e sua complexidade sugere que a matéria pode ser mais profundamente explorada. Ademais, pode-se elencar a viabilidade de implementação das sugestões citadas acima, além de se realizar uma análise mais detalhada de cada medida, especialmente acerca de sua efetividade para possíveis aprimoramentos do ensino nos diversos estabelecimentos de ensino.

REFERÊNCIAS

ACADEMIA MILITAR DAS AGULHAS NEGRAS(AMAN). **Cadeira de Cibernética**. Publicado: Segunda, 03 de Julho de 2017, 19h01 | Última atualização em Segunda, 03 de Julho de 2017, 19h01 | Acessos: 4586. Disponível em: <http://www.aman.eb.mil.br/divisao-de-ensino/editora-academica-4> Acesso em 02 JUN 22.

ACADEMIA MILITAR DAS AGULHAS NEGRAS(AMAN). **Histórico**. Publicado: Segunda, 21 de outubro de 2013, 18h02 | Última atualização em Terça, 02 de Julho de 2019, 13h55. Disponível em: <http://www.aman.eb.mil.br/historico> Acesso em 02 JUN 22.

BBC NEWS. **Guerra na Ucrânia: os três ciberataques russos que as potências ocidentais mais temem**. 27 MAR 2022. Disponível em: <https://www.bbc.com/portuguese/internacional-60843427> Acesso em 28 abr. 22.

BELLI, Luca. Rússia inicia ataques cibernéticos contra a Ucrânia, dizem especialistas. **CNN,** 25 fev. 2022. Disponível em: <https://www.cnnbrasil.com.br/internacional/russia-inicia-ataques-ciberneticos-contra-a-ucrania-dizem-especialistas/> Acesso em 28 abr. 22.

BRANDÃO, J. E. M. D. S.; IZYCKI, E. A. Poder Ofensivo no Espaço Cibernético. In: ANDRADE, I. D. O., et al. **Desafios contemporâneos para o Exército Brasileiro**. Brasília, DF: Ipea, 2019. cap. 10, p. 241-273. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/180826_desafios_contemporaneos_para_o_exercito_brasileiro.pdf>. Acesso em: 28 ago.2019.

BRASIL. Exército. Estado-Maior. **Catálogo de Capacidades do Exército 2015-2035** (EB20-C-07.001). Brasília, 2013.

BRASIL. Exército. Estado-Maior. **Doutrina Militar Terrestre**. 1. ed. Brasília, DF. 2014a.

BRASIL. Exército. Estado-Maior. **Força Terrestre Componente**. 1. ed. Brasília, DF. 2014b.

BRASIL. Exército. Estado-Maior. **Força Terrestre Componente nas Operações**. 1. ed. Brasília, DF. 2014c.

BRASIL. Exército. Estado-Maior. **Glossário de Termos e Expressões para Uso no Exército**. 5. ed. Brasília, DF. 2018.

BRASIL. Exército. Estado-Maior. **Guerra Cibernética**. 1. ed. Brasília, DF. 2017a.

BRASIL. Exército. Estado-Maior. **Lista de Tarefas Funcionais**. 1. ed. Brasília, DF. 2016.

BRASIL. Exército. Estado-Maior. **Operações**. 5. ed. Brasília, DF. 2017b.

BRASIL. Exército. Estado-Maior. **Operações Ofensivas e Defensivas**. 1. ed. Brasília, DF. 2017c.

BRASIL. Exército. Estado-Maior. **Plano estratégico do Exército 2020-2023** (EB10-P-01.007). Brasília, 2019c.

BRASIL. Exército. **PROFORÇA**: projeto de força do Exército Brasileiro 2030. Brasília, 2012.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. 1. ed. Brasília, DF. 2014d.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas 2º Volume** (MD30-M-01). 2ª edição. Brasília, 2020a.

BRASIL. Ministério da Defesa. **Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas**. 3ª edição. Brasília, DF. 2008.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, 2020b.

CENTRO DE INSTRUÇÃO DE GUERRA ELETRÔNICA(CIGE). **Centro de Instrução de Guerra Eletrônica**. Disponível em: <http://www.cige.eb.mil.br/index.php/en/sobre-o-cige> Acesso em 04 JUN 22.

CORRÊA, F. G. Planejamento baseado em capacidades e transformação da Defesa: desafios e oportunidades do Exército Brasileiro. **Artigos estratégicos**, Brasília, v. 8 (1), p. 27-54, jan/jun. 2020, ISSN 2525-7099.

DEPARTAMENTO DE PESQUISA E PÓS-GRADUAÇÃO - ECEME. **Elaboração de Projetos de Pesquisa na ECEME**. – Rio de Janeiro, 2012.

ESCOLA DE COMUNICAÇÕES (EsCom). **O Comunicante Revista Científica Volume 7 Nr** Brasília, DF. 2017.

ESCOLA DE COMUNICAÇÕES (EsCom). **Histórico**. Disponível em: <https://escom.eb.mil.br/historico> Acesso em 04 JUN 22.

ESCOLA DE SARGENTOS DAS ARMAS (ESA). **O Curso de CFGS**. 02 JUN 2022. Disponível em: <https://esa.eb.mil.br/index.php/pt/missao/> Acesso em 02 JUN 22.

ESCOLA DE SARGENTOS DAS ARMAS (ESA). **Resumo Histórico**. 02 JUN 2022. Disponível em: <https://esa.eb.mil.br/index.php/pt/resumo-historico/> Acesso em 02 JUN 22.

GAZETA DO POVO. **Falha grave em segurança do Wi-Fi deixa redes à mercê de ataques.** Disponível em: <http://www.gazetadopovo.com.br/economia/novaeconomia/falha-grave-em-seguranca-do-wi-fi-deixa-redes-a-merce-de-ataques39gs7cb1o64n6> Acesso em: 17 de outubro de 2017.

GAZETA DO POVO. **Hackers norte-coreanos roubaram táticas de guerra dos EUA e da Coreia do Sul**. Disponível em: <http://www.gazetadopovo.com.br/mundo/hackers-norte-coreanos-roubaram-taticasde-guerra-dos-eua-e-da-coreia-do-sul-d4jcdi77i3tr0lwviz1aen8lz> Acesso em: 11 de outubro de 2017.

IZYCKI, E. A. ; Cortinhas, J. S.; **Conflito Cibernético - Evolução ou Revolução?** (UNB - Universidade de Brasília); Disponível em: <https://www.enabed2021.abedef.org/trabalho/view?ID_TRABALHO=4985> Acesso em: 26 de abril de 2022.

JOVEN PAN NEWS. **Rússia coordena ataques cibernéticos e militares na Ucrânia, diz Microsoft**. 27 abr. 2022. Disponível em: <https://jovempan.com.br/noticias/mundo/russia-coordena-ataques-ciberneticos-e-militares-na-ucrania-diz-microsoft.html> Acesso em 28 abr. 22.

NEVES, Eduardo Borba; DOMINGUES, Clayton Amaral. **Manual de Metodologia da Pesquisa Científica.** Rio de Janeiro: EB/CEP, 2007.

NEUVALD, M. A. B. O processo de reestruturação do Exército alemão. **PADECEME**, Rio de Janeiro, v. 9, n. 18, p. 12-21, 2017.

SANTOS FILHO, J. F. C. O processo de transformação do Exército sul-coreano. **PADECEME**, Rio de Janeiro, v. 9, n. 18, p. 22-35, 2017.

SCHNAUBELT, C. M.; LARSON, E. V.; BOYER, M. E. **Vulnerability Assessment Method Pocket Guide:** a tool for center of gravity analysis. Santa Monica, CA: RAND Corporation, 2014. 142 p. UNITED KINGDOM. Ministry of Defence. **Cyber Primer**. 2. ed. Swindon: Development, Concepts and Doctrine Centre of Ministry of Defence, 2016. Disponível em: <www.gov.uk/mod/dcdc>. Acesso em: 5 set. 2019.

SILVA, Washington Rodrigues da. **Análise econômica dos impactos de ataques cibernéticos**. 2018. 107 f., il. Dissertação (Mestrado em Economia) - Universidade de Brasília, Brasília, 2018.

TZU, Sun. **A arte da guerra**. Tradução de José Sanz. Rio de Janeiro: Record, 1999.

UNITED STATES. Department of the Army. **2005 Army Modernization Plan**. Washington, 2005.

US ARMY. **Cyberspace Operations Concept Capability Plan 2016-2028:** TRADOC Pamphlet 525-7-8. Newport News: U.S. Army Capabilities Integration Center, 2010.

US ARMY. **Intelligence Preparation of the Battlefield:** ATP 2-01.3. Washington, DC: Department of the Army, 2019.

USA. Departament of Defense. **Cyberspace Operations:** JP 3-12. Washington: Departament of Defense, 2018.

VEGETIUS. The military institutions of the romans. In: PHILLIPS, T. R. (org.). **Roots of strategy**: the 5 greatest military classics of all time. v. 1. Harrisburg: Stackpole Books, 1985.

VASQUEZ, V. L. O Processo de Elaboração da Lista de Alvos Cibernéticos no Nível Tático, **CIGE**, Brasília – DF, v.1, n.1, p. 42-46, 2020.

APÊNDICES A, B, C, D e E - QUESTINÁRIOS PARA AMAN(A), ESA(B), CIGE(C), especialistas(D) e EsCom(E).

Questionário acerca da formação e especialização em Cibernética

Este questionário de caráter exploratório, constitui-se em um instrumento de pesquisa sobre: A IMPORTÂNCIA DOS CURSOS DE FORMAÇÃO E ESPECIALIZAÇÃO DO EXÉRCITO BRASILEIRO PARA UMA PREPARAÇÃO MAIS ADEQUADA DE RECURSOS HUMANOS VOLTADA PARA A GUERRA CIBERNÉTICA, estudo a ser apresentado à Escola de Comando e Estado-Maior do Exército(ECEME) pelo TC Inf JONAS MOLZ, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Qualquer dúvida, entrar em contato pelo e-mail: jonasmolz1152@gmail.com ou molz.jonas@eb.mil.br ou pelo Nº (51)995492070.

CONSENTIMENTO DE PARTICIPAÇÃO: o Senhor concorda em participar voluntariamente do presente estudo respondendo o presente questionário? O pesquisador (TC MOLZ) informa que sua participação poderá ocorrer por meio deste questionário e pelo envio de materiais complementares ao pesquisador, caso seja necessário, tudo para validar as sugestões de aperfeiçoamento a serem inseridas no estudo em questão. Ademais, o pesquisador garante que o Senhor poderá sair da pesquisa a qualquer momento, e que esta decisão não trará nenhum tipo de penalidade. Ainda, quaisquer dúvidas podem ser sanadas por meio dos e-mails: jonasmolz1152@gmail.com ou molz.jonas@eb.mil.br ou por meio do Telefone (51)99549-2070. *Marcar apenas uma oval.*

( ) ACEITO PARTICIPAR ( ) NÃO ACEITO PARTICIPAR

Termo de consentimento livre e esclarecido. Ressalta-se que não será obrigatória a identificação neste questionário. Nesse contexto, o Senhor concorda com a divulgação dos resultados do presente questionário e autoriza o uso dos dados levantados na pesquisa científica em desenvolvimento? *Marcar apenas uma oval.*

( ) Sim ( ) Não

A pesquisa acerca da importância dos Cursos de Formação e Especialização do Exército Brasileiro para uma preparação mais adequada de recursos humanos, voltada para a Guerra Cibernética, tem por finalidade levantar concepções baseadas no conhecimento especializado e na experiência de profissionais da área da Cibernética.

Como corolário, tem-se a expectativa de compreender, de maneira mais detalhada, como ocorre a formação e a especialização de Oficiais e Sargentos na área da Cibernética, e VERIFICAR A VIABILIDADE DE APRESENTAR POSSÍVEIS SUGESTÕES DE APERFEIÇOAMENTOS NO PROCESSO DE ENSINO-APRENDIZAGEM.

1. Inicialmente, cite abaixo somente sua OM, seu Curso/Seção e seu Posto/ Graduação. Não é necessária sua identificação.

1.1 Caso deseje se identificar, use o espaço abaixo para colocar os dados que deseje, como nome, telefone, e-mail, etc.

2. Qual sua função desempenhada, detalhando sua participação atual ou passada na instrução / formação em G ou Def Ciber?

3. Por quanto tempo / em que período desempenha(ou) essa função?

4. Poderia comentar a sua experiência profissional relacionada ao setor cibernético?

5. Em sua percepção, qual(is) o(s) principal(ais) objetivo(s) da Cibernética ou da Instrução de Ciber?

6. Qual a sua análise sobre a formação em G Ciber do Curso de Comunicações da Escola? *Marcar apenas uma oval.*

( ) Excelente

( ) Muito boa

( ) Boa

( ) Regular

( ) Fraca ou Insuficiente

6.1 Complemente sua resposta anterior (SFC)

7. Qual a sua análise sobre a formação em G Ciber das demais Armas, Quadro e Serviço da Escola? *Marcar apenas uma oval.*

( ) Excelente

( ) Muito boa

( ) Boa

( ) Regular

( ) Fraca ou Insuficiente

( ) Inadequada

( ) Outra percepção...

7.1 Caso tenha selecionado o item "Outra percepção" na questão anterior, favor citar alguma(s).

8. Quais são as maiores dificuldades enfrentadas durante a formação em Cibernética? (aceita-se mais de uma resposta) *Marque todas que se aplicam.*

( ) falta de carga horária disponível

( ) falta de interesse do Cadete/ Aluno no assunto

( ) falta de entendimento da necessidade de uma mentalidade em proteção/ defesa cibernética durante operações

( ) falta de uma base de conhecimentos, a exemplo da transmitida ao C Com, para que o assunto seja mais aprofundado nos demais cursos

( ) Outras dificuldades...

8.1 Caso tenha selecionado o item "Outras dificuldades" na questão anterior, favor citar alguma(s).

9. Em sua opinião, a formação básica em Guerra e Proteção/Defesa Cibernética deve ser a mesma para todas as Armas, Quadros e Serviço? Justifique.

( ) SIM, deve ser igual a todos os Cursos.

( ) Deve ser igual somente em Proteção/ Defesa Ciber.

( ) Deve ser igual somente em G Ciber.

( ) Não deve ser igual, deve manter privilegiando o C Com.

( ) Não deve ser igual.

9.1 Justifique sua resposta anterior acerca da formação básica em Guerra e Proteção/ Defesa Cibernética?

10. Quais medidas o Sr. visualiza que poderiam ser incrementadas na formação em Cibernética, especialmente com foco na defesa/ proteção? *Marque todas que se aplicam.*

( ) Nivelar a formação de todos os cursos em Cibernética

( ) Aumentar a carga horária em Proteção/ Defesa e Guerra Cibernética

( ) Aumentar a carga horária em Proteção/ Defesa Cibernética

( ) Aumentar a carga horária em Guerra Cibernética

( ) Ampliar a utilização e o emprego da Proteção/ Defesa Cibernética em simulações virtuais, construtivas e reais de combate

( ) Ampliar a utilização e o emprego da Guerra Cibernética em simulações virtuais, construtivas e reais de combate

( ) Aperfeiçoar o aproveitamento do tempo disponível para o assunto

( ) Com foco no ensino por competências, no qual todos os conceitos devem ser trabalhados em conjunto, poder-se-ia elevar o foco na cibernética nos diversos temas já trabalhados na escola.

( ) Outras medidas...

10.1 Caso tenha selecionado o item “Outras medidas” na questão anterior, favor citar alguma(s).

11. Seria possível uniformizar o PLADIS de todos os cursos no assunto? Justifique

( ) SIM ( ) NÃO ( ) Depende

11.1 Justificativa(s) para a resposta anterior. *Marque todas que se aplicam.*

( ) A gama de conhecimento para trabalhar na área é muito grande: programação, sistemas operacionais, protocolos de comunicação, criptografia. Tudo isso pode exigir um conjunto de pré-requisitos maior que, talvez, não possam ser passados em todos os cursos de formação.

( ) A carga horária não permite

( ) Falta de maturidade do Cadete/ Aluno para entender a importância e os riscos da utilização imprópria e sem autorização de meios constantes do assunto

( ) Outras justificativas...

11.2 Caso tenha selecionado o item “Outras justificativas” na questão anterior, favor citar alguma(s).

12. Qual a necessidade/ frequência de atualização de conhecimento/cursos na área para manter-se em dia com as novidades e tecnologias disruptivas?

( ) Constante, de forma diária

( ) Constante, com periodicidade semanal

( ) Constante, com periodicidade mensal

( ) Constante, com periodicidade semestral

( ) Constante, com periodicidade anual

( ) Pouco necessária

13. Qual(ais) a(s) melhor(es) forma de atualização? *Marque todas que se aplicam.*

( ) Cursos na área

( ) Por buscar na internet

( ) Por sites corporativos(Forças Armadas, EB, CIGE, C DEF CIBER, etc)

( ) Por meio de livros

( ) Por meio de artigos científicos (TCC, Monografias, Teses, etc)

( ) Outras formas...

13.1 Caso tenha selecionado o item “Outras formas” na questão anterior, favor citar alguma(s).

14. Existe alguma plataforma corporativa que permita, apoie ou facilite essa atualização?

( ) Sim ( ) Não

15. Seria interessante a criação de uma plataforma que permitisse essa constante atualização, que trouxesse as novidades e inovações aos interessados, além de realizar constante reciclagem nos especialistas na área? *Marcar apenas uma oval.*

( ) Sim ( ) Não

16. Qual seria o Centro de referência mais apto a criar e manter uma plataforma que atendesse a essa necessidade? *Marcar apenas uma oval.*

( ) CIGE

( ) EsCOM

( ) AMAN

( ) ESA

( ) CCOMGEX

( ) Outro Centro/ Local.

( ) Não é o caso ser criada uma plataforma com essa finalidade

16.1 Caso tenha selecionado o item Outro Centro/ Local na questão anterior, favor citar qual.

17. Quais Meios de Emprego Militar (MEM) podem ser elencados como dependentes de meios de TI, como armamentos e/ ou equipamentos, e que são ou que poderiam ser destacados como vulneráveis a atuação da G Ciber para o Cadete?

( ) Sistema de Armas.

( ) SARP Rec.

( ) SARP Ataque.

( ) Radares/ sensores.

( ) Sistemas de C^2.

( ) Sistemas/ Meios de ataque.

( ) Sistemas e meios de Proteção/ defesa cibernética.

( ) Outros

17.1 Cite exemplo(s) e, se possível, descreva alguns MEM dependentes de meios de TI, que podem sofrer interferências cibernéticas (sistema de Armas, SARP, radares,

sensores, sistemas de C^2, sistemas/ meios de ataque e Proteção/ defesa cibernética, etc).

18. O estudo mais aprofundado das possíveis ameaças a estes sistemas aperfeiçoaria a formação do futuro oficial no assunto em tela? *Marcar apenas uma oval.*

( ) Sim ( ) Não

19. De que maneira a G Ciber pode ser integrada as Funções de Combate (Movimento e Manobra, Inteligência, Fogos, Comando e Controle, Proteção e Logística), potencializando os efeitos dessas no combate? (aceita-se mais de uma resposta)

( ) Atacando sistema de Armas. Quais; de que forma?

( ) Controlando SARP Rec e/ ou Ataque.

( ) Dificultando a utilização de Radares/ sensores de vigilância. Como?

( ) Dificultando o uso de sistemas de C^2. De que forma?

( ) Atacando sistemas de redes. Como?

( ) Realizando a proteção/ defesa cibernética de nossos meios. De que forma?

( ) Outras. Quais?

19.1 Complemente a resposta anterior, detalhando formas de integração da Cibernética (Atq e Def) com as funções de Combate.

20. E qual o papel e a importância dos operadores nessa integração? (aceita-se mais de uma resposta) *Marque todas que se aplicam.*

( ) Executam as ações

( ) Assessoram o Cmdo acerca das possiblidades e limitações da G Ciber.

( ) Executam Ataques não cinéticos ao Inimigo.

( ) Realizam/ auxiliam na proteção/ defesa dos nossos meios.

( ) Outros papéis. Quais?

20.1 Caso tenha selecionado o item “Outros papéis” na questão anterior, ou queria complementar sua resposta, use o espaço abaixo.

21. Essa integração é ensinada ao Aluno de todos os Cursos?

( ) Sim ( ) Não

22. O Sr possui mais alguma ideia ou ponto para destacar, no que tange à contribuição para uma formação mais adequada em G Ciber ou acerca de qualquer outro aspecto atinente ao estudo em questão?

23. Por fim, o senhor já escreveu alguma publicação, artigo ou trabalho atinente ou relacionado ao assunto em tela?

( ) Sim ( ) Não.