ESCOLA DE GUERRA NAVAL

CC WAGNER GONÇALVES PEREIRA

GESTÃO CIBERNÉTICA:

possibilidades e capacidades na Guerra Cibernética

Rio de Janeiro

2019

CC WAGNER GONÇALVES PEREIRA

GESTÃO CIBERNÉTICA:

possibilidades e capacidades na Guerra Cibernética

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CMG (FN-RM1) William

Rio de Janeiro

Escola de Guerra Naval

2019

À minha família por compreender minha carreira.

AGRADECIMENTOS

Aos meus orientadores, CMG (FN-RM1) William, pela paciência e orientações.

A todos os Docentes da Escola de Guerra Naval por colaborarem com o desenvolvimento da turma CEMOS-2019.

Aos servidores militares e civis da Escola de Guerra Naval pelo grande empenho e por proporcionarem aos Oficiais-Alunos do CEMOS-2019 o melhor apoio possível.

Aos amigos da turma CEMOS-2019, pela camaradagem e salutar convivência ao longo de todo o curso.

Aos amigos: Capitã (QCO) Alessandra Augusta de Santana e Silva Monteiro, Capitão de Corveta Warisson Guimarães Alves e CT (EN) Mauro Quiles de Oliveira Lustosa por colaborarem nesta pesquisa com seus conhecimentos e experiências.

A minha esposa, Ana Roberta, e minha filha, Lara, pela paciência e por saberem esperar.

Aos meus pais, Fernando e Lenita, pelas visitas semanais e pela atenção dada a minha filha.

À Marinha do Brasil, por conceder-me esta oportunidade.

A Deus, por tudo. Sempre.

A esperança tem duas filhas lindas, a indignação e a coragem; a indignação nos ensina a não aceitar as coisas como estão; a coragem, a mudá-las.

Santo Agostinho

RESUMO

Na era da informação, a Guerra Cibernética se tornou uma das maiores ameaças aos Estados, às empresas, às infraestruturas críticas, assim como aos Navios de Guerra. Isso ocorre porque os navios das Marinhas modernas são conectados entre si e com suas bases em terra por meio de uma imensa rede. Essa rede pode ser a Internet, intranet ou rede segura de uma força naval. Porém, ainda que se configurem de maneiras distintas, todas estão contidas no ciberespaço ou espaço cibernético. Tendo em vista esse cenário, o objetivo dessa pesquisa é promover a reflexão quanto à necessidade de inovar a Doutrina Militar Naval de emprego operacional de Guerra Cibernética, apontando lacunas interpretativas encontradas em documentos e normas navais. Para tanto, a condução deste trabalho seguiu a metodologia de pesquisa aplicada, exploratória, bibliográfica e documental, de modo a demonstrar, por meio de argumentos e fatos coletados em literatura aberta, que está provado que ações cibernéticas podem ser convertidas em resultados físicos ou cinéticos, uma vez que os navios estão cada vez mais dependentes da interconectividade, a fim de conseguir melhores informações em tempo oportuno. Assim, aponta-se, nesta dissertação que essa dependência traz consigo vulnerabilidades e riscos que devem ser mitigados com adoção de técnicas, tecnologias, sistemas e principalmente por meio do emprego de guerreiros cibernéticos devidamente capacitados. Por isso, ao longo da pesquisa, fatos e argumentos encontrados iluminaram a premente necessidade de iniciar a capacitação dos oficiais da Armada.

Palavras-chave: Guerra Cibernética. Espaço Cibernético. Ciberespaço. Capacitação. Gestão de Pessoas por Competência.

LISTA DE ABREVIATURAS E SIGLAS

AMAN -	Academia Militar das Agulhas Negras
AMD -	Análise Multicritério à Decisão
CA -	Corpo da Armada
CCB-	Corveta Classe Barroso
CDCiber -	Centro de Defesa Cibernética
CHA -	Conhecimentos, Habilidades e Atitudes
CIAW -	Centro de Instrução Almirante Wandenkolk
ComDCiber -	Comando de Defesa Cibernética
CTMSP -	Centro Tecnológico da Marinha em São Paulo
DHS -	Department of Homeland Security
DMNGCiber -	Doutrina Militar Naval de Guerra Cibernética
EB -	Exército Brasileiro
EN -	Escola Naval
ENaDCiber -	Escola Nacional de Defesa Cibernética
FFAA -	Forças Armadas
FCG -	Fragatas Classe Greenhalgh
FCN -	Fragatas da Classe Niterói
GPC -	Gestão de Pessoas por Competências
HC -	Habilitação em Comunicações
HE -	Habilitação em Eletrônica
IPqM-	Instituto de Pesquisas da Marinha
MB -	Marinha do Brasil
MD -	Ministério da Defesa
PND -	Plano Nacional de Defesa
QFE -	Qualificação Funcional Específica
QTE -	Qualificação Técnica Especial
RDS-Defesa -	Rádio Definido por *Software* de Defesa
SC -	Sistemas Ciberfísicos
SCM -	Sistema de Controle e Monitoração das Corvetas da Classe Inhaúma
SCMPA -	Sistema de Controle e Monitoração da Propulsão e Auxiliares das Fragatas da Classe Niterói
TI -	Tecnologia da Informação
TIC -	Tecnologia da Informação e Comunicações
VANT -	Veículo Aéreo Não Tripulado

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

No mundo pós-Guerra Fria (1947-1989), as ideologias dos dois grandes blocos, capitalista e soviético, deixaram de ser os principais impulsionadores do clima de tensão entre as grandes potências. Nesse sentido, interesses, principalmente econômicos, passaram a ditar as interações e conflitos em diversos níveis e os sistemas de Tecnologia da Informação (TI), outrora criados para potencializar resultados organizacionais, e que começaram a ser atacados ou utilizados em proveito de operações de guerra cibernética. Assim como as ferrovias no final do século XIX, que aproximaram povos ao mesmo passo que simplificaram o deslocamento de tropas em combate, as tecnologias da informação no século XXI exercem as mesmas funções, aproximação e guerra.

Nesse cenário emerge a possibilidade do empreendimento da "Guerra Cibernética". Por meio dela, o inimigo descaracterizado e anônimo é capaz de atuar em proveito de interesses nacionais e/ou particulares sem a necessidade de recorrer ao combate físico armado. Isso ocorre porque a permeabilidade do ambiente cibernético traz possibilidades diversas em qualquer ambiente de guerra. No que diz respeito ao seu impacto nas forças navais, assim como a Guerra Eletrônica[1], a Guerra Cibernética pode ser capaz de "cegá-las", "ensurdecê-las" e "calá-las", além de "imobilizá-las" e, por que não, "destruí-las", haja vista seu poder de alcance[2] e impacto muito maior.

O tráfico (de pessoas, armas e entorpecentes), o contrabando e o descaminho são conduzidos pelo mar desde a Antiguidade, sendo, hoje, os grandes responsáveis pela desordem pública vivenciada em terra. Apesar de não constituir uma nova ameaça, a pirataria segue

---

1 As ações de guerra eletrônica são aquelas que visam explorar as emissões do oponente, em toda a faixa do espectro eletromagnético, com a finalidade de conhecer sua ordem de batalha eletrônica, intenções e capacidades, e, também, utilizar medidas adequadas para negar o uso efetivo dos seus sistemas, enquanto se protege e utiliza, com eficácia, os próprios sistemas (BRASIL, 2017a, p. 56).

2 A guerra cibernética possui Alcance Global, pois possibilita a realização de ações em escala global, sem limitações físicas de distância e espaço; e causa a Vulnerabilidade das Fronteiras Geográficas pois suas ações não se limitam a fronteiras geograficamente definidas. Os agentes podem atuar a partir de qualquer local e provocar efeito em qualquer lugar (BRASIL, 2014a).

ampliando em ocorrência e a cada dia trazendo mais riscos ao tráfego marítimo, sendo, assim, uma ameaça significativa a ser enfrentada pelas marinhas de guerra (WEDIN, 2015). Contudo, à semelhança dos piratas, apresentam-se hoje *hackers* capazes de atacar forças navais e suas infraestruturas em terra sem sequer saírem de suas casas. Nesse contexto, a Marinha do Brasil (MB) procura, sem se esquecer do preparo para o combate naval, incrementar o preparo de seus militares para empregar a sua capacidade cibernética, ofensiva e defensiva, a fim de enfrentar as novas ameaças até então consideradas atividades subsidiárias[3], e que hoje tornaram-se parte das atividades-fim[4] como capacidade operacional à luz das exigências do combate moderno, da sociedade brasileira e dos compromissos internacionais assumidos.

Em face desse cenário, o presente trabalho se propõe a promover reflexões que dizem respeito às experiências dos Estados mais avançados no campo cibernético, como os Estados Unidos da América e a Rússia; às vulnerabilidades observadas em nossa Marinha e as inferidas por meio das experiências estudadas; às capacidades técnico-operacionais; e às possibilidades de emprego da Guerra Cibernética em proveito de uma Força Naval. Desse modo, tem-se como objetivo a inovação do pensamento naval quanto ao emprego da doutrina de guerra cibernética da MB.

Cabe apontar que a ideia deste estudo nasceu das leituras dos livros e publicações para o concurso do CEMOS 2019, em especial do texto transcrito abaixo de Wedin (2015, p. 172):

> Um navio de guerra pode ser compreendido como um vasto sistema de informação [...] com a finalidade de conectar os homens e as máquinas. A informação em questão depende do mesmo modo da técnica (o estado do sistema de propulsão, por exemplo) ou da administração como dos dados que alimentam os sistemas de armas. Uma grande parte dessa informação transita por cabos, entretanto, fez-se necessário, também, obter informação vinda do exterior, a qual passa pela via eletromagnética.
> O navio de guerra do futuro irá pôr em serviço os "drones" de vigilância, até mesmo os de combate, acima, sobre e abaixo da superfície do mar. Quanto aos drones submarinos, a conexão é efetuada, como já se viu, por meio de sinais sonoros, o que

[3] Atividades subsidiárias são todas as atividades não relacionadas diretamente com o combate naval propriamente dito, mas que estão sob responsabilidade de execução ou fiscalização da MB (BRASIL, 2017a).

[4] Atividades-fim são todas as Operações e Ações militares relacionadas com a guerra naval (BRASIL, 2017a).

> apenas permite um volume de informações de pequena monta. Os outros drones são conectados por meio de enlaces eletromagnéticos.
> Os navios de uma força naval são conectados, também, entre eles dentro de uma imensa rede. Hoje em dia, é possível utilizar a informação coletada por um navio para acionar os sistemas de armas de um outro navio. Isto exige uma grande quantidade de dados trocados entre computadores. No caso de a força naval ter que cobrir uma vasta área, o que é geralmente o caso, é preciso utilizar os enlaces por satélites. Os satélites são igualmente necessários para a navegação, [...].
> Finalmente, a força naval está conectada aos estados-maiores em terra, o que demanda aqui, mais uma vez, os enlaces por satélites. Fala-se, então, de um sistema dos sistemas, os quais são, geralmente, ligados entre eles por via eletromagnética, assim como, por cabos. Se é seguido o pensamento do almirante Greenert, pode-se dizer que toda essa vasta rede constitui o ciberespaço.

Ademais, compreende-se que, segundo Bizerra (2017), a guerra cibernética acontece no ciberespaço, mas seus resultados, dentro do ambiente de guerra naval[5], podem ser tão danosos quanto um ataque bélico convencional; porque as ações cibernéticas se iniciam no "mundo virtual" mas podem impactar cineticamente a dimensão física.

Por isso, o problema apontado como norteador desta pesquisa está representado na conjugação das citações diretas abaixo listadas e extraídas da Doutrina Militar Naval (DMN) (BRASIL, 2017a) e da Estratégia de Ciência, Tecnologia e Inovação (CT&I) da MB, que apresenta a visão estratégica de fortalecimento da "capacidade da Marinha de atuar na defesa do ambiente cibernético" (BRASIL, 2015, p. 12) da seguinte maneira:

> [...] realizar o monitoramento dos riscos e das ameaças ao espaço cibernético da MB, incrementando ações para ampliar a capacidade de defesa cibernética e minimizar as vulnerabilidades identificadas, especialmente no tocante ao Tráfego de Rede, Armazenamento de Dados e Telefonia, e incrementar a mentalidade de SID. (BRASIL, 2015, p. 12)

> As *ações de guerra cibernética* são aquelas que envolvem o emprego de ferramentas disponíveis nos campos da Tecnologia da Informação e Comunicações para desestabilizar os *ativos de informação* do inimigo e, também, para possibilitar a proteção dos *ativos de informação* de interesse. (BRASIL, 2017a, p.57-58)

Ao observar as citações, percebe-se um possível subaproveitamento das possibilidades de emprego da arma cibernética haja vista limitações demasiadas ao uso do ciberespaço para assegurar/desestabilizar as Informações Digitais, os Ativos de TI e as

---

5 Entende-se como ambientes de guerra: o naval, o terrestre e o aeroespacial. (BRASIL 2014a)

Comunicações Navais. Cabe apontar que essa situação tem lugar ainda que Brasil (2017a) liste e defina as Operações e Ações de Guerra Cibernética como potencializadoras das Operações Navais. Por conseguinte, a doutrina de emprego operacional de guerra cibernética (Publicação Reservada EMA-416) poderá apresentar lacunas de aprofundamento quanto às possibilidades reais de conjugação da arma cibernética com as demais ações de guerra naval.

Nesse sentido, o presente estudo tem o intuito de provocar reflexões a respeito dos três "pilares" da DMN: experiência, tecnologia e capacidades (BRASIL, 2017a), além de fomentar a inovação da guerra cibernética na MB sob o enfoque da Armada. Também tenta-se compreender, ao longo de toda a pesquisa, qual dos três pilares da Doutrina deve ser modificado para que se inicie a caminhada rumo a "inovação cibernética". Também tenta-se demonstrar outras concepções e formas de abordagens (sem o objetivo de esgotá-las), a fim de desenvolver uma doutrina moderna, exequível e adequada ao ambiente naval para mitigar ameaças cibernéticas e capacitar a MB para empregar técnicas de exploração e ataque cibernéticos, visando a vantagem tática e operacional das forças navais brasileiras quando em operação de combate. Para alcançar tal objetivo, este estudo tentará responder a seguinte pergunta: como elaborar, inovar ou incrementar uma doutrina de emprego operacional de guerra cibernética específica para o ambiente naval, a Doutrina Militar Naval de Guerra Cibernética (DMNGCiber)?

De modo a empreender esta pesquisa, utilizou-se a metodologia de pesquisa aplicada[6], exploratória[7], bibliográfica e documental[8], por meio de argumentos e fatos coletados em literatura aberta, a fim de responder à pergunta de pesquisa. Portanto, a pesquisa foi elaborada de forma flexível e ampla, a fim de permitir o estudo do tema sob diversos ângulos e

---

6 Visa à geração de conhecimentos a serem utilizados, a fim de buscar soluções para um problema específico: fomentar a inovação da Doutrina Militar Naval de Guerra Cibernética (DMNGCiber) (PRODANOV e FREITAS, 2013).

7 Tem como finalidade proporcionar mais informações sobre o assunto, orientar a fixação de objetivos e descobrir um novo tipo de enfoque para a guerra cibernética (PRODANOV; FREITAS, 2013).

8 Foi redigido "a partir de material já publicado, constituído principalmente de: livros, revistas, publicações em periódicos e artigos científicos, boletins, monografias, dissertações" (PRODANOV; FREITAS, 2013, p. 54), além de sítios da Internet.

aspectos, visto que sua proposta é apresentar a visão de um Gestor de Cibernética no processo de inovação de sua área na MB. Contudo, o assunto em tela carece muito de bibliografia, principalmente no que tange aos critérios experiências, tecnologias e capacidade de *hackers*. Isso porque o assunto é tratado com sigilo por Estados e por profissionais do ramo. Sendo assim, as experiências foram buscadas no livro de Richard A. Clarke e Robert K. Knake, disponível para o *Kindle*[9].

As tecnologias foram estudadas em grande parte na monografia do CMG Marco Eugênio Madeira Di Beneditto (2016) e dos trabalhos de Vitor M. S. X. Bizerra e Samuel C. Cruz Jr. (2017). O embasamento doutrinário foi buscado no Manual de Defesa Cibernética do MD, na DMN e no *Navy Cyber Power* 2020. As capacidades foram exploradas e apresentadas mediante aplicação adequada dos conceitos, de Gestão de Pessoas por Competência, pesquisados em livros como o de Maria Rita Miranda Gramigna (2007), dentre outros. Também foram utilizados documentos da Escola Naval (EN), do Exército Brasileiro (EB), uma entrevista feita com a Psicóloga da Escola Nacional de Defesa Cibernética (ENaDCiber) e conceitos de Inovação por meio da Estratégia de CT&I da MB e o conteúdo das aulas do Professor Ricardo Yogui (PUC-RJ). Também se utilizou a experiência da carreira naval, do período trabalhando na ENaDCiber e das contribuições de colaboradores diretos.

Por fim, cabe apontar que além desta introdução, em que se aponta o objeto de estudo, bem como os objetivos, problemas e métodos que guiam esta pesquisa, esta dissertação apresenta outros quatro capítulos. Assim, no capítulo 2 é apresentada a metodologia aplicada na pesquisa. No capítulo 3, explora-se uma base conceitual balizada nos critérios experiências, tecnologias, riscos, possibilidades e capacidades. No capítulo 4, são propostos métodos de inovação da doutrina de guerra cibernética da MB em vigor. Por fim, no capítulo 5, encerra-se o trabalho com uma conclusão que tenta apresentar as concepções e ideias deste autor.

---

9 Aplicativo para compras e leitura de livros da empresa estadunidense "*Amazon*".

2 OS PILARES DA DOUTRINA ATUAL

Não restam dúvidas de que guerra cibernética é um assunto complexo. Não somos, naturalmente, formados para sermos *hackers*[10] e entendermos de programação em Linux[11]. Por isso, nesta pesquisa, não há a pretensão de esgotar o assunto que diz respeito à Guerra Cibernética. Assim, apresenta-se a capacidade de proteção do ciberespaço que demonstra sua complexidade, uma vez que

> […] abrange um grande número de áreas, como a capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional e gestão de pessoal. Compreende, também, a proteção de seus próprios ativos e a capacidade de atuação em rede. (BRASIL, 2012, p. 69)

Segundo Clarke e Knake (2015), o ciberespaço está presente em quaisquer redes de computadores e em todos os periféricos a elas conectadas, ou por elas controlados. Incluem-se a Internet e todas as redes de computadores que não são (ou não deveriam ser) acessíveis por meio da Internet. Para Brasil (2014a), o espaço cibernético é o espaço virtual composto por dispositivos computacionais, conectados em redes ou não, nos quais as informações digitais transitam, são processadas e/ou armazenadas. Contudo, as facilidades trazidas pelo ciberespaço e suas tecnologias são acompanhadas de vulnerabilidades que permeiam todos os ambientes de guerra. Nesse sentido apresentam-se, a seguir, os conceitos mais importantes para melhor compreensão da presente pesquisa.

2.1 Definições

As definições de Segurança e Defesa Cibernética são atribuídas aos níveis de

---

10 O *hacker* autorizado por um Estado para empregar seus conhecimentos em atividades de guerra cibernética é chamado de "Guerreiro Cibernético". Atualmente os *hackers* que operam sem a sanção do Estado são denominados de "Criminosos Cibernéticos". Quando o termo *hacker* for utilizado nesta pesquisa, intencionalmente é deixado em aberto se a ação cibernética foi ou não sancionada por um Estado.

11 Sistema operacional de código fonte aberto que permite a colaboração de programadores voluntários, sendo o principal código de programação utilizado por *hackers* nos dias atuais na versão *PITON*.

decisão Político e Estratégico por Brasil (2014a). Contudo, esta pesquisa trata da "Guerra Cibernética" e, assim, tem enfoque nos níveis de planejamento e decisão Operacional e Tático (BRASIL, 2014a). Nesse sentido, a pesquisa busca ampliar os conhecimentos sobre o campo de estudo de Gestão Cibernética aplicando-os ao campo da Doutrina Cibernética. Por isso, ao longo da pesquisa, o conceito de Guerra Cibernética[12] é respeitado de acordo com a Doutrina Militar de Defesa Cibernética. Porém, cabe apontar que, quando há referências aos termos "Segurança" ou "Defesa Cibernéticas", não há correlação com os níveis de planejamento e decisão Político e Estratégico (BRASIL, 2014a), senão o emprego semântico das palavras "segurança" e "defesa".

No Comando de Defesa Cibernética (ComDCiber), para melhor empregar e especializar os profissionais da área, foram denominados os campos de estudo e emprego da Guerra Cibernética como Proteção, Exploração, Ataque[13], Gestão[14] e Doutrina Cibernética (BRASIL, 2018b).

A DMN descreve Doutrina como: "um conjunto de princípios, conceitos, normas e procedimentos, fundamentado principalmente na **experiência**, destinado a estabelecer linhas de pensamento e a orientar ações, exposto de forma integrada e harmônica" (BRASIL 2017, p. 8, grifo nosso). Descreve, ainda, que as Ações de Guerra Cibernética são "aquelas que

---

12 "[…] corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, 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 (STIC2) do oponente e defender os próprios STIC2. 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, 2014a, p. 19).

13 As definições das ações cibernéticas de proteção, exploração e ataque cibernético podem ser encontradas em Brasil (2014a, p. 23), mas não são foco desta pesquisa. Há um movimento interno no ComDCiber visando a mudança do termo Ataque para Defesa Ativa, tendo em vista a política internacional brasileira de não agressão. Defesa ativa é a Capacidade de identificar o ataque cibernético e sua origem e na mesma medida, se oportuno for retaliar o atacante e seus sistemas com a finalidade de neutralizar o ataque ou exploração cibernética em andamento.

14 O profissional de Gestão Cibernética deve se preocupar com a gestão das seções de guerra cibernética das organizações, com a formação, atualização, adestramento, preparo e emprego dos guerreiros cibernéticos para suas atividades-fim, planejamento e comando de operações de guerra cibernética, gestão de riscos cibernéticos, inovação constante e ampla do setor cibernético e principalmente com a condução das atividades de atualização da Doutrina Cibernética.

envolvem o emprego de ferramentas disponíveis nos campos da Tecnologia da Informação e Comunicações" (BRASIL 2017, p. 57). Desta forma, destaca-se a **tecnologia** como segundo pilar que afeta diretamente o grau de atualização de uma doutrina militar. Por último, mas não menos importante, a **capacitação**, extraída da seguinte passagem, significa que: "uma doutrina racional produz efeitos na reflexão sobre a guerra, no planejamento de força, na instrução e no adestramento" (BRASIL 2017, p. 9, grifo nosso). Esses "pilares" da DMNGCiber atualmente empregados pela MB serão explorados, aproveitando experiências adquiridas pelo autor como gestor de TI, como oficial de comunicações e de operações e como Adjunto na ENaDCiber para conduzir a pesquisa.

2.2 Experiências

Segundo Clarke e Knake (2015), os mais famosos conflitos no ciberespaço – como o ataque cibernético alegadamente atribuído à Rússia contra a Estônia em 2007 – utilizaram-se apenas de técnicas cibernéticas simples, como o ataque de negação de serviços distribuído (DDoS, na sigla em inglês). Para isso, são atribuídas duas razões possíveis: a primeira, por ser possível alcançar o objetivo naquele momento com uma ação simples; e a segunda, e mais aceita, de acordo com Clarke e Knake (2015), é que os atacantes não quiseram revelar suas capacidades mais sofisticadas ou não foram detectados em suas ações.

Cabe ressaltar que os Estados capazes de atuar no espaço cibernético, assim como o Brasil, tratam a capacidade de realizar guerra cibernética como estratégica, conforme pode ser observado na Estratégia Nacional de Defesa (END) e em Brasil (2014a, p. 25): "por ser um dos componentes da Defesa Nacional". Sendo assim, fica patente a dificuldade de encontrar subsídios sólidos sobre experiências na guerra cibernética, visto que a matéria é tratada com sigilo pelos Estados e por *hackers*, fato que não reduz sua importância para o incremento da DMNGCiber.

Clarke e Knake (2015) discorrem sobre o ataque israelense, efetuado em 2007,

contra os sírios. Naquela ocasião, pulsos de luz e elétricos foram utilizados para transmitir códigos binários, a fim de "cegar" os radares de busca e defesa antiaérea sírios. Uma engenhosa combinação tecnológica da guerra eletrônica com a guerra cibernética que possibilitou o efeito surpresa aos israelenses, que, por sua vez, conseguiram atacar seu alvo principal sem anunciar a ação com ataques secundários. Três hipóteses foram apontadas por Clarke e Knake (2015) para o sucesso da missão: sabotagem (um *backdoor*[15] no sistema de combate, ou cavalo de Troia[16], instalado nos computadores); transmissão de códigos por veículo aéreo não tripulado (VANT); ou um acesso físico ao cabo de fibra ótica da rede síria por um agente israelense. Percebe-se, então, que qualquer uma das três hipóteses de Ação de Guerra Cibernética afetaram diretamente a capacidade de guerra antiaérea síria. E, assim como no caso sírio, esse tipo de ataque pode ser empregado contra os radares antiaéreos de forças navais.

Explorando a primeira teoria apresentada por Clarke e Knake (2015), Bizerra (2017) relata que um *malware*[17], espalhado mundialmente em estado "adormecido", afetou apenas o sistema nuclear iraniano, alterando a velocidade dos rotores das usinas ao passo que impedia seu sistema ciberfísico[18] de identificar o ocorrido e reparar a ação. O superaquecimento gerado levou a destruição das plantas de produção. Um exemplo de ação cibernética (virtual) que proporcionou consequências cinéticas[19] (físicas).

Clarke e Knake (2015) relatam que a Rússia conjugou ataques cibernéticos de DDoS em meios de comunicação e sítios do governo da Geórgia com ataques cinéticos a fim

---

15 *Backdoor* é um método não documentado de entrada em sistemas (*software*, plataformas, dispositivos etc.) que pode ser usado de forma legítima por fabricantes para restaurar acessos. Porém, existem ameaças cibernéticas que tentam explorar o mesmo método para dar acesso remoto a um centro de comando e controle externo ao ecossistema invadido, criando uma via permanente para futuras contaminações. Disponível em: <https://www.blockbit.com/pt-br/2017/09/19/como-evitar-backdoors/>. Acesso em 17 maio 2019.

16 Cavalo de Tróia é um tipo de vírus que pretende ser útil ou divertido enquanto na verdade causa problemas e rouba dados. São geralmente espalhados por meio de um anexo de e-mail infectado ou um download que esconde games gratuitos, aplicativos, filmes ou cartões de visita. Disponível em: <https://www.avast.com/pt-br/c-trojan> Acesso em 17 maio 2019.

17 Programa concebido para causar danos ou para aceder ilegalmente a informação em sistemas informáticos. Disponível em: <https://dicionario.priberam.org/malware>. Acesso em 3 abr. 2019.

18 SCF são bem explicados por Beneditto (2016) e são explorados no próximo capítulo desta pesquisa.

19 As Forças Armadas Estadunidenses consideram como cinéticos os ataques realizados ou efeitos causados por ações físicas em decorrência de operações de combate convencionais entre forças.

de expulsar as Forças Armadas georgianas da Ossétia do Sul. Nesse sentido, a Marinha estadunidense vem se preparando para a guerra cibernética, para maximizar seus resultados, por meio da organização e treinamento de uma força de guerreiros cibernéticos, e pelo desenvolvimento de projetos de cooperação e capacidades resilientes do ciberespaço para se contraporem a um adversário no ciberespaço (EUA, 2012).

Por isso, pesquisadores continuam a buscar formas de quebrar códigos e interceptar comunicações. Clarke e Knake (2015) relatam que cientistas suíços, especialistas em computação da Escola Politécnica Federal de Lausana, utilizaram uma antena de rádio para reproduzir teclas digitadas, inspecionando a radiação eletromagnética emitida por elas. Assim, possibilidades como a interceptação de um enlace de dados estabelecido por transceptores a bordo dos navios se mostram cada vez maiores.

Clarke e Knake (2015) e Meserve (2007 *apud* BENEDITTO, 2016) afirmam que *hackers* do *Department of Homeland Security* (DHS) invadiram uma rede de controle de plantas de energia pela Internet e, ao encontrarem o *software* que regulava as velocidades de rotação do gerador, confirmaram a possibilidade de transformar um ataque cibernético em cinético, podendo danificar severamente o gerador.

Neste ponto, é possível trazer a preocupação para o ambiente de guerra naval, pois os geradores podem vir a ser de navios. Outras considerações podem ser discutidas, como a possibilidade de diversão[20], por meio da qual é possível inserir dados errados nas redes operacionais criadas entre navios pelo enlace de dados dos sistemas de combate.

Segundo Schneider (2015 *apud* BENEDITTO, 2016), pesquisadores controlaram um carro em movimento por meio de uma rede de dados de telefonia celular disponibilizada pela central multimídia do veículo. Uma possibilidade de ação no ciberespaço com efeito no espaço físico. Percebe-se então que ações de *hackers* podem fazer com que sistemas se desliguem, se auto danifiquem, danifiquem outras coisas ou enviem navios, aviões e tropas

[20] Tática de combate que visa iludir, despistar ou enganar o oponente.

para lugares errados. Clarke e Knake (2015) citam que, pela experiência adquirida pelo Ex-Diretor Nacional de Inteligência estadunidense, Mike McConnell, nenhuma frota de navios, míssil intercontinental ou exército permanente pode se defender de ataques cibernéticos. Nesse sentido faz-se mister experimentar técnicas de proteção, exploração e ataque para, a partir dos resultados, ser possível definir os procedimentos operacionais de emprego da guerra cibernética. Contudo, para definir os procedimentos operacionais adequados, é preciso conhecer tecnologias e vulnerabilidades que podem ser exploradas por inimigos em potencial; é preciso aprender a mitigá-las e, no futuro, como empregá-las para efetuar ataques e explorações cibernéticas. Ressalta-se que essas ideias são aprofundadas no próximo capítulo.

2.3 Tecnologia

Na introdução desta pesquisa, foi apresentado o conceito de ciberespaço segundo Clarke e Knake (2015) e a partir da Doutrina Militar de Defesa Cibernética (BRASIL, 2014a). Ao ampliar a pesquisa, descobriu-se que a definição de espaço cibernético para a MB é igual à da Doutrina Militar citada. Conforme Brasil (2017a, p. 25), as ações de guerra cibernética visam "desestabilizar os ativos de informação do inimigo" e "possibilitar a proteção dos ativos de informação de interesse".

Beneditto (2016) demonstra sua preocupação com a segurança cibernética dos Sistemas Ciberfísicos (SCF)[21], citando que tanto Brasil (2014a) quanto Brasil (2017a) não consideram as ações cibernéticas atuando em processos físicos. Essas definições consideram apenas resultados "virtuais", ou seja, que se desenvolvem dentro do ciberespaço, sobre dados e informações, sem afetarem o "mundo físico", afligindo a percepção de que os SCF também devam ser protegidos. Alves (2019) e Bizerra (2017) concordam com Beneditto (2016). O

[21] SCF são sistemas que permitem o controle de processos físicos por meio de redes de computadores, empregando sensores de aquisição de dados e atuadores que realizam as ações de controle determinadas pela rede de computadores (BENEDITTO, 2016).

segundo, mais especificamente, ao afirmar que o espaço cibernético é o ambiente capaz de sediar conflito de consequências idênticas às de uma guerra convencional. Em outras palavras, ambos acreditam no potencial de geração de danos físicos por meio da arma cibernética. Assim, este capítulo visa ampliar o conceito por meio de comentários acerca das tecnologias de interesse da MB e suas possíveis vulnerabilidades cibernéticas.

2.3.1 Sistemas Ciberfísicos e Sistemas de Combate

Para Clarke e Knake (2015), estão no contexto do ciberespaço as redes de computadores que servem de sistemas de controle e comunicações de máquinas, ainda que não exista troca de informações à distância, por Internet, rádio ou conexão física, como os sistemas de controle digital que monitoram atividades e acionam comandos para motores, válvulas, interruptores, dentre outros. Nesse sentido, os SCF embarcados se tornam alvos de interesse no ambiente de guerra cibernética. Segundo Beneditto (2016), um ataque cibernético a um SCF envolve o aproveitamento pelo *hacker* de uma vulnerabilidade, que terá como consequência um efeito no espaço físico, ou seja, transformará ações virtuais em cinéticas e pode, por exemplo, parar a propulsão ou a geração de energia de um navio.

Segundo Clarke e Knake (2015), um *hacker* pode derrubar um sistema SCADA[22], o que pode preocupar a MB pois seus navios possuem sistemas de controle SCADA e semelhantes, como o Sistema de Controle e Monitoração da Propulsão e Auxiliares das Fragatas da Classe Niterói (SCMPA) das Fragatas da Classe Niterói (FCN). Sendo assim, questiona-se o porquê de sua utilização uma vez que são tão vulneráveis. Segundo Nakamura e Geus (2002), os benefícios trazidos pela TI resultam em eficiência. Beneditto (2016) concorda, explicando que eles permitem ganhos de desempenho e a possibilidade de redução de pessoal empregado nas tarefas de monitoramento e controle, como atualmente é observado na MB.

---

[22] Sistema SCADA é o *software* que controla redes, como o de energia elétrica.

Cita-se, como exemplo de SCF, o SCMPA, desenvolvido pelo Centro Tecnológico da Marinha em São Paulo (CTMSP), e acrescenta-se o Sistema de Controle e Monitoração das Corvetas da Classe Inhaúma (SCM), desenvolvido pelo Instituto de Pesquisas da Marinha (IPqM), além do Sistema da Corveta Classe Barroso e, nesse sentido, os futuros Escoltas Classe Tamandaré seguirão a tendência. Segundo Brasil (2019b), as Corvetas Classe Tamandaré foram selecionadas com base em 2 instrumentos basilares para a tomada de decisão: Análise Multicritério à Decisão (AMD) e Análise de Riscos, que analisaram, dentre outros, os Sistemas de Combate, Comunicações e Tecnologia da Informação, preocupando-se com a transferência de Tecnologia. Portanto, são consideradas aqui algumas preocupações, pois, ao não haver tecnologia nacional corre-se o risco de que sistemas com vulnerabilidades projetadas sejam recebidos, como *backdoors* físicas e lógicas.

Corroborando a preocupação de Beneditto (2016), percebe-se que os estadunidenses já identificaram a importância e vulnerabilidade de seus SCF, Sistemas de Combate, dentre outros, ao definirem o ciberespaço como de alcance completo dentro do ambiente de informação, composto por todas as redes e infraestruturas de TI (EUA, 2012). Ao incluírem os controladores incorporados aos sistemas de computador, estão claramente assumindo a vulnerabilidade de seus SCF e Sistemas de Combate. Por isso, Clarke e Knake (2015) afirmam que a China está desenvolvendo capacidades cibernéticas “navais” para que sua força naval obtenha vantagem tática sobre a marinha estadunidense haja vista a inferioridade bélica chinesa.

Os Sistemas de Combate, como SICONTA das FCN e da Corveta Classe Barroso (CCB) e, como o CAAIS 400 e 450 das Fragatas Classe Greenhalgh (FCG) e Corvetas Classe Inhaúma (CCI) operam interconectados por meio do enlace de dados por radiofrequência (Link YB). Esses sistemas não estão interconectados a outras redes ou sistemas por meio da Internet, mas eventualmente podem ser conectados a ela ou à rede interna do navio, quer por manutenção, quer por acidente. Outro “caminho” é a infecção desses sistemas por meio de mídias removíveis contaminadas (*pendriver* por exemplo). Também há a possibilidade dos

sistemas nacionais estarem submetidos a falhas de programação (intencionais ou não) que podem ser acionadas por tecnologias ainda desconhecidas. Os ataques cibernéticos sofridos por esses sistemas podem resultar em diversão, confusão ou má compilação do quadro tático. É possível, inclusive, efeitos físicos, como lançamento ou explosão de armamentos e inoperância ou mal funcionamento dos mesmos. Os estadunidenses se preocupam diretamente com isso, pois um de seus principais armamentos o *Tomahawk* Tático depende de informações provenientes do ciberespaço para atualização de informações de voo e alvo (EUA, 2012).

Clarke e Knake (2015) comentam o artigo da revista *Time* que aborda a exploração de técnicas complicadas e ações geopolíticas relacionadas ao ciberespaço pelos estadunidenses muito antes de outros governos entenderem qualquer coisa sobre guerra cibernética. A reportagem expõe o "programa clandestino" para inserir *backdoors* físicas em artefatos de computadores de Sistemas de Combate de fabricantes de Estados potencialmente hostis, definido pelos autores como técnica de *chipping*. Clarke e Knake (2015) também demonstram que o Sistema Operacional Windows possui milhões de linhas de código e que em cada versão lançada elas aumentam. Com isso, cresce o número de erros de programação, criando *backdoors* lógicas.

Nesse sentido, Beneditto (2016) se preocupa com a cadeia de erros hereditários da linha de *softwares* empregada nos Sistemas de Combate da Marinha, como o SICONTA, que nas FCN é a versão II, enquanto na CCB é a III. O próprio CAAIS 400 foi propriedade dos britânicos que, por sua vez, conhecem suas vulnerabilidades ou podem ter feito *chipping* antes de entregar as FCG ao Brasil. Falliere, Murchu e Chien (2011 *apud* CRUZ JR, 2013), também citam a possibilidade de vazamento de vulnerabilidades *zeroday*[23] do sistema de controle e aquisição de dados SCADA, que tornaram possível o sucesso do *malware* Stuxnet. Portanto, além de ser necessária a proteção cibernética de SCF e Sistemas de Combate nacionais, também é mister incrementar a própria capacidade de exploração e ataque

[23] Uma nova vulnerabilidade que ainda não conta com pacotes de revisões e pode ser explorada para realização de um ataque.

cibernéticos, para obter vantagem tática no enfrentamento de forças de maior poder combatente.

Nesta seção, buscou-se apresentar as possibilidades e vulnerabilidades a que estão submetidos os SCF e os Sistemas de Combate e que os efeitos decorrentes de uma falha nesses sistemas podem causar danos físicos em um navio. Como visto, há uma preocupação quanto à interpretação da alta administração naval em relação ao emprego da guerra cibernética, pois os possíveis efeitos cinéticos da guerra cibernética sobre os SCF e Sistemas de Combate ainda não são considerados. Contudo, há uma grande preocupação em prover segurança cibernética aos sistemas de comunicações satelitais e à intranet da MB.

2.3.2 Sistemas de comunicações

Beneditto (2016) comenta que os sistemas de um meio naval podem ser substituídos ou removidos. Equipamentos novos podem trazer novas vulnerabilidades, intencionais, por falhas de projeto ou má instalação. Clarke e Knake (2015) citam alguns exemplos de equipamentos que possuem comunicação com seus fabricantes, como o exemplo da fotocopiadora para resolver problemas e atualizar seu *framework*[24]. Citam, ainda, casos de espionagem em que trituradores de papel fotografam documentos antes de picotá-los. Nesse sentido, Beneditto (2016) demonstra sua preocupação com os sistemas de comunicações satelitais empregados pela MB, como as antenas das bandas Ku, Ka e X que podiam ser remotamente controladas e monitoradas pelo fabricante ou por quem invadir sua rede de Internet. No caso das bandas acima, utilizadas pela MB, a Internet é provida à rede interna dos navios por meio da rede privada virtual da MB, que pode ser invadida. Uma forma conhecida desse tipo de ataque é comentada por Clarke e Knake (2015) como “erro humano”. Esses autores afirmam que redes que não deveriam estar conectadas à Internet pública muitas vezes estão conectadas sem o conhecimento de seus proprietários, por erro ou

[24] Um conjunto de técnicas, ferramentas ou conceitos pré-definidos usados para resolver um problema de um projeto ou domínio específico.

intencionalmente.

Beneditto (2016) aponta três motivos que possibilitam a guerra cibernética: o primeiro, falhas de projeto da Internet; o segundo, falhas de *hardware* e *software*; e o terceiro, a interconexão dos SCF com redes de computadores de monitoramento remoto por meio da Internet. Clarke e Knake (2015) acrescentam que pessoas erram ou negligenciam, criando oportunidades. Como visto anteriormente, no exemplo citado por Clarke e Knake (2015) do ataque israelense à Síria, uma das ferramentas que possibilitou o sucesso do ataque cibernético pode ter sido sabotagem, possivelmente o quinto motivo. Existem certamente várias outras formas que ainda não foram reveladas pelos *hackers*, porém, para efeito desta pesquisa, mais importante do que saber como fazem, é saber qual impacto eles podem conseguir. No caso dos SCF, Beneditto (2016) e Clarke e Knake (2015) demonstram bem como é possível transferir a ação cibernética para a cinética. Já nos sistemas de comunicações, prevalece a percepção naval brasileira e o senso empresarial comum sobre a possibilidade de roubo e comprometimento de informações e conhecimentos:

> [...] as informações atravessam fronteiras com velocidade espantosa, a proteção do conhecimento é de vital importância para a sobrevivência das organizações. Uma falha, uma comunicação com informações falsas ou um roubo ou fraude de informações podem trazer graves consequências para organização, como perda de mercado, de negócios e, consequentemente, perdas financeiras (NAKAMURA; GEUS, 2002, p. 28).

O roubo de informações sigilosas, como planos de batalha com suas tabelas de autenticação, pode proporcionar a inserção posterior de informações e ordens falsas, devidamente autenticadas, criando diversão em uma força naval por completo, utilizando ou não a Internet. Observa-se um transceptor de comunicações que opera na faixa de frequências de VHF, por meio de IP[25], para estabelecimento de enlace automático de dados (EAD) táticos ou rede tática de dados (RTD). Havendo IP, um *hacker* que opere na mesma faixa de frequência pode invadir o EAD ou RTD e tramitar informações que induzam ao erro de

[25] *Internet Protocol* (Protocolo de Internet).

interpretação, assim como falsos contatos no sistema de combate da força naval. Como os navios de guerra operam em EAD para compartilhamento de contatos detectados por radares e outros sensores, pode-se imaginar o quão fácil seria desviar um GT[26] por completo da direção desejada. Da mesma maneira, o protótipo do Rádio Definido por *Software* de Defesa (RDS-Defesa[27]) opera no ciberespaço[28], estando submetido à exploração e ataques cibernéticos, sobre suas falhas em *hardware*, *software* ou humana.

Guimarães e Grivet (2003) comprovam em sua publicação a possibilidade de geolocalizar terminais de comunicações móveis. Nesse sentido, pode-se apontar a preocupação apreciada em decorrência do resultado de uma experiência realizada, em parceria com a ANATEL, pelo então Chefe de Operações da Estação Rádio da Marinha do Rio de Janeiro em 2017. Mostrou-se ser possível geolocalizar um terminal móvel satelital em funcionamento a bordo de um navio de guerra navegando no rio Amazonas, por meio do monitoramento da Radio Frequência transmitida pelo satélite para o navio que esteja operando dentro do mesmo *footprint*[29] da estação de controle e monitoramento. Isso demonstra que um *hacker* com acesso à rede de operação da estação terrena de controle do satélite poderá ter acesso à posição dos navios que trafegam dados com eles.

Beneditto (2016) e Clarke e Knake (2015) citam a integração das tecnologias embarcadas, como Sistemas de Comunicações, de TI, de SCF e de Combate para possibilitar melhores desempenhos operacionais e fontes de informações mais confiáveis para a tomada de decisões. Os militares estadunidenses são incapazes de operar sem Internet, pois toda logística, comando e controle, posicionamento de frota, compartilhamento de dados táticos entre unidades e ataques a alvos está baseada em TI e Internet, bastando uma falha humana ou um roteador mal protegido para que *hackers* entrem na rede militar para conseguirem vantagem tática em combate (CLARKE, KNAKE, 2015). Essa interconectividade de sistemas traz

---

26 Acrônimo de Grupo-Tarefa: Organização tática de navios de guerra, em uma mesma missão de combate.

27 Sendo desenvolvido no Centro Tecnológico do EB (CTEx) em parceria com a MB (DCTIM, IPqM, CASNAV e CTIM).

28 Em VHF, protocolo IP, ou STANAG-5066, mesmo utilizado pelo Datronlink, Gateway-HF ainda em uso pela MB.

29 Área de cobertura de um satélite.

vantagens e desvantagens, sob a forma do Paradoxo Tecnológico[30] que traz a necessidade de proteção cibernética, mas também abre a oportunidade para que ataques cibernéticos sejam efetuados por meio da exploração das vulnerabilidades de forças navais de maior poderio combatente.

2.3.3 Mitigação de vulnerabilidades

A mitigação de vulnerabilidades é um requisito para manutenção da segurança cibernética nacional e para se opor a possíveis ataques cibernéticos. Nesse sentido, a Política Nacional de Defesa (PND) considera "essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade" (PND, 2005, p. 9)31 dos sistemas que empreguem tecnologia da informação e comunicações (TIC).

Dessa forma, Beneditto (2016) ensina que o ciberespaço, onde os SCF, os Sistemas de Combate e os Sistemas de Comunicações e TI estão contidos, é ampliado com o passar do tempo devido à necessidade crescente de informações para a tomada de decisão. De maneira simplificada, os sistemas se tornam cada vez mais integrados entre si e, possivelmente, também com a Internet. Dessa maneira estudam e planejam os estadunidenses, buscando identificar as vulnerabilidades latentes e prevendo as possibilidades futuras de ameaças para os sistemas da Marinha estadunidense: "Praticamente todos os principais sistemas em navios, aeronaves, submarinos e veículos não tripulados estão conectados em rede em algum grau[32]" (EUA, 2012, p. 7, tradução nossa). Com o intuito de aumentar a eficiência e o desempenho operacional em algum quesito. Conforme ensinado por Beneditto (2016),

---

30 "[…] quanto mais tecnologicamente desenvolvido estiver um sistema, mais dependente da TI estará e consequentemente mais vulnerável às ações cibernéticas. Contudo, paradoxalmente, este mesmo oponente possuirá mais condições de se defender dos ataques cibernéticos, em virtude de seu alto grau de desenvolvimento tecnológico." (BRASIL, 2014a, p. 21)

31 Decreto Nº. 5484, de 30 de Junho de 2005. Disponível em: <https://www.defesa.gov.br/arquivos/2012/mes07/ pnd.pdf>. Acesso em 17 maio 2019.

32 "Practically all major systems on ships, aircraft, submarines, and unmanned vehicles are "networked" to some degree."

esses sistemas tornam-se ainda mais vulneráveis. Nesse sentido, o Gestor de Guerra Cibernética deve constantemente realizar exercícios reais e mentais, buscando identificar e encontrar vulnerabilidades e propor soluções para eliminar os riscos crescentes e modificar a DMNGCiber para que seu emprego operacional seja eficaz para a operação.

Beneditto (2016) afirma que projetistas devem coibir a criação indesejada de vulnerabilidades durante a concepção do produto e cita Baybutt (2004 *apud* BENEDITTO, 2016), que menciona a necessidade de implantação de processos de gerenciamento de riscos para SCF. Alves (2019) afirma também que os desenvolvedores devem buscar a solução em algoritmos de proteção com regras de correlação aplicadas aos bancos de dados. Neste ponto, ousa-se ampliar as preocupações para todos os sistemas.

Segundo Nakamura e Geus (2002), a segurança da informação deve ter independência total para atuar e, segundo Alves (2019), o conhecimento é uma vantagem importante para a defesa, a ser efetuada por pessoas capacitadas para proteção cibernética. Nesse sentido, considera-se que, além dos desenvolvedores, é preciso pensar na possibilidade de empregar consoles para Operadores de Guerra Cibernética monitorarem os SCF, Sistemas de Combate e de Comunicações, durante as operações, a fim de possibilitar a proteção cibernética em curso e, quando viável, realizar explorações e ataques cibernéticos.

Beneditto (2016) menciona que, a longo prazo, um programa sistemático de gerenciamento de riscos permita acumulação de conhecimentos de requisitos de segurança para futuros navios e sistemas. Nessa passagem, o autor claramente se preocupa com o planejamento de segurança desde o projeto do meio naval. Em seu trabalho, compara segurança cibernética com algo físico, que deve ser planejado e que se degrada ao longo do tempo. Contudo, não menciona a segurança no curso das operações e tampouco a proteção cibernética a ser realizada por guerreiros cibernéticos. Essa lacuna permite que esta pesquisa foque na importância de desenvolvermos capacidades próprias de guerra cibernética pelos militares combatentes[33] da MB.

[33] Terminologia usada no EB para distinguir militares das especialidades operacionais (Infantaria, por

Segundo Pagliusi (2017), para alcançar a maturidade da gestão de riscos, não é necessário investir tanto em tecnologia, mas sim em pessoas e processos, adotando um modelo de sistema resiliente, capaz de conter os danos causados por um ataque cibernético; seguro, com dispositivos adequados de segurança da informação; e "vigilante: com capacidade de detecção proativa, inteligência e consciência situacional sobre ameaças cibernéticas" (PAGLIUSI, 2017, p. 23). Nesse sentido, Nakamura e Geus (2002) afirmam que os sistemas de detecção de intrusão, em sua maioria, detectam ataques que ocorreram, mas normalmente não podem evitar o ataque. Para que isso seja possível ou, pelo menos, para mitigar seus efeitos, faz-se necessária a operação em consoles próprios para proteção cibernética dos Sistemas, com capacidade de alteração de parâmetros de programação e configuração de portas lógicas, dentre outras técnicas específicas. Por fim, para cada sistema, um operador especializado na linguagem de programação específica e devidamente capacitado para a ação cibernética que se fizer necessária.

Clarke e Knake (2015) citam o programa de varredura de tráfego estadunidense "Einstein", que, à época da elaboração do livro, havia evoluído até segunda versão, a qual é capaz, além de procurar por *malwares*, de detectar intrusões. Sua terceira versão, também à época do livro, incorporaria a capacidade bloquear pacotes maliciosos. A versão estadunidense atual pode ter evoluído ainda mais e, nesse mesmo sentido, a MB vem trabalhando com o sistema *Dreadnought*, que já possui essas capacidades. Segundo Clarke e Knake (2015), *hackers* bem capacitados dificilmente são impedidos de invadir um sistema ou rede, mesmo que seus operadores acreditem que eles não estão conectados à Internet. É importante ressaltar que quando, nesta pesquisa, é feita referência a uma capacidade humana de burlar regras e sistemas, acredita-se na ideia de que nada é melhor para se contrapor a um *hacker* do que um guerreiro cibernético bem treinado em proteção cibernética.

Nakamura e Geus (2002) muito referenciam a necessidade de investimento em

exemplo) das de apoio e técnicas (engenheiros militares, por exemplo). No caso da MB, Armada e Fuzileiros Navais.

sistemas criptográficos, em se tratando de Sistemas de Comunicações e TI. A questão levantada por Beneditto (2016) é carência de preocupação com os SCF, e, a ela, acrescenta-se a preocupação com gestão de riscos dos Sistemas de Combate. Quanto ao Sistemas de Comunicações e TI, a Doutrina de Tecnologia da Informação da Marinha (EMA-416) é bem completa, mas não abrange a capacidade operacional de realizar proteção cibernética dos sistemas.

Uma boa maneira de reduzirmos as vulnerabilidades nacionais seria o desenvolvimento e integração nacional dos Sistemas utilizados a bordo, assim como orienta Amorim (2013, p. 308): "[...] hoje o desenvolvimento de capacidades autônomas na indústria de defesa é um objetivo fundamental de nossa política." Contudo, segundo Cruz Jr. (2013), o Brasil ainda conta com um pequeno parque empresarial de desenvolvimento de soluções robustas em segurança ou defesa cibernética. Um Gestor de Guerra Cibernética deve buscar soluções inovadoras para aumentar suas capacidades e, nesse sentido, o modelo "tríplice hélice"[34] deve ser melhor aproveitado pela MB para o desenvolvimento das capacidades de guerra cibernética, no que se refere a tecnologias e capacitação, principalmente em conjunto com o polo tecnológico de Santa Catarina e de São Paulo, coadunando com a filosofia estratégica da MB para P&D e C&TI: "[…] lançando-se mão, quando necessário, dos demais integrantes da "Tríplice Hélice", composta pela Academia, Governo e a Base Industrial de Defesa (BID)." (BRASIL, 2017b, p. 29)

Principalmente no caso de um Estado que não produza seus próprios sensores e equipamentos de comunicação, há a necessidade de possuir a capacidade de proteção cibernética, pois os equipamentos podem ser fornecidos com *backdoors* lógicas. Mesmo que o Estado produza os sensores, ele não está isento de sofrer intervenção por espionagem, carecendo de constate gestão de riscos a ser realizada pelos Gestores de Guerra Cibernética. Clarke e Knake (2015) relatam a preocupação estadunidense com a possibilidade de uma

[34] "O modelo de Tríplice Hélice foi desenvolvido por Henry Etzkovitz na década de 90, sendo hoje uma das metáforas mais populares e aceitas para explicar a capacidade de transformar o conhecimento científico em inovação tecnológica." (BRASIL, 2017b, p .29)

suposta disposição de “bombas-lógicas” em suas redes elétricas, instaladas por russos ou chineses. Relatam, ainda, que a venda de roteadores cisco produzidos na China com *backdoors* para derrubar redes e enfraquecer sistemas criptográficos (CLARKE; KNAKE, 2015). Ao observar-se o Programa de Defesa Cibernética do EB, pode-se constatar a preocupação daquela Força quanto ao estabelecimento de um Sistema de Certificação e Homologação de Produtos de Defesa Cibernética (BRASIL, 2014b). Nesse sentido, considera-se a importância de pensar em algo semelhante para os sistemas embarcados nacionais, da mesma forma para os *softwares* utilizados, como o Sistema Operacional Linux por exemplo. Há *startups*, no polo tecnológico de Santa Catarina, desenvolvendo sistemas operacionais seguros, o que pode vir a ser interessante para os sistemas operacionais dos Sistemas de Combate, TI e SCF.

Como visto, boa parte do conhecimento é gerenciada por sistemas que envolvem TI e, de acordo com Alves (2019), as evoluções tecnológicas, drones, carros e navios autônomos, grandes plantas de geração de energia, como hidrelétricas e nucleares mais recentes, além de sistemas de combate, comunicações e SCF começam a depender da TI e da Internet, não estando livres das possíveis falhas humanas. Assim, depara-se com a necessidade de possuir tecnologia adequada para contribuir para o cumprimento da missão naval, corroborando com a visão de futuro[35] da MB de se tornar uma Força moderna, equilibrada e balanceada.

Para alcançar, nacionalmente, o equilíbrio tecnológico e o nível de modernidade almejados, é preciso balancear o Paradoxo Tecnológico, incrementar as capacidades de realizar guerra cibernética e dimensionar as tropas de Guerra Cibernética a altura da MB e suas necessidades operacionais. Nesse sentido, Takemura, Osajima e Kawano (2009 *apud* CRUZ JR, 2013) citam que a proteção cibernética depende muito mais da capacitação de pessoas que de investimentos em equipamentos. Clarke e Knake (2015) afirmam que a Coreia do Norte não

[35] Disponível em: <https://www.marinha.mil.br/content/o-que-compete-marinha-do-brasil>. Acesso em 06 abr. 2019.

investiu muito no desenvolvimento de uma infraestrutura interna de Internet, mas massificou a capacitação de seus profissionais. Estima-se que sua Unidade Conjunta de Guerra Cibernética tenha mais de seiscentos *hackers* capacitados. Essa ideia considera que não adianta ter tecnologia sem saber empregá-la de forma adequada e com segurança. Portanto, o foco da política naval de emprego da guerra cibernética deve ser no treinamento e formação de pessoal.

Assim, apresenta-se a MB as recomendações de Hamel e Prahalad (1995): além de avaliar os processos internos, os desafios e as ameaças externas que tem influência sobre a instituição, para uma organização manter-se atuante e no estado da arte, também se faz necessário identificar as competências críticas indispensáveis que são objeto da próxima seção.

2.4 Capacidades

Uma das responsabilidades do Oficial Gestor de Guerra Cibernética é prover a capacitação dos guerreiros cibernéticos, zelar pela manutenção desta capacidade e posteriormente desenvolver os mais aptos para as funções de exploração e ataque cibernéticos. Bizerra (2017), em seu estudo sobre o Canadá, chegou à conclusão da existência de um consenso no cenário cibernético de que a segurança cibernética é muito mais dependente da qualificação pessoal do que da tecnologia. Esse consenso também pode ser observado por meio da leitura dos estudos de Cruz Jr (2013) e da obra de Clarke e Knake (2015).

Assim, Pacheco et al. (2009) ensinam que as organizações precisam se adaptar às exigências internas e externas, não bastando apenas incorporar novas tecnologias ou sistemas. Assim, é necessário investir na ampliação das competências individuais de seu pessoal. Nesse sentido, Beneditto (2016) cita a importância de capacitar profissionais, formando grupos de especialistas envolvendo pessoal de centros de manutenção e diretorias especializadas, além de pessoal do setor operativo, com conhecimento sobre todos os sistemas e sobre o domínio cibernético.

Após examinar EUA (2012), concorda-se com Cruz Jr (2013) em sua assertiva:

"segurança e defesa cibernética dependem muito mais da capacitação de pessoas, ou capacidade intelectual, que de produtos e equipamentos." (CRUZ JR, 2013, p. 18). Assim, pode-se considerar a capacitação em guerra cibernética como prioridade, ainda que a MB não detenha tecnologias avançadas para realização de explorações e ataques cibernéticos contra alvos de interesse.

Desse modo, é aplicada nesta pesquisa a base teórica da Gestão de Pessoas por Competências para demonstrar a importância da capacitação no ramo da guerra cibernética. Para tratar sobre as capacidades cibernéticas, busca-se fomentar a importância da "adequação das competências requeridas dos servidores aos objetivos das instituições" (BRASIL, 2006a, Art 1º-Alínea III), corroborando com o que é ensinado por Gramigna (2007), que afirma que a GPC possui vantagens como: a clara definição dos perfis profissionais que permitam o incremento da produtividade e o objetivo focal no desenvolvimento de equipes de profissionais que atendam às necessidades da organização, respeitando o perfil de seus funcionários. Valorizar a formação de um capital intelectual na organização, definir claramente os perfis profissionais que possam favorecer à elevação da produtividade, melhorar a definição dos programas de treinamento e desenvolvimento, de acordo com as necessidades da organização e priorizar os investimentos em capacitação também são vantagens facilmente observadas na utilização desse modelo de gestão (GRAMIGNA, 2007).

2.4.1 Competências individuais e o seu *gap* para ações de guerra cibernética na MB

Para o propósito desta pesquisa, são enfatizadas as competências[36] individuais para o emprego operacional de militares em ações de guerra cibernética, apesar do problema apontado na Introdução estar diretamente relacionado com a carência de competência organizacional da MB para a guerra cibernética. Nesta seção, pretende-se demonstrar que o investimento em capacitação individual dos militares da MB promoverá a médio e longo prazo

[36] Classificadas como individuais, profissionais, por equipe e organizacionais. (CARBONE, 2016)

o desenvolvimento de competências organizacionais de guerra cibernética necessários a MB.

Na visão de Gramigna (2007), ter competência significa apresentar conhecimentos, habilidades e atitudes (CHA) compatíveis com o nível de desempenho exigido, assim como colocar em prática sua experiência, sempre que for necessário. Os conhecimentos são informações adquiridas e interpretadas pelo profissional, sejam elas obtidas em instituições de ensino, nos livros, no trabalho ou na prática. Trata-se do "saber o que fazer", se transformando em competência quando é materializado (LEME, 2008); as habilidades se referem à aptidão, às capacidades técnicas e à destreza, sendo orientadas para a aplicação prática do conhecimento, o "saber como fazer" algo concreto (LEME, 2008); e as atitudes são afetas ao comportamento do profissional enquanto operando seus conhecimentos e habilidades, o comprometimento, a motivação e o interesse, "o querer fazer" (GRAMIGNA, 2007). As habilidades e atitudes serão exploradas adiante pela apresentação de um possível processo de seleção dos profissionais de guerra cibernética com base nessas características para que, posteriormente, capacitem-se e desenvolvam-se[37] os mais aptos.

Assim, para realizar ações de guerra cibernética será necessário alcançar um conjunto de competências individuais que se traduzirão na competência organizacional da MB adequada para a guerra cibernética. Será preciso selecionar os mais aptos para a realização de ações de guerra cibernética, avaliando o perfil dos candidatos, dando a capacitação básica para formação da massa crítica, bem como valorizando e motivando os profissionais selecionados para desempenhar essas ações.

Para entender o problema, é preciso ter em mente que para realizar guerra cibernética é necessário ter diversas competências individuais para permitir "o emprego de ferramentas disponíveis nos campos da Tecnologia da Informação e Comunicações" (BRASIL, 2017a, p. 25). As competências necessárias (o saber o que fazer) são estudadas ainda neste capítulo, mas para dar prosseguimento ao estudo do problema em questão, a redução do *gap* de competências em guerra cibernética, consideraram-se as duas propostas de Orlean e

[37] Capacita-se para o cargo atual e desenvolve-se para as funções e cargos futuros. (GRAMIGNA, 2007)

Ferreira (2005), quais sejam: a captação ou o desenvolvimento de competências internas[38].

Ao longo da pesquisa, foi possível perceber as possibilidades de emprego de técnicas de guerra cibernética contra navios de guerra, o que aponta para a necessidade de possuir militares adequadamente qualificados e servindo embarcados. Conforme pode-se verificar no Aviso de Convocação 05/2017[39] do Comando do 1º Distrito Naval, constata-se que a MB sente grande necessidade de contratar militares temporários da área técnica de Informática para reduzir o *gap* de competência no campo de TI. Esta evidência junto à análise de Brasil (2018a), que demonstra a baixa carga horária de ensino de TI para os Aspirantes da EN, confirmam a existência do *gap*[40] existente em guerra cibernética, pois o simples fato de não possuir profissionais capacitados em TI é uma vulnerabilidade para condução das atividades navais, mitigando riscos cibernéticos.

Quanto à captação de oficiais temporários, as vantagens trazidas pela diversificação das correntes de pensamentos, ideias, práticas e visões profissionais são visíveis e importantes para a evolução da MB, contudo as desvantagens também são impactantes, como a frustração do profissional concursado quanto à redução das possibilidades de engrandecimento profissional e a insegurança trazida para a organização, que no âmbito da contrainteligência[41] estão relacionadas ao acesso aos ativos de informação mais valiosos, restritos e sigilosos por profissionais sem histórico naval conhecido. Estes riscos não são observados em oficiais concursados, pois seu perfil e padrões comportamentais já são conhecidos e acompanhados. Por outro lado, a vantagem das novas visões e ideias talvez não sejam obtidas.

Para reduzir o *gap* e os riscos pode-se aumentar as vagas para militares concursados do Quadro Técnico na área de TI. Contudo, tal alternativa, independentemente das vantagens e desvantagens, requer a redução de vagas para outras especialidades, visto que o

---

38 Para efeito deste trabalho, este autor refere-se a este conceito como "capacitação".

39 Disponível em: <https://www.concursovirtual.com.br/admin/links/74616_marinha_2017.pdf >.

40 "*Gaps* (ou lacunas) são as diferenças existentes entre o padrão ideal desejado pela Empresa para cada Competência identificada nos vários processos e o grau de intensidade (domínio/proficiência) de uso da Competência por parte do empregado." (SILVA, 2005, p. 100)

41 Ramo da inteligência que se preocupa com salvaguarda das informações sigilosas de uma organização.

Comandante da Marinha determinou[42] a redução do efetivo de militares de carreira, implementando o uso da força de trabalho de militares temporários e da reserva remunerada. Outro fator limitador seria o despreparo do Quadro Técnico para o embarque em navios de guerra e para o desempenho das atividades de operações navais. A política de pessoal da MB não permite a inclusão desse Quadro nas tabelas de lotação dos navios.

Importante esclarecer que se concorda, aqui, com a eficácia de ambos os métodos expostos para preenchimento do *gap* de competências, quando considerado o seu emprego no ambiente terrestre, já nos navios os oficiais da Armada não podem ser substituídos por outra profissão. Seria possível ainda pensar em outra forma de recrutamento de pessoal já capacitado em TI diretamente para a Escola Naval. Contudo esta solução não é considerada neste trabalho. Sendo assim, por exclusão das alternativas relacionadas à captação e pelas nuances apresentadas, depreende-se que há necessidade de capacitar oficiais da Armada para ações de guerra cibernética.

2.4.2 A capacitação do oficial da Armada

A guerra cibernética, em toda sua complexidade, permeia todos os outros ambientes de guerra, possui diversas possibilidades de emprego e utiliza diversas linguagens de programação, técnicas, além de requerer diversos cuidados. Os conhecimentos são complexos e amplos e, para continuar estudando o porquê da necessidade de qualificar o oficial da Armada, apresenta-se, a seguir, a estratégia estadunidense para a capacitação de todo o pessoal de sua Marinha: "[…] um treinamento cibernético abrangente e modelo de educação que pode se adaptar rapidamente à indústria, avanços e evolução das necessidades do Comandante Conjunto[43]." (EUA, 2012, p. 12, tradução nossa)

Então, constata-se que a preocupação estadunidense é com a implementação de um

---

42 Memorando nº2 de 2017 do Comandante da Marinha.

43 "[…] a comprehensive cyber training and education model that can rapidly adapt to industry advances and evolving joint commander needs." (EUA, 2012, p.12)

processo de capacitação completo, com a massificação do conhecimento básico para todos os militares, treinamento de seus Gestores de Cibernética e, principalmente, com a formação de guerreiros cibernéticos. Além de preverem a atuação de seus militares no com *Us Cyber Command*[44], os Gestores de Cibernética do Brasil são os Oficiais da Armada, que, a bordo dos navios, também poderão realizar a proteção cibernética dos sistemas embarcados. Os mesmos oficiais poderão ser designados para trabalhar no ComDCiber.

A TI é uma ciência volátil que se aperfeiçoa e evolui rapidamente, criando sempre novas técnicas e possibilidades. Nesse sentido, Bayma (2005) sugere políticas de pessoal que privilegiem o desenvolvimento de competências, propiciando educação continuada dentro da própria instituição. Quando a necessidade estratégica da instituição requer capacitação em assuntos complexos, como é o caso da guerra cibernética, Pacheco et al. (2009) afirmam que estágios não são suficientes para assimilar os conhecimentos necessários de forma completa. Milkovich e Boudreau (2000) também afirmam que treinamentos ou estágios, por serem de curta duração, não são suficientes para contemplar todo o arcabouço teórico e técnico de um conteúdo mais complexo, requerendo, assim, o desenvolvimento de competências dentro da própria instituição.

Portanto, para possibilitar a capacitação necessária em guerra cibernética, é preciso adotar um método de desenvolvimento mais completo, abrangente e de longo prazo destinado a habilitar o indivíduo não somente com as qualificações cibernéticas, mas também com os conhecimentos requeridos em operações navais e navegação, dentre outros necessários para o serviço embarcado. Ao assumir a complexidade do assunto, percebe-se a importância de selecionar militares que estejam em início da carreira, ainda na Escola Naval, de forma a possibilitar o máximo de conhecimento e aperfeiçoamento em guerra cibernética, alinhando-se com os objetivos estratégicos da Instituição.

Como visto, a guerra cibernética, por ser capaz de afetar às missões dos navios de guerra, requer que a MB capacite os oficiais da Armada para que estes se contraponham aos

---

44 Equivalente estadunidense ao Comando de Defesa Cibernética Brasileiro (ComDCiber).

ataques e as explorações cibernéticas sofridas a bordo de seus navios. Para isso, Ferreira (2012) ensina a definir quais as competências que precisam ser desenvolvidas, relacionando detalhadamente todos os cursos necessários e, após isso, selecionar quem deverá adquirir tais conhecimentos. Dessa maneira, a seguir aprecia-se o currículo da Escola Naval, comparando-o com a formação proposta pela ENaDCiber, e, em sequência, pensa-se em como selecionar o pessoal adequado.

2.4.3 A Escola Naval e a Guerra Cibernética

Nesta seção especifica-se "o que saber para fazer" e, nesse sentido, Hamel e Prahalad (1995) elucidam que a partir do momento que a organização define as competências a serem desenvolvidas, deve-se envidar esforços para atingir esse fim. Assim, ao longo dos anos, a MB vem aperfeiçoando o currículo dos oficiais formados pela Escola Naval (EN), de acordo com as necessidades operacionais e técnicas. Em 2003, observada a importância do Oficial especialista em Comunicações, o Centro de Instrução Almirante Wandenkolk (CIAW) voltou a aperfeiçoar os Oficiais formados em eletrônica pela EN, em comunicações. Em 2004, os Aspirantes Intendentes de Marinha deixaram de estudar Navegação 3 e 4 em prol de uma qualificação mais especializada e adequada às funções de intendência. E, mais recentemente, os 3º e 4º "anistas" da EN começaram a estudar Introdução a Logística Naval e Inteligência respectivamente. Demonstra-se, assim, que a MB percebe a necessidade de melhor formar seus militares e faz uso da prerrogativa do Artigo 23 de Brasil (2006b) para adequar os currículos do Sistema de Ensino Naval.

Ao longo da pesquisa, foi possível perceber a importância da guerra cibernética para a Armada e sua necessidade de capacitação. Sendo assim apresenta-se, a seguir, uma análise superficial de viabilidade sobre a capacitação em guerra cibernética desenvolvida com apoio de dois documentos, um ostensivo da MB (BRASIL, 2018a) e extratos da parcela não sigilosa de documento de acesso restrito do EB (BRASIL, 2018b): o "conhecimento

cibernético” e as quantidades de horas-aula dos conteúdos fundamentais, básicos e intermediários das Trilhas de Conhecimentos[45] de Guerra Cibernética.

Ao observar a forma como são empregados os Oficias da Armada quando apresentados para o serviço embarcado, verifica-se que cada habilitação é empregada em sua área específica, ou seja, armamentistas nos departamentos de armamento, eletrônicos nos departamentos de operações, e maquinistas nos departamentos de máquinas. Dessa forma, é equilibrado assumir que as disciplinas atinentes a outras especialidades, estudadas ao nível de fundamentos, não são utilizadas pelos Oficiais ao longo da carreira, salvo em casos muito específicos.

QUADRO 1

Carga horária de conteúdos da Trilha de Conhecimentos de Guerra Cibernética

Trilha	Horas	Domínio	Nível
Fundamentos (módulos de 40h)[46]	440	Todos	Fundamental
Administração de Sistemas	40	Proteção	Básico
Administração de Banco de Dados	60	Proteção	Básico
Administração de Redes	80	Proteção	Básico
Segurança de TIC	40	Proteção	Básico
Criptografia Digital	60	Proteção	Intermediário
Forense Digital I	40	Proteção	Intermediário
Tratamento de Incidentes	40	Proteção	Intermediário
Governança de TI	40	Gestão	Básico
Direito Digital	40	Gestão	Básico
Gestão de Projetos de TI	40	Gestão	Básico
Inteligência de Fontes Abertas	40	Exploração	Básico
Análise de Inteligência	40	Exploração	Intermediário
Operações de Inteligência Cibernéticas	60	Exploração	Intermediário
Exploração de vulnerabilidade em Rede, Sistemas, BD e Web	60	Exploração	Intermediário

Fonte: Brasil (2018b)

Ao examinar a disciplina Treinamento Físico Militar (TFM), percebe-se que as 190 horas anuais podem ser distribuídas em 45 minutos diários (11 meses com 22 dias úteis). Salvo nas segundas-feiras, a disciplina é ministrada no período vespertino após a parada escolar até o horário do jantar, ou seja, na prática 3 horas. No período em questão, além das aulas obrigatórias

45 As Trilhas de Conhecimentos de Guerra Cibernética foram elaboradas por profissionais de Guerra Cibernética, com participação das três Forças Armadas e membros do Ministério da Defesa e Gabinete de Segurança Institucional da Presidência da República e encontram-se registradas e detalhadas por itinerário formativo específico para cada profissão em Brasil (2018b).

46 Curso elaborado em módulos de 40 horas que serão disponibilizados no Ambiente Virtual de Aprendizagem da ENaDCiber.

de TFM, são realizados os treinamentos das equipes esportivas, mas nem todos os Aspirantes são membros de equipes, o que indica haver tempo disponível no período da tarde para realização de atividades tanto para identificação de talentos, quanto para capacitação ou treinamento em Guerra Cibernética em caráter de voluntariado.

A partir do 3º ano, os Aspirantes começam a aprender disciplinas específicas de suas habilitações, sendo que o quarto eletrônico (CA-HE) aprende as de eletrônica e de comunicações. Dessa forma, a partir de Brasil (2018a), foram extraídas as cargas horárias das disciplinas de interesse para o estudo apresentadas na TABELA 1:

TABELA 1

Carga horária anual do Oficiais Habilitados em Eletrônica pela EN (CA-HE)

	Tecnologia da Informação	Específicas de Eletrônica	Específicas de Comunicações	Fundamentos de outras habilitações	Um tempo de aula a tarde antes do TFM (45 min)
1º ano	80 h	-	-	-	180 h
2º ano	-	-	-	-	180 h
3º ano	-	216 h	174 h	80 h	180 h
4º ano	-	188 h	66 h	132 h	180 h

Fonte: Brasil (2018a)

Na tabela 2, é considerada a possibilidade de estender a formação dos Oficiais da Armada Habilitados em Comunicações para a EN, criando o CA-HC, e ousa-se considerar a possibilidade da retirada dos fundamentos de outras habilitações do currículo do CA-HE e CA-HC e a inclusão de um tempo de aula de 45 minutos à tarde, tendo em vista que Milkovich e Boudreau (2000) ressaltam a necessidade de efetuar uma formação completa para assuntos complexos. Assim, compara-se a sobra de carga horária na coluna “tempo disponível” com a carga horária dos conteúdos básico e intermediário de guerra cibernética extraído do quadro 1.

TABELA 2

Tempo disponível versus conteúdo básico e intermediário de guerra cibernética

		Tempo disponível	Fundamentos de guerra cibernética	Proteção Cibernética	Gestão Cibernética	Exploração Cibernética
1º ano	-	180 h	80 h	-	-	-
2 º ano	-	180 h	120 h	-	-	-

3º ano	CA-HE	425 h	240 h	180		
	CA-HC	460 h	240 h	220		
4º ano	CA-HE	375 h	-	180	120	40
	CA-HC	497 h	-	140	120	200

Percebe-se, então, que o ganho de horas-aula ainda não é adequado para uma formação completa em guerra cibernética. Assim, considera-se a possibilidade de ministrar os conteúdos de gestão básico e de proteção básico e intermediário para ambos os quartos, para os CA-HE exploração básico e para os CA-HC, básico e intermediário de exploração. Isso ocorre porque compreende-se que a ampliação das capacidades de guerra cibernética da MB poderá ser realizada no período do Curso de Aperfeiçoamento ou em Cursos Especiais ao longo da carreira do Oficial, uma vez que verdadeiros talentos para a guerra cibernética possam ser despertados ou descobertos na EN.

Dessa maneira, considera-se que a organização do ensino em atividades de identificação de talentos e capacitação fundamental são mais interessantes se aplicadas nos dois primeiros anos escolares quando não há muito espaço para inclusão de disciplinas no currículo e, principalmente, para fomentar as práticas de guerra cibernética. Na organização pensada, a capacitação básica e intermediária seria melhor aplicada aos quartos CA-HE e CA-HC nos dois últimos anos. Ademais, pode-se considerar a possibilidade de adequar o conteúdo da disciplina de TI do 1º ano de forma que atenda parte do conteúdo fundamental de guerra cibernética, a fim de proporcionar 80 horas de prática laboratoriais no 4º ano. Assim, ao descartar os fundamentos de outras habilitações e ao desmembrar as especialidades, eletrônica e comunicações, ainda na EN, pode-se proporcionar ganho de carga horária satisfatório para ministrar conteúdos básicos e intermediários de guerra cibernética.

É importante ter em mente que esta é apenas uma das possíveis visões estratégicas para promover o aumento do conhecimento de guerra cibernética na MB. A ideia inicial não é formar um *hacker* ainda na EN, senão proporcionar, em um primeiro momento, os conhecimentos básicos necessários à capacidade de análise, julgamento e formação de juízo de

valor sobre guerra cibernética. Justamente em um ano em que se discute o aumento do tempo de serviço na ativa de 30 para 35 anos, não seria este o momento de pensar em melhor capacitar nosso pessoal? Caso a resposta da Alta Administração Naval para esta pergunta seja sim, o aumento de tempo em sala de aula para os Aspirantes da EN será uma boa solução a longo prazo. Feito isso, na próxima seção são explorados a seleção, o trato e a identificação dos potenciais operadores de guerra cibernética.

2.4.4 Identificação de Potenciais Humanos para Guerra Cibernética

Nesta seção, explora-se o "querer fazer" de cada profissional e tenta-se demonstrar que, mesmo sem ter o perfeito domínio do que se deve saber, é possível encontrar os profissionais corretos para capacitar e futuramente desenvolver para a guerra cibernética. Assim, é feita aqui a tentativa de promover a reflexão quanto à importância de identificar corretamente os potenciais humanos a serem empregados nas ações de guerra cibernética para, mais especificamente, serem capacitados para proteção e gestão cibernética e o básico de exploração.

Para isso, conta-se com a colaboração da Capitã (QCO) Alessandra Augusta de Santana e Silva Monteiro[47], que compartilhou um pouco de sua experiência e conhecimentos sobre a identificação de potenciais *hackers*, seus comportamentos e características. A psicóloga se formou na Universidade Católica de Goiás e compôs grupo de estudo sobre personalidade do *hacker* para o EB em 2015. O resultado obtido pelos pesquisadores foi registrado em documento de acesso restrito do EB, mas as informações ostensivas de interesse para este trabalho foram repassadas.

A Oficial foi realizou entrevistas individuais e em grupo, e avaliação psicológica por intermédio de um instrumento psicológico projetivo (investigação da personalidade). Essas

---

47 Psicóloga Militar da ENaDCiber, graduada pela Universidade Católica de Goiás em 2001, Pós-graduada *"lato sensu"* em Psicologia Jurídica, em 2003 e Pós-graduada "lato sensu" em Psicodrama (foco sócioeducacional), em 2009.

ferramentas possibilitaram o detalhamento do perfil do profissional de guerra cibernética, facilitando a identificação dos potenciais humanos, por meio da observação das seguintes características: interesse pela guerra cibernética, comportamento autodidata voltado para o aperfeiçoamento, curiosidade intelectual e interesse em colaborar com o desenvolvimento da área.

A partir dessas características, a Psicóloga indicou mecanismos para seleção dos futuros guerreiros cibernéticos, como palestras sobre a importância de atuação no setor, entrevistas e realização de competições, como o "Desafio *Cyber*" realizado na EN sob coordenação do Comando de Operações Navais em 2017. O EB realiza, na Academia Militar das Agulhas Negras (AMAN), o exercício conhecido como "Manobra Escolar", em que cada arma põe em prática seus conhecimentos teóricos. Os Cadetes de Comunicações exercitam seus conhecimentos aprendidos de guerra cibernética, seguindo as orientações do relatório da pesquisa. Nesse sentido, o sistema de grêmios escolares pode ser uma boa solução haja vista que já é aplicado na EN em diversas atividades. Como é feito em algumas universidades, estabelecer uma pontuação mínima anual a ser atingida pelos Aspirantes também pode servir para atrair interessados pelo assunto. Como, um sistema de disciplinas eletivas ou de atividades acadêmicas voluntárias.

Bizerra (2017) informa em sua pesquisa que o Canadá aumentará o efetivo de suas Forças Armadas (FFAA) em 3.500 militares, de forma a possibilitar o engajamento delas em ações de guerra cibernética, promovendo maior interoperabilidade com os aliados, em todo o espectro de conflitos e mantendo vantagem operacional sobre as ameaças atuais e futuras. Esta solução para as FFAA brasileiras não é viável, pois, conforme apontado anteriormente, há uma necessidade premente de redução de efetivos. Por isso, Rocha-Pinto et al. (2007) afirmam ser necessária a formação de profissionais polivalentes e com maior diversidade de conhecimentos. Para Pacheco et al. (2009), indivíduos que desenvolvem suas competências e se alinham aos objetivos estratégicos e organização, acabam por dedicar-se melhor em suas atribuições.

Nesse sentido, a Capitã orientou esta pesquisa quanto os principais medos e

ansiedades observados nestes profissionais, principalmente por se tratarem de militares que podem vir a se distanciar da carreira tradicional do oficial da Armada regular. Os guerreiros cibernéticos têm receio de trabalhar em locais onde não exista a cultura de compartilhar informações e conhecimentos e uma forma de mitigar estes sentimentos seria criar a cultura de envolvimento destes profissionais nas decisões da área (guerra cibernética) de forma a desenvolver um sentimento de pertencimento entre eles. Concordando com Alessandra, Clarke e Knake (2015) citam o pensamento do Major-General William Lord, da Força Aérea estadunidense, que reforça a necessidade de ser estabelecida uma cultura organizacional onde os guerreiros cibernéticos possam engajar-se. Por isso, esta pesquisa vem tentando conduzir o leitor a esse pensamento, apresentando a necessidade de qualificar os Oficiais da Armada para melhor assessorar, gerir, operar e conduzir a guerra cibernética.

Por fim, Rocha-Pinto et al. (2007) propõem um programa interno de desenvolvimento de competências, baseado no perfil de seus funcionários, suas habilidades, atitudes e posturas. Contudo, não se espera que todos os Oficiais Eletrônicos e Comunicativos consigam ter a capacidade plena de realizar proteção, exploração e quiçá ataques cibernéticos. Muitos serão apenas bons Gestores Cibernéticos, alguns serão bons Operadores de Proteção Cibernética, poucos serão bons Operadores de Exploração e Ataque cibernéticos e todos serão melhores Gestores e Operacionais de Eletrônica e Comunicações.

Dessa forma, a semente principal terá sido plantada no caminho do desenvolvimento tecnológico da força naval, pois interdependência entre as tecnologias, os seres humanos e suas capacidades é a base da guerra cibernética. Por isso, Bizerra (2017) afirma que a formação de guerreiros cibernéticos é uma política de Estado na China, Rússia e Coreia do Norte, corroborando com Pacheco et al. (2009), que ensinam que a capacitação do público interno pode alçar um patamar estratégico. Conclui-se então que o conhecimento é imperativo, uma vez que somente por ele serão alcançadas as competências para realizar ações de guerra cibernética, formar juízo de valor adequado para definição de tecnologias e determinação de padrões, técnicas e métodos. Esta questão será discutida de forma sintética no próximo capítulo.

3 INOVAÇÃO DA DOUTRINA ATUAL

Neste capítulo, tenta-se fomentar a inovação da DMNGCiber e promover a capacitação e desenvolvimento dos guerreiros cibernéticos navais. Assim, explora-se o "saber como fazer", ainda que sem qualificação necessária para tal. Isso porque, Clarke e Knake (2015) afirmam que a guerra cibernética é real, já teve início, ignora qualquer campo de batalha e o que é conhecido está longe de ser uma indicação de tudo que ainda pode ser feito.

O Livro Branco de Defesa Nacional trata a guerra cibernética como um desafio, denominando-a de "conflito do futuro" (BRASIL, 2012, p. 28). Nesse sentido, quando a DMN[48] define Ações de Guerra Cibernética da mesma forma que a Doutrina de Tecnologia da Informação da Marinha, um manual técnico, ignora-se a guerra cibernética como uma Ação de Guerra Naval que pode causar efeitos físicos aos navios de guerra.

> As ações de guerra cibernética são aquelas que envolvem o emprego de ferramentas disponíveis nos campos da Tecnologia da Informação e Comunicações para desestabilizar os ativos de informação do inimigo e, também, para possibilitar a proteção dos ativos de informação de interesse. (BRASIL, 2017a, p. 57-58)

Dessa maneira, observa-se que a concepção de emprego operacional da guerra cibernética pela MB compreende apenas os sistemas de TI e de Comunicações, não abrangendo os SCF e Sistemas de Combate e, por sua vez, não considerando os possíveis resultados cinéticos de ações cibernéticas.

Nesse sentido, Bizerra (2017), ao analisar a política canadense, afirma que ela é preditiva e não se prende às tecnologias passadas. Bizerra (2017) escolheu o Canadá para fazer sua pesquisa pela facilidade de encontrar informações e principalmente pela semelhança em dimensões e potencial econômico com o Brasil. Assim, observou que aquele Estado está se preparando em diversos campos do conhecimento e tecnológico para a guerra cibernética, com grande flexibilidade, adaptabilidade e fluxo de investimentos. Esta preparação, por sua vez, se dá, não apenas em capacitação pessoal, mas também em aquisição de novas tecnologias,

[48] Manual doutrinário que define os conceitos de emprego operacional das capacidades militares da MB.

integração de sistemas, criptografia e outras medidas de segurança no espaço cibernético. Medidas para mitigar as vulnerabilidades inerentes aos seus sistemas de operações, comando e controle e de seus sistemas de armas. Nesse sentido, é preciso pensar mais a fundo qual será a real capacidade, dependência e contribuição da MB para o setor cibernético nacional.

3.1 A DMNGCiber atual e a inovação de seus conceitos

Antes de inovar e incrementar a doutrina atual de forma efetiva, eficiente e eficaz, é necessário alcançar uma doutrina factível, conhecendo o nível atual de dependência do ciberespaço, para depois buscar as capacidades e definir o nível de dependência a elas associado, seguindo o exemplo estadunidense para alcançar este objetivo. Assim como eles, nossa dependência do ciberespaço está aumentando, portanto, deve-se alavancar todas as oportunidades em conjunto com a indústria, academia, interagências (EUA, 2012).

Para Clarke e Knake (2015), a dependência é o grau de confiança e de conectividade, em redes e sistemas, depositados por um usuário, um Estado, uma força armada ou um navio de guerra. Nesse sentido, Wedin (2015) menciona o "*mix high-low*" que os Estados precisam balancear ao desenvolverem navios. Mais robustos e com menos tecnologias em maior número para materializar a presença e a patrulha naval (parte *low* do *mix*). E, em menor quantidade, os altamente tecnológicos para suas forças navais (parte *high* do *mix*), cuja "capacidade de C4ISTAR[49] […] dão-lhe uma capacidade bastante elevada para a missão de conhecimento e de antecipação." (WEDIN, 2015, p. 216). Essa capacidade é acompanhada da dependência que os tornam vulneráveis a ataques e exploração cibernética. Quanto à capacidade a ser alcançada, Clarke e Knake (2015) definem defesa[50] como a habilidade dos usuários bloquearem ou mitigarem o ataque cibernético.

Clarke e Knake (2015) afirmam que a Coreia do Norte e a China possuem poucos

---

49 *Command, Control, Communications, Computers, Information/Intelligence, Surveillance, Targeting Acquisition and Reconnaissance.* (WEDIN, 2015, p. 216). A MB opera apenas C4ISR.

50 Mesmo conceito de "proteção cibernética" de Brasil (2014a).

sistemas dependentes, uma lacuna da guerra cibernética que os permite, sob ataque, desligar a conexão com o ciberespaço como medida eficaz de proteção cibernética. Ao apreciar-se o cenário nacional, pode-se questionar se realmente há vantagens no uso dos sistemas integrados por Internet. Segundo Clarke e Knake (2015) não depender da Internet pode reduzir a vulnerabilidade. Contudo, Beneditto (2016) aponta vantagens, como alta capacidade de compilação do cenário tático, consciência situacional, além de monitoramento e correção de parâmetros diversos. Portanto, até a MB decidir se integrará os sistemas navais à Internet, ou rede naval segura, é preciso ter a capacidade completa de guerra cibernética, a fim de gerenciar corretamente o risco envolvido.

Também é possível considerar a possibilidade de que, enquanto a MB não estiver "tão dependente" para operar seus navios em situações de guerra convencional, é possível desenvolver a capacidade de efetuar ataques e explorações cibernéticas. Os estadunidenses acreditam que "as salvas iniciais da próxima guerra provavelmente ocorrerão no ciberespaço e a Marinha deve estar pronta"[51] (EUA, 2012, p. 6, tradução nossa). Nesse sentido, Clarke e Knake (2015) citam que o Tenente-General Robert Elder[52] acredita que apenas se defender no ciberespaço deixa a força muito atrasada e afirma que para dominar os outros ambientes de guerra se faz necessário dominar completamente as capacidades de operar no ciberespaço.

Segundo Yogui (2019), para inovar não se deve tolher iniciativas e criticar ideias, mas sim identificar as necessidades do cliente, modificar seu produto e entregá-lo sem se "apaixonar" pelo produto anterior. Nesse sentido, reavaliar vulnerabilidades atuais, adequar procedimentos e capacitar os oficiais da Armada são medidas iniciais de inovação que poderão trazer bons resultados para a MB. Diversas ideias úteis, razoáveis e inovadoras poderão surgir provenientes da massa crítica, possibilitando o alcance do patamar de Força Naval Moderna almejado pela MB.

---

51 "The opening salvos of the next war will likely occur in cyberspace and the Navy must be ready."

52 Diretor da Força-Tarefa de Operações no Ciberespaço da Força Aérea estadunidense na primeira edição de Clarke e Knake (2015).

3.2 DMNGCiber: inovação no emprego da Guerra Cibernética

Após estudar as capacidades da guerra cibernética, comparando-as com táticas de batalha historicamente conhecidas e bem-sucedidas, como a *blitzkrieg*[53], Clarke e Knake (2015) especulam que os Estados Unidos da América, Estado inventor da tecnologia e das táticas de guerra cibernética, pode perder a vantagem estratégica conferida pela sua capacidade se seus militares permaneçam focados em doutrinas de emprego ultrapassadas e com excesso de confiança em armas obsoletas teoricamente superiores. Nesse sentido, Leon E. Panetta[54] cita que "Forças armadas modernas não podem conduzir operações rápidas e eficazes, sem redes confiáveis de informação e comunicação e acesso garantido ao espaço e ao ciberespaço."[55] (EUA, 2012, p. 2, tradução nossa)

Ao observar que forças navais mais poderosas que a MB não deixarão de depender do ciberespaço, nasce a oportunidade de pensar no emprego tático da guerra cibernética a semelhança da guerra eletrônica. O emprego operacional israelense contra as forças sírias, similar ao bloqueio eletrônico, deixou a defesa antiaérea do oponente completamente inutilizável (CLARKE; KNAKE, 2015). Nesse sentido, navios com maior capacidade de banda de Internet no mar e maior infraestrutura podem ser empregados em constante "varredura" de exploração cibernética, tentando localizar as forças adversárias ou suas ordens de batalha eletrônicas, além de realizar ataques cibernéticos nos sistemas de C4ISTAR, pois "[…] o ciberespaço e forneceu aos comandantes vantagens operacionais. Isso permitiu que a Marinha agisse com rapidez, agilidade e precisão [...][56]". (EUA, 2012, p. 6, tradução nossa)

A comparação entre a guerra cibernética e a guerra eletrônica é inevitável por vários aspectos, seja pela inovação trazida ao campo do combate, seja pelas possibilidades de ataque

---

53 Tática de ataque rápido empregando de carros de combate em conjunto com artilharia e aviação, implementada com amplo sucesso pelos alemães na Segunda Grande Guerra. (CLARKE; KNAKE, 2015)

54 Leon Edward Panetta foi o Secretário de Defesa dos Estados Unidos na administração do presidente Barack Obama. (EUA, 2012)

55 "Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to space and cyberspace."

56 "In the past the Navy has leveraged cyberspace and provided commanders with operational advantages. This has enabled the Navy to act with speed, agility, and precision [...]"

com capacidade de destruição ou inoperância de sistemas, seja, ainda, pelas medidas de furtividade, mascaramento ou diversão possíveis. No caso da primeira, suas possibilidades são ainda maiores, mas a segunda pode ser empregada como vetor para permitir a primeira. A diferença básica entre as duas "guerras" é que a guerra cibernética, para ser empregada com sucesso, requer a exploração de algum tipo de protocolo de Internet, ou vulnerabilidade conferida por *backdoors* lógicas e físicas. Para exemplificar, a seguir é feita a comparação entre o bloqueio eletrônico[57] de ponto sobre uma frequência específica de comunicações em VHF com um ataque ou exploração cibernética operados na mesma frequência. Para que o bloqueio eletrônico de comunicações seja exitoso, basta ter potência suficiente e a mesma frequência sendo transmitida contra os alvos para que eles sejam bloqueados[58]. A segunda medida requer identificar a frequência correta e explorá-la sem a necessidade de medidas invasivas que podem denunciar a presença ou posição do atacante por meio de medidas de apoio à guerra eletrônica.

Os alvos que trafegam suas comunicações em VHF-IP possibilitarão ao atacante, ou explorador cibernético, empregar técnicas específicas sobre as vulnerabilidades, como *backdoors*, *zeroday* de sistemas operacionais, dentre outros, para "destruir" o sistema de EAD adversário ou explorar informações. O explorador também poderá monitorar a rede tática de dados, buscar dados de interesse armazenados na rede de computadores associada aos transceptores de VHF-IP. Pode-se perceber que nesse caso não foi necessário empregar a Internet para que fosse realizada a guerra cibernética, ou seja, as possibilidades são diversas e o campo está plenamente aberto para exploração.

3.3 Carreira de Guerra Cibernética no Corpo da Armada

A presente seção tem o objetivo de realizar uma análise da possibilidade de criação da Qualificação Técnica Especial em Defesa Cibernética, comparando-a com a Carreira em

---

57 Medida de Ataque Eletrônico (MAE) não destrutiva que visa o impedimento do uso efetivo, por parte do inimigo, do espectro eletromagnético (BRASIL, 2017a).

58 O resultado será o impedimento na comunicação na frequência bloqueada.

"Y"[59] praticada atualmente no EB. Trata-se do passo posterior à capacitação da massa crítica, o desenvolvimento dos guerreiros cibernéticos que serão empregados no ataque e na exploração cibernética. Durante o período que este autor trabalhou na ENaDCiber, observou-se que militares de diversas Armas[60] desempenham alguma função no Centro de Defesa Cibernética (CDCiber) e no ComDCiber. Diferente da MB, onde se tem a cultura organizacional de empregar oficiais da Armada Eletrônicos e Comunicativos na Gestão de TI, no EB limitam-se menos as especialidades, como visto na Finalidade do Curso de Guerra Cibernética para Oficiais[61].

A capacitação do Oficial da Armada é premente e a proposta inicial foi de manter o foco nos Eletrônicos e Comunicativos, mas uma formação completa ainda na EN é inviável. Além disso, segundo a Psicóloga Militar, há a possibilidade de Oficiais de outras especialidades desenvolverem capacidade para guerra cibernética por autodidatismo. Nesse sentido, considera-se a possibilidade de prever a capacitação desses militares por meio de uma Qualificação Técnica Especial (QTE) ou da extensão do Curso de Aperfeiçoamento.

A MB voltou a realizar o Curso de Aperfeiçoamento Avançado para Oficiais da Armada (C-ApA)[62], abrangendo vários campos do conhecimento. Para isso, será necessário que a MB monte o curso para Oficiais em alguma instituição de ensino naval, ou aperfeiçoe o curso atualmente aplicado às Praças no Centro de Instrução Almirante Alexandrino (CIAA) (BRASIL, 2013). Por fim, também será preciso utilizar instituições de ensino extra-MB, como a estrutura do EB (ENaDCiber, CIGE, EsCom e CIE) e universidades vocacionadas para o assunto.

---

59 Disponível em <http://www.eb.mil.br/-/adocao-da-sistematica-de-aproveitamento-de-qualificacoes-funcionais-especificas-no-exercito- brasileiro>. Acesso em: 07 abr. 2019.

60 Infantaria, Cavalaria, Artilharia, etc. Disponível em: <http://www.eb.mil.br/armas-quadros-e-servicos > Acesso em 08 abr. 2019.

61 Habilitar os tenentes e os capitães de carreira das Armas, do Quadro de Material Bélico, do Serviço de Intendência e, em caráter excepcional, do Quadro de Engenheiros Militares […] e do Quadro Complementar de Oficiais […], para ocuparem cargos [...] no Sistema de Guerra Cibernética do Exército. (BRASIL, 2019a, p.257)

62 Disponível em: <https://www.marinha.mil.br/noticias/centro-de-instrucao-almirante-wandenkolk-conclui-curso-de-aperfeicoamento-avancado-para>. Acesso em: 07 abr. 2019.

4 CONCLUSÃO

Esta conclusão é iniciada com algumas reflexões: o que difere uma Marinha de Guerra de uma Guarda Costeira? Fora as questões de políticas de emprego e de marco legal regulatório, pode-se dizer que é o armamento utilizado. Ora, Guardas Costeiras não precisam de mísseis e torpedos, afinal, não foram criadas para destruição. Pelo contrário, foram criadas, no máximo, para neutralização, uma vez que sua tarefa é apresar infratores de legislação nacional nas águas jurisdicionais de seus Estados. Mas essa resposta satisfaz o questionamento?

Um canhão também tem o poder para destruir outro navio. Portanto, por que não utilizar somente canhões nos navios da Marinha de Guerra? A resposta parece simples: não podemos permanecer somente com canhões, pois as outras Marinhas de Guerra empregam mísseis, com poder de destruição e precisão muito maior. Então resta citar a tecnologia, pois ela sim é verdadeira divisora de águas entre uma Força Armada Moderna e uma Guarda Costeira. Precisamos melhor balancear o *high-low mix* da Força Naval brasileira, sem abrir mão de navios altamente tecnológicos.

Durante a operação *COMPTUEX*-2018[63] com a Marinha estadunidense, a bordo da Fragata Greenhalgh, este autor ficou convencido de que não adianta termos somente mísseis, torpedos e canhões, pois um simples avião Prowler[64] modificado para guerra eletrônica foi capaz de bloquear os radares e equipamentos de comunicações brasileiros. Naquela época, a MB ainda não tinha disponibilizado contramedidas para este tipo de ataque eletrônico e, por isso, ficou impossibilitada de reagir com seu armamento, ou seja, naquele momento a MB se encontrava no *low* do *mix*. A questão que ora se apresenta é que a guerra cibernética é hoje o que foi a guerra eletrônica nos anos 1990.

---

63 COMPTUEX is the final pre-deployment exercise which certifies the combined Essex Amphibious Ready Group and 13th Marine Expeditionary Unit's abilities to conduct military operations at sea and project power ashore during their upcoming deployment in summer of 2018. Dsiponível em <https://www.flickr.com/photos/navyoutreach/41772843355>. Acesso 02 abr. 2019.

64 Northrop Grumman EA-6B Prowler

Como visto nesta pesquisa, a Marinha estadunidense está se preparando para que sua primeira ação em combate seja um ataque cibernético e outros Estados estão investindo nesta capacidade para se contrapor àquela Força Naval. Por que a MB deveria ficar para trás? Com a evolução e aumento da complexidade das operações navais que MB está participando, até quando será possível que seus sistemas permaneçam sem integração mútua, sem poderem ser monitorados, operados e regulados remotamente? O acesso à informação por meio da Internet certamente permite maior velocidade e melhores condições para a tomada de decisões. A troca de dados táticos entre sistemas de combate pela Internet (EAD satélite) já é uma realidade em Marinhas de Guerra avançadas a muito tempo. Os transceptores de HF são para aquelas Marinhas o que é, hoje, o atuador de código Morse para a MB.

Os Pilares da Doutrina de Guerra Cibernética na MB são a experiência, a tecnologia e a capacitação, sendo igualmente importantes para a definição das ações de guerra cibernética possíveis de serem realizadas. Contudo, para a execução de ações de guerra cibernética, a capacitação se destaca em importância. O conhecimento de causa dá ao militar combatente a capacidade de operar, planejar, propor tecnologias, gerenciar riscos e desenvolver técnicas e procedimentos operacionais.

Na situação atual, a experiência contribui pouco para que a MB tenha uma doutrina adequada, pela falta de dados e exemplos comprovados e, principalmente, por não conseguir gerar suas próprias lições aprendidas e por possuir poucos profissionais com capacidade. As experiências em ações de guerra cibernética de outros Estados não são divulgadas, senão aquelas de conhecimento geral, o que dificulta a pesquisa bibliográfica por parte de um profissional empenhado em aperfeiçoar a DMNGCiber.

A tecnologia traz consigo diversas nuances, como portas lógicas e físicas abertas propositalmente, falhas de programação acidentais, ações de sabotagem e espionagem e, principalmente, carece de investimento da MB. É preciso, assim, utilizar uma forma adequada para congregar o conhecimento científico nacional para esta missão, como o modelo tríplice hélice já adotado pela MB em sua Estratégia de P&D e C&T.

A mitigação de riscos cibernéticos depende sobremaneira de conhecimento técnico, tanto nas técnicas específicas de guerra cibernética, quanto nas linguagens de programação dos sistemas navais em uso e sendo desenvolvidos. O risco de *chipping* e vazamento de informações de *zerodays* é grande, comprometendo a confiabilidade dos sistemas atuais, o que aumenta o risco de ataques cibernéticos serem convertidos em resultados físicos, direta ou indiretamente.

Sistemas de comunicações atualmente utilizados pela MB podem sofrer ataques cibernéticos, mesmo se utilizado o modelo *Dreadnought*, pois nenhuma solução de programação substitui integralmente o monitoramento humano por guerreiro cibernético. É preciso pensar em consoles de monitoramento, proteção, exploração e ataque específicos para cada sistema e na capacitação da linguagem de programação deles.

Percebe-se, assim, que, por não ter sistemas de combate e ciberfísicos dependentes da Internet, a MB é menos vulnerável, porém tem menos informações úteis, de qualidade e em tempo real para tomada de decisões. A ausência da tecnologia específica de guerra cibernética não exclui a necessidade de a MB estar preparada para empregar a capacidade de realizar ataques e exploração cibernética contra forças navais mais poderosas, a fim de obter vantagens táticas. Por isso, para obter qualquer capacidade significativa, será necessário ampliar a qualificação dos oficiais da Armada e tudo passará pela Gestão do Conhecimento de Cibernética no âmbito operacional da MB, afinal, serão os oficiais da Armada de hoje que decidirão em que nível de tecnologia a MB deverá ser capaz de operar.

Inovação em doutrina requer trazer para o tempo presente possibilidades futuras. Depende-se, assim, de investimento em tecnologias e capacitação para poder observar as próprias experiências e incrementar a DMNGCiber de acordo com critérios viáveis e factíveis. Para inovar, deve-se saber aproveitar as oportunidades que se apresentam e ter o sentimento de como o mundo pode ser afetado por uma ideia. A mudança no tempo de serviço ativo de 30 para 35 anos pode ser a oportunidade ideal para que a MB incremente a formação de seus militares. A tecnologia embarcada e as suas capacidades reais de emprego, acrescidas de

técnicas de proteção, exploração e ataque cibernéticos desenvolvidas por nossos militares será o diferencial para a concretização da visão de futuro da MB.

Não existe resposta padrão para a pergunta formulada na introdução. Mas o principal caminho começa pela capacitação e desenvolvimento dos militares brasileiros, para que eles tenham o discernimento para definir o objetivo final. Há uma lacuna de competências organizacionais na MB, pois esta Força ainda não considera a ameaça cibernética como algo que possa ser convertido em resultados físicos nocivos para um Navio ou Força Naval. Por consequência, existe uma lacuna de conhecimentos funcionais, inerentes aos oficiais da Armada, para a condução da guerra cibernética em todos os campos, Proteção, Exploração, Ataque, Gestão e Doutrina. A MB precisa reavaliar os riscos inerentes a guerra cibernética e definir bem seus objetivos relacionados com a dependência dos Sistemas Operacionais, Ciberfísicos e de TI.

A definição dos objetivos tecnológicos, da capacidade de compilação do quadro tático em tempo real e a ampliação da consciência situacional dos decisores dependerá enormemente da capacitação em massa de oficiais da Armada, futuros assessores de guerra cibernética em todos os níveis, assim como dos futuros tomadores de decisão da MB. Assim encerram-se as considerações desta pesquisa. Espera-se, desse modo, que o firme propósito de contribuir para a descoberta do caminho mais adequado a ser seguido pela MB no ramo da guerra cibernética tenha sido alcançado. E, sem a vaidade de tentar esgotar o assunto, sugere-se que novas pesquisas sejam realizadas por oficiais da Armada na busca de vulnerabilidades de nossas tecnologias e formas de melhorar a capacitação de nosso pessoal.

“Se você não sabe onde quer ir, qualquer caminho serve”

Lewis Carroll

REFERÊNCIAS

ALVES, Eder Júnior. **A evolução dos sistemas físico-cibernéticos ou ciberfísicos promove o aumento da complexidade dos riscos nas organizações contemporâneas**. Disponível em: <http://igti.com.br/blog/riscos-advindos-da-evolucao-fisico-cibernetica/>. Acesso em 01 abr. 2019.

AMORIM, Celso. Se**gurança Internacional: novos desafios para o Brasil. Contexto Internacional**, Rio de Janeiro, v. 35, n.1, p.287-311, 2013. Disponível em: <http://www.scielo.br/pdf/cint/v35n1/a10v35n1.pdf >. Acesso em: 05 abr. 2019.

BAYBUTT, Paul. *Sneak Path Security Analysis (SPSA) for Industrial Cyber Security.* Intech. 2004 *Apud* BENEDITTO, Marco Eugênio Madeira Di. **Defesa cibernética: proposta de estrutura para o âmbito da MB**. Rio de Janeiro: EGN, 2016.

BAYMA, Fátima (Org.). **Educação Corporativa: Desenvolvendo e Gerenciando Competências**. São Paulo: Pearson Prentice Hall, 2005.

BENEDITTO, Marco Eugênio Madeira Di. **Defesa cibernética: proposta de estrutura para o âmbito da MB**. Rio de Janeiro: EGN, 2016.

BIZERRA, Vitor M. S. X. **Segurança e Defesa Cibernéticas: Estratégia Canadense (2010-2017).** Edição do Kindle. Rio de Janeiro: ESG, 2017.

BRASIL. Decreto nº 5.707, de 23 de fevereiro de 2006. **Institui a Política e as Diretrizes para o Desenvolvimento de Pessoal da administração pública federal direta, autárquica e fundacional, e regulamenta dispositivos da Lei nº 8.112, de 11 de dezembro de 1990.** Brasília, 2006a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5707.htm>. Acesso em 31 mar. 2019.

_____. Lei 11.279, de 9 de fevereiro de 2006. **Dispõe sobre o Ensino na Marinha.** 2006b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11279.htm>. Acesso em 31 mar. 2019.

_____. Ministério da Defesa. **Livro Branco de Defesa Nacional.** Brasília: MD, 2012. Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 01 abr. 2019.

_____. Anexo do of nº 370/2013, da DensM ao CIAA: **Currículo do Curso Especial de Defesa Cibernética para Praças (C-Esp-DefCiber-PR).** 2013.

_____. MD31-M-07. **Doutrina Militar de Defesa Cibernética.** 1. ed. Brasília, 2014a.

_____. Portaria Normativa nº2.777-MD, de 27 de outubro de 2014. **Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências**. 2014b.
Disponível em: http://www.sgex.eb.mil.br/sistemas/be/copiar.php?codarquivo=1314&act=bre Acesso em 1º abr. 2019.

_____. PETIM 2016-2019. **Plano Estratégico de Tecnologia da Informação da Marinha.** 2015. Disponível em: https://www.marinha.mil.br/sites/default/files/petim_mb.pdf. Acesso 1º abr. 2019.

_____ . Estado-Maior da Armada. EMA-305. **Doutrina Militar Naval**. 1ª ed. Brasília, DF, 2017a.

_____. Estado-Maior da Armada. EMA-415. **Estratégia de Ciência, Tecnologia E Inovação da Marinha do Brasil**. 1ª ed. Brasília, DF, 2017b.

_____. Anexo (426), do Of nº 226/2018, da DEnsM à EN: **Currículo dos Cursos de Graduação de Oficiais**. 2018a.

_____. Relatório Técnico da Consultoria Técnica do Departamento de Educação e Cultura do Exército Brasileiro (DECEx) ao Comando de Defesa Cibernética (ComDCiber). **Entrega do pacote de trabalho da Estrutura Analítica do Projeto de Criação da Escola Nacional de Defesa Cibernética, nº 1.5.2: "Trilhas do conhecimento cibernético"**. ACESSO RESTRITO**.** 2018b.

_____. **Catálogo de Cursos do Departamento de Educação e Cultura do Exército.** Rio de Janeiro: DECEx, 2019a. Disponível em: <http://www.decex.eb.mil.br/images//pdfs_2019/catalogo-de-cursos-decex-versao-2019.pdf>. Acesso em 08 abr. 2019.

_____. **Press Release Projeto "Classe Tamandaré"**. 28 de março de 2019. 2019a. Disponível em: <https://www.marinha.mil.br/sites/default/files/press_release_-_projeto_classe_tamandare_-_marinha_seleciona_a_melhor_oferta.pdf >. Acesso em 08 abr. 2019b.

CARBONE, Pedro Paulo. et tal. **Gestão por competências.** Rio de Janeiro. Editora FGV, 2016.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética**. BRASPORT. Edição do Kindle. 2015.

CRUZ JR. Samuel C. **A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual, Texto para Discussão, Nº1850,** SAE. IPEA. Brasília 2013.
Disponível em:
<https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.econstor.eu/bitstream/10419/91261/1/756394686.pdf&ved=2ahUKEwjehO7X6LPhAhXdIbkGHQ2vBD8QFjABegQIAhAB&usg=AOvVaw1byairJZQDtY-iLEFOabhd.> Acesso 03 abr. 2019

EUA. **Navy Cyber Power 2020 (NCP 2020).** 2012. Disponível em: <https://www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf>. Acesso em 3 abr. 2019.

FALLIERE, N.; MURCHU, L. O.; CHIEN, E. *W32.Stuxnet dossier.* Cupertino: Symantec. 2011 *Apud* CRUZ JR. Samuel C. **A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual, Texto para Discussão, Nº1850,** SAE. IPEA. Brasília 2013.
Disponível em:
<https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.econstor.eu/bitstream/10419/91261/1/756394686.pdf&ved=2ahUKEwjehO7X6LPhAhXdIbkGHQ2vBD8QFjABegQIAhAB&usg=AOvVaw1byairJZQDtY-iLEFOabhd.> Acesso 03 abr. 2019

FERREIRA, Victor Cláudio Paradela. **Gestão de Pessoas.** Rio de Janeiro: FGV, 2012.

GRAMIGNA, Maria Rita Miranda. **Modelo de competência e gestão de talentos.** 12. ed. São Paulo: Pearson Education, 2007.

GUIMARÃES. Alberto; GRIVET. Marco Antonio. **Radiolocalização de Terminais de Comunicações Móveis.** Telecomunicações - Volume 06 - Número 01 - Junho de 2003. 2003. Disponível em: <https://www.inatel.br/revista/busca/193-radiolocalizacao-de-terminais-de-comunicacoes-moveis-s801196-1/file>. Acesso em 05 abr. 2019.

HAMEL, Gary; PRAHALAD, C. K.. **Competindo pelo Futuro:** Estratégias inovadoras para obter o controle do seu setor e criar os mercados de amanhã. Rio de Janeiro: Campus, 1995.

LEME, Rogerio. **Aplicação Prática de Gestão de Pessoas por Competências**. 2.ed. Rio

de Janeiro: Qualitymark Editora, 2008. 244p.

MESERVE, Jeanne. ***US Sources: Staged cyber attack reveals vulnerability in power grid.*** Cable News Networ k (CNN), 2007 *Apud* BENEDITTO, Marco Eugênio Madeira Di. **Defesa cibernética: proposta de estrutura para o âmbito da MB**. Rio de Janeiro: EGN, 2016.

MILKOVICH, George T.; BOUDREAU, John W. **Administração de Recursos HUMANOS.** São Paulo: Atlas, 2000.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos.** Berkeley Brasil, 2002.

ORLEAN, Daniel; FERREIRA, Francisco. **Mapeamento e gestão por competências na prática: metodologias e soluções tecnológicas. Congresso Nacional Sobre Gestão de Pessoas** (CONARH). São Paulo, 2005. Disponível em: <http://moodle.fgv.br/cursos/centro_rec/docs/mapeamento_gestao_competencias.pdf>. Acesso em 09 abr. 2019.

PACHECO, Luzia et al. **Capacitação e Desenvolvimento de Pessoas.** 2. ed. Rio de Janeiro: FGV, 2009. 144 p.

PAGLIUSI, Paulo. **Riscos Cibernéticos Tendências, Desafios e Estratégia para IoT.** 2017. Disponível em: <https://www.institutodeengenharia.org.br/site/wp-content/uploads/2017/10/arqnot10354.pdf.> Acesso abr. 2019.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico [recurso eletrônico]: métodos e técnicas da pesquisa e do trabalho**. 2. ed. Novo Hamburgo: Feevale, 2013. Disponível em: <http://www.feevale.br/Comum/midias/8807f05a-14d0-4d5b-b1ad-1538f3aef538/E-book%20Metodologia%20do%20Trabalho%20Cientifico.pdf.> Acesso em 20 fev. 2019.

ROCHA-PINTO, Sandra Regina da; PEREIRA, Cláudio de Souza; COUTINHO, Maria Teresa Correia; JOHANN, Sílvio Luiz. **Dimensões Funcionais da Gestão de Pessoas.** 9. ed. Rio de Janeiro: Fgv, 2007.

SILVA, Mateus de Oliveira. **Gestão de pessoas através do sistema de competências**. Rio de Janeiro: Qualitymark, 2005.

SCHNEIDER, David. ***Jeep Hacking 101***. IEEE Spectrum, 2015 *Apud* BENEDITTO, Marco Eugênio Madeira Di. **Defesa cibernética: proposta de estrutura para o âmbito da MB**. Rio

de Janeiro: EGN, 2016.

TAKEMURA, T.; OSAJIMA, M.; KAWANO, M. *Positive analysis on vulnerability, information security incidents, and the countermeasures of Japanese Internet service providers*. International journal of business, economics, finance and management sciences, v. 1, n. 3, 2009 *Apud* CRUZ JR. Samuel C. **A Segurança e Defesa Cibernética no Brasil e uma Revisão das Estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual, Texto para Discussão, Nº1850,** SAE. IPEA. Brasília 2013.
Disponível em: <https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.econstor.eu/bitstream/10419/91261/1/756394686.pdf&ved=2ahUKEwjehO7X6LPhAhXdIbkGHQ2vBD8QFjABegQIAhAB&usg=AOvVaw1byairJZQDtY-iLEFOabhd.> Acesso 03 abr. 2019

WEDIN, Lars. **Estratégias Marítimas no Século XXI: A contribuição do Almirante Castex**. Rio de Janeiro: Escola de Guerra Naval, 2015. Disponível em: <http://www.egn.mb/cemosexameselecao.php> (INTRANET)

YOGUI, Ricardo. **Seminário de Inovação para o Setor Público.** 2019. Disponível em: <https://eadpos.iag.puc-rio.br/login/index.php>. Acesso em 07 abr. 2019.

Por favor qualifique-se profissionalmente, funcionalmente e dentro do processo de estudo dos hackers: Psicóloga militar

1 - A sra participou do estudo sobre personalidade do profissional de defesa cibernética para o Exército Brasileiro?

Sim, em 2015.

2 - Qual foi a sua participação no estudo?

Realizei entrevistas individuais e em grupo, e avaliação psicológica por intermédio de instrumento psicológico projetivo (investigação da personalidade).

3 - O estudo gerou um relatório sigiloso sobre o assunto?

Relatório de acesso restrito.

4 - Baseado em vossa experiência no assunto e atual participação do corpo de profissionais da Escola Nacional de Defesa Cibernética responda o que for ostensivo a cerca das questões seguintes:

4.1) conhecendo o perfil do profissional em questão, como a Sra orienta a busca por estes potenciais humanos nas escolas de formação da Marinha do Brasil?

Interesse pela área, comportamento auto-didata voltado para o aperfeiçoamento, curiosidade intelectual, interesse em colaborar com o desenvolvimento da área.

4.2) como a Sra implementaria o processo de seleção destes profissionais?

Palestras sobre a importância de atuação no setor; entrevistas; realização de competições.

4 3) conhecendo a psique humana quais os principais medos e ansiedades observadas nestes profissionais, quando os mesmos decidiram traçar uma carreira em um setor diferente do cibernético?

Receio de trabalhar em um local onde não exista a cultura de compartilhar as informações e conhecimentos.

4.4) como a Sra mitigaria este medo a fim de melhor aproveita-los como profissionais para a força?

Criar a cultura de envolvimento destes profissionais nas decisões da área de forma a desenvolver um sentimento de pertencimento entre eles.

Cap QCO Alessandra Augusta de Santana e Silva Monteiro – Psicóloga da ENaDCiber