MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

GUERRA CIBERNÉTICA: OS DESAFIOS IMPOSTOS POR ESSE NOVO TIPO DE COMBATE À MARINHA DO BRASIL

PRIMEIRO TENENTE IGOR LUIZ DE FREITAS COBELLAS

Rio de Janeiro
2018

PRIMEIRO TENENTE IGOR LUIZ DE FREITAS COBELLAS

GUERRA CIBERNÉTICA: OS DESAFIOS IMPOSTOS POR ESSE NOVO TIPO DE COMBATE À MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança das Informações e Comunicações.

Orientador: Capitão de Mar e Guerra (RM1) Dario

CIAW
Rio de Janeiro
2018

Cobellas, Igor Luiz de Freitas
Guerra cibernética: Os desafios impostos por esse novo
Tipo de combate `a Marinha do Brasil / Igor Luiz de Freitas Cobellas. -- Rio de Janeiro, 2018.
42 f.

Orientador técnico e acadêmico: CMG (RM1) Dário Antônio Martins Leite Sant'anna.
Trabalho de Conclusão de Curso (Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações). -- Centro de Instrução Almirante Wandenkolk, Centro de Coordenação de Pós-Graduação, 2018.

1. Guerra Cibernética. 2. Segurança da informação. 3. Marinha do Brasil. 4. Ciberespaço. I. Sant'anna, CMG (RM1) Dário Antônio Martins Leite. II. Título.

FOLHA DE APROVAÇÃO

PRIMERIO TENENTE IGOR LUIZ DE FREITAS COBELLAS

GUERRA CIBERNÉTICA: OS DESAFIOS IMPOSTOS POR ESSE NOVO TIPO DE COMBATE À MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança das Informações e Comunicações.

Aprovada em _____

Banca Examinadora:

Capitão de Mar e Guerra (RM1) Dário _____

Capitão de Mar e Guerra (RM1) Huback _____

Professor Guilherme _____

CIAW
Rio de Janeiro
2018

Dedico esse trabalho à minha família.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, meu refúgio e Fortaleza. Sem a fé e esperança que tenho Nele não conseguiria chegar até aqui. Foram muitas as barreiras que, por minhas forças, não conseguiria transpor e por Sua misericórdia todas foram transpostas.

Agradeço a minha madrinha por sempre acreditar em mim, por nutrir meus sonhos e ajudar a conquistá-los. Saiba que cada vitória que tiver no decorrer da minha carreira e vida a senhora sempre se fará presente.

A minha esposa por ter me dado forças nos momentos que precisei. São mais de 10 anos de relacionamento em que, por muitas vezes, não pude me fazer presente e em todas elas você soube entender, e mais do que isso, me motivou e me apoiou. Meu amor, saiba que te amo e peço a Deus que preserve nossa relação para sempre.

Aos meus pais, por sempre estarem ao meu lado, por chorarem minhas lágrimas e sorrir comigo nos momentos de alegria. Vocês são minha base, minha essência.

A minha tia Célia e prima Michelle por estarem sempre preocupadas, por ligar e entender os motivos que me fizeram estar um pouco afastado. Agradeço por ter cuidado de mim desde meus tempos de criança e agora, na conclusão desse trabalho, não foi diferente.

Ao meu irmão Victor, por entender que os momentos que não pude ajudá-lo foi decorrente da necessidade de dedicação e falta de tempo que esse trabalho exigiu.

Ao Tenente Coronel Fábio Alexandre, meu primo, que sempre foi meu norte, aquele que desde de criança me espelho. Obrigado por mostrar o único caminho que leva a verdadeira paz, por desde de criança andar ao meu lado e me ajudar a formar o homem que sou. Se sou oficial da Marinha do Brasil, saiba que você foi motivador disso tudo.

Ao meu Orientador e 1º comandante, o Capitão de Mar e Guerra (RM-1) Dário, que, antes de ser meu orientador nesse trabalho, foi exemplo a ser seguido no comando da Corveta Julio de Noronha. Sua justiça e forma de comandar são as primeiras orientações que o senhor ministrou. Seguirei seu exemplo em todos os meus postos da carreira.

Aos amigos de longa data, Leonardo e José Jr, irmãos que a Marinha me deu. Contem sempre comigo da mesma forma que sei que posso contar com vocês. Vocês são a verdadeira tradução de amizade.

As amigas Lara e Valéria, obrigado por me aturar nesses momentos complicados de término do trabalho, por aceitarem ficar escutando assuntos relacionados a guerra cibernética sem reclamar.

A amiga e Primeiro Tenente (RM2-S) Paula Sabino. Agradeço todo apoio prestado e suas horas de dedicação a correção desse trabalho. Saiba que sua ajuda contribuiu sobremaneira para finalização do mesmo. Muito obrigado por tudo.

Bendito seja o Senhor, rocha minha, que adestra minhas mãos para guerra e meus dedos para o combate. Salmos 144, versículo 01.

GUERRA CIBERNÉTICA: OS DESAFIOS IMPOSTOS POR ESSE NOVO TIPO DE COMBATE À MARINHA DO BRASIL

Resumo

O controle da informação sempre foi imprescindível para o sucesso das operações militares. Com isso, os avanços tecnológicos têm imputado aos comandos militares uma nova visão sobre a Guerra Cibernética. O ciberespaço é um ambiente relativamente novo e complexo, ainda não mapeado e totalmente desconhecido e todos os dias, vários países estão enfrentando desafios a fim de proteger suas infraestruturas essenciais e estratégicas. Com o domínio da tecnologia digital de ataque e defesa, forças militares ou civis poderão agir diretamente nos computadores inimigos provocando danos imprevisíveis de elevado custo político, social, econômico e militar aos invasores. O presente trabalho procura determinar a magnitude do problema e instigar o pensamento sobre a forma de resolvê-lo para evitar que o cenário no ciberespaço saia do controle. Apresenta o tema da Guerra Cibernética, sua importância no cenário atual e os desafios da nova era da informação, caracterizada pela grande convergência das tecnologias dos computadores e das comunicações, empregadas para processar, transmitir e armazenar a informação. Como resultado do trabalho, pretende-se apresentar os desafios e as perspectivas para a Marinha do Brasil enfrentar nos próximos anos a fim de se preparar para as novas ameaças no espaço cibernético.

Palavras Chave: Guerra Cibernética; Segurança da Informação; Marinha do Brasil; Ciberespaço.

LISTA DE FIGURAS

Figura 1 – Quantidade de ataques ocorridos em 2010.……..…..…… página 23
Figura 2 – Equação de Segurança da Informação…….....… página 28
Figura 3 – Sequência de Ações nas Fases de Exploração e Ataque Cibernético..... página 31
Figura 4 – Impactos de ações cibernéticas contra um sistema de Comando e Controle..... página 31
Figura 5 – Sequência de Ações e Proteções Cibernéticas nas Fases de Exploração e Ataque Cibernético..... página 33

LISTAS DE SIGLAS E ABREVIATURAS

CAp	Curso de Aperfeiçoamento
CApA-SIC	Curso de Aperfeiçoamento Avançado em Segurança das Informações e Comunicação
CASNAV	Centro de Análises de Sistemas Navais
CIAW	Centro de Instrução Almirante Wandekolk
CLT	Centros Locais de Tecnologia da Informação
CTIM	Centro de Tecnologia da Informação da Marinha
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DIPNAV	Diretrizes para Planejamento Naval
DSIC	Departamento de Segurança da Informação e Comunicações
END	Estratégia Nacional de Defesa
ESG	Escola Superior de Guerra
EUA	Estados Unidos da América
FFAA	Forças Armadas
GovTI	Governança de Tecnologia da Informação
ICP-BRASIL	Infraestrutura de Chaves Públicas-BRASIL
MB	Marinha do Brasil
MD	Ministério da Defesa
OM	Organização Militar
PEM	Plano Estratégico da Marinha
PTIM	Plano de Tecnologia da Informação da Marinha
SI	Segurança da Informação

TI	Tecnologia da Informação
WAN	*Wide Area Network* (Rede de Longa Distância)

SUMÁRIO

1 INTRODUÇÃO 12
1.1 Apresentação do Problema 14
1.2 Justificativa e Relevância 15
1.3 Objetivos 15
1.3.1 Objetivo Geral 15
1.3.2 Objetivos Específicos 16

2 REFERENCIAL TEÓRICO 17

3 METODOLOGIA 18
3.1 Classificação da Pesquisa 18
3.1.1 Classificação Quanto aos Fins 18
3.1.2 Classificação Quanto aos Meios 18
3.2 Limitações do Método 19
3.4 Coleta e Tratamento dos Dados 19

4 O BRASIL FRENTE AO CENÁRIO DE GUERRA CIBERNÉTICA.....20
4.1 A Marinha no Ciberespaço.....24
5 CAPACITAÇÃO DOS MILITARES DA MARINHA DO BRASIL PARA GUERRA CIBERNÉTICA 26
6 ATAQUES CIBERNÉTICOS.....29
6.1 Proteção para Sistemas Baseados em Rede 32
6.2 Os Desafios da Guerra Cibernética para a Marinha do Brasil.....33
7 CONCLUSÃO.....36
7.1 Considerações Finais.....37
7.2 Sugestões para Trabalhos Futuros.....39
REFERÊNCIAS BIBLIOGRAFICAS.....40

1. INTRODUÇÃO

Controlar o uso da informação é fato marcante nas operações militares. A integração das telecomunicações e da informática, por meio das redes computacionais, criou o denominado ciberespaço, onde as informações circulam e são fundamentais para sobrevivência das organizações (ALENCAR, 2010).

Com os avanços tecnológicos crescentes e o frequente uso da internet faz com que os altos comandos militares mudem sua forma de pensar sobre a guerra cibernética (GC). É necessário conhecer bem o local onde esta guerra é travada. Entende-se como espaço cibernético o ambiente baseado em redes de computadores e comunicações para intercâmbio de informações. É um ambiente que oferece o suporte para a interação entre pessoas, empresas e instituições (DEFESA AÉREA E NAVAL, 2014).

O mundo virtual é o campo de batalha dessa guerra que é uma forma silenciosa de conflito travado entre indivíduos, grupos não-estatais, governos e forças militares por meio de ações que podem produzir resultados no mundo real. Os ataques virtuais se manifestam de forma constante. Recentemente empresas em vários países foram alvo de mais um grande ataque cibernético como mostra matéria publicada no jornal "O Globo" do dia 27 de junho de 2017 que informou a ocorrência de um ataque de proporções mundiais. Na Ucrânia afetou desde saques em contas bancárias até a monitoração eletrônica de radiação da usina desativada de Chernobyl. Em outros países como Rússia, Noruega, Romênia, Espanha, Holanda, Reino Unido e Estados Unidos o ataque também foi sentido. Nos Estados Unidos por exemplo, o departamento de segurança monitorou as ameaças que afetaram, pelo menos, duas grandes empresas multinacionais. No Brasil, o vírus paralisou as oito unidades do hospital do câncer de Barretos. (O GLOBO, 2017).

As redes de computadores fazem parte do arsenal de guerra de qualquer Força Armada bem treinada e evoluída tecnologicamente. Segundo alguns especialistas, ataques cibernéticos bem-sucedidos contra a infraestrutura de países fortemente dependentes de tecnologia da informação (TI), como os sistemas financeiros, redes de energia, controles de tráfego aéreo, entre outros, podem provocar danos imprevisíveis e de elevado custo político, social e econômico. Segundo SALDAN, o ambiente cibernético pode ser considerado um novo domínio ou palco de batalha,

depois da terra, do mar, do ar, do espaço exterior e do espectro eletromagnético. Em conflitos anteriores, esses componentes críticos citados acima se tornaram alvos pelo fato de sua destruição poder gerar uma série de entraves a uma nação. Estes mesmos componentes já não precisam mais ser fisicamente atacados por serem baseados em sistemas de rede. Eles poderão sofrer ataque cibernéticos com efeitos tão devastadores como um ataque físico (KAMAL, 2005).

Por tais motivos as redes de computadores, nos dias atuais, fazem parte do arsenal de guerra de qualquer Força Armada bem treinada e evoluída tecnologicamente. Segundo alguns especialistas, ataques cibernéticos bem-sucedidos contra a infraestrutura de países fortemente dependentes de tecnologia da informação (TI), como os sistemas financeiros, redes de energia, controles de tráfego aéreo, entre outros podem provocar danos imprevisíveis e elevado custo político, social e econômico. Desse modo, a Guerra Cibernética representa o método para pequenas frações mal-intencionadas possam realizar ataques contundentes até mesmo em poderosas potências mundiais.

Com domínio das formas adequadas de ataque e defesa cibernética, as Forças Armadas (FFAA), então capacitadas, poderão coibir o inimigo no uso adequado da informação podendo até mesmo manipular mensagens falsas a fim de confundir as forças inimigas. Com o amplo crescimento dos ataques à redes de computadores onde FFAA, empresas e órgãos do governo são atacados, é necessário que o Brasil adote políticas que visem atentar os principais pontos vulneráveis e a eliminação desses riscos (PINTO, 2009).

Como parte integrante das FFAA, a Marinha do Brasil deverá aperfeiçoar políticas de segurança da informação internas tendo em vista que, no campo militar, esta nova modalidade do conflito está sempre pronta a criar novas armas e enfraquecer defesas, aumentando a vulnerabilidade das organizações militares à medida que se tornam mais dependentes de TI.

Essa nova espécie de conflito parece ser altamente dispersa e bastante indefinida. Sendo assim, a distinção entre guerra e paz pode ser facilmente mascarada pelo fato dessa nova modalidade de combate estar inserida no contexto de uma guerra não convencional. Grandes instalações militares tais como pistas de pouso, comunicações fixas e grandes quartéis-generais tornam-se extremamente vulneráveis e o mesmo pode ser dito dos equivalentes civis isso inclui postos de governo, instalações de energia e fábricas de serviços e manufaturas. O sucesso

contra a guerra cibernética depende maciçamente da eficiência de ações em conjunto, uma aglutinação de mentalidade de segurança e medidas de proteção contra a GC.

A tecnologia intervém de forma definitiva em muitas áreas de trabalho nos campos civis e militares e está em constante evolução. As forças militares adequam o desenvolvimento das tecnologias às necessidades que elas possuem. Um exemplo foi a criação do primeiro computador, o ENIAC, cujo projeto teve início em 1943 durante a Segunda Guerra Mundial (PINTO, 2009).

Nos dias atuais os Estados convivem com a constante possibilidade de ataques cibernéticos. A realidade da Guerra Cibernética lança desafios e impõe transformações às nações, modificando as suas formas de trabalho e de defesa de ataques à rede que as afetam civil e militarmente. Não obstante, a Marinha do Brasil (MB) deverá se adequar à essa nova modalidade de Guerra, desenvolvendo sistemas de proteção como novos softwares de proteção explorando todo seu potencial de desenvolvimento no uso de TI, pois possui sistemas administrativos e operativos que são alvos pertinentes a um ataque cibernético, o qual pode enfraquecer a defesa do país. Sendo assim faz-se mister analisar e compreender esta nova frente de combate cujas consequências poderão ultrapassar os limites dos meios militares tendo implicações que poderão afetar toda a sociedade (PINTO, 2009).

1.1 Apresentação do Problema

Entende-se como espaço cibernético o ambiente que se refere a um espaço baseado em redes de computadores e de comunicações para troca de informações. Sintetizando, é o ambiente que oferece o suporte para a interação entre pessoas, empresas e instituições. Nos dias atuais esse espaço trouxe muitos benefícios facilitando o trânsito de informações, a interação e a aproximação entre indivíduos, grupos sociais, políticos e econômicos e até entre nações, por outro lado nos deixou mais vulneráveis na medida em que nossas informações navegam livremente por esses sistemas, sejam eles civis ou militares.

Esse tema passou a integrar, oficialmente, o cenário da Marinha do Brasil a partir de 2008. A Marinha do Brasil, como uma das primeiras instituições nacionais a

fazer uso da Tecnologia da Informação, possui diversos sistemas, tanto administrativos quanto operativos, que podem ser alvo de um ataque cibernético. Com isso é necessário implantar medidas de defesa e ataque para sua proteção, compreender este novo tipo de embate e lançar ofensivas cibernéticas tudo em prol de sua integridade.

1.2 Justificativa e Relevância

A Marinha precisa estar apta a proteger suas informações, para isso é necessário adotar medidas de proteção, mediante a elaboração de uma doutrina e formulação de uma mentalidade de defesa contra a guerra cibernética. Tais medidas de proteção serão eficientes a medida que doutrinas e estratégias de segurança de defesa do espaço cibernético sejam feitas.

Além disso, no mundo cibernético o conceito de fronteiras não está bem definidos quando não possuem de uma legislação que os ampare. A Guerra Cibernética também pode constituir-se de valiosa ferramenta para produzção de conhecimentos de inteligência sobre indivíduos ou países que se utilizam da furtividade do ciberespaço para realizar ou patrocinar atividades criminosas, terroristas ou que atentem contra a soberania nacional.

1.3 Objetivos

Como objetivos delineados para realização desse trabalho, pode-se elencar objetivos distintos, sendo o objetivo geral como um foco de busca por meio da presente dissertação, e os objetivos específicos sendo aqueles que precisam ser alcançados para que o foco do trabalho seja alcançado.

1.3.1 Objetivo Geral

Através desse trabalho pretende-se mostrar que o estudo da guerra cibernética é imprescindível para Marinha. A guerra cibernética não constitui ficção científica. Ela é real. Apesar de as ações ofensivas dessa natureza serem pouco divulgadas, a ocorrência das mesmas pode ser indicada por meio de vários

episódios de ataques cibernéticos coordenados a infraestruturas críticas de determinados países por motivações diversas. Assim, deseja-se difundir a mentalidade que nenhuma força armada pode deixar de adotar medidas rígidas frente a possibilidade de ataques no ciberespaço, principalmente quando tais ataques podem ser direcionados as suas estruturas de defesa. Esse trabalho também pretende elucidar como esse novo tipo de tecnologia também pode ser uma ferramenta pra produção de conhecimento de inteligência, uma vez que podem ser produzidos informes sobre indivíduos, grupos ou países que usam o ciberespaço para realizar ou patrocinar atividades criminosas.

1.3.2 Objetivos Específicos

- Estabelecer o posicionamento do Brasil e da MB frente ao cenário mundial de segurança cibernética;
- Capacitação do pessoal da MB para Guerra Cibernética;
- Conhecer os tipos de ataque, métodos de proteção e mostrar os desafios que a guerra cibernética impõe para Marinha.

2. REFERENCIAL TEÓRICO

Dentre as diversas e relevantes bibliografias referenciadas para realização deste presente estudo, algumas foram de decisiva importância pra a integração das ideias e encaixe do formato que se segue.

Segundo Nunes, a Marinha é uma das instituições pioneiras a fazer uso da tecnologia da informação. O autor faz uma análise sobre a guerra cibernética uma propõe uma base doutrinária para seu emprego, realiza uma análise do posicionamento da Marinha em relação ao tema e sugere medidas para aperfeiçoar sua capacidade face as novas ameaças e oportunidades oferecidas pelo ciberespaço (NUNES, 2010).

Nesse contexto Pinto apresenta um resumo histórico de dos perigos da evolução tecnológica dos sistemas computacionais e apresenta como os países e organizações internacionais abordam esse assunto no que tange a segurança da informação. Elucida as leis existentes sobre o assunto e ao final mostras os desafios e perspectivas para a Marinha a fim de se prepararas novas ameaças do ciber espaço (PINTO, 2009).

Alencar apresenta o tema da Guerra Cibernética, sua importância no cenário atual, e os desafios da nova Era da Informação, caracterizada pela grande convergência das tecnologias dos computadores e das comunicações, empregadas para processar, transmitir e armazenar a informação. Em seguida, apresenta uma visão panorâmica da estratégia nacional de segurança cibernética dos EUA, da Rússia e da China, além de apresentar como o Brasil vem construindo os passos iniciais de sua trilha sobre o tema da Guerra Cibernética (ALENCAR, 2010).

3. METODOLOGIA

Para a realização do estudo, levando em consideração a complexidade do tema, e como pode ser aplicado de forma efetiva com mediadas que viabilizam uma maior preocupação da Marinha para a guerra, foram sugeridas determinadas medidas que se adequassem ao cenário atual do tema na Marinha.

A forma mais indicada para a execução desta tarefa, segue a classificação da maneira como foi realizada a pesquisa em lide, para que os objetivo geral seja alcançado, deixando de modo claro como cada levantamento e informação obtido.

3.1 Classificação da Pesquisa

Por meio de análise de fins e meios.

3.1.1 Quanto aos fins

Esta pesquisa terá natureza explicativa, apresentando as formas que a guerra cibernética vem sendo utilizada. Será ainda do tipo aplicada, pois apresentará conceitos já consolidados no âmbito militar para resolver um problema real que a Marinha etá passando. Não será, entretanto, desenvolvido nenhuma tecnologia, será apenas proposto uma solução, desvinculando essa pesquisa do caráter intervencionista.

3.1.2 Quanto aos meios

Será utilizado a revisão bibliográfica como fonte de coleta de dados para esse trabalho, através da revisão de teses e monografias que abordam se a marinha está ou não apta aos desafios e perspectivas de guerra cibernética. Possivelmente alguns objetivos não serão atingidos, por isso não estão listados na relação de objetivos específicos. Outros objetivos serão atingidos apenas parcialmente, devido a metodologia escolhida.

3.2 Limitações do Método

Este trabalho se limitará a uma pesquisa bibliográfica, por tal motivo não será desenvolvida nenhuma solução para o problema aqui proposto, serão apenas citadas medidas que poderão contribuir para formulação de uma doutrina de guerra cibernética dentro da Marinha do Brasil. A insuficiência de tempo hábil para a pesquisa influenciou bastante na metodologia adotada neste trabalho.

3.3 Coleta e Tratamento de Dados

A coleta de dados e informações foi feita através de revisão bibliográfica de trabalhos acadêmicos brasileiros e estrangeiros.

4. O BRASIL FRENTE AO CENÁRIO MUNDIAL DE SEGURANÇA CIBERNÉTICA

O Brasil é considerado um dos países mais vulneráveis do mundo em relação à segurança da informação (SI). Por possuir uma baixa produção cienífica nessa área o país é rotulado como “seguidor” por lançar tecnologias muito tempo depois dos outros países (PINHEIRO, 2011).

Devido a essas vulnerabilidades, cria-se o desafio de gerir a segurança do ciberespaço, uma vez que esta é muito mais do que apenas uma questãoo de soberania Nacional ou Defesa Militar, ela é uma questão integrada e, para tal, necessita de esforços dos setores civil e militar. Exemplos bem-sucedidos de medidas para o trato da gguerra cibernética devem ser seguidos como criar órgãos específicos para tal. Nos EUA já são estudados esse tipo de assunto há mais de uma década. Os mesmos possuem diversos órgãos que têm objetivos diretamente relacionados com a guerra cibernética. Podemos citar:

• *United States Cyber Command (Comando Cibernético dos Estados Unidos)*, cuja missão é coordenar a rede de computadores dos EUA contra-ataques cibernéticos;

• *National Security Agency (NSA) ou Agência de Segurança Nacional,* que tem por missão, dentre outras, operar o sistema de monitoramento global Echelon e proteger as comunicações relativas à segurança nacional, enquanto explora as de outros países;

• *National Computer Security Center - NCSC* (Centro Nacional de Segurança Computacional), que conduz a segurança dos sistemas de informação dentro da NSA;

• *Defense Information Systems Agency – DISA* (Agência de Defesa de Sistemas de Informação), que trata de segurança de TI no Departamento de Defesa;

• *Computer Emergency Response Team Coordination Center (CERT-CC)* que coordena várias outras equipes de resposta à emergência nos EUA;

• *Federal Computer Incident Response Center – FEDCIRC* (Centro Federal de Resposta a Incidentes em Computadores), que tem por missão prover uma ampla capacidade de resposta a incidentes no âmbito governamental;

• *Office of Science and Technology Policy – OSTP* (Escritório de Política Científica e Tecnológica), que coordena pesquisa e desenvolvimento em apoio à proteção de infraestruturas críticas;
• *Central Intelligence Agency – CIA* (Agência Central de Inteligência);
• *Federal Bureau of Investigation – FBI* (Escritório Federal de Investigação);
• *Defense Intelligence Office for Information Operations* (Gabinete de Informação da Defesa para as Operações de Informação), criado em virtude da necessidade de conhecer o potencial que eventuais adversários poderiam ter em realizar "ataques digitais" e, também, com o objetivo de apoiar as atividades relacionadas a information operations; e
• *Joint Task Force – Computer Network Operations - JTF-CNO* (Força Tarefa Conjunta – Operações de Rede de Computadores), responsável por ações defensivas e ofensivas de G Ciber;

Ressalta-se o United States Cyber Command como o principal órgão dos EUA que trata sobre Guerra Cibernética. É um comando conjunto para coordenar as atividades de Defesa Cibernética das Forças Armadas. Esse comando centraliza as operações americanas no ciberespaço melhorando a capacidade do Departamento de Defesa de garantir a segurança da informação e a confiabilidade das redes de comunicação (ALENCAR, 2010). A missão do United States Cyber Command compreende integrar as operações no ciberespaço e sincronizar os efeitos do combate, prestar apoio às autoridades civis e aos aliados internacionais, operar a Rede de Informação Global e executar sua defesa, executar operações militares no ciberespaço, coordenar, no âmbito do Departamento de Defesa, as operações ofensivas no ciberespaço de modo a evitar interferência entre as ações, aprimorar a consciência situacional das operaçõeses no ciberespaço, incluindo alertas, e compartilhá-la e representar o setor militar junto às agências nacionais e comerciais do governo e agências internacionais, nos assuntos relacionados ao ciberespaço, a fim de possibilitar ações em todos os domínios, assegurar a liberdade de ação no ciberespaço aos EUA e seus aliados e negá-la aos seus oponentes (ESTADOS UNIDOS DA AMÉRICA, 2010a, 2010b).

No Brasil em virtude da Estratégia Nacional de Defesa (END), o Exército Brasileiro criou o Centro de Defesa Cibernética que é encarregado de coordenar e integrar as atividades de defesa cibernética no âmbito do Ministério da Defesa (MD). Essa missão foi definida por portaria do MD e publicada em meados de 2012. Em outras palavras, isso significa que o Centro de Defesa Cibernética é uma Organização Militar (OM), responsável pela coordenação das ações de defesa cibernética e pela integração dos esforços das diversas organizações vocacionadas para atuação nesse setor, no âmbito do MD (DEFESA AÉREA E NAVAL, 2014).

No entanto, não existe no setor cibernético uma autoridade central para delegar tarefas, esforços e ditar caminhos a serem seguidos por organizações governamentais e privadas. A falta de definição das responsabilidades é consequência da descentralização do setor cibernético. Assim, não há uma definição sobre quem será o responsável pela retaliaçãoo, caso necessário, de um ataque à redes governamentais ou privadas do Brasil (CORDEIRO, 2015).

A criação e investimentos em diversos órgãos, tais como os citados, criados por potências como os Estados Unidos, mostra a seriedade que o assunto é tratado. Por ser rotineiro os relatos desses ataques, a invasão do espaço cibernético virou assunto cotidiano tanto no meio militar quanto no civil. O ano 2000 é marcado como um dos pioneiros em estratégias de ataque. A partir desse ano nações e grupos terroristas usaram hackers para atacar estrutura governamentais ou empresariais com fim político-ideológico. Em 2005 o governo Norte Coreano recrutou 500 hackers, que conseguiram penetrar nas redes governamentais da Coréia do Sul, Japão e outros países. Alvos não faltam para esses ataques: ferrovias, metros, hospitais, refinarias, polos químicos, oficinas federais, sistemas bancários e redes elétricas (PINHEIRO, 2011).

O Engenheiro Simon Rosental, integrante do Corpo Permanente da Escola Superior de Guerra (ESG), afirmou que as potencias mundiais não querem permitir que o Brasil e outros países emergentes tenham acesso ao que se chama de tecnologias sensíveis. Esse entrave faz com que o Brasil fique bastante defasado na corrida tecnológica contra os ataques cibernéticos (ROSENTAL, 2010). O resultado desse descompasse fica evidenciado na figura 1 que mostra a quantidade de ataques ocorridos no ano de 2010.

400 mil ataques somente no ano passado

Notificações de incidentes na internet, como tentativas de fraudes ou agressões a redes e páginas, quase triplicaram em 2010

	Incidentes	em 2011	%*	Legenda
	Worm	26.897	6	Processo automatizado de propagação de códigos maliciosos na rede
	DoS	272	0	Denial of Service: ataques tiram do ar um serviço, computador ou rede
	Invasão	106	0	Acesso não autorizado a um computador ou rede
	Web	15.491	3	Comprometimento de servidores *web* ou desfigurações de páginas na internet
	Scan	119.755	30	Varreduras em redes de computadores, amplamente usadas para identificar potenciais alvos vulneráveis
	Fraude	40.381	10	Incidentes em que ocorre tentativa de se obter vantagem
	Outros	196.613	49	
	Total	399.515	100	

* Valores aproximados

Fonte: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (Cert), mantido pelo Comitê Gestor da Internet no Brasil

Figura 1 – Tipos de incidentes ocorridos na internet no Brasil no ano de 2010 e uma previsão da quantidade de ataques para o ano de 2011 (ROSENTHAL, 2010).

Não resta dúvidas quanto à insegurança cibernética no mundo e em espacial no Brasil. Devido a debilidade em criação de mecanismos de segurança da informação e a não percepção da gravidade do assunto pelo Brasil, o país possui uma vasta lacuna a ser preenchida quando o assunto é a guerra no ciberespaço.

4.1 A Marinha no Ciberespaço

O Plano Estratégico da Marinha (PEM), em seu capítulo 6, define os objetivos navais da MB. Um destes objetivos aborda a necessidade de manter a segurança dos sistemas digitais de TI e de comunicações no Estado da Arte, a fim de se evitar ataques cibernéticos. No capítulo 11, em suas Diretrizes para o Planejamento Naval (DIPNAV) no setor de Ciência e Tecnologia e TI afirma-se que deve estabelecer ações para garantia do uso da informação de interesse da MB e negar a sua utilização de forma contrária (PINTO, 2009).

Com base no exposto, a partir de 2008, a guerra cibernética foi transferida para o setor de apoio. A Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) ficou responsável por elaborar normas, instruções técnicas e procedimentos padronizados para áreas de conhecimento concernentes ao emprego da Tecnologia da Informação na MB, incluindo a guerra cibernética. O Centro de Tecnologia da Informação da Marinha (CTIM) foi designado como Órgão de Execução Operacional para a guerra cibernética sendo responsável por operar os recursos tecnológicos, planejar os exercícios gerais sobre o assunto, subsidiar a DCTIM nos aspectos de capacitação técnica do pessoal envolvido com as atividades específicas de guerra cibernética e mobilizar o pessoal qualificado para o emprego em situações de conflito de acordo com a doutrina estabelecida pela MB (NUNES, 2010).

A atual estrutura de Governança de Tecnologia da Informação (GovTI) da MB implantada desde 2007, estabeleceu a guerra cibernética como um dos temas de interesse, estando inserida também no Plano de Tecnologia da Informação da Marinha (PTIM). Para execução das atividades de proteção cibernética, a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) é auxiliada, pelo Centro de Tecnologia da Informação da Marinha (CTIM) e por outras estruturas distribuídas pelas diversas regiões do País tais como os Centros Locais de Tecnologia da Informação (CLTI) para apoiar as quase 400 organizações militares.

A partir dessas mudanças, a MB vem aumentando sua preocupação no que diz respeito a segurança das informações e, consequentemente, a guerra cibernética. O Centro de Análises de Sistemas Navais (CASNAV) vem aprimorando uma forte infraestrutura em metodologias, softwares e equipes na área de

criptologia, análise de vulnerabilidade de software, técnicas de varredura e desenvolvimento de softwares seguros.

O projeto Guerra Cibernética Objetiva, que tem desenvolvido softwares inteligentes para minimizar ataques praticados nos sistemas de informações digitais da Marinha do Brasil e o Projeto Metodologia para Avaliação e Homologação de Aplicações de Sistemas Criptográficos (PINHEIRO, 2013).

Essas medidas são algumas das atividades de proteção empregadas pela MB e que são monitoradas e avaliadas de forma contínua, em busca de novas ameaças, à luz dos princípios aplicados à guerra cibernética, em consonância com as normas específicas para o assunto. Nos últimos anos foram realizados exercícios com simulações no espaço cibernético da Marinha visando explorar este novo domínio e sua importância para o Comando e Controle das Operações Militares, contando ainda, em algumas oportunidades, com a participação de especialistas das demais Forças, estreitando a integração e o compartilhamento do conhecimento (LIMA, 2014).

Estes são exemplos de projetos os quais demonstram o aumento da preocupação por parte da Marinha do Brasil frente a guerra cibernética. São marcos de ações indispensáveis ligados a Ciência, Tecnologia e Inovação, tendo como objetivo concorrer para a realização do desenvolvimento da estratégia da guerra cibernética que a Marinha está adotando para proteger com eficiência as fronteiras digitais do País.

5. CAPACITACÃO DOS MILITARES DA MARINHA DO BRASIL PARA GUERRA CIBERNÉTICA

O Livro Verde de Segurança Cibernética define vulnerabilidade como propriedade intrínseca de algo resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência. Também a define como o conjunto de fatores internos ou causa potencial de um incidente indesejado que podem resultar em risco para um sistema ou organização os quais podem ser evitados por uma ação interna de segurança da informação (BRASIL, 2010).

Neste trabalho as vulnerabilidades, quando o assunto é Guerra Cibernética, são tratadas como falta de pessoal capacitado na área, uma doutrina bem formulada e a melhoria dos meios de execução. É importante que haja um esforço para que essas lacunas sejam preenchidas, de maneira encontrar soluções e melhores práticas de segurança da infraestrutura crítica da informação que melhore a resposta e minimize os riscos cibernéticos.

A Guerra Cibernética depende de pessoal com alto nível de qualificação. No atual cenário potências mundiais sofrem ataques cibernéticos e se defendem dele. Investir na capacitação de pessoal é fundamental para que se possa ter as estruturas necessárias, para atuar efetivamente diante de investidas contra a Nação no ciberespaço e criar medidas de uma mentalidade da segurança da informação que estejam difundidas difundida entre seu pessoal.

Essa necessidade possui o desafio de atrair pessoas com esse tipo de qualificação. Na maioria dos casos esses profissionais tendem a buscar a iniciativa privada por possuir atrativos maiores quando comparados aos do setor público que muitas vezes não possuem tais atrativos (KRAMER, 2009; RATTRAY, 2009).

Para que possa eliminar as dependências de tecnologias e conhecimentos estrangeiros, algumas etapas devem ser estabelecidas a fim de garantir níveis aceitáveis contra atividades de GC e de segurança da informação (SI). Deve ser estabelecido um programa de capacitação e treinamento de segurança contra atividades de GC e de SI, com a meta de ter uma contínua capacitação, treinamento e educação de todos os setores da Marinha para atender às necessidades de ssegurança contra atividades de Guerra Cibernética e de Segurança da Informação (PINTO, 2009).

É observado que a dependência de recursos computacionais faz com que os conhecimentos sobre a GC demorem a ser atualizados no país e, consequentemente, nas FFAA. Porém, uma vez possuindo o conhecimento de que a GC é real, não existe mais a possibilidade de militares da MB não conhecerem as vulnerabilidades que um navio ou uma OM de terra podem ser expostos ao ter as portas USB dos computadores funcionais com livre acesso ou utilizar máquinas com sistemas operacionais sem atualização, por exemplo. É necessário desenvolver alternativas de trabalho, somando conhecimento para que possam ter a segurança necessária ao usar a rede e trafegar dados de elevada importância.

Assim, é verificado que a preparação dos militares para as novas ameaças que guerra cibernética expõem exige bastante atenção. Não se pode separar os fundamentos técnicos dos operativos pois, não se trata apenas de segurança cibernética, mas sim de ações desenvolvidas no ciberespaço em prol de uma operação militar. Para Nunes, tanto a parte técnica como a operativa devem trabalhar de forma conjunta, de maneira que uma venha atender as necessidades da outra (NUNES, 2010). Em concordância, Kevin Mitnick declarou que o fator humano é o principal culpado pela maioria das falhas de segurança que levam a invasões de sistemas, roubos de dados e golpes cibernéticos em geral (ALMEIDA, 2010).

Exemplificando a dimensão do problema quando um usuário não possui conhecimentos de segurança da informação, recorre-se a vulnerabilidade explorada em um dos principais comandos dos EUA, o *U.S. Central Command*. Militares lotados nesse comando sem os conhecimentos específicos de segurança cibernética aliados ao impulso da curiosidade, utilizaram *pen-drives* infectados que foram deixados em locais próximos ao *U.S. Central Command*, comprometendo os sistemas mais sigilosos e expondo todo o tráfego de dados, comunicações e operações durante várias semanas (PINTO, 2009).

Este exemplo serve como ensinamento aos militares da MB. Deve-se difundir a mentalidade de segurança, o entendimento que cada computador ligado à Rede Integrada de Comunicações da Marinha pode ser alvo a qualquer momento de um ataque é primordial. A SI é o resultado da equação de pessoas somadas a processos e tecnologia como mostrado na figura 2 (informação verbal)[1].

1 Informação fornecida em aula ministrada ao Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações no CIAW).

Essa equação serve para elucidar que com tais conhecimentos os usuários terão a consciência que a defesa da MB começa na sua estação de trabalho, sendo este pensamento o principal motivador para a criação de uma conscientização de segurança em todos os usuários.

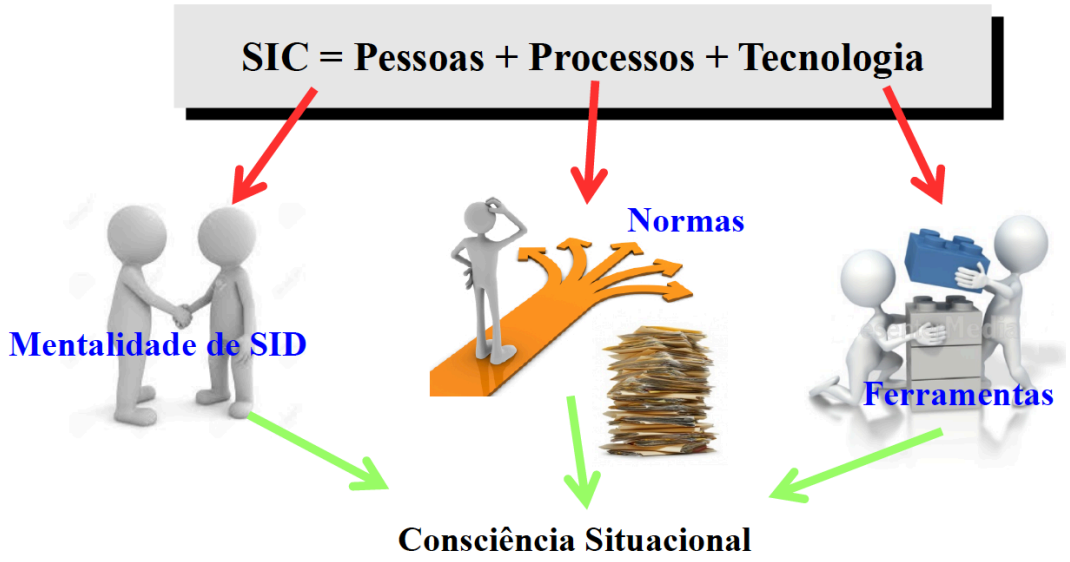

Figura 2 – Equação de Segurança da Informação (CERVEIRA, 2018).

A barreira a ser transposta é a formação desses militares. Atualmente a MB possui cursos que ministram esse tema aos seus alunos porém, os assuntos ministrados deveriam ser de conhecimento de todos. Como forma de solucionar essa lacuna, a disciplina de segurança da informação poderia ser iniciada nas escolas de formação de oficiais e praças. Na Escola Naval e CIAW os oficiais poderiam aprender assuntos relacionados ao tema bem como as atribuições do Oficial de Segurança da Informação e Comunicações. Já nas Escolas de Aprendizes seriam ministrados assuntos relacionados ao tema e os deveres do administrador da rede.

6. ATAQUES CIBERNÉTICOS

Com relação aos setores de importância estratégica, o qual é fruto das diretrizes estabelecidas na Estratégia Nacional de Defesa (END), o Ministério da Defesa definiu o Exército Brasileiro como responsável pelo setor cibernético (BRASIL, 2009a, 2009b). Porém, vale ressaltar que esse assunto é de suma importância a todas as FFAA brasileiras, uma vez que são utilizadoras de sistemas baseados em redes.

Devido às pressões comercias para o desenvolvimento de produtos de TI, graças ao grande fluxo tecnológico, a indústria de software, em geral, tem deixado a segurança ao segundo plano. Com a tendência de lançar produtos o mais rápido possível e somente disponibilizar as correções à medida que os erros são detectados, fica notória, entre os profissionais de segurança da informação, a existência de vulnerabilidades conhecidas exclusivamente por determinados grupos, normalmente pertencentes ao submundo cibernético (COLARIK E JANCZEWSKI, 2008; CSIS, 2008; SHIMEALL *et al.*, 2002).

A MB é utilizadora de enlaces providos por empresas privadas para ligar *Wide Area Network (WAN's)* distritais. Essa interligação propicia a ocorrência de riscos como: interrupção de fluxo normal, interceptarão de mensagem, interceptação com alteração da mensagem ou falsa identidade (BRASIL, 2017).

Essas soluções comerciais proporcionam uma falta de segurança na infraestrutura de tecnologia e com isso tornam as redes da MB vulneráveis diante do aumento das ameaças que causam prejuízos em seus respectivos sistemas de informação. A falta de controle do ambiente tecnológico é uma grande vulnerabilidade e, na maioria das vezes, não é possível quantificar o prejuízo com os problemas de segurança e nem mesmo ter ciência dos ataques. Para se proteger dessas ações, torna-se necessário conhecer profundamente tanto o ataque como a filosofia dos atacantes, pois, desta forma, será possível escolher a melhor contramedida a ser empregada.

Como forma de elucidar as formas de ataques, entende-se exploração cibernética como ações de busca ou coleta nas redes de dados ou sistemas do inimigo, a fim de obter informações relevantes que podem ser empregadas em

proveito da inteligência ou podem servir de subsídio para o planejamento de um ataque cibernético propriamente dito (MINISTÉRIO DA DEFESA, 2012).

Durante a exploração cibernética, o atacante utiliza todas as ferramentas à disposição para levantar informações a respeito do alvo, explorando vulnerabilidades na infraestrutura de sua rede de dados, em algum software e/ou servidor, ou em erros de contrainteligência dos operadores e/ou administradores. Para atingir tal objetivo, a exploração poderá fazer uso, inclusive, de técnicas de invasão, desde que não causem danos ou prejuízos aos sistemas e redes de dados do oponente. As sequências desses ataques são mostradas na figura 3.

O ataque cibernético é mais contundente, pois compreende em ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente (MINISTÉRIO DA DEFESA, 2012).

A engenharia social também é uma forma de ataque e tem-se mostrado bastante eficaz. Por intermédio dela, tenta-se iludir a vítima para que acredite nas informações prestadas e se convença a executar alguma tarefa ou usar algum aplicativo que venha a causar danos ao computador ou à rede como um todo. É importante destacar que, nesse tipo de ataque, a principal vulnerabilidade é a vítima, que não possui a devida conscientização sobre os perigos que correm por acreditar em todas as informações que chegam até ela. A figura 4 evidencia os impactos que um ataque cibernético causa em um Sistema de Comandos e Controle.

Nesse contexto a GC é entendida como ações militares no espaço cibernético conduzidas com o propósito de negar, explorar, destruir ou comprometer a integridade de ativos do adversário baseados em informações, sistemas de informações e redes de computadores. Assim, sua inserção no Planejamento Estratégico Militar, principalmente no que tange às medidas de dissuasão, é imprescindível e torna-se possível por meio da classificação das ações cibernéticas que são divididas em ataque, exploração e proteção cibernéticas (LIMA, 2014).

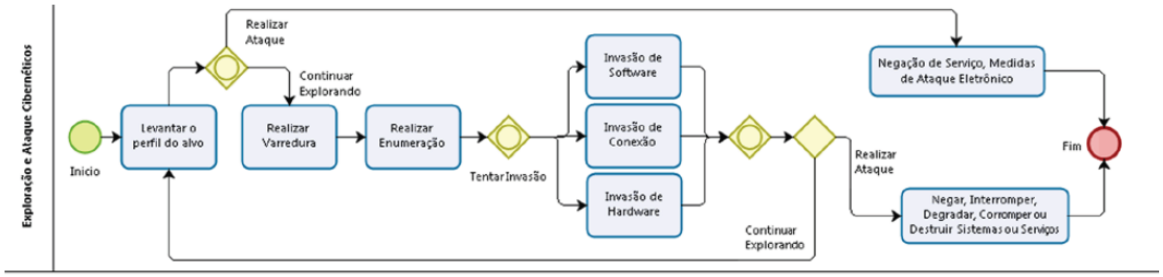

Figura 3 – Sequência de Ações nas Fases de Exploração e Ataque Cibernéticos (GOMES *et al.*, 2016).

Figura 4 – Impactos de ações cibernéticas contra um sistema de Comando e Controle (GOMES *et al.*, 2016).

6.1 Proteção para sistemas baseados em redes

Não existe 100% de eficácia quando o assunto é proteção rede de dados. Ter o equilíbrio entre utilização e segurança é tarefa árdua para os administradores de redes nos dias atuais. Ao adotar a premissa de que a segurança perfeita é inexequível, a principal estratégia por trás de um bom projeto de contramedidas se torna simples que é aumentar o custo de um ataque de modo que o investimento nele se torne alto demais em comparação com o ganho obtido pelo invasor.

Para se atingir a proteção de sistemas baseados em redes de dados, inicialmente, três medidas são fundamentais no planejamento de contramedidas: prevenir, detectar e responder (JUNIOR, 2010). Desta forma, todo planejamento de proteção e resposta a ataques cibernéticos deve conter medidas preventivas e repressivas (figura 5). As ações de prevenção devem atuar na detecção de vulnerabilidades. Já as medidas repressivas deverão ser as respostas propriamente ditas aos incidentes.

As medidas de segurança cibernética também podem ser divididas em três tipos conforme sua orientação. Primeiramente podem ter medidas técnicas, orientadas ao uso de recursos de TI e voltados à segurança, como sistemas de detecção de intrusão, firewalls, recursos criptográficos, ferramentas de análise de rede entre outras. A segunda refere-se às políticas e doutrinas de segurança, ou seja, são medidas orientadas ao processo. Já o terceiro tipo está relacionado às medidas orientadas aos usuários que se referem à conscientização de segurança voltada às boas práticas no uso de sistemas de informação (NUNES, 2010).

Existe também a possibilidade de estruturação de um plano de contramedidas, baseados em cinco camadas de TI tais como física, rede, host ou computador, aplicação e lógica. Por intermédio desse tipo de estratégia torna-se possível corrigir vulnerabilidades em cada ponto de junção, impondo barreiras às diferentes formas de invasão (JUNIOR, 2010).

Sun Tzu afirma que é tão importante conhecer o inimigo como a si mesmo. Este princípio deve ser empregado na GC. É preciso explorar o próprio espaço cibernético em busca de vulnerabilidades que possam ser empregadas pelos adversários. Simulações de ataque em sistemas ou rede de computadores da MB, através de exercícios operativos, propiciam as condições necessárias para

aprimoramento dos sistemas de proteção e dos usuários. Com a utilização dessas simulações será possível adotar uma escala progressiva dos níveis de alarmes cibernéticos e contribuirá para execução de ações reativas com proporcional dispêndio de esforço e, de custos compatíveis com os riscos identificados, nos exercícios ou em situações reais, contribuindo para minimizar ou neutralizar o efeito indesejável do ataque sofrido (LIMA, 2014).

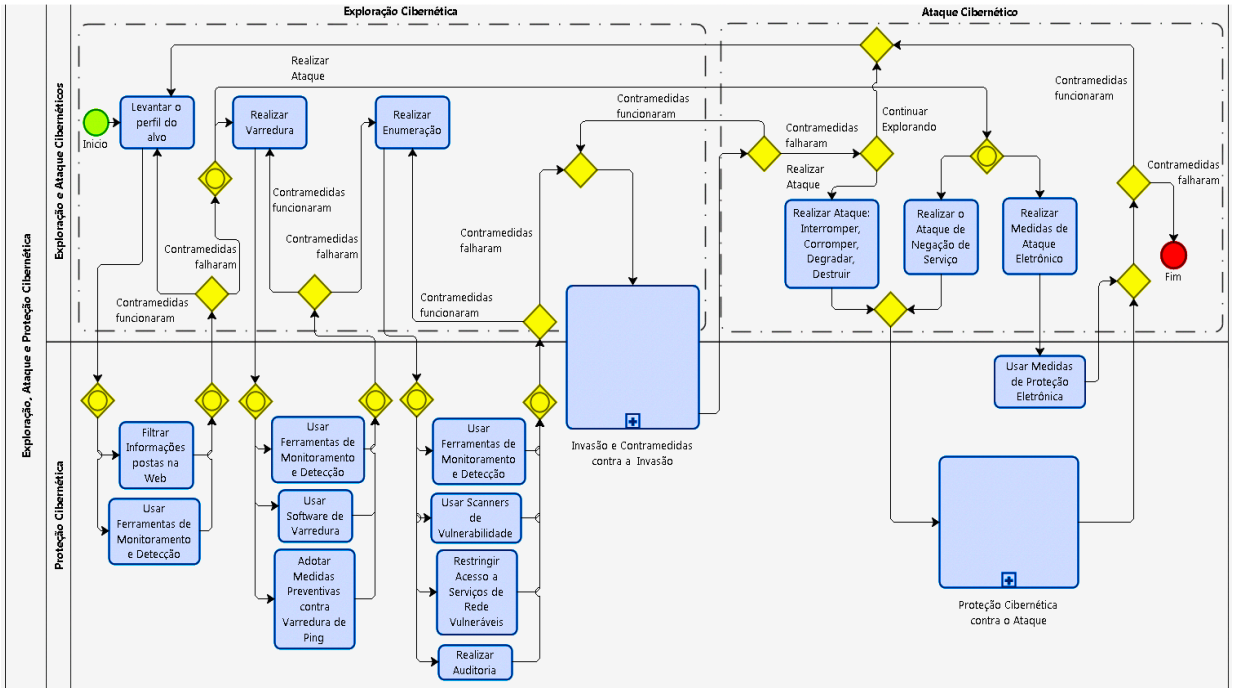

Figura 5 - Sequência de Ações e Proteções Cibernéticas nas Fases de Exploração e Ataque Cibernético (GOMES *et al.*, 2016).

6.2 Os Desafios da Guerra Cibernética para Marinha do Brasil

A eficácia das ações de defesa cibernética depende fundamentalmente da atuação colaborativa da sociedade brasileira incluindo, não apenas o Ministério da Defesa, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. As atividades de defesa cibernética no MD são orientadas para atender às necessidades da defesa nacional. Para isso, a capacitação tecnológica do setor cibernético deve ser buscada de maneira harmônica com a política de ciência, tecnologia e inovação para a defesa nacional.

Entretanto, a decisão de alguns governos de investir em poderio cibernético e tecnologias nessa área ainda enfrentam alguns obstáculos, entre eles, a falta de conscientização sobre a importância do assunto. No caso do Brasil, depois da confirmação por parte do ex-agente norte americano Edward Snowden, a agência de Segurança Nacional dos EUA dispõe de um sistema que monitora as comunicações dentro e fora do país. Ainda que fosse comprovado a espionagem da Ex-Presidente da República Dilma Rousseff e da Petrobras, a reação do governo brasileiro foi contundente, mas limitou-se a esfera diplomática onde mais uma vez não foi levado em consideração a utilização de contramedidas a GC (FERRAÇO, 2014).

As ferramentas na Guerra Cibernética são produtos sucetíveis a adaptações conforme o ambiente que irão ser empregadas. Essas ferramentas podem ser empregadas como alternativas para uma estratégia de guerra assimétrica, maximizando os efeitos de uma atividade ofensiva, porém com um reduzido custo para o atacante. Assim, o emprego eficaz da Guerra Cibernética pode ter soluções bastante simplificadas para o atacante, contrastando com uma complexidade crescente para o defensor (ALENCAR, 2010).

Logo, adquirir ferramentas de defesa cibernética fornecidas por governos ou empresas estrangeiras é uma solução de alto risco. Certamente, caso a Marinha ou qualquer órgão do governo venha a ser alvo de ataque, essas soluções poderão ter suas funções neutralizadas, tornadas sem uso seja por sua inutilização por meio de desligamento digital ou por meio da venda de contramedidas a nossos possíveis adversários, além de constituírem grave ameaça à segurança de nossos próprios sistemas, que poderão estar sendo vítimas de ações de exploração. Na pior das hipóteses, esses programas poderão conter códigos que as façam se voltar contra nossas próprias forças (PINTO, 2010).

Fruto dessa preocupação existe a necessidade em fomentar o desenvolvimento de soluções nacionais para esse tema. Até dezembro de 2013, diversas ações foram concretizadas tais como a instalação de laboratórios de pesquisa junto a representantes do sistema acadêmico nas escolas militares e em diversas instituições civis parceiras. São exemplos dessa integração, os laboratórios criados e os trabalhos realizados na Universidade de Brasília, que desenvolvem protocolos, o Centro de Análises de Sistemas Navais da Marinha do Brasil (CASNAV), que se dedica a trabalhos na área de criptografia, o Centro de Tecnologia da Informação “Renato Archer”, em Campinas, São Paulo, que estuda

técnicas de implementação e a Universidade Federal de Campina Grande, na Paraíba, que produz conhecimento nas áreas de computação e criptografia quântica (DEFESA AÉREA E NAVAL, 2014).

Essas integrações são apoiadas pelo diretor do DSI e permitirá a MB por intermédio do Centro de Análise de Sistema Navais (CASNAV) a desenvolver suas ferramentas de neutralizações de ameaças. A partir desses estudos e com os conhecimentos adquiridos para proteção desses ataques, será possível a criação de armas cibernéticas nacionais que poderão ser usadas oportunamente em um ataque e livrará a MB da dependência de tecnologia estrangeira (JUNIOR, 2009).

7. CONCLUSÃO

Os usuários do espaço cibernético aumentam exponencialmente a cada dia. Esse aumento acontece por conta da internet onde, atualmente, não existe uma política de segurança e controles bem definidos. Por tal motivo existe uma proliferação de criminosos e, consequentemente, atos criminosos no ciberespaço.

A Guerra Cibernética vem despontando com um potencial considerável. Suas ações podem desestruturar esses sistemas e prejudicar a tomada de decisão precisa e oportuna. Desta maneira, conhecer suas formas de ataque e defesa permite identificar contramedidas que possam ser tomadas no intuito de eliminar ou pelo menos reduzir os seus efeitos sobre os sistemas.

A complexidade e dimensão das atividades civis e militares levam a uma dependência dos sistemas corporativos, que armazenam informações não mais disponíveis de outra forma. As FFAA não podem permitir a invasão nos sistemas computacionais pois, tais atos podem inviabilizar toda uma estratégia de defesa e levar um país ao caos pela sua total paralisia estratégica.

Esse trabalho mostra a dimensão cibernética como uma nova infraestrutura a ser cuidada pelo Brasil. Devido a suas debilidades, as atividades nela ocorridas refletem sobremaneira no mundo real e tem-se mostrado bastante crítica. Dessa forma é necessário incrementar o setor cibernético nas FFAA, em função do aumento de sua importância para a soberania nacional e das fragilidades de segurança em TI.

O estabelecimento da capacidade tecnológica para reagir ou se defender contra atividades de Guerra Cibernética pode contribuir para a redução do fosso digital que os países mais avançados no setor cibernético impõem aos países menos desenvolvidos nesta área. Os exemplos de países desenvolvidos devem ser seguidos citando os EUA e os órgão governamentais que tratam do assunto como exemplos a serem seguidos em termos de defesa contra-ataques cibernéticos. O assunto da guerra no ciberespaço tem ganhado força dentro da MB e esta ainda precisa de mais investimentos em tecnologias e conhecimento que poderão contribuir para proteção das fronteiras digitais do país.

.

A necessidade de investimento na preparação de recursos humanos para a condução das ações da Guerra Cibernética deve envolver, necessariamente, as vertentes técnica e operativa. Nesse sentido, a sugestão de incluir no currículo de formação de pessoal da MB, iniciando a preparação de oficiais e praças em matérias que geram o conhecimento relacionado aos assuntos pertinentes à segurança da informação e complementar com um curso de aperfeiçoamento específico, nos moldes do curso de Segurança da Informação e Comunicações (SIC). Concluindo a formação desses profissionais seria importante juntar os conhecimentos da parte operativa com a técnica numa turma composta de Oficiais combatentes e técnicos. Compartilhar conhecimentos de ambas as partes contribuiria para formular combatentes com conhecimentos sobre guerra cibernética e técnicos com dimensão real das particularidades de um navio.

Para que a MB possa se proteger das ações de ataque e exploração, torna-se necessário conhecer profundamente tanto o ataque como a filosofia dos atacantes. Desta forma será possível escolher a melhor contramedida a ser empregada. Ainda que não existam sistemas 100% seguros. Um equilíbrio entre utilização e segurança de redes é necessário para que a segurança e a soberania nacional sejam garantidas.

Por fim, a aquisição do conhecimento, a antecipação dos riscos e a pronta resposta a um possível ataque cibernético exige do momento atual que a Marinha desenvolva as capacidades necessárias para enfrentar os desafios do presente e as incertezas do amanhã.

7.1 Considerações Finais

O investimento na formação de pessoal próprio deve ter início nos cursos de formação de oficiais e praças. Atualmente esses cursos não fazem menção ao tema Guerra Cibernética. É necessário a introdução de matérias relacionadas aos fundamentos de segurança cibernética para fundamentar a importância de segurança das informações digitais em todo os setores da Marinha do Brasil. Atualmente os alunos recebem o primeiro contato com assuntos relacionados a SI a partir do Curso de Aperfeiçoamento (CAp) ou em alguns cursos expeditos. Esse contato com tema é muito tardio uma vez que nem todos terão a oportunidade de

cursar ou terão uma lacuna de alguns anos com assunto até o CAp. No caso dos oficiais que desejarem aprofundar e estudar disciplinas mais específicas sobre o assunto podem entrar no Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações (CApA-SIC) o qual ministra matérias que permitem o conhecimento relacionados a guerra cibernética. Assim os alunos têm contato com matérias que abordam vários temas do ciberespaço e, difundir esse conhecimento é fundamental para aprofundamento sobre a segurança das informações digitais. Por mais que não formem especialistas em guerra cibernética, esses cursos contribuem para conscientizar os oficiais e praças sobre as vulnerabilidades que as redes da MB estão expostas e como utilizar as técnicas de defesa e ataque para proteção.

Com isso, a hipótese de que a capacitação de pessoal especializado, a normatização de procedimentos com base em uma nova doutrina de conhecimento sobre a GC e a melhoria dos meios físicos, técnicos e de desenvolvimento de novos softwares são imprescindíveis para fazer frente ao avanço ao combate à Guerra Cibernética. Acredita-se que as principais razões que levam a uma maior vulnerabilidade cibernética da MB são a dependência externa de sistemas corporativos, pesquisa incipiente na área de segurança da informação, falta de procedimentos para respostas à incidentes, falta de uma cultura de segurança da informação e pequena dotação de recursos financeiros.

Dessa forma, a aquisição do conhecimento, a antecipação dos riscos e a pronta resposta à um possível ataque cibernético exige do momento atual que a Marinha desenvolva as capacidades necessárias para enfrentar os desafios do presente e as incertezas do amanhã. É necessário um esforço coordenado e integrado do Ministério da Defesa (MD) e das outras Forças com as demais áreas governamentais e privadas com interesses e responsabilidades semelhantes. Estes projetos são formas indispensáveis ao desenvolvimento de uma possível solução ao desenvolvimento da estratégia contra a guerra cibernética que a Marinha poderá adotar para proteger com eficiência as fronteiras digitais do País.

7.2 Sugestões para Trabalhos Futuros

Sugere-se as abordagens para futuros trabalho:

- Analisar as vulnerabilidades no que tange aos *backdoor,* devido aos roteadores utilizados pela Marinha do Brasil;

- Implementação da mentalidade de segurança da informação nas organizações militares da Marinha do Brasil.

REFERÊNCIAS BIBLIOGRÁFICAS

ALMEIDA, Eduardo. Ex-hacker mais procurado dos EUA ensina na Campus Party como evitar ser vítima de golpes cibernéticos. O Globo.
Disponível em: <https://oglobo.globo.com/sociedade/tecnologia/ex-hacker-mais-procurado-dos-eua-ensina-na-campus-party-como-evitar-ser-vitima-de-golpes-3062457>. Acessado em 18 de maio de 2018.

ALENCAR, M.F. Guerra Cibernética: cenário atual e perspectivas. Escola de Comando e Estado Maior do Exército Naval. Trabalho de monografia como requisito parcial para obtenção do título de Especialista em Ciências Militares. Escola de Comando e Estado Maior do Exército, Rio de Janeiro, 2010.

BRASIL. Ministério da Defesa. Diretriz Ministerial número 14. Integração e Coordenação dos Setores Estratégicos da Defesa. Brasília, 9 nov. 2009a.

BRASIL. Gabinete do Comandante do Exército. Ofício número 1046, de 22 de dezembro de 2009, ao Chefe de Gabinete do Ministro de Estado da Defesa. Integração e Coordenação dos Setores Estratégicos da Defesa. Brasília, 22 de dezembro de 2009b.

BRASIL. Ministério da Defesa. Estratégia Nacional de Defesa: paz e segurança para o Brasil. Brasília, 2008.

BRASIL. Diretoria-Geral do Material da Marinha. DGMM-540: Normas de Tecnologia da Informação da Marinha. 2 rev. Rio de Janeiro, 2017.

CERVEIRA, C.R. Agenda da Diretoria de Comunicações e Tecnologia da Informação da Marinha, 2018. Material apresentado para disciplina de Virtualização e Computação em Nuvem para Curso de Aperfeiçoamento Avançado para Oficiais da parceria PUC-Rio – CIAW.

COLARIK, A.M., JANCZEWSKI, L.J. Cyber Warfare and Cyber Terrorism. Hershey, EUA: Information Science Reference, p.532, 2008.

DEFESA AÉREA E NAVAL. Defesa cibernética descomplicada. Disponível em: <http://www.defesaaereanaval.com.br/defesa-cibernetica-descomplicada>. Acessado em 18 de maio de 2018.

ESTADOS UNIDOS DA AMÉRICA. Senado Federal. Advanced Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command. EUA, p 32, 2010a.

ESTADOS UNIDOS DA AMÉRICA. U.S. Cyber Command Fact Sheet. EUA, 25 maio 2010b. Disponível em:<http://www.defense.gov/home/features/2010/0410 >. Acessado em 01 de maio de 2018.

GOMES. M. G. F. M, CORDEIRO. S. S, PINHEIRO. W. A. A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle. *Revista Militar de Ciência e Tecnologia*: Edição Brasileira, Rio de Janeiro, BRASIL, v. 33, n. 2, p.11-18, 1. trim. 2016.

JUNIOR, M.R. Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético Brasileiro. 2009b. 156 f. Especialização em Ciência da Computação: Gestão da Segurança da Informação e Comunicações – Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2009.

KAMAL, A. The Law of Cyber-space - an invitation to the table of negotiations. 1a. ed. Suiça: UNITAR - United Nations Institute of Training and Research, 2005.

KRAMER, F. D. Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. Cyberpower and National Security. 1. ed. Dulles, EUA: National Defense University Press and Potomac Books, cap. 1, p. 3-23, 2009.

LIMA, G.M.P.S. Cibernética: A Guerra em Curso . Revista Marítima Brasileira: Edição Brasileira, Rio de Janeiro, BRASIL, v. 134, n. 01/03, p.178-190, 1. trim. 2014.

MINISTÉRIO DA DEFESA. Política Cibernética de Defesa - MD31-P-02. 1. ed. Brasília, DF, 2012.

NUNES, L.A.R. Guerra cibernética: Está a MB preparada para enfrentá-la? Escola de Guerra Naval. Trabalho de monografia de conclusão do curso de política e Estratégia Marítimas. Escola de Guerra Naval, Rio de Janeiro, 2010.

O GLOBO - Ataque Cibernético na Europa
<https://g1.globo.com/tecnologia/noticia/ucrania-e-empresas-da-europa-sao-alvo-de-ataque-cibernetico.ghtml >.
Acessado em 10 de fevereiro 2018.

PINHEIRO, F.P. A Cibernética como Arma de Combate**.** Escola Superior de Guerra. Trabalho de monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia. Escola Superior de Guerra, Rio de Janeiro, 2013.

PINTO, M.L.S. Guerra cibernética na MB: desafios e perspectivas para próxima década. Escola de Guerra Naval. Trabalho de monografia de conclusão do curso de política e Estratégia Marítimas. Escola de Guerra Naval, Rio de Janeiro, 2010.

FERRAÇO, R. Espionagem Cibernética Rede Vulnerável. Revista em Discussão: Edição Brasileira, Brasil, Brasília, v. 5, n. 21, p.7, 2. trim. 2014.

ROSENTAL, S. Tecnologias Sensíveis**.** Escola Superior de Guerra. Trabalho de monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia. Escola Superior de Guerra, Rio de Janeiro, 2008.

SALDAN, Eliane. Doutrina precisa definir guerra cibernética. Disponível em: <http://www.conjur.com.br/2011-ago-06/guerra- -cibernetica-urgentemente-definicao-doutrina>.
Acessado em 21 de maio de 2018.