UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE ESTUDOS ESTRATÉGICOS
MBA EM ESTUDOS ESTRATÉGICOS E RELAÇÕES INTERNACIONAIS

LEONARDO MATTOS DE PAULA

A MARINHA DO BRASIL E AS AMEAÇAS CIBERNÉTICAS

Niterói
2021

LEONARDO MATTOS DE PAULA

A MARINHA DO BRASIL E AS AMEAÇAS CIBERNÉTICAS

Trabalho de conclusão de curso de MBA apresentado ao Instituto de Estudos Estratégicos da Universidade Federal Fluminense com parceria ao Centro de Instrução Sylvio de Camargo (Marinha do Brasil) como requisito parcial para a obtenção do título de MBA em Estudos Estratégicos e Relações Internacionais.

Orientador: Prof. Dr. Vitelio Marcos Brustolin

Niterói
2021

Folha de Aprovação de Trabalho de Conclusão de Curso em Relações Internacionais (Monografia)

Título do Trabalho: A Marinha do Brasil e as Ameaças Cibernéticas

Aluno: Leonardo Mattos de Paula

Avaliadores

_____

Avaliador 01: Prof. Dr. Vitelio Marcos Brustolin

_____

Avaliador 02: Prof. Dr. Márcio Rocha

Notas dos Avaliadores	
Nota 1	
Nota 2	

RESUMO

Percebemos que a guerra tradicional como nós a conhecíamos deixou de ser considerada como a principal ameaça global; hoje diversas outras questões afetam o mundo igualmente. Nesse contexto de novas ameaças, surgem as ameaças cibernéticas, colocando em risco a integridade de infraestruturas críticas, essenciais à operação de diversos sistemas relacionados à segurança nacional. Verificamos que essas ameaças cibernéticas passam a representar um perigo cada vez maior para as nações. A proteção do espaço cibernético abrange um grande número de áreas, incluindo, a proteção dos ativos de informação, de infraestruturas críticas e a capacidade de atuação em rede. O objetivo desta pesquisa é analisar a presença da Marinha do Brasil no Espaço Cibernético, mostrando se a Marinha está preparada para enfrentar as ameaças cibernéticas. Para isso, foi realizada uma pesquisa bibliográfica de artigos científicos, teses e livros que abordem o tema sobre o Espaço Cibernético, bem como o estudo da atual doutrina cibernética da Marinha do Brasil.

Palavras-chave: Cibernética, Domínio Cibernético, Defesa Cibernética, Espaço Cibernético, Guerra Cibernética, Ameaça Cibernética

ABSTRACT

We realized that the traditional war as we knew it, it is no longer considered as the main global threat, today several other issues affect the world equally. In this context of new threats, cyber threats arise, putting at risk the integrity of critical infrastructure, essential to the operation of various systems related to national security. We see that these cyber threats pose an ever-increasing danger to nations. The protection of cyberspace covers a large number of areas, including the protection of information assets, critical infrastructure and the ability to act in a network. The objective of this research is to analyze the presence of the Brazilian Navy in Cyber Space, showing whether the Navy is prepared to face cyber threats. For this, bibliographic research of scientific articles, theses and books that address the topic of Cyberspace was carried out, as well as the study of the current cybernetic doctrine of the Brazilian Navy.

Key-Words: Cybernetics, Cyber Domain, Cyber Security, Cyber Space, Cyber War, Cyber Threat

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ADMIN - Administrador da rede local

AGCiber - Ações de Guerra Cibernética

APF - Administração Pública Federal

BGP - *Border Gateway Protocol*

CASNAV - Centro de Análises de Sistemas Navais

CASOP - Centro de Apoio a Sistemas Operativos

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CIM - Centro de Inteligência da Marinha

CLTI - Centros Locais de Tecnologia da Informação

CSRECIM - Central de Suporte aos Serviços e Ativos da RECIM

CTIM - Centro de Tecnologia da Informação da Marinha

CTIR Gov - Centro de tratamento e resposta de incidentes nas redes de computadores da APF

ComOpNav - Comando de Operações Navais

CoNavOpEsp - Comando Naval de Operações Especiais

COTEC-TIC - Comissão Técnica de Tecnologia da Informação e Comunicações

COTIM - Conselho de Tecnologia da Informação da Marinha

DCTIM - Diretoria de Comunicações e Tecnologia da Informação da Marinha

DDoS - Ataque Distribuído de Negação de Serviço

DGMM - Diretoria Geral do Material da Marinha

DN – Distrito Naval

DNS - Sistema de Nomes de Domínio

DSIC - Departamento de Segurança da Informação e Comunicações

EMA - Estado Maior da Armada

END - Estratégia Nacional de Defesa

FA - Forças Armadas

GC - Guerra Cibernética

GSI-PR - Gabinete de Segurança Institucional da Presidência da República

ICANN - *Internet Corporation for Assigned Names and Numbers*

ISIC - Instrução de Segurança da Informação e Comunicações

ISP - Provedores de Serviço de Internet

LAN - Rede Local

MAN - Rede Metropolitana

MB – Marinha do Brasil

MD - Ministério da Defesa

NSA - *National Security Agency*

OCDE - Organização para Cooperação e Desenvolvimento Econômico

OM - Organizações Militares

OSIC - Oficial de Segurança da informação e Comunicações

PETIM - Plano Estratégico de Tecnologia da Informação da Marinha

PND - Política Nacional de Defesa

RCC - Recursos Computacionais Críticos

RECIM - Rede de Comunicações Integradas da Marinha

SCF - Sistema Ciber-Físico

SGDC - Satélite Geoestacionário de Defesa e Comunicações Estratégicas

SGSI - Sistema de Gestão da Segurança da Informação

SIC - Segurança da Informação e Comunicações

SID - Segurança da Informação Digital

SMDC - Sistema Militar de Defesa Cibernética

TI - Tecnologia da Informação

USCYBERCOM - Comando Cibernético dos Estados Unidos

VPN - *Virtual Private Network*

WAN - Rede de Grande Área

SUMÁRIO

1. INTRODUÇÃO

Se pudermos definir a sociedade atual, seria aquela em qual predominam a tecnologia da comunicação e da informação, seja através da Internet ou das Redes Sociais, estamos conectados em todas as atividades diárias, sejam elas sociais ou profissionais. Estamos vivendo em um mundo onde a tecnologia já permeia toda a sociedade, com isso percebemos que a guerra tradicional como nós a conhecíamos, descrita classicamente pelo emprego do fogo, da manobra e da violência, deixou de ser considerada como a principal ameaça global, hoje diversas outras questões como: políticas, econômicas, culturais, diplomáticas, étnicas, religiosas, e até pandêmicas afetam o mundo igualmente, sendo os danos sofridos comparáveis ao de um conflito regular.

Essa utilização de forma indiscriminada da tecnologia pela sociedade, através da contínua evolução tecnológica das redes sociais e de dispositivos móveis inteligentes, tornou-se uma porta de entrada para a exploração de vulnerabilidades das redes de computadores e para o acesso a qualquer tipo de informação, seja ela sigilosa ou não.

A informação é um bem de valor intangível e nem sempre mensurado. Atualmente, os maiores repositórios de informações são os ambientes computacionais, especialmente os interconectados por redes. Para proteger as informações, tais ambientes devem ser considerados seguros, sendo fundamental que eles sejam sempre protegidos adequadamente.

Nesse contexto tecnológico de novas ameaças, surgem as ameaças cibernéticas, vislumbrado por Joseph Nye (2009) como um dos Desafios Transnacionais à Segurança no período pós-Guerra Fria. A ameaça cibernética tornou-se uma preocupação, colocando em risco a integridade de infraestruturas críticas, essenciais à diversos sistemas relacionados à segurança nacional.

Verificamos que as ameaças cibernéticas passam a representar um perigo cada vez maior para as nações soberanas, além de sérios adversários para qualquer Exército nacional. Todas os Estados que desejam permanecer soberanos, já deram início à ampliação das fronteiras da segurança, estendendo-as ao espaço cibernético, ampliando o tradicional conceito de domínio territorial para incorporar, também, os interesses nacionais. Dispor apenas de armas tradicionais para a Segurança Nacional, no amplo nível da segurança a que nos referimos, não é mais o suficiente.

“A proteção do espaço cibernético abrange um grande número de áreas, como capacitação, inteligência, 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, 2017, p.59).

No cenário da Marinha do Brasil, as redes estão cada vez mais conectadas, chegando aos meios navais e Organizações Militares no Brasil e exterior. Com isto, a informação fica exposta a uma "variedade de ameaças e vulnerabilidades inerentes aos sistemas, protocolos de rede, configurações e compartilhamento dos canais de transmissão e recepção de dados, voz e vídeo". (BRASIL, 2019, p.III-2).

A pesquisa se justifica devido à grande relevância do tema na geopolítica atual, pois a questão do Espaço Cibernético vem se tornando a área dos novos conflitos, com vários exemplos de ataques cibernéticos realizados pelo mundo. Em concordância com este importante tema o Estado brasileiro através da Estratégia Nacional de Defesa (2017), definiu o setor cibernético, junto com o setor nuclear e o setor espacial, um dos três setores tecnológicos essenciais para a Defesa Nacional. Portanto, são considerados estratégicos e devem ser fortalecidos. Mais especificamente na Marinha do Brasil (MB), alinhados com a Estratégia Nacional de Defesa, na elaboração dos projetos de articulação, obtenção e modernização de meios e equipamentos da Marinha, foi considerado como premissa que o setor cibernético é decisivo para a Defesa Nacional, junto com os setores nuclear e espacial.

Essa pesquisa foca na presença da Marinha do Brasil no Espaço Cibernético atual (2021), comparando sua doutrina e práticas, as doutrinas do Brasil e do Mundo em relação as atuais ameaças cibernéticas.

Entretanto, este tema e sua importância ainda são poucos conhecidos na Marinha do Brasil, por isso a presente pesquisa visa disseminar um pouco de conhecimento sobre o espaço cibernético presente no mundo atual e a presença da Marinha do Brasil nesse novo espaço. Dentro desse cenário, é preciso verificar se a Marinha do Brasil está preparada para essas novas ameaças e qual postura ela irá adotar para se contrapor a essas ameaças.

1.1. Escopo

Esta pesquisa se limita a uma análise da presença da Marinha do Brasil no Espaço Cibernético, abrangendo como a Marinha do Brasil está capacitada para se contrapor as atuais Ameaças Cibernéticas, bem como que postura irá adotar, se é a de defesa de seus ativos de informação, através da proteção de seus dados e dos seus sistemas de informação, como os relacionados ao Programa Nuclear da Marinha, ou se é o emprego da tecnologia cibernética como uma ferramenta de combate, causando danos lógicos e físicos ao adversário e negando-lhe a capacidade do uso da internet e do espectro eletromagnético.

1.2. Objetivos

O objetivo geral desta pesquisa é analisar a presença da Marinha do Brasil no domínio cibernético, analisando se as capacidades cibernéticas que a Marinha do Brasil possui são as necessárias para se contrapor as Ameaças Cibernéticas e o posicionamento da Marinha do Brasil no Espaço Cibernético nacional.

Para alcançar as repostas do objetivo geral deste estudo, os seguintes objetivos específicos foram delineados:

a) Definir conceitos importantes relacionados ao domínio cibernético;

b) Apresentar as principais ações no espaço cibernético, em termos de capacidades cibernética, realizadas no mundo, bem como os ataques e incidentes cibernéticos mais significativos no mundo; e

c) Mostrar a legislação que ampara a atuação da Marinha do Brasil no espaço cibernético e sua organização no setor cibernético.

1.3. Metodologia

A pesquisa é do tipo exploratória, onde são levantadas informações sobre a doutrina Cibernética vigente na Marinha do Brasil e como podem ser enfrentadas as ameaças cibernéticas, os métodos de pesquisa utilizados são: pesquisa bibliográfica, elaborada através da revisão bibliográfica de artigos científicos, teses e livros que abordem o tema, bem como o estudo da atual doutrina cibernética da Marinha do Brasil, com intuito de definir os principais conceitos abordados no Espaço Cibernético, com intuito de construir o arcabouço teórico desta pesquisa; e pesquisa documental, dos documentos e minutas de âmbito interno da Marinha do Brasil sobre o tema, da legislação vigente, do Livro Verde: Segurança Cibernética no Brasil, Livro Branco, Política Nacional de Defesa e Estratégia Nacional de Defesa, que mostram o amparo legal para atuação da Marinha do Brasil no espaço cibernético, e as estratégias nacionais no Espaço Cibernético.

São utilizadas as técnicas de coleta de dados de pesquisa bibliográfica e pesquisa documental, já a técnica de análise de dados será qualitativa.

1.4. Descrição dos capítulos

No capítulo 1, é feita uma apresentação sobre o tema da pesquisa, A Marinha do Brasil e as Ameaças Cibernéticas, onde é mostrado que as ameaças cibernéticas são uma ameaça global, trazendo a preocupação do risco a integridade de infraestruturas críticas.

Dentro da introdução é apresentado o problema que a pesquisa se propõe a resolver que é como está a presença da Marinha do Brasil no Domínio Cibernético, ela encontra-se preparada para se contrapor as atuais Ameaças Cibernéticas? Qual postura irá adotar quanto ao domínio cibernético no cenário nacional?

São apresentados ainda, os objetivos, justificativas e contribuições que se pretende alcançar com a confecção deste trabalho. Além da metodologia de pesquisa empregada, materializada por pesquisa exploratória, onde são levantadas informações sobre a doutrina Cibernética na Marinha do Brasil e como podem ser enfrentadas as ameaças cibernéticas, os métodos utilizados.

No capítulo 2, são explicados os principais termos e conceitos sobre o espaço cibernético consagrados pela literatura internacional e pelos documentos oficiais brasileiros, que são utilizados ao longo do trabalho, pois durante a pesquisa foi percebida essa necessidade, devido a alguns conceitos terem diferentes definições na literatura mundial. Tais conceitos são extremamente importantes para o entendimento do trabalho e servem de base teórica para o desenvolvimento da pesquisa.

No capítulo 3, é apresentado um breve histórico do que está sendo realizado no mundo em termos de capacidades Cibernética, seus princípios, possibilidades e limitações de ações no espaço cibernético, incluindo os países mais atuantes no Espaço Cibernético, cujo conhecimento contribui para uma percepção global sobre as capacidades Cibernéticas. Também é abordado, brevemente, os ataques e incidentes cibernéticos mais significativos no mundo. Esse capítulo serve como uma referência de boas práticas que estão sendo adotadas no mundo, necessário para que se possa no próximo capítulo situar a Marinha do Brasil nesse contexto, bem como quais serão as prováveis ameaças que a Marinha do Brasil irá se contrapor.

No capítulo 4, é apresentada a presença da Marinha do Brasil no Domínio Cibernético, apoiada pelos conceitos e conhecimentos obtidos dos capítulos anteriores, primeiramente mostrando a legislação que ampara a atuação da Marinha do Brasil no espaço cibernético, mostrando que a atividade de defesa cibernética possui amparo na legislação atual para o emprego a cargo das Forças Armadas, pois enquadra-se como um dos componentes da Defesa Nacional. Posteriormente, é apresentada a organização da Marinha do Brasil no setor cibernético, abordando as suas atuais capacidades, possibilidades, limitações de emprego e deficiências no domínio cibernético, incluindo o atual esforço quanto ao posicionamento que a Marinha do Brasil pretende adotar para o domínio cibernético no cenário nacional, compatível com as tarefas a ela atribuídas, uma vez que, pela Estratégia Nacional de Defesa, a coordenação da Guerra Cibernética é do Exército Brasileiro. Por fim, é realizada uma análise sobre a

presença da Marinha do Brasil no setor cibernético, sugerindo alterações necessárias para que a ameaça cibernética seja mitigada e se obtenha um posicionamento eficiente no Espaço Cibernético nacional.

Finalmente, no capítulo 5, é apresentada uma breve conclusão com o objetivo de sintetizar os principais aspectos do trabalho, verificando se as hipóteses levantadas se confirmaram ou não. Para responder os problemas da pesquisa de forma assertiva, é essencial o estabelecimento de parâmetros, tais como a base legal para a atuação da Marinha do Brasil no setor cibernético nacional; definir a organização da Marinha do Brasil no setor cibernético nacional; analisar os princípios, possibilidades, limitações de emprego e deficiências no domínio cibernético adotados pela Marinha do Brasil; e esclarecer seu posicionamento no domínio cibernético no cenário nacional. Conclui-se ainda que esta pesquisa pretende atender aos objetivos, alinhados com as justificativas apresentadas na introdução da pesquisa. Dessa maneira, pretende-se ampliar a compreensão de forma a consolidar a conscientização sobre as ameaças cibernéticas apresentadas e as ações cibernéticas desenvolvidas na Marinha do Brasil.

2. CONCEITOS SOBRE O ESPAÇO CIBERNÉTICO

Este capítulo tem o objetivo de apresentar algumas definições importantes encontradas nos termos usados no Espaço Cibernético, em virtude de ser um tema recente, existem algumas variações entre as definições consagradas sobre esse assunto, o que pode dificultar o entendimento dos próximos capítulos. Portanto, para que a presente pesquisa alcance seus objetivos, faz-se necessário padronizar alguns termos e definições importantes que servirão como alicerce para o desenvolvimento desta pesquisa. Visto que será feita uma análise mais de caráter militar, os termos em português que serão analisados são, principalmente, os documentos oficiais brasileiros do Poder Executivo, mais especificamente os do Ministério da Defesa, os da Política e Estratégia Nacional de Defesa e os da própria Marinha do Brasil.

2.1. Conceitos

De acordo com Kramer, Starr e Wentz (2009), em um estudo realizado em 2009 foram encontradas 28 definições de Espaço Cibernético, o mais importante desse estudo é que essas definições não limitam sua compreensão, para eles o Espaço Cibernético é definido como "um domínio global dentro do ambiente de informação, que faz uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações usando redes". (KRAMER, STARR e WENTZ, p.28, 2009). Já o Ministério da Defesa define o Espaço Cibernético como "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas". (BRASIL, 2014, p.18).

Como observado no parágrafo anterior existem muitas definições para o termo Espaço Cibernético, o mesmo ocorre para os diversos termos empregados no Espaço Cibernético, para que essa pesquisa não fique muito extensa mostrando as discussões envolvidas mundialmente para cada termo que será apresentado nesta pesquisa, seguem abaixo algumas tabelas com os conceitos mais basilares para a compreensão do Espaço Cibernético definidos pelo Ministério da Defesa e pela Marinha do Brasil. Na tabela abaixo seguem os conceitos definidos pela Doutrina Militar de Defesa Cibernética, MD31-M-07, do Ministério da Defesa.

Tabela 1 – Conceitos sobre o Espaço Cibernético pelo Ministério de Defesa

1 – “Ameaça Cibernética: causa potencial de um incidente indesejado, que pode resultar em dano ao Espaço Cibernético de interesse.”
2 – “Ativos de informação: meios de armazenamento, transmissão e processamento de dados e informação, os sistemas utilizados para tal, os sistemas de informação de um modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.”
3 – “Cibernética: termo que se refere à comunicação e controle, atualmente relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação.”
4 – “Defesa Cibernética: conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa.”
5 – “Dia-Zero: designação atribuída à situação na qual há uma ameaça capaz de explorar uma vulnerabilidade de segurança descoberta em sistemas computacionais e que não teve, ainda, correção disponibilizada pelo desenvolvedor ou fabricante.”
6 – “Domínios Operacionais: o Espaço Cibernético é um dos cinco domínios operacionais e permeia todos os demais. São eles: o terrestre, o marítimo, o aéreo e o espacial, que são interdependentes.”
7 – “Guerra Cibernética: corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C^2 do adversário.”
8 – “Infraestruturas Críticas: instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.”
9 – “Segurança Cibernética: arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas.”

Fonte: BRASIL (2014, p.18 e 19)

Dos conceitos supracitados é interessante destacar a diferença entre Defesa Cibernética e Segurança Cibernética, a ideia de Defesa Cibernética é relacionada, de forma resumida, as ações realizadas no Espaço Cibernético, coordenadas e integrada pelo Ministério da Defesa, ou seja, pelas Forças Armadas, já a Segurança Cibernética diz respeito a garantia e proteção do Espaço Cibernético de toda a nação.

Carneiro (2012) nos mostra que de acordo com essas duas definições, podem ser resumidas duas vertentes, cada uma com suas ações e medidas específicas, conforme mostrado na tabela abaixo:

Tabela 2 – Formas de atuação de atores e órgãos do governo no Espaço Cibernético

Vertente	Ações / Atitudes	Medidas
Segurança Cibernética	Preventivas	- Criação e aplicação de metodologias de gestão de risco - Desenvolvimento de planos de contingência e continuidade de infraestruturas críticas - Resposta à incidentes de rede - Correções contra artefatos maliciosos - Disseminação de melhores práticas para proteção de redes e segurança das informações - Especificação e desenvolvimento de algoritmos criptográficos e equipamentos de segurança cibernética
	Repressivas	- Identificação e combate à conduta criminosa caracterizada como crime cibernético - Medidas contra terrorismo cibernético e sabotagem
Defesa Cibernética	Ações operacionais ofensivas e defensivas	- Medidas contra terrorismo cibernético e sabotagem - Medidas de apoio à operações militares conduzidas em situação de emprego militar

Fonte: CARNEIRO (2012, p.55)

Dessas duas vertentes percebemos que a Segurança Cibernética atua em todo o momento, desde os tempos de paz, através de suas ações preventivas, melhorando a Segurança Cibernética nacional, enquanto que as medidas repressivas se dão em uma situação de não guerra, já as ações ofensivas e defensivas da Defesa Cibernética, por ser de caráter militar, são utilizadas em situação de conflito e em apoio a exercícios e operações militares. É interessante notar que ambas as vertentes, Segurança Cibernética e Defesa Cibernética, atuam em medidas contra terrorismo cibernético e sabotagem, por se tratarem de ameaças assimétricas de difícil identificação do agressor.

Além das definições já apresentadas pelo MD, outros importantes conceitos relacionados à segurança da informação e comunicação são necessários para o entendimento desta pesquisa, esses conceitos foram retirados da Norma de Tecnologia da Informação da Marinha, e fazem referência ao Sistema de Gestão da Segurança da Informação (SGSI) da MB, para atender os requisitos desta Norma é necessária a observação da tabela abaixo.

Tabela 3 – Quanto à Segurança da Informação e Comunicações (SIC) e suas propriedades

1 – “Disponibilidade: garante a acessibilidade e utilização da informação ou dos ativos de informação.”
2 – “Integridade: garante que a informação não seja modificada ou destruída de maneira não autorizada ou acidental.”
3 – “Confidencialidade - garante que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada.”
4 – “Autenticidade: garante que a informação seja produzida, expedida, modificada ou destruída por uma determinada pessoa física, órgão, entidade ou determinado sistema.”
5 – “Não-repúdio: garante que o autor de uma informação ou dado não negue falsamente a sua autoria.”
6 – “Incidente de Segurança da Informação: eventos de segurança da informação indesejados ou inesperados, por agentes internos ou externos, voluntários ou não, que tenham probabilidade de comprometer as operações de sistema de comunicações e ameaçar a segurança da informação.”
7 – “Segurança da Informação e Comunicações (SIC): ações que objetivam assegurar a disponibilidade, a integridade e a confidencialidade de dados e informações de forma a minimizar os incidentes de segurança da informação.”

Fonte: BRASIL (2019, p.7-2)

Das definições apresentadas pela MB, percebemos que as cinco primeiras, disponibilidade, integridade, confidencialidade, autenticidade e não-repúdio, são propriedades essenciais para a segurança das comunicações, independentemente, da forma que se de essa comunicação, o comprometimento de pelo menos uma delas já faz com que uma comunicação não seja mais segura.

Outro importante conceito para o entendimento do Espaço Cibernético diz respeito a sua característica, a Doutrina Militar de Defesa Cibernética do Ministério da Defesa apresenta algumas dessas características.

Tabela 4 – Características do Espaço Cibernético

CARACTERÍSTICA	**DESCRIÇÃO**
Insegurança Latente.	Nenhum sistema computacional é totalmente seguro, tendo em vista que as vulnerabilidades nos ativos de informação serão sempre objeto de exploração por ameaças cibernéticas.

Alcance Global.	O Espaço Cibernético possibilita a condução de ações em escala global, simultaneamente, em diferentes frentes. Limitações físicas de distância e espaço não se aplicam ao Espaço Cibernético.
Vulnerabilidade das Fronteiras Geográficas.	As ações no Espaço Cibernético não se limitam a fronteiras geograficamente definidas, pois os agentes podem atuar a partir de qualquer local e provocar efeito em qualquer lugar.
Mutabilidade.	Não existem leis de comportamento imutáveis no Espaço Cibernético, pois podem adaptar-se as condições ambientais e da criatividade do ser humano.
Incerteza.	As ações no Espaço Cibernético podem não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados.
Dualidade.	As mesmas ferramentas podem ser usadas por atacantes e administradores de sistemas com finalidades distintas: por atacantes para encontrar oportunidades de ataque e, por administradores, para descobrir as fraquezas nas redes.
Paradoxo Tecnológico	Quanto mais tecnologicamente desenvolvido estiver um sistema, mais dependente da TI estará e mais vulnerável às ações cibernéticas. Contudo, possuirá mais condições de se defender dos ataques cibernéticos, em virtude de seu desenvolvimento tecnológico
Função Assessoria.	As ações de Defesa Cibernética não são um fim em si mesmas, sendo, geralmente, empregadas para apoiar a condução de outros tipos de operação.
Assimetria.	Baseada no desbalanceamento de forças, causado pela introdução de um ou mais elementos que podem vir a causar danos tão prejudiciais quanto aqueles perpetrados por Estados ou organizações com maiores condições econômicas

Fonte: BRASIL (2014, p.21)

Da tabela acima conseguimos tirar algumas conclusões sobre o Espaço Cibernético, a primeira delas é que não existe nada totalmente seguro no Espaço Cibernético, sempre existira um meio para explorar, pois foi desenvolvido por pessoas adaptando-se a sua engenhosidade, outra consideração importante é que o Espaço Cibernético não respeita o espaço físico e nem

suas fronteiras, podendo pessoas de lugares diferentes interagirem nele, executando ações muito distantes de onde elas estão fisicamente. Além disso, uma pessoa sozinha consegue produzir enormes estragos no Espaço Cibernético, podendo afetar milhares de outras pessoas direta ou indiretamente.

2.2. Vulnerabilidades na Internet

Dentro do Espaço Cibernético o local mais sensível e mais vulnerável para exploração é a Internet.

Dentre as diversas vulnerabilidades existentes na Internet são apresentadas, de acordo com Clarke e Knake (2015), seis grandes vulnerabilidades. A primeira delas é relacionada ao seu sistema de endereçamento, o Sistema de Nomes de Domínio (DNS), consiste em uma tabela que descobre para onde ir a partir de um endereço específico, o DNS pode ser alterado por Hackers mudando suas informações e encaminhado para páginas falsas. A segunda vulnerabilidade é o roteamento entre os Provedores de Serviço de Internet (ISP), um sistema conhecido como o *Border Gateway Protocol* (BGP). O BGP é o principal sistema usado para roteamento de pacotes na Internet, ele que decide qual será o próximo ponto que um pacote será enviado, ele também estabelece as relações ponto a ponto entre roteadores de duas redes distintas, contudo o BGP não possui mecanismos internos que o protejam contra ataques de modificação ou réplica de dados, isso significa que uma mensagem não é verificada quanto a sua autenticidade, ou seja, caso essa falha seja explorada todo o comportamento de roteamento da rede será perturbado. A terceira vulnerabilidade é apontada pela ICANN como a falta de governança na Internet, pois não existe ninguém realmente no comando. A quarta vulnerabilidade é a falta de criptografia, pois quase tudo que faz a Internet funcionar não está criptografado, ou seja, a maioria das informações são enviadas as claras, o que permite que uma terceira pessoa possa ter acesso a esse tráfego e consequentemente as informações enviadas. A quinta vulnerabilidade é a facilidade de propagação de tráfego malicioso projetado para atacar computadores, esses códigos maliciosos se aproveitam das falhas dos usuários e dos softwares, causando problemas em computadores, fornecendo um ponto de acesso ao computador ou copiando e roubando informações pessoais. A sexta vulnerabilidade se dá ao fato de a Internet ser uma grande rede com arquitetura descentralizada, sendo dada maior prioridade nesta descentralização do que na segurança.

Concluímos que a Internet por ser descentralizada e preocupada com a velocidade do tráfego de informação, deixa muitas brechas na segurança, logo, se quisermos segurança em uma rede a primeira coisa a ser feita é deixá-la de fora da Internet.

2.3. Tipos de ações cibernéticas

De acordo com Daultrey (2017), as ações no Espaço Cibernético incluem pelo menos seis elementos: dissuasão e defesa cibernética, espionagem cibernética, manipulação da informação, ataque generalizado, ataque sem ser detectado e operações com outros Estados.

Já no Brasil as ações cibernéticas clássicas são: Ataque Cibernético, Proteção Cibernética e Exploração Cibernética

Segundo a Doutrina Militar de Defesa Cibernética, Brasil (2014), Ataque Cibernético, são as ações realizadas para interromper ou destruir informações ou sistemas computacionais em dispositivos ou redes do adversário, enquanto que a Proteção Cibernética, são as ações para neutralizar ataques e exploração cibernética dos nossos dispositivos e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em uma situação de crise ou conflito, já Exploração Cibernética, são ações de busca ou coleta, nos dispositivos ou sistemas computacionais de interesse, a fim de obter a consciência situacional do ambiente cibernético. Devem servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas.

2.4. Tipos de ameaças cibernéticas

As ameaças cibernéticas, de acordo com as Normas de Tecnologia da Informação da Marinha, podem ser definidas como: “conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização”. (BRASIL, 2019, p. A-IX-1). Dentre as principais ameaças cibernéticas cabem destacar:

Tabela 5 – Principais ameaças cibernéticas

a) Ataque Distribuído de Negação de Serviço (DDoS) – segundo Clarke e Knake (2015), é um ataque onde centenas ou milhares de computadores são mobilizados para enviar *pings* a um alvo na Internet, os computadores atacantes são chamados de *botnet*, computadores controlados remotamente sem o conhecimento de seus proprietários, esse excesso de tráfego provocados pelos *botnets* são projetados para congestionar ou derrubar uma rede.
b) *Backdoor* – entrada oculta, para a maioria dos usuários, de um programa ou de um sistema, que pode ser utilizada para realizar ações nesses sistemas, sem serem percebidas.
c) Bomba-lógica – Clarke e Knake (2015) aponta que uma bomba-lógica é desenvolvida para apagar todos os softwares em um computador, o deixando inútil.

d) Engenharia Social – “Conjunto de técnicas utilizadas por hackers para se obter ou comprometer informações sobre uma organização ou seus sistemas computacionais, utilizando-se como ferramenta as habilidades e fragilidades sociais do ser humano”. (BRASIL, 2019, p. 9-20).

e) *Keylogger* – “pequeno pedaço de código malicioso instalado de modo invisível em seu computador, que pode capturar tudo que você digita e transmitir secretamente”. (CLARKE e KNAKE, 2015, p.69).

f) *Malware*: “termo proveniente da fusão das palavras *malicious software*, é também conhecido por código malicioso”. (NUNES, 2010, p.91).

g) *Phishing Scams* – “tentam enganar o usuário para que ele forneça informações como números de contas bancárias e códigos de acesso, criando mensagens de e-mail e sites falsos que fingem estar relacionados a negócios legítimos”. (CLARKE e KNAKE, 2015, p.69).

h) SPAM – segundo Brasil (2019), mensagem não-solicitada, mas que foi enviada a um usuário da Internet. Atualmente, é a técnica mais empregada para disseminação de código malicioso na Internet, muito utilizada em correios eletrônicos.

i) *Spyware*: “programas projetados para coletar dados de computadores ou outros dispositivos e enviá-los a uma terceira parte sem o consentimento ou conhecimento do usuário”. (COSTA, 2018, p.37).

j) *Worm*: “algoritmo ou programa autônomo capaz de se replicar em uma rede de computadores e de desempenhar ações maliciosas, como consumir os recursos computacionais e possivelmente desligar o sistema”. (COSTA, 2018, p.37).

Fonte: Elaboração própria (2021)

As ameaças, listadas na tabela acima, são os principais tipos de ameaças cibernéticas usadas no Espaço Cibernético para explorar suas vulnerabilidades, causando danos a terceiros ou simplesmente roubando informações de pessoas ou instituições presentes no Espaço Cibernético.

2.5. Divisão do Espaço Cibernético

Como mostrado por Clarke e Knake (2015), a Internet é uma rede aberta de computadores, a partir de um computador conectado à Internet, você poderá se comunicar com qualquer outro computador conectado à Internet. O Espaço Cibernético inclui a Internet, além de diversas outras redes de computadores que não deveriam estar acessíveis na Internet. As

redes privadas são exatamente como a Internet, mas estão, teoricamente, separadas. Outras redes do Espaço Cibernético são as redes transacionais, que por exemplo, enviam dados sobre fluxos de dinheiro, operações do mercado de ações e transações de cartão de crédito. Algumas redes são apenas sistemas que permitem que máquinas se comuniquem com outras máquinas, como por exemplo, painéis de controle de bombas hidráulicas, de geradores e de centrífugas.

Ainda segundo Clarke e Knake (2015), essas redes podem ser invadidas, controladas ou até mesmo destruídas por hackers. Ao invadirem uma rede, os hackers podem roubar suas informações ou mandar instruções para movimentar dinheiro, derramar petróleo, espalhar gás, explodir geradores, descarrilar trens, causar um apagão em uma cidade, colidir com os aviões ou fazer com que um míssil exploda no lugar errado. Esse novo cenário apresentado constitui o campo de batalha do Espaço Cibernético.

O Espaço Cibernético, assim como o terrestre, o marítimo, o aéreo e o espacial, é um domínio operacional, como mostrado por Kramer, Starr e Wentz (2009), e permeia todos os outros domínios. De acordo com Carneiro (2012), estes cinco domínios são interdependentes. Atividades no Espaço Cibernético podem criar liberdade de ação para atividades em outros domínios assim como atividades em outros domínios também criam efeitos no Espaço Cibernético. O objetivo central da integração entre os domínios é a habilidade de se alavancar capacidades de vários domínios criando efeitos únicos. No combate moderno, todos os domínios são interconectados pelas operações no Espaço Cibernético.

Esse novo domínio operacional, o Espaço Cibernético, pode ser dividido em três camadas, existindo apenas divergências na literatura na nomenclatura dessas camadas, para Even e Siman-Tov (2012) essas camadas são: humana, lógica e física, enquanto que para Liaropoulos (2012), essas camadas são: física, composta basicamente pelo hardware; a camada do software, composta pelos programas e a camada concreta, composta pelos dados, já para Camelo essas camadas seriam: física, lógica e da pessoa cibernética. Para essa pesquisa as três camadas são: a física, a lógica e a social.

A Camada Física, conforme apresentada por Camelo (2020), é composta, como o próprio nome diz, pelos componentes físicos do Espaço Cibernético, ou seja, sua infraestrutura que suporta a rede e os conectores físicos, hardwares e equipamentos físicos de armazenamento, transporte e processamento de informação que precisam de segurança física própria. Carneiro (2012) nos diz também, que a camada física inclui o componente geográfico de rede, que seria a localização física dos elementos da rede.

Já a Camada Lógica, é formada, basicamente, por componentes que não existem fisicamente, onde são processadas as informações da camada social para a camada física, sendo composta pelos softwares, aplicativos, programas, dados, processos, entre outros.

Por fim, a Camada Social segundo Camelo (2020), é a rede ou a conta de usuário, nesse conceito, é possível que um indivíduo crie inúmeros usuários, por exemplo, diferentes contas de endereço eletrônico em computadores diferentes, o que dificulta a atribuição de responsabilidade das ações do mundo virtual para o mundo real, pois torna-se difícil identificar o usuário ou o autor real das ações.

3. AÇÕES NO DOMÍNIO CIBERNÉTICO

De acordo com Clarke e Knake (2015), organizações militares e as agências de inteligências dos países estão desde o tempo de paz, preparando o terreno do futuro campo de batalha no espaço cibernético, colocando "explosivos virtuais" em outros países, tais explosivos são os *backdoors* e as "bombas lógicas". Ainda segundo esses autores, atualmente a guerra cibernética pode ser utilizada de duas formas, usando da própria guerra cibernética para facilitar um ataque convencional, desativando, por exemplo, as defesas do inimigo, ou seja, apoiando ou executando ações cinéticas, ou enviando propaganda para desmoralizar ou desestabilizar o inimigo, através da divulgação de *fake News*, de e-mails e outra mídias da Internet, como as redes sociais, ou seja, utilizando a Guerra Cibernética como ferramenta para a Guerra da Informação.

3.1. Possibilidades e Limitações das operações no Espaço Cibernético

A aplicação da Defesa Cibernética pelas Forças Armadas é pautada por princípios, possibilidades e limitações. Estas pautas são essenciais para a escolha das estratégias militares a serem adotadas no domínio cibernético, bem como as ações a serem executadas nos níveis operacionais e táticos das operações militares.

Segundo Nunes (2010), a Guerra Cibernética não é um fim em si mesma, seu principal emprego não é a destruição da capacidade de controle inimiga, mas a obtenção da superioridade de controle. Assim, os sistemas de informação serão atacados no Espaço Cibernético não apenas para a destruição da informação, mas, principalmente, para assumir o controle da infraestrutura de informação, causando um dilema no inimigo e agindo diretamente em seu processo decisório. Podendo essa mesma informação ser manipulada para criar uma diversão tática.

A Guerra Cibernética pode, ainda, "ser empregada para enfraquecer a capacidade inimiga, obtendo-se uma vantagem temporária, mas potencialmente decisiva. Isso pode ocorrer durante o conflito, de modo a facilitar uma ação militar convencional, ou mesmo antes de seu início". (NUNES, 2010, p.40).

Já algumas limitações das Operações no Espaço Cibernético são apresentadas pelo Ministério da Defesa como:

> limitada capacidade de identificação da origem de ataques cibernéticos; existência de vulnerabilidades nos sistemas computacionais; dificuldade de identificação de talentos humanos; grande vulnerabilidade a ações de oponentes com poder assimétrico; dificuldade de acompanhamento da evolução tecnológica na área cibernética; e possibilidade de ser surpreendido

> com base nas vulnerabilidades dos próprios sistemas de informação. (BRASIL, 2014, p.22).

Podemos observar que devido as suas possibilidades e capacidades os Estados vem executando operações no Espaço Cibernético de forma estratégica, incluindo até ações cinéticas executadas a partir desse espaço.

3.2. Incidentes cibernéticos no mundo e no Brasil

Para compreendermos as potencialidades da exploração no Espaço Cibernético, este capítulo mostra os principais incidentes que ocorreram no Espaço Cibernético no mundo até o momento.

Em 2007, conforme nos mostra CSIS (2021), Hackers Chineses invadiram a rede do Pentágono e roubaram dados relacionados ao caça F-35.

Ainda em 2007, Souto (2018) nos mostra que, a Estônia foi vítima de um ataque cibernético em massa à sua infraestrutura de informação. Sendo este ataque considerado o primeiro ataque cibernético direcionado à soberania de um país. O mais impressionante nesse incidente, é que a Estônia é um país que visto como um modelo para o futuro, pois desenvolvem e utilizam a tecnologia da Internet para diversos fins, como votação, educação, segurança e serviços bancários, sendo um dos países mais desenvolvido nessa área. Os ataques começaram por divergências sobre derrubar uma estátua de um soldado de bronze do Exército Vermelho, situada na capital da Estônia, erguida para lembrar o sacrifício feito pelo Exército Soviético na II Guerra mundial, este fato provocou uma forte indignação nos russos. Como retaliação, os russos executaram um ataque cibernético que levaram ao colapso os principais servidores da Estônia, durando semanas e atingindo servidores que apoiavam os principais serviços do país, como os da rede telefônica, do sistema de cartões de crédito, do maior banco do país, entre outros, afetando o comércio e os serviços de comunicação, provocando desordem e prejuízos ao país. A Estônia solicitou apoio à OTAN, que mobilizou uma equipe para apoiar o país, contudo os ataques continuaram. Especialistas rastrearam os ataques e identificaram que o ataque partia da Rússia. A Rússia negou qualquer participação nos ataques, mas se recusou a identificar os autores que se alegava estarem em seu território. O governo russo admitiu que os ataques poderiam ter partido de nacionalistas russos em seu território, inconformados com os acontecimentos na Estônia. Contudo, a Rússia negou que tais nacionalistas fossem apoiados pelo governo russo.

Também em 2007, conforme De Paula (2016) aponta, Israel relatou um ataque cibernético contra a defesa aérea Síria, interrompendo seu funcionamento, antes de seus caças entrarem no espaço aéreo sírio para bombardearem instalações de um suposto reator nuclear.

Em 2008, segundo Clarke e Knake (2015), um *spyware* russo começou a vasculhar os endereços militares americanos na Internet, quando o *spyware* conseguiu invadir a rede, ele começou a procurar por *pendrives* para se auto armazenar e se propagar. Alguns desses *pendrives* foram inseridos por usuários autorizados em computadores da rede secreta do Departamento de Defesa americano, supostamente, como essa rede é separada fisicamente da rede conectada a Internet, ela estaria protegida de vírus e *Worms*, por isso a maioria de seus computadores não possuía antivírus, *firewalls* ou software de segurança. Em pouco tempo, o *spyware* já tinha infectado milhares de computadores de nível secreto de militares dos Estados Unidos, do Afeganistão, Iraque e Qatar.

Em 2009, Clarke e Knake (2015) relatam que, foi descoberto por canadenses um programa de computador altamente sofisticado, apelidado de *GhostNet*. Este programa invadiu aproximadamente 1.300 computadores em embaixadas de vários países ao redor do mundo e tinha capacidade de ligar remotamente a câmera e o microfone de um computador sem alertar o usuário, enviando imagens e sons para servidores na China. A operação durou 22 meses até ser descoberta. No mesmo ano, a inteligência dos EUA vazou para a imprensa que hackers chineses tinham invadido a rede elétrica do país e instalado ferramentas que poderiam ser usadas para derrubar a rede.

Em 2010, um dos incidentes mais famosos foi o *worm Stuxnet*, conforme Beneditto (2016), o *Stuxnet* fez uso de seis vulnerabilidades “Dia-Zero”, tanto do sistema operacional quanto de aplicações, sendo descoberto em 17 de junho de 2010 por uma firma de segurança. O *Stuxnet* era capaz de se propagar por meio da porta USB, da rede de computadores e de vulnerabilidades do sistema operacional Windows. Ele incluía um mecanismo de acesso privilegiado a Controladores Lógicos Programáveis. Foi por meio desse acesso privilegiado que o *Stuxnet* causou os efeitos que levaram a destruição das instalações da usina de enriquecimento de urânio. Ele alterava a frequência dos conversores enquanto mascarava os dados para o sistema de controle, ou seja, tudo parecia dentro da normalidade. Essa variação de frequência causou o estresse mecânico das centrífugas levando-as à falha. O *Stuxnet* foi cuidadosamente desenvolvido com a intenção de sigilosamente, causar dano significativo em uma infraestrutura crítica. O ataque efetuado por meio do *Stuxnet*, contra a usina de enriquecimento de urânio no Irã, serve como exemplo do uso de armas cibernéticas cinéticas e, seu sucesso, pode ter dado início a uma nova corrida armamentista entre os Estados.

Em 2013, De Paula (2016) nos mostra um ataque DDoS que foi realizado contra a organização internacional *Spamhaus*, que monitora em tempo real ameaças virtuais em todo o mundo. No mesmo ano, a empresa estadunidense *Target* teve sua rede invadida durante as vendas de Natal por um ataque sofisticado que roubaram informações de cartões de crédito, custando à empresa quase US$ 1 bilhão.

Um levantamento do *Center for Strategic and International Studies* (CSIS), instituição que compila os incidentes cibernéticos internacionais, nos mostra uma lista de todos incidentes cibernéticos já relatados no mundo até o presente ano (2021), dessa lista destacamos alguns incidentes que são apresentados na tabela abaixo.

Tabela 6 – Incidentes Cibernéticos

ANO	**INCIDENTE**
2014	O governo da Alemanha reconheceu que um *malware* causou danos materiais no sistema de produção de uma usina de aço no país.
2015	Hackers Russos, realizaram um ataque coordenado ao sistema de distribuição de energia elétrica ucraniano, causando a interrupção dos serviços de energia elétrica por 6 horas, deixando sem luz cerca de 225.000 ucranianos.
2018	Hackers chineses invadiram uma empresa que desenvolve submarinos para a Marinha dos Estados Unidos, roubando um grande volume de material relacionado a um míssil anti-navio supersônico, juntamente com informações das comunicações de submarinos e sistemas criptográficos.
2018	Funcionários do Departamento de Segurança Interna dos Estados Unidos, confirmaram que hackers russos conseguiram ter acesso as listas de registro eleitoral de vários estados dos EUA antes da eleição de 2016.
2018	Hackers norte-coreanos roubaram US $ 13,5 milhões do *Cosmos Bank* da Índia após autorizarem milhares de saques em caixas eletrônicos, bem como várias transferências ilegais de dinheiro.
2019	O Serviço de inteligência do Irã hackeou o ex-chefe da Força de Defesa de Israel e o celular do líder da oposição antes das eleições em Israel.
2021	O sistema de transporte do Irã foi vítima de um ataque cibernético, o ataque causou atrasos e cancelamentos de centenas de trens em todo o Irã.

Fonte: CSIS (2021)

Os incidentes supracitados são apenas uma pequena amostra dos incidentes já realizados, cabendo destacar que grandes nações já foram vítimas de algum incidente cibernético, nos mostrando que não existe rede e nem país totalmente seguros, e outra conclusão que podemos chegar sobre os fatos analisados, é que muitas infraestruturas críticas foram atingidas por ataques cibernéticos, gerando não apenas danos lógicos, mas também danos físicos a essas infraestruturas.

Assim como a maioria dos países o Brasil não poderia passar ileso, Souto (2018) nos mostra que em 2013, o ex-agente de segurança da NSA, Edward Snowden, divulgou arquivos confidenciais que mostravam que o governo dos EUA espionavam diversos países, incluindo o Brasil. Dentre esses arquivos divulgados, estava um e-mail pessoal da então presidente Dilma Rousseff e a Petrobrás, outros documentos divulgados mostram que os escritórios da Embaixada do Brasil em Washington e da missão brasileira nas Nações Unidas, em Nova York, também teriam sido alvos da agência. Tal fato gerou um incidente diplomático entre os países. Após o ocorrido, o governo brasileiro determinou a implantação de um sistema de correio eletrônico que protegesse as mensagens oficiais.

Em agosto de 2016, Souto (2018) nos mostra que, momentos antes da cerimônia de abertura dos Jogos Olímpicos, no Rio de Janeiro, o grupo *hacktivista Anonymous* Brasil lançou uma série de ataques distribuídos de negação de serviço (DDoS) para os sites nacionais e internacionais dos jogos, o site do Ministério do Esporte, o site do Comitê Olímpico Brasileiro e o portal do governo do Rio de Janeiro, como forma de protesto às Olimpíadas.

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), órgão do Comitê Gestor da Internet no Brasil, de janeiro a dezembro de 2020, foram notificados 665.079 incidentes. A Figura 1 nos mostra a evolução dos incidentes no Espaço Cibernético brasileiro ao longo dos anos.

Analisando a figura abaixo, percebemos que o Brasil vem apresentando uma crescente na quantidade de incidentes cibernéticos tendo um pico em 2014, em virtude da Copa do Mundo que foi realizada no Brasil, esses grandes eventos funcionam como uma propaganda de um país para o mundo, atraindo todo o tipo de atenção para o país, e que desde esse ano o Brasil tem mostrado grande quantidade de incidentes por ano, o que revela um aumento da sua presença no sistema internacional.

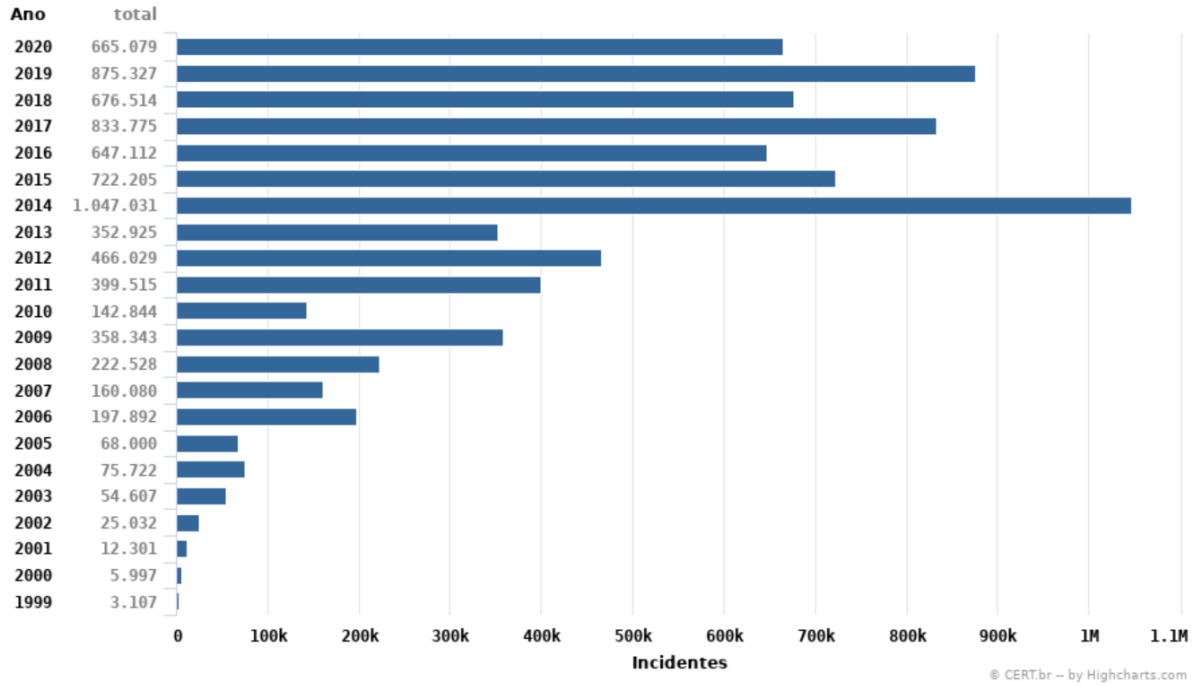

Figura 1 – Total de incidentes reportados ao CERT.br por ano

Fonte: < www.cert.br/stats/incidentes >

Podemos tirar algumas lições dos incidentes mostrados nesse capítulo, como nos mostra Clarke e Knake (2015):

1. **“A guerra cibernética é real”.** Do que foi apresentado até agora em termos de incidentes cibernéticos no mundo estamos longe do que ainda pode ser feito, pois na maioria desses incidentes foram utilizadas armas cibernéticas primitivas, supõem-se que os atacantes ainda não quiseram revelar suas capacidades mais sofisticadas.
2. **“A guerra cibernética acontece à velocidade da Luz”.** O tempo entre um ataque e seus efeitos é difícil de mensurar, devido à grande velocidade e quantidades de ações cibernéticas que podem ser realizadas, tornando-se um risco para a tomada de decisão e consequentemente, reação a este ataque.
3. **“A guerra cibernética é global”.**
4. **“A guerra cibernética ignora o campo de batalha tradicional.”** Os sistemas de um país são acessíveis a partir do Espaço Cibernético, não sendo preciso enfrentar as defesas tradicionais de um país.
5. **“A guerra cibernética já começou”.** De forma a se antecipar a futuras hostilidades, ainda em tempos de paz, as nações já estão se preparando, invadindo redes, sistemas e infraestrutura de outras nações, instalando bombas-lógicas e *backdoors*. Esse estado permanente de guerra cibernética leva a uma perigosa sensação de instabilidade.

3.3. Ações no domínio cibernético pelo mundo

É interessante notar que cada vez mais os Estados têm buscado seu espaço no domínio operacional cibernético, porém alguns Estados estão mais à frente na presença no Espaço Cibernético, seja por estarem a mais tempo nesse espaço, por terem mais tecnologia, ou por ser uma política estratégica nacional.

Os Estados Unidos têm como principal órgão responsável pela condução da política nacional de segurança da informação a *National Security Agency* (NSA). A NSA é a agência responsável por todas as questões relativas à segurança cibernética do governo dos Estados Unidos. A NSA integra a estrutura do Departamento de Defesa dos Estados Unidos. Segundo De Paula (2016), a NSA opera o sistema de vigilância global de comunicações e de espionagem ECHELON que foi largamente empregado para rastrear as atividades terroristas após o ataque ao *World Trade Center*, e atualmente, é acusada de espionar comunicações privadas em todo o mundo.

Em 2010 foi criado o Comando Cibernético dos Estados Unidos (USCYBERCOM) para a condução de um novo tipo de guerra de elevada tecnologia. O USCYBERCOM está inserido na estrutura das Forças Armadas subordinada ao Comando Estratégico dos Estados Unidos. Desta forma, o USCYBERCOM foi criado para cooperação tanto das forças militares como de outros órgãos integrantes de inteligência.

A missão do USCYBERCOM, é defender o Espaço Cibernético do Departamento de Defesa dos Estados Unidos e dos órgãos do governo. Clarke e Knake (2015) afirmam que ainda não há planos ou recursos para defender a infraestrutura civil, nem o Departamento de Defesa nem o Departamento de Segurança Interna possuem, atualmente, capacidade de defender o Espaço Cibernético corporativo que faz a maior parte do país funcionar.

O comandante do USCYBERCOM também exerce a função de diretor da NSA, Júnior (2013) nos mostra que assim, uma só pessoa é responsável tanto pela segurança quanto pela defesa nos Estados Unidos. Segundo De Paula (2016), o comando único permite ao governo norte-americano operar com eficiência, maximizando as suas capacidades operacionais.

Conforme apontado por De Paula (2016), a importância do Espaço Cibernético e da Guerra Cibernética para os Estados Unidos mostra sua força quando o Departamento de Defesa menciona que realizará missões cinéticas para preservar a liberdade de ação e a vantagem estratégica no Espaço Cibernético. No campo diplomático, os EUA já estabeleceram diversos acordos bilaterais com outros países amigos a fim de unir forças no combate as ameaças comuns no domínio cibernético.

Já na China, conforme mostrado por Clarke e Knake (2015), as redes que fazem parte de sua infraestrutura na Internet são controladas pelo governo, com participação direta ou em parceria com o setor privado. Para o governo chinês não existem discussões sobre o custo de segurança quando autoridades chinesas definem novas medidas para ela. As redes chinesas são segmentadas entre uso governamental, acadêmico e comercial. O governo chinês tem o poder de desconectar parte da China, da Internet do restante do mundo, ou seja, a Internet da China se assemelha muito mais a uma Intranet de uma empresa, com isso o governo chinês é o provedor de serviços da Internet e está ativamente defendendo sua rede.

Segundo De Paula (2016), a Estratégia Militar da China, publicada em 2015, divulgou, pela primeira vez, o compromisso chinês de construção de uma Força cibernética capaz de se envolver em ações ofensivas. De Paula (2016) também afirma, que segundo relatórios da *Freedom House*, a China é o país que mais censura na Internet. O Projeto Escudo Dourado, ou Grande *Firewall* da China, é um projeto de vigilância e de censura operado pelo governo chinês desde 2003. Ele bloqueia alguns serviços ocidentais como o Google, o Facebook, Instagram e o Youtube, além desses serviços ele bloqueia seletivamente páginas com termos considerados sensíveis pelo governo. A ideia é fazer com que os quase 900 milhões de internautas chineses se comuniquem com o resto do mundo, mas, ao mesmo tempo, bloquear as opiniões e interferências ocidentais, usadas como ferramenta ideológica.

Carneiro (2012) nos mostra que a China criou um Batalhão de Guerra da Informação na cidade de Guangzhou. A unidade é composta de três companhias com missões distintas, porém integradas em sua finalidade: uma Companhia de Comunicações, uma Companhia de Guerra Eletrônica e uma Companhia de Operações em Redes de Computadores, demonstrando, a concepção chinesa do uso integrado da Guerra Eletrônica e das Operações em Redes de Computadores, em virtude da grande similaridade dessas atividades, para interromper ou atrapalhar os sistemas de informação do inimigo, buscando a superioridade da informação.

Carneiro (2012) afirma ainda, que a Academia Chinesa de Ciências fornece assessoria sobre a Política Nacional de Segurança da Informação e do Direito, criou o Laboratório de Estado da Segurança da Informação. Esse laboratório conduz o Projeto Nacional de Ataque como um dos seus programas de pesquisa. Além disso, profissionais selecionados foram infiltrados em diversas organizações para incrementar a capacidade de combate em guerras futuras. Desta forma, a China mostra sua preocupação às estratégias ofensivas no Espaço Cibernético ao mesmo tempo em que se concentra na Guerra da Informação de forma defensiva.

A Rússia tem uma extensa história de acusações de ataques no Espaço Cibernético,

incluindo o incidente da Estônia, que muitos acreditam ser o primeiro caso de uma nação atacar outra usando o Espaço Cibernético.

Além disso, Daflon (2020) aponta que, a Rússia já demonstrou ao mundo inúmeras vezes o seu potencial de Guerra Cibernética. Aliados à hackers, a Rússia mostrou destreza em articular a Guerra Cibernética propriamente dita com diversas outras ferramentas de informação, sem mencionar as operações militares de guerra convencional como foi o caso da Geórgia em 2008.

Segundo De Paula (2016), nos episódios contra a Estônia e a Geórgia, os russos demonstraram bastante moderação no uso de suas armas cibernéticas e, provavelmente, não utilizaram suas melhores armas cibernéticas para quando realmente precisarem delas.

A Rússia e a China assinaram um acordo de cooperação digital no qual os dois países se comprometem a não realizar ataques cibernéticos um contra o outro.

Na Coréia do Norte, o governo criou uma academia militar em 1984, o *Mirim College*, que treina anualmente 100 guerreiros cibernéticos selecionados, em um programa rígido de treinamento com duração de cinco anos, onde o guerreiro cibernético aprende a criar vírus e invadir sistemas militares de segurança. Originalmente localizado em *Pyongyang*, foi transferido para o distrito montanhoso de *Hyungjaesan*, oficialmente conhecido como *Automated Warfare Institute* ou *University of the Gifted*. Atualmente, estima-se que a Coréia do Norte mantém um exército de 500 a 1000 especialistas em tempo integral em guerra cibernética e destina cerca de US $56 milhões para esses esforços.

Na Argentina, no ano de 2010 foi criado o Serviço de Segurança das Informações da Armada Argentina, com a finalidade de resguardar e preservar seus ativos de informação e seus sistemas. Esse Serviço de Segurança das Informações é formado por pessoal da especialidade de informática oriundos da Escola de Suboficiais da Armada, após passarem dois anos estudando, e pelos oficiais pós graduados em análise de sistemas.

No Exército Argentino, o Centro de Defesa Cibernética tem a missão de executar as ações necessárias para desenvolver as capacidades de Defesa Cibernética, o monitoramento das infraestruturas críticas e respostas aos incidentes, de forma a assegurar a utilização, a todo o tempo, do seu Espaço Cibernético. No que diz respeito aos Recursos Humanos, os requisitos de pessoal estão relacionados com os diferentes níveis da organização: engenheiros militares e engenheiros civis da área de informática e especialistas em segurança da informação.

Já na Força Aérea Argentina, a Diretoria de Defesa Cibernética, tem como missão a preservação de suas infraestruturas críticas. A Diretoria de Defesa Cibernética é subordinada ao Chefe do Estado-Maior da Força Aérea, e em sua organização prevê uma Diretoria com um

Departamento de Planos e Doutrina, um Departamento de Operações e um Departamento de Apoio. No que diz respeito aos recursos humanos, segundo o departamento de defesa cibernética, a área de recursos humanos constitui o centro de gravidade e fator determinante da defesa cibernética, idealmente o pessoal desta área deve vir de áreas como a Informática, Comunicações, Inteligência, Guerra Eletrônica e Operações, bem como pessoal que tenha algum tipo de certificação internacional na área de segurança da informação.

Paez (2010) aponta, que as três Forças estão desenvolvendo seus centros de defesa cibernética com doutrinas próprias, e que das três forças, a Armada Argentina é a que tem mais experiência no assunto.

Segundo Paez (2010), embora não haja uma padronização no treinamento e na organização do Espaço Cibernético de cada força, os propósitos são os mesmos e todos têm interesse em um Comando Conjunto de Defesa Cibernética para atuar com a flexibilidade necessária neste novo campo de batalha denominado Espaço Cibernético.

Podemos perceber que os países têm se preocupados em regulamentar o Espaço Cibernético, bem como aumentar a presença dos governos nesse espaço, seja para o controle interno de sua população ou para um posicionamento em relação aos outros Estados, e com isso, os Estados vem se capacitando, criando órgãos, formando pessoal qualificado, desenvolvendo pesquisas, e definindo suas políticas estratégicas para uma presença nesse espaço.

3.4. Mensurando a força da Guerra Cibernética no mundo

Mensurar a capacidade cibernética de uma Nação não é uma tarefa fácil, pois a maioria dos países não mostrou sua capacidade máxima no Espaço Cibernético, contudo Clarke e Knake (2015) criaram, empiricamente, uma tabela de comparação de Força Total na Guerra Cibernética, atribuindo pontuações para os países baseado em três fatores: Ataque Cibernético, Defesa Cibernética e Dependência Cibernética.

Clarke e Knake (2015), atribuíram pesos iguais em cada um dos fatores e a soma desses fatores mostra a força total de um país na guerra cibernética, as pontuações atribuídas a cada país são baseadas nas avaliações e experiências desses autores na área.

Tabela 7 – Força Total na Guerra Cibernética

NAÇÃO	ATAQUE CIBERNÉTICO	DEPENDÊNCIA CIBERNÉTICA	DEFESA CIBERNÉTICA	TOTAL
Coreia do Norte	2	9	7	18
Rússia	7	5	4	16
China	5	4	6	15
Irã	4	5	3	12
Estados Unidos	8	2	1	11

Fonte: (CLARKE e KNAKE, 2015, p.122)

Os resultados são reveladores, neles, Clarke e Knake (2015), mostram que a dependência cibernética analisada está relacionada a dependência das infraestruturas críticas a sistemas em rede, e com isso países que possuem poucas infraestruturas críticas ligadas a rede ou têm capacidade de desconectar essas infraestruturas da rede receberam uma pontuação alta em Dependência e Defesa Cibernética, como é o caso da China que tem capacidade para desconectar as redes de todo o país do resto do Espaço Cibernético, e da Coreia do Norte que pode desconectar sua limitada presença no Espaço Cibernético ainda mais facilmente e eficazmente que a China, já os Estados Unidos não tem essa capacidade, visto que a maioria das conexões americanas no Espaço Cibernético são privadas.

Logo esses países, que não estão tão conectados à rede ou que podem desconectar suas redes facilmente, em caso de uma Guerra Cibernética, sofrerão poucos ou até nenhum dano as suas rede e infraestruturas críticas.

3.5. As ameaças no Espaço Cibernético

Conforme nos mostra a DGMM-0540 (2019, p.9-1) “uma ameaça ao ambiente computacional consiste na possibilidade de não se resistir a um ataque à rede que produza algum tipo de efeito”. A tabela a seguir mostra as principais categorias de ameaças cibernéticas existentes.

Tabela 8 – Tipos de ameaças cibernéticas

AMEAÇA	DESCRIÇÃO
de interrupção	possibilidade de não se resistir a um ataque que impeça o acesso, pelo usuário, à informação digital desejada
de modificação	possibilidade de não se resistir a um ataque que permita a alteração do conteúdo da informação digital por alguém não autorizado
de interceptação	possibilidade de não se resistir a um ataque que permita o acesso à informação digital por alguém não autorizado para tal
de fabricação	possibilidade de não se resistir a um ataque que permita a geração, por alguém não autorizado, de informações digitais falsas ou em nome de outrem.

Fonte: Brasil (2019, p.9-2)

Esses quatro tipos de ameaças devem ser objetos de estudo para melhorar a segurança no Espaço Cibernético. Essas ameaças são materializadas através dos atores do Espaço Cibernético.

Segundo Costa (2018) as ameaças no Espaço Cibernético podem vir através dos seguintes agentes agressores:

a) interno, ação realizada normalmente por um funcionário;

b) grupos de Hackers organizados: podem ser grupos estatais, hackers contratados por Estados para agir como forças tarefas especiais, grupos terroristas, organizações criminosas cujos ataques possuem propósito financeiro, ou ativistas hackers (*Hacktivists*), quando seus ataques possuem uma motivação política;

c) aventureiro (*Hobbyist / Script kiddies*), pessoas que realizam ataques por curiosidade, desafio ou alguma outra motivação pessoal; e

d) pesquisador, grupos que testam a segurança com o objetivo de identificar fragilidades e propor melhorias na segurança.

Além dos Hackers e dos terroristas o Estado é o mais presente no Espaço Cibernético. Nunes (2010) nos mostra que, o Estado é o principal ator presente no Espaço Cibernético em função de sua imensa capacidade de recursos, lhe propiciando grande capacidade de atuar nesse domínio. É, atualmente, o único ator com capacidade de desenvolver ferramentas para ataques com elevado grau de sofisticação, em função dos elevados custos envolvidos para tal desenvolvimento.

Segundo Nunes (2010), de acordo com a Organização para Cooperação e Desenvolvimento Econômico (OCDE), um em cada três computadores está invadido, sendo possível o seu controle por terceiros. Hoje nenhum um usuário precisa ter grande conhecimento ou saber construir programas de invasão, na Internet é possível adquirir uma arma cibernética e aprender a usá-la. Além disso, atualmente, é possível contratar serviços e grupo Hackers, um exemplo disso é a *Russian Business Network* uma das maiores redes de crime cibernético do mundo, onde é oferecido uma completa infraestrutura para atividades criminosas, desde ferramentas de ataque cibernético até serviços de mercenários cibernéticos.

O elemento interno, como mostrado por Nunes (2010), pode introduzir uma vulnerabilidade por meio de ação humana direta, ou seja, por meio físico. Essa ação pode se dar durante o projeto, desenvolvimento, teste, operação ou manutenção da rede ou do sistema. Um dos mais sérios ataques que se tem conhecimento a uma infraestrutura crítica já ocorrido foi realizado por um elemento interno. Neste caso, em 2000, um ex-funcionário de uma companhia de tratamento de esgotos na Austrália, insatisfeito por não ter conseguido uma promoção e possuindo conhecimento do sistema que ele próprio instalou, invadiu o sistema de controle de bombas da companhia, causando o derramamento de milhões de litros de esgoto in natura.

Logo, a ameaça interna é a origem da maioria dos ataques conhecidos as infraestruturas críticas, e por isso não pode ser ignorada. Sua existência deve ser considerada, “uma vez que uma das fases mais difíceis de um ataque cibernético já foi superada: o acesso ao sistema, e medidas de segurança orgânica deverão ser implementadas de modo a negar a oportunidade ou, no mínimo, reduzir sua chance de sucesso”. (NUNES, 2010, p.27).

Além das redes de computadores existem os Sistemas Ciber-Físico (SCF), conforme mostra Costa (2018), caracterizados pela integração entre uma planta física e a computação. Por meio dessa integração, é possível monitorar, coordenar e controlar a dinâmica dos processos físicos. Um SCF tem como arquitetura básica um conjunto de sensores que coletam os dados e os enviam a um sistema de redes que os transmite aos subsistemas computacionais.

Historicamente, a maior preocupação das equipes de desenvolvimento dos SCF sempre foi com o desempenho, deixando as questões de segurança um menor grau de preocupação. Inicialmente, essa decisão era baseada no fato desses sistemas operarem isoladamente, sem contato com as redes externas, e serem desenvolvidos utilizando padrões não comerciais, o que limitava o número de profissionais conhecedores da tecnologia. Entretanto, com o intuito de diminuir os custos envolvidos nesses sistemas, passou-se a adotar cada vez mais equipamentos comerciais, o que trouxe fragilidades a esses sistemas por acabar com o isolamento entre os

sistemas de TI e de SCF. Com isso surgiram diversos agentes agressores pelo mundo que passaram a usar essa vulnerabilidade para atacar sistemas de infraestruturas críticas.

Os impactos gerados por esses ataques vão desde dano físico, passando por alteração dos dados e modificações do sistema, até a interrupção total do sistema.

Como exemplo de impacto gerado em um SCF, Beneditto (2016) mostra o Projeto AURORA, conduzido pelo governo dos Estados Unidos da América, foi um experimento feito para mostrar que um ataque cibernético pode destruir componentes físicos de um equipamento pertencente a rede de geração de energia elétrica estadunidense, mais especificamente um diesel gerador de energia elétrica. No experimento os pesquisadores, por meio de uma ação cibernética, abriram e fecharam os disjuntores do gerador fora de sincronia, para maximizar o estresse decorrente da variação de carga.

O projeto AURORA nos mostra que os equipamentos de geração de energia e os motores de combustão associados, precisam ter o seu risco avaliado do ponto de vista cibernético. Para a MB, o projeto AURORA levanta uma preocupação para o projeto do submarino de propulsão nuclear, especificamente, sobre os futuros motores e turbinas de propulsão, motores e geradores de energia, e respectivos mecanismos de controle.

Para conseguirmos nos contrapor a essas ameaças existem algumas técnicas que podem aumentar a segurança no Espaço Cibernético, principalmente, nas infraestruturas críticas. Serão mostradas algumas dessas técnicas, contudo essas técnicas que serão apresentadas não esgotam todas as possibilidades existentes.

Segundo Clarke e Knake (2015), uma dessas técnicas seria o emprego de *lasers* de grande largura de banda para transportar comunicações por satélites, visto que satélites são seguros contra hackers, com isso seriam reduzidas as vulnerabilidades associadas aos cabos de rede, de fibra ótica e roteadores espalhados ao redor do mundo.

Outras técnicas importantes dizem respeito a arquitetura de rede, com tecnologia mais acessível que a de satélites, e que podem ser executadas mais rapidamente para aumentar a segurança em uma rede.

Tabela 9 – Boas práticas de segurança no Espaço Cibernético

• Instalação de *firewalls*, software antivírus e sistemas de prevenção de intrusão em todos os computadores pessoais de todas as redes, sendo elas conectadas a Internet ou não, além de proteger a própria rede.

- Exigência que os usuários ao se conectarem provem sua identidade através de pelo menos dois fatores de autenticação.
- Segmentação das redes de acordo com a necessidade de conhecimento para limitar as conexões externas.
- Criptografar todo tráfego da rede que trafega pelos cabos de fibra ótica e roteadores, e também criptografar todos os arquivos em todos os computadores, incluindo os dados armazenados nos servidores.
- Monitoramento de todas as redes à procura de conexões não autorizadas, desconectando automaticamente dispositivos desconhecidos.

Fonte: Clarke e Knake (2015)

Ainda segundo Clarke e Knake (2015), uma outra importante ferramenta para melhorar a segurança das redes é a Segurança Ofensiva, pois um bom diagnóstico de segurança precisa apresentar dados concretos da rede avaliada, ou seja, quais são as suas atuais vulnerabilidades, quais são os ataques possíveis e seus impactos. Os chamados Testes de Invasão são a ferramenta que mais se adapta a essa nova ideia de Segurança Ofensiva, na qual o analista de segurança se coloca como atacante da rede e a partir daí consegue visualizar com mais precisão os danos que é capaz de causar a rede.

Além das técnicas apresentadas até aqui, um outro conceito importante relativo as questões de segurança, principalmente em infraestruturas críticas, é que para garantir que os dados de uma rede não sejam invadidos, essa rede não deve estar conectada a nenhuma outra, principalmente a Internet.

4. AÇÕES NO DOMÍNIO CIBERNÉTICO DA MARINHA DO BRASIL

O domínio cibernético tornou-se essencial para as estratégias organizacionais da Marinha do Brasil, onde o Espaço Cibernético consolida-se como a espinha dorsal do Sistema de Comunicações da Marinha (SISCOM), as ações nesse domínio são um importante suporte às atividades de Comando e Controle de Forças Navais e de suas infraestruturas críticas. Neste contexto reforça-se a preocupação com a necessidade de definição e normatização de práticas capazes de reduzir os riscos operacionais e garantir a continuidade dos serviços.

4.1. Legislação de amparo para atuação da MB no Espaço Cibernético

A atuação das Forças Armadas é amparada pela Constituição Federal de 1988, que prevê, que as Forças Armadas se destinam à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem. Já a Estratégia Nacional de Defesa (END), aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, estabelece diretrizes para a preparação e capacitação das Forças Armadas, de modo a garantir a segurança do país desde tempo de paz até situações de crise, vinculando a política de soberania nacional as Forças Armadas para resguardar nossa soberania.

A END aborda as questões políticas e institucionais ligadas a soberania nacional, definindo também, que as Forças Armadas são responsáveis pelo cumprimento da Defesa Nacional. Desta forma, como já mencionado na introdução dessa pesquisa, conforme Brasil (2017), três setores foram definidos como essenciais para a Defesa Nacional a cargo do Ministério da Defesa (MD): o espacial, o cibernético e o nuclear. Nesse contexto o MD, Brasil (2017), através da Diretriz Ministerial nº 14/2009, determinou que o setor nuclear ficasse sob a coordenação da Marinha, o cibernético, com o Exército e o setor espacial, com a Força Aérea.

Contudo, mesmo com a coordenação do setor cibernético a cargo do Exército, a Defesa Cibernética, por ser um dos componentes da Defesa Nacional, é missão das Forças Armadas (FA). Portanto, é responsabilidade de cada FA a adoção de medidas de proteção e Defesa Cibernética dos seus Ativos de Informação e de suas infraestruturas críticas.

O setor Cibernético brasileiro foi dividido em dois campos distintos: a Segurança Cibernética, a cargo da Presidência da República, e a Defesa Cibernética, a cargo do MD por meio das Forças Armadas, e a atuação no Espaço Cibernético foi dividida em quatro níveis, de acordo com o nível de decisão: político, estratégico, operacional e tático.

No nível estratégico o MD executa a Defesa Cibernética, uma atividade integrada das Forças Armadas, composta por ações realizadas no Espaço Cibernético para proteger os

sistemas de informação de interesse da Defesa Nacional. Quando o nível de decisão for o operacional ou o tático, a Doutrina Militar de Defesa Cibernética, Brasil (2014), nos mostra que, as ações cibernéticas são definidas como Guerra Cibernética.

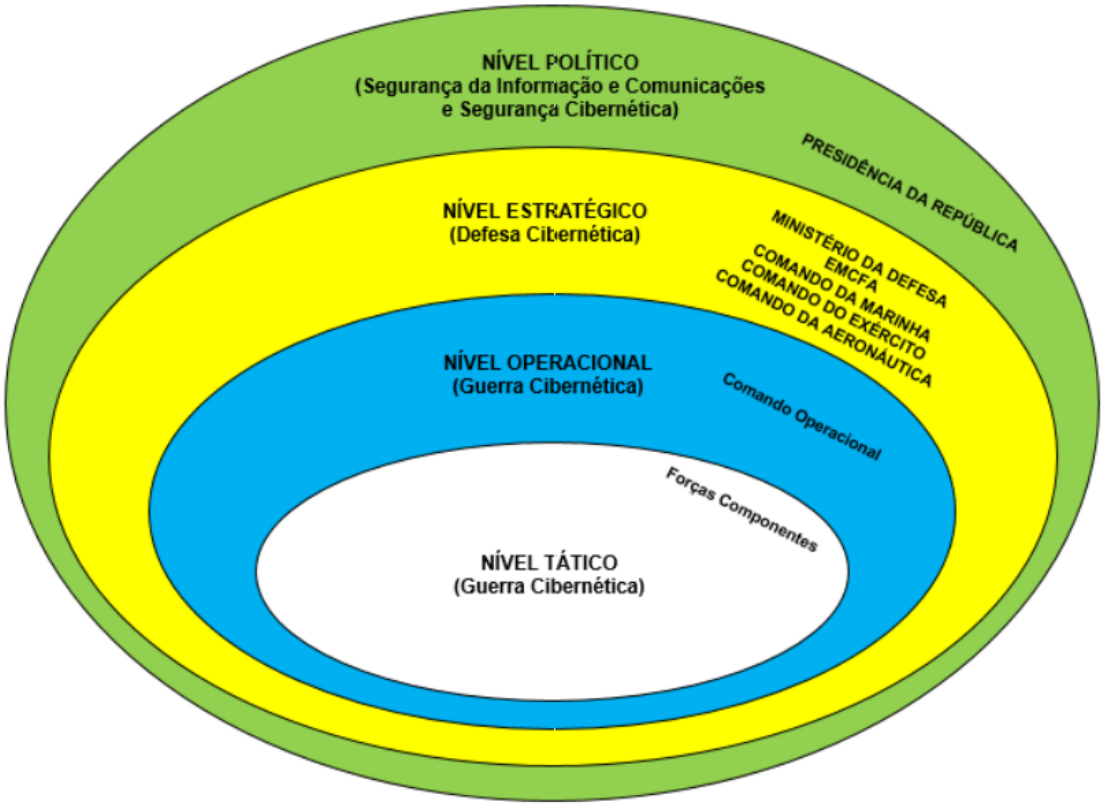

Figura 2 – Organização do setor cibernético brasileiro de acordo com os níveis de decisão
Fonte: (BRASIL, 2014, p. 17/36)

Detalhando mais as estruturas e órgãos do Sistema Militar de Defesa Cibernética, podemos observar na figura 3 as atribuições no Espaço Cibernético com base nos níveis de decisão: Nível Político, de responsabilidade da Presidência da República, Nível Estratégico, de responsabilidade do Ministério da Defesa e Comandos das Forças Armadas e o Nível Operacional e Tático, de responsabilidade das Forças Armadas.

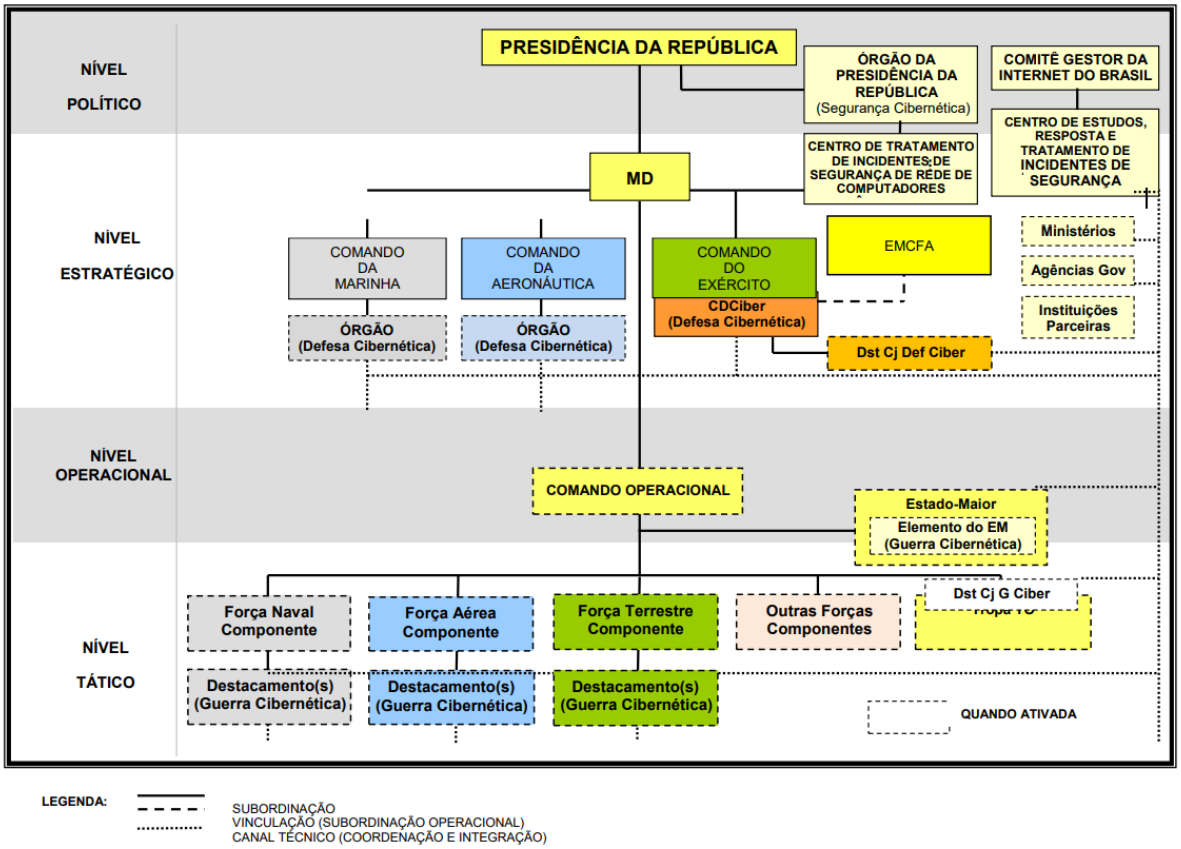

Figura 3 – Estruturas e órgãos do Sistema Militar de Defesa Cibernética

Fonte: BRASIL (2014, p. 35/36)

A aplicação da Política Cibernética de Defesa inclui todos os componentes da expressão militar do Poder Nacional, Brasil (2012). Essa política obedece a alguns pressupostos básicos dentre eles cabe destacar: que as atividades de Defesa Cibernética e as ações cibernéticas no âmbito do MD são orientadas para atender à Defesa Nacional.

Tabela 10 - Objetivos da Política Cibernética de Defesa

1. Assegurar o preparo e emprego operacional pelas Forças Armadas do Espaço Cibernético para seu efetivo uso e impedir ou dificultar sua utilização contra interesses da Defesa Nacional.
2. Capacitar os recursos humanos necessários à condução das atividades do Setor Cibernético no âmbito do MD.
3. Colaborar com a produção do conhecimento de Inteligência de interesse para o Sistema de Inteligência de Defesa.
4. Desenvolver e manter atualizada a doutrina de emprego do Setor Cibernético.
5. Implementar atividades de pesquisa e desenvolvimento no Setor Cibernético.

6. Nortear a criação de normas específicas no Setor Cibernético.
7. Cooperar com o esforço nacional para a capacidade dissuasória do Setor Cibernético.
8. Contribuir para a segurança dos ativos de informação da Administração Pública Federal (APF), referente à Segurança Cibernética fora do âmbito do MD.

Fonte: Brasil (2012)

Percebemos que a Política Cibernética de Defesa brasileira ainda é incipiente, assim como a Política Cibernética da maioria dos países, carecendo de toda uma estrutura regulamentar, e isso também se reflete nas instituições nacionais.

Para alcançar esses objetivos da Política Cibernética de Defesa, o MD criou diretrizes que mostram as atividades a serem implementadas, na tabela a seguir algumas são destacadas.

Tabela 11 – Diretrizes do MD para a Política Cibernética de Defesa

• "conceber e implantar o Sistema Militar de Defesa Cibernética (SMDC), contando com a participação de militares das FA e civis";
• "criar a estrutura para realizar a coordenação e a integração do Setor Cibernético no âmbito do MD, como órgão central do SMDC, com a possibilidade de participação de militares das FA e civis";
• "levantar as infraestruturas críticas de informação associadas ao Setor Cibernético para contribuir com a formação da consciência situacional necessária às atividades de Defesa Cibernética";
• "definir os perfis do pessoal necessário para a condução das atividades do Setor Cibernético";
• "identificar, cadastrar e selecionar o pessoal com competências ou habilidades, existente nos ambientes interno e externo das FA";
• "capacitar, de forma continuada, pessoal para atuar no Setor Cibernético, sob a orientação do órgão central do SMDC, aproveitando estruturas existentes";
• "viabilizar a participação de pessoal envolvido com o Setor Cibernético em cursos, estágios, congressos, seminários, simpósios e outras atividades similares relacionadas no Brasil e no exterior";
• "incluir o conteúdo Defesa Cibernética nos currículos dos cursos, em todos os níveis, no que couber, dos estabelecimentos de ensino do MD";
• "criar estruturas de Inteligência Cibernética";

- criar a doutrina de Defesa Cibernética;
- "promover intercâmbio doutrinário, normativo e técnico, com instituições civis e militares, nacionais e de nações amigas";
- "inserir a Defesa Cibernética nos exercícios de simulação de combate e nas operações conjuntas";
- "identificar competências específicas em Ciência e Tecnologia, de interesse do Setor Cibernético, no âmbito do MD e dos centros de pesquisa e desenvolvimento civis (públicos e privados), estabelecendo parcerias entre centros de excelência, em nível nacional";
- "criar parcerias e cooperação entre os centros militares de pesquisa e desenvolvimento e os centros de pesquisa e desenvolvimento civis (públicos e privados), para estimular a integração das iniciativas de interesse do Setor Cibernético"; e
- "elaborar propostas de criação e adequação de legislação federal, a fim de amparar as atividades de Defesa Cibernética".

Fonte: BRASIL (2012, p. 15/20, p. 16/20 e p. 17/20)

De forma análoga e alinhada com a Política Cibernética de Defesa do MD, foram criadas diretrizes no âmbito da MB com o objetivo de uma melhor gestão dos recursos e uma maior qualidade na prestação dos serviços de TI, assim foi criado o Plano Estratégico de Tecnologia da Informação da Marinha (PETIM).

O PETIM possibilitará que a MB "se adapte a um cenário de constantes mudanças, atuando de maneira proativa contra as ameaças e agindo a favor das oportunidades, explorando e desenvolvendo os seus pontos fortes e mitigando ou eliminando os pontos fracos". (BRASIL, 2015, p.1).

Para alcançar esse resultado foram criados alguns objetivos estratégicos a serem alcançados. Dentre esses Objetivos Estratégicos, conforme Brasil (2015), podemos destacar:

Tabela 12 – Objetivos Estratégicos para a Política Cibernética da MB

- Fortalecer a capacidade da Marinha de atuar na defesa do ambiente cibernético, dentro das atribuições da MB e da sua visão estratégica. Assim, enquadram-se nesse Objetivo Estratégico as Orientações no sentido de 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, e incrementar a mentalidade de Segurança da Informação Digital (SID). Também devem ser levados em consideração os seguintes aspectos: obtenção e disseminação da expertise técnica; alocação de recursos financeiros continuados para Pesquisa e Desenvolvimento; desenvolvimento de projetos de pesquisa na área cibernética; atualização ou criação de laboratórios; e continuidade e aumento da complexidade e abrangência dos exercícios de Guerra Cibernética;

- Fomentar o Software Livre na MB, com o propósito de obter uma otimização do emprego de recursos de TI e à aquisição de maior independência tecnológica. Abrangendo as soluções de TI em Software Livre, de uso generalizado, voltadas para a execução de tarefas administrativas rotineiras nas Estações de Trabalho e nos servidores da MB, excluindo-se, portanto, as estações de trabalho e servidores destinados a tarefas especificamente operativas. Como principais aspectos, destacam-se os seguintes: padronização dos sistemas operacionais; adoção do Sistema Operacional Linux nas estações de trabalho e servidores; e capacitação de pessoal em tecnologias homologadas, entre outros.
- Fomentar a captação de recursos extraorçamentários aplicáveis à Pesquisa, Desenvolvimento e a evolução da capacidade de TI da MB. Por essa razão, as oportunidades de parcerias devem ser aproveitadas. Seguindo essa lógica, destacam-se os seguintes fatores: existência de convênios, patrocínios, parcerias público privadas, dentre outros ligados à TI com entidades extra-MB.

Fonte: Brasil (2015)

Observando a tabela supracitada, percebemos que os objetivos da MB estão alinhados com a Política Cibernética de Defesa e suas diretrizes, focando no desenvolvimento de tecnologia e doutrina próprias, bem como parcerias com outras instituições para desenvolvimento e capacitação para utilização do Espaço Cibernético.

4.2. Organização da MB no Espaço Cibernético

Primeiramente, como mostrado por Guimarães (2018, p.15), “o Setor Cibernético da MB possui a estrutura organizacional cibernética, orientada ao processo decisório, dividida em níveis estratégico, operacional e tático, envolvendo a atuação integrada de várias Organizações Militares (OM)”, conforme ilustrado pela figura abaixo.

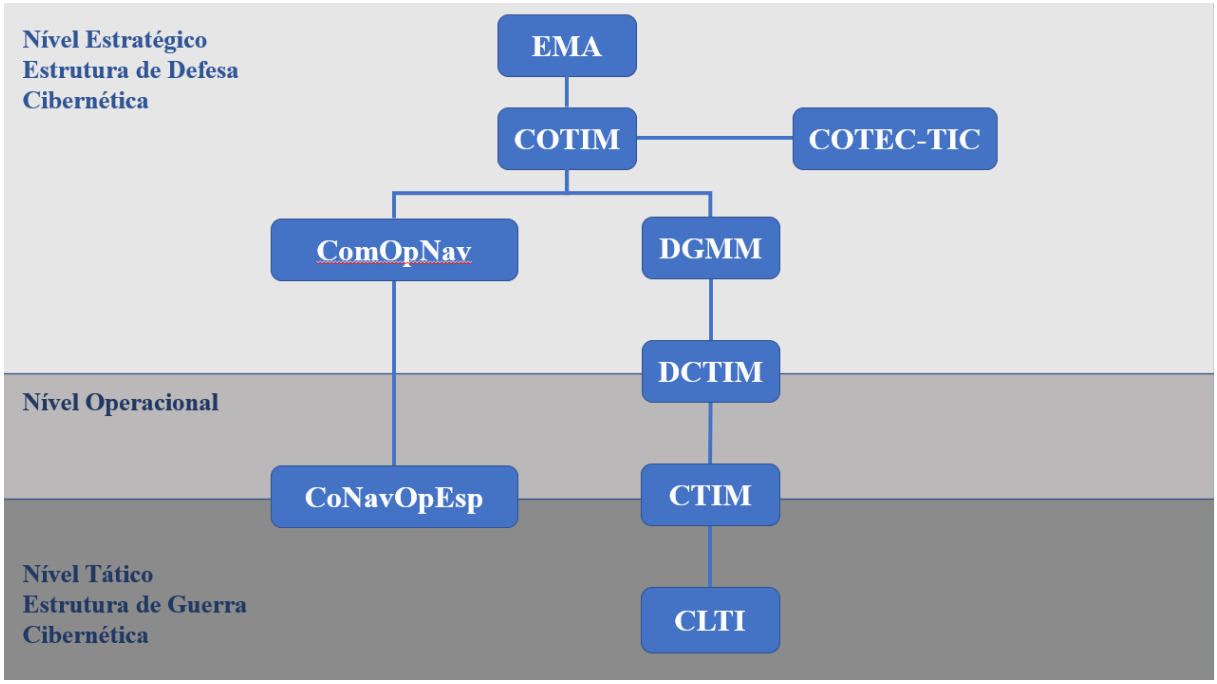

Figura 4 – Organograma da Estrutura de Defesa e Guerra Cibernética da MB

Fonte: Elaboração própria (2021)

O nível estratégico é constituído pelo Estado Maior da Armada (EMA), o Conselho de Tecnologia da Informação da Marinha (COTIM), a Comissão Técnica de Tecnologia da Informação e Comunicações (COTEC-TIC), a Diretoria Geral do Material da Marinha (DGMM) e o Comando de Operações Navais. Ao EMA, compete a gestão estratégica de TI na MB, estabelecendo o Plano Estratégico da Marinha, ao qual fundamenta todo o planejamento institucional. De acordo com as diretrizes estabelecidas pelo Plano Estratégico da Marinha, o COTIM, presidido pelo Chefe do Estado Maior da Armada, é a autoridade de TI da MB e responde pela formulação e disseminação corporativa dos princípios que orientam o emprego de TI, elabora o Plano Estratégico de TI da Marinha (PETIM) a cada quatro anos. Ao COTIM, apoiado tecnicamente pela COTEC-TIC, compete assessorar o Comandante da Marinha no trato dos assuntos relacionados à Governança da TI na MB, que envolvam a participação dos Órgãos de Direção Setorial de uma forma coordenada. À DGMM, é atribuída a competência de atuar como órgão de supervisão funcional da execução das deliberações do COTIM pela DCTIM. Ao ComOpNav, compete, através do Comando Naval de Operações Especiais (CoNavOpEsp), assessorar o Comandante de Operações Navais nos assuntos de Guerra Cibernética.

No nível estratégico e operacional, atua a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM). A DCTIM atua como diretoria especializada e órgão

executor das deliberações do COTIM, com o propósito garantir a defesa do Espaço Cibernético da MB.

No nível operacional e tático, atuam o Centro de Tecnologia da Informação da Marinha (CTIM), ao gerenciar e executar, sob a supervisão da DCTIM, os tratamentos de incidentes de rede e a Defesa Cibernética da MB, e o Comando Naval de Operações Especiais (CoNavOpEsp) as Ações de Guerra Cibernética (AGCiber).

O CoNavOpEsp é a mais recente OM do Espaço Cibernético da MB, portanto se faz necessário uma breve explicação sobre a mesma.

O CoNavOpEsp é uma Organização Militar com semiautonomia administrativa, subordinado ao Comando de Operações Navais (ComOpNav). De acordo com a Portaria Nº113/ComOpNav, de 22 de agosto de 2019, para a consecução do seu propósito, cabem ao CoNavOpEsp as seguintes tarefas:

I. Comandar e compor Forças-Tarefas de Operações Especiais e de Guerra Cibernética, Singulares, Combinadas ou Conjuntas, quando determinado;

II. Assessorar o Comandante de Operações Navais e os setores da MB nos aspectos relativos às Operações Especiais, Operações de Informação, Operações Psicológicas, Ações de Guerra Eletrônica, Ações de Guerra Cibernética e Ameaças Assimétricas;

III. Planejar e coordenar a participação da MB nas operações, adestramentos e exercícios conjuntos e combinados de Operações Especiais, Operações de Informação, Operações Psicológicas, Ações de Guerra Eletrônica e Ações de Guerra Cibernética; e

IV. Conduzir as Ações de Guerra Cibernética de caráter operativo na MB.

O CoNavOpEsp é divido em dois departamentos: o Departamento de Operações Especiais e o Departamento de Operações de Informação, além de duas assessorias: Assessoria de Inteligência e Assessoria de Ameaças Híbridas.

O Departamento de Operações de informação possui em sua estrutura as divisões: de Operações Psicológicas, de Produção de Informação, de Relações Civis e Institucionais, de Guerra Acústica e Eletrônica, e de Guerra Cibernética, que atua não apenas no nível operacional, mas também no nível tático, sendo prevista em sua lotação, militares especializados para a condução de ações cibernéticas de proteção, exploração e ataque, além de desenvolver armas cibernéticas e procedimentos para realização de ações cibernéticas, atuar como elemento de ligação do setor operativo com o Comando de Defesa Cibernética, e planejar e conduzir os exercícios e adestramentos de Guerra Cibernética no âmbito da MB.

Antes da criação do CoNavOpEsp a atividade de Guerra Cibernética era conduzida pela CTIM, percebemos então que a Marinha sentiu a necessidade de separar a Guerra Cibernética

da Defesa Cibernética, trazendo a Guerra Cibernética para o setor operativo da Marinha, destacando ainda que a Guerra Cibernética ficou junta com outras capacidades especiais da MB, mostrando que a Marinha está pronta para usar a Guerra Cibernética também como uma ferramenta ofensiva.

No nível tático, atuam os Centros Locais de Tecnologia da Informação (CLTI), como elementos organizacionais de apoio ao CTIM na resolução de incidentes de redes e nas ações de proteção cibernética, nos locais sob sua área de jurisdição.

Além dessa estrutura, A MB conta ainda com o Centro de Apoio a Sistemas Operativos (CASOP), que realiza atividades de guerra eletrônica, e do Centro de Análises de Sistemas Navais (CASNAV), que dentre seus diversos projetos, desenvolve projetos de segurança voltados para a certificação digital, conforme mostra Silva (2014, p.205), "seus programas serviram de modelo para a implementação da Infraestrutura de Chaves - Públicas da Defesa e inspiram a implementação de um sistema de chaves - públicas de segurança para ser utilizado em toda administração pública federal". Segundo Giffoni (2020, p.207), o CASNAV ajuda também "nas investigações de casos de ataques cibernéticos".

4.3. RECIM

A RECIM, como mostrado pelas Normas de Tecnologia da Informação da Marinha, Brasil (2019, p. 3-1), "é o conjunto de elementos computacionais, organizados em rede, que compõem a infraestrutura responsável pelo tráfego de informações na Marinha do Brasil". Segundo Brasil (2019), a integração das comunicações ocorre com a combinação do tráfego de dados, voz e vídeo. A RECIM abrange a rede de telefonia da Marinha, além de utilizar a Intranet para prover aos seus usuários o acesso a recursos e serviços de TI no âmbito da MB. A RECIM também possui dispositivos de conexão e barreiras de segurança que permitem sua interligação de forma mais segura à Internet e a outras redes de interesse da MB, disponibilizando o acesso controlado de seus usuários aos serviços de TI disponibilizados nas redes externas, bem como a oferta, também, controlada, de serviços de TI a usuários da MB fora da RECIM. A figura abaixo exemplifica a Estrutura da RECIM.

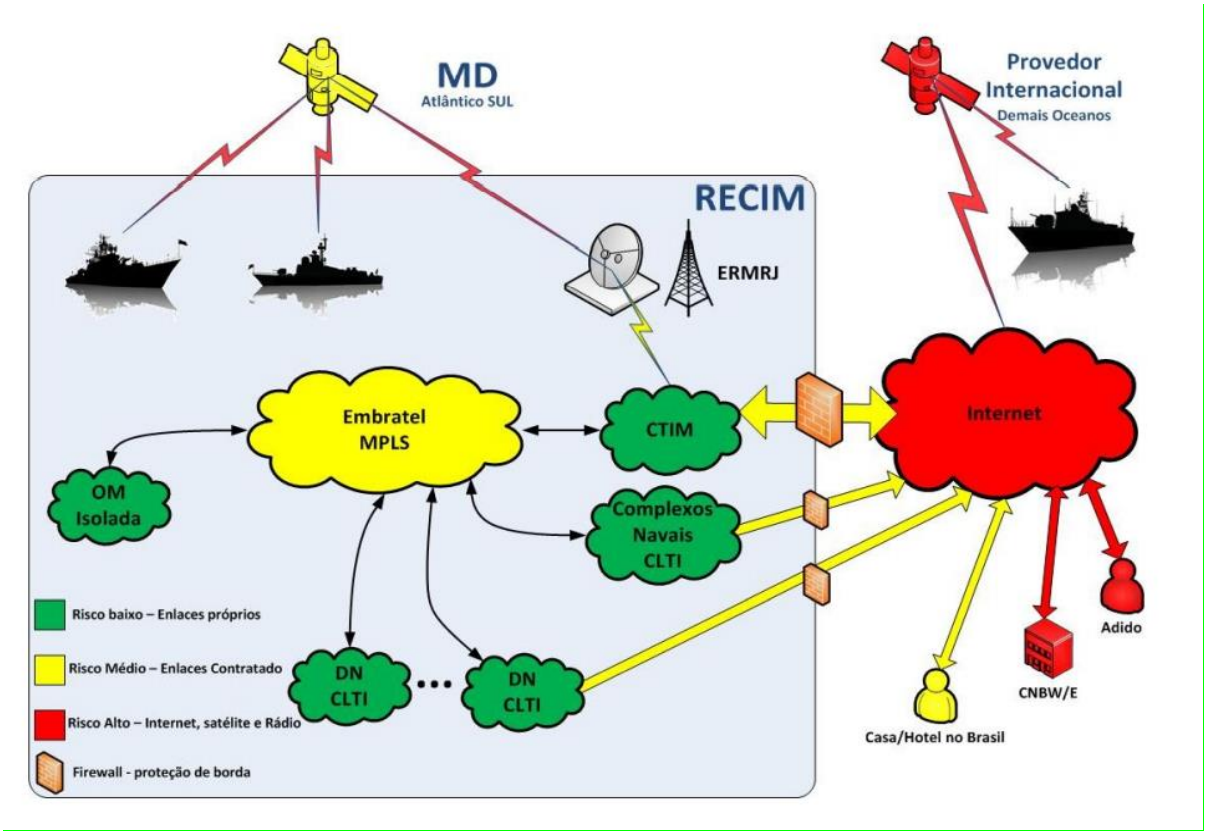

Figura 5 - RECIM

Fonte: Diretoria-Geral do Material da Marinha. Cartilha de segurança da informação digital. (BRASIL, 2016, p.5)

Ao fornecer os recursos de TI para todos usuários da MB, internos e externos, a RECIM deve obedecer, segundo Brasil (2019, p.3-3), "aos seguintes requisitos básicos: confiabilidade, rapidez nas respostas às solicitações, disponibilidade, eficiência e segurança".

Brasil (2019) nos mostra que, a Disponibilidade consiste na garantia do acesso contínuo aos recursos, aos serviços e aos aplicativos existentes na RECIM a seus usuários, para isso são usados enlaces de contingência, infraestrutura e dispositivos computacionais de redundância, e sistemas de fornecimento ininterrupto de energia. Já a Eficiência é um requisito ligado às tecnologias e aos procedimentos operacionais utilizados pela RECIM, de forma a satisfazer às expectativas dos usuários, com o menor dispêndio de recursos possível. Enquanto que a Segurança é um requisito que visa garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das informações que trafegam pela RECIM. O emprego de recursos criptológicos, barreiras de segurança (firewalls), zonas desmilitarizadas, registros de autenticação, programas antivírus, redes privadas virtuais e processos de auditoria são exemplos de técnicas relacionadas com a segurança.

Como nos mostra a DGMM-0540, a RECIM pode ser comparada como uma rede de grande área (WAN), de caráter corporativo, ligando as redes metropolitanas (MAN) Distritais que, são compostas pelas diversas redes locais das OM concentradas em uma região. Por ser uma rede corporativa, a RECIM deve, preferencialmente, ser constituída por recursos próprios da MB, tornando-se independente de soluções privadas. Contudo, para atender os requisitos de eficiência, disponibilidade e rapidez, em virtude da abrangência e a capilaridade necessárias para atingir OM situadas em locais remotos do Brasil, torna-se necessária a contratação de enlaces de dados de provedores privados.

Cada OM pode ter ao menos uma rede de dados local (LAN) que são integradas à RECIM. Para melhor eficiência operacional da OM, um militar ou servidor civil é designado formalmente como responsável administrativo e técnico dessa rede, ficando a critério da própria OM a indicação do mesmo, com base nas qualificações para exercer a função. Além de um Oficial designado, com a qualificação necessária, para exercer a função de Oficial de Segurança das Informações e Comunicações (OSIC), de forma a garantir o cumprimento dos procedimentos de segurança às atividades de TI da OM.

Ainda segundo as Normas de Tecnologia da Informação da Marinha, a Área dos Distritos Navais ou Complexos Navais constitui uma rede integrada, rede metropolitana, formada pelas redes locais das OM situadas em sua área de responsabilidade, sendo a responsabilidade administrativa e técnica dessas redes a cargo dos CLTI regionais.

A RECIM possibilita a integração de todas as redes da Marinha. Compete ao CTIM, as responsabilidades técnica e administrativa dessa rede. Cabe à DCTIM a supervisão técnica do CTIM, bem como o gerenciamento de nível doutrinário e estratégico, além das responsabilidades administrativa e técnica pelos projetos e contratos que impliquem alteração na RECIM.

Conforme as Normas de Tecnologia da Informação da Marinha, a estrutura organizacional da RECIM é composta por um coordenador no nível estratégico, a DCTIM, e um Coordenador no nível operacional, a CTIM. Dentro do nível operacional, cada área de responsabilidade conta com um CLTI, cada CLTI apoia os administradores de redes locais de sua área de jurisdição. Os militares e civis componentes dos CLTI deverão, preferencialmente, ter formação acadêmica compatível. Os CLTI, dentre outras atribuições, deverão dar suporte aos recursos e serviços de TI das OM de sua área de responsabilidade, mantendo um relacionamento de subordinação funcional com o CTIM.

A CTIM ainda desenvolve suporte a serviços, apoiado pelos CLTI, no âmbito de suas áreas de responsabilidade, composto por gerenciamento de incidentes e problemas, contando ainda com uma central de serviços.

Dentro dessa estrutura de suporte a serviços, existe a Central de Suporte aos Serviços e Ativos da RECIM (CSRECIM), que segundo Brasil (2019), é responsável por tratar e gerenciar os incidentes, garantindo a disponibilidade e confiabilidade do serviço, restaurando-o rapidamente ao estado normal quando necessário. É composta por uma equipe de profissionais qualificados que, assumem a perspectiva do usuário para perceber o impacto e a urgência no tratamento do incidente.

De acordo com Souza (2011, p.17), **"**no final do ano de 2010, a MB, através do CTIM, gerenciava 27.200 usuários de rede, 50.000 acessos diários e até 5.000 acessos simultâneos à Internet e disponibilizava 256 sítios eletrônicos de Intranet e 163 de Internet". Ainda segundo Souza (2011, p.17), "o correio eletrônico da MB possui 32.000 usuários, enviando e recebendo 16.500 mensagens externas por dia, das quais 90% são filtradas como SPAM".

Brasil (2019) nos mostra que, a MB está conectada à Internet de várias formas, possuindo conexões principais e redundantes com pontos físicos de acesso situados no CTIM. Existem também os acessos secundários, situados nos Comandos de Distritos Navais (ou grandes complexos). Esses acessos, fora da área do Rio de Janeiro, são chamados, no âmbito da MB, de enlaces de Internet Distrital. Os acessos de Internet Distrital são encarados como uma opção para aumento de flexibilidade e de desempenho das OM situadas nos diversos Distritos Navais, uma vez que os acessos baseados no 1ºDistrito Naval, no Rio de Janeiro, continuarão disponíveis para toda a MB, independentemente da contratação da Internet Distrital. Todo acesso à Internet, a partir das estações interligadas à RECIM, deve ser realizado por uma das formas de conexão mencionadas, não sendo autorizada nenhuma outra forma de interligação à Internet. Dessa forma, nenhuma OM está autorizada a contratar serviço de acesso à Internet para uma de suas estações de trabalho pertencentes à RECIM. Também não é permitido que um usuário, porventura possuidor de modem particular de acesso, possa conectar esse dispositivo a uma estação de trabalho da RECIM. Além disso, em todos os casos supracitados, para fins de garantia do cumprimento das leis de informática vigentes no país, o acesso à Internet é analisado por dispositivos intermediários (proxies) e as páginas visitadas estão sujeitas a ferramentas de controle de conteúdo que bloqueiam acessos a páginas de conteúdo considerados impróprios, no ambiente corporativo da MB. Todos os acessos são, portanto, registrados para fins de auditorias interna e externa. Qualquer exceção a essas formas de acesso deve ser solicitada formalmente à DCTIM, com as devidas justificativas para análise.

Segundo Brasil (2019), a DCTIM juntamente com o CTIM, planejou diversas medidas de segurança para a RECIM, dentre essas medidas, o CTIM instalou mecanismos, tais como IPS, firewall e analisadores de conteúdo, a fim de controlar os acessos à Internet. Por causa desses mecanismos, é proibido o acesso não autorizado do público externo à Intranet da Marinha, e o acesso à Internet a partir da RECIM está condicionado a serviços, protocolos, aplicações e usuários autorizados. Todos os acessos são registrados em arquivos de transações (logs), sendo examinados pelo CTIM e pela DCTIM, ficando disponíveis para eventuais auditorias, durante um período de tempo limitado, conforme previsto em lei. Sendo possível identificar a origem de todo e qualquer acesso a sites externos, individualmente. O planejamento das auditorias é atribuição da DCTIM, podendo ser solicitadas pelas próprias OM, em caráter especial.

Também estão instalados mecanismos que restringem acessos indevidos, incluindo restrições a alguns tipos de arquivos com determinadas extensões, a alguns sites específicos ou sites pertencentes a uma dada categoria, como sites pornográficos, e definindo períodos do dia para determinados acessos. Esses mecanismos, analisadores de conteúdo, procuram restringir a ocupação de recursos com tráfego de informações não relacionadas com as atividades da Marinha.

Para tentar diminuir a entrada de SPAM na RECIM, foram incluídas algumas verificações de segurança, como medidas AntiSpam no servidor de correio eletrônico localizado no CTIM, domínio “marinha.mil.br” na Internet.

Essas medidas AntiSpam verificam a autenticidade do servidor origem da mensagem, examinando se esse servidor se encontra fora das listas negras de servidores remetentes de SPAM, a correta formação dos nomes do remetente e do destinatário da mensagem, o número total de destinatários de uma mesma mensagem e o tamanho total da mensagem enviada para o destinatário da MB.

A Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República de 13JUN2008 (IN nº 01 GSI/PR/2008), elaborada pelo Comitê Gestor de Segurança da Informação e aprovada pela Secretaria Executiva do Conselho de Defesa Nacional, é a norma que orienta a atividade de Segurança da Informação e Comunicações no âmbito do Governo Federal, apresentando a estrutura administrativa para a gestão da segurança das informações e comunicações nos órgãos da Administração Pública Federal (APF). A DGMM-0540 nos mostra que:

> a estrutura administrativa da MB referente a SIC é aderente ao proposto pela IN nº 01 GSI/PR/2008, mostrando assim, a atenção que a MB despende ao

> assunto buscando e mantendo-se atualizada em relação às melhores práticas de SIC. Com o objetivo de manter a MB alinhada à Instrução Normativa, a MB criou a estrutura de gestão de segurança da informação e comunicações, dentro da estrutura de TI da MB, onde a DCTIM atua como Gestor de Segurança da Informação e Comunicação (GSIC). (BRASIL, 2019, p.III-3).

A Doutrina de TI da MB mostra que, a Segurança da Informação e Comunicações (SIC) é um conjunto de medidas que objetivam a garantia dos requisitos de sigilo, autenticidade, integridade e disponibilidade em face dos riscos corretamente medidos em função do valor do ativo de informação ou da infraestrutura crítica, das ameaças e das vulnerabilidades dos ambientes que a armazenam, a processam e a trafegam. Além disso, é vital uma permanente construção de mentalidade de segurança da informação em todos os integrantes da MB, desde os altos escalões até as escolas de formação.

A SIC visa negar, impedir ou minimizar a possibilidade de obtenção do conhecimento de dados que trafeguem ou sejam armazenados digitalmente nos sistemas de redes locais, incluindo, as ações voltadas às Seguranças física, lógica, de tráfego e criptológica das Informações Digitais. Portanto, a SIC não é só um conjunto de procedimentos, como também os recursos, programas, equipamentos específicos de segurança, e normas aplicáveis que garantem os seus requisitos básicos.

As medidas de Segurança Orgânica relativas à Segurança da Informação e Comunicações, segundo as Normas de Tecnologia da Informação da Marinha, são divididas em quatro partes: Segurança física, lógica, de tráfego e criptológica das Informações Digitais.

A Segurança Física está relacionada aos procedimentos e dispositivos usados para assegurar a integridade física dos Recursos Computacionais Críticos (RCC). A Segurança física que estabelece uma barreira de proteção, paredes, salas, cofres, cujo os acessos físico possuam controle eletrônico ou sejam vigiadas por pessoal de serviço. Cada barreira representa um perímetro ou camada física de segurança que melhora a proteção total. O acesso físico a cada perímetro de segurança existente na OM precisa ser controlado, identificando-se cada visitante e permitindo o acesso aos perímetros de segurança que contenham RCC somente ao pessoal autorizado. A entrada ou a saída do perímetro de segurança de dispositivos de armazenamento, tais como *pendrives* e discos externos, ou de quaisquer outros dispositivos de armazenamento de informações digitais ou dispositivos móveis, assim como quaisquer outros equipamentos eletrônicos com capacidade de registro de informações devem ser proibidos.

De acordo com a Doutrina de TI da MB, a segurança lógica é dividia em: Segurança Lógica dos Equipamentos Servidores e Segurança Lógica das Estações de Trabalho. A

Segurança Lógica dos Equipamentos Servidores é feita pela instalação das versões atualizadas dos programas existentes nos servidores, assim como de todas as correções disponibilizadas pelos fabricantes e distribuidores. Além disso, todos os serviços não necessários devem ser desabilitados, desinstalando-se todos os programas e aplicativos desnecessários e fechando-se todas as portas lógicas que não estiverem sendo utilizadas. Estes dispositivos serão habilitados somente quando for estritamente necessário ao serviço.

A Segurança Lógica das Estações de Trabalho, corresponde a maior quantidade de equipamento no conjunto de RCC existentes na RECIM, sendo assim, requerem maior atenção em relação à SIC. Na estação de trabalho não pode estar disponível nenhum serviço e nem acesso remoto, pois não é um equipamento servidor, sendo, desta forma, apenas um meio para acessar os serviços e programas disponibilizados e homologados pela DCTIM. Para este RCC, a maior vulnerabilidade está no próprio usuário.

A Segurança do Tráfego da Informação e Comunicações compreende as medidas para impedir a obtenção não autorizada das informações digitais quando estas estiverem trafegando em uma rede local. Caso seja necessário conectar duas instalações afastadas fisicamente de forma a constituir uma mesma rede local, deverão ser tomadas medidas de proteção às informações digitais que trafegam entre as mesmas. Quando o enlace for de fora da MB, como no caso dos enlaces contratados de empresas comerciais, os dados deverão trafegar por meio de uma Rede Privada Virtual (VPN–*Virtual Private Network*).

A segurança criptológica emprega a codificação ou cifração para alterar-se o conteúdo original da informação, tornando-o incompreensível quando examinado sem o uso dos mesmos códigos ou cifras. As informações digitais sigilosas devem trafegar e ser armazenadas cifradas, utilizando-se os recursos criptográficos existentes na MB, atendendo o preconizado nas normas referentes.

O esforço para as atividades de SIC deve ser de todos os usuários da RECIM e não somente do pessoal de informática da OM. O mais importante para a SIC é a existência de uma mentalidade de segurança incutida em todo o pessoal. Pois, pouco adiantará o estabelecimento de rigorosas medidas de segurança se o pessoal responsável pela sua aplicação não tiver consciência plena de suas implicações. As OM devem se esforçar para desenvolver e manter um alto nível de conscientização do pessoal quanto à SIC. Isto pode ser feito, por exemplo, por meio de palestras, adestramentos, exercícios internos, dentre outras atividades.

Cada usuário da Marinha do Brasil precisa entender que seu computador ligado à RECIM está, constantemente, na linha de contato da Guerra Cibernética. Assim, é fundamental que cada um compreenda que a defesa cibernética da Marinha do Brasil começa em seu

computador, sendo este pensamento vital para a criação de uma forte mentalidade de segurança em todos os usuários.

4.4. Órgãos de Execução

Conforme mostrado em Brasil (2019), os órgãos de execução são todas as OM da MB que utilizam serviços de TI. Os atores que atuam nesses órgãos são: o Titular da OM, o Oficial de Segurança da informação e Comunicações (OSIC), o Administrador da Rede Local (ADMIN) e o Usuário. A seguir são mostradas as principais obrigações desses atores.

Tabela 13 – Responsabilidades dos atores do Espaço Cibernético da MB

TITULAR DA OM
a) manter o fiel cumprimento das normas, procedimentos e instruções pertinentes à SIC na sua OM; b) zelar para que a operação e a manutenção dos equipamentos, instalações e sistemas da rede local da OM sigam as instruções em vigor; c) zelar pelo fortalecimento da mentalidade de segurança; d) reportar prontamente os incidentes de SIC ao CTIR.mar, após uma avaliação preliminar; e) designar o Oficial de Segurança da informação e Comunicações (OSIC) da OM; e f) designar o Administrador da rede local (ADMIN) da OM.
OFICIAL DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (OSID)
a) coordenar, junto aos demais setores da OM, o estabelecimento dos Planos de Adestramento de SIC e zelar pelo seu cumprimento; b) assessorar o Titular da OM nos assuntos de SIC; d) reportar prontamente os incidentes de SIC, após uma avaliação preliminar, ao Titular da OM; e) garantir que todos estejam cientes das instruções em vigor para a segurança das informações digitais do ambiente computacional da OM, por meio da assinatura do Termo de Responsabilidade Individual pelos usuários que acessam a rede local; f) realizar auditoria interna de SIC na OM, com apoio do CLTI; g) exigir do pessoal da MB externo à OM, autorizado a executar serviços na rede local, o cumprimento das regras estabelecidas para guarda e proteção do sigilo das informações que possa ter acesso. Além disso, deverá ser cumprido os procedimentos sobre segurança orgânica, previstos em publicações específicas da MB;

h) divulgar recomendações referentes as técnicas de Engenharia Social para todo o pessoal da OM, a fim de minimizar a probabilidade de estranhos à OM obterem sucesso na aplicação de tais técnicas pelos meios de comunicações disponíveis; e

i) coordenar o tratamento de resposta à incidentes de SIC em sua OM.

ADMINISTRADOR DA REDE LOCAL (ADMIN)

a) operar e manter os ativos de TI existentes na sua rede local, em conformidade com as normas vigentes;

b) resguardar a integridade física dos equipamentos de conectividade da RECIM, porventura instalados no âmbito de sua OM, comunicando qualquer avaria detectada ou a impossibilidade de manter os referidos equipamentos em um ambiente adequado ao seu funcionamento;

c) manter o CLTI informado sobre a atualização (aquisição/baixa) dos ativos de TI da OM;

d) promover adestramentos periódicos aos usuários da OM quanto aos procedimentos e serviços de TI;

e) não permitir a divulgação de características da rede local a pessoas externas à OM sem a autorização prévia e formal do OSIC;

f) criar, apagar ou alterar perfis ou privilégios de usuários ou grupos de usuários;

g) controlar e gerenciar os acessos aos sistemas;

h) manter um cadastro atualizado de todos os usuários que utilizam os sistemas da rede local e os que não têm autorização para tal;

i) efetuar e garantir as atualizações dos sistemas existentes no ambiente computacional e rede local;

j) configurar as estações de trabalho com privilégio mínimo para o usuário;

k) coibir acessos à Internet por modem, conexões 3G, 4G, WiMAX, WiFi e outras redes sem fio não autorizadas pela DCTIM; e

l) atualizar os sistemas operacionais da OM e ferramentas de segurança homologadas pela DCTIM.

USUÁRIOS

a) utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso da MB exclusivamente para o interesse do serviço;

b) preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

c) não se fazer passar por outro usuário usando a identificação de acesso (login) e senha de terceiros;
d) não alterar o endereço de rede ou qualquer outro dado de identificação de sua estação de trabalho;
e) utilizar em sua estação de trabalho somente programas homologados para uso na MB;
f) não compartilhar, transferir, divulgar ou permitir o conhecimento das suas autenticações de acesso (senhas) utilizadas no ambiente computacional da OM, por terceiros;
g) responder, perante a MB, as auditorias e o OSIC da OM, por acessos, tentativas de acessos ou uso indevidos da informação digital, realizados com a sua identificação ou autenticação;
h) não realizar nenhum tipo de acesso a redes "P2P" e redes sociais sem a devida autorização e obedecer a instruções próprias para os casos autorizados;
i) não transferir qualquer tipo de arquivo que pertença à MB para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;
j) estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional da OM; e
k) estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada, recebida ou retransmitida no ambiente computacional da OM deve obedecer a este preceito.

Fonte: Brasil (2019)

De acordo com as Normas de Tecnologia da Informação da Marinha, Brasil (2019), o OSIC é um Oficial, ou civil assemelhado, escolhido pelo titular da OM para exercer tal função, que tenha, preferencialmente, realizado o curso necessário para auditoria em redes locais, sendo desejável possuir conhecimentos mínimos de redes locais de computadores, serviços disponibilizados pela rede (Intranet, correio eletrônico e assinaturas digitais) e conhecimento em auditoria de redes.

O Administrador da Rede Local (ADMIN), de acordo com as Normas de Tecnologia da Informação da Marinha, Brasil (2019), é uma Praça da MB de qualquer especialidade ou civil, nomeado pelo Titular da OM, que tenha realizado os cursos necessários para atuar como administrador de rede local da OM em que serve, devendo ter, preferencialmente, capacitação em Administração de Rede de Computadores e, se possível, para os sistemas operacionais que estejam sendo utilizados dentro da OM, assim como conhecimentos mínimos em auditoria de

sistemas computacionais. Compete ao ADMIN gerenciar a rede local de forma a mantê-la operando dentro dos seus requisitos operacionais e com todos seus serviços em funcionamento.

O usuário de serviços e equipamentos interligados pela rede local da OM, seja militar, servidor civil ou prestador de serviço, deverá estar ciente das suas responsabilidades sobre SIC.

Da análise da tabela acima, verificamos a grande preocupação da MB em tentar proteger um dos pontos críticos de qualquer sistema informacional, o usuário final, que como foi mostrado, encontra-se na camada Social do Espaço Cibernético. Essa proteção se dá inicialmente pela responsabilização dos atos de cada ator dentro do Espaço Cibernético da MB, da criação e capacitação de elementos internos em cada OM, responsáveis por verificarem a SIC, e pôr fim a criação de uma mentalidade de segurança em todos os usuários da RECIM, através da imputação de responsabilidades, adestramentos, cartilhas, palestras e etc.

4.5. Recursos Humanos

Uma questão importante no Espaço Cibernético mundial, diz respeito a capacitação dos recursos humanos para atuarem nesse domínio, Nunes (2010) nos mostra que o Espaço cibernético é uma construção do homem dependente de suas capacidades. A Guerra Cibernética, como está inserida no Espaço Cibernético, é altamente dependente de pessoal especializado. Ocorre que esse tipo de capital humano, qualificado, é um recurso cada vez mais disputado pelo mercado de trabalho, o que faz com que as crescentes demandas dos setores militar e governamental enfrentem um grande desafio para atrair e manter esses recursos.

Portanto, segundo Nunes (2010) uma solução seria investir na formação de pessoal próprio. Atualmente, não existe nenhuma disciplina específica de Guerra Cibernética nos currículos dos cursos de formação de oficiais e praças na Marinha do Brasil. Esse conhecimento seria importante para criar e difundir uma mentalidade de segurança cibernética, logo a criação de uma disciplina relacionada a segurança cibernética em todos os cursos de formação, bem como os de especialização e de aperfeiçoamento, se faz necessária.

Contudo, Henriques (2021) aponta que, a capacitação militar é complexa, pois exige do profissional militar desde o mais simples procedimento, até as mais complexas e variadas habilidades, nesse sentido espera-se que o profissional capacitado para atuar no Espaço Cibernético atue em operações de amplo espectro, operações de guerra e benignas, em operações conjuntas, interagências e multinacionais, desenvolvendo pensamento crítico e gerenciando conflitos, bem como a responsabilidade de promover a segurança e a defesa da nação, tudo somado a utilização de maneira mais eficiente possível os recursos financeiros e tecnológicos disponibilizados pela nação.

Para Costa (2012), as competências para aprender, incorporar e bem utilizar as novas tecnologias são tão relevantes quanto desenvolvê-las. Sendo necessário investir na capacitação, sabendo que o conhecimento e o recursos humanos são os principais atores nesse processo. Nesse sentido a educação militar merece destaque para que as organizações militares não corram o risco de depender dos investimentos financeiros ou mesmo nos custos de desenvolvimento de tecnologias ou de novas aquisições. Dessa forma, a capacitação militar deve ser estimulada, de forma a utilizar políticas curriculares e práticas pedagógicas adequadas e validadas para enfrentar os desafios impostos pelos novos cenários operacionais.

Logo, para que a Marinha possa estar em melhores condições presente no Espaço Cibernético, surge a necessidade de criação de um curso para habilitar os futuros guerreiros cibernéticos, ou até mesmo a criação de uma especialidade própria, principalmente no setor operativo. Atualmente, os militares que atuam no Espaço cibernético da MB são formados em cursos extra-MB.

4.6. Pesquisa e Desenvolvimento

Os programas e ferramentas utilizados na Guerra Cibernética são produtos customizados, uma vez que devem ser adaptados aos sistemas específicos a que se destinam. Esse fato gera a necessidade por uma customização dos programas, ou seja, a existência de centros de desenvolvimento de ferramentas para a Guerra Cibernética, que trabalharão desde os tempos de paz produzindo códigos específicos.

Segundo Nunes (2010), o uso de armas cibernéticas adquiridas ou fornecidas por governos estrangeiros ou empresas privadas apresenta um grave risco. Pois essas soluções privadas poderão ter suas funções alteradas ou até mesmo neutralizadas, além de constituírem grave ameaça à segurança de nossos próprios sistemas, que poderão ser vítimas de ações de exploração. Na pior das hipóteses, esses programas poderão conter códigos maliciosos que poderão ser usados contra nós. Decorre, então, a necessidade de uma solução autóctone, confiar somente na solução adquirida pode significar não só a destruição de toda a capacidade, como também por em risco as operações militares.

Da mesma forma os softwares pagos passam a impressão de que são mais seguros que os livres, mas, na verdade, os softwares livres por terem código aberto, podem ser totalmente customizados, podendo ser modificados, aperfeiçoados e auditados diferentemente de softwares pagos que podem possuir *backdoors* sem possibilidade de auditoria.

De Paula (2016) afirma que para minimizar a dependência externa de produtos e serviços privados, é preciso investir em produtos e serviços nacionais destacando-se:

a) o investimento em satélites e cabos submarinos de comunicação próprios, conforme aponta a Estratégia Nacional de Defesa;

b) o desenvolvimento de software livre e de um correio eletrônico nacional para uso do governo; e

c) a criação de criptografia de dados genuinamente brasileira.

De Paula (2016) nos mostra ainda, que em termos de hardware, as universidades brasileiras já possuem capacidade de desenvolver roteadores com elevada transferência de dados, compatíveis com os padrões internacionais. Paralelamente ao desenvolvimento de hardware e software nacionais, deverá ser criado e adotado um sistema de criptografia brasileiro, assim como os feitos pelo CASNAV.

No setor espacial, o Brasil vem desenvolvendo o projeto do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC) com o objetivo de assegurar a soberania nas comunicações estratégicas brasileiras. O satélite será operado pelo Ministério da Defesa na banda X (militar), e pela Telebrás na banda Ka (civil). As comunicações, o controle da órbita e da altitude do satélite será feito por instituições nacionais. O tráfego de voz e dados ocorrerão por rede própria permitindo a troca segura de informações governamentais.

Portanto, a Marinha do Brasil deve buscar o desenvolvimento de suas próprias ferramentas para a Guerra Cibernética, o que gera a demanda por pessoal qualificado, por centros de desenvolvimento e por parcerias com outras instituições. Assim como já vem fazendo com a substituição de softwares pagos por softwares livres, adotando um correio eletrônico próprio, desenvolvendo sistemas e criptografia próprios, através de suas OM e de parcerias com outros órgãos e instituições, da administração pública e da iniciativa privada.

5. CONCLUSÃO

Esta pesquisa procurou identificar as capacidades e deficiências da presença da Marinha do Brasil no Espaço Cibernético, bem como identificar os procedimentos necessários para que a MB enfrente as ameaças cibernéticas descritas nesta pesquisa.

A primeira conclusão desta pesquisa, é que não existe nada totalmente seguro no Espaço Cibernético, sempre existira um meio para explorá-lo, pois o Espaço Cibernético foi desenvolvido por pessoas, adaptando-se a sua inventividade. Desta conclusão, percebe-se que o maior risco no Espaço Cibernético vem das vulnerabilidades associadas a camada social, ou seja, aquelas associadas à falta de mentalidade de segurança por parte do usuário. Tais vulnerabilidades são as mais fáceis de explorar e as mais difíceis de prevenir e detectar, sendo o fator humano a principal causa pela maioria das falhas de segurança que levam a invasões de sistemas e roubos de dados em geral. Dentro dessa camada social destacam-se diversos agentes capazes de realizar ataques, desde aventureiros, que por meio de vulnerabilidades exploram brechas no sistema, até grupo de hackers, por vezes financiados por um estado, capazes de elaborarem complexos ataques a sistemas, através do desenvolvimento de códigos maliciosos discretos e altamente nocivos. Contudo, a ameaça interna, os usuários, é a origem da maioria dos ataques conhecidos no Espaço Cibernético, sua existência deve ser considerada, pois ela já superou as medidas de segurança física e encontra-se com acesso ao sistema.

Portanto, existe a necessidade de uma forte política de conscientização de segurança no Espaço Cibernético. Por meio de uma mentalidade que deve ser comum a todos e cultivada no âmbito da OM por meio de palestras e programas de adestramento. Pois pouco adiantará o estabelecimento de rigorosas medidas de segurança se o pessoal responsável pela sua aplicação não tiver consciência de sua importância.

Esta pesquisa mostra que a MB tenta se proteger dessa ameaça interna, dando responsabilidades específicas para os diversos atores que participam do Espaço Cibernético da MB, criando e capacitando elementos internos em cada OM, responsáveis por verificarem e atuarem na SIC, e fortalecendo a mentalidade de segurança em todos os usuários da RECIM, através de adestramentos, instruções, cartilhas e palestras.

Esta pesquisa também revela que a Marinha vem adotando as boas práticas de segurança no Espaço Cibernético: tais como uso de *firewalls* e software antivírus nos computadores dos usuários da RECIM, sendo eles conectados a Internet ou não, além de proteger a própria rede; exigindo que os usuários ao se conectarem provem sua identidade através de autenticação; segmentando as redes de acordo com a necessidade de conhecimento para limitar as conexões

externas; criptografando o tráfego da rede que trafega pelos cabos de fibra ótica e roteadores, e também criptografando os arquivos sensíveis nos computadores, incluindo os dados armazenados nos servidores; e monitorando continuamente as atividades da rede, à procura de conexões não autorizadas, desconectando dispositivos desconhecidos, identificando comportamento suspeitos e mitigando as possíveis vulnerabilidades.

Ao longo desta pesquisa, foi mostrado que a legislação vigente ampara a atividade da Marinha no Espaço Cibernético nacional, nos níveis estratégico, operacional e tático, bem como o de todas as Forças Armadas. Apesar disso, a Política Cibernética de Defesa brasileira ainda é incipiente, assim como a Política Cibernética da maioria dos países, carecendo de toda uma estrutura regulamentar, e isso também se reflete na Marinha do Brasil.

Foi analisada também, a organização e a estrutura da Marinha nas atividades relacionadas ao Espaço Cibernético. Além disto, foi identificado o esforço constante de aperfeiçoamento de suas estruturas, de maneira a melhorar suas capacidades cibernéticas e assim proporcionar a adequada presença no Espaço Cibernético nacional, como a criação em 2019 do CoNavOpEsp, onde a Guerra Cibernética foi inserida no setor operativo da MB, e dentro das Operações Especiais, dando maior flexibilidade para seu emprego durante as operações conduzidas pela MB. Estes esclarecimentos serviram para responder a resposta do problema principal desta pesquisa.

Portanto, a criação do CoNavOpEsp nos mostra que a MB está buscando dominar o seu Espaço Cibernético, pois de acordo com Clarke e Knake (2015), se uma nação está apenas se defendendo no Espaço Cibernético ela está muito atrasada, pois se ela não domina o Espaço Cibernético, não pode controlar outros domínios.

No entanto, na Marinha do Brasil ainda existe a necessidade de uma Doutrina específica para a Guerra Cibernética, visto que atualmente não existe uma Doutrina própria de Guerra Cibernética, a mesma encontra-se ainda em fase de desenvolvimento. Apenas nas Normas de Tecnologia da Informação da Marinha, é que se encontram as questões relativas ao tema e que se define o termo Guerra Cibernética, porém com enfoque mais administrativo. Todavia, não se pode esquecer que a Guerra Cibernética se constitui em um diferencial fundamental às operações de qualquer força militar que queira operar em qualquer conflito, sendo, portanto, uma importante capacidade operativa.

Ainda sobre a organização da MB, a participação de diversas OM atuando no Espaço Cibernético da Marinha do Brasil, onde as atribuições no nível estratégico são confiadas ao EMA, COTIM, COTEC-TIC, ComOpNav, DGMM e DCTIM, e as atribuições do nível tático são confiadas à DCTIM, CoNavOpEsp, CTIM e CLTI, acabam fragmentando as ações no

Espaço Cibernético da MB, contribuindo para dificultar a tomada de decisão neste domínio operacional. A criação de um órgão centralizador, com capacidades cibernéticas ofensivas e defensivas, que possa agir, em caso de um ataque cibernético ou preventivamente, por interesse da MB, conjuntamente com o Exército Brasileiro e a Força Aérea Brasileira, supra essa dificuldade.

Pela análise da pesquisa, a MB deve dedicar especial atenção à capacitação do seu pessoal, para que a Marinha possa estar em melhores condições para atuar no Espaço Cibernético, surge a necessidade da criação de um curso para habilitar os futuros guerreiros cibernéticos, ou até mesmo a criação de uma nova especialidade militar na MB, principalmente para atuarem no setor operativo.

Isoladamente, nem a Marinha do Brasil e nem nenhuma outra instituição conseguirão proteger suas redes sozinhos. Assim, faz-se necessário a cooperação com outros órgãos e instituições nacionais que atuem no Espaço Cibernético, seja através do desenvolvimento de tecnologia ou da colaboração.

A Marinha do Brasil vem aumentando a utilização de soluções próprias para o Espaço Cibernético, através da utilização de sistemas operacionais e de correio eletrônico próprios, e diminuindo a utilização de soluções comerciais que, incluindo o uso da Internet como parte de sua infraestrutura de comando e controle, se torna uma grande vulnerabilidade a suas infraestruturas críticas, contribuindo para essa vulnerabilidade o uso de programas sem licença, impedindo que o produto seja atualizado. Logo, além do desenvolvimento de soluções próprias, a Marinha do Brasil executa uma constante supervisão das redes de modo a banir a utilização de qualquer software que não esteja licenciado para uso, pois basta um único computador vulnerável e conectado à rede para possibilitar um ataque cibernético a toda rede.

Conclui-se, com a análise desta pesquisa que ainda existem lacunas a serem preenchidas no desenvolvimento das capacidades cibernéticas na MB, neste sentido, apresenta-se como oportuno para trabalhos futuros o acompanhamento de tal desenvolvimento. Contudo, a luz da doutrina em vigor, a Marinha do Brasil adota os princípios adequados em suas operações, além estar melhorando a atuação conjunta com outros sistemas públicos e privados em prol da otimização do sistema de Defesa Cibernética, inserindo presença no Espaço Cibernético de modo permanente, com estruturas cada vez mais capacitadas e eficientes, desenvolvendo também, além da Defesa Cibernética de seus ativos de informação e de suas estruturas críticas, ações ofensivas neste novo domínio operacional.

REFERÊNCIAS BIBLIOGRÁFICAS

BARAK, Ohad. Cyber Warfare Revolution?: 1982-2014. 2015. Tese de Doutorado. Bar-Ilan University.

BRASIL. Livro verde: Segurança Cibernética no Brasil/ Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010. 63 p.

_____MD30-M-01 - DOUTRINA DE OPERAÇÕES CONJUNTAS 1º VOLUME. 2011.

_____MD31-P-02 – POLÍTICA CIBERNÉTICA DE DEFESA, 2012.

_____MD31-M-07 - DOUTRINA MILITAR DE DEFESA CIBERNÉTICA, 2014.

_____Plano Estratégico de Tecnologia da Informação da Marinha. PETIM 2016-2019. Conselho de Tecnologia da Informação da Marinha (COTIM), 2015.

_____Diretoria-Geral do Material da Marinha. Cartilha de segurança da informação digital. Rio de Janeiro, 2016.

_____ EB70-MC-10.2 – MANUAL DE GUERRA CIBERNÉTICA. 2017.

_____Mensagem do congresso nacional no 2, de 2017. Política Nacional de Defesa, Estratégia Nacional de Defesa e Livro Branco Nacional. 2017.

_____Decreto nº 9.637, de 26 de dezembro de 2018. Política Nacional de Segurança da Informação – PNSI.

_____Diretoria-Geral do Material da Marinha. DGMM-0540 – NORMAS DE TECNOLOGIA DA INFORMAÇÃO DA MARINHA 3ª REVISÃO. 2019.

_____Decreto nº 10.222, de 5 de fevereiro de 2020. Estratégia Nacional de Segurança Cibernética - E-Ciber.

BRUSTOLIN, Vitelio. Comparative Analysis of Regulations for Cybersecurity and Cyber Defence in the United States and Brazil. Revista Brasileira de Estudos de Defesa. v. 6, no 2, jul./dez. 2019, p. 93–123.

CAMELO, Michel Silva. Guerra Cibernética: a aderência à doutrina brasileira nas ações da segunda guerra do golfo em 2003. Escola de Guerra Naval. Rio de Janeiro, 2020.

CANABARRO, Diego Rafael. The Fog of (Cyber)War: Controversies Revised. 54th ISA Annual Conference. San Francisco (CA), USA. 2013.

CARNEIRO, João Marinonio Enke. A Guerra Cibernética: uma proposta de elementos para formulação doutrinária no Exército Brasileiro. Tese (Doutorado) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

CHAPETTA, Tiago Araujo. Tecnologia e Guerra Cibernética. Escola de Guerra Naval. Rio de Janeiro, 2020.

CLARKE, Richard A.; KNAKE, Robert K. Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito. Brasport, 2015.

COSTA, Cristiano da Silva. Ameaça da guerra cibernética aos sistemas de comando e controle: o impacto que um ataque cibernético pode gerar a um submarino nuclear de ataque. Escola de Guerra Naval. Rio de Janeiro, 2018.

CRAIGEN, Dan; DIAKUN-THIBAULT, Nadia; PURSE, Randy. Defining cybersecurity. Technology Innovation Management Review, v. 4, n. 10, 2014.

DA SILVA, Júlio Cezar Barreto Leite. Guerra cibernética: a guerra no quinto domínio, conceituação e princípios. Revista da Escola de Guerra Naval, Rio de Janeiro, v. 20, n. 1, p. 193, 2014.

DAFLON, Marlon Anderson Santiago. Modelos de dominação do espaço cibernético: as abordagens Brasileira e Russa à guerra cibernética. Rio de Janeiro, 2020.

DARKO Galinec, DARKO Moz nik e BORIS Guberina. “Cybersecurity and cyber defence: national level strategic approach.” In Automatika Journal for Control, Measurement, Electronics, Computing and Communications. 2017.

DAULTREY, Sally. Cyber warfare: a primer. 2017

DE PAULA, Eduardo Rodrigues. Guerra Cibernética: Perspectivas para a consolidação de uma Estratégia cibernética para o Estado brasileiro. Escola de Guerra Naval. Rio de Janeiro,2016.

SOUZA, Leandro Ferrone Demétrio de. A guerra cibernética na marinha do brasil: desafios e aplicações. Escola de Guerra Naval. Rio de Janeiro, 2011.

BENEDITTO ,Marco Eugênio Madeira Di. Defesa cibernética: proposta de estrutura para o âmbito da MB. Defesa dos sistemas ciber-físicos dos meios operativos de superfície da MB. Escola De Guerra Naval. Rio de Janeiro, 2016.

EILSTRUP-SANGIOVANNI, m. Why the World Needs an International Cyberwar Convention. *Philos. Technol.* 2017.

GIFFONI, Marcel de Macedo Lima. O posicionamento das forças armadas brasileiras nos conflitos da guerra cibernética. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 6, n. 11, p. 08-08, 2020.

GUIMARÃES, Flávio de Queiroz. Possibilidades e limitações de emprego da guerra cibernética na MB: métricas para estabelecimento de uma consciência situacional cibernética do eciber-mb. Escola de Guerra Naval. Rio de Janeiro, 2018.

HATHAWAY, Oona A. and Crootof, Rebecca. The Law of Cyber-Attack. Faculty Scholarship Series. 2012.

HENRIQUES, Henrique de Queiroz. Capacitação em cibernética: os desafios do processo de formação de oficiais do Exército Brasileiro para o enfrentamento das demandas da Guerra Cibernética. Rio de Janeiro, 2021.

JÚNIOR, Samuel. A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e índia para o espaço virtual, no 1850, discussion papers, instituto de pesquisa econômica aplicada – ipea. Brasília, 2013.

KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. (Ed.). Cyberpower and national security. Potomac Books, Inc., 2009.

LEITE, Alexandre Cesar Cunha; OLIVEIRA, Ahmina Raiara Solsona. "Cyber conflict: an overview about the recent Asian participation/Conflitos ciberneticos: um overview sobre a participacao asiatica recente." *Meridiano 47*, no. 144, 2014.

LIAROPOULOS, Andrew. Deterrence in Ciberspace: Implications for National Security. MCIS Yearbook. 2012.

NUNES, Luiz Artur Rodrigues. Guerra cibernética: está a MB preparada para enfrentá-la? Escola de Guerra Naval. Rio de Janeiro, 2010.

NYE, Joseph S. Cooperação e conflito nas relações internacionais: Uma leitura essencial para entender as principais questões da política mundial. Editora Gente, 2009.

OTTIS, R. e LORENTS, P. Cyberspace: Definition and Implications. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8 9 April. Reading: Academic Publishing Limited, p. 267-270. 2010.

PAEZ, Eduardo Pablo. La Guerra cibernética en el nivel operacional. Escuela Superior de Guerra Conjunta de Las Fuerzas Armadas. Argentina, 2014.

PALUDETO, Vinicius Luis. A capacidade relacionada à informação de guerra cibernética nas operações de informação. Escola de Aperfeiçoamento de Oficiais. Rio de Janeiro, 2020.

SHMUEL Even e DAVID Siman-Tov, Cyber Warfare: Concepts and Strategic Trends, Institute for National Security Studies. 2012.

SIGNIFICANT CYBER INCIDENTS. Center for Strategic and International Studies (CSIS), 2021. Disponível em: <Significant Cyber Incidents | Center for Strategic and International Studies (csis.org)>. Acesso em: 05 de set. De 2021.

SOUTO, Luís Sérgio da Costa. O uso da guerra cibernética em conflitos: as infraestruturas críticas como alvo. Escola De Guerra Naval. Rio de Janeiro, 2018.

TEIXEIRA JÚNIOR, A. W. M.; LOPES, G. V.; FREITAS, M. T. D. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. Carta Internacional, *[S.*

l.], v. 12, n. 3, p. 30–53, 2017. DOI: 10.21530/ci.v12n3.2017.620. Disponível em: https://www.cartainternacional.abri.org.br/Carta/article/view/620. Acesso em: 16 jul. 2021.

WARF, B.; FEKETE, E. Relational geographies of cyberterrorism and cyberwar. Space & Polity, *[s. l.]*, v. 20, n. 2, p. 143–157, 2016.

WARF, Barney. Cyberwar: A new frontier for political geography, Political Geography, Volume 46, 2015, Pages 89-90.