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

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DAS INFORMAÇÕES E COMUNICAÇÕES

A INFLUÊNCIA DA GUERRA CIBERNÉTICA NO AMBIENTE MILITAR DA MARINHA

1º Ten. EDUARDO VIEIRA CRISTO JUNIOR

Rio de Janeiro
2020

1º Ten. EDUARDO VIEIRA CRISTO JUNIOR

A INFLUÊNCIA DA GUERRA CIBERNÉTICA NO AMBIENTE MILITAR DA MARINHA

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

Orientador: CC Érico da Silva Dias de Oliveira Martins

CIAW
Rio de Janeiro
2020

Cristo Junior, Eduardo Vieira.

A influência da Guerra Cibernética no ambiente militar da Marinha / Eduardo Vieira Cristo Junior. — Rio de Janeiro, 2020.

61f.: il.

Orientador: CC Érico da Silva Dias de Oliveira Martins

Monografia (Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações) — Centro de Instrução Almirante Wandenkolk, Rio de Janeiro, 2020.

1. Defesa Cibernética. 2. Guerra Cibernética. 3. Vulnerabilidades. 4. Marinha. I. Centro de Instrução Almirante Wandenkolk. II. Título.

FOLHA DE APROVAÇÃO

1ºTen. EDUARDO VIEIRA CRISTO JUNIOR

A INFLUÊNCIA DA GUERRA CIBERNÉTICA NO AMBIENTE MILITAR DA MARINHA

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

Aprovada em _____

Banca Examinadora:

_____

CMG (RM1-EN) Gian Karlo Huback Macedo de Almeida

_____

CF (RM1-T) William Augusto Rodrigues de Souza

_____

CC Érico da Silva Dias de Oliveira Martins

CIAW
Rio de Janeiro
2020

Dedico esse trabalho aos homens e mulheres que trabalham nas diversas instituições do governo e cujos silenciosos esforços em manter a Segurança e Defesa Cibernéticas do país nem sempre são reconhecidos. Que vosso trabalho, Guerreiros Cibernéticos, mantenha a Paz e quando necessário facilite a guerra.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela saúde e disposição que nos permite prosseguir nessa jornada, aos meus pais Eduardo e Marlene e à minha irmã Ana Paula por sempre me apoiarem e estarem presentes na minha vida apesar da distância geográfica que limita nosso contato, ao coordenador do curso, comandante Huback pelo exemplo que passou aos alunos quanto à sua constante disposição e boa vontade em participar do curso e ajudar sempre que possível, ao comandante Érico Martins pelas sugestões e orientações que enriqueceram grandemente este trabalho e aos meus colegas de curso pela ótima convivência ao longo desse ano.

A guerra cibernética não é um novo tipo de guerra, limpa e sem vítimas, que devemos adotar. Nem mesmo um tipo de arma secreta que deva ser escondida do público em geral. Pois é o público e as organizações públicas que operam serviços críticos quem provavelmente sofrerão em uma guerra cibernética.

Clarke, R. A e Knake, R. K.

A INFLUÊNCIA DA GUERRA CIBERNÉTICA NO AMBIENTE MILITAR DA MARINHA

Resumo

Este trabalho tem como objetivo estudar as características e os aspectos importantes da guerra cibernética a fim de fomentar o conhecimento necessário para uma análise dos possíveis impactos de um ataque cibernético aos sistemas embarcados em navios e suas consequências para a capacidade operacional dos mesmos. Inicialmente foi apresentado o contexto histórico referente à importância da comunicação na evolução da civilização seguida pela evolução dos sistemas computacionais e seu uso no ambiente militar, surgindo a partir dos desenvolvimentos da Internet e da guerra eletrônica. Em seguida foram apresentados os fundamentos, conceitos e definições da guerra cibernética, necessários para o estabelecimento de um conhecimento básico quanto às possibilidades e riscos que surgiram decorrentes do ambiente cibernético. Seguindo os conceitos referentes ao ambiente cibernético foi apresentada a forma como o Brasil e suas instituições posicionam-se sobre o tema, baseando-se, entre outros documentos, na Estratégia Nacional de Defesa e na Doutrina Militar de Defesa Cibernética. Complementando as características da guerra cibernética foram apresentados as principais formas de ataques cibernéticos, seus possíveis efeitos e estudos de caso, destacando dois tipos de ataques com grande importância para as forças militares devido à sua capacidade de afetar e comprometer fisicamente estruturas críticas e industriais, o Stuxnet e o Triton. Em seguida foram apresentadas as documentações internas da Marinha do Brasil referentes ao tema e feita a análise de como a guerra cibernética pode influenciar na correta condução operacional dos meios navais. A análise dos impactos de um ataque cibernético aos sistemas de um navio foi dividida em três macrossistemas, propulsão, governo e geração de energia, armas e sensores; e comunicações, Comando e Controle. A análise apresenta as restrições que um ataque poderia infligir em determinados sistemas e na operação do navio como um todo. Como último elemento do trabalho realizou-se uma conclusão acerca dos elementos anteriormente analisados, pontuando as vulnerabilidades presentes e que tendem a aumentar com a modernização de meios e o emprego cada vez maior de elementos computacionais, reforçando a grande importância do continuado estudo do tema e da necessidade de se aprimorar as capacidades de defesa cibernética da Marinha para que essa possa continuar realizando suas atribuições, de forma eficiente, num cenário mundial cada vez mais dependente do ambiente cibernético.

Palavras – chave: Defesa Cibernética, Guerra Cibernética, Marinha, Vulnerabilidades.

LISTAS DE SIGLAS E ABREVIATURAS

ADMIN	Administrador da Rede
C2	Comando e Controle
CLP	Controlador Lógico Programável
Cmt	Comandante(s)
COTS	*Comercial off The Shelf*
CTIM	Centro de Tecnologia da Informação da Marinha
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DDoS	*Distributed Denial of Service*
DFARS	*Defense Federal Acquisition Regulation Supplement*
DGMM	Diretoria Geral de Material da Marinha
DNS	*Domain Name System*
DoS	*Denial of Service*
DVR	*Digital Video Recorder*
ELF	*Executable and Linkable Format*
EMA	Estado-Maior da Armada
EUA	Estados Unidos da América
FA	Forças Armadas
GCR	Guerra Centrada em Redes
GPS	*Global Positioning System*
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
ICS	*Industrial Control Systems*
IoT	*Internet of Things*
ISIC	Instrução de Segurança da Informação e Comunicação
MAGE	Medidas de Apoio à Guerra Eletrônica

MB	Marinha do Brasil
MCA	Motor de Combustão Auxiliar
MCP	Motor de Combustão Principal
OMs	Organizações Militares
OSIC	Oficial de Segurança da Informação e Comunicação
RECIM	Rede de Comunicações Integradas da Marinha
RSA	Rivest – Shamir – Adleman
SHA	*Secure Hash Algorythm*
SIS	*Safety Instrumented System*
STIC2	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
VPN	*Virtual Private Network*

SUMÁRIO

1 – INTRODUÇÃO

Desde os primórdios da civilização as comunicações entre pessoas, grupos e povos teve um papel fundamental para a evolução da civilização humana como a conhecemos hoje, mesmo antes da escrita o homem já expressava aos demais suas necessidades, aspirações, dúvidas e medos através de formas diferentes de arte como a pintura, dança e música. A fala tem como produto do seu conhecimento coletivo, a língua, um dos fatores que determinam a identidade e união de um povo.

A comunicação evoluiu junto com a humanidade, a invenção da escrita cerca de 3000 a.C. permitiu que houvesses registros mais detalhados e específicos de fatos e situações pois deferentemente de uma pintura, não dependiam da interpretação de quem estava vendo. As civilizações mais avançadas do passado tinham sistemas de comunicação e registro avançados que nos permite conhecer seus costumes e sua história mesmo após milhares de anos. Já no Império Romano, no auge dos conhecimentos clássicos da filosofia, arte e política, surgiu a necessidade não apenas de se comunicar, mas de fazê-lo de forma que apenas o endereçado da mensagem saiba seu conteúdo, surgiu assim a necessidade da comunicação segura e com ela o uso das primeiras mensagens cifradas e códigos secretos. Os séculos se passaram e com o advento da prensa mecânica por Gutemberg em 1450 os documentos e livros que antes eram manuscritos e reservados à elite das nações tornaram-se de uso público, uma verdadeira revolução no acesso à informação.

No século XIX a comunicação escrita já era uma realidade global e serviços de correios levavam cartas e entregas para todos os continentes, porém o ser humano, em sua busca incansável pelo aprimoramento e pela evolução, não estava satisfeito com o tempo necessário para a entrega dessas mensagens, então com base nos estudos de eletricidade e magnetismo surgiu em 1843 o primeiro telégrafo de longa distância, criado por Claude Chappe 45 anos antes e aprimorado para um modelo funcional por Samuel Morse. Passados trinta anos da implementação do telégrafo Alexander Graham Bell e Thomas Watson apresentaram ao mundo o telefone, outros cinquenta anos seriam necessários para que todos os continentes estivessem interligados por linhas telefônicas, uma mensagem que em 1830 levaria meses para ir da Inglaterra à Austrália agora poderia ser entregue em minutos, porém isso ainda não era suficiente para o ser humano.

No início do século XX, mais precisamente 1901, o inventor italiano Guglielmo Marconi desenvolveu o que chamava de telegrafia sem fios, conhecida posteriormente como comunicação via rádio. Tal invenção espalhou-se rapidamente e em poucos anos já era utilizada em todos os países e de forma inédita também em meios móveis como trens e navios. Durante a Primeira Guerra Mundial a utilização do rádio foi fundamental para a organização estratégica das forças militares e consequentemente a segurança e confiabilidade de tais informações tornou-se muito valiosas, dessa formas surgem as primeiras tentativas de interceptar as comunicações inimigas e de proteger as próprias, primórdios da Inteligência Eletrônica e da Guerra Eletrônica. O emprego intensivo de criptografia e a utilização de técnicas para decifrar as comunicações inimigas tornaram-se necessários e permanentes.

No período entreguerras mantiveram-se os estudos sobre as comunicações via rádio e tecnologias capazes de mantê-la segura, grande parte dos países avançados possuíam seus próprios sistemas de rádio e instituições dedicadas ao estudo de sistemas criptográficos e à interceptação e análise das comunicações de outros países.

A corrida armamentista observada nesse período também pôde ser verificada nos meios e métodos de coleta de informações e de dados criptológicos. Segundo dados apresentados pela U.S. Fleet Cyber Command (2019), a Marinha dos EUA devido à sua extensa operação de Inteligência de Comunicações interceptou e decifrou grande quantidade de comunicações militares japonesas por ocasião de manobras e exercícios militares ocorridos em 1930, essas comunicações continham diversos planos e possibilidades de ações caso o Japão entrasse em guerra contra os EUA.

Quando os EUA entraram na Segunda Guerra Mundial, em 07 de dezembro de 1941, já haviam decifrado entre 10 e 15% das comunicações japonesas e esse porcentual foi sendo incrementado progressivamente até que 19 de maio de 1942 a equipe responsável pela quebra dos códigos japoneses, situada em Pearl Harbor, conseguiu deduzir que a próxima grande investida japonesa ocorreria contra as ilhas Midway em 04 de junho, tal informação foi fundamental para o preparo das forças norte-americanas e seu sucesso nessa batalha tida como o ponto de inflexão da guerra no pacífico. A partir desse momento grande parte das comunicações japonesas eram interceptadas e decifradas de forma que os EUA obtiveram uma vantagem considerável sobre os japoneses até o fim da guerra.

Nos anos que se sucederam após o fim Segunda Guerra Mundial e com o surgimento da Guerra Fria a tecnologia manteve sua acelerada evolução, dessa vez baseada em uma máquina desenvolvida e utilizada por Allan Turing durante a guerra para decifrar os códigos de guerra alemães, essa “máquina de computar” acompanhado do protótipo Mark-1

da universidade de Harvard tornaram-se a base teórica para o surgimento dos primeiros computadores modernos e para o surgimento de uma nova ciência, a computação. O computador, como tecnologia, apresentou uma evolução muitas vezes mais rápida que seus sucessores. O advento dos transistores não só incrementou grandemente sua capacidade cálculo e processamento como também possibilitou a miniaturização de seus componentes, transformando-o de uma gigantesca máquina de calcular com fins acadêmicos e militares para uma máquina menor que uma geladeira, que poderia ser utilizada pela indústria para fins de automação, pelas empresas para gerenciamento de informações e cálculos complexos e posteriormente pela população como ferramenta de trabalho ou diversão. Em paralelo à evolução do computador, surge outra tecnologia que mudaria definitivamente os rumos da comunicação, proporcionando a maior disponibilidade de dados e informações já vista na humanidade, a Internet.

Segundo Tanenbaum (2002), a Internet, como a conhecemos hoje, teve suas raízes na antiga ARPANET, uma rede de comando e controle do Departamento de Defesa dos EUA, criada no início da guerra fria com o objetivo de integrar seus centros de comando de uma forma mais segura e com maior tolerância a falhas que as redes telefônicas usadas na época. A solução encontrada foi o uso de tecnologia digital, utilizando comutação por pacotes e formando uma rede de máquinas (computadores) que poderiam utilizar o sistema para se comunicar. Após sua implementação, diversas universidades começaram a unir suas redes locais a essa rede nacional formando assim a rede física embrionária do que hoje é a Internet.

A Internet extrapolou os limites da aplicação militar e popularizou-se originalmente como forma de buscas e pesquisas acadêmicas e posteriormente pelos mais variadas formas de serviços e entretenimentos oferecidos. Para que se tenha uma ideia da dimensão do crescimento e da utilização da Internet ao longo do tempo, o Internet World Stats (2019) estima que em 1995 havia 16 milhões de usuários, representando 0,4 % da população mundial. Em dezembro de 2017 estima-se que o número de usuários fosse de 4,157 bilhões de usuários, representando 54,4% da população mundial. Essa grande inserção da Internet na sociedade trouxe diversos benefícios e facilidades, podendo conectar qualquer pessoa do planeta a qualquer outra pessoa, instituição ou objeto, desde que esteja conectado à rede.

Devido à grande utilização de computadores e posteriormente da Internet nos mais diversos ramos da sociedade, e assim como qualquer tecnologia emergente, não demorou para que pessoas mal intencionadas, agentes maliciosos, desenvolvessem formas de explorar suas características, erros e vulnerabilidades nos sistemas digitais a fim de obter benefícios próprios. A princípio a exploração dessas vulnerabilidades era vista apenas como brincadeiras

de mal gosto ou novas formas de realizar crimes e fraudes, mas rapidamente organizações militares ao redor do mundo perceberam o grande potencial oculto nas ações que ocorrem no ambiente cibernético e que são capazes de gerar consequências no mundo real, tais aplicações poderiam ser utilizado como uma nova forma de armamento e de combate, uma evolução da Guerra Eletrônica.

Atualmente a chamada Guerra Cibernética tornou-se a forma mais abrangente de afetar um oponente devido justamente ao alto nível de dependência que todas as pessoas e consequentemente os países possuem em relação aos sistemas computacionais e à Internet. O estudo e desenvolvimento de novas técnicas e tecnologias associadas a Guerra Cibernética, à Defesa Cibernética e à Segurança Cibernética vêm recebendo uma crescente atenção dos principais agentes globais, e atualmente é utilizada não somente por países buscando vantagens estratégicas em um conflito futuro, mas também entre organizações e empresas rivais.

1.1 Apresentação do Problema

A atual abrangência do uso de elementos computacionais nos sistemas embarcados dos navios e sua tendência em serem integrados uns aos outros e à Internet propiciou o surgimento de uma nova vulnerabilidade aos meios navais, mas que já possui longos estudos entre o público civil, os Ataques Cibernéticos. Com a popularização da internet a partir década de 1990 surgiram também agentes maliciosos com o objetivo de tirar proveito e buscar benefícios ilícitos dos erros e brechas presentes nos sistemas computacionais ligados à Internet. As chamadas vulnerabilidades estavam presentes tanto na forma física, nos computadores e elementos que compunham a rede, quanto na forma lógica, nos programas e códigos que compunham os serviços disponibilizados.

Como qualquer outra tecnologia promissora, a internet e a integração computacional de sistemas foram rapidamente incorporados aos sistemas militares, porém acompanhando as facilidades adquiridas vieram as vulnerabilidades intrínsecas do ambiente cibernético e também a oportunidades de explorar as vulnerabilidades dos sistemas inimigos, dessa forma, os recursos de Tecnologia da Informação tornaram-se arma contra os sistemas computacionais de um país oponente e consequentemente o ambiente cibernético deixou de ser apenas um espaço de pesquisas, compras e entretenimento para tornar-se o mais novo campo de batalha.

1.2 Objetivos

Este trabalho tem como objetivo principal a reunião de informações acerca do surgimento e evolução da guerra cibernética ao longo dos anos, apresentando suas características, oportunidades e vulnerabilidades de forma clara e direta e com base nessas informações, realizar uma análise e exposição sucinta sobre as possíveis implicações do seu uso em um ambiente militar moderno tendo como público-alvo os militares e civis que trabalham na Marinha.

Ao reunir e analisar grande quantidade de informações referentes à guerra cibernética esse trabalho se torna mais um subsídio ao estudo do tema, ainda em desenvolvimento na Marinha, podendo também contribuir para a criação de trabalhos futuros e o fomento da mentalidade de segurança atinente ao assunto para o público interno da Marinha.

1.3 Metodologia

A metodologia adotada nesse trabalho é qualitativa quanto aos dados analisados e bibliográfica quanto ao meio pois grande parte dos materiais utilizados são oriundos de livros, artigos acadêmicos e doutrinas das Forcas Armadas referentes ao tema. Quanto aos fins, a metodologia utilizada é considerada descritiva e aplicada pelo seu objetivo prático de demonstrar, com base nos dados analisados, as implicações reais que a guerra cibernética pode ter para a Marinha do Brasil e seus meios operacionais.

2 – REFERENCIAL TEÓRICO SOBRE GUERRA CIBERNÉTICA

Este capítulo tem como objetivo apresentar definições importantes para a formação de uma base conceitual e correto entendimento da dimensão e importância atuais da guerra cibernética e que tendem a crescer cada vez mais. Para tal serão apresentados conceitos quanto à guerra e ao espaço cibernético, suas divisões, classificações e a descrição de como atuam os ataques no meio cibernético, apresentando os principais exemplos ocorridos ao redor do mundo. Para chegarmos à guerra cibernética devemos passar por dois passos importantes na construção do conhecimento, constituídos pela definição de dois termos: Guerra e Cibernética.

2.1 – A Guerra

A Guerra é um conceito que vem evoluindo ao longo do tempo e se estabelece desde a definição simples de um dicionário como "a luta armada entre dois ou mais países ou grupos ou situação de forte competição entre lados opostos" (CAMBRIGE, 2020) passando por definições mais complexas como a de Clausewitz (2007):

> (…) a guerra não é meramente um ato de política, mas um verdadeiro instrumento político, uma continuação das relações políticas realizada com outros meios. O que continua sendo peculiar na guerra é simplesmente a natureza peculiar dos seus meios (…) O propósito político é a meta, a guerra é o meio de atingi-lo, e o meio nunca deve ser considerado isoladamente do seu propósito. (CLAUSEWITZ, 2007, p. 91).

Chega-se à definição contemporânea de Long (2012) que a define a guerra como "a execução coerente de <u>todos os meios</u> para garantir adesão suficiente à vontade de uma nação na arena internacional (global), resultando em <u>conflito armado somente quando todos os outros meios falham</u>" (tradução nossa e grifo do autor). Observa-se que a última definição apresenta a guerra não apenas como um conflito armado, mas como um conjunto de ações a fim de se obter uma vantagem ou impor sua vontade sobre os outros, praticada entre nações e sendo considerada como o último recurso quando os demais já falharam.

2.2 – Cibernética

Conceito muito antigo cuja origem grega "*kybernetikos*" ou "boa direção" foi usado por cientistas e pesquisadores ao longo dos anos para se referir a uma "ciência sobre controle, governo e comunicação nos animais e máquinas" (BRITANNICA, 2014, apud WIENER, 1948). Atualmente o conceito de cibernética está intrinsecamente ligado à informática, computação e comunicação digital como apresentado por (BRASIL 2017, p.2-2) "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".

2.3 – Espaço Cibernético

O Espaço Cibernético é o ambiente digital que abrange e conecta redes físicas, definido como "espaço virtual composto por dispositivos computacionais conectados em rede ou não, onde as informações digitais transitam e são armazenadas" (AMORIM, 2014, p. 18) pensamento alinhado à definição de Kuehl (2009) que apresenta o espaço cibernético como um domínio caracterizado pelo uso de eletrônicos e do espectro eletromagnético para armazenar, modificar e trocar informações através de sistemas interconectados.

2.4 – Guerra Cibernética

Tendo definido esses termos é possível estabelecer uma ligação entre eles e construir uma ideia acerca da Guerra Cibernética como sendo o conflito no Espaço Cibernético, essa conclusão básica é melhor explicada pela seguinte definição onde a guerra cibernética:

> Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações

> ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC (AMORIM; 2014, p. 19).

Cabe mencionar que de maneira genérica a Guerra Cibernética apresenta um contexto de conflito entre estados e não deve ser confundida com Crime Cibernético:

> Crime onde um computador é o objeto do crime ou é usado como uma ferramenta para cometê-lo, acessando informações pessoais de usuários; informações confidenciais de negócios, informações governamentais ou desativando dispositivos. (SECURITY, 2018).

Fica claro que ambas definições possuem muito em comum sendo difícil separá-las uma da outra, em última análise a guerra cibernética seria a aplicação de um conjunto de crimes cibernéticos que têm como alvo as instituições e infraestruturas críticas de um país oponente, a fim de prejudicá-las e consequentemente afetar a capacidade de tal país em garantir seus interesses e/ou sustentar um conflito, ao mesmo tempo que utiliza práticas para manter as próprias redes e sistemas funcionando de forma segura.

Com base nos fatos expostos chega-se à conclusão de que "O ambiente cibernético pode ser considerado um novo domínio ou palco de batalha; depois da terra, do mar, do ar, do espaço exterior e do espectro eletromagnético" (SALDAN, 2011). A guerra cibernética assumiu junto com a guerra eletrônica como as formas de guerra capazes de atuar e influenciar em todos os outros ambientes de um conflito e com possibilidade de ser utilizada antes mesmo do início das hostilidades de um conflito armado.

As Forças armadas de diversos países já consideram o Espaço Cibernético e suas peculiaridades no planejamento e condução de suas operações devido ao intenso uso de componentes computacionais em suas forças e da integração entre eles, a chamada Guerra Centrada em Rede:

> A GCR parte do princípio da integração dos diversos sistemas de apoio ao combate no intuito de se obter uma consciência compartilhada, com vistas a facilitar a tomada de decisão dos comandantes (Cmt) nos diversos níveis. Ela busca um maior grau de sincronização da informação, levando a um aumento significativo na agilidade e eficácia dos processos. (GUEDES, 2016, p. 12)

2.5 – Ações Cibernéticas

Para uma melhor análise da Guerra Cibernéticas essa é classificada em três tipos abrangentes de Ações Cibernéticas, Ataque, Proteção e Exploração Cibernéticos.

> Ataque Cibernético – Compreende as ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de comunicação do oponente.
> Proteção Cibernética – abrange as ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações (…) É uma atividade de caráter permanente.
> Exploração Cibernética – consiste em ações de busca ou coleta, nos Sistemas de Tecnologia da Informação de interesse, a fim de obter a consciência situacional do ambiente cibernético. Essas ações devem preferencialmente evitar o rastreamento e servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas. (AMORIM, 2014, p. 23).

3 – A ESTRUTURA CIBERNÉTICA BRASILEIRA

Neste capítulo será apresentada a estrutura estabelecida no Brasil Referente à segurança e defesa cibernéticas e suas divisões, características, objetivos e responsabilidades.

3.1 – Os fundamentos da Guerra Cibernética no Brasil

No Brasil os estudos relacionados ao Setor Cibernético ganharam crescente interesse a partir do início dos anos 2000, porém ainda faltava uma correta regulamentação legal e doutrinária, bem como a atribuição de responsabilidades aos agentes envolvidos. Essas lacunas foram preenchidas com a criação da Política Nacional de Defesa em 2012 que estabelece entre suas orientações que:

> Os setores espacial, cibernético e nuclear são estratégicos para a Defesa do País; devem, portanto, ser fortalecidos. (…) Para se opor a possíveis ataques cibernéticos, é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam seu pronto restabelecimento (BRASIL, 2012a, p. 32)

Ficou clara a importância e prioridade que o estudo do Setor Cibernético possui. Na Estratégia Nacional de Defesa, documento diretamente associado à Política Nacional de Defesa fica reforçada tal importância e são apresentados oito enfoques a serem trabalhados:

> **(a)** Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;
> **(b)** Aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à cerificação digital (….);
> **(c)** Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional (…) com vistas à criação da Escola Nacional de Defesa Cibernética;
> **(d)** Desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;

> **(e)** Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional (…);
> **(f)** Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;
> **(g)** Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e
> **(h)** Estruturar a produção de conhecimento oriundo da fonte cibernética. (BRASIL, 2012b, p. 94).

Fica também estabelecido que no Setor Cibernético:

> o Ministério da Defesa e o Ministério da Ciência Tecnologia e Inovação, por intermédio do Departamento de Ciência e Tecnologia do Exército, promoverão ações que contemplem a multidisciplinaridade e a dualidade das aplicações, o fomento da Base Industrial de Defesa com duplo viés: aquisição de conhecimento e geração de empregos, e a proteção das infraestruturas estratégicas, com ênfase para o desenvolvimento de soluções nacionais inovadoras (BRASIL, 2012b, p. 142).

Ficou assim definida a divisão dos três eixos vitais de desenvolvimento entre as três Forças Armadas onde a Marinha, o Exército e a Forca Aérea coordenam respectivamente os Setores Nuclear, Cibernético e Espacial. A Estratégia Nacional de Defesa ainda determinou a realização dos estudos que culminaram na criação da Escola Nacional de Defesa Cibernética em Fevereiro de 2019 como uma instituição com "estrutura de ensino de caráter dual, civil e militar, contribuindo para a formação e especialização de recursos humanos que atuarão no setor cibernético" (BRASIL, 2019).

Os assuntos relacionados à cibernética foram divididos entre Segurança cibernética, a cargo da Presidência da República, e com o objetivo 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" (AMORIM, 2014, p. 19) e a Defesa Cibernética a cargo do Ministério da Defesa e das Forças Armadas, definida como o:

> Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com a finalidade de proteger os

> sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponente. (AMORIM, 2014, p. 18).

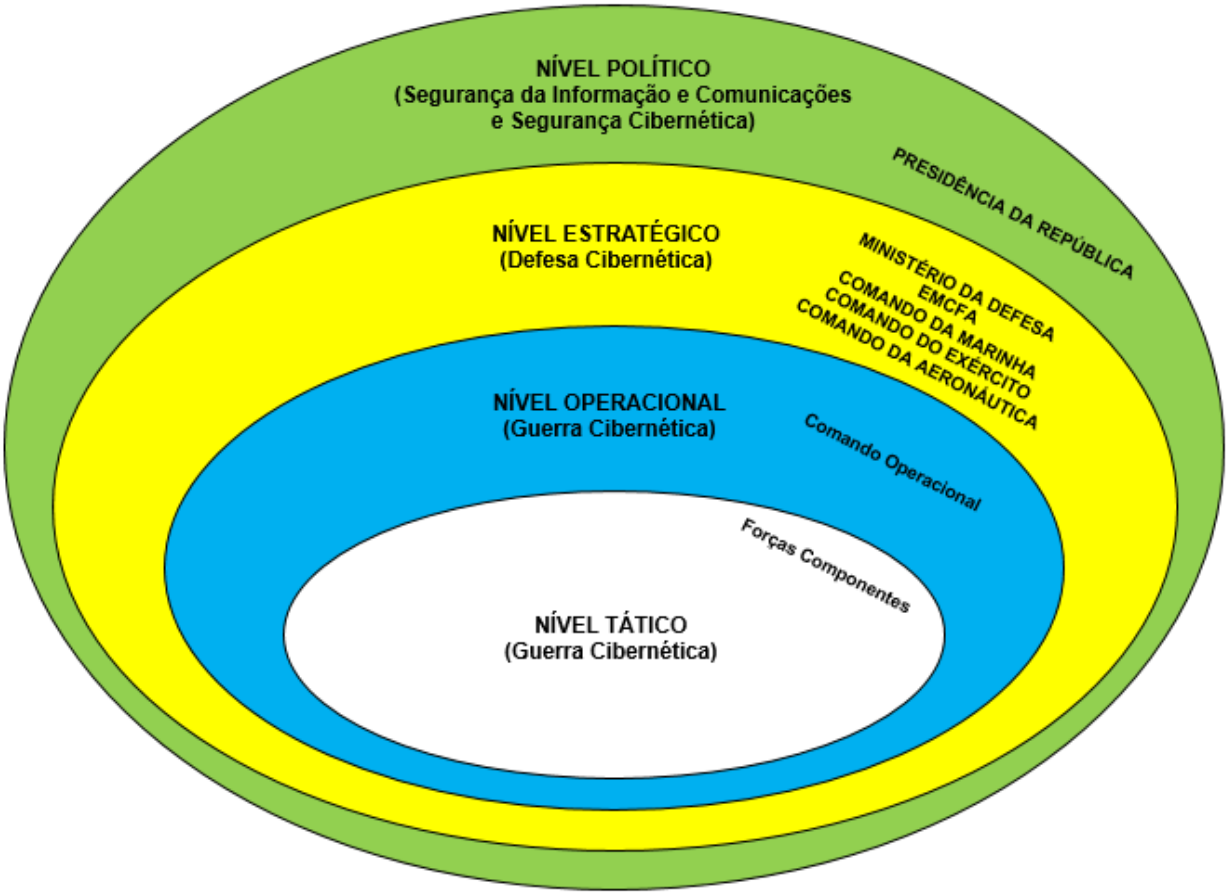
Dessa forma delimitou-se o objetivo e competência dos agentes envolvidos ainda que diversas situações requeiram uma ação conjunta dos órgãos envolvidos.

3.2 – As Divisões da Guerra Cibernética no Brasil

As Ações Cibernéticas também possuem definições diferentes de acordo com um dos três níveis de decisão envolvidos:

> **Nível político –** Segurança da Informação e Comunicações e Segurança Cibernética – coordenadas pela Presidência da República e abrangendo a Administração Pública Federal direta e indireta, bem como as infraestruturas críticas da Informação Nacionais;
> **Nível estratégico –** Defesa Cibernética – a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal; e
> **níveis operacional e tático –** Guerra Cibernética – denominação restrita ao âmbito interno das Forças Armadas. (AMORIM, 2014, p. 17).

Figura 3.1: Níveis de Decisão



Fonte: Doutrina Militar de Defesa Cibernética; 2014, p.17.

3.3 – Defesa Cibernética

Dentre as diversas características da Defesa Cibernéticas apresentadas na Doutrina militar de Defesa Cibernética, Amorim (2014), destacam-se:

- Alcance Global, o que possibilita a execução de ações em escala global, limitações físicas de distância não se aplicam no Espaço Cibernético;
- Mutabilidade e Incerteza, onde as ações no Espaço Cibernético podem não gerar os efeitos desejados devido às diversas variáveis afetadas pelas condições ambientes que alteram o comportamento dos sistemas informatizados; e
- Dualidade e Paradoxo Tecnológico, onde as mesmas ferramentas usadas para detectar falhas e vulnerabilidades dos sistemas podem ser usadas por atacantes tentando explorá-las ou por administradores dos sistemas tentando

> corrigi-las bem como quanto mais tecnologicamente desenvolvido está um sistema, mais dependente da Tecnologia de informação ele também estará, necessitando, consequentemente, desenvolver sua capacidade de defesa cibernética.

3.4 – A Política Cibernética de Defesa

A Política cibernética de Defesa apresenta nove objetivos relacionados ao tema, apresentando diretrizes específicas a serem implementadas para alcançar cada objetivo. Dentre os objetivos destaca-se os diretamente relacionados ao setor operativo:

> – Assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas (FA) e impedir ou dificultar sua utilização contra interesses da Defesa Nacional;
> – Colaborar com a produção do conhecimento de Inteligência, oriundo da fonte cibernética, de interesse para o Sistema de Inteligência de Defesa (SINDE) e para os órgãos de governo envolvidos com a SIC e Segurança Cibernética, em especial o Gabinete de Segurança Institucional da Presidência da República (GSI/PR); e
> – Cooperar com o esforço de mobilização nacional e militar para assegurar a capacidade operacional e, em consequência, a capacidade dissuasória do St Ciber. (BRASIL, 2012c, p.13).

Os demais itens apresentam a importância da capacitação pessoal, pesquisa, desenvolvimento e a criação e constante atualização de legislação e doutrinas específicas ao Setor Cibernético.

4 – ATAQUES CIBERNÉTICOS E SUAS CARACTERÍSTICAS

Neste capítulo serão apresentados os tipos mais comuns de ataques cibernéticos praticados nos últimos anos, suas formas de atuação e exemplos de como podem afetar sistemas e corporações.

4.1 – Definições

Para melhor compreensão de como os sistemas computacionais funcionam e como ataques cibernéticos podem afetá-los é importante que sejam apresentadas algumas definições acerca do tema.

4.1.1 – Vulnerabilidade

Em linhas gerais a vulnerabilidade é tida como uma fraqueza ou defeito de um sistema que pode ser explorado por um atacante, ou como explicado pela Kaspersky (c2019) uma das maiores empresas no ramo de segurança digital, a vulnerabilidade está associada a violações em uma política de segurança, explorando regras de segurança fracas ou problema no próprio software, de forma que todos os sistemas computacionais têm vulnerabilidades, que podem ou não usadas para causar danos ao sistema.

4.1.2 Rede de Computadores

Ligação entre dois ou mais componentes eletrônicos com capacidade de se comunicarem via códigos ou dados, “estabelece uma arquitetura coesa que permita a vários tipos de equipamentos transferir informações de maneira quase perfeita” (BRITANNICA, 2019, tradução nossa).

4.1.3 – Ataques Cibernéticos e seus tipos

Seguindo a definição de ataque cibernético apresentada no capítulo 2, suas principais formas de atuação são baseadas no ataque à rede em que o alvo está ligado e no

ataque ao alvo propriamente dito. Tradicionalmente os ataques cibernéticos são divididos quanto à sua forma de ataque entre Passivos e Ativos.

a) O Ataque Passivo visa obter informações úteis ao analisar o fluxo e o tráfego de dados bem como inspecionar suas características e seu conteúdo com a finalidade de utilizar tais informações para obter vantagem em um futuro ataque ao alvo. Por sua característica passiva, que não altera nenhuma informação, e pelo fato de geralmente estar aplicado na rede em que o alvo se conecta e não no próprio alvo, torna-se difícil de se detectar e para evitá-lo é necessária a utilização de ferramentas criptológicas na comunicação a fim de garantir a confidencialidade dos dados transmitidos. Utiliza-se também técnicas conhecidas como Tunelamento da Comunicação ou mais popularmente como *VPN* que utilizam o método de preenchimento do tráfego, inserindo informações inúteis e aleatórias no trafego, para dificultar sua análise.
b) O Ataque Ativo utiliza-se da interceptação e alteração de dados e informações trafegando na rede e também da alteração de dados e do estado de funcionamento do próprio sistema, explorando suas vulnerabilidades a fim de se obter acesso não autorizado a informações sigilosas ou alterar internamente seu funcionamento visando algum lucro, benefício ou outros objetivos ilícitos.

4.2 – Os *Malwares*

Os ataques propriamente ditos são feitos através de diversas ferramentas e programas conhecidos como *Malware* ou *malicious software,* alterados a partir de um *software* legítimo ou especificamente criados para um fim malicioso. O *Malware* também pode ser definido como um "*software* usado ou criado para interromper a operação de um computador, coletar informações confidenciais ou obter acesso a sistemas de computadores privados". (HARRIS, 2013 p. 3, tradução nossa). Os malwares possuem diversas formas e tipos, dentre os mais difundidos estão:

a) Virus - "Um vírus de computador é um programa que pode se espalhar por computadores e redes fazendo cópias por si mesmo, geralmente sem o conhecimento do usuário." (OLDFIELD, 2001, p. 8, tradução nossa).

b) Verme – os vermes ou *Worms* possuem atuação e objetivos semelhantes aos do vírus, porém torna-se ainda mais perigoso pois não necessita de hospedeiro para se reproduzir, "*Worms* simplesmente criam cópias de si mesmos e usam a comunicações entre computadores para se espalhar." (OLDFIELD, 2001, p. 9, tradução nossa).

c) Cavalo de Troia – *Trojan*, em analogia a lenda grega, consiste em um programa ou função legítima utilizado pelo usuário, mas que contém um conteúdo oculto que é executado sem seu conhecimento. "Uma vez ativados, os Trojans podem permitir que cibercriminosos o espionem, roubem seus dados confidenciais e obtenham acesso *backdoor* ao seu sistema. (….) Interrompendo o desempenho de computadores ou redes de computadores" (KASPERSKY, c2020a, tradução nossa)

d) *Backdoor* – São vulnerabilidades implantadas no sistema por um vírus ou *Trojan* que permitem ao atacante um acesso facilitado nas próximas vezes que atacar esse sistema, "um backdoor refere-se a qualquer método pelos quais usuários autorizados e não autorizados possam contornar as medidas normais de segurança e obter acesso (…) a um sistema de computador, rede ou aplicativo de software (…) para roubar dados pessoais e financeiros, instalar malwares adicionais e invadir dispositivos." (MALWAREBYTES, c2020, tradução nossa).

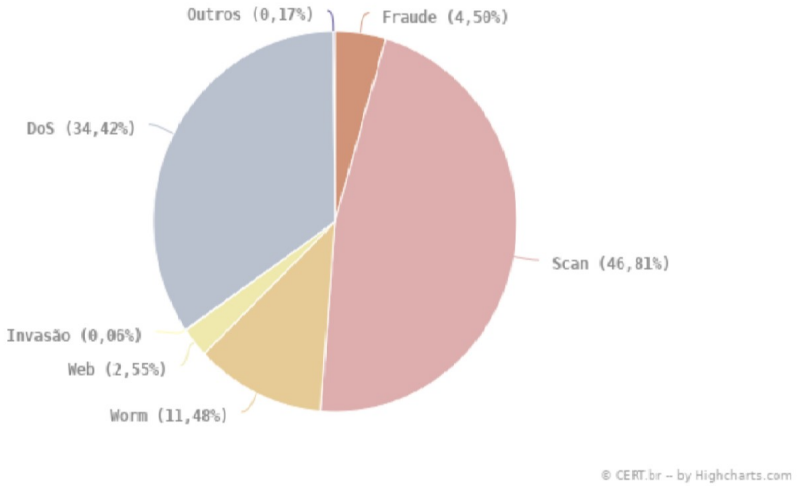
e) *Bot/botnet – Bot,* abreviação do termo inglês *Robot,* refere-se à forma como um atacante acessa o sistema de um computador através de um *Trojan* ou vírus, e instala um programa que permita controlá-lo remotamente, como um robô. O processo de criação é então repetido em diversas outras máquinas formando uma verdadeira rede de robôs ligados ao atacante, a *Robot Network* ou *Botnet*. O atacante utiliza a *Botnet* para executar ataques de grande escala contra um alvo específico que não tem recursos computacionais suficientes para se defender de dezenas ou centenas de milhares de computadores atacando-o ao mesmo tempo. Todo esse processo ocorre muitas vezes sem que os usuários das máquinas *bots* saibam que estão infectados e que fazem parte de uma *Botnet*. Mais recentemente, com a grande expansão da conectividade via rede e Internet nos mais diversos aparelhos, a chamada Internet das Coisas aumentou e muito a quantidade de alvos que podem ser utilizados de forma maliciosa como *bot,* praticamente

qualquer dispositivo com um grau mínimo de processamento e memória como eletrodomésticos e até mesmo câmeras de vigilância podem ser infectados e incluídos em uma *Botnet*.

4.3 – Os *Malwares* no Brasil

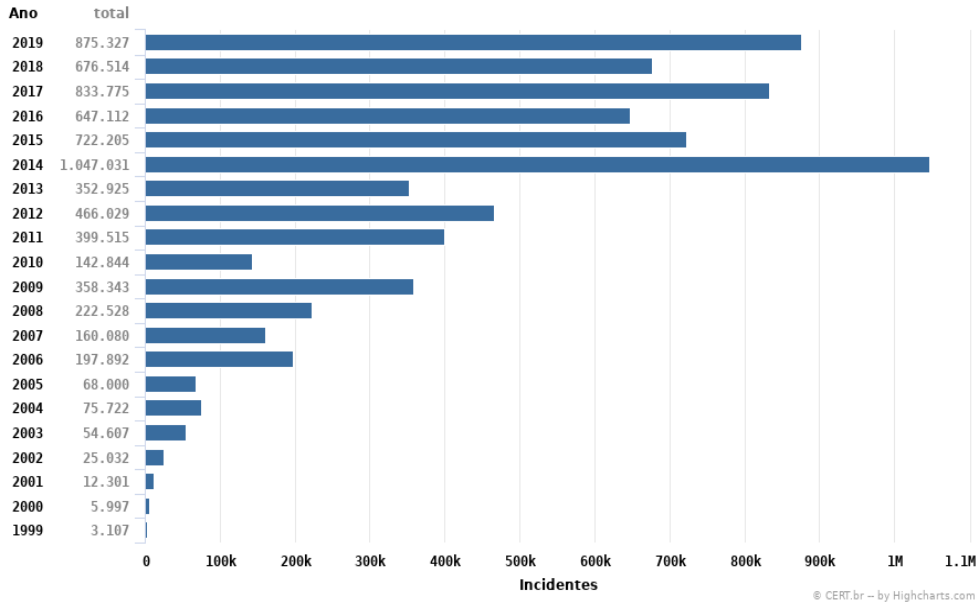
Os gráficos abaixo, elaborados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) apresentam os principais ataques cibernéticos reportados no Brasil no ano de 2019 e demonstram a grande quantidade de incidentes reportados, em seguida segue uma breve definição dos ataques eminentemente digitais como o *Scan*, *DoS*, *Web* e *Worm*.

Figura 4.1 – Tipos de incidentes reportados ao CERT.br em 2019



Fonte: CERT.br.

Figura 4.2 – Total de incidentes reportados ao CERT.br em 2019



Fonte: CERT.br.

4.3.1 – *Scan*

Nesse gráfico fica clara a preponderância dos ataques tipo Scan, que aplicam técnicas ativas e passivas com o intuito de identificar quais computadores estão ativos e os serviços disponíveis neles, de forma a identificar potenciais alvos e associar as vulnerabilidades aos serviços habilitados.

4.3.2 – Negação de Serviço

Em segundo lugar destaca-se o ataque ativo do tipo Negação de Serviço ou *Denial of Service* (DoS), tipo de ataque complexo que se utiliza das características e limitações do alvo e da sua rede contígua para forçar uma sobrecarga em sua infraestrutura a fim de reduzir sua capacidade em fornecer serviços aos seus usuários legítimos ou reduzir sua capacidade de se comunicar, podendo alcançar o bloqueio total do alvo. O atacante pode realizar este tipo de ataque diretamente contra seu alvo, explorando uma vulnerabilidade, ou de forma indireta, utilizando diversos outros dispositivos previamente infectados, uma *Botnet,* para que esses dispositivos ao mesmo tempo realizem grande quantidade de troca de dados ou solicitações inválidas ao alvo, esgotando sua capacidade de responder a todas elas e dificultando o processamento das comunicações legitimas. A Negação de Serviço também é

possível de ser realizada ao se atacar a rede em que o alvo está ligado, manipulando suas características e rotas de forma que todo tráfego chegando ou saindo do alvo seja desviado para um domínio malicioso ou fique perdido na rede.

4.3.3 – Ataque tipo *Web*

Ataque do tipo *Web* é direcionado aos domínios da Internet e aos servidores que os mantêm. Manipula dados a fim de obter acesso não autorizado aos sistemas e serviços por meio de métodos como o Disfarce (*Spoofing*), onde o atacante altera suas características digitais a fim de se passar por um usuário válido. Outro ataque, chamado Man-in-the-middle, onde o atacante se "posiciona entre duas partes que tentam comunicar-se, intercepta mensagens enviadas e depois se passa por uma das partes envolvidas" (MALENKOVICH, 2013).

4.3.4 – *Worm*

Ataque do tipo verme ou *Worm,* como apresentado anteriormente, é caracterizado pela sua forma automatizada de propagação, "Worm é um tipo de malware que espalha cópias de si mesmo de computador para computador. Um Worm pode se replicar sem interação humana e não precisa se conectar a um programa de software para causar danos" (NORTON, c2020, tradução nossa).

4.3.5 – Força Bruta

O ataque conhecido como Força Bruta, apesar de não ser exclusivamente digital e não estar incluso dentre os elementos da análise do CERT.br ainda é muito utilizado e seu método consiste em tirar vantagem do grande poder computacional do atacante a fim de:

> Quebrar uma senha ou nome de usuário ou encontrar uma página da Web oculta ou encontrar a chave usada para criptografar uma mensagem, usando uma abordagem de tentativa e erro e esperando, eventualmente, adivinhar corretamente. Este é um método de ataque antigo, mas ainda é eficaz e popular entre os hackers. Dependendo do tamanho e da complexidade da senha, a quebra pode levar de alguns segundos a muitos anos. (KASPERSKY, c2020b, tradução nossa).

4.4 – Exemplos de Ataques Cibernéticos

Estabelecidas as definições dos tipos mais comuns de ataques passivos e ativos faz-se mister apresentar exemplos concretos e recentes de como esses ataques foram utilizados por agentes maliciosos, para burlar sistemas de segurança e praticar Crimes Digitais e sabotagem industrial e governamental, podendo ser considerado como um ato de guerra cibernética ou de terrorismo cibernético.

4.4.1 – Dragonfly

Em 2011 surge no cenário internacional um grupo de hackers conhecido como dragonfly que tinha como principal alvo o setor de energia e indústrias. Seus ataques visaram inicialmente empresas de defesa e aviação nos EUA e Canadá, mudando seu foco para empresas de energia dos EUA e da Europa no início de 2013 e recentemente incluindo empresas relacionadas a sistemas de controle industrial. O grupo usou duas formas conhecidas de malware: O *Trojan* Karagany e o *Backdoor* Oldrea.

O grupo Dragonfly utilizou três formas de invasão para obter acesso aos sistemas das empresas de energia e controle industrial, como demonstrado posteriormente no relatório produzido pela Symantec, (2014).

O primeiro método foi uma campanha de *phishing*, e-mails maliciosos visando obter dados pessoais importantes de pessoas influentes em um meio, visando executivos selecionados e funcionários seniores, ocorreu de fevereiro até junho de 2013. Os tópicos dos e-mails estavam relacionados a problemas de administração do escritório, como lidar com uma conta ou problemas com uma entrega e possuíam um anexo que quando aberto infectava a máquina do usuário.

O segundo método, utilizado a partir de junho de 2013 foi baseado em ataque do tipo *Watering Hole* onde o grupo comprometia diversos sites relacionados à empresa de energia e injetaram códigos maliciosos em cada um deles. Esses códigos então redirecionavam os visitantes para outros sites aparentemente legítimos, mas que hospedavam o *exploitkit* “Lightsout” que por sua vez, explorava aplicações *Java* e de *Internet Explorer* a fim de efetuar o *download* do *backdoor* Oldrea ou do *trojan* Karagany no computador da vítima.

O terceiro método consiste em uma nova abordagem usada pelos atacantes envolvendo o comprometimento de sites de atualização remota de vários sistemas de controles industriais. Inserindo o *Backdoor* Oldrea junto das atualizações legítimas dos Programas.

4.4.2 – Mirai DDoS

Em setembro de 2016 um grande ataque de Negação de Serviço Distribuído (*Distributed Denial of Service,* DDoS) muito maior do que todos os seus antecessores foi praticado contra o site/blog do pesquisador de segurança digital Brian Krebs, a prestadora de serviços de cyber segurança Akamai tentou mitigar os efeitos do ataque de mais de 600 Gbps, porém em última análise decidiu que não conseguiria manter o site de Krebs em funcionamento e deixou de protegê-lo o qual ficou indisponível por 5 dias. Estudos foram feitos por diversas empresas e agências de segurança cibernética e chegaram à conclusão de que a origem do ataque foi uma nova rede de *botnets* chamada Mirai. A MiraiBotnet difere das demais pois não ataca somente a partir de computadores.

> (…) foi criada usando códigos binários ELF (*Executable and Linkable Format*), um formato de arquivo comum para sistemas baseados em *Linux* e *UNIX*. Esse formato é usado no *firmware* de muitos dispositivos de IoT [Internet das Coisas], incluindo roteadores, DVRs e câmeras IP. (NJCCIC, 2016, tradução nossa).

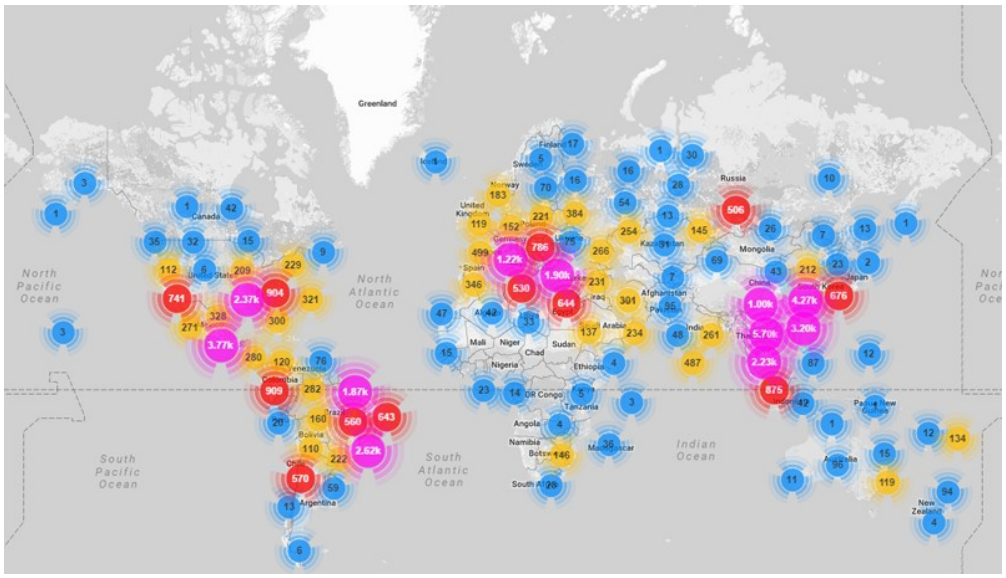
A Célula Integrada de Cibersegurança e Comunicação de New Jersey, (c2019) conhecida como (NJCCIC) detalha em seu relatório a preocupação com a capacidade do Mirai em transformar dispositivos IoT (*internet Of Things*) em *bots*, tais dispositivos nunca foram vistos como potenciais alvos e como tal seu nível segurança sempre foi mantido baixo tanto por parte dos desenvolvedores quanto dos usuários. No mesmo período ocorreu um ataque de proporções semelhantes, à empresa OVH, grande provedora de serviços *web na França*. Estudos posteriores indicaram que o ataque à OVH partiu de mais de 150000 câmeras e equipamentos DVR pertencentes a *botnet* Mirai. Ambos ataques propiciaram o início dos estudos das vulnerabilidades presentes em dispositivos IoT, porém o ataque que se seguiu deixou as autoridades de segurança digital em alerta e mostrou a real capacidade dessa *botnet*. Em 22 de outubro de 2016 a empresa Dyn, dona da infraestrutura de servidores DNS (responsáveis por associar nomes de sites aos respectivos endereços IP) de milhares de sites

nos EUA foi alvo de três ataques sucessivos que reduziram drasticamente sua operação por cerca de 12 horas:

> Devido à força dos ataques que atingiram 1 Tbps. Muitas empresas grandes e populares sentiram os efeitos pois os usuários não conseguiram acessar seus sites por longos períodos de tempo. Os sites afetados incluem: Twitter, Potifar, Amazona, Paypal, GitHub, Netflix, CNBC, entre outros. (NJCCIC, 2016, tradução nossa).

A própria empresa Dyn posteriormente relatou ter sofrido ataques de dezenas de milhões de endereços IP ao mesmo tempo. Um estudo pela companhia de cibersegurança Imperva no fim de outubro de 2016 apontou que a Mirai *botnet* já possuía dispositivos infectados em todo o globo, fato apresentado nos gráficos abaixo:

Figura 4.1 – Quantidade de Maquinas infectadas pelo Mirai Botnet em 2016



Fonte: HERZBERG, BECKERMAN, ZEIFERMAN, 2016.

Figura 4.2 – Localização dos dispositivos Pertencentes à Botnet Mirai em 2016

Country	% of Mirai botnet IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

Fonte: HERZBERG, BECKERMAN, ZEIFERMAN, 2016.

Tais figuras representam a extensão dessa *Botnet* de onde é possível verificar a grande quantidade de dispositivos infectados no Brasil, o que reflete o elevado grau de vulnerabilidade que o país ainda apresenta, atrás apena do Vietnã.

4.4.3 – O Caso do Verme Stuxnet

O Stuxnet é um *Malware* tipo *worm* (verme), descoberto em 2010 é considerado a primeira Ciber Arma realmente aplicada contra a estrutura de um país, inaugurou uma nova era onde os *Malwares* não buscam somente efeitos no mundo virtual como vantagens empresariais, golpes ou roubo de dados, a partir do Stuxnet o *Malware* poderia ser usado para afetar diretamente o mundo real, criando um risco direto à segurança de estruturas e pessoas. Apesar da sua característica de disseminação típica de um *Worm,* foi considerado único pois:

> O que o diferenciou dos milhares de outros worms anteriores a ele é que ele foi projetado para liberar sua carga apenas quando entrava em um sistema de controle

> industrial (ICS) que correspondia às características da instalação de enriquecimento nuclear do Irã em Natanz. (DENNING, 2012, p. 672, tradução nossa).

Apesar de terem sido encontrados rastros da sua infecção em diversos países, foi no Irã que se encontrou grande parte das máquinas infectadas o que caracteriza que o *Worm* foi implementado na rede a partir daquele país para facilitar e agilizar a infecção até o alvo. Foi questão de tempo até o Stuxnet conseguir chegar nas máquinas da instalação de enriquecimento e iniciar seu ataque:

> Adulterou o código do controlador lógico programável (CLP) usado para controlar as centrífugas em Natanz, destruindo cerca de mil centrífugas e interrompendo o programa nuclear do Irã. Nenhum *worm* relatado anteriormente havia feito algo assim antes, seja em termos de precisão de alvos ou causando danos físicos através da manipulação do ICS. (DENNING, 2012 apud FALLIERI, MURCHU, CHIEN, 2011, tradução nossa).

A ação do *Worm* se prolongou desde Junho de 2009 a Maio de 2010 "O ataque foi tão bem-sucedido que o vírus funcionou sem ser detectado por meses, e suas vítimas não o souberam até que as empresas de segurança em todo o mundo o descobriram e começaram a falar sobre ele." (FRANCESCHI, 2016). O emprego do Stuxnet deixou claro a vulnerabilidade intrínseca que as infraestruturas críticas dos países possuem em relação a segurança digital e aos efeitos que um ataque cibernético podem causar, desde atrasos e prejuízos em linhas de produção a acidentes com grandes danos ao material e pessoal em empresas metalúrgicas e petroquímicas podendo provocar grandes *blackouts* de energia elétrica ou falhas de comunicação causadas pela interrupção intencional e sistemática das suas malhas de distribuição.

4.4.4 – O Cavalo de Troia Triton

O último exemplo a ser apresentado refere-se ao ataque cibernético ocorrido em agosto de 2017 em uma empresa petroquímica da Arábia Saudita utilizando-se o *Malware* Triton. O Triton é um tipo de Cavalo de Troia desenvolvido para afetar diretamente os sistemas de controle industriais do modelo Triconex, desenvolvidos pela empresa Schneider Electric, (c2020) que afirma ter implementado seu sistema em mais de 18000 plantas industriais em 80 países. O funcionamento do Triton é semelhante em alguns pontos ao do

Stuxnet de 2010, baseia-se em ganhar acesso aos sistemas tanto por meio de *phishing,* vírus ou *Watering Hole,* uma vez dentro do sistema, instala um backdoor que permite ao atacante acessar e modificar as características do sistema e suas configurações de funcionamento, afetando não só a operação e a produção dessas empresas, mas principalmente alterando os parâmetros de seus sistemas de segurança. A atuação complexa do Triton pode ocasionar diversas consequências aos sistemas industriais como explicado por Johnson et al. (2017):

a) Usar o sistema de segurança para paralisar os processos de produção "O invasor pode reprogramar a lógica do SIS (sistema de segurança instrumental) para fazer com que ele desarme e encerre um processo que está, na realidade, em um estado seguro. Em outras palavras, desencadeie um falso alarme. Implicando em perdas financeiras devido ao tempo de inatividade do processo e ao complexo procedimento de inicialização após o desligamento."
b) Reprogramar o SIS para permitir que o sistema permaneça funcionando em um estado inseguro "O invasor pode reprogramar a lógica do SIS para permitir que condições inseguras persistam, aumentando o risco de uma situação perigosa causar consequências físicas"
c) Reprogramar o SIS para permitir um estado inseguro enquanto usa o sistema de controle da produção para criar um estado inseguro, de risco, cuja consequência é o impacto à segurança humana, ao meio ambiente ou danos aos equipamentos

O Triton é reconhecido como o primeiro Malware que não busca a obtenção de dados ou degradação de sistemas e serviços visando alguma vantagem, devido à sua atuação específica nos sistemas de segurança, sua utilização está diretamente ligada ao seu potencial impacto no mundo real e à segurança das pessoas e que trabalham nas instalações e seus arredores. Apesar da sua grande complexidade e do preparo dos atacantes o ataque do Triton não atingiu o efeito desejado:

> Agora sabemos que um ataque real provavelmente nunca ocorreu. Houve um erro no desenvolvimento do malware que acidentalmente causou a atuação do Triconex e levando-o para um estado seguro. Como resultado, o malware que estava em desenvolvimento foi descoberto. (JACKSON, 2018 apud KLING, 2018, tradução nossa).

Cabe ressaltar que da mesma forma que o Triton ataca plantas industriais ele também poderia ser utilizado contra infraestruturas criticas de um país como sistemas controladores da rede de distribuição elétrica ou de comunicações. O Triton é mais um grande exemplo de como a guerra cibernética pode influenciar diretamente a guerra cinética ao desestabilizar e inutilizar indústrias, instalações e outras infraestruturas críticas do oponente.

Com os exemplos apresentados pode-se observar a grande especificidade e complexidade dos recentes ataques cibernéticos, permitindo que sejam precisos, eficiente e muitas vezes imperceptíveis até que já estejam atuando. Uma parte importante desses ataques é a coleta de informações sobre os alvos, pelos mais diferentes métodos, montando uma análise completa a fim de personalizar o ataque e maximizar sua eficiência, o Stuxnet e o Triton são grandes exemplos disso.

> Os ataques de sabotagem geralmente são precedidos por uma fase de coleta de informações, na qual os atacantes coletam informações sobre redes e sistemas de destino e adquirem credenciais que serão usadas em campanhas posteriores. (SYMANTEC, 2017, tradução nossa).

5 – APLICAÇÕES DA GUERRA CIBERNÉTICA NA MARINHA DO BRASIL

Conforme apresentado no capítulo 3 deste trabalho, a Estratégia Nacional de Defesa atribuiu ao Exército Brasileiro a função e a responsabilidade do desenvolvimento e manutenção da defesa cibernética do Brasil. Esse fato não exime as demais forças de realizarem estudos e desenvolvimentos nessa área tanto para proteger seus próprios sistemas como para contribuir umas com as outras pelo interesse comum, assim sendo, neste capítulo será apresentada de forma sucinta a estrutura montada pela Marinha do Brasil relacionados à sua própria defesa cibernética e será feita uma exposição de como os sistemas da Marinha poderiam ser afetados caso fossem alvos de ataques cibernéticos.

5.1 – A Estrutura Cibernética da Marinha

Na Marinha o tema é abordado principalmente pelas publicações DGMM-540 (Normas de Tecnologia da Informação da Marinha) e EMA-416 (Doutrina de Tecnologia da Informação da Marinha) as quais apresentam diversos conceitos já abordados nesse trabalho e também as atribuições e responsabilidades dos órgãos da MB afetos ao tema.

Fica definido pela DGMM-540 que as instruções de Segurança da Informação e Comunicação (SIC) devem ser aplicadas a:

> a) todas as atividades que envolvam algum trâmite, processamento ou arquivamento de informação em meio eletrônico nas redes locais da MB;
> b) todos os ativos da MB;
> c) todo usuário dos serviços disponibilizados pela rede local; e
> d) contratos efetuados pela MB com empresas privadas, cujo escopo envolva algum tratamento de informações em meio eletrônico ou integradas por meio de uma rede local. (BRASIL, 2019, p. 7-5).

Para o sistema da administração naval foram atribuídas diversas funções, de acordo com sua complexidade, abrangência e importância; entre os diversos níveis de decisão e organização da Marinha. A fim de manter a praticidade deste estudo, serão listadas as atribuições diretamente envolvidas com a Defesa Cibernética na Força.

Dentre as diversas atribuições da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) destacam-se:

> – Planejar, coordenar e controlar as atividades técnicas e administrativas de SIC;
> – Supervisionar e analisar todas as atividades que possam afetar os requisitos de SIC da MB;
> – Promover e fomentar o incremento progressivo da mentalidade de SIC; e
> – Determinar as necessidades e adotar programas, equipamentos e materiais específicos para as atividades de SIC. (BRASIL, 2019, p. 8-1).

Ao Centro de Tecnologia da Informação da Marinha (CTIM) destacam-se as seguintes atribuições:

> – Monitoramento da RECIM (Rede de Comunicações Integradas da Marinha);
> – Configuração de dispositivos de conectividade e de segurança de redes;
> – Varreduras de vulnerabilidades em servidores e redes;
> – Gerência dos recursos criptológicos em uso; e
> – Execução técnica das atividades de defesa cibernética. (BRASIL, 2019, p. 8-2).

E por último, de responsabilidade de cada Organização Militar, por meio do seu Comandante ou Diretor, auxiliados pelo Oficial de Segurança da Informação e Comunicação (OSIC) e pelo Administrador da Rede Local (ADMIN), as seguintes atribuições:

> – Manter o fiel cumprimento das normas, procedimentos e instruções pertinentes à SIC;
> – Zelar pelo fortalecimento da mentalidade de segurança;
> – Estabelecer e divulgar, por meio de Ordem Interna, a Instrução de Segurança da Informação e Comunicações (ISIC) – para a OM, bem como verificar sua implementação;
> – Identificar os recursos de informática que necessitam de proteção, de acordo com o respectivo grau de sigilo da informação por eles processada ou armazenada;
> – Garantir que todos estejam cientes das instruções em vigor para a segurança das informações digitais do ambiente computacional da OM;
> – Resguardar a integridade física dos equipamentos de conectividade, porventura instalados no âmbito de sua OM; e
> – Elaborar procedimentos para o acesso ao sistema computacional da OM; estabelecendo um rígido controle dos acessos aos serviços disponibilizados na rede local. (BRASIL, 2019, p. 8-3).

Ainda que foram selecionadas e apresentadas as atribuições de caráter mais prático, é possível observar seu inerente foco nos processos e sistemas administrativos, mesmo quando aplicadas às organizações do "Setor Operativo" como por exemplo os navios. A ausência de uma visão operativa da guerra cibernética, presente em outros setores do governo brasileiro e em outros países e marinhas, deve ser sanada o quanto antes, seguindo os moldes adotados pelos EUA e pela China que já reconheceram sua importância e estão na vanguarda de tais estudos.

5.2 – A Influência da Guerra Cibernética Sobre a Marinha

O espaço Cibernético e sua influência representam uma mudança de paradigmas na condução dos conflitos modernos, torna-se uma preocupação cuja importância é proporcional ao nível tecnológico dos países e forças envolvidas. Particularmente nas forças navais, como defendido por Thiele (2018), observa-se que cada vez mais sistemas embarcados dependem de dados e comunicações digitais. Praticamente todos os principais sistemas de navios, aeronaves e submarinos estão conectados em rede e frequentemente conectados à Internet. A dependência digital dos sistemas de controle mecânicos e elétricos, sistemas de armas e navegação, sistemas de aviação, de posicionamento e de navegação, incluindo toda a constelação de satélites GPS (*Global Positioning System*) constituem uma grande vulnerabilidade técnica e aumentam o risco de ataques maliciosos aos sistemas e redes de navios.

O comprometimento desses sistemas e a perda de dados afetam diretamente na correta e completa compilação das ações em curso e no poder decisório das autoridades envolvidas, ocasionando em um excesso de ações complementares que poderiam ser evitadas ou reduzidas e que não só reduzem a eficiência do emprego da força naval, mas também a expõe a riscos desnecessários.

Para reforçar a importância do estudo e desenvolvimento nacional do setor cibernético serão apresentados os recentes fatos vivenciados pelo governo norte-americano e sua Marinha. Na última década os EUA, na vanguarda da tecnologia militar, viu-se obrigado a fortalecer consideravelmente seus sistemas de segurança cibernética devida ao grande número de ataques que sofria diariamente, e que vinham se intensificando com o passar dos anos.

Conforme apresentado por Gouré (2019) pesquisador e especialista em defesa, no ano de 2018, hackers do governo chinês invadiram com sucesso a rede de uma grande

empresa prestadora de serviços da Marinha norte-americana, extraindo mais de 600 GB de dados sensíveis e secretos, incluindo informações sobre o programa de desenvolvimento de mísseis anti-navio supersônico. Nesse mesmo artigo é apresentado a atual preocupação dos EUA relacionada à possibilidade de ataques à sua infraestrutura, nos moldes dos ataques previamente apresentados, Stuxnet e Triton, e das possíveis consequências desastrosas.

Uma forma prática de analisar as vulnerabilidades de um sistema é apresentada por Thiele (2018), ele divide os objetos de um ataque cibernético a uma força militar em quatro camadas:

Camada Física – definida pelos Hardwares que compõe a infraestrutura do espaço cibernético de interesse;

Camada Lógica – constituída pelos sistemas e programas que utilizam espaço cibernético;

Camada de Informação – constituída pelos dados, conteúdos das comunicações que trafegam nas redes; e

Camada do Usuário – constituída pelas pessoas que possuem acesso direto ao espaço cibernético de interesse.

5.2.1 – As Vulnerabilidades Cibernéticas dos Sistemas Administrativos

Baseando-se nessas quatro camadas é possível elaborar uma analisa sobre os sistemas computacionais da Marinha do Brasil, abordando suas vulnerabilidades e os possíveis efeitos de um ataque cibernético.

A principal infraestrutura de comunicação interna da Marinha chamada RECIM baseia-se na utilização de fibra ótica do sistema nacional para comunicação terrestre à longa distância (entre Distritos Navais) e de redes metropolitanas seguras para a comunicação entre as organizações dentro da área de jurisdição de um Distrito Naval. Apesar de a comunicação via fibra ótica ser considerada bastante segura em relação à comunicação via satélite ou rádio, devido à dificuldade física que um agente externo à rede teria para interceptar as suas comunicações, o fato de que a Marinha e as outras Forças Armadas não possuem uma rede própria e segregada da rede nacional torna suas comunicações mais vulneráveis a ataques cibernéticos. Qualquer agente malicioso que possua acesso à parte aberta dessa rede poderia analisar seu trafego dos dados, interceptar seus pacotes de dados nos pontos de transição entre rede aberta e a rede segura e também praticar ataques do tipo Negação de Serviço aos pontos vulneráveis dessa rede.

Nas Normas de Tecnologia de Informação da Marinha (2019) no item 3.2.4 destaca-se o fato de que está normatizado a contratação de provedores e serviços de comunicação privados para realizarem as comunicações a grandes distâncias, ficando claro que o trâmite de informações à longa distância passa por serviços de empresas particulares das quais torna-se difícil assegurar a correta prática das políticas de Segurança da Informação e Comunicação, ficando assim enfraquecida a segurança da "Camada Física" dessas comunicações. Tal vulnerabilidade poderia ser corrigido ou mitigada pela implementação de uma rede isolada, de abrangência nacional, a fim de ser interligar os comandos militares em Brasília aos comandos regionais das três Forças, garantindo segurança e disponibilidade nas comunicações e mantendo a rede de fibra ótica nacional como uma redundância.

Ao fazer uma análise das redes internas das Organizações Militares é possível verificar diversas vulnerabilidades que poderiam ser facilmente corrigidas. As publicações internas previamente citadas explicam e determinam de forma clara o cumprimento de diversas orientações a serem adotadas e boas praticas a serem seguidas, porém vários fatores levam ao precário cumprimento de tais determinações. Dentre tais fatores destacam-se a falta de pessoal especializado na área de TI para assumir as funções de OSIC e ADMIN em todas as Organizações Militares, funções essas que por vezes são assumidas por militares que não estão completamente familiarizados às suas características. Outro fator relevante que propicia o surgimento de vulnerabilidades é o pouco conhecimento básico de medidas de SIC, parte integrante de um problema maior, a baixa Mentalidade de Segurança por parte dos usuários comuns das redes internas da Marinha. Anualmente boletins de notícias e artigos são divulgados ao pessoal interno à Marinha referente às boas práticas de segurança na tentativa incrementar tal mentalidade, porém o que se observa é um certo ceticismo quanto à importância e aplicabilidade de tais regras que são vistas geralmente como um empecilho ou um trabalho extra a ser realizado pelo usuário.

5.2.2 – A Vulnerabilidade dos Equipamentos e Componentes COTS

Outra fonte de vulnerabilidades ainda menos conhecida e que geralmente passa despercebida esta relacionada à tendência mundial de emprego, por parte das forças armadas e de segurança, de equipamentos e componentes produzidos para o comércio em geral, chamados COTS (*Comercial Off The Shelf*). As ideias que sustentam o emprego de elementos COTS são as de possibilitar a redução de custos, na construção e manutenção de equipamentos, e a de garantir alta disponibilidade de sobressalentes que por serem produzidos

e distribuídos em larga escala, podem ser adquiridos de diversos fornecedores. Tais vantagens realmente são atrativas e tendem a ser utilizadas cada vez mais nos meios operativos à medida que são modernizados e integrados por sistemas computacionais mais complexos, porém tais produtos podem tornar-se fontes de vulnerabilidades devido a dois fatores:

- Não terem sido feitos sob rígidas regras de segurança exigidas para o emprego militar ou de instalações críticas, podendo ter seus componentes alterados na fabricação ou distribuição a fim de se instalar um *kill-switch.*
  O *Kill-Switch* é definido como um componente malicioso, escondido entre os legítimos e que tem a capacidade de paralisar ou danificar todo o aparelho quando ativado, podendo ser acionado de forma remota, através de um comando ou quando alguma condição é satisfeita como data, hora ou algum dado específico de um sensor.
- Outro fator de vulnerabilidade é referente à utilização desses componentes em outros lugares, o que possibilita que agentes maliciosos que já tenham atacado outros usuários do mesmo componente, de forma que quanto mais empregado é um componente ao redor do globo maiores as chances de que suas vulnerabilidades já tenham sido descobertas, exploradas e divulgadas.

Tal fato fica evidenciado pelas recentes medidas tomadas pela Marinha dos EUA a qual enrijeceu os parâmetros de segurança estabelecidos pela DFARS (*Defense Federal Acquisition Regulation Supplement*) para a aquisição de diversos componentes provenientes da indústria da defesa e do comércio comum. Como demonstrado por Gouré (2019) a Marinha dos EUA passou a pedir de seus parceiros do setor militar que incrementem sua segurança cibernética. O próprio secretário-assistente da Marinha para Pesquisa, Desenvolvimento e Aquisição, James Geurts, publicou um memorando exigindo que os empreiteiros e fabricantes implementassem padrões avançados de segurança cibernética para suas redes, incluindo melhores controles de acesso e de monitoramento. Ambas determinações demonstram a preocupação da Marinha dos EUA não só pela segurança de suas instalações e meios, mas também de todos os agentes envolvido diretamente no desenvolvimento e fornecimento dos seus equipamentos.

5.3 – As Vulnerabilidades Cibernéticas dos Sistemas Operativos Embarcados

Direcionando o estudo aos meios operativos da Marinha do Brasil, notadamente aos navios, é possível observar o incremento no uso de complexos sistemas digitais, muitas vezes integrados em rede e que trazem consigo uma vasta gama de fatores que podem se tornar vulnerabilidades se explorados por um agente malicioso. Com o atual nível de

integração e computação dos sistemas pode-se dizer que todas as principais funções de um navio são gerenciadas e controladas por sistemas computacionais, e quanto maior a integração computacional dos sistemas maiores serão as vulnerabilidades associadas. Para facilitar o estudo dos efeitos de um ataque cibernético sobre os diversos sistemas componentes de um navio os mesmos serão divididos em três áreas abrangentes, Sistemas de propulsão, governo e geração de energia; sistemas de armas e sensores e sistemas de comunicação, comando e controle.

5.3.1 – Sistemas de Propulsão, Governo e Geração de Energia

Os sistemas de propulsão, governo geração de energia são é responsáveis por impulsionar o navio e fornecer energia para os demais componentes elétricos e eletrônicos do navio. A utilização de elementos computacionais integrada à automação desses sistemas permite um melhor gerenciamento dos componentes dos sistemas e a redução do pessoal, necessário para mantê-los em funcionamento, reduzindo também a exposição desse pessoal ao ambiente inóspito de uma praça de máquinas em pleno funcionamento. Os motores responsáveis pela propulsão do navio, chamados de MCP (motor de combustão principal) e os motores responsáveis por toda a geração de energia do navio, chamados de MCA(motor de combustão auxiliar) e seus respectivos geradores acoplados são monitorados por uma grande variedade de sensores responsáveis por medir diversos parâmetros, entre eles as pressões de admissão e descarga do combustível, da água para resfriamento, da descarga de gases, e do óleo lubrificante. Os sensores também verificam as diversas temperaturas envolvidas nos sistemas como a do óleo lubrificante, a dos cilindros dos motores e do líquido de arrefecimento, são também são responsáveis por medir a rotação dos motores e a energia produzida nos geradores.

Toda essa vasta gama de sensores se comunica com um sistema de gerenciamento que monitora o correto funcionamento do sistema e atua de forma independente, procedendo pequenas correções, a fim de manter o funcionamento dentro dos padrões ideais previamente estabelecidos. As alterações que ultrapassem seu parâmetro de automatismo fazem com que o sistema apresente um alarme sonoro e visual, indicando ao operador a alteração relevante em algum dos parâmetros medidos e a necessária intervenção humana. Todo esse sistema integrado é concebido devido à grande importância de se manter a propulsão e geração energia do navio funcionando ininterruptamente, as vezes por semanas, e demonstra que uma falha ou interrupção podem ser críticas à segurança do mesmo. Caso os sistemas de controle e

automação da propulsão e geração de energia sejam invadidos por um ataque cibernético poderiam ser levados a um funcionamento incorreto de seus sensores e atuadores, assim como o ocorrido no ataque Stuxnet em 2010 e na tentativa de ataque Triton em 2017.

A alteração de tais parâmetros poderia levar ao desligamento dos motores, prejudicando toda a operação do navio ou ainda pior, poderia levá-los a funcionar fora dos parâmetros de segurança, sem que as correções automáticas necessárias fossem feitas ou os alertas fossem indicados ao operador. Um ataque cibernético que alcance esses sistemas poderia ocasionar consequências catastróficas ao navio, pois ao permitir que os motores funcionem fora dos parâmetros de segurança aumenta-se consideravelmente a probabilidade da ocorrência de um acidente de grandes proporções dentro do navio o que poderia levar à grande perda de vidas e do navio em si. Um ataque que desligue um desses sistemas ocasiona também a perda de grande parte da capacidade de locomoção e de combate do navio, tornando-o completamente vulnerável à ataques cinéticos do inimigo.

5.3.2 – Sistemas de Armas e Sensores

Os sistemas de Armas e Sensores são os elementos principais que diferenciam um navio civil de um navio militar. A evolução dos navios militares ao longo do tempo é acompanhada diretamente pelo desenvolvimento de novas armas e sensores, e essa evolução ocorreu de forma acelerada principalmente nos últimos cem anos. Nesse período foram incorporados mísseis e torpedos que junto aos canhões constituem a base dos armamentos embarcados. Os sensores evoluíram de instrumentos óticos, utilizados para localizar os inimigos, para Radares, Sonares e sistemas de detecção eletromagnética (MAGE). O grande avanço nos referidos sistemas deveu-se à evolução do emprego dos circuitos eletrônicos e a automação de componentes, que deixaram de ser hidráulicos e manuais para eletromecânicos e automatizados. Apesar dos grandes avanços, assim como observado nos sistemas de propulsão, o avanço da eletrônica embarcada trouxe consigo o risco de que esses sistemas tornem-se alvos de ataques cibernéticos.

Em um navio de guerra esses sistemas podem ser agrupados em sistemas de detecção e acompanhamento de alvos, sistemas de combate e compilação do quadro tático, sistemas de lançamento e guiagem dos armamentos e os sistemas das próprias armas inteligentes (mísseis e torpedos). Esses sistemas geralmente encontram-se em uma rede própria e isolada de qualquer contado com a internet, porém ainda dependem de aferições e atualizações periódicas de seus *softwares.* As atualizações desses sistemas, feitas pelas OMs

especializadas da Marinha ou pelas empresas contratadas para a manutenção dos sistemas, podem ter sido infectadas previamente por um agente malicioso, podendo inserir instruções danosas em meio aos códigos legítimos do programa, essas instruções chamadas de Bombas Lógicas funcionam de forma similar a um *kill-switch,* porém atuam na parte lógica dos programas, desativando-os e destruindo-os ao receber um comando específico ou atingir as condições necessárias para seu ativamento.

Essa vulnerabilidade lógica que pode afetar todos os tipos de sistemas a bordo torna-se mais evidente nos sistemas de armas e comunicações devido ao seu alto grau de dependência de sistemas digitais, esse caso se torna claro quando leva-se em conta o sistema MAGE e o banco de dados Fênix pois possuem suas bibliotecas de dados táticos atualizadas a cada nova missão. A atual cultura de utilização de componentes eletrônicos comerciais (COTS) também pode se tornar uma vulnerabilidade no sistema pois os mesmos já trazem em si vulnerabilidades desde sua fabricação e que já podem ser de conhecimento do inimigo ou podem ter sido alterados por um agente malicioso que tenha instalado secretamente elementos *kill-switch*.

A infecção de vírus ou *Worms* nos sistemas de detecção e acompanhamento pode levar ao processamento incorreto dos sinais recebidos e a uma apresentação de dados não condizentes com a realidade, afetando diretamente a capacidade do sistema em acompanhar alvos e realizar a compilação do quadro tático. Caso essa compilação não seja confiável resultará em um atraso na correta análise por parte dos operadores, e nas ações a serem tomadas. Caso os sistemas de lançamento e guiagem dos armamentos sejam infectados a utilização dos armamentos pode ser consideravelmente degradada, a perda na automação do acompanhamento e da guiagem implicaria em uma queda acentuada na precisão e eficiência do emprego dos armamentos embarcados ou mesmo completa inutilização, tal fato restringiria o navio à utilização manual dos seus canhões e metralhadoras, reduzindo consideravelmente o seu poder combativo e de autodefesa.

Como exemplo da atuação cibernética sobre armamentos e sensores Clarke e Knake (2015) apresentam a ação da Força Aérea de Israel que em 06 de Setembro de 2007 atacou uma instalação síria em construção e cujos informes de inteligência indicavam que seria utilizada para a produção de armas nucleares. Os aviões israelenses invadiram o espaço aéreo sírio, efetuaram o ataque e saíram sem serem atacados ou mesmo detectados pelos avançados sistemas de defesa antiaérea adquiridos da Rússia. Estudos posteriores indicaram que a rede dos sistemas de defesa foi invadida e alterada, os dados e imagens apresentados pelos sensores não representavam a situação real, mas eram apenas gravações de dias

anteriores. Tal fato demonstra que treze anos atrás um ataque cibernético foi capaz de inutilizar toda a rede de defesa aérea de um país, claramente tais ataques continuaram evoluindo, daí a necessidade de que a defesa cibernética dos sistemas também esteja em constante evolução.

5.3.3 – Sistemas de Comunicação, Comando e Controle

O último aspecto a ser analisado é referente aos sistemas de comunicações embarcados e à capacidade de Comando e Controle de uma força naval. As comunicações sempre tiveram importante papel para operações militares nos mais diversos ambientes, são responsáveis pela correta orientação e posicionamento das unidades, sincronismo de ações, disseminação de ordens e da troca de informações entre as diversas partes envolvidas na operação. A capacidade de se comunicar é um fator essencial para qualquer Marinha ao redor do mundo e permite que se mantenham os elevados níveis de mobilidade e consciência situacional, fundamentais para o sucesso e eficiência de uma força naval.

Desde a antiguidade a mobilidade provou-se um fator fundamental para o sucesso de um combate naval, ainda que no século XXI o emprego de misseis e torpedos inteligentes tenha reduzida a função operacional da mobilidade naval essa ainda mantém sua importância tática e estratégica. O Comando e Controle de uma força naval abrange todo o aspecto da mobilidade e do emprego coordenado e eficiente dos recursos que cada unidade dispõe, no momento e local correto, contra ameaças específicas e empregando as armas mais adequadas para cada situação. O eficiente emprego das comunicações permite ao comandante o gerenciamento do complexo sistema que é uma força naval no mar, de forma que seu potencial de emprego vai além da soma das capacidades individuais de suas unidades. Como já visto anteriormente o que hoje entende-se como Guerra Centrada em Redes já vem sendo utilizado pelas marinha há muito tempo, caracterizado pela integração dos diversos sistemas embarcados a fim de disponibilizar uma melhor consciência situacional e compartilhá-la com as demais unidades, e claramente seu uso tende a se intensificar com a modernização dos sistemas embarcados.

A facilidade proporcionada pelo avanço da tecnologia digital trouxe consigo novas vulnerabilidades também aos sistemas de comunicação e controle embarcados. As primeiras formas de interferir diretamente nas comunicações vieram através da Guerra Eletrônica, utilizando o espectro eletromagnético a fim de interferir, confundir ou mesmo negar a comunicação ao adversário e obter dados e características da sua comunicação.

Atualmente ataques muito mais sutis estão à espreita dos sistemas de comunicação e podem afetá-los sem que seu operador tome conhecimento, são os ataques cibernéticos. Como quaisquer outros sistemas computacionais, que podem ser invadidos, *hackeados* e alterados de forma física e lógica, os sistemas de comunicação se tornaram mais vulneráveis a ataques cibernéticos com o aumento da sua dependência a elementos computacionais e digitais.

A implementação da tecnologia de Rádios Definidos por Software contribuiu para uma maior flexibilidade e melhor gerenciamento das diversas linhas e redes de comunicação que são utilizadas, simultaneamente, por um navio no mar. Sua utilização permite tornar um computador comum em um sistema completo de transmissão e recepção, na sua parte lógica e de controle dos elementos físicos envolvidos na transmissão e recepção, tal centralização de funções em um meio computacional possibilita que todo o sistema de comunicação de um navio possa ser desligado ou inutilizado por um ataque cibernético.

As comunicações poderiam ser exploradas de forma passiva na qual o inimigo utilizaria métodos como o *sniffing* ou *man-in-the-middle* para obter dados sigilosos e detalhes da operação e das unidades envolvidas. Ataques cibernéticos ativos também poderiam ser utilizados a fim de impedir que as unidades aliadas comuniquem-se entre si gerando um grande atraso na disseminação de ordens proveniente do comando e no cumprimento das mesmas devido à desconfiança quanto à sua validade, forçando a utilização de métodos menos eficientes, como a comunicação visual, na tentativa de mitigar os efeitos da negação de comunicação via rádio. O atraso também ocorreria no compartilhamento de informações indispensáveis para a correta compilação do quadro tático, esses dados ainda não possuem outra forma ágil e moderna de serem transmitidos durante um combate a não ser pelo seu *link* de dados, atualmente feito via rádio; consequentemente ocorreria uma perda considerável na capacidade da força naval em compilar seu quadro tático de forma integrada, dificultando o estabelecimento da consciência situacional necessária para a tomada de importantes decisões.

Como mencionado anteriormente, uma precária compilação do quadro tático afeta diretamente a rapidez das respostas às ameaças, que tendem a ser mal coordenadas e provavelmente ineficientes, colocando em risco a segurança das unidades e o objetivo da missão. Pode-se observar que a comunicação é fator preponderante para a manutenção de alto nível de coordenação das unidades de uma força naval, sua perda ou grande deterioração poderia causar inúmeros problemas à condução de uma missão chegando ao ponto de ser cancelada pela total falta de comunicação entre as unidades componentes.

6 – CONCLUSÃO

Este capítulo tem como finalidade apresentar as conclusões acerca das vulnerabilidades e consequências apresentadas, abrangendo também as ações iniciais que poderiam ser implementadas para mitigar tais problemas.

Como demonstrado ao longo desse trabalho o ambiente cibernético há muito deixou de ser um coadjuvante dos demais ambientes e ganhou uma importância autossuficiente. Desde pequenas brincadeiras e trotes a grandes acidentes industriais, o alcance dos efeitos de um ataque cibernéticos tende a crescer junto com a acelerada introdução de elementos computacionais nos mais variados aspectos da vida humana, de forma que todo ser humano pode ser alvo de um ataque cibernético e muitas vezes nem saberá que foi atacado. As ações cibernéticas, ao serem utilizadas como arma contra os sistemas de outros países, tornaram a guerra cibernética o objeto de estudos das maiores forças militares do mundo que já vêm utilizando tais métodos de maneira sutil, apenas alguns níveis abaixo do que causaria uma retaliação física.

A Guerra e o Terrorismo Cibernéticos vem sendo amplamente utilizados em diversos graus de complexidade, EUA, China, Rússia, Irã e Coreia do Norte são agentes continuamente ativos que mantêm ataques constantes uns contra os outros. Um exemplo recente deixa claro que as ações cibernéticas, apesar de ocultas, estão sempre presentes, Abdollah (2019) apresenta em seu artigo que em junho de 2019, após um drone de reconhecimento americano ser abatido por forças iranianas, os EUA lançaram um ataque cibernético contra os sistemas militares iranianos como forma de retaliação direta, mas sem vítimas.

Nos últimos vinte anos, as nações que encontram-se na vanguarda da tecnologia cibernética bem como grupos não governamentais expandiram suas áreas de atuação na tentativa de inserir suas bombas lógicas em pontos-chave da internet como uma forma de "preparar o terreno" para futuras guerras que porventura possam ocorrer, e que poderão ter seu resultado decidido antes mesmo que o primeiro disparo no mundo real seja efetuado. A ação cibernética de um país poderá degradar os sistemas do oponente a tal ponto que iniba a escalada do conflito para uma guerra cinética; esse futuro já está sendo construído.

O Brasil ainda tem muito o que evoluir nesse novo ambiente cibernético que traz consigo grandes oportunidades e desafios, os centros de tecnologia das forças armadas

necessitam reforçar sua integração com as pesquisas realizadas no meio acadêmico a fim de desenvolver novas técnicas de segurança de dados e de comunicação, bem como atualizar as já empregadas. Soluções híbridas em parceria com as universidades nacionais podem ser a melhor forma de incrementar a defesa das comunicações e dos dados no ambiente militar e também a segurança dos dados e das infraestruturas criticas no ambiente civil, proporcionando uma solução conjunta que promova o avanço da pesquisa, desenvolvimento e indústria tecnológica nacional, e também reduzindo a necessidade de utilização de componentes COTS importados, fontes de possíveis vulnerabilidades aos nossos sistemas.

Tão importante quanto mitigar a vulnerabilidades dos sistemas críticos, militares ou civis, e protegê-los de possíveis ataques é o quão resiliente esses sistemas são quando estão efetivamente sob ataque, como explicado por Tighe (2017) os sistemas devem ser capazes de segmentar e isolar as áreas com atividades suspeitas e prosseguir sua função até que seja restaurada a integridade e a capacidade daquela parte afetada do sistema. A descentralização de controles e segregação seletiva de partes das redes nacionais reforçariam grandemente a defesa cibernética nacional, proporcionando o tempo necessário para que as ações de contra-ataque sejam postas em prática e reduzindo e isolando o efeito de ataques.

Em vista do que foi apresentado e focando-se na Marinha do Brasil, conclui-se que a defesa e segurança cibernéticas das redes administrativas, ainda que possua grande importância e seja fator crucial ao correto funcionamento da Marinha no futuro, deve ser complementada por normas e atribuições atinentes ao uso operacional das ações cibernéticas, que podem e provavelmente serão utilizados como armas contra os meios operativos e operações em curso.

A ausência dessa abordagem operativa nas publicações internas pode ser atribuída, dentre outros fatores, à rápida mudança no cenário global, tanto na tecnologia quanto na forma de aplicá-la, e à dificuldade em desenvolver por conta própria estudos referentes a essa área, seja por falta de pessoal especializado, seja por reduções orçamentárias. Tais fatores dificultam o estabelecimento de um conhecimento avançado, concreto e atualizado sobre os impactos que uma guerra cibernética poderia causar sobre a força e consequentemente tais estudos tornam-se tarefas secundárias e a atualização das publicações e divulgação das mesmas ao publico interno acaba por ser postergada. A fim aprimorar a defesa e segurança cibernéticas da Marinha e baseando-se nas características e vulnerabilidades apresentados no capítulo anterior recorre-se novamente ao processo de análise em quatro camadas de Thiele (2018) de forma a chegar às seguintes conclusões:

Ataques cibernéticos à camada física, por atuarem principalmente na infraestrutura que mantém o espaço cibernético, têm maior probabilidade de afetar os sistemas de dados e de comunicação em terra que constituem entre outros elementos o banco de dados da Marinha e diversos sistemas de gerenciamento de recursos, equipamentos e pessoal. A Marinha necessita estabelecer políticas e sistemas de segurança cibernéticas mais rígidos para suas instalações críticas, responsáveis pelo funcionamento da força tanto no aspecto gerencial, como seus comandos operativos e Distritos Navais, quanto no aspecto logístico, aqui representado pelos centros de intendência regionais e depósitos centrais como o Depósito de combustíveis da Marinha, Base de abastecimento da Marinha no Rio de Janeiro, Centro de Munições da Marinha, Centro de Mísseis e Armas Submarinas.

A camada lógica, definida pelos sistemas e programas que utilizam o espaço cibernético, e a camada de informação, constituída pelos dados transportados e processados pelos sistemas, estão presentes em todos os ambientes da Marinha, desde os computadores das centrais de bancos de dados aos sistemas de comunicações digitais presentes nos navios. A fim de incrementar o nível de segurança dessas camadas é necessário que a Marinha concentre esforços em robustecer os elementos da sua Defesa em Profundidade.

A defesa em profundidade é constituída de diversas camadas de seguranças sequenciais e diferentes, de forma que o comprometimento de uma das camadas não afeta as demais e consequentemente o ativo a ser protegido continua seguro. Essa forma de defesa é constituída por programas *Firewall,* sistemas de triagem de dados, sistemas de detecção de intrusão, VPNs, entre outros métodos que juntos agem sobre os mais diversos tipos de ataques cibernéticos. Outro fator importante para a segurança e defesa cibernética dos sistemas é a segregação das redes de dados, empregando uma divisão entre redes abertas ao público, redes internas administrativas e redes de dados operativos. O emprego da segregação de redes permite que mesmo que uma rede seja atacada e tenha seus serviços ou dados comprometidos as demais redes não serão afetadas e manterão seu funcionamento normal e seus dados seguros. A segregação das redes deve ser utilizada tanto em sua parte lógica quanto na física, de forma que os computadores que acessam as redes internas não podem ter contato com as redes que se conectam à internet.

O uso da criptografia e da criptoanálise são fatores fundamentais para a segurança das comunicações há centenas de anos, porém desde que Allan Turing utilizou uma máquina de cálculos para decifra o código alemães produzido pela máquina “Enigma” na Segunda Guerra Mundial ficou claro que o advento da computação moderna, acompanhada por sua grande capacidade de calcular, tornaria os antigos métodos de criptografia obsoletos. Os

tempos modernos exigiram também a evolução da criptografia que passou a ser feita por potentes computadores de forma a incrementar exponencialmente sua capacidade, alcançando números inimagináveis para os cientistas e analistas de setenta anos atrás.

A utilização da criptografia, em suas diversas formas modernas como a RSA e a SHA (*secure hash algorythm*), constituem uma peça fundamental em grande parte dos sistemas de segurança cibernéticos. O uso da criptografia e dos componentes de segurança que a utilizam necessita ser intensificado na camada lógica, de informação e do usuário a fim de se garantir:

- Autenticação do acesso de usuários a sistemas e informações restritas;
- Integridade dos dados transmitidos e armazenados para que não sejam alterados indevidamente;
- Confidencialidade dos dados, para que mesmo que um invasor tenha acesso aos arquivos, não consiga obter nenhuma informação relevante em tempo hábil; e
- Disponibilidade dos dados e dos sistemas que o utilizam.

A implementação e o aprimoramento de uma defesa em camadas e do extenso uso da criptografia seriam as formas de se incrementar a segurança e a defesa cibernéticas dos sistemas embarcados nos meios navais, porém tais mudanças seriam pouco efetivas caso não ocorra, de forma conjunta, uma mudança na camada do usuário.

A camada do usuário é por vezes considerada como a maior vulnerabilidade dos sistemas em relação a ataques cibernéticos, tanto pela má utilização e desleixo com as atividades de segurança quanto pelos ataques realizados diretamente sobre os usuários dos sistemas, como o phishing e a engenharia social. A engenharia social é definida por Hadnagy (2011) como o ato de manipular uma pessoa para que tome uma ação que pode ou não ser do seu interesse, podendo assim induzir o alvo a executar determinadas ações que a fim de obter informação ou acesso restritos. A percepção limitada dos usuários quanto à relevância da SIC leva à repetição de erros básicos, dentre eles destacam-se a utilização de senhas fracas ou mesmo compartilhadas entre usuários, o controle de acesso deficiente, o comodismo de alguns usuários que relutam em aprender e empregar os novos sistemas homologados pela DCTIM e a conexão de periféricos não seguros (celulares, pendrives e HDs externos) em computadores com acesso à rede da Marinha. As práticas citadas geram vulnerabilidades aos sistemas pois facilitam tanto o acesso à rede interna por pessoas não autorizadas quanto a infecção do sistema por diversos tipos de Malwares.

Existem duas formas principais de mitigar a vulnerabilidade humana em sistemas. A primeira forma seria uma maior restrição tanto ao acesso aos compartimentos que possuem computadores ligados as redes internas da Marinha, quanto aos próprios computadores e seus sistemas, através de políticas de controle de acesso mais rígidas, mantendo sistemas de *login* e senha em todas as estações de trabalho e registros históricos de todos os acessos feitos em cada computador. Esse primeiro método é eficiente a curto prazo, porém caso não seja constantemente instruído e cobrado, com o passar do tempo tende a ser relaxado e esquecido pelos usuários, que voltam a cometer os mesmos erros e vícios.

A Segunda forma, consideravelmente mais difícil e lenta de implementar que a primeira, entrega um ótimo resultado a médio e longo prazos, é baseada no incremento da Mentalidade de Segurança dos militares e deve ser introduzida em todos os ciclos hierárquicos por meio de cursos, adestramentos e palestras sobre o tema. Militares bem adestrados e comprometidos com a segurança cibernética não só evitarão cometer erros como auxiliarão e fiscalizarão os demais para que também não os cometam. Somente quando todos compreenderem a importância da SIC para a Marinha e para o Brasil começarão a ter um comportamento condizente com a doutrina estabelecida. Essas duas formas apresentadas não são excludentes, podem e devem ser implementadas simultaneamente como parte de uma política de conscientização e incremente da SIC. Como último fator alinhado com a camada do usuário torna-se digna de nota a dificuldade em manter militares altamente capacitados no gerenciamento dos recursos cibernéticos das OMs em face à grande demanda desses profissionais pelo setor privado e dos vantajosos salários oferecidos.

Em face ao apresentado, esse trabalho chega ao fim com a expectativa de ter alcançado seu objetivo, tornando-se uma ferramenta que facilite o entendimento dos elementos básicos da guerra cibernética, suas possibilidades e consequências para a Marinha e seus meios. Sugere-se que sejam elaborados trabalhos futuros que abordem as novas técnicas que surgirão e os novos estudos acerca da complexidade e constante evolução da Defesa Cibernética.

REFERÊNCIAS

ABDOLLAH, Tami. **US struck Iranian military computers this week**. Disponível em: <https://apnews.com/f01492c3dbd14856bce41d776248921f>. Acesso em 04 dezembro de 2019.

AMORIM, Celso. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética.** Brasília, DF, 2014.

BRASIL. Estado-Maior da Armada. **Doutrina de tecnologia da informação da Marinha.** Brasília, DF, 2007.

_____. Ministério da Defesa. **Política Nacional de Defesa**. BRASÍLIA, DF, 2012.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa**. BRASÍLIA, DF, 2012.

_____. Ministério da Defesa. **Política Cibernética de Defesa**. BRASÍLIA, DF, 2012.

_____. Comando de Operações Terrestres. **Manual de Campanha de Guerra Cibernética do Exército.** BRASÍLIA, DF, 2012.

_____. Diretoria Geral do Material da Marinha. **DGMM-0540: Normas de Tecnologia da Informação da Marinha.** Rio de Janeiro-RJ, 2019

_____. **Escola Nacional de Defesa Cibernética é inaugurada em Brasília**. Disponível em: <https://www.defesa.gov.br/noticias/52690-escola-nacional-de-defesa-cibernetica-e-inaugurada-em-brasilia>. Acesso em 12 de setembro de 2019.

BRITANNICA. Apud WIENER, Norbert. **Cybernetics**. Disponível em: <https://www.britannica.com/science/cybernetics>. Acesso em 01 de dezembro de 2019.

_____. **Computer Network**. Disponível em: <https://www.britannica.com /technology/computer-network>. Acesso em 22 de dezembro de 2019.

CAMBRIDGE. **War**. Disponível em: <https://dictionary.cambridge.org /us/dictionary/english/war>. Acesso em 17 de outubro de 2019.

CERT.BR. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em < http://www.cert.br/stats/incidentes/ >. Acesso em 14 de novembro de 2019.

_____. **Incidentes Reportados ao CERT.br.** Disponível em <https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html>. Acesso em 14 de novembro de 2019.

CLARKE, R. A.; KNAKE, R. K. **Guerra Cibernética**: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro-RJ. Editora Brasport Livros e Multimídia LTDA, 2015.

CLAUSEWITZ, Carl Von**. Da Guerra:** Livro Um. Tradução Para o Inglês Michael Howard e Peter Paret. Tradução do inglês para o português Luiz Carlos Nascimento e Silva Valle, 2007.

DENNING, Dorothy E. **Stuxnet**: What Has Changed?**.** Disponível em: <https://www.researchgate.net/publication/272646277_Stuxnet_What_Has_Changed>. Acesso em 12 de novembro de 2019.

FRANCESCHI, Lorenzo E. **The History of Stuxnet**: The World's First True Cyberweapon. Disponível em: <https://www.vice.com/en_us/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee>. Acesso em 01 de novembro de 2019.

GOURÉ, Daniel . **Navy Must Work To Secure Its Platforms, Networks And Installations From Cyber Attack**. Disponível em: <https://www.realcleardefense.com/articles/2019/11/14/navy_must_work_to_secure_its_platforms_networks_and_installations_from_cyber_attack_114851.html>. Acesso em 22 de setembro de 2019.

GUEDES, Mauro.; SILVA, Sandro. ANACLETO, Wallace. **A Guerra cibernética no comando e controle**. Revista Militar de Ciência e Tecnologia VOL.33 Nº2 2016.

HADNAGY, Christopher. **Social Engineering**: The Art of Human Hacking. Crosspoint Boulevard Indianapolis, IN 46256. Wiley Publishing, Inc.10475, 2011. Disponível em: <https://www.academia.edu/8660875/Social_Engineering_The_Art_of_Human_Hacking>. Acesso em 27 de dezembro de 2019.

HARRIS, Mohd. **Computing Basics – Chapter 8 - Malware**. Disponível em: <https://ftms.edu.my/v2/wp-content/uploads/2019/02/csca0101_ch08.pdf>. Acesso em 13 de novembro de 2019.

HERZBERG, Ben.; BEKERMAN, Dima.; ZEIFMAN, Igal. **Breaking Down Mirai**: An IoT DDoS Botnet Analysis**.** Disponível em: <https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/>. Acesso em 11 de novembro de 2019.

INTERNET WORLD STATS. **Internet Growth Statistics**. Disponível em < https://www.internetworldstats.com/emarketing.htm >. Acesso em 03 de janeiro de 2020.

JACKSON, Kelly. **Schneider Electric**: TRITON/TRISIS Attack Used 0-Day Flaw in its Safety Controller System, and a RAT. Disponível em: <https://www.darkreading.com/ vulnerabilities---threats/schneider-electric-triton-trisis-attack-used-0-day-flaw-n-its-safety-controller-system-and-a-rat/d/d-id/1330845>. Acesso em 30 de outubro de 2019.

JOHNSON, Blake. et al. **Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure.** Disponível em: <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>. Acesso em 30 de setembro de 2019.

KASPERSKY. **Software Vulnerabilities**. Disponível em: <https://encyclopedia.kaspersky.com/knowledge/software-vulnerabilities/>. Acesso em 21 de dezembro de 2019.

_____. **What is a Trojan Virus**. Disponível em: <https://www.kaspersky.com/resource-center/threats/trojans>. Acesso em 22 de dezembro de 2019.

_____. **What's a Brute Force Attack**. Disponível em: <https://www.kaspersky.com/resource-center/definitions/brute-force-attack>. Acesso em 13 de novembro de 2019.

KUEHL, Daniel T. **From cyberspace to cyberpower**: Defining the problem. Cyberpower and national security, 2009. Disponível em < http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf>. Acesso em 14 de setembro de 2019.

LAMBERT, Tim. **A Brief History of Communication**. Disponível em < http://www.localhistories.org/communications.html>. Acesso em 21 de outubro de 2019.

LONG, Jill. **What Is War a New Point of View**. Disponível em: <https://smallwarsjournal.com/jrnl/art/what-is-war-a-new-point-of-view>. Acesso em 28 de outubro de 2019.

MALENKOVICH, Serge. **O que é um Ataque Man-in-the-Middle**. Disponível em: <https://www.kaspersky.com.br/blog/what-is-a-man-in-the-middle-attack/462/>. Acesso em 13 de novembro de 2019.

MAWAREBYTES. **Backdoor.** Disponível em: <https://www.malwarebytes.com/backdoor/>. Acesso em 13 de novembro de 2019.

NAVY. **Navy Information Warfare Then and Now: From the Civil War to Midway to 21st Century Great Power Competition**. Disponível em < https://navylive.dodlive.mil/2019/10/23/navy-information-warfare-then-and-now-from-the-civil-war-to-midway-to-21st-century-great-power-competition/>. Acesso em 03 de novembro de 2019.

NJCCIC. **Mirai.** Disponível em: <https://www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet>. Acesso em 27 de outubro de 2019.

NORTON. **What is a Computer Worm and How it Work?**. Disponível em: <https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html>. Acesso em 09 de novembro de 2019.

OLDFIELD, Paul. **Computer Viruses Demystifield**. Disponível em: **<**http://www.mssl.ucl.ac.uk/www_computing/buns/Viruses_demystified.pdf>. Acesso em 14 de novembro de 2019.

PANDA SECURITY. **Types Of Cybercrime**. Disponível em <https://www.pandasecurity.com /mediacenter/panda-security/types-of-cybercrime/>. Acesso em 21 de novembro de 2019.

SALDAN, Eliane. **Doutrina precisa definir guerra cibernética**. Disponível em: <http://www.conjur.com.br/2011-ago-06/guerra-cibernetica-urgentemente-definicao-doutrina>. Acesso em 7 de dezembro de 2019.

SCHNEIDER. **The history of Triconex.** Disponível em: **<**https://www.se.com/ww/en/brands/triconex/triconex-history.jsp>. Acesso em 17 de novembro de 2019.

SYMANTEC. **Dragonfly**: Cyberespionage Attacks Against Energy Suppliers. Disponível em: **<**https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf>. Acesso em 27 de novembro de 2019.

_____. **Dragonfly**: Western energy sector targeted by sophisticated attack group. Disponível em: **<**https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks>. Acesso em 27 de novembro de 2019.

TANENBAUM, Andrew. **Computer Networks**. Disponível em < http://www.teraits.com/pitagoras/marcio/gpi/b_ATanenbaum_RedesDeComputadores_4aEd.pdf#page=3&zoom=100,730,842>. Acesso em 04 novembro de 2019.

THIELE, Ralph D. **Game Changer** – Cyber Security in the Naval Domain. Disponível em: **<**http://www.ispsw.com/wp-content/uploads/2018/01/530_Thiele.pdf>. Acesso em 03 de novembro de 2019.

TIGHE, Jan. **Cyber Warfare in the Maritime Domain**. Disponível em: <https://www.csis.org/analysis/cyber-warfare-maritime-domain>. Acesso em 02 de outubro de 2019.