ESCOLA DE GUERRA NAVAL

CC (AA) José Carlos de Sá

ESTRATÉGIA DE EMPREGO DA GUERRA CIBERNÉTICA EM OPERAÇÕES CONJUNTAS E NA DEFESA DE ESTRUTURAS CRÍTICAS

Rio de Janeiro

2022

CC (AA) José Carlos de Sá

ESTRATÉGIA DE EMPREGO DA GUERRA CIBERNÉTICA EM OPERAÇÕES CONJUNTAS E NA DEFESA DE ESTRUTURAS CRÍTICAS

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador: CF (FN) Salvador Mota Junior

Rio de Janeiro

Escola de Guerra Naval

2022

AGRADECIMENTOS

A Deus, que com sua imensa sabedoria, permitiu-me enfrentar as adversidades e aprender com elas.

Aos meus pais (*In Memoriam*) que pela força do exemplo e dedicação, conduziram-me até aqui, muito mais longe do que eu imaginava.

A minha amada esposa por todo o suporte para vencermos mais esse desafio e ao meu jovem filho, Jean, que sempre foi o motivo para sempre seguirmos lutando.

Aos meus irmãos, familiares e amigos pelo carinho, consideração e apoio que me ofertaram, compreendendo a minha ausência nesse ano especial.

A meu Orientador CF (FN) Salvador Mota Junior por compartilhar seus conhecimentos, pela paciência e profissionalismo com que me conduziu neste trabalho.

A toda a equipe a Escola de Guerra Naval pela dedicação e profissionalismo e comprometimento com seus alunos.

Aos meus Chefes e colegas de trabalho pelo apoio e compreensão sem os quais esta missão seria muito mais difícil.

RESUMO

Com os avanços tecnológicos implementados em todas as frentes, a internet tornou-se um campo de batalha sem fronteiras, de modo que todas as nações têm realizado ações para a proteção de dados e informações de suma importância que venham a afetar o funcionamento de infraestruturas críticas. A Guerra Cibernética caracteriza-se como atividades para obter informações e dados importantes sobre outra nação, bem como proteger seus próprios ativos. Nesse contexto, destaca-se a atuação da Marinha do Brasil (MB) que abrange a proteção de diversos ativos *in e offshore*, os quais podem influenciar no bom funcionamento do país. O presente estudo visa analisar a atuação da MB considerando os aspectos de interdependência como requisito para identificação de infraestruturas críticas no âmbito cibernético por meio de uma análise das principais normas e artigos, destacando-se a publicação EMA-419, que trata sobre a doutrina cibernética da Marinha. Verifica-se que a identificação das Infraestruturas Críticas mostra-se de suma importância para uma proteção eficiente e eficaz dos ativos navais. O reconhecimento dessas estruturas promove um constante aprimoramento do sistema de C^2 e melhoria da proteção cibernética. Depreende-se que o país encontra-se no caminho certo na análise de novos conhecimentos e aquisição de talentos para o setor cibernético e a adoção de medidas protetivas no âmbito digital amplia a conscientização sobre a importância desta temática e da relação custo-benefício favorável na cooperação para a Segurança e Defesa Cibernética.

Palavras-chave: Defesa Cibernética, Guerra Cibernética, Interdependência, Infraestruturas Críticas.

LISTA DE ABREVIATURAS E SIGLAS

AGCiber	Ações de Guerra Cibernética
AtqCiber	Ataque Cibernético
C^2	Comando e Controle
CERT.BR no Brasil	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CIM	Centro de Inteligência da Marinha
ComOpNav	Comando de Operações Navais
CoNavOpEsp	Comando Naval de Operações Especiais
CTIM	Centro de Tecnologia da Informação da Marinha
DC	Defesa Cibernética
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DGMM	Diretoria-Geral de Material da Marinha
DIIM	Modelos de Entrada e Saída de Inoperabilidade Dinâmica
DMDC	Doutrina Militar de Defesa Cibernética
DMN	Doutrina Militar Naval
ECiber	Espaço Cibernético
ECiber-MB	Espaço Cibernético de interesse da Marinha
END	Estratégia Nacional de Defesa
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
ExpCiber	Exploração Cibernética
FA	Forças Armadas
GptOpGCiber	Grupamento Operativo de Guerra Cibernética
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IEC	Infraestruturas Críticas
MB	Marinha do Brasil
MD	Ministério da Defesa
IIM	Modelo de Entrada-Saída de Inoperabilidade
NATO CCD COE *of Excellence*	*North Atlantic Treaty Organization Cooperative Cyber Defence Centre*

NuCDCiber	Núcleo do Comando de Defesa Cibernética
OMOT	Organização Militar Orientadora Técnica
PtçCiber	Proteção Cibernética
P&D	Pesquisa e Desenvolvimento
RECIM	Rede de Comunicações Integrada da Marinha
SegCiber	Segurança Cibernética
SCF	Sistemas Ciberfísicos
SIC	Segurança de Informação e Comunicação
SIEC	Sistemas de Infraestrutura Crítica
SisNavGCiber	Sistema Naval de Guerra Cibernética
TI	Tecnologia da Informação
USCyberComm	United State Cyber Command

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica da guerra sempre foi o fator decisivo nas conquistas e no predomínio das nações. Foi assim ao longo de toda a história, desde a invenção da pólvora até o uso de drones em combate pelas forças ucranianas na recente invasão russa naquele país. Porém, não foi só o setor bélico que evoluiu, toda a sociedade beneficiou-se com essas inovações, experimentando um crescimento e dependência sem precedentes nos últimos tempos, principalmente na área computacional.

A possibilidade de ameaças a ativos de grande importância para os Estados, transformou-se em alvos de interesse e objetivos de Operações Militares. Citam-se ataques cibernéticos dos israelenses, que desabilitaram a rede de defesa aérea síria, permitindo o bombardeio de uma instalação suspeita de ser nuclear.

Nesse prisma, os ataques cibernéticos passaram a ser uma preocupação para os governos e sociedades de todos os países. Na década de 1990, com o crescimento dos sistemas de rede de computadores e a utilização de tecnologia em combates, o Pentágono já avaliava o problema de vulnerabilidades nos sistemas de informação, que evoluía com muito mais velocidade que a tecnologia de segurança de informação.

No Brasil, os primeiros movimentos no sentido de implantação da Defesa Cibernética ocorreram no ano de 2008, quando foi aprovada a primeira versão da Estratégia Nacional de Defesa (END), que abrangia o assunto. A defesa do ciberespaço e a necessidade de segurança dos dados no ambiente digital para o desenvolvimento mostram-se como assuntos de interesse nacional e de grande importância e complexidade no contexto contemporâneo, pois abrange a elaboração e aplicação de estratégias operacionais, administrativas, tecnológicas, entre outras.

Nesse contexto, o objetivo deste trabalho é analisar os aspectos de interdependência como requisito para identificação de infraestruturas críticas no âmbito cibernético. Como objetivos específicos apresentam-se: analisar o conceito de Infraestrutura Crítica (IEC) quanto ao aspecto de interdependência no contexto cibernético; explorar quais são consideradas as Infraestruturas Críticas para a Marinha do Brasil, Instalações, sistemas ou usuários; identificar quais são as Ações de Guerra Cibernética que a Marinha utiliza para salvaguardar as IEC de interesse, explorando os procedimentos a serem executados por

ocasião da elevação do alarme cibernético e por fim, apontar os aspectos positivos e as oportunidades para que a proteção seja eficiente e eficaz.

Para tanto, apresentam-se como questões norteadoras as seguintes: no contexto cibernético, como utiliza-se o conceito de interdependência para a identificação de uma infraestrutura crítica? Como a Marinha define suas estruturas críticas? Quais as ações de guerra cibernética que a Marinha realiza para salvaguardar seus ativos de interesse e quais os principais desafios para alcançar os objetivos?

Visando prover um arcabouço teórico que fundamente os argumentos apresentados neste estudo, recorreu-se aos marcos normativos que alicerçam o assunto, como a Política Cibernética de Defesa, que estabelece as orientações, no âmbito das Forças Armadas, para atividades de Defesa Cibernética (BRASIL, 2012) e a Doutrina Militar de Defesa Cibernética, que "introduz a unidade de pensamento sobre o assunto no âmbito do Ministério da Defesa, visando contribuir para a atuação conjunta das Forças Armadas na defesa do espaço cibernético, atendendo assim política vigente" (BRASIL, 2014) e, mais especificamente, a Doutrina Cibernética da Marinha, que "estabelece nos níveis estratégico, operacional e tático, as ações de Guerra Cibernética no âmbito da Força" (BRASIL, 2021).

A metodologia, neste trabalho, baseia-se na abordagem descritiva qualitativa utilizando-se a pesquisa bibliográfica e documental por meio das palavras-chave: Defesa Cibernética, Guerra Cibernética, Interdependência, Infraestruturas Críticas, Grandes Eventos, priorizando o período entre 2008 e 2021.

Foram consultadas as bases de dados disponíveis como Rede BIM, EBSCO, RI-MB, sites do Exército Brasileiro e do Ministério da Defesa e Gov.br, além de busca em Teses e Dissertações acerca dos assuntos em pauta. Destaca-se que a revisão bibliográfica e documental promove um melhor suporte teórico e reforçam o entendimento, pautando-se nos acontecimentos recentes, permitindo assim, ampliar o alcance da importância do tema.

Outras doutrinas que tratam de Operações Conjuntas e Análise de Riscos, por exemplo, poderiam ser abordadas neste estudo, porém, em virtude da limitação imposta a este trabalho, estará focado nas Doutrinas específicas da área no contexto militar.

A relevância desse assunto fica evidenciada pela extensão das Ameaças Cibernéticas, que podem variar desde vazamentos de informações sensíveis, até o comprometimento de infraestruturas críticas como comunicações, energia, transportes,

finanças e fornecimento de água, podendo assim comprometer seriamente toda uma sociedade.

A estrutura desta pesquisa constitui-se de quatro capítulos. Após a introdução, o capítulo dois introduziu o referencial teórico, com os pontos principais sobre a guerra cibernética, abrangendo o conceito de interdependência como instrumento para a análise das infraestruturas críticas no contexto cibernético. No capítulo três buscou-se abordar como a MB trata suas Infraestruturas Críticas, analisando a defesa cibernética e a segurança de seus ativos da informação como Infraestruturas Críticas.

Já o capítulo quatro tratou das ações implementadas, no âmbito da Força Naval, para a salvaguarda dos ativos de interesse, explorando os alarmes cibernéticos. Ao término, foram elaboradas as conclusões, observando se o objetivo do estudo foi atingido.

Assim, o alvo desse estudo está focado na análise da interdependência como requisito para avaliar a importância de uma Infraestrutura Crítica, explorar as ações de Guerra Cibernética no escopo na MB, tomando por base as primeiras experiências de relevância no país, quanto à defesa das infraestruturas críticas nacionais: os Grandes Eventos realizados no Brasil entre 2012 e 2016, mais especificamente, a Copa do Mundo Fifa 2014. Além disso, explorar as ações de guerra cibernética implementadas na MB.

2 INFRAESTRUTURAS CRÍTICAS E INTERDEPENDÊNCIA NO CONTEXTO CIBERNÉTICO

De acordo com Silva (2016), a Guerra Cibernética pode ser considerada como uma das cinco áreas de Domínio Operacional, além dos domínios Terrestre, Marítimo, Aéreo e Espacial. Diversas infraestruturas importantes como aeroportos, usinas de energia, centros de comunicações podem ser alvo de ações cibernéticas, principalmente se tiverem com alta dependência tecnológica e, desse modo, prejudicar seriamente o funcionamento harmônico de um país, colocando em risco o bem-estar da população e até sua economia.

De acordo com Teixeira Júnior (2017) os primeiros ataques cibernéticos a infraestruturas críticas se deram contra o sistema de informações dos Estados Unidos. A operação denominada *Titan Rain* consistiu em invasões nos sistemas de e-mail do secretário de Defesa dos Estados Unidos, redes do Pentágono, empresas de gás e petróleo, no Google e outros sistemas do Departamento do governo americano. Outro caso histórico ocorreu em 2007, na Estônia, um dos países mais conectados do mundo, o que permitiu que hackers

entrassem no site do parlamento do governo daquele país e depois o site do Ministério da Defesa, também mencionado por Vianna (2020).

Segundo o mesmo autor, o ataque teve impacto global e deu início à criação do *North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence* (NATO CCD COE), Centro de Excelência e Cooperação de Defesa Cibernética da Organização do Tratado do Atlântico Norte, com a finalidade de apoiar as nações-membros com competências cibernéticas nas áreas de tecnologia, estratégia, operações e legislação. O caso mais conhecido é o ataque de 11 de setembro contra as Torres Gêmeas nos Estados Unidos.

Diversos países empreenderam ações em prol da defesa cibernética com a entrada em vigor da Convenção de Budapeste, em 2004, envolvendo um tratado internacional sobre crimes perpetrados pela internet; publicação de estratégias nacionais de segurança cibernética de diversos países da Europa e; a criação, em 2009, do *U.S. Cyber Command (USCyberComm*), órgão subordinado ao Comando Estratégico norte-americano, responsável pela coordenação das ações de prevenção e defesa cibernéticas. Tais fatos impulsionaram ações de defesa cibernética também no Brasil (VIANNA, 2020).

A Defesa Cibernética (DC) abrange as atividades realizadas no ciberespaço, dentro de um planejamento nacional estratégico, coordenado e integrado pelo Ministério da Defesa (MD), com a função de proteger as informações de interesse de defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente, corroborando os preceitos da Doutrina Militar de Defesa Cibernética (DMDC) (BRASIL, 2014).

Nesse contexto, o ciberespaço ou espaço cibernético, na concepção de Singer e Friedman (2014) caracteriza-se como o ambiente das redes de computadores e seus usuários em que as informações são armazenadas e compartilhadas *online*.

A Doutrina Militar de Defesa Cibernética (DMDC) define a guerra cibernética como a utilização ofensiva e defensiva de dados e sistemas de informação para afetar as capacidades de Comando e Controle (C^2) do inimigo dentro de um planejamento militar de nível operacional, tático ou de uma operação militar (BRASIL, 2014)

Clarke (2015), conceitua a guerra cibernética como as ações de um Estado para penetrar na rede de computadores de outra nação com o intuito de causar prejuízos ou interrupções.

A DC engloba importantes estruturas que compõem um Estado, as quais são denominadas como Infraestruturas Críticas (IEC), as quais se caracterizam como instalações ou serviços, bens ou sistemas que permitem um setor cumprir sua função e, se destruídos ou desabilitados, trarão sérios impactos sociais, políticos e econômicos à sociedade e à segurança do país (BRASIL, 2019a). As IEC possuem um cunho estratégico devido ao papel essencial que desempenham na segurança e na soberania nacional em prol do desenvolvimento do país.

O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) elenca cinco áreas prioritárias das infraestruturas críticas, sem prejuízo de outras que vierem a ser definidas, quais sejam: transporte, água, energia, telecomunicações e finanças. Os impactos causados nos serviços prestados pela IEC de um país devem ser reduzidos aos níveis aceitáveis para o sucesso da Sistemas de Infraestrutura Crítica (SIEC) (BRASIL, 2019a).

A evolução tecnológica permitiu que as IEC estivessem cada vez mais automatizadas e integradas, o que pode afetar ainda mais o bom andamento do Estado ou mesmo a segurança cibernética, isto é, as ações voltadas para a segurança de operações, visando garantir que os sistemas de informação possam resistir a situações fora do comum no ciberespaço que possam comprometer a funcionalidade, a integridade, a confidencialidade e a autenticidade dos dados ali armazenados, processados ou transmitidos e dos serviços ofertados por esses sistemas (BRASIL, 2019a).

A integração entre os sistemas cibernéticos requer que os mecanismos de controle empregados estejam em constante atualização, podendo apresentar novas vulnerabilidades, fator que exige avaliação contínua. No âmbito da MB tal fato tem relação direta com seus equipamentos e mecanismos de controle. A conectividade entre esses sistemas abre espaço para violações onde as avaliações de risco de segurança da informação complementam o gerenciamento de risco no mundo físico, (DI BENEDITTO, 2016).

Mostra-se fundamental uma integração do nível informacional até o nível organizacional para constituir uma política de segurança que preveja e gerencie todos os riscos e vulnerabilidades relacionados às IEC, visto que a segurança dessas estruturas se constitui no reforço da resiliência dos setores estratégicos, vitais para o funcionamento do Estado, com o intuito de prevenir incidentes e garantir o fornecimento contínuo dos serviços prestados pelas IEC (SANTOS, 2021).

De acordo com Huang, Liou e Chuang (2014a) a criação de uma definição de IEC permite, com base nos critérios e impactos presentes no conceito de IEC, identificar e estruturar um conjunto de setores estratégicos ao funcionamento do país. Assim, o principal objetivo de uma nação consiste na garantia do bem-estar da população, estando este dependente de quatro setores: Segurança, Governança, Economia, Valores Simbólicos.

Em seguida, mede-se o grau de criticidade das infraestruturas, com o recurso de probabilidades condicionadas, visando obter os índices de interdependências entre setores/infraestruturas. Essa metodologia abrange o conceito de criticidade como um conjunto de variáveis (risco, vulnerabilidade, consequência), aspectos abstratos para calcular com exatidão. Nesse contexto, conclui-se que uma infraestrutura pode ser mais crítica que outra. O passo seguinte consiste na elaboração de uma Matriz de Dependências no sentido de identificar e quantificar, através das probabilidades supracitadas, as dependências existentes entre os Setores Dependentes (linhas) e os Setores de Segurança, Governança, Economia, Valores Simbólicos.

A etapa seguinte consiste no cálculo das probabilidades condicionadas entre setores através da aplicação do algoritmo para obter as probabilidades dos setores se afetarem mutuamente. Esse processo permite avaliar os efeitos de interdependências entre setores e Infraestruturas, bem como identificar e quantificar aqueles que podem ser mais impactadas em relação a outras infraestruturas do mesmo setor ou de outros setores, e ainda aquelas que podem ser mais afetadas pela disfunção de outras. Por fim, com a obtenção de uma Matriz de Incidências que indica os rankings relativos aos setores, infraestruturas ou outros elementos, pode-se proceder à classificação das estruturas como “críticas” pelo nível de impacto (HUANG, LIOU E CHUANG, 2014).

Nesse sentido, a interdependência entre as IEC é abordada por Sun, Bocchini e Davison (2021), como uma forma de facilitar a coordenação geral dos serviços. Assim, em caso de ataques cibernéticos, todos os atores responsáveis devem atuar de forma integrada para solucionar a questão.

A Doutrina para o Sistema Militar de Comando e Controle (MD31-M-03) requer que as Forças Armadas (FA) atuem de forma conjunta, de modo que a interoperabilidade organizacional necessita da instauração de sistemas de C^2 eficientes e bem dimensionados, baseados em redes de comunicações para a troca de informações entre todas as forças empregadas nas operações (BRASIL, 2015).

Por outro lado, essa interdependência pode atuar como um multiplicador sob ameaça, causando falhas em cascata e dificultando a resiliência. Desde modo, otimizar a recuperação de Sistemas de Infraestrutura Crítica (SIEC) mostra-se como o principal objetivo para o planejamento e gerenciamento de ataques, considerando a guerra cibernética SUN, BOCCHINI e DAVISON (2021).

Os autores esclarecem que os componentes de infraestrutura representam cada estrutura individual ou entidade física que constitui um sistema de infraestrutura, enquanto os elementos menores, dentro das estruturas, são denominados subcomponentes. As dependências são relações unidirecionais. Um componente influencia a funcionalidade ou recuperação de outro, através de uma determinada conexão, mas o segundo componente não afeta necessariamente o primeiro da mesma forma. As interdependências são bidirecionais entre duas infraestruturas/componentes, cuja funcionalidade ou restauração se afetam.

Para identificar interdependências, faz-se necessário verificar as relações entre componentes e subcomponentes, visto que podem surgir através de uma cadeia de dependências. Há diversas classificações e modelos que podem estabelecer o nível de interdependência. Classificam-se as dependências em duas categorias: intra e intersistema. O primeiro abrange dois componentes do mesmo sistema, em que os recursos de recuperação são compartilhados entre vários componentes, conforme Sun, Bocchini e Davison (2021).

Na visão dos autores, a dependência entre sistemas são relacionamentos entre componentes de diferentes sistemas de infraestrutura, através dos quais o estado de um impacta e/ou se correlaciona com outro. O ambiente cibernético e o meio físico possuem vulnerabilidades que devem abarcar as duas esferas, dentro de suas singularidades, em que o processo de segurança deve considerar os aspectos relacionados aos sistemas digitais, processos físicos e interseção entre eles.

As dependências podem causar interrupções dentro ou entre infraestruturas em forma da cascata ou em falhas crescentes. As primeiras ocorrem em um sistema onde a falha de um componente se propaga para outros componentes na forma de danos e/ou interrupções de funcionalidade. As falhas em escala remetem ao fato de que uma interrupção/falha existente em um sistema de infraestrutura piora uma interrupção/falha independente em outro sistema de infraestrutura, normalmente aumentando a gravidade

da interrupção ou atrasando a restauração da segunda interrupção/falha (SUN, BOCCHINI E DAVISON, 2021).

Segundo os mesmos autores, há diversas categorizações de interdependências sendo as principais: física, cibernética, geográfica e lógica. A dependência cibernética entre dois sistemas de infraestrutura modela o fato de que o estado de funcionalidade de uma infraestrutura depende informações que transitam pela infraestrutura de comunicação, como sistemas de controle computadorizados.

A caracterização de modelos práticos de interdependências complexas pode envolver uma gama de interações e dados. Dentre os modelos qualitativos está a tabela de dependência, a qual considera a combinação de dois sistemas ou componentes reunindo termos descritivos. Esses dados resultam em uma compreensão preliminar de interações entre diversas infraestruturas com maior facilidade. Em seguida, deve-se quantificar as relações de dependência e interdependência substituindo termos descritivos por números, o que resulta em uma matriz de dependência com coeficientes que podem ser determinados através de estatísticas de dados ou modelos de simulação (SUN, BOCCHINI E DAVISON, 2021).

Os termos descritivos representam o quão forte é a interação entre duas infraestruturas em condições normais de serviço, mas podem representar outros aspectos como na fase de dano e na fase de restauração. Contudo, esses termos não fornecem uma análise quantitativa das interações de infraestrutura por não serem bem dimensionados.

As tabelas quantitativas descrevem a existência, a força e o nível de impacto de uma interação entre dois componentes/sistemas em um cenário de dano. As dependências e interdependências são representadas como coeficientes numéricos, que podem ser computados de diferentes maneiras. Com base nessa metodologia descrita por Sun, Bocchini e Davison (2021), a interdependência se enquadra nas seguintes subclasses: tabelas quantitativas baseadas em pesquisas, tabelas baseadas em correlação, matrizes de adjacência baseadas em teoria gráfica e tabelas de peso, tabelas baseadas em probabilidade condicional, bem como tabelas baseadas em teoria econômica.

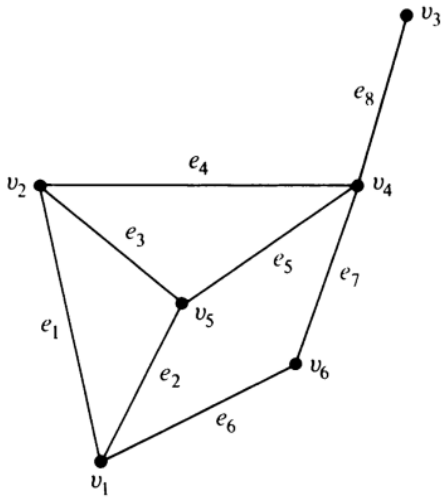
Tabelas quantitativas baseadas em pesquisas são preenchidas com coeficientes determinados através de pesquisas após um evento extremo, considerando o número total de consequências de falhas em cascata, a quantidade de tarefas de restauração para cada sistema de infraestrutura ou a importância das interdependências para um sistema

individual. Essa análise pode facilmente identificar as relações interdependentes mais críticas. Por outro lado, os dados são provenientes de um evento específico, o que pode dificultar a aplicação da tabela de dependência (figura 1) para outro tipo de evento ou nível de intensidade.

Fixed effects	Model 4 coefficient (standard error)	Model 5 coefficient (standard error)	Model 6 coefficient (standard error)
Power restoration	0.125***	0.116***	0.075***
	(0.023)	(0.023)	(0.023)
Constant (intercept)	0.956***	0.944***	0.826**
	(0.024)	(0.024)	(0.019)
Random-effect[b] parameters			
var (more than 3 days without electricity)	0.161***	0.019*	0.030*
	(0.017)	(0.013)	(0.023)
var (intercept)	0.131***	0.098***	0.023***
	(0.041)	(0.013)	(0.002)
var (residuals)	0.133***	0.102**	0.108**
	(0.045)	(0.005)	(0.005)
Model parameters			
Wald chi-square	29.710	25.250	10.840
Log-likelihood	−260.302	−269.093	−286.952
Prob > chi-square	0.000	0.000	0.000

Figura 1: Exemplo de tabela quantitativa baseada em pesquisas
Fonte: Mitsova et. al. (2020, p. 9)

As matrizes baseadas em teoria de grafos referem-se a infraestruturas fisicamente interconectadas como redes, representando a conectividade topológica de rede como uma maneira de modelar interdependências. A matriz de adjacência consiste em coeficientes binários para representações de conexão. Os coeficientes são 1 se houver uma ligação entre dois componentes (os chamados “nós” ou “vértices” do grafo), ou 0 caso contrário. A matriz de adjacência, figura 2, consiste em coeficientes binários para representar as conexões. Coeficientes binários na matriz de adjacência fornecem informações somente sobre a existência de ligação. Na teoria dos grafos, os pesos são normalmente adicionados para representar várias propriedades dos links, como a capacidade de fluxo ou o comprimento do enlace, formando uma rede ponderada (SUN, BOCCHINI E DAVISON, 2021).



$$X = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{array} \begin{array}{c} \begin{array}{cccccc} v_1 & v_2 & v_3 & v_4 & v_5 & v_6 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Figura 2: Exemplo de matriz de adjacência
Fonte: Oliveira e Rangel (2013)

Quando usados para análise de resiliência, os nós de rede representam componentes críticos e os links representam conexões físicas; a matriz de adjacência ou a matriz de peso representam links e suas características como capacidade de fluxo e comprimento.

Estudos de interdependência usando modelos de rede foram implementados principalmente para avaliar o impacto das dependências da funcionalidade de composição na vulnerabilidade, confiabilidade e resiliência da rede. A funcionalidade do sistema geralmente é definida com base na topologia da rede e/ou fluxo de rede, em termos de perda de conectividade, número de componentes funcionais ou com falha ou reparados, caminho mais curto recíproco, fluxo de capacidade, ou número de clientes com ou sem serviço (SUN, BOCCHINI E DAVISON, 2021).

Além disso, o fluxo de rede pode ser usado como a métrica de funcionalidade para avaliar o impacto das interdependências na funcionalidade da rede, considerando a capacidade. O impacto das dependências de funcionalidade de composição em uma rede pode ser avaliado simplesmente comparando a funcionalidade do sistema e a resiliência de diferentes casos. Ao expandir os modelos de rede, figura 3, para sistemas interdependentes, o conceito de link pode ser generalizado para descrever diferentes tipos de relacionamentos e dependências, não necessariamente enraizados em conectividade de fluxo físico e geralmente existente entre redes.

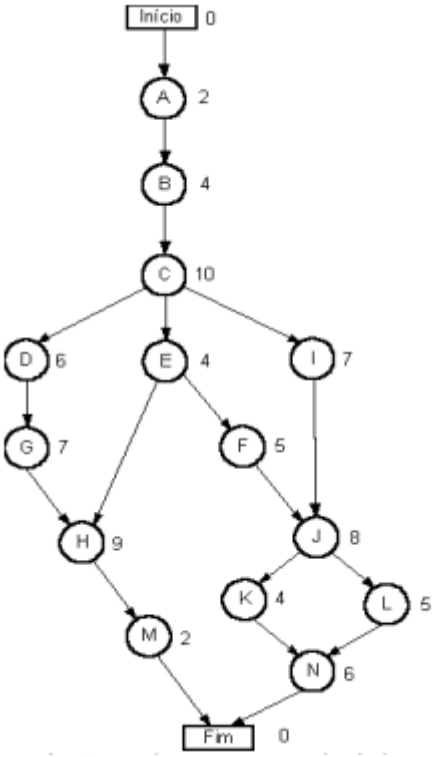


Figura 3: Exemplo de modelo de rede
Fonte: Nogueira (2020, p. 2)

A dependência de um componente em uma infraestrutura em outro componente em uma infraestrutura diferente ao modelar falhas em cascata pode ser descrita por uma probabilidade, a qual pode ser determinada como a probabilidade de falha de um componente em um evento intenso a partir de análises de fragilidade interdependentes ou a probabilidade de falha supracitada. Cada coeficiente na matriz conjunta de probabilidade é a probabilidade de falha em cascata (condicional) de um componente devido à falha de outro componente, dada a intensidade do evento, ou dada a falha do segundo componente (SUN, BOCCHINI E DAVISON, 2021).

Ao aplicar as matrizes baseadas em teoria dos grafos, os modelos de rede podem simular a propagação de dados de componentes iniciais dentro de um sistema e entre sistemas, bem como simular a evolução da recuperação de sistemas interdependentes devido a restaurações progressivas. Como interdependências de rede podem resultar em uma transição de fase de ‘filtragem’, aprimorando nós críticos que têm fortes interdependências com outros sistemas, o que contribui para uma maior robustez dos sistemas de rede interdependentes (SUN, BOCCHINI E DAVISON, 2021).

A implementação de modelos de rede de alta fidelidade segundo os autores citados, para simular falhas e recuperações pode ajudar identificar componentes críticos e

avaliar o impacto das dependências e interdependências sobre a resiliência do sistema. Contudo, o custo computacional dos modelos de rede cresce com o número de componentes e relações interdependentes. Integração de modelos de rede e a otimização técnicas são comuns para simular decisões humanas de *retrofit* e restauração sob um cenário de perigo.

Os coeficientes de dependência em uma tabela quantitativa também podem ser determinados a partir de outras análises de simulação, como tabelas baseadas em teoria econômica, em que as infraestruturas estão interligadas para avaliar os aspectos econômicos. As tabelas baseadas na teoria econômica se dividem em duas categorias: modelos de entrada-saída e análises de equilíbrio geral computáveis.

O primeiro modelo insumo-produto, figura 4, visa modelar quantitativamente a natureza interativa dos processos de produção e consumo entre os setores. As tabelas de entrada-saída (I-O) representam os fluxos monetários dentro de um período escolhido. As interdependências são representadas por transações intersetoriais com um conjunto de equações lineares, que são os saldos entre a entrada total e a produção agregada para cada setor em um tempo escolhido. Desde então, modelos de entrada-saída têm sido aplicados com sucesso para desenvolver políticas econômicas em diversos países (SUN, BOCCHINI E DAVISON, 2021).

Insumo/Produto (custos ↓ receitas →)	Setores		Demanda Final (Y)	Valor Bruto da Produção ($X = \sum X_{ij} + Y_i$)
	X_1	X_2		
X_1	X_{11}	X_{12}	Y_1	X_1
X_2	X_{21}	X_{22}	Y_2	X_2
Valor Adicionado (V)	V_1	V_2		
Valor Bruto da Produção ($X = \sum X_{ij} + V_j$)	X_1	X_2		

Figura 4: Modelo insumo-produto
Fonte: Mortari e Oliveira (2016, p. 348)

Com base no modelo de entrada-saída de Leontief, o Modelo de Entrada-Saída de Inoperabilidade (IIM) foi desenvolvido para gestão de infraestrutura, isto é, capturar o serviço de infraestrutura interrompido, chamado de “inoperabilidade”, ruptura na demanda e oferta. O IIM usa os mesmos princípios do modelo básico de entrada-saída, mas difere pela

utilização de um vetor de perturbação que modela a inoperabilidade de 0 a 1 para uma interrupção do sistema resultante de uma interrupção direta em um setor ou em um conjunto de setores, o que destaca os impactos financeiros e inoperáveis devido aos efeitos em cascata entre as infraestruturas.

Com base no IIM, as partes interessadas podem concentrar recursos limitados nas interações financeiramente mais importantes e nos setores financeiramente mais afetados no planejamento de eventualidades e identificar setores críticos na avaliação pós-evento, conforme relatam Sun, Bocchini e Davison (2021).

Considerando o impacto econômico na recuperação, foram desenvolvidos Modelos de Entrada e Saída de Inoperabilidade Dinâmica (DIIM). O modelo, figura 5, pode relacionar a inoperabilidade inicial e o estado de recuperação ao sistema resiliência em um processo de recuperação dinâmico, de modo a representar a evolução de interdependências ao longo do tempo.

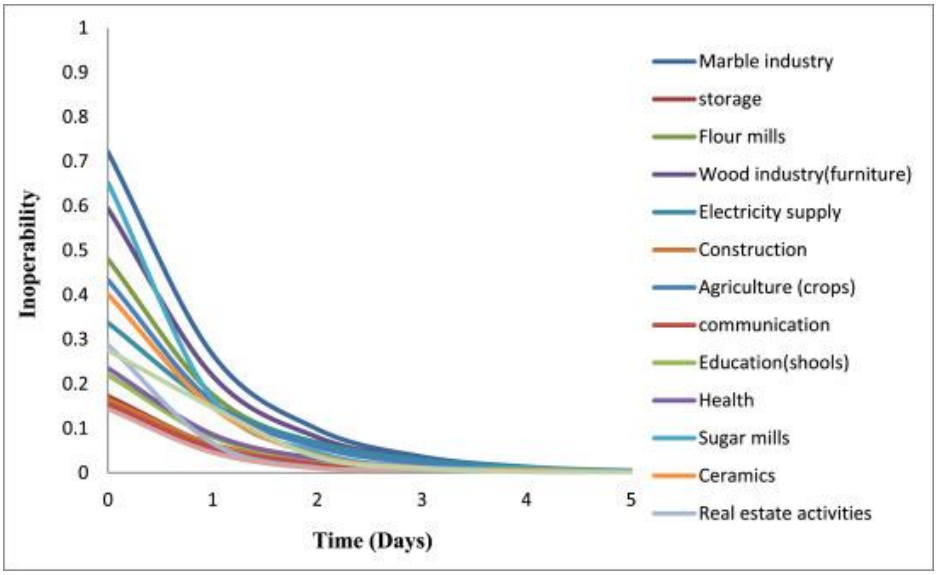


Figura 5: Modelos entrada e saída de inoperabilidade dinâmica
Fonte:Yaseen (2020, p. 876)

Esses modelos de entrada-saída são eficientes computacionalmente. No entanto, a coleta e o pré-processamento de dados são complicados para representar todas as despesas e receitas por uma tabela, quando muitos sistemas/setores são envolvidos. Além disso, os modelos de entrada-saída são limitados a análises em nível de sistema, podendo não representar interdependências no nível do componente. Como mencionado para outros modelos, este torna difícil estender os resultados obtidos para um local e cenário de perigo

para outros. Outros fatores como restrições de recursos, tendências de mercado e fatores humanos podem levar a uma variação significativa tanto na operabilidade quanto na economia, mas os modelos de entrada e saída falham em abordá-los (SUN, BOCCHINI E DAVISON, 2021).

As críticas sobre o uso desses modelos de entrada e saída para entender as interdependências em desastres abrangem a perda de produção econômica que pode não variar de forma linear com os danos na infraestrutura devido a redundâncias do sistema e planos de contingência e os coeficientes constantes geralmente representam um equilíbrio estático em um tempo fixo, desconsiderando as variações de interação sob condições extremas (SUN, BOCCHINI E DAVISON, 2021).

Considerando esses modelos apresentados por Sun, Bocchinie Davison (2021), para constituir um método de avaliação preliminar da interdependência no contexto cibernético podem-se considerar o aspecto econômico, o qual se limita a interdependências em nível sistêmico e não é capaz de lidar com o problema baseado em interdependências elementares ou outros modelos de interdependência que podem lidar com incertezas e são adequados para avaliar os danos potenciais em diferentes níveis de confiança e comparando planos de reforma e restauração opcionais. Os modelos de rede podem adequar dependências e interdependências crescentes e são particularmente adequados para avaliar a vulnerabilidade das redes.

O conhecimento do impacto de diferentes interdependências pode permitir a tomadores de decisão a realização de operações eficientes ao desacoplar sistemas ou reduzir o impacto adverso nas interdependências, para desenvolver um de plano de gestão de riscos mais eficiente no âmbito cibernético.

3 AS INFRAESTRUTURAS CRÍTICAS NA MB

O Decreto 9.637 de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, descreve a abrangência da Segurança da Informação englobando a Segurança Cibernética, a Defesa Cibernética, a Segurança Física, além da consequente proteção dos dados organizacionais e demais ações que visem garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação (BRASIL, 2018a).

Já a Doutrina Militar de Defesa Cibernética (DMDC) entende como Segurança de Informação e Comunicação (SIC) como “ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações” (BRASIL, 2014).

O conceito de segurança cibernética abrange as ações voltadas para a segurança de operações, visando garantir os que os sistemas de informação possam resistir a situações fora do comum no ciberespaço que possam comprometer a funcionalidade, a integridade, a confidencialidade e a autenticidade dos dados ali armazenados, processados ou transmitidos e dos serviços ofertados por esses sistemas (BRASIL, 2019).

A Estratégia Nacional de Defesa (END) esclarece que o monitoramento da superfície marítima, a partir do espaço, deve integrar as práticas e capacidades operacionais disponíveis na MB, utilizando as doutrinas e sistemas já em uso. Por meio de monitoramento, as forças navais fortalecem suas capacidades de atuar em rede com as forças terrestre e aérea (BRASIL, 2016).

Na Marinha, as ações de Guerra Cibernética, no nível operacional e tático, estão a cargo do Comando Naval de Operações Especiais (CoNavOpEsp), órgão subordinado ao Comando de Operações Navais (ComOpNav), aliados com as medidas de Segurança da Informação, normatizadas, tecnicamente, pela Diretoria de Comunicações e Tecnologia da Informação (DCTIM), com concurso do Centro de Inteligência da Marinha (CIM). O CoNavOpEsp é responsável por assessorar o ComOpNav e o Almirantado na operação do Sistema Naval de Guerra Cibernética (SisNavGCiber), com o objetivo de aplicar as capacidades operacionais das Ações de Guerra Cibernética (AGCiber) em prol das Operações de Guerra Naval.

Nesse contexto, cabe à Diretoria-Geral de Material da Marinha (DGMM) criar normas, instruções técnicas e procedimentos padronizados para áreas de conhecimento relativas ao emprego da Tecnologia da Informação (TI) na MB, especialmente em projetos de desenvolvimento e manutenção de sistemas digitais de informação, segurança de informação digital, auditoria computacional, criptologia, guerra cibernética, forense computacional e tecnologias de suporte à preservação digital e à gestão arquivística cuja execução estará a cargo do DCTIM (BRASIL, 2019).

Compete também a DCTIM a definição de doutrinas e normas relacionadas às atividades SIC e da defesa cibernética, bem como a coordenação, execução e análise dos projetos que resultem em ações de SIC e DC (BRASIL, 2019).

O Poder Naval que integra o Poder Marítimo engloba os meios operacionais da MB, bem como as estruturas de C^2 de logística e administrativa (BRASIL, 2017). Nesse aspecto, o setor cibernético também se mostra relevante para reduzir os riscos de ataques cibernéticos sobre os sistemas digitais da MB e evitar impactos no Poder Naval. Conforme a Brasil (2021), a atuação da segurança de informação (SI) abrange as atividades de prevenção e resposta para proteção dos sistemas de informação para assegurar a utilização dos serviços pelos usuários autorizados e evitar violações das informações digitais armazenadas. Do mesmo modo, envolve a segurança do pessoal, do material e das áreas e instalações, onde esses materiais estão armazenados.

No escopo da Guerra Cibernética, compete ao Centro de Tecnologia da Informação da Marinha (CTIM) operar os recursos tecnológicos, planejar os exercícios e subsidiar a Organização Militar Orientadora Técnica (OMOT) para a capacitação técnica do pessoal que atua em suas atividades. Também compete ao CTIM a gerência e a execução, sob a supervisão da DCTIM, das atividades de SIC assim como a execução técnica das atividades de DC (BRASIL, 2019).

A Segurança Cibernética (SegCiber) com auxílio da SI visa prevenir, detectar, deter e documentar eventuais ameaças ou ataques às pessoas, detentoras de informação, bem como identificar vulnerabilidades em seus ativos e realizar ações voltadas para eliminá-las ou mitigá-las. Incluem-se também os ambientes que armazenam a informação, processam-na e trafegam. O Sistema Naval de Guerra Cibernética (SisNavGCiber) caracteriza-se o conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e recursos humanos e financeiros essenciais para a realização de Ações de Guerra Cibernética (AGCiber) no Espaço Cibernético (ECiber).

Nesse contexto, a estrutura cibernética deve ser dinâmica, permitindo que os níveis tático e operacional atuem com rapidez e flexibilidade. A MB deve se adequar para atender os objetivos previstos na Política Naval, servindo de base para o estabelecimento das AGCiber no nível estratégico, o que resulta em um maior desenvolvimento da Capacidade Cibernética militar (BRASIL, 2019).

Considera-se que há diversas infraestruturas de grande importância e que merecem atenção. No entanto, há a necessidade de estabelecer estratégias de proteção ao nível nacional e internacional. Para construir essa capacidade faz-se necessário identificar, dentro dessas estruturas aquelas que são críticas. Este processo difere entre as nações, considerando características culturais, históricas, capacidades adquiridas, legislação, políticas e geografia.

Ademais, Di Beneditto (2016) esclarece sobre a interconexão entre os sistemas digitais e físicos (Sistemas Ciberfísicos) os quais apresentam mecanismos de controle que utilizam sistemas cibernéticos para controlar sistemas físicos. A integração desses sistemas requer uma avaliação de riscos sistemática e o emprego de princípios de segurança. Considerando os Sistemas Ciberfísicos (SCF), a possibilidade de ameaças é crescente, pois durante o ciclo de vida, novos componentes são atualizados ou adicionados aos sistemas existentes e podem trazer vulnerabilidades no software e no hardware.

Assim, novos meios navais podem dispor de sistemas com alta integração entre os subsistemas que o compõem, de modo que essa característica deve ser cuidadosamente analisada, quanto à segurança, desde sua criação ou aquisição, até as outras etapas ao longo do ciclo de vida.

As diretrizes para SI visam garantir um nível aceitável de segurança, considerando os possíveis riscos em atividades que envolvam processamento de dados em meio eletrônico nas redes locais da MB; todos os ativos da MB; todos os usuários dos serviços disponibilizados pela rede local; e contratos efetuados pela MB com empresas privadas que envolva o tratamento de informações digitais ou integradas por meio de uma rede local, conforme a publicação DGMM-0540 (BRASIL, 2019a).

Para a MB, os reflexos da implantação de um processo de gerenciamento de riscos permitem compreender as ameaças nos sistemas, que podem afetar a execução das suas tarefas, permitindo ao comando do meio ou dos escalões mais elevados ter conhecimento do seu grau de vulnerabilidade e, consequentemente, dos riscos ao cumprimento de alguma missão (SANTOS, 2021).

A Doutrina Militar Naval (DMN) define o Poder Marítimo como “resultante da integração dos recursos de que dispõe a Nação para a utilização do mar e das águas interiores, quer como instrumento de ação política e militar, quer como fator de

desenvolvimento econômico e social, visando a conquistar e manter os objetivos nacionais" (BRASIL, 2017).

Desse modo, o Poder Marítimo insere-se no contexto da Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), aprovada pelo Decreto nº 10.569/2020, por sua participação. Como exemplo, citam-se os navios petroleiros, a navegação de cabotagem e as infraestruturas portuárias. Mesmo que a responsabilidade primária seja das instituições proprietárias as IEC, as Forças Armadas (FA) podem ser chamadas a reforçar as ações de segurança cibernética, visando contribuir com a efetiva Resiliência Cibernética, que permitam a contínua prestação daqueles serviços essenciais, em caso de ataque a essas estruturas (BRASIL, 2020).

As primeiras experiências práticas neste sentido se deram com a participação efetiva das Forças Armadas nos chamados Grandes Eventos. A realização desses eventos no Brasil, contou com participação da Marinha, Exército e a Aeronáutica, sob a coordenação do Estado-Maior Conjunto das Forças Armadas (EMCFA), bem como com a participação de vários Órgãos Governamentais (BRASIL, 2018).

Em 2012, foi criado o Núcleo do Comando de Defesa Cibernética (NuCDCiber) na Estrutura Regimental do Comando do Exército, tendo como primeira missão operacional coordenar e integrar as principais equipes de segurança cibernética do país para planejar a segurança do primeiro grande evento internacional, a Conferência das Nações Unidas sobre Desenvolvimento Sustentável (Rio+20), em junho de 2012 (VIANNA, 2020).

Outras ações de defesa cibernética ocorreram na Copa das Confederações em 2013, seguida pela Copa do Mundo de 2014 e nos Jogos Olímpicos de 2016. Foram estabelecidas estruturas e a consequente interação de componentes das Forças Armadas e interagências com conhecimentos afins com a missão de coordenar e integrar, em operações conjuntas, ações de segurança e defesa cibernéticas (BRASIL, 2018).

Destaca-se que, durante a Copa do Mundo FIFA 2014, ainda não havia uma doutrina cibernética estabelecida e várias dificuldades foram enfrentadas pelos Destacamentos de Defesa Cibernética (BRASIL, 2018), inclusive com um aumento significativo de tentativas de ataques cibernéticos, como reportou o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), com um recorde de incidentes de segurança reportados naquele ano, atingindo a marca de 1.031.047 milhões de incidentes reportados (CERT.BR, 2020).

Brasil (2021) define que são estruturas críticas para a Marinha, os sistemas de informação de Organizações Militares sensíveis às Infraestruturas Críticas (IEC) Navais, à Rede de Comunicações Integrada da Marinha (RECIM) ou àquelas estabelecidas para ações de Guerra Naval, empregadas nas atividades de emprego limitado da força e para atividades benignas, conforme previsto em Brasil (2017).

Incluem também instalações nucleares, sistemas C^2, meios de comunicação ou sistemas de inteligência, redes cabeadas e sem fio, equipamentos criptográficos, sistemas de armas, sistemas de combate, equipamentos embarcados em meios operativos, dentre outros.

Os espaços marítimos e fluviais mostram-se de elevada relevância para a manutenção desenvolvimento nacional e devem ser prioritários no escopo do sistema defensivo. Além disso, em um aspecto mais amplo, essas áreas, englobando linhas de comunicação marítimas e hidrovias, incluindo arquipélagos e ilhas oceânicas; os recursos vivos e a biodiversidade marinha, bem como os recursos naturais não vivos, devido a sua importância para o crescimento econômico da nação, também podem ser considerados como estruturas críticas.

Em consequência, associados a esse escopo estão os navios mercantes, a navegação de cabotagem e as infraestruturas portuárias, que se ameaçadas por um conflito ou um ataque passam a ter sua proteção correlacionada a Força Naval.

Da mesma forma, internamente, as redes cabeadas e sem fio, equipamentos criptográficos, sistemas de armas, sistemas de combate, equipamentos embarcados em meios operativos. Cada elemento integrante dos interesses marítimos nacionais está relacionado à sua importância estratégica e possíveis ameaças, as quais exigem uma postura defensiva (BRASIL, 2021).

Os cabos submarinhos também se enquadram nessa concepção de infraestruturas críticas. De acordo com Farahani e Rezapour, (2011), a introdução de sistemas de TIC pode atuar como aspecto importante na gestão da cadeia de suprimentos e de logística, com implicações na coleta e análise de dados. Essa infraestrutura de cabos de fibra ótica submarinos proporciona o fluxo contínuo de informação entre as cadeias logísticas mundiais, mostrando-se como a única capaz, atualmente, de suportar o tráfego de informações.

Clark (2016), relata que quase todas as informações de voz e internet, incluindo as transmissões militares e financeiras, transitam por cabos submarinos. Neste caso, danos às linhas de comunicação podem causar sérios prejuízos, sendo caracterizadas como infraestruturas críticas.

Por meio de normatização interna, especificamente no campo da Segurança da Informação e Comunicação, DGMM-0540, a Marinha adota uma estratégia de abordagem *Buttom Up*, onde cada organização militar, ligada à Força, recebe a atribuição de classificar quais os recursos computacionais críticos devem receber tratamento diferenciado, no aspecto de segurança, tanto física, quanto da informação e do pessoal, além de designar Gestores responsáveis pela SIC em todas as organizações Militares da Marinha (BRASIL, 2019a).

Sempre se levando em consideração a análise de risco e/ou auditorias internas com o objetivo de salvaguardar esses ativos, visando alcançar o cumprimento de sua respectiva missão, prevendo ações de restabelecimento das estruturas críticas em caso de paralização do serviço por qualquer motivo, como preconiza a publicação DGMM-540 (BRASIL, 2019a).

Verifica-se que um longo caminho já foi percorrido no intuito de promover a segurança das infraestruturas críticas do País. Nesse contexto, a MB tem empregado esforços para promover a segurança de seus ativos, atuando em conjunto com as FA para salvaguardar os interesses nacionais. Contudo, esse é um trabalho de constante aprimoramento, visto que o dinamismo do ambiente cibernético permite a incidência no novas modalidades de ataque.

4. GUERRA CIBERNÉTICA E A MARINHA BRASILEIRA

O Livro Branco de Defesa do Brasil (LBDB) destaca que a ameaça cibernética se tornou um foco de atenção do país, pois coloca em risco a integridade de infraestruturas sensíveis, fundamentais à operação e ao controle de vários sistemas e órgãos diretamente relacionados à segurança nacional (BRASIL, 2012).

A Estratégia Nacional de Defesa (END), em relação ao setor cibernético, requer a capacitação de todos os entes envolvidos, incluindo as tecnologias de comunicação como prioridade entre todos os contingentes das FA. Tais ações ressaltam a necessidade de criar

uma política de Pesquisa e Desenvolvimento (P&D) de cientistas de dados, assim como para as outras áreas que compõem a defesa nacional, como reitera a referida estratégia (BRASIL, 2013).

A Doutrina Cibernética da Marinha (DCM) aponta que a realização de uma operação cibernética requer ações específicas no âmbito operacional/tático que apliquem as capacidades cibernéticas e gerem efeitos desejados no espaço cibernético, conhecidas como Ações de Guerra Cibernética (AGCiber). Atuam nessas ações a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), o Comando Naval de Operações Especiais (CoNavOpEsp) e o Centro de Inteligência da Marinha (CIM), envolvem o emprego de instrumentos na área de Tecnologia de Informação e Comunicação para impactar os ativos de informação do inimigo e permitir a proteção de ativos de informação de seu interesse.

O nível estratégico encontra-se a cargo do Comando Operações Navais, já no nível operacional e tático cabe uma FA ou de uma Força Componente. As AGCiber podem impactar a MB na esfera administrativa e operativa em todos os níveis e são classificadas em Proteção Cibernética) (PtçCiber), Ataque Cibernético (AtqCiber) e Exploração Cibernética (ExpCiber) (BRASIL, 2021).

A DMDC remete que o AtqCiber abrange ações para degradar ou anular sistemas ou informações computacionais armazenadas em dispositivos e redes computacionais e de comunicações do oponente, disposto no espaço cibernético.

As ações de ataque cibernético englobam o reconhecimento de fontes abertas do inimigo; escaneamento (scanning) para encontrar falhas na proteção cibernética do oponente; explorar vulnerabilidades; manipular os meios eletrônicos do alvo, com o intuito de disponibilizar uma entrada para acesso futuro e ocultar as ações realizadas no sistema alvo para impedir o rastreamento (BRASIL, 2014).

A Proteção Cibernética refere-se às medidas empregadas para neutralizar ataques e exploração cibernética contra os dispositivos computacionais e redes de computadores e de comunicações nacionais, aumentando as ações de Segurança, Defesa e Guerra Cibernética diante de uma situação de crise ou conflito. Neutraliza ações ofensivas de AtqCiber e/ou ExpCiber contra ativos de informação de interesse.

Essas ações possuem perspectivas permanentes. Já a Exploração Cibernética consiste em ações de busca ou coleta nos Sistemas de TI, de interesse, com o objetivo de obter a Consciência Situacional (CS) do ECiber, subsidiar ações de AtqCiber e produzir

conhecimento de inteligência. Essas ações devem evitar o rastreamento e servir para a elaboração de novos conhecimentos ou identificar as vulnerabilidades desses sistemas, (BRASIL, 2021).

Atuando na defesa ativa, a Proteção Cibernética, com ações de detecção, identificação, avaliação e neutralização das vulnerabilidades nas redes de computadores e SI em uso pela MB, antes que sejam afetadas, quando ordenada, desencadeia ações ofensivas contra a fonte de ameaça, mesmo quando fora o ECiber. Empregando técnicas de criptografia e implementando controles de segurança; autorizando e estabelece procedimentos de segurança no ambiente operativo, com o objetivo de proteger instalações, equipamentos, dados e pessoal contra ameaças físicas aos ativos de informação (BRASIL, 2019).

Já a Exploração Cibernética consiste em ações de busca ou coleta, nos Sistemas de TI de interesse para obter a consciência situacional do ciberespaço. Essas ações devem evitar o rastreamento e servir para a elaboração de novos conhecimentos ou identificar as vulnerabilidades desses sistemas (BRASIL, 2017).

A DCTIM estabelece a elaboração do Relatório de Inteligência de Ameaças Cibernéticas (RIAC) que tem como objetivo estabelecer procedimentos operacionais sobre a elaboração do relatório a partir de conhecimentos coletados das ferramentas de gerenciamento e segurança de redes de computadores adotadas pela MB como Firewalls, *Intrusion Detection System* (IPS), *Data Loss Prevention (DLP), Web Gateway, Security Information and Event Management* (SIEM), *ePolicy Orchestrator* (ePO), antivírus e em fontes abertas na Internet para identificar possíveis vulnerabilidades, ameaças internas e externas, propor a mitigação das vulnerabilidades detectadas e alterações dos níveis de alarmes cibernéticos vigentes na RECIM (BRASIL, 2018b).

Quando ocorre um ataque cibernético, essas ações ocorrem em sequência e, por isso, são conhecidas como fases, que são executadas em cada tarefa, como condutas técnicas, que variam em grau de complexidade, e são descritas em manuais técnicos das atividades de GCiber.

Um alarme cibernético caracteriza-se como o estado do Espaço Cibernético de interesse da Marinha (ECiber-MB) quanto à possibilidade de concretização de Ameaças Cibernéticas. Um nível de alerta cibernético define o grau de prontidão do guarnecimento da defesa cibernética por um Grupamento Operativo de Guerra Cibernética (GptOpGCiber) na

MB em uma escala progressiva relacionada ao nível de risco de um ataque cibernético e contribui para a coordenação das atividades e ações para salvaguarda do ciberespaço (BRASIL, 2021).

Um acréscimo do nível de Alerta Cibernético sinaliza a escalada das medidas, visando a neutralizar ou impedir o avanço das ameaças cibernéticas identificadas (BRASIL, 2019). O alarme cibernético indica o progressivo aumento do nível de risco da ocorrência de ataques cibernéticos. Cada alarme refere-se a um nível de alerta cibernético que reflete um conjunto de ações cibernéticas defensivas adequadas. O agravamento da indicação dos sensores de Proteção Cibernética implica na mudança do nível de alerta e no estado de alerta da PtçCiber da Força (BRASIL, 2021).

Consideram-se como critérios para a definição de alarmes cibernéticos e as alterações nos níveis de alerta: a probabilidade; o cenário, a mudança de nível; interoperabilidade; procedimentos específicos, a identificação e as prerrogativas. Os níveis de Alerta Cibernético são empregados quando houver a probabilidade de concretização de ameaças cibernéticas no ECiber-MB e a interpretação de cada nível relaciona-se a um ou mais cenários de riscos, hipotéticos ou concretos (BRASIL, 2021).

As mudanças de nível podem ser sequenciais, ou não, conforme o grau da ameaça cibernética. A variação de nível está relacionada a mudança da probabilidade de ocorrência das ameaças cibernéticas existentes, conforme os critérios de análise de riscos adotados; a concretização de ameaças existentes; e a abrangência do impacto da concretização de ameaças, segundo os critérios de análise de risco adotados, podendo todos ocorrerem em conjunto ou individualmente (BRASIL, 2021).

Os níveis de alerta cibernético são compatíveis e relacionáveis com as metodologias de gestão de riscos adotadas pelas Forças Armadas (FA) e pelo Ministério da Defesa (MD). Cada nível de alerta exige certos procedimentos os quais devem atender as especificidades da MB e devem estar descritos no planejamento da operação ou em publicações pertinentes. A identificação de cada nível de alerta é feito por cor e grau que distinguem o risco de concretização de ameaças cibernéticas no ECiber-MB (BRASIL, 2021).

Por fim, na esfera do MD, é prerrogativa do Chefe do Estado-Maior Conjunto das Forças Armadas (EMCFA) ratificar o nível de alerta cibernético acima de amarelo, sugerido pelos órgãos de Defesa Cibernética (DCiber) das FA (BRASIL, 2021).

5 CONCLUSÃO

O ambiente cibernético faz parte do cotidiano de todos e se mostra atualmente como a base de funcionamento de diversas estruturas do país. Este espaço virtual não possui limites definidos e apresenta um grande potencial para que elementos adversos e nações tentem colocar seus interesses acima do bem-estar de outros países.

A incidência de ataques cibernéticos é crescente ao redor do mundo e diversos Estados vêm empreendendo e aprimorando suas medidas para combater a guerra cibernética, caracterizada pelo ataque aos ativos de um país dentro do Espaço Cibernético. No Brasil, diversas normas já atentam para as ações que devem ser realizadas em caso de ataque. Tanto em seu mais elevado nível, por meio de políticas, doutrinas e estratégias, quanto em ações de Guerra Cibernética bem empreendidas no nível tático e operacional.

Este estudo teve como objetivo analisar os aspectos de interdependência como requisito para identificação de infraestruturas críticas (IEC) no âmbito cibernético. Uma IEC caracteriza-se como um setor estratégico para o bem-estar econômico e social de um país e que pode afetar o bom andamento do desenvolvimento de uma sociedade. Verificou-se que para identificar uma estrutura crítica, há a necessidade de identificar o grau de criticidade dessas estruturas utilizando probabilidades condicionadas para obter os índices de interdependências entre setores/infraestruturas.

A partir da elaboração de uma Matriz de Dependências no sentido de identificar e quantificar as dependências existentes entre as infraestruturas e nos ativos de importância estratégica. O processo permite avaliar o nível de criticidade, gerando um ranking que indica a criticidade de determinada infraestrutura.

Nesse contexto, demonstraram-se os principais modelos utilizados para determinar a interdependência, utilizadas como ferramenta de análise situacional dos ativos de importância para qualquer instituição. Conclui-se que não só o aspecto econômico associado a um modelo de rede, mas também, as consequências da paralisação de dado sistema, representa um método adequado para avaliar a interdependência no contexto cibernético.

Ressalta-se que o reconhecimento das interdependências permite aos tomadores de decisão a realização de operações com um impacto reduzido em outros setores, gerando um plano de gestão de riscos mais eficiente no âmbito computacional.

No domínio da Marinha do Brasil são consideradas as Infraestruturas Críticas, as instalações Portuárias, as hidrovias, cabeamentos marinhos subterrâneos, os sistemas de informação de Organizações Militares sensíveis, a Rede de Comunicações Integrada da Marinha (RECIM) ou aquelas estabelecidas para ações de Guerra Naval, instalações nucleares, sistemas C^2, meios de comunicação ou sistemas de inteligência, equipamentos criptográficos, sistemas de armas, sistemas de combate, os espaços marítimos e fluviais, equipamentos embarcados em meios operativos, linhas de comunicação marítimas e navios mercantes, além da navegação de cabotagem.

A MB está em constante atuação visando a proteção cibernética, a neutralização de ações cibernéticas contra os dispositivos computacionais e redes nacionais, desenvolvendo ações de Segurança, Defesa e Guerra Cibernética. Assim como as atividades preventivas, visando antecipar possíveis ataques, como exemplo, tem-se a elaboração do Relatório de Inteligência de Ameaças Cibernéticas (RIAC) que tem como objetivo estabelecer procedimentos operacionais a partir de conhecimentos coletados das ferramentas de gerenciamento e segurança de redes de computadores da Força.

Ressalta-se ainda que a Segurança da Informação no âmbito da Administração Naval, já prevê em seus normativos com um sólido arcabouço de ações, atribuições e procedimentos quanto a essa gestão da Segurança da Informação, consolidando a cultura da segurança em uma abordagem *Buttom Up*, alcançando todos as Organizações Militares da Marinha.

A Doutrina Cibernética da Marinha (DCM) aponta a realização de ações específicas voltadas para a proteção cibernética como a gestão de risco entre ativos de informação, patrimônio digital, ameaças, vulnerabilidades, impactos, incidentes de segurança da informação, além da definição sobre o nível de ameaça adequada e o tratamento, comunicação e o monitoramento contínuo desses riscos.

Um alarme cibernético caracteriza-se como o estado do ambiente cibernético de interesse da MB quanto à concretização de ameaças cibernéticas. Nesse prisma, o nível de alerta cibernético define o grau de prontidão das equipes da defesa cibernética na MB em uma escala progressiva relacionada ao nível de risco de um ataque cibernético e contribui para a coordenação das atividades e ações para salvaguarda do ciberespaço.

Assim, as medidas adotadas no âmbito da Guerra Cibernética nas FA e em especial na MB mostram-se pertinentes para trilhar o melhor caminho na defesa do espaço

cibernético. O treinamento e o aprimoramento dos gestores e equipes alocadas para as ações cibernéticas devem ser constantes, assim como o monitoramento dos ativos navais. A Doutrina Cibernética Naval veio para consolidar a importância do assunto para a proteção do ambiente digital e dos limites invisíveis que cercam o país nesse contexto.

Depreende-se que o país encontra-se no caminho certo na análise de novos conhecimentos e aquisição de talentos para o setor cibernético, o que torna as ações de proteção mais eficazes. A competência na adoção dessas medidas no âmbito digital promove a conscientização sobre a importância desta temática e da relação custo-benefício favorável na cooperação para a Segurança e Defesa Cibernética.

REFERÊNCIAS

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa.** Brasília, DF: MD, 2016. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/copy_of_pnd_e_end_2016.pdf Acesso em 09/07/2022.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Política Cibernética de Defesa. MD31-P-02**. Brasília-DF, 2012.

BRASIL. Ministério da Defesa. **Estado-Maior Conjunto das Forças Armadas. Doutrina Militar de Defesa Cibernética. MD31-M-07**. Brasília-DF, 2014b. Disponível em: www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf. Acesso em: 18/04/2022.

BRASIL, **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal**. Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações, 2015. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/noticias/2015/estrategia-de-seguranca-da-informacao-e-comunicacoes-sic-e-de-seguranca-cibernetica-da-administracao-publica-federal-apf. Acesso em 27/07/2022.

BRASIL. Estado-Maior da Armada. **EMA-305: Doutrina Militar Naval**. Brasília-DF, 2017 – 1ª Rev.

BRASIL. **Comando de Operações Terrestres: A Participação do Exército na Segurança dos Grandes Eventos – O Legado**, Brasília, DF, 2018. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/1/1130/1/Grandes%20Eventos_O%20Legado.pdf. Acesso em: 19/04/2022.

BRASIL. **Decreto nº 9.573 de 22 de novembro de 2018**. Institui a Política Nacional de Segurança de Infraestruturas Críticas. Brasília, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9573.htm Acesso em: 13/06/2022.

BRASIL. Diretoria Comunicações e Tecnologia da Informação da Marinha. **DCTIMBOTEC 30/002/2018**. Rio de Janeiro-RJ, 2018b – 1ª Rev.

BRASIL. Diretoria-Geral de Material da Marinha. **DGMM-0540 Normas de Tecnologia da Informação da Marinha.** Rio de Janeiro, 2019 – 3ª Rev.

BRASIL. **Portaria nº 93 de 26 de setembro de 2019**. Gabinete de Segurança Institucional da Presidência da República. 2019a. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663 Acesso em 23/05/2022

BRASIL. Gabinete de Segurança Institucional. Departamento de Segurança da Informação. **Glossário de segurança da Informação**. Brasília, 2019b. Disponível em: http://dsic.planalto.gov.br/arquivos/documentos-pdf/glossario_completo.pdf. Acesso em:

BRASIL. **Decreto nº 10.222 de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm Acesso em: 22/06/2022.

BRASIL. Marinha do Brasil. Estado Maior da Armada. **PEM 2040 – Plano estratégico da Marinha**. Brasília, 2020b. Disponível em https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/book.html Acesso em: 21/05/2022

BRASIL. Estado-Maior da Armada. **EMA-419: Doutrina Cibernética da Marinha**. Brasília-DF, 2021 – 1ª Rev.

CERT.BR. Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil. **Estatísticas dos Incidentes reportados ao CERT.BR**. 2020. Disponível em: https://www.cert.br/stats/incidentes/ Acesso em: 13/06/2022

CLARK, Bryan. **Undersea cables and the future of submarine competition**. Bulletin of Atomic Scientists, v. 72, No. 4, p. 234-237, 2016

CLARKE, Richard A. **Guerra cibernética: a próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro: Brasport Livros e Multimídia, 2015. [5288] p. Ebook.

DI BENEDITO, Marcos Eugênio Medeiros. **Defesa Cibernética: Proposta de Estrutura para o âmbito da Marinha – Defesa dos Sistemas ciber-físicos dos meios Operativos de superfície da Marinha.** Orientador: CF(RM1) Ohara Barbosa Nagashima. 2016. 61f. Dissertação de Doutorado – Curso de Política e Estratégia Marítimas. Escola de Guerra Naval – Rio de Janeiro – RJ. 2016. Disponível em <https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/TESE%20CPEM%2030%20DI%20BENEDITTO%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20-2016.pdf.> Acesso em 14jun.2022.

FARAHANI, Reza; REZAPOUR, Shabnam. **Logistics Operations and Management: concepts and models**. London: Elsevier, 2011 –

HUANG, Chun-Nen; LIOU, James JH; CHUANG, Yen-Ching. **A method for exploring the interdependencies and importance of critical infrastructures**. Knowledge-Based Systems, v. 55, p. 66-74, 2014.

MITSOVA, Diana et al. **Evaluating the impact of infrastructure interdependencies on the emergency services sector and critical support functions using an expert opinion survey**. Journal of Infrastructure Systems, v. 26, n. 2, 2020.

MORTARI, Valéria Silva; OLIVEIRA, Maria Aparecida Silva. **Dependência setorial de insumos importados do setor agropecuário e da indústria intensiva em recursos naturais: uma análise do período de 1995 a 2009**. Economia e Desenvolvimento, 2016.

OLIVEIRA, Valeriano A.; RANGEL, Socorro; DE ARAUJO, Silvio A. **Teoria dos Grafos**. Universidade Estadual Paulista Júlio de Mesquita Filho. 2013

SANTOS, Adriano A. e Silva, António Ferreira da**. Simulation and Control of a Cyber-Physical System under IEC 61499 Standard,** Procedia Manufacturing, Volume 55, 2021

SILVA, Júlio Cezar Barreto Leite da**. Guerra cibernética: a guerra no quinto domínio, conceituação e princípios**. Revista da Escola de Guerra Naval, [S.l.], v. 20, n. 1, p. 193-211, Ago. 2016. ISSN e-2359-3075. Disponível em: <https://revista.egn.mar.mil.br/index.php/revistadaegn/article/view/194/156>. Date accessed: 14 Ago. 2022.

SINGER, Peter W.; FRIEDMAN, Allan. **Cybersecurity and cyberwar: what everyone needs to know.** Oxford University Press (UK), 2014.

SUN, Wenjuan; BOCCHINI, Paolo; DAVISON, Brian D. **Quantitative models for interdependent functionality and recovery of critical infrastructure systems**. Objective resilience: manual of practice. ASCE, Under Review, 2021.

TEIXEIRA JÚNIOR, Augusto Wagner Menezes Teixeira; LOPES, Gills Vilar; FREITAS, Marco Túlio Delgobbo. **As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica.** Carta Internacional, v. 12, n. 3, p. 30-53, 2017.

VIANNA, Eduardo Wallier, CAMELO, José Ricardo de Souza. **Defesa Cibernética no Brasil: Primícias de uma história de sucesso.** Revista da Escola Superior de Guerra, v.35, n.75, p.127-154, set./dez. 2020. Disponível em: https://revista.esg.br/index.php/revistadaesg/article/view/1144/941. Acesso em: 21/04/2022.

YASEEN, Qazi Muhammad et al. **Dynamic inoperability input-output modeling for economic losses estimation in industries during flooding**. Socio-Economic Planning Sciences, v. 72, p. 100876, 2020.