ESCOLA DE GUERRA NAVAL

CMG ROBSON DE MACEDO NASCIMENTO

GUERRA CIBERNÉTICA:
A IMPORTÂNCIA DOS MECANISMOS DE ATUAÇÃO NO DOMÍNIO CIBERNÉTICO PARA O PODER NAVAL

Rio de Janeiro
2021

CMG ROBSON DE MACEDO NASCIMENTO

GUERRA CIBERNÉTICA:
A IMPORTÂNCIA DOS MECANISMOS DE ATUAÇÃO NO DOMÍNIO CIBERNÉTICO PARA O PODER NAVAL

Tese apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CF (RM1) Fabiano Rebello Cantarino

Rio de Janeiro
Escola de Guerra Naval
2021

AGRADECIMENTOS

Primeiramente, gostaria de agradecer ao CF (RM1) Fabiano Rebello Cantarino, meu orientador, pelas precisas e oportunas orientações durante a elaboração desta tese. Sempre disposto a atender minhas demandas, inclusive em seus períodos de descanso, norteou minhas pesquisas e indicou oportunidades de melhorias no ordenamento dos conceitos apresentados, permitindo as correções necessárias durante o desenvolvimento do trabalho.

Aos instrutores da Escola de Guerra Naval, pelos conhecimentos transmitidos e pelo inconteste entusiasmo ao elucidar as dúvidas que lhes foram apresentadas, contribuindo para orientar este trabalho.

Às minhas amadas esposa e filha, minha eterna gratidão pelo incondicional apoio e carinho, determinantes para o amadurecimento deste trabalho científico.

Aos colegas e amigos da turma do Curso de Política e Estratégia Marítimas 2021 da Escola de Guerra Naval, que, de forma direta ou indireta, contribuíram para minha formação, o meu muito obrigado.

Por fim, a Deus, por permitir, outra vez, que eu tivesse saúde, equilíbrio e entusiasmo no decurso do trabalho.

RESUMO

O advento da internet, considerado uma das maiores invenções do século XX, fez surgir o espaço cibernético e transformou a forma de comunicação. Com alcance global e elevada capacidade de trafegar informações, a internet tem impulsionado o desenvolvimento de novas tecnologias empregadas pela sociedade, entre elas as de informação e comunicações. Essa transformação digital torna Estados e organizações dependentes do espaço cibernético, pois a conectividade por ele proporcionada traz consigo benefícios aos usuários. Entretanto, apresenta vulnerabilidades que devem ser consideradas. Mesmo em tempo de paz, a guerra cibernética está presente e o gerenciamento de riscos cibernéticos tornou-se essencial para os Estados e organizações internacionais, como Estados Unidos da América, República Popular da China e Organização do Tratado do Atlântico Norte, que se dedicam há mais tempo ao enfrentamento de tais ameaças e, por conseguinte, apresentam maior maturidade no setor. Assim, sob o conceito de guerra cibernética, eles se mantêm capazes de realizar ações defensivas e ofensivas nesse domínio operacional, reafirmando seu poder cibernético. Há anos, o setor cibernético brasileiro vem se desenvolvendo, por meio da publicação da Política de Defesa Nacional, Estratégia Nacional de Defesa, Política Cibernética de Defesa, Doutrina Militar de Defesa Cibernética, Política Nacional de Segurança da Informação, Estratégia Nacional de Segurança da Informação, criação do Comando de Defesa Cibernética, do Centro de Defesa Cibernética e da Escola Nacional de Defesa Cibernética. Para a atuação integrada no setor, o Estado brasileiro criou o Sistema Militar de Defesa Cibernética, que visa a assegurar o efetivo emprego do espaço cibernético pela Defesa Nacional e negar ou complexificar ações hostis contra os interesses brasileiros. Inserida nesse sistema, a Marinha do Brasil exerce suas atribuições por meio de sua estrutura de defesa e guerra cibernética. O presente trabalho, de forma descritiva e analítica, verificará, por meio de pesquisa bibliográfica-documental, se a estrutura organizacional da Marinha é adequada para atender as demandas do Ministério da Defesa, que requerem da Força um poder cibernético compatível com as atuais ameaças. A implementação de um sistema de guerra cibernética da Marinha do Brasil, com a presença de um órgão central na estrutura organizacional do Comando de Operações Navais, certamente concorrerá para o aprimoramento das ações cibernéticas efetuadas pela Marinha, integrando e coordenando as atividades associadas à guerra e à defesa cibernética, contribuindo para o aumento do seu poder cibernético.

Palavras-chave: Espaço cibernético; Guerra cibernética; Defesa cibernética; Sistema Militar de Defesa Cibernética; Poder cibernético.

ABSTRACT

The advent of the internet, considered one of the greatest inventions of the 20th century, gave rise to cyberspace and transformed the way of communication. With a global reach and high capacity to transfer information, the internet has driven the development of new technologies used by society, including information and communication technologies. This digital transformation has made states and organizations dependent on cyberspace, since its connectivity provides benefits to its users. However, it is open to much vulnerability. Even in peacetime, cyber warfare is present, and cyber risk management has become essential for states and international organizations. The United States of America, the People's Republic of China and the North Atlantic Treaty Organization have all been dedicated to confronting such threats for a long time and are, therefore, more mature in this sector. Thus, within the concept of cyber warfare, they remain capable of carrying out defensive and offensive actions in this operational domain, reaffirming their cyber power. The Brazilian cyber sector, in turn, has been promoted over the years through the publications of the National Defense Policy, the National Defense Strategy, the Cyber Defense Policy, the Military Doctrine of Cyber Defense, the National Information Security Policy, the National Information Security Strategy, and through the creation of the Cyber Defense Command, the Cyber Defense Center and the National Cyber Defense School. For integrated action in the sector, the Brazilian state created the Military Cyber Defense System, which aims to ensure the effective use of cyber space by the National Defense and deny or complexify hostile actions against Brazilian interests. As part of this system, the Brazilian Navy exercises its attributes through its defense structure and cyber warfare. The present work will descriptively and analytically verify, through a literature review, whether the organizational structure of the Navy is adequate to meet the demands of the Ministry of Defense, which requires from the Navy a cybernetic power able to address the current threats. The implementation of a Brazilian Navy cyber warfare system with the presence of a central body in the organizational structure of the Naval Operations Command will certainly contribute to the improvement of the cyber actions carried out by the Navy, as it will integrate and coordinate the activities associated with war and cyber defense, and thus contribute to increasing the Navy's cyber power.

Keywords: *Cyber space; Cyber warfare; Cyber defense; Military Cyber Defense System; Cyber power.*

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AEN –	Ação Estratégica Naval
ANA –	Agência Nacional de Águas
Anatel –	Agência Nacional de Telecomunicações
AFCYBER –	Força Aérea Cibernética dos Estados Unidos da América
ARCYBER –	Comando Cibernético do Exército dos Estados Unidos da América
B Com –	Batalhão de Comunicações
B Com GE –	Batalhão de Comunicações e Guerra Eletrônica
BGE –	1º Batalhão de Guerra Eletrônica
BIM –	Batalhão de Inteligência Militar
C^2 –	Comando e Controle
CCA-BR –	Centro de Computação da Aeronáutica de Brasília
CCDCOE –	Centro de Excelência de Defesa Cibernética Cooperativa da OTAN
CDCAER –	Centro de Defesa Cibernética da Aeronáutica
CDCiber –	Centro de Defesa Cibernética
Cia C^2 –	Companhia de Comando e Controle
Cia Com –	Companhia de Comunicações
CIM –	Centro de Inteligência da Marinha
CISA –	*Cybersecurity and Infrastructure Security Agency*
CITEx –	Centro Integrado de Telemática do Exército
CM –	Comando da Marinha
ComDCiber –	Comando de Defesa Cibernética
ComOpNav –	Comando de Operações Navais
CoNavOpEsp –	Comando Naval de Operações Especiais
CRI –	Capacidades Relacionadas à Informação
CT –	Centro de Telemática
CTA –	Centro de Telemática de Área
CT&I –	Ciencia, Tecnologia e Inovação
CTIM –	Centro de Tecnologia da Informação da Marinha
CTIR –	Centro de Tratamento de Incidentes de Rede
CyOC –	Centro de Operações do Ciberespaço da OTAN
DC –	Defesa Cibernética

DCTIM – Diretoria de Comunicações e Tecnologia da Informação da Marinha
DGMM – Diretoria-Geral do Material da Marinha
DMN – Doutrina Militar Naval
DoD – Departamento de Defesa dos Estados Unidos da América
Dst Cj G Ciber – Destacamento Conjunto de Guerra Cibernética
DTTI – Destacamento Técnico de Tecnologia da Informação
E-Ciber – Estratégia Nacional de Segurança Cibernética
EB – Exército Brasileiro
ELP – Exército de Libertação Popular
EMA – Estado-Maior da Armada
EMAER – Estado-Maior da Aeronáutica
EMCFA – Estado-Maior Conjunto das Forças Armadas
EME – Estado Maior do Exército
END – Estratégia Nacional de Defesa
ENSI – Estratégia Nacional de Segurança da Informação
ENaDCiber – Escola Nacional de Defesa Cibernética
ESG – *Enterprise Strategy Group*
EsqdGCiber – Esquadrão de Guerra Cibernética
Etta Def Ciber – Estrutura de Defesa Cibernética
Etta G Ciber – Estrutura de Guerra Cibernética
Etta Mi D – Estrutura Militar de Defesa
EUA – Estados Unidos da América
F Cj G Ciber – Força Conjunta de Guerra Cibernética
F Ter – Força Terrestre
FA – Força Armada
FAB – Força Aérea Brasileira
FLTCYBER – Comando Cibernético da Esquadra dos Estados Unidos da América
FS – Força Singular
G Ciber – Guerra Cibernética
GCI – Índice Global de Segurança Cibernética
IoT – *Internet of Things*
ISSA – *Information Systems Security Association*
M-40 – Subchefia de Logística do Estado-Maior da Armada

MARFORCYBER –	Comando do Ciberespaço das Forças do Corpo de Fuzileiros Navais dos Estados Unidos da América
MB –	Marinha do Brasil
MD –	Ministério da Defesa
NCDOC –	*Navy Cyber Defense Operations Command*
NCSI –	*National Cyber Security Index*
NETWARCOM –	*Naval Network Warfare Command*
NIOC –	*Naval Information Operation Commands*
NSD –	*Network Systems Department*
NuCDCAER –	Núcleo do Centro de Defesa Cibernética da Aeronáutica
OCGCiber –	Órgão Central de Guerra Cibernética
OM –	Organização Militar
OMOT –	Organização Militar Orientadora Técnica
OpInfo –	Operação de Informação
OTAN –	*Organização do Tratado do Atlântico Norte*
PCT –	Programa de obtenção das Fragatas Classe Tamandaré
PDN –	Política de Defesa Nacional
PEM –	Plano Estratégico da Marinha
PNM –	Programa Nuclear da Marinha
PNSI –	Política Nacional de Segurança da Informação
PPC –	Processo de Planejamento Conjunto
PPM –	Processo de Planejamento Militar
PR –	Presidência da República
RECIM –	Rede de Comunicações Integradas da Marinha
RPC –	República Popular da China
SDA –	Sistemas Digitais Administrativos
SDO –	Sistemas Digitais Operativos
SEC²Ex –	Sistema Estratégico de Comando e Controle do Exército
SGC –	Sistema de Guerra Cibernética
SGCEx –	Sistema de Guerra Cibernética do Exército
SIC –	Segurança da Informação e Comunicações
SINAMOB –	Sistema Nacional de Mobilização
SINDE –	Sistema de Inteligência de Defesa
SISCEAB –	Sistema de Controle do Espaço Aéreo Brasileiro

SisCTID –	Sistema de Ciência, Tecnologia e Inovação de Interesse da Defesa Nacional
SISDABRA –	Sistema de Defesa Aeroespacial Brasileiro
SISFRON –	Sistema Integrado de Monitoramento de Fronteira
SisGAAz –	Sistema de Gerenciamento da Amazônia Azul
$SISMC^2$ –	Sistema Militar de Comando e Controle
SISMOMIL –	Sistema de Mobilização Militar
SisTEx –	Sistema de Telemática do Exército
SMDC –	Sistema Militar de Defesa Cibernética
SSF –	*Strategic Support Force*
TI –	Tecnologia da Informação
TIC –	Tecnologia da Informação e Comunicação
USAFRICOM –	Comando dos Estados Unidos da América para a África
USCENTCOM –	Comando Central dos Estados Unidos da América
USCYBERCOM –	Comando Cibernético dos Estados Unidos da América
USEUCOM –	Comando Europeu dos Estados Unidos da América
USINDOPACOM –	Comando Indo-Pacífico dos Estados Unidos da América
USNORTHCOM –	Comando Norte dos Estados Unidos da América
USSOCOM –	Comando de Operações Especiais dos Estados Unidos da América
USSOUTHCOM –	Comando Sul dos Estados Unidos da América
USSPACECOM –	Comando Espacial dos Estados Unidos da América
USTRANSCOM –	Comando de Transporte dos Estados Unidos da América
USSTRATCOM –	Comando Estratégico dos Estados Unidos da América

SUMÁRIO

1 INTRODUÇÃO

A internet surgiu na década de 1960, no âmbito do exército dos Estados Unidos da América (EUA), e se desenvolveu a partir da década de 1980, tornando-se uma rede global de computadores na década de 1990.

Uma das maiores invenções do século XX, desde o seu surgimento, graças ao alcance global, à agilidade na troca de informações e à compressão do tempo-espaço[1], ela vem alavancando novos desenvolvimentos tecnológicos e gerando, até hoje, transformações no modo como a sociedade vive e se relaciona. Pode-se afirmar, assim, que viver sem a internet é impensável na contemporaneidade.

Uma rede global aberta que possibilita a comunicação entre redes de computadores de todo o mundo, formando o espaço cibernético, a internet propicia que redes privadas conectadas a ela sejam acessadas por pessoas não autorizadas. Nesse cenário, há diversos tipos de redes privativas, tais como: sistemas de controle e monitoramento, que permitem que máquinas e sistemas sejam operados remotamente, via rede de dados; e sistemas corporativos, desenvolvidos para atenderem a gestão da organização de maneira integrada.

Essa grande mudança no âmbito das comunicações gerada pelo advento da internet trouxe consigo inúmeras vantagens, como as já citadas acima, mas, também, vulnerabilidades[2] que são exploradas por atores diversos, sejam eles estatais ou não-estatais intencionalmente preparados ou não, os quais passaram a realizar ações no espaço cibernético com diferentes propósitos, como atividades criminosas ou em benefício de um Estado.

É nesse contexto que o ciberespaço se apresenta como mais um domínio operacional de guerra, empregados pelas forças militares dos Estados, por meio de seus guerreiros cibernéticos e que passam a atuar de maneira sinérgica, para ampliar a probabilidade de sucesso de ações em terra, no mar, ar ou espaço.

Ademais, mesmo em tempo de paz, Estados, organizações, instituições e empresas convergem suas atenções para a proteção de suas infraestruturas de redes, pois tornaram-se alvos de ataques, cujas ocorrências vêm se intensificando e cujo grau de sofisticação eleva-se cada vez mais. Assim, não dispor de poder cibernético[3] torna-se um fator de fraqueza[4] para

---

[1] Compressão do espaço-tempo é um conceito de David Harvey que nasce no contexto da globalização, em que as distâncias são superadas e as transformações tecnológicas são capazes de acelerar os acontecimentos globais (PENA, 2021).

[2] De acordo com a norma ISO 27000, vulnerabilidade é "uma fraqueza de um ativo que poderia ser potencialmente explorada por uma ou mais ameaças".

[3] Habilidade na utilização do ciberespaço para alcançar resultados específicos ou estratégicos (BARROS, 2015).

[4] "Circunstância ou elemento que, em um exame da situação, destaca-se como desvantagem para um dos contendores" (BRASIL, 2015, p. 116).

qualquer Estado, nele inseridas suas Forças Armadas (FA).

A Marinha do Brasil (MB), para cumprir a sua missão[5], tendo como suas condicionantes o artigo 142 da Constituição Federal (CF) e a Lei Complementar (LC) nº 97/99, busca, para a condução das tarefas do Poder Naval nos ambientes de guerra naval (submarino, superfície, aéreo e anfíbio) (BRASIL, 2020b), dispor de meios e sistemas tecnologicamente atualizados. Por meio de suas Ações Estratégicas Navais (AEN) alinhadas à permanente busca da independência tecnológica, no que diz respeito a meios, sistemas e equipamentos de defesa (BRASIL, 2020b), a MB procura modernizar a Força Naval naqueles ambientes, estando tais necessidades inseridas em Programas Estratégicos.

Empregar sistemas tecnologicamente modernos significa, na atualidade, usar formas de tecnologia de informação[6] (TI) para a sua operação e manutenção, podendo ser suscetíveis a ataques cibernéticos. Assim, para a MB alcançar a liberdade de ação no ciberespaço, torna-se fundamental que ela se estruture e desenvolva as capacidades e habilidades defensivas, a fim de fazer frente às ameaças cibernéticas, bem como às ofensivas, para utilizar este domínio operacional, visando ao atingimento de resultados específicos ou estratégicos.

Cabe ressaltar, ainda, que a conjuntura internacional somada à rápida evolução tecnológica, indicam que a maioria dos conflitos transcenderá o campo de batalha tradicional e, por consequência, os limites entre os períodos de paz e de guerra serão cada vez menos nítidos. Assim, esta tese traz como questão central: Considerando o constante processo evolutivo das ameaças no ciberespaço, a estrutura organizacional da MB, voltada à defesa e à guerra cibernética, é adequada para atuar nos três campos – ofensivo, defensivo e exploratório?

Nesse contexto, o presente trabalho tem como propósito apresentar a importância do ciberespaço para o Poder Naval, analisar a adequabilidade da estrutura organizacional da MB para atuar defensiva e ofensivamente no ciberespaço e identificar oportunidades de melhoria, com foco na estrutura organizacional da MB voltada para a guerra e a defesa cibernética, adotando como *benchmark* os EUA, a Organização do Tratado do Atlântico Norte (OTAN) e a República Popular da China (China).

A relevância do trabalho está associada à crescente dependência da tecnologia pela MB, o que lhe exige uma adequada estrutura para atuar no espaço cibernético. Isso posto, o trabalho possibilitará a verificação da adequabilidade de sua estrutura para esse fim ou a

[5] Missão da MB: "Preparar e empregar o Poder Naval, a fim de contribuir para a Defesa da Pátria; para a garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem; para o cumprimento das atribuições subsidiárias previstas em Lei; e para o apoio à Política Externa" (BRASIL, 2020b, p. 6).

[6] É um conjunto de todas as atividades e soluções providas por recursos de computação que visam à produção, ao armazenamento, à transmissão, ao acesso, à segurança e ao uso das informações.

identificação de oportunidades de melhorias, visando à atuação ofensiva nesse domínio operacional, bem como à proteção de seus sistemas de informação [7] administrativos e operativos, potenciais alvos de ataques e fonte de preocupações manifestadas na Estratégia Nacional de Defesa (END).

Para responder à questão central supramencionada, este trabalho terá como objetivo geral: à luz das condicionantes de alto nível e com base na ordenação adotada pelos EUA, OTAN e China, analisar a adequação da estrutura organizacional da MB e seu mecanismo, para atuar nos três campos da defesa e da guerra cibernética (ofensivo, defensivo e exploratório) e apresentar sugestões para o aprimoramento da atual organização, para este fim.

Com o intuito de fundamentar a consecução do objetivo geral, o desenvolvimento do trabalho perpassará pelos seguintes objetivos específicos: identificar os conceitos de guerra cibernética, sua evolução e os aspectos relacionados ao emprego do poder militar; examinar o espaço cibernético sob a perspectiva dos EUA, OTAN e China e como eles se organizam para atuar no ciberespaço; analisar como a MB, o Exército Brasileiro (EB) e a Força Aérea Brasileira (FAB) estão organizados para defenderem seus interesses no espaço cibernético, à luz dos documentos condicionantes.

O trabalho foi elaborado, por meio de pesquisa exploratória, com uma abordagem essencialmente qualitativa, empregando, como procedimento para a coleta de material de estudo, a pesquisa bibliográfica-documental associada à técnica de documentação indireta, fundamentada na legislação, em livros, periódicos, publicações doutrinárias e artigos relacionados ao tema.

Para orientar a leitura e compreensão, o trabalho constará de três capítulos e uma conclusão.

O primeiro capítulo apresenta a concepção do espaço cibernético como um novo domínio operacional, assim como os conceitos de guerra e defesa cibernética, realçando a relevância de tal tema no século XXI e os aspectos relacionados ao emprego do poder militar. Ademais, o capítulo aborda o amadurecimento do setor cibernético brasileiro e apresentará como o Brasil tem se estruturado, de forma a ter liberdade para atuar no ciberespaço.

No segundo capítulo, será analisada a importância do espaço cibernético sob a ótica dos EUA, OTAN e China e será identificado como eles se encontram organizados, para atuar neste domínio operacional.

O terceiro capítulo analisa como a MB, o Exército Brasileiro (EB) e a Força Aérea

[7] Sistema para coletar, processar, armazenar e transmitir informações, de modo a facilitar o acesso de usuários, atender às suas necessidades e solucionar problemas (Disponível em: <https://portal.unigranrio.edu.br/blog/o-que-e-sistemas-de-informacao>. Acesso em: 01 jun. 2021).

Brasileira (FAB), inseridos no Sistema Militar de Defesa Cibernética (SMDC) brasileiro, estão organizados para defender seus interesses e os do país no espaço cibernético, à luz dos documentos condicionantes. Adicionalmente, aponta oportunidades de melhorias na atual estrutura da MB diretamente ligada às ações cibernéticas.

Ao término deste trabalho, espera-se evidenciar a relevância do espaço cibernético para o Poder Naval brasileiro e concluir acerca da adequabilidade da atual estrutura organizacional da MB voltada à guerra e à defesa cibernética.

2 O ESPAÇO CIBERNÉTICO E SUAS IMPLICAÇÕES

A internet surgiu na década de 1960, no contexto da Guerra Fria, a partir de um projeto do exército dos Estados Unidos da América (EUA), que objetivava a criação de um sistema de informação e comunicações em rede, para dinamizar a permuta de informações, assim como descentralizar os conhecimentos gerados pelos centros de pesquisa científica. Esse projeto deu origem à Arpanet, o embrião da internet, que vivenciamos no presente (GILES, 2010).

A internet como é conhecida hoje, desenvolveu-se a partir da década de 1980 e expandiu-se na década de 1990, como uma rede global de computadores, possibilitando a comunicação simultânea de inúmeras pessoas localizadas em diferentes regiões do mundo (CASTELLS, 2003).

Uma das maiores invenções do século XX (CASTELLS, 2003), desde o seu surgimento e, graças ao alcance global, à agilidade na troca de informações e à compressão do tempo-espaço[8], ela vem alavancando novos desenvolvimentos tecnológicos e gerando, até hoje, transformações no modo como a sociedade vive e se relaciona.

Por ser uma rede aberta para redes de computadores, a internet permite que várias outras redes se conectem a ela, formando o nominado espaço cibernético (CLARKE; KNAKE, 2010). Seu crescimento contínuo exige visão estratégica e liderança, por parte dos Estados, para gerenciarem sua utilização e os riscos cibernéticos.

Este capítulo abordará a concepção do ciberespaço como um novo domínio operacional e os conceitos de guerra e defesa cibernética, os quais orientam o desenvolvimento do setor cibernético brasileiro, no tocante à Defesa Nacional.

2.1 Espaço cibernético

A Organização do Tratado do Atlântico Norte (OTAN) compreende domínio operacional como o espaço de interesse e influência em que as atividades e operações são executadas, no intuito de exercer o controle sobre um oponente e de cumprir missões, objetivando os resultados pretendidos (GOŹDZIEWICZ, 2016). Welch (2011), entende-o como a esfera, por meio da qual, as operações militares geram os efeitos desejados.

[8] Compressão do espaço-tempo é um conceito de David Harvey que nasce no contexto da globalização, em que as distâncias são superadas e as transformações tecnológicas são capazes de acelerar os acontecimentos globais (PENA, 2021).

O ciberespaço, considerado como um dos cinco domínios operacionais[9] – terrestre, marítimo, aéreo, espacial e cibernético – desenvolveu-se a partir do último quarto do Século XX, com o surgimento das redes de comunicações globais, especialmente da internet que, como consequência da explosão tecnológica, passou a fazer parte da vida pública e privada. Dessa forma, a sociedade passa a interagir em um novo espaço onde, independentemente de distância, todos estão ligados a todos. No entanto, essa nova dimensão de interação humana trouxe consigo conflitos de interesse e passou a ser um ambiente de ações hostis, que se intensificaram, especialmente, a partir do início do Século XXI.

Visando à defesa de seus interesses, Estados e Organizações Intergovernamentais passaram a considerar o espaço cibernético como um novo domínio operacional, acompanhando a sua constante evolução. Em 2016, a OTAN, por exemplo, reconheceu o ciberespaço como um domínio de operações, que deve ser defendido tão eficazmente como se faz no ar, em terra e no mar (OTAN, 2016). Essa visão é reafirmada em 2021 (OTAN, 2021). No entanto, defender o espaço cibernético não é uma tarefa fácil. Como lembra Somtochukwu (2017), o campo da segurança de rede é amplo e está em constante mudança, exigindo que novas soluções tecnológicas sejam projetadas, para lidarem com as existentes, as novas e as potenciais ameaças.

2.2 Poder

No decorrer da história, o termo poder recebeu inúmeros significados. Em suas diferentes expressões[10], a princípio interpretado, por alguns, como uma capacidade de gerar (ou de resistir a) mudanças e, por outros, como a habilidade de se conseguir o que se quer (BOULDING, 1989, p. 15 *apud* NYE, 2012, p. 26), o poder resulta de um conjunto de inter-relações que combinam recursos e comportamentos. Essas inter-relações alcançam as grandes áreas de conhecimento[11], penetrando na política, economia, educação, ecologia, imunologia, ciência da computação, dentre outras, tornando-se um diferencial competitivo para aqueles que possuem habilidade para empregá-las em seu benefício.

No âmbito deste trabalho, será adotado o conceito de poder expresso por Nye Jr. (2011) que o entende como a capacidade de alterar o comportamento dos outros, para produzir os resultados esperados.

---

[9] BRASIL, 2014, p.18.

[10] Expressões do Poder Nacional: política, econômica, científico-tecnológica, militar e psicossocial.

[11] As áreas de conhecimento, segundo a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), são classificadas, no 1º nível, em nove grandes áreas. Cada uma delas concentra áreas do conhecimento, de acordo com a afinidade de seus objetos, métodos cognitivos e recursos instrumentais.

O ciberespaço, um domínio de interação nacional e internacional, diante da constante disputa pelo poder entre Estados, passa a fazer parte de suas agendas e a permear as relações internacionais. Assim, considerando que o poder cibernético (*cyber power*) é entendido como a habilidade na utilização do ciberespaço para alcançar resultados específicos ou estratégicos (BARROS, 2015), Estados e Organizações Intergovernamentais necessitam investir recursos, na tentativa de reduzirem suas vulnerabilidades e terem liberdade para atuar neste domínio operacional.

2.3 Guerra cibernética e defesa cibernética

Em seu livro Da guerra, Carl von Clausewitz (1780-1831) define a guerra como uma forma de subjugação por meio da força, obrigando o inimigo a submeter-se à nossa vontade (CLAUSEWITZ, 2017).

Distintamente a esse pensamento, em que a guerra está associada, exclusivamente, ao uso da força, Michel Foucault (2005, *apud* BARROS, 2015, p. 91) afirma que a guerra não é meramente um ato político e, sim, um mecanismo da política.

As tradicionais definições para estado de guerra estão intimamente ligadas à existência de conflitos armados, envolvendo Estados, por motivos políticos. No entanto, tal conceito não atinge o novo domínio da guerra – o espaço cibernético – ao limitar que apenas a política ou a força instauram duelos entre os Estados.

O ciberespaço, diferentemente dos demais domínios, é peculiar por não ser um domínio físico. Ademais, seu constante crescimento, graças à liberdade de conexões, torna-o imprevisível (BARROS, 2015) e requer regras relacionais entre seus diversos atores.

O desenvolvimento de novas tecnologias faz com que o homem reflita sobre os efeitos que tais inovações trazem à sociedade e às relações entre Estados. O domínio dos mares trouxe as discussões sobre o poder naval; já o aéreo, gerou debates a respeito do poder aeronáutico (NYE JR., 2011). De maneira similar, o domínio do ciberespaço fez surgir questões sobre o *cyber power*. Com uma grande diferença. Ele ainda não se encontra regulamentado pelo Direito Internacional (BARROS, 2015).

O espaço cibernético distingue-se por ter sido criado pelo homem e é, ainda, objeto de constantes e rápidas mudanças que podem alterar as relações de poder entre os atores internacionais. É um domínio de fácil manipulação sem fronteiras definidas, o que dificulta a construção de barreiras legais e eleva, ainda mais, a instabilidade das complexas relações internacionais (PREBLE, 2011).

O fato de que nesse domínio dificilmente consegue-se identificar que ator possui o maior poder, haja vista que para alcançar o efeito desejado não é necessário ser econômico ou militarmente poderoso, preocupa os Estados. Assim, o complexo espaço cibernético requer dos Estados investimentos para absorção de capacidade que permitam empregar a cibernética como arma para a sua proteção e atuação, bem como para a defesa do domínio cibernético militar (BARROS, 2015).

Segundo Clarke e Knake (2010), a guerra cibernética é uma realidade e há indícios de que tal tipo de guerra acompanhará as futuras guerras cinéticas[12], podendo ocorrer de forma isolada. Além disso, mesmo em tempo de paz, Estados deram início a ela, invadindo redes e infraestruturas, ao instalarem *backdoors*[13] e bombas-lógicas[14].

Até a Segunda Guerra Mundial (II GM) (1939-1945), as guerras ocorriam, essencialmente, em três domínios: terrestre e marítimo e aéreo. Após a II GM, no transcurso da Guerra Fria, surgiu o 4º domínio operacional – o espaço – decorrente da exploração do espaço e da corrida espacial. Com as inovações tecnológicas, o mundo contemporâneo passou a dispor de mais um domínio operacional, o espaço cibernético (ciberespaço), criado pelo ser humano, com uma atuação cada vez maior em todos os demais domínios – terrestre, marítimo, aéreo e espacial. Nesse contexto, guerra cibernética é definida, então, como ações de um Estado-nação para acessar os computadores ou redes de outra nação, com o propósito de causar dano ou transtorno (CLARKE; KNAKE, 2010).

Enfatizando o emprego militar das ações, no Brasil, o Ministério da Defesa (MD) conceitua guerra cibernética como o "uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C^2 do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar" (BRASIL, 2014, p. 19).

Embora não haja uma definição comumente aceita para guerra cibernética, a RAND Corporation[15] entende que esse tipo de guerra é o conjunto de ações de um Estado-nação ou uma organização internacional que visa a danificar computadores ou redes de informação de

---

[12] Guerras convencionais, segundo Clarke e Knake (2010): A Doutrina Militar de Defesa define guerra convencional como "conflito armado realizado dentro dos padrões clássicos e com emprego de armas convencionais" (BRASIL, 2007a, p. 24). Arma convencional é aquela que não é motivo de contestações. Não se incluem nesta categoria as armas nucleares, radiológicas, biológicas e químicas, com algumas exceções (BRASIL, 2015).

[13] *Backdoors* - porta de acesso ao sistema, criada a partir de um programa instalado, que não foi autorizado pelo proprietário do sistema e que permite o acesso ao computador por pessoas não autorizadas.

[14] Bombas lógicas - é um programa malicioso (*malwares*) que se instala em computadores de forma similar aos vírus. Muitos desses *malwares* têm como objetivo destruir dados ou danificar o disco rígido.

[15] Organização global de pesquisa que desenvolve soluções para desafios de políticas públicas, com objetivo de contribuir para a segurança, a saúde e a prosperidade mundial.

outra nação, por meio, por exemplo, de vírus de computador ou ataques de negação de serviço (RAND, 2021).

Pode-se observar que os conceitos de guerra cibernética apresentados por Clarke e Knake (2010) e pelo MD brasileiro (BRASIL, 2014) são análogos ao utilizado pela RAND Corporation no presente, pois os modos de operação dos ataques cibernéticos podem ter evoluído no decorrer do tempo, mas o efeito desejado – causar danos ou transtorno – pelos seus autores, está mantido.

Contudo, há mudança neste período. A era da informação[16], tendo como base o advento da internet e caracterizada pela conectividade em rede, ao trazer uma nova forma organizacional para as sociedades, trouxe consigo um novo desafio, a segurança do ciberespaço. Nesta era, as redes ou sistemas empregados para trafegar a informação no espaço cibernético tornaram-se, não só, recursos dos quais indivíduos, organizações e sociedades dependem para suas atividades e seu desenvolvimento, mas também, alvos de ciberataques[17] de diferentes tipos[18] que, em alguns casos, podem representar um grave risco à segurança nacional[19].

De acordo com o *Internet Security Threat Report* (SYMANTEC, 2019) divulgado em fevereiro de 2019, referente ao ano de 2018, houve um crescimento de 56% nos ataques cibernéticos, o que deu destaque à fragilidade na segurança dos dispositivos de *Internet of Things* (IoT). Ressalta, também, o aumento de ataques do tipo *ransomware* a empresas. Segundo o mesmo relatório, o Brasil ocupou, em 2018, o quarto lugar em ataques por *ransomware*, ficando somente atrás da China, Índia e EUA (SYMANTEC, 2019, p. 37). Ademais, é o terceiro país que mais recebeu ataques cibernéticos no segmento de IoT, com 9,8% das ameaças detectadas pela Symantec, superado apenas pela China (24%) e pelos EUA (10,1%) (SYMANTEC, 2019, p. 54).

Nesse contexto, a Trend Micro[20] divulgou, em seu relatório anual de 2020, sobre segurança cibernética, que os 5 setores mais atingidos no mundo por ataques de ransomware[21] foram: Governo, bancário, manufatura, saúde e financeiro (TREND MICRO, 2020, p. 7-8). E, por conta da importância dos alvos, os pedidos de resgate cresceram significantemente nos

[16] Era em que a realidade tecnológica é mediadora das relações humanas e das interações entre máquinas.
[17] É o mesmo que ataque cibernético.
[18] Principais tipos de ataque cibernético: DDoS (*Distributed Denial of Service* ou negação de serviço distribuída), *criptojacking*, *malware*, *phishing*, *ransomware* e trojan ou cavalo de troia.
[19] Segurança Nacional é uma percepção "entendida como a condição que permite a preservação da soberania e da integridade territorial, a realização dos interesses nacionais, a despeito de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais" (BRASIL, 2020, p. 11).
[20] *Trend Micro Smart Protection Network infrastructure*. Empresa multinacional de cibersegurança.
[21] Tipo de código malicioso que torna os dados armazenados, em um equipamento, inacessíveis, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*), normalmente feito via *bitcoins,* para restabelecer o acesso ao usuário.

últimos anos (TREND MICRO, 2020, p. 4).

Como consequência dessa crescente ameaça – ciberataque – Estados-nação viram-se obrigados a desenvolver uma cultura[22] de segurança cibernética e defesa cibernética em que um conjunto de atitudes, práticas, objetivos e valores com foco coletivo foram incorporados e evoluem, constantemente, para contrapô-la. Para mensurar o preparo dos países no tocante à segurança cibernética em nível global, surgiram índices envolvendo especialistas de diversas origens e organizações, tais como: *Global Cybersecurety Index*[23] (GCI) e *National Cyber Security Index*[24] (NCSI). De acordo com o NCSI de julho de 2021, o qual apresenta análise de 160 países, o Brasil ocupa a 66ª posição global, com um índice de 46,75 (NCSI, 2021).

O gráfico 1, com base no NCSI de julho de 2021, apresenta, de forma ranqueada, em que nível de desenvolvimento e envolvimento uma parcela de Estados avaliados encontra-se no que diz respeito à segurança cibernética.

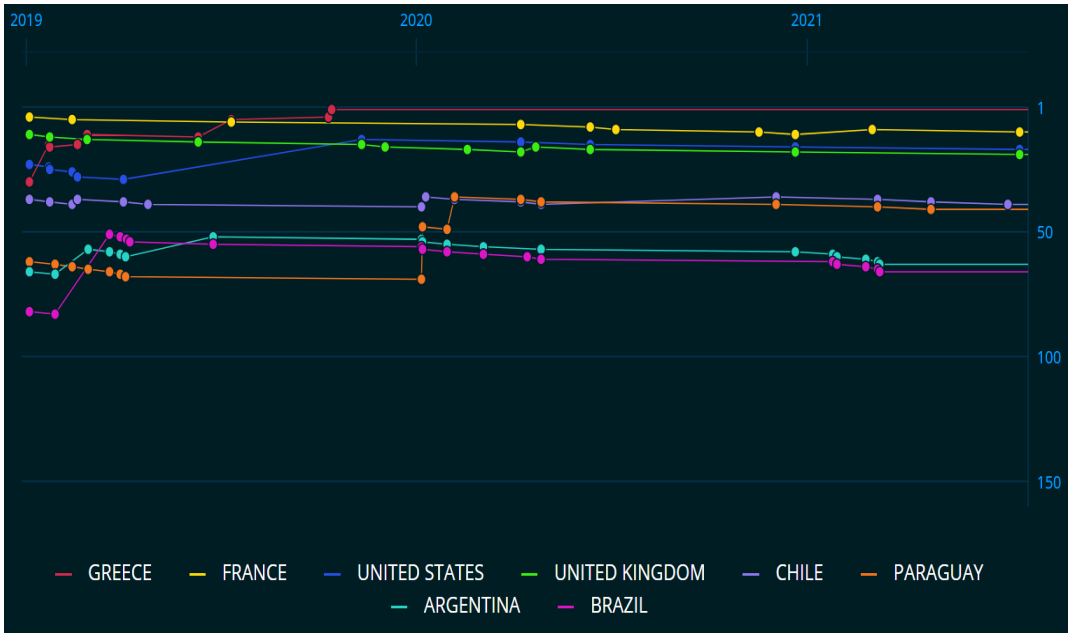


GRÁFICO 1 – **Ranqueamento de índices globais de segurança cibernética de 2019 a 2021.**
Fonte: NCSI, 2021.

Pode-se observar que o Brasil, no primeiro semestre de 2019, apresentou um crescimento no índice se segurança cibernética, superando o Paraguai e a Argentina. No entanto,

[22] "Todo aquele complexo que inclui o conhecimento, as crenças, a arte, a moral, a lei, os costumes e todos os outros hábitos e capacidades adquiridos pelo homem como membro de uma sociedade" (EDWARD B. TYLOR).
[23] Índice Global de Segurança Cibernética (GCI) é uma iniciativa da *International Telecommunication Union*.
[24] Índice Nacional de Segurança Cibernética é mantido e desenvolvido pela *e-Governance Academy*, da República da Estônia. Mede o comprometimento dos países com a segurança cibernética em nível global. A análise de cada país tem como pilares medidas legais, medidas técnicas, medidas organizacionais, desenvolvimento de capacidades e cooperação, que são agregados em uma pontuação geral.

atualmente, o Paraguai (índice 57,14) e a Argentina (índice 48,05) estão melhor classificados e ocupam as 41ª e 63ª posições, respectivamente (NCSI, 2021).

A crescente exploração do espaço cibernético traz preocupações e requer especial atenção dos Estados, organizações, instituições e empresas, pois esse ambiente pode ser empregado para ataques a suas infraestruturas, como nos recentes casos envolvendo a EMBRAER S.A.[25], em 2020 (GARCIA, 2020), e a Colonial Pipeline[26], em 2021. O ataque a esta última causou a suspensão de operações da rede de oleodutos na costa leste dos EUA (TIDY, 2021).

Os ataques cibernéticos, que alcançam inúmeros alvos e são executados por diferentes atores com propósitos diversos, fizeram com que especialistas em ciberespaço fossem além dos limites da análise dos mecanismos de defesa particular ou organizacional, voltando-se para os complexos sistemas de defesa de governo e de infraestruturas críticas do Estado-nação (SABBAT, 2019), visando à segurança nacional. Para isso, o Estado distingue segurança cibernética de defesa cibernética.

A segurança, segundo o conceito do MD em sua Doutrina Militar de Defesa, é uma condição que permite ao Estado a manutenção da soberania e da integridade territorial, assim como a realização dos seus interesses nacionais, sem quaisquer tipos de pressão ou ameaça, e a garantia aos seus cidadãos do exercício dos direitos e deveres constitucionais (BRASIL, 2007a). Em relação ao ambiente cibernético, o conceito acima reveste-se de um conjunto de ações e procedimentos voltados para sua proteção e sua operação contínua, frente a possíveis ataques cibernéticos.

Dessa maneira, no Brasil, a segurança cibernética é compreendida como um conjunto de técnicas e procedimentos que visam a assegurar a existência e a continuidade da sociedade da informação (redes) de uma nação, de modo a garantir e proteger seus ativos de informação e suas infraestruturas críticas (BRASIL, 2007a).

Sem distanciar dessa compreensão, segurança cibernética, segundo a *Cybersecurity and Infrastructure Security Agency*[27] (CISA), é a capacidade de proteger redes, dispositivos e dados contra acesso não autorizado ou uso criminoso, assim como garantir a confidencialidade, integridade e disponibilidade de informações[28].

Ao escrutinar como os temas segurança e defesa cibernética são abordados no

[25] Sofreu ataque cibernético, resultando na divulgação de dados supostamente atribuídos à Companhia, em 30 de novembro, de 2020. O ataque foi identificado em 25 de novembro, de 2020 e indisponibilizou o acesso a um ambiente de arquivos da Companhia (GARCIA, 2020).
[26] Sistema de oleoduto para produtos petrolíferos refinados nos EUA.
[27] Um dos componentes operacionais do Departamento de Segurança Interna - *Department of Homeland Security* dos EUA.
[28] https://us-cert.cisa.gov/ncas/tips/ST04-001.

mundo, observa-se que, distinto do constatado para aquele primeiro tema, os EUA, França, China e a OTAN laboram a defesa cibernética, essencialmente, com um caráter militar, tendo as Forças Armadas um importante papel na concepção de suas estratégias de defesa cibernética. Ou seja, seu conceito fundamentalmente bélico, objetiva contribuir para a Defesa Nacional, cuja definição, no Brasil, é "o conjunto de atitudes, medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território nacional, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas" (BRASIL, 2020, p. 11). Assim, a defesa cibernética objetiva preservar o ciberespaço nacional de uma ação (ou iminente ação) agressora nesse ambiente, atuando, preferencialmente, de modo a se antecipar a um ataque cibernético.

Nesse cenário, o relatório elaborado pelo Grupo de Peritos Governamentais das Nações Unidas sobre desenvolvimentos no campo da informação e telecomunicações, no contexto da Segurança Internacional, em 2015, requer atenção, pois já apresentava a necessidade de os Estados não admitirem o uso de recursos de TIC para causar danos internos ou a outro país, afetando ativos e serviços, públicos ou privados, essenciais ao funcionamento da sociedade e da economia, ou seja, atingindo infraestruturas críticas e sistemas do governo. Além disso, reconhecia a dificuldade para rastrear a fonte de ataque, impossibilitando, assim, a determinação do responsável pelos danos (ONU, 2015, p. 12-13).

O Grupo ainda estabelece como sendo de direito de um país se defender no espaço cibernético quando atacado, porém, ressalta como obrigatória a inequívoca atribuição de responsabilidade para uma possível resposta no mesmo ambiente, observando os princípios jurídicos estabelecidos no direito internacional (ONU, 2015, p. 12-13). Logo, coadunando as preocupações do domínio cibernético às da Defesa Nacional, pode-se concluir que a defesa cibernética, de caráter essencialmente bélico, deve contribuir para a defesa do Estado, com ênfase nas infraestruturas críticas, nos sistemas do governo e na manutenção dos serviços nacionais essenciais, além de ser capaz de atuar de maneira ofensiva (realizar ataque), defensiva (deter ataque) e exploratória.

2.4 Defesa cibernética no Brasil

A preocupação com a defesa cibernética no Brasil deu-se a partir da Política de Defesa Nacional (PDN), estabelecida em 2005, que já fomentava o estabelecimento de uma doutrina cibernética brasileira, ao abordar que os avanços da tecnologia da informação traziam consigo vulnerabilidades que poderiam ser exploradas, para se impossibilitar o emprego de

sistemas associados à defesa do país (BRASIL, 2005).

Em 2008, o MD apresentou a Estratégia Nacional de Defesa (END), aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008, passando a dispor de um plano, contendo as ações estratégicas para modernizar a estrutura de Defesa Nacional (BRASIL, 2008).

Em 2010, o EB ativou o Núcleo do Centro de Defesa Cibernética (NuCDCiber) (BRASIL, 2010), visando à criação do Centro de Defesa Cibernética (CDCiber) na estrutura regimental do Comando do Exército, o que ocorreu em 2012. Até a ativação do ComDCiber, o CDCiber foi responsável pela coordenação e integração das atividades de defesa cibernética no âmbito do MD.

Também em 2012, foi publicada a Política Cibernética de Defesa, visando a nortear as atividades de defesa cibernética, em nível estratégico e de guerra cibernética, nos níveis operacional e tático, no âmbito do MD (BRASIL, 2012).

Em 2014, visando à potencialização da defesa cibernética nacional, o MD cria o Comando de Defesa Cibernética (ComDCiber) e a Escola Nacional de Defesa Cibernética (ENaDCiber) na estrutura regimental do Comando do Exército (BRASIL, 2014a). O ComDCiber e a ENaDCiber foram ativados em 2016 e 2019, respectivamente.

Ainda em 2014, foi estabelecida a Doutrina Militar de Defesa Cibernética, de modo a assegurar uma única concepção sobre o tema no âmbito do MD, assim como contribuir para a atuação conjunta das Forças Armadas (FA) no espaço cibernético, para a defesa do Estado Brasileiro (BRASIL, 2014).

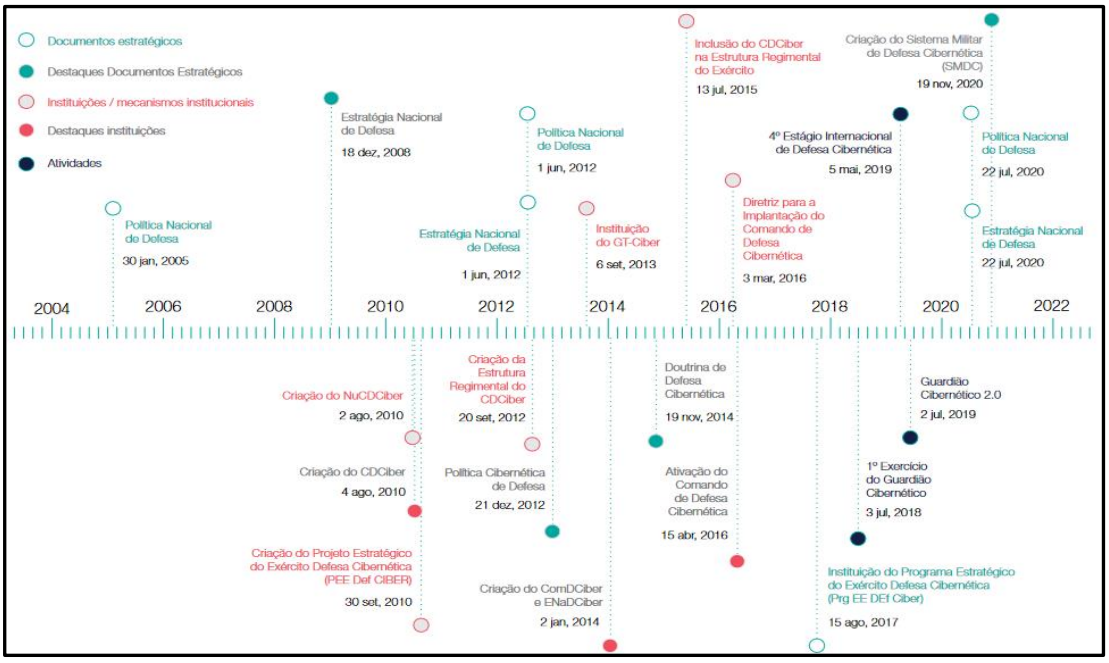


FIGURA 1 - Linha do Tempo: Defesa Cibernética no Brasil.
Fonte: HUREL, 2021, p. 16.

A linha do tempo apresentada na FIG. 1 expõe o desenvolvimento da defesa

cibernética nacional a partir de 2005. Observa-se que, por conta dos nominados grandes eventos – Rio + 20 (2012), Copa do Mundo (2014) e os Jogos Olímpicos (2016) – sediados no país, os esforços se concentraram entre os anos 2010 e 2016, mas as medidas voltadas para o incremento da defesa cibernética não cessaram após o último evento.

O Brasil, em sua atual Política Nacional de Defesa (PND), manifesta preocupação com a segurança e a defesa do ciberespaço nacional, focando, em especial, na garantia do funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional (BRASIL, 2020). Segundo a sua Política Nacional de Segurança da Informação (PNSI) os temas segurança cibernética e defesa cibernética estão inseridos no conceito de segurança da informação (BRASIL, 2018).

Diante de tal inquietação o país trabalha na criação de instrumentos associados a esse domínio operacional – o ciberespaço – dentro de uma grande estratégia nominada Estratégia Nacional de Segurança da Informação (ENSI), que se encontra em fase de elaboração e será constituída por módulos, de modo a abranger a segurança cibernética, a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados (BRASIL, 2018 e BRASIL, 2020). Seu primeiro módulo – segurança cibernética – foi concluído com a aprovação da Estratégia Nacional de Segurança Cibernética (E-Ciber), em fevereiro de 2020 (BRASIL, 2020). O módulo da ENSI que tratará, especificamente, da defesa cibernética ainda não foi criado.

Apesar de o setor cibernético ser considerado fundamental para a Defesa Nacional do país, o Brasil ainda não apresentou uma estratégia nacional de defesa cibernética. Assim, o Ministério da Defesa (MD) brasileiro, a quem compete a defesa nacional contra ataques cibernéticos, não possui, formalmente documentado, um direcionamento estratégico para orientar a elaboração de diretrizes e procedimentos decorrentes.

Mesmo com essa lacuna normativa, o MD, em sua Doutrina Militar de Defesa Cibernética, conceitua defesa cibernética como

> [...] 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 as finalidades 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 (BRASIL, 2014, p. 18).

Contudo, ao dispor sobre guerra cibernética (G Ciber), compreendendo-a como o emprego ofensivo e defensivo de informação e sistemas de informação, no intuito de explorar, degradar ou obstar capacidades de C² do oponente, no cenário de um planejamento ou de uma

operação militar (BRASIL, 2014), evidencia o seu foco no sistema de comando e controle (C^2), em nível operacional e tático, empregado nas ações de combate, para abreviar a completude do ciclo OODA[29]. E confere importância a esse entendimento, ao afirmar que a G Ciber contém em si ações cibernéticas munidas de ferramentas de Tecnologia da Informação e Comunicações (TIC), para desestruturar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle ($STIC^2$) do inimigo e proteger os próprios $STIC^2$ (BRASIL, 2014).

Ademais, associa os conceitos de defesa cibernética e guerra cibernética ao nível de decisão a que o planejamento e a execução de ações estão inseridos. Se o nível de decisão é estratégico, é entendido como defesa cibernética. Se ele é operacional ou tático, recebe a intitulação de guerra cibernética (BRASIL, 2014, p. 18).

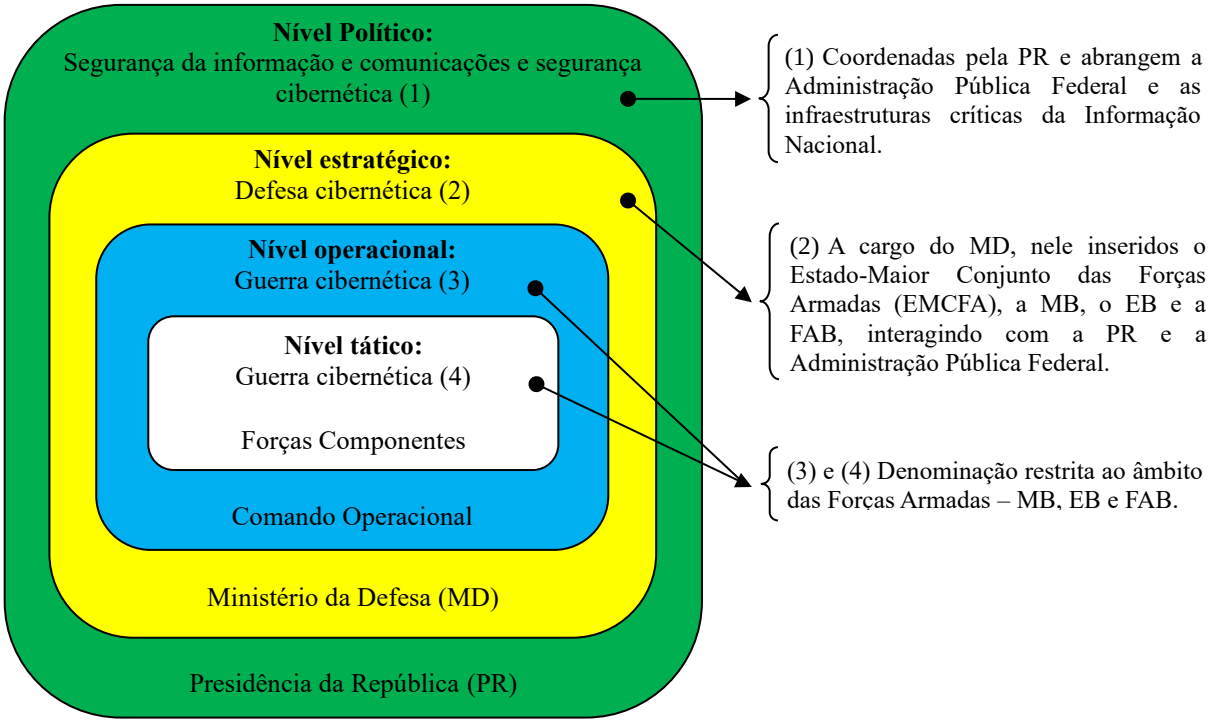


FIGURA 2 – Níveis de decisão.
Fonte: Doutrina Militar de Defesa Cibernética (BRASIL, 2014).

O Sistema Militar de Defesa Cibernética (SMDC) brasileiro tem como órgão central o Comando de Defesa Cibernética (ComDCiber)[30], um comado operacional conjunto – MB, EB e FAB – permanente ativado, e como propósito realizar ações, a fim de assegurar o efetivo emprego do ciberespaço pela Defesa Nacional, assim como impedir ou complexificar possíveis

[29] Ciclo de comando e controle: observação, orientação, decisão e ação. O mesmo que ciclo de Boyd (BRASIL, 2015).
[30] Criado de acordo com a Portaria Normativa nº 2.777 do Ministério da Defesa, de 27 de outubro de 2014. Foi ativado no ano de 2016.

ações hostis contra o Estado brasileiro (BRASIL, 2020h). A concepção do SMDC tem como característica a atuação colaborativa interagências, ou seja, envolve representantes da administração pública federal, de infraestruturas críticas e de órgãos, instituições e empresas de interesse da Defesa.

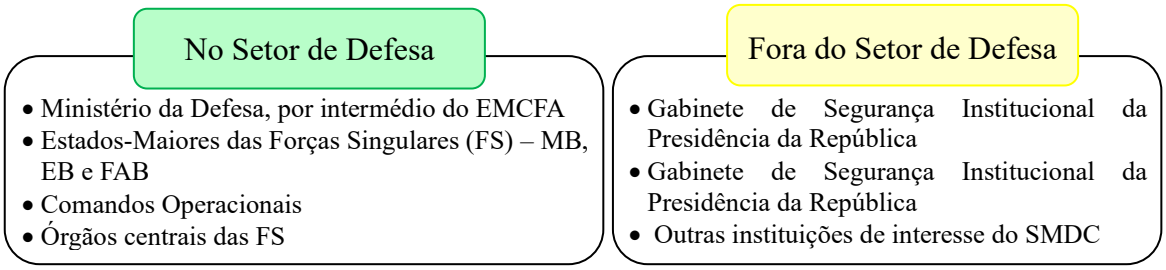


FIGURA 3 – Relações institucionais do órgão central do SMDC com as agências.
Fonte: O autor, com base na Portaria de criação do SMDC (BRASIL, 2020h).

Inserida nesse mundo amplamente conectado e no SMDC, a MB emprega, cada vez mais, sistemas de informação, interligando suas diversas Organizações Militares, com a finalidade de administrar o fluxo de informações geradas e distribuídas dentro da Força. Tais mecanismos computacionais permeiam, entre outras áreas, a de Ciência, Tecnologia e Inovação (CT&I) e de desenvolvimento de importantes programas estratégicos, como o Programa Nuclear da Marinha (PNM) e o Programa de Construção do Núcleo do Poder Naval, neste inserido o Programa de obtenção das Fragatas Classe Tamandaré (PCT). Logo, torna-se essencial que a MB disponha de mecanismos e medidas voltados à defesa cibernética da Força (nível estratégico), bem como para atuar na guerra cibernética (nível operacional e tático), em consonância com o MD e as doutrinas brasileiras.

3 A ESTRATÉGIA DE DEFESA CIBERNÉTICA DE ATORES PROTAGONISTAS NO CENÁRIO MUNDIAL

O uso da internet no mundo está crescendo cada vez mais, por meio de incrementos e melhorias nas mídias sociais, utilização por setores privados e de redes de empresas estatais, proporcionando um acesso, cada vez maior, a novos conhecimentos, negócios e serviços. O incremento na dependência das interconexões em rede para a operação das infraesruturas nacionais críticas e os ataques cibernéticos introduziram uma complexa realidade aos Estados, impondo-lhes a inclusão do tema segurança cibernética em suas agendas de segurança nacional. Este capítulo abordará três importantes atores do cenário mundial – EUA, OTAN e China – no tocante ao espaço cibernético.

3.1 Estados Unidos da América

De a cordo com o Departamento de Defesa dos EUA (Departament of Defense - DoD), "a prosperidade, liberdade e segurança americanas dependem do acesso aberto e confiável às informações" (EUA, 2018a, p.1, tradução nossa). Afirma, também, que computadores e tecnologias de rede são a base para a superioridade militar dos EUA, ao permitir que uma Força, singular ou conjunta, obtenha vantagem de informação, exerça comando e controle global, além de ataque a longa distância. Como paradoxo, a era digital cria desafios para o Estado, pois as características da internet que se busca manter – aberta, transnacional e descentralizada – trazem significativas vulnerabilidades.

Nesse universo, os EUA veem a República Popular da China (China) e a Federação Russa (Rússia) como grandes competidores no ciberespaço e, também, um risco estratégico de longo prazo para eles, bem como para seus aliados. Segundo o DoD americano, a China estaria minando a superoridade militar e a vitalidade econômica dos EUA ao exfiltrar informações confidenciais de instituições dos seus setores público e privado. Já a Rússia, teria usado operações de informação, por meio do espaço cibernético, para influenciar a população estadunidense e interferir em seus processos democráticos. Afirma, também, que outros atores, como a Coreia do Norte e o Irã, teriam empregado ações cibernéticas maliciosas, para ameaçarem os interesses dos EUA (EUA, 2018a). Diante do constante incremento global de atividade cibernética maliciosa associado à relação de dependência dos EUA com o ciberespaço, para quase todas as funções civis e militares, não dominar esta dimensão operacional torna-se um risco inaceitável para o país (EUA, 2018a).

Com base nessa assertiva, seu Departamento de Defesa age no espaço cibernético na busca pela preservação das vantagens militares dos EUA, assim como para a defesa dos interesses do Estado, focando, particularmente na China e na Rússia, por entender que estes podem representar ameaças estatégicas para a prosperidade e segurança do país (EUA, 2018a). Para tanto, o DoD adota ações estratégicas, tais como (EUA, 2018a):

– Conduz operações no ciberespaço para coletar dados de inteligência e prepara capacidades cibernéticas militares a serem empregadas em caso de crise ou conflito.

– Efetua a defesa proativa [31], interrompendo ou impedindo as atividades cibernéticas maliciosas em sua origem, incluindo aquelas que estejam abaixo do nível de conflito armado.

– Fortalece a segurança e a resiliência de redes e sistemas que contribuem para as vantagens militares atuais e futuras dos EUA.

– Prepara os guerreiros cibernéticos para, em tempo de guerra, atuar em conjunto com suas forças aéreas, terrestres, marítimas e espaciais. Visando à obtenção da vantagem militar, a Força Conjunta deverá ser capaz de empregar ações cibernéticas ofensivas que permitam a utilização do ciberespaço em toda a extensão do conflito.

Em suma, a Estratégia Cibernética dos EUA (2018a) mostra a visão de seu Departamento de Defesa para lidar com as ameaças cibernéticas e para implementar as prioridades da Estratégia de Segurança Nacional e da Estratégia de Defesa Nacional para o ciberespaço. Além disso, destaca que

> os Estados Unidos não podem se permitir à passividade: nossos valores, competitividade econômica e vantagem militar estão expostos a ameaças que se tornam mais perigosas a cada dia. Devemos defender assertivamente nossos interesses no ciberespaço em tempo de paz e garantir a prontidão de nossos operadores do ciberespaço para apoiar a Força Conjunta em crises e conflitos (EUA, 2018a, p. 2, tradução nossa).

No campo militar, tal importância é reforçada pelo Comando Cibernético dos EUA (USCYBERCOM)[32] ao afirmar que a obtenção da superioridade nos domínios aéreo, terrestre, marítimo e espacial, em grande parte, depende da superioridade no ciberespaço (EUA, 2018).

[31] Identifica possíveis atividades hostis e toma a iniciativa das ações, antecipadamente, ou seja, antes de a ameaça ser concretizada.

[32] Elevado a comando combatente unificado em 2017 (EUA, 2017), está no mesmo nível dos comandos regionais – Comando para a África (USAFRICOM), Comando Central (USCENTCOM), Comando Europeu (USEUCOM), Comando Indo-Pacífico (USINDOPACOM), Comando Norte (USNORTHCOM), Comando Sul (USSOUTHCOM) – e dos demais comandos combatentes unificados: Comando Espacial (USSPACECOM), Comando de Operações Especiais (USSOCOM), Comando Estratégico (USSTRATCOM) e Comando de Transporte (USTRANSCOM).

À vista disso, de forma contínua, o USCYBERCOM atua no ciberespaço, de modo a conter os ataques antes que eles transponham suas defesas cibernéticas ou prejudiquem suas forças militares. Por meio de contrainformação, busca influenciar o comportamento dos oponentes e introduzir incertezas em seus pressupostos. Para isso, as ações de sua força cibernética têm que ser ágeis, integradas e contínuas em âmbito nacional (EUA, 2018).

Segundo esse Comando, é fundamental que as políticas, doutrinas e os processos acompanhem a velocidade da evolução tecnológica e a crescente sofisticação dos ataques nesse domínio operacional, para a manutenção de uma vantagem julgada essencial para os EUA (EUA, 2018).

Em síntese, os EUA objetivam a superioridade no espaço cibernético, para terem liberdade de ação nesse domínio, proporcionando-lhes a iniciativa tática e operacional no ciberespaço e culminando em uma vantagem estratégica sobre os adversários. Tais esforços intentam, também, que atores adversários compreendam que as atividades hostis no ciberespaço contra os EUA não são vantajosas, o que contribui para a dissuasão (EUA, 2018).

3.1.1 USCYBERCOM

O Comando Cibernético dos EUA (USCYBERCOM), um comando opercional conjunto permanente, conforme representado na FIG. 4, sincroniza os esforços cibernéticos das forças militares: United States Army Cyber Command, o Fleet Cyber Command/Tenth Fleet, o Sixteenth Air Force (Air Forces Cyber) e o Marine Corps Forces Cyberspace Command.

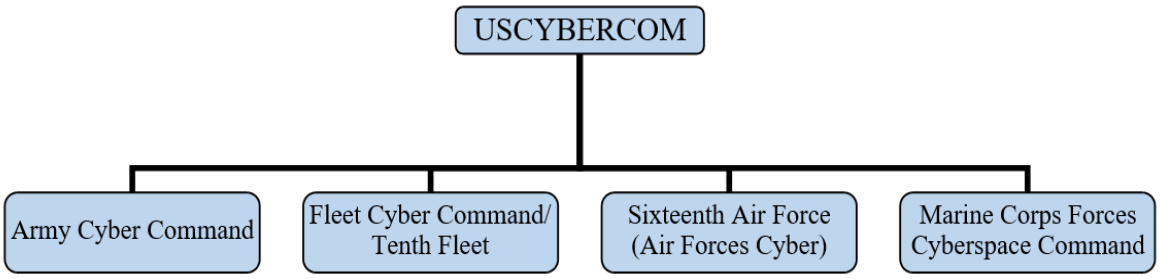


FIGURA 4 – Estrutura organizacional simplificada do U.S. Cyber Command.
Fonte: O autor, com base no sítio do U.S. Cyber Command (Disponível em: <https://www.cybercom.mil>. Acesso em: 11 jun. 2021).

O USCYBERCOM, criado em 2010 (EUA, 2021b), tem por missão conduzir e coordenar o planejamento e as operações no ciberespaço no intuito de defender e promover os interesses do EUA, em colaboração com seu parceiros nacionais e internacionais (EUA, 2021a).

O Comando, em sua essência, atua em três eixos: defesa da rede de informações do Departamento de Defesa dos EUA (DoD); apoio a um Comando de Força, singular ou conjunto,

na execução de suas tarefas em todo o mundo; e desenvolvimento da capacidade de a nação estadunidense responder e resistir a possíveis ataques cibernéticos (EUA, 2018).

Nesse contexto, o USCYBERCOM fortalece a capacidade cibernética do DoD, planeja e integra as atividades de segurança e defesa cibernética dos EUA, além de projetar a estrutura necessária para tal fim. Na execução de sua missão, ele trabalha em estreita colaboração com parceiros interinstitucionais e internacionais (EUA, 2018). Assim, prepara-se para uma possível condução de ações cibernéticas, em sincronia com as atividades desenvolvidas nos demais domínios operacionais, com a finalidade de garantir a liberdade de ação dos EUA e seus aliados no ciberespaço e negá-la aos oponentes.

3.1.1.1 U.S. Army Cyber Command (ARCYBER)

O Comando Cibernético do Exército dos EUA (ARCYBER) conduz, de forma integrada, operações de informação e ações de guerra cibernética e de guerra eletrônica, para assegurar a liberdade de ação da forças amigas no ciberespaço e, por meio dele, nos demais domínios, bem como no ambiente informacional e negá-las aos seus adversários (EUA, 2021).

3.1.1.2 Fleet Cyber Command (FLTCYBER) / Tenth Fleet

O Comando Cibernético da Esquadra dos EUA (FLTCYBER) é o elemento operacional da Marinha junto ao USCYBERCOM e responsável pelas ações ofensivas e defensivas no ciberespaço da Força, tendo como seu braço operativo, para esse fim, a Décima Esquadra (*U.S. TENTH Fleet*), que passa a exercer o controle operacional sobre as forças atribuídas ao FLTCYBER e atua de modo a garantir os efeitos táticos e operacionais desejados no ciberespaço e por meio desse domínio, bem como no espaço e no espectro eletromagnético empregado pela Marinha dos EUA (EUA, 2021d).

Integrando o FLTCYBER, entre outros elementos, encontram-se o Comando Naval de Guerra em Rede (*Naval Network Warfare Command* - NETWARCOM), os Comandos Navais de Operação de Informação (*Naval Information Operation Commands* - NIOC) e o Comando de Operações de Defesa Cibernética da Marinha (*Navy Cyber Defense Operations Command* - NCDOC) (EUA, 2021c). Este último, fazendo jus ao seu lema “Guerreiros cibernéticos. Sempre vigilantes”, é responsável por executar as operações de defesa cibernética, de modo a possibilitar uma projeção de poder de forma global, por meio de defesa proativa da rede da Marinha dos EUA (EUA, 2021c).

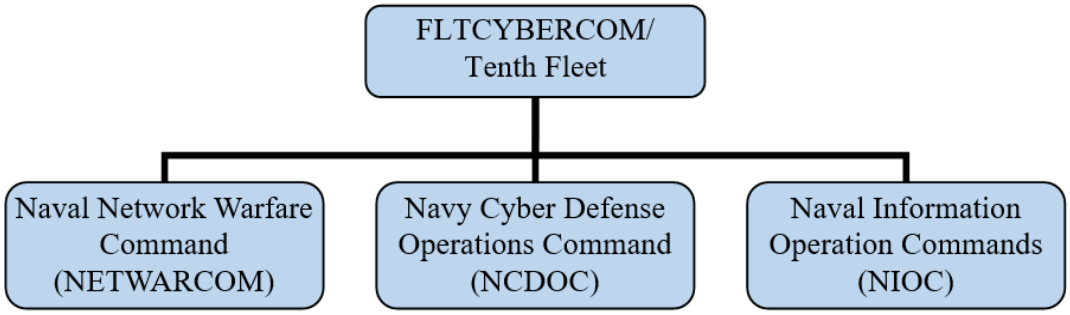


FIGURA 5 – Estrutura organizacional simplificada do FLTCYBER.
Fonte: O autor, com base no sítio do U.S Fleet Cyber Command / U.S. Tenth Fleet (Disponível em: <https://www.fcc.navy.mil>. Acesso em: 11 jun. 2021).

Como reconhecimento à "weaponização[33]" do espaço cibernético, a FLTCYBER / Tenth Fleet divulgou, em julho de 2020, o seu plano estratégico para os próximos cinco anos – 2020 a 2025 – que abarca, entre outras prioridades, o incremento de suas capacidades para atuar nesse domínio operacional, seja defensiva ou ofensivamente (EUA, 2020a).

Segundo o Vice-Almirante *Timothy White*, comandante da FLTCYBER / Tenth Fleet, as ações preliminares decorrentes do grande conflito de poder no século 21, especialmente aquelas que afetem o domínio marítimo, serão lançadas nos domínios cibernético ou espacial ou no espectro eletromagnético. E acrescenta que, se Marinha dos EUA deseja vencer os futuros combates, suas redes devem ser capazes de resistir às ações cibernéticas inimigas – exploração e ataque – assim como superarem os danos sofridos. Para isso, seu pessoal deve estar capacitado para se opor a essas incursões (EUA, 2020a).

Adicionalmente, o Vice-Almirante *Timothy White* afirma que o espaço cibernético já circunscreve um *continuum* de ações, por conta de competições e conflitos entre os diversos atores globais, entre eles Estados, e que, mesmo em tempo de paz, as redes da Marinha americana se encontram sob constantes ataques e sofrem tentativas de exploração de dados e informações (EUA, 2020a).

A FLTCYBER / Tenth Fleet demonstra preocupação com as tecnologias emergentes[34], pois considera que elas moldarão o futuro das guerras. Assim, o desenvolvimento de tais tecnologias deve ser acompanhado, para que a FLTCYBER / Tenth Fleet passe a empregá-las, assim que possível, conjugando-as a atualizações de técnicas e procedimentos utilizados no espaço cibernético, a fim de manter o oponente em situação tática desfavorável (EUA, 2020a).

[33] Emprego como arma.
[34] Exemplos de tecnologias que estão surgindo: inteligência artificial, aprendizado de máquina (*machine learning*), computação quântica e internet móvel de 5ª geração (5G) e 6ª geração (6G) (EUA, 2020a).

3.1.1.3 Sixteenth Air Force (Air Forces Cyber - AFCYBER)

A Força Aérea Cibernética (AFCYBER) é voltada para a guerra de informação, integrando capacidades de inteligência, guerra cibernética, guerra eletrônica, operações de informação e vigilância e reconhecimento de múltiplas fontes, visando a assegurar a pronta resposta da Força Aérea, na paz ou em um conflito, em nível operacional e tático (EUA, 2020b).

3.1.1.4 Marine Corps Forces Cyberspace Command (MARFORCYBER)

O Comando do Ciberespaço das Forças do Corpo de Fuzileiros Navais dos EUA, como componente do USCYBERCOM, atua em prol dos intereses do Corpo de Fuzileiros Navais no domínio cibernético, de modo a permitir sua liberdade de ação em todos os domínios de combate e negar o mesmo às forças adversárias (EUA, 2021e).

Ao analisar o Comando Cibernético dos EUA (USCYBERCOM), constata-se que ele está estruturado, de modo a integrar as operações cibernéticas, fortalecendo as capacidades cibernéticas do DoD. Ao empregar o ARCYBER, AFCYBER , FLTCYBER e o MARFORCYBER reforça a capacidade cibernética do DoD, conferindo grande autonomia a cada um deles em seus ambientes de guerra.

A abordagem estadunidense no 5º domínio operacional não se limita a instituição de um Comando Operacional Conjunto voltado ao ciberespaço, o USCYBERCOM. Cada Força possui seu Comando Cibernético, os quais contribuem para a missão do USCYBERCOM, tendo cada uma delas a sua própria missão, de modo a permitir a liberdade de ação em todos os domínios de combate e negá-la às forças oponentes.

3.2 Organização do Tratado do Atlântico Norte

Apesar dos esforços, as ameaças cibernéticas têm evoluído mais rapidamente do que as contramedidas dos Estados. Diante do cenário em que os ciberataques ficam mais comuns, sofisticados e prejudiciais, a defesa cibernética tornou-se parte da tarefa central – defesa coletiva – da Organização do Tratado do Atlântico Norte (OTAN) (OTAN, 2018).

Com foco na proteção de suas próprias redes e no aumento da resiliência no ciberespaço da Aliança[35], a OTAN afirma que o direito internacional se aplica ao espaço

[35] O mesmo que OTAN.

cibernético (OTAN, 2021) e persegue a promulgação do compromisso de defesa cibernética[36] pelos Estados membros (BRENT, 2019).

Desde que a Aliança reconheceu o ciberespaço como um domínio operacional, em 2016, a OTAN atingiu alguns marcos que demonstram a sua evolução para se contrapor aos desafios impostos por esse novo domínio, que impactam na segurança e na defesa dos Estados membros.

Nessa trajetória, em fevereiro de 2017, a atualização do plano de ação de defesa cibernética foi aprovada, assim como o planejamento para a implementação do ciberespaço como um domínio operacional. Tais ações incrementaram as relações entre os Estados membros, propiciando o desenvolvimento de capacidades e o compartilhamento de informações. Em dezembro do mesmo ano, a União Europeia (EU) e a OTAN concordaram em intensificar a cooperação entre as duas organizações em diversas áreas, entre elas, a segurança e a defesa cibernética (OTAN, 2021).

Em junho de 2018, a visão estratégica sobre o ciberespaço como um domínio operacional foi formalmente aprovada pelos países membros (BRENT, 2019), o que permite o desenvolvimento contínuo deste domínio pela Aliança, ou seja, possibilita desenvolver a política, as capacidades e doutrinas, assim como planejar e executar suas tarefas associadas ao espaço cibernético.

Nesse contexto, ainda em 2018, na Cúpula de Bruxelas, na Bélgica, a OTAN decidiu criar o Centro de Operações do Ciberespaço[37] para fortalecer a sua estrutura de comando, proporcionando a consciência situacional e a coordenação de suas atividades no espaço cibernético. Durante a Cúpula, foi acordado, também que a OTAN pode recorrer às capacidades cibernéticas dos Estados para as suas missões e operações (OTAN, 2021).

Em janeiro de 2020, foi publicada a primeira doutrina de operações cibernéticas da OTAN[38], visando, especialmente, a orientar comandantes, estados-maiores e forças da OTAN na condução de uma operação cibernética combinada, além de fornecer orientação para uma coalizão entre Estados membros, parceiros, estados não pertencentes à Aliança e outras organizações (OTAN, 2020a).

Para a sua defesa no ciberespaço, a OTAN conta com a seguinte estrutura (OTAN, 2020):

---

[36] *Cyber Defence Pladge*. Documento aprovado na cúpula da OTAN, que assevera que os aliados garantirão que a Aliança acompanhe a evolução do cenário de ameaças cibernéticas (BRENT, 2019).
[37] *Cyberspace Operations Centre,* instalado na cidade de Mons, na Bélgica.
[38] Allied Joint Publication (AJP-3.20): Allied Joint Doctrine for Cyberspace Operations.

– NATO *Computer Incident Response Capability* (NCIRC)[39] (Capacidade de Resposta a Incidentes de Segurança da Informação da OTAN), que protege as redes da OTAN por meio de ininterrupto suporte de defesa cibernética. Lida com os incidentes de rede e fornece, à OTAN e aliados, análise atualizada dos desafios cibernéticos a serem enfrentados. Como componente da Agência de Comunicações e Informação da OTAN, o NCIRC apoia as operações da OTAN, conectando seus sistemas de informação e comunicação e defendendo suas redes.

– NATO *Cyberspace Operations Centre* (CyOC) (Centro de Operações do Ciberespaço da OTAN), em fase de implementação, para reforçar a defesa cibernética da OTAN. O CyOC estará totalmente operacional em 2023 e apoiará os comandantes militares, proporcionando a eles consciência situacional para as operações da Aliança, bem como coordenará as ações da OTAN no ciberespaço, para promover maior resiliência aos ataques cibernéticos e garantir a liberdade de atuação neste domínio durante as operações.

– NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE)[40] (Centro de Excelência de Defesa Cibernética Cooperativa da OTAN), que fornece conhecimentos sobre defesa cibernética para a OTAN e estrutura exercícios cibernéticos, envolvendo os países membros e parceiros.

– NATO *School*[41], que conduz a educação associada à defesa cibernética, para apoiar a política, a estratégia, os procedimentos e as operações da OTAN.

– NATO *Communications and Information Academy*[42], que proporciona a formação da força de trabalho para a defesa cibernética da OTAN.

– NATO *Defence College*[43], que fomenta o pensamento estratégico a respeito de assuntos político-militares, entre eles as questões de defesa cibernética.

Com essa estrutura e mantendo o entendimento de que a defesa cibernética é parte da tarefa central da OTAN (ela está inserida em seu conceito de defesa coletiva), a Aliança, por meio da declaração do Conselho do Atlântico Norte sobre atividades cibernéticas maliciosas, de junho de 2020, mostra-se determinada a empregar todo a sua capacidade, incluída a

[39] Instalada no *Supreme Headquarters Allied Powers Europe* (SHAPE), na cidade de Mons, na Bélgica.
[40] Instalado em Tallinn, capital da Estônia, é um centro de pesquisa e treinamento em defesa cibernética credenciado pela OTAN. O Centro conta com pessoal e financiamento da Áustria, Bélgica, Bulgária, Canadá, Croácia, República Tcheca, Dinamarca, Estônia, Finlândia, França, Alemanha, Grécia, Hungria, Irlanda, Itália, Japão, Letônia, Lituânia, Luxemburgo, Montenegro, Holanda, Noruega, Polônia, Portugal, Romênia, Eslováquia, Eslovênia, Coreia do Sul, Espanha, Suécia, Suíça, Turquia, Reino Unido e Estados Unidos (CCDCOE, 2021).
[41] Instalada em Oberammergau, Alemanha.
[42] Com sede em Oeiras, Portugal.
[43] Em Roma, Itália.

cibernética, para se contrapor às ameaças inerentes ao ciberespaço. Para tanto, ela permanecerá, moldando-se ao cenário evolutivo de ameaças cibernéticas, empenhando-se para a proteção das infraestruturas críticas nacionais, ao desenvolvimento da defesa cibernética dos Estados membros e suas resiliências e para elevar os custos de um ataque cibernético praticado por atores estatais e não estatais, incluindo aqueles patrocinados por Estado (OTAN, 2020b). No entanto, para isso, torna-se fundamental a implementação do compromisso de defesa cibernética da OTAN.

Inserido no conceito de defesa coletiva no ciberespaço, anualmente é organizado pelo CCDCOE da OTAN exercício cibernético internacional intitulado *Locked Shields*, que simula um cenário de atuação em apoio a Estado fictício, visando à restauração de sistemas atacados, tais como abastecimento de água e defesa aérea. Adicionalmente, são apresentados incidentes cibernéticos (hipotéticos) para a avaliação do grau de maturidade dos países envolvidos em relação à segurança cibernética e à proteção de dados (BRASIL, 2021b).

O *Locked Shields* 2021 envolveu 23 Estados, reunindo mais de dois mil especialistas da área. E, segundo o Chefe de exercícios cibernéticos da CCDCOE, Carry Kangur, o exercício atingiu o mais alto nível de complexidade organizacional desde a sua idealização, pois foi realizado de forma remota em sua maior parte (BRASIL, 2021b). Considerado o mais complexo exercício nesse domínio, ele é uma excelente oportunidade para os especialistas dos países testarem suas habilidades e capacidades em um ambiente seguro, ao confrontarem oponentes altamente qualificados (BRASIL, 2021b; ATECH, 2021). É fato, portanto, que a OTAN, dentro do conceito de defesa coletiva, busca desenvolver uma compreensão cristalina a respeito da guerra cibernética em termos defensivos e ofensivos.

Nessa senda, a obtenção de melhores resultados, ao se lidar com as ameaças no espaço cibernético, decorre da conjugação coordenada de esforços dos Estados membros, de modo transparente, interdependente e colaborativo. Dessa forma, a ela cabe garantir a própria segurança cibernética e contribuir para a defesa cibernética da Aliança.

3.3 República Popular da China

Em relação à República Popular da China (RPC, China), cabe salientar que a limitada transparência do Estado chinês, imposta por seu regime político, leva à escassez de informações, tornando–se necessária a utilização de fontes secundárias, especialmente, sob a ótica ocidental, para a obtenção de informações sobre a estratégia e a estrutura cibernética da RPC.

Com uma geopolítica baseada no sinocentrismo[44], a China tornou-se a segunda potência mundial. A competição entre os EUA, um Estado com um poder já estabelecido, e a RPC, de poder em ascernção, influencia hoje, em grande parte, a geopolítica mundial.

Segundo o DoD dos EUA (EUA, 2020), a China manifesta publicamente que o ciberespaço é um domínio crítico para a segurança nacional e procura acelerar o desenvolvimento de suas forças cibernéticas. Nesse sentido, o constante aperfeiçoamento de capacidades de guerra cibernética é uma meta do Exército de Libertação Popular (ELP), por entender que a operação de informação (OpInfo) – aí inclusas as guerras cibernética, eletrônica e psicológica – é fundamental para a obtenção da superioridade informacional e um meio eficaz para combater um oponente mais forte (EUA, 2020).

Para isso, no contexto cibernético, o ELP, consoante a orientação do presidente chinês, Xi Jinping, tem criado uma força altamente informatizada, capaz de exercer o domínio do espaço cibernético, a fim de ampliar a segurança do Estado e defender seus interesses de desenvolvimento. Ademais, de acordo com o DoD, a RPC apresenta uma enérgica atividade de espionagem cibernética, o que representa uma ameça, pois é capaz de conduzir ataque cibernétco a sistemas militares e infraestruturas críticas de um Estado (EUA, 2020).

Com o objetivo de desevolver cada vez mais sua capacidade militar, o ELP incorpora sistemas de informação para emprego em operações militares, em um conceito por ele nominado guerra informatizada[45], para que suas forças realizem suas missões com maior eficácia (EUA, 2020). Tal prática justifica-se, visto que o ELP entende que é fundamental construir fortes capacidades cibernéticas para proteger as redes chinesas, além de defender a ideia de conquista da superioridade do ciberespaço, ao empregar ações cibernéticas ofensivas,

[44] Ideologia de que a China é o centro cultural, político ou econômico do mundo. Pensamento filosófico clássico chinês que considerava que no mundo existia um único centro de poder – o império chinês.

[45] De a cordo com o Relatório Anual para o Congresso 2020, os militares chineses descrevem a guerra informatizada como o emprego de TI para criar um sistema de sistemas operacional que permitiria o ELP adquirir, transmitir, processar e utilizar informações para conduzir as operações militares em todos os domínios operacionais durante um conflito (EUA, 2020).

que impeçam ou degradem a capacidade de um adversário para conduzir operações militares contra a China (EUA, 2020).

Para a RPC as operações cibernéticas permitem que o Estado gerencie a escalada de um conflito, pois os ataques cibernéticos representam uma deterrência de baixo custo. De acordo com o DoD, o ELP considera a capacidede cibernética como um dos pilares da estratégia de dissuasão chinesa, a lado da nuclear e da espacial, empregando seus recursos de guerra cibernética em prol das atividades de inteligência e para ataques cibernéticos (EUA, 2020). No entanto, as capacidades cibernéticas da China e as competências de seus guereiros cibernéticos são inferiores às dos EUA. Assim sendo, ela empenha-se para aperfeiçoar seus treinamentos e alavancar a inovação doméstica no campo cibernético, para superar os EUA em operações cibernéticas (EUA, 2020).

O entendimento apresentado pelo DoD no Relatório Anual para o Congresso 2020, a respeito do posicionamento chinês quanto ao ciberespaço, está alinhado com o ambicioso projeto chinês, divulgado em 2016 e intitulado "Esboço da Estratégia Nacional de Desenvolvimento de Tecnologia da Informação" que, com metas audaciosas, segundo Zhao e Heatley (2016), permitirá que, eventualmente, a China supere líderes globais em tecnologia, como Estados Unidos e Alemanha nesta década (2020 a 2029). Até 2025, por exemplo, a China tem como meta conceber uma rede de comunicação móvel capaz de competir com os países mais avançados industrialmente. Seu intuito é ser um país avançado tecnologicamente, com uma indústria proeminente e um espaço cibernético habilmente empregado e impenetrável (ZHAO; HEATLEY, 2016).

Na área militar, segundo Jinghua (2019)[46], as discussões acadêmicas sobre guerra cibernética deram-se na China, na década de 1990, quando ainda era denominada guerra de informação. As vantagens que os militares dos EUA obtiveram na Guerra do Golfo (1991) e, ulteriormente, nas operações em Kosovo (1999), no Afeganistão (2001) e no Iraque (2003), ao aplicarem novas tecnologias, fizeram com que a China entendesse a importância da tecnologia da informação (TI) na condução da guerra. Diante dessa nova percepção, em 1993, os chineses reorientaram sua estratégia militar, estabelecendo como objetivo principal do preparo para o conflito militar (*preparations for military struggle* - PMS) "winning local wars in conditions of modern technology, particularly high technology"[47]. Em 2004, o PMS voltou-se para "winning

[46] Lyu Jinghua - coronel da reserva do ELP - foi um professor visitante da *Carnegie's Cyber Policy Initiative,* da organização *Carnegie Endowment for International Peace*. Sua pesquisa se concentra, essencialmente, nas relações de defesa EUA-China, com ênfase na segurança cibernética.

[47] Vencer guerras locais em condições de tecnologia moderna, particularmente de alta tecnologia (tradução do autor).

local wars under conditions of informationization"[48], dando destaque à aplicação da tecnologia da informação (TI) nas operações militares (FRAVEL, 2015).

Apesar de os militares chineses entenderem que o emprego da TI eleva a capacidade de combate de uma força armada, segundo Jinghua (2019), somente em 2013, eles abordaram abertamente a guerra cibernética sob uma visão holística na *The Science of Military Strategy 2013*, um estudo da Academia de Ciências Militares da China, qualificando o ciberespaço como um novo e indispensável domínio operacional a ser empregado nos conflitos militares. Por conseguinte, a China ratifica o entendimento da importância do espaço cibernético ao inserir, em sua Estratégia Militar de 2015, como ponto principal do PMS "winning informationized local wars"[49] e ao defini-lo como a base para o desenvolvimento econômico e social do Estado e um domínio vital para a segurança nacional (CHINA, 2015).

Pode-se observar que a postura da China a respeito da governança e emprego do espaço cibernético decorre das mudanças nas abordagens e práticas da guerra cibernética de outros países. O destaque dado pelo governo chinês sobre a guerra cibernética é expresso em sua estratégia militar, modificada, de modo a promover a segurança nacional, com base nas atividades de forças militares estrangeiras e na situação interna chinesa.

Por outro lado, de acordo com a estratégia Militar da China (CHINA, 2015), o pensamento estratégico militar do Partido Comunista da China tem como ideia central a estratégia de defesa ativa[50], que abarca um conjunto de conceitos aderidos por suas Forças Armadas, entre eles a adoção da postura de não atacar a menos que sejam atacados e que, de decerto, contra-atracarão, se forem atacados. Orientado por tais preceitos, o objetivo precípuo da RPC é ser resiliente no ciberespaço, ou seja, aprimorar suas capacidades de defesa cibernética para suportar e contra-atacar, após ser alvo de um ataque cibernético.

No intuito de conter as suas vulnerabilidades, entre elas as advindas da democracia no ciberespaço, a China criou, em 2015, a Força de Apoio Estratégico (*Strategic Support Force* -SSF) do ELP, uma nova organização concebida para integrar as capacidades de guerra espacial, cibernética, eletrônica e psicológica, nas operações do ELP (ZHAO; HEATLEY, 2016; POLLPETER; CHASE; HEGINBOTHAM, 2017).

---

[48] Vencer guerras locais sob as condições de informatização (tradução do autor).
[49] Vencer guerras locais informatizadas (tradução do autor).
[50] Defesa ativa é um conjunto de conceitos estratégicos que se resumem a: adesão à unidade de defesa estratégica e ofensiva operacional e tática; adesão aos princípios de defesa, autodefesa e ataque pós-vazio; e adesão à postura de que "Não atacaremos a menos que sejamos atacados, mas certamente contra-atacaremos se atacados" (CHINA, 2015, p. 10).

Como afirmam Kania e Costello (2018), a criação da SFF tem por finalidade o domínio do espaço, do ciberespaço e do espectro eletromagnético de interesse chinês, ou seja, a sua concepção está voltada para a guerra do futuro, na qual o ELP visa a capacidade de projetar poder muito além de suas fronteiras territoriais.

Nesse contexto, a SSF tornou-se uma das forças que compõem o ELP[51], reportando-se, diretamente, à Comissão Militar Central que é o órgão militar de mais alto nível de tomada de decisão na China, atualmente presidido por Xi Jinping (EUA, 2020).

Visão geral da Força de Apoio Estratégico do ELP.

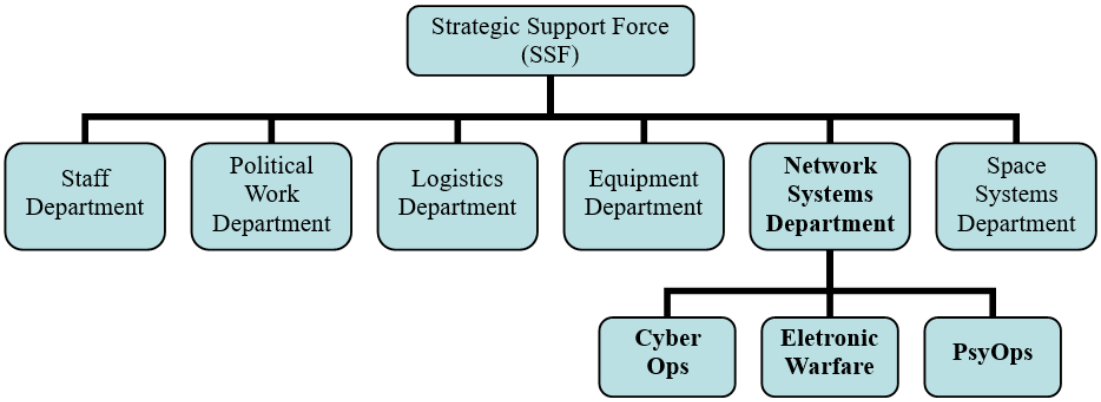
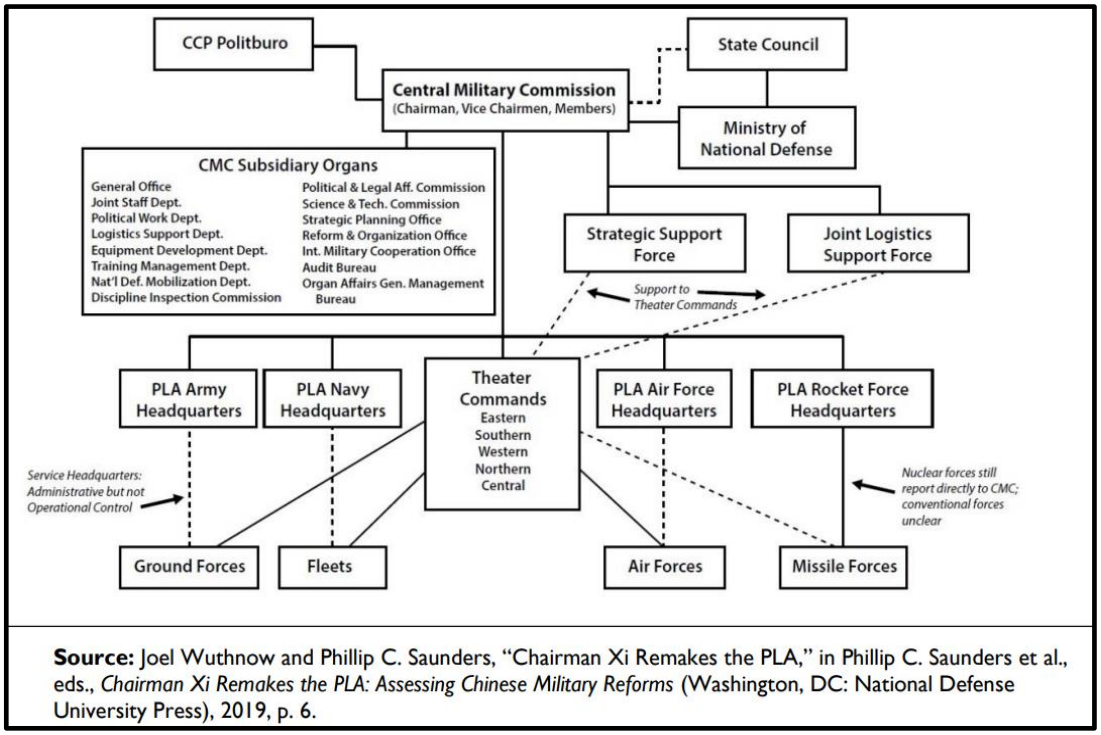


FIGURA 6 – Estrutura organizacional simplificada da *Strategic Support Force*.
Fonte: COSTELLO; McREYNOLDS, 2018, p. 11.

Subordinado à SSF, cabe ao Departamento de Sistemas de Rede (*Network Systems Department* - NSD), também chamado de força cibernética (COSTELLO; McREYNOLDS, 2018), a responsabilidade pela guerra cibernética em uma força conjunta (POLLPETER; CHASE; HEGINBOTHAM, 2017). Não obstante seu nome, o NSD é responsável pelas operações de informação (OpInfo) e, para isto, incorpora as unidades estratégicas voltadas para as OpInfo, entre elas, as relacionadas à guerra cibernética, guerra eletrônica e guerra psicológica (COSTELLO; McREYNOLDS, 2018).

[51] Forças que compõem o ELP: Exército, Marinha, Força Aérea, Força de Foguete, Força de Apoio Estratégico e Força de Apoio Logístico Conjunto (EUA, 2020).



Source: Joel Wuthnow and Phillip C. Saunders, "Chairman Xi Remakes the PLA," in Phillip C. Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms* (Washington, DC: National Defense University Press), 2019, p. 6.

FIGURA 7 – Estrutura Militar de Defesa da República Popular da China.
Fonte: CRS, 2021, p. 13.

De forma centralizada, o Departamento coordena as forças de exploração cibernética e de ataque cibernético, no âmbito estratégico e atua em apoio aos Comandos Regionais[52] e forças componentes, em nível operacional e tático (COSTELLO; McREYNOLDS, 2018).

FIGURA 8 – Comandos Regionais do Exército de Libertação Popular.
Fonte: CRS, 2021, p. 12.

[52] *Theater commands: Eastern, Southern, Western, Northern and Central.*

A criação da SFF em 2015 evidenciou a evolução do pensamento militar chinês a respeito da guerra do futuro (hoje presente), reconhecendo o importante papel que a guerra cibernética desempenha em prol de suas forças, assim como, as consequentes vulnerabilidades decorrentes da crescente dependêrncia de sistemas de informação.

Diferentemernte dos EUA, o modelo chinês concentra os componentes voltados à guerra cibernética em uma única Força – a *Strategic Support Force* – em vez de dispersá-los e integrá-los de forma conjunta, exigindo que a tomada de decisão e o controle das ações sejam efetuados a partir do ou próximo ao topo hierárquico do Estado, haja vista que esta Força reporta-se diretamente à Comissão Militar Central, cujo chefe é Xi Jinping, atual presidente e líder do Partido Comunista da China.

4 A GUERRA E A DEFESA CIBERNÉTICA NAS FORÇAS ARMADAS BRASILEIRAS

A guerra cibernética particulariza-se por sua assimetria, ou seja, um ataque cibernético realizado por ator com limitados recursos pode alcançar resultados expressivos e, pela grande dificuldade de rastrear a fonte do ataque, impossibilitando determinar o responsável pelos danos.

O Brasil manifesta preocupação com o uso do 5º domínio operacional – o ciberespaço – na Estratégia Nacional de Defesa (END) encaminhada ao Congresso Nacional. No que diz respeito à Marinha, a END ressalta a necessidade de a Força ter capacidade de operar, ofensiva e defensivamente, no ambiente cibernético (BRASIL, 2020, p. 47). Assim, possuir as habilidades necessárias à defesa cibernética, atuando nos três campos – ofensivo, defensivo e exploratório – de acordo com o estabelecido pelo Ministério da Defesa (BRASIL, 2014, p. 18), torna-se fundamental para o Poder Naval.

4.1 O Sistema Militar de Defesa Cibernética brasileiro

Como apontado no Capítulo 2, as FA brasileiras estão inseridas no Sistema Militar de Defesa Cibernética (SMDC) brasileiro. Esse sistema, recentemente criado (2020), em cumprimento à Política Cibernética de Defesa aprovada em 2012 (BRASIL, 2020h), encontra-se em fase de implementação.

Utilizando-se do conceito da Teoria Geral de Sistemas[53], em que um sistema envolve sempre as ideias de relação e organização de subsistemas, o SMDC é definido como

> um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses (BRASIL, 2020h, p.1).

Logo, o SMDC é concebido, de forma conjunta, tendo por objetivo assegurar o uso indelével do espaço cibernético pelas Forças Armadas, assim como impedir ou dificultar a sua utilização contra interesses da Defesa Nacional.

---

[53] Teoria Geral de Sistemas, formulada pelo biólogo alemão Ludwig Von Bertalanffy, estabelece que todo sistema deve constituir um todo harmônico e coerente, integrado por um conjunto de subsistemas interdependentes, que, dentro de um conceito de divisão do trabalho, realizam funções especializadas que se complementam e, de forma sinérgica, geram o produto do sistema (ARAÚJO; GOUVEIA, 2016).

Considerando que nenhum sistema é completo por si só, uma característica dos sistemas é a subsidiariedade, ou seja, cada um deles, envolto em uma circunscrição, é um subsidiário nos elementos que recebe ou fornece a outros sistemas. Tal característica encontra-se presente no SMDC, uma vez que, tendo como seu órgão central o ComDCiber, vale-se de estruturas de defesa cibernética das Forças Singulares, dos Comandos Operacionais ativados e de outras organizações de interesse do MD e interage com outros sistemas associados à Defesa Nacional, dos quais podemos destacar o Sistema Militar de Comando e Controle (SISMC^2), o Sistema de Inteligência de Defesa (SINDE), o Sistema de Defesa Aeroespacial Brasileiro (SISDABRA), o Sistema de Controle do Espaço Aéreo Brasileiro (SISCEAB), o Sistema de Mobilização Militar (SISMOMIL), o Sistema Nacional de Mobilização (SINAMOB) e o Sistema de Ciência, Tecnologia e Inovação de Interesse da Defesa Nacional (SisCTID). No futuro, dois grandes sistemas de sistemas figurarão nesse grupo, o Sistema de Gerenciamento da Amazônia Azul (SisGAAz) e o Sistema Integrado de Monitoramento de Fronteira (SISFRON).

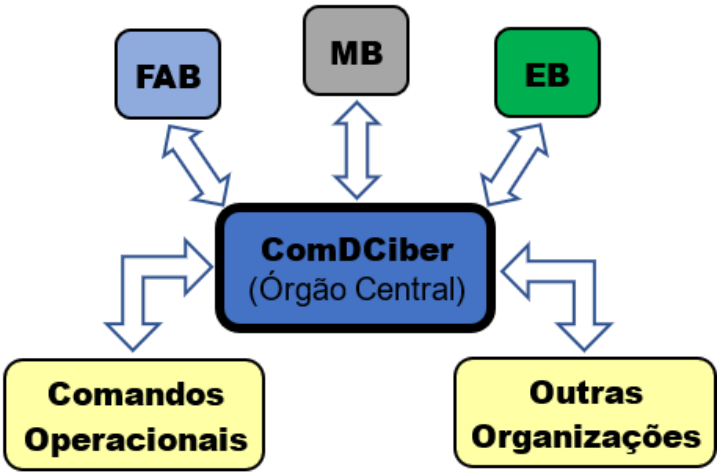


FIGURA 9 – Composição do SMDC.
Fonte: O autor, com base na Portaria de criação do SMDC (BRASIL, 2020h).

Dentro desse grande sistema, em nível estratégico, o ComDCiber interage com a MB e as demais FA, por meio de seus Estados-Maiores, para a obtenção e aplicação de capacidades de defesa cibernética, o tratamento de incidentes de rede e a realização de atividades de inteligência no ciberespaço (BRASIL, 2020h). Dessa forma, compete ao Estado-Maior da Armada (EMA), Estado-Maior do Exército (EME) e Estado-Maior da Aeronáutica (EMAER) formular e disseminar a doutrina de defesa cibernética da MB, do EB e da FAB, respectivamente, de modo a enunciar os conceitos e os princípios em que se baseiam a defesa cibernética em

cada Força. Para tanto, a defesa cibernética é tratada pela Subchefia de Logística (M-40), no EMA, 2º Subchefia – Informações e Defesa Cibernética –, no EME e 3º Subchefia, no EMAER.

Adicionalmente, seguindo as boas práticas[54] empregadas em todo o mundo para a segurança de rede, cada Força Singular (FS), sob a orientação do ComDCiber, por meio do Centro de Defesa Cibernética (CDCiber)[55], dispõe de um Centro de Tratamento de Incidentes de Rede (CTIR), cujas atribuições são exercidas pelo Centro de Tecnologia da Informação da Marinha (CTIM), na MB, Centro Integrado de Telemática do Exército (CITEx), no EB e Centro de Computação da Aeronáutica de Brasília (CCA-BR), na FAB. Nessa estrutura, o CDCiber troca informações com os CTIR de cada FS e emite, para elas (FS), alertas de incidentes recebidos de outros setores nacionais ou internacionais.

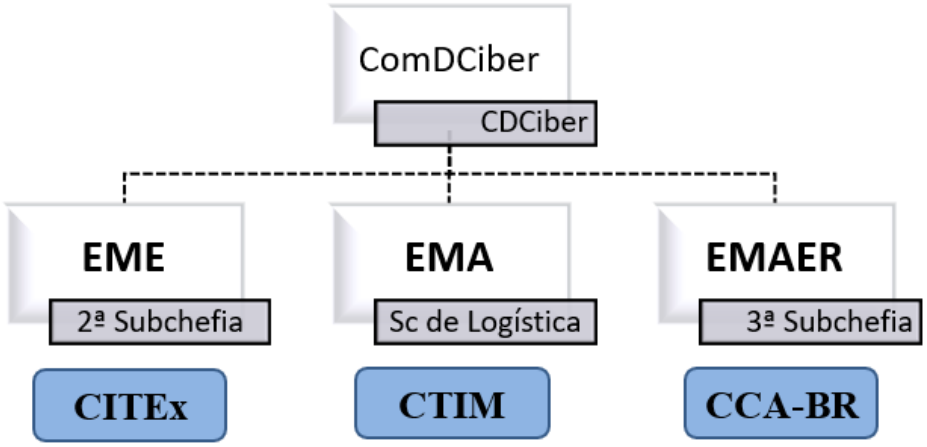


FIGURA 10 – SMDC: Organização das Forças Armadas, em nível estratégico, e respectivos CTIR.
Fonte: O autor, com base na Portaria de criação do SMDC (BRASIL, 2020h).

Para a capacitação do recurso humano nacional[56] demandado pelo setor cibernético, assim como para contribuir com as áreas de pesquisa, desenvolvimento, operação e gestão de defesa cibernética, o ComDCiber conta com a Escola Nacional de Defesa Cibernética (ENaDCiber)[57] (BRASIL, 2019a).

Considerando que a defesa cibernética depende, essencialmente, do talento humano, como cita o General Guido Amin Naves, ex-Comandante de Defesa Cibernética (BRASIL, 2019a), a ENaDCiber, como um braço acadêmico do ComDCiber, exerce um papel fundamental

[54] Boas práticas é o conjunto de processos, procedimentos, atividades e técnicas.
[55] É o braço operacional do ComDCiber para as ações de defesa cibernética e atividades de inteligência.
[56] Até o presente, a ENaDCiber formou apenas pessoal das FA, mas a ideia é que servidores civis de outros órgãos, que necessitam ter conhecimento para atuar na proteção de sistemas coorporativos, sejam capacitados por essa Escola.
[57] A ENaDCiber foi ativada em fevereiro de 2019. Ela funcionava como núcleo, criado em 2015, de acordo com a Portaria Normativa nº 2.777 do Ministério da Defesa, de 27 de outubro de 2014 e da Portaria nº 002 do Comandante do Exército, de 2 de janeiro de 2015.

na capacitação da força de trabalho para o setor.

Com intuito de elevar a maturidade no setor cibernético e a capacidade militar de defesa cibernética do país, o ComDCiber conduz, no âmbito do MD, a competição cibernética conhecida como "Mandabyte"[58] (BRASIL, 2020c) e participa de exercícios internacionais coordenando equipe composta por especialistas em cibernética das Forças Armadas e de agências[59] nacionais.

Nesse contexto, o país participou do exercício *Locked Shields* 2021, já mencionado no Capítulo 3, tendo sido o único representante da América Latina em um conceito de operações interagências. No evento, a equipe foi constituída por especialistas das três Forças e representantes de agências governamentais – Agência Nacional de Águas (ANA) e Agência Nacional de Telecomunicações (Anatel) (TECNOLOGIA & DEFESA, 2021) – e organizações ligadas à infraestrutura associada ao exercício – Atech Negócios em Tecnologias S/A[60] e Avibras Indústria Aeroespacial S/A (ATECH, 2021). Cada um deles tinha funções específicas nos problemas simulados, para produzir unidade de esforços em prol de um objetivo comum (BRASIL, 2021).

4.1.1 A guerra cibernética em três níveis

De maneira distinta ao apresentado no Capítulo 3, em que os atores estudados tratam as ações cibernéticas – proteção, exploração e ataque – sob uma única concepção, o conceito de guerra cibernética, no Brasil, como exposto no Capítulo 2, conceitua guerra ou defesa cibernética, de acordo com o nível de decisão em que o planejamento e a execução das ações cibernéticas se desenvolvem. Se o planejamento e as ações ocorrem no nível operacional ou tático, é denominado guerra cibernética (G Ciber). Se acontecem em nível estratégico, passa a ser titulado defesa cibernética.

Dessa forma, utilizando-se do conceito mais amplo para o emprego das ações cibernéticas, o ComDCiber, além de atuar como órgão central do SMDC, será o elo entre os níveis estratégico e operacional no que se refere à G Ciber, quando for ativada a estrutura militar de defesa (Etta Mi D).

---

[58] A competição tem como propósito desenvolver e difundir a cultura de segurança e defesa cibernética, aperfeiçoar militares das FA nas áreas de conhecimento cibernético e descobrir novos talentos na área cibernética (BRASIL, 2020c).

[59] Organização, instituição ou entidade governamental ou não, militar ou civil, nacional ou internacional, com estrutura e competência formalmente estabelecidas (BRASIL, 2017c).

[60] Empresa do grupo Embraer.

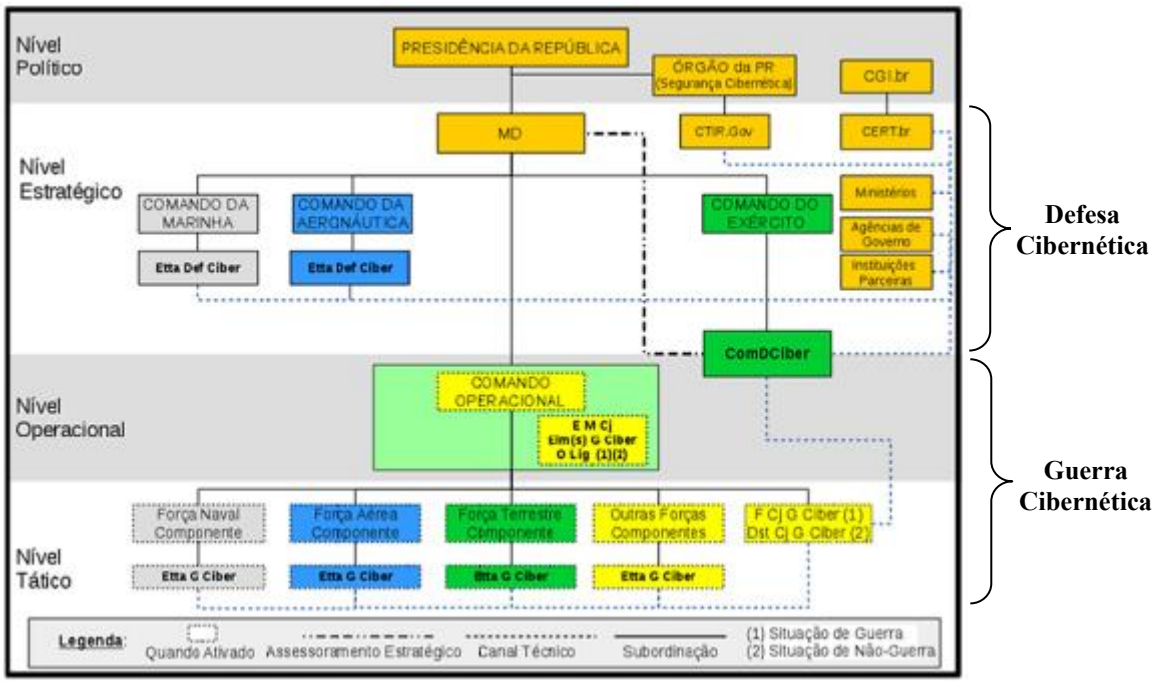


FIGURA 11 – Sistema Militar de Defesa Cibernética.
Fonte: BRASIL, 2017, cap. 3, p. 1.

Como pode-se observar na FIG. 11, a atuação do ComDCiber permeia os níveis estratégico, operacional e tático. Neste último nível, por meio de uma Força Conjunta de Guerra Cibernética (F Cj G Ciber) ou um Destacamento Conjunto de Guerra Cibernética (Dst Cj G Ciber) (BRASIL, 2017). Adicionalmente, cada uma das forças componentes contará com o apoio de uma estrutura de guerra cibernética (Etta G Ciber) que operará em coordenação com a F Cj G Ciber ou Dst Cj G Ciber (BRASIL, 2017). Portanto, para atender ao estabelecido no SMDC, cada FS deve manter uma Etta G Ciber capaz de apoiar suas respectivas Forças Navais, Terrestres e Aéreas, estejam elas operando de forma conjunta ou singular.

4.2 Guerra cibernética e defesa Cibernética no EB e na FAB

4.2.1 Exército Brasileiro

O Centro Integrado de Telemática do Exército (CITEx) e suas Organizações Militares (OM) diretamente subordinadas – os Centros de Telemática de Área (CTA), os Centros de Telemática (CT) e o Destacamento Técnico de Tecnologia da Informação (DTTI) – compõem o Sistema de Telemática do Exército (SisTEx) e têm como missão coordenar a infraestrutura lógica e física de TI dos sistemas de informação do EB, garantindo-lhe uma

elevada disponibilidade dos sistemas corporativos e do Sistema Estratégico de Comando e Controle do Exército (SEC²Ex) (BRASIL, 2021a). Logo, inseridas no SisTEx, compete àquelas OM a proteção cibernética no âmbito do EB, ao se pensar em defesa cibernética.

Nos níveis operacional e tático, o EB lida com a G Ciber empregando um grande sistema denominado Sistema de Guerra Cibernética do Exército (SGCEx)[61], para executar as ações de guerra cibernética e assegurar a liberdade de ação no espaço cibernético, ou seja, garantir o efetivo emprego desse domínio pelo EB, assim como negar ou obstaculizar a sua utilização pelo oponente. Dentro desse conceito, o SGCEx visa à proteção cibernética do sistema de comando e controle do EB, para atuar em rede com segurança, assim como objetiva à coordenação e a integração da proteção das infraestruturas críticas da informação[62] sob a sua responsabilidade (BRASIL, 2017).

A Etta G Ciber, que atuará em proveito da Força Terrestre (F Ter), será composta, em princípio, por subestruturas formadas por elementos do 1º Batalhão de Guerra Eletrônica (BGE), Batalhão de Comunicações (B Com), Batalhão de Comunicações e Guerra Eletrônica (B Com GE), Batalhão de Inteligência Militar (BIM), da Companhia de Comando e Controle (Cia C^2) e das Companhias de Comunicações (Cia Com), cada qual com sua atribuição no que tange ao espaço cibernético (BRASIL, 2017).

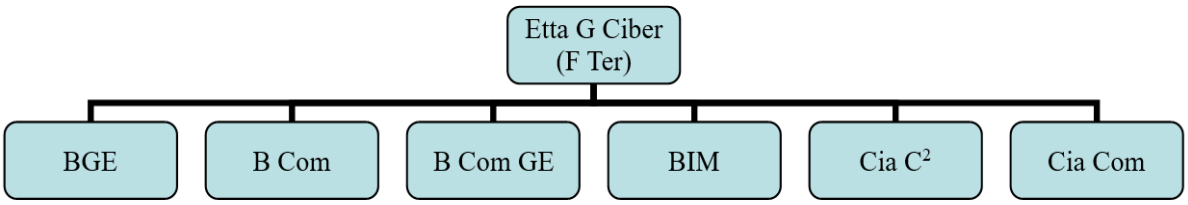


FIGURA 12 – Estrutura de Guerra Cibernética em apoio à Força Terrestre.
Fonte: BRASIL, 2017.

Essa estrutura poderá variar de acordo com a missão da FTer.

Nesse contexto, entre os tipos de ações cibernéticas – ataque cibernético, proteção cibernética e exploração cibernética –, competirá, exclusivamente, ao BGE realizar ataques. Este Batalhão, o B Com GE e o BIM serão responsáveis pela exploração cibernética. A proteção, em maior ou menor amplitude, caberá a todas as subestruturas.

---

[61] Doutrina, instalações, procedimentos, serviços e pessoal fundamentais para efetuar as ações de guerra cibernética (BRASIL, 2017).
[62] "Subconjunto dos ativos de informação que afeta diretamente a consecução e a continuidade da missão do estado e a segurança da sociedade" (BRASIL, 2017, cap. 2, p. 2).

QUADRO 1
Ações cibernéticas realizadas por cada subestrutura que compõe a estrutura militar de G Ciber que apoia a F Ter

Subestrutura	A	E	P	Responsabilidade
Batalhão de Guerra Eletrônica (BGE)	X	X	X	Realiza ataque e exploração cibernéticos em prol da Força Terrestre (F Ter) apoiada e proteção cibernética dos sistemas de informação da própria unidade.
Batalhão de Comunicações (B Com)			X	Realiza proteção cibernética dos sistemas de informação do grande comando apoiado (Divisão de Exército).
Batalhão de Comunicações e Guerra Eletrônica (B Com GE)		X	X	Realiza proteção cibernética dos sistemas de informação da F Ter apoiada, bem como a exploração cibernética (com limitações) em proveito deste escalão. Quando o BGE não estiver presente, será responsável por planejar e assessorar as ações de proteção cibernética e de exploração cibernética da F Ter.
Batalhão de Inteligência Militar (BIM)		X	X	Realiza exploração cibernética em proveito da F Ter apoiada e proteção cibernética dos sistemas de informação da própria unidade.
Companhia de Comando e Controle (Cia C^2)			X	Realiza proteção cibernética dos postos de comando da F Ter.
Companhia de Comunicações (Cia Com)			X	Realiza a proteção cibernética dos sistemas de informação de uma grande unidade (Brigada).

Legenda: A - Ataque cibernético. E - Exploração. P - Proteção.

Fonte: BRASIL, 2017.

4.2.2 Força Aérea Brasileira

Como já citado neste capítulo, a FAB está inserida no SMDC, sendo o EMAER responsável por orientar as atividades cibernéticas no âmbito da Força. A proteção cibernética da FAB é realizada pelo Centro de Computação da Aeronáutica de Brasília (CCA-BR), contando com a CTIR.FAB[63] em sua estrutura interna. No entanto, até o presente, a FAB não possui uma organização formalmente estabelecida para realizar as ações ofensivas no ciberespaço.

Por entender que, em decorrência dos avanços tecnológicos, as ameaças no espaço cibernético estão cada vez mais proeminentes e mais danosas, a FAB considera que a DC vem se estabelecendo como atividade essencial para a ampliação do Poder Militar. Tratando-se da

[63] Centro de Tratamento de Incidentes de Rede (CTIR) da FAB.

Força, a DC é fundamental para o Poder Aeroespacial, "por meio da proteção dos ativos de informação, degradação de redes computacionais e de comunicações do oponente, assim como na coleta de informações de interesse" (BRASIL, 2020a, p. 8). Nesse diapasão, a importância do emprego do espaço cibernético, sob as perspectivas de proteção, exploração e ataque cibernético, é manifesta na Concepção Estratégica "Força Aérea 100" da FAB,[64] ao afirmar que o espaço cibernético é um dos domínios, nos quais a Força possui relevante interesse, sendo indispensável para sua operação (BRASIL, 2016).

Nessa senda, a FAB, para atuar de forma efetiva no SMDC e em prol da própria Força, decidiu implantar o Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER) na estrutura organizacional do Centro de Computação da Aeronáutica de Brasília (CCA-BR), visando à ativação do Centro de Defesa Cibernética da Aeronáutica (CDCAER), até dezembro de 2023. O CDCAER terá a tarefa de planejar, executar, controlar e supervisionar todas as ações associadas à DC – proteção, exploração e ataque cibernético –, no âmbito do COMAER e tornar-se-á o órgão central do Sistema de Defesa Cibernética da FAB (BRASIL, 2020a, 2020d). A estrutura a ser empregada pela FAB, para efetuar ações cibernéticas nos níveis estratégico, operacional e tático, encontra-se em estudo e será estabelecida até a ativação do CDCAER.

4.3 Guerra cibernética e defesa cibernética na MB

A evolução da TI permitiu o desenvolvimento de complexos sistemas de informação, presentes na maioria das organizações, instituições e empresas, empregados, com vistas ao atingimento de melhores resultados, ou seja, com uma perspectiva que foca a eficiência e a eficácia das tarefas. Com a MB não é diferente. Os sistemas digitais administrativos (SDA)[65] e os sistemas digitais operativos (SDO)[66] estão cada vez mais presentes nas suas Organizações Militares (OM) e nos seus meios – navais, aeronavais ou de fuzileiros navais – empregados na guerra naval, o que exige atenção quanto às ameaças cibernéticas.

Ao compreender que o Poder Naval, um dos componentes da expressão militar do Poder Nacional[67] e parte integrante do Poder Marítimo, abrange os meios operativos da MB,

[64] Estabelece a visão de futuro para a FAB e orienta o Planejamento Estratégico Militar da Aeronáutica (PEMAER).
[65] Sistemas de informação concebidos para apoiar as atividades administrativas da MB (BRASIL, 2019).
[66] Sistemas de informação concebidos para o emprego em operações navais ou em seu benefício (BRASIL, 2019).
[67] Componentes da expressão militar do Poder Nacional: Poder Naval, Poder Militar Terrestre e Poder Militar Aeroespacial (BRASIL, 2017a).

bem como as estruturas de C^2, de logística e administrativa (BRASIL, 2017a), torna-se claro que dominar o setor cibernético é essencial, para mitigar o risco de que ataques cibernéticos sobre SDA e SDO sejam exitosos, a ponto de impactar o Poder Naval brasileiro. Uma amostra de que navios podem ser suscetíveis a tais ameaças está no alerta de segurança emitido pela Guarda Costeira dos EUA, em julho de 2019, apontando possíveis vulnerabilidades em navios comerciais. Tal fato se deu, por conta de um incidente cibernético que degradou a rede de dados de um navio comercial, com destino a dois portos dos EUA – New York e New Jersey – em fevereiro de 2019 (EUA, 2019). Nesse quadro, de acordo com a Doutrina Militar Naval (DMN), a guerra cibernética é uma das ações de guerra naval[68] empregadas em uma operação naval[69] (BRASIL, 2017a).

Para o desenvolvimento da capacidade cibernética do setor operativo da MB foi criada, em 2013, a Divisão de Guerra Cibernética subordinada à Subchefia de Inteligência Operacional do Comando de Operações Navais (ComOpNav). Constantemente analisada no âmbito da Marinha, a questão G Ciber desenvolveu-se, para permitir a atuação no espaço cibernético de forma segura e em prol de uma Força Conjunta ou Singular.

No presente, com um nível de maturidade mais avançado, a condução de ações de G Ciber no setor operativo está sob a responsabilidade do Comando Naval de Operações Especiais[70] (CoNavOpEsp), criado em 2019, a fim de contribuir com o preparo e o emprego das Forças Navais, Aeronavais e de Fuzileiros Navais (BRASIL, 2019b), centralizando os assuntos associados às operações especiais, à guerra assimétrica e à operação de informação[71] (OpInfo), nesta contidas as ações de guerra cibernética e as demais capacidades relacionadas à

[68] Compreendem as técnicas, as táticas e os procedimentos empregados em uma operação. De acordo com a DMN, são ações de guerra naval: ações de defesa aeroespacial, de guerra eletrônica, de guerra cibernética, de guerra acústica, de defesa nuclear, biológica, química, radiológica e artefatos explosivos (NBQRe), de despistamento, de submarinos, de superfície, aeronavais, aéreas e terrestres.

[69] Tipos de operações navais, segundo a DMN: operação de ataque, operação antissubmarino, operação anfíbia, operações de minagem e de contramedidas de minagem, operação de esclarecimento, operação de bloqueio, operação de apoio logístico móvel, operações especiais, operação de defesa de porto ou de área marítima restrita, operação de defesa do tráfego marítimo, operação de informação, operação de interdição marítima, operação psicológica, operação de busca e resgate em combate ou de combate SAR, operação ribeirinha, operação terrestre de caráter naval, operação civil-militar, operação de inteligência e operação de defesa de ilhas e arquipélagos oceânicos.

[70] Organização militar subordinada ao ComOpNav.

[71] "Conjunto de ações coordenadas dirigido para alcançar superioridade no ambiente informacional, por meio da negação, exploração, degradação ou destruição da informação e redes associadas oponentes, reais ou potenciais, enquanto protege suas próprias do ataque adversário. Pode ser desencadeada por meio da operação psicológica e das ações de guerra eletrônica, de guerra cibernética e de despistamento, além de medidas de segurança orgânica e das informações digitais. A destruição física dos alvos de comando e controle, embora parte integrante da OpInfo, será levada a cabo por intermédio de operações de ataque ou especiais, podendo haver o concurso de ações de superfície, de submarinos e/ou aeronavais" (BRASIL, 2017a, cap. 3, p. 15).

informação (CRI)[72] (BRASIL, 2020e).

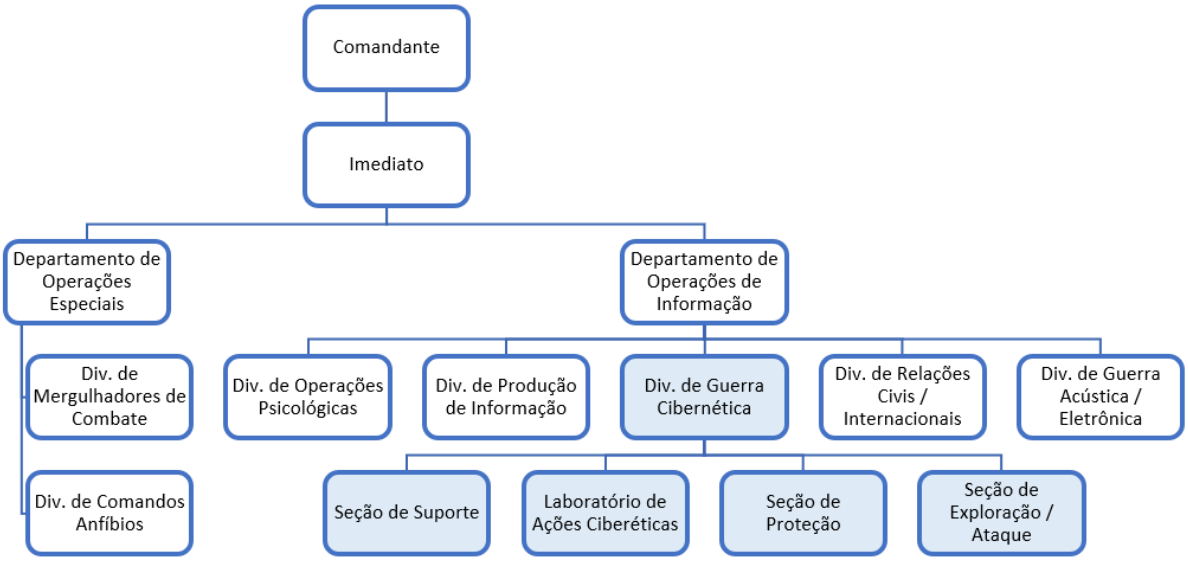


FIGURA 13 – Estrutura organizacional simplificada do CoNavOpEsp.
Fonte: BRASIL, 2020e.

Confirmando a importância dada pelo Setor Operativo aos assuntos relacionados ao emprego do ambiente cibernético, como se pode observar na FIG. 13 acima, o CoNavOpEsp possui a Divisão de Guerra Cibernética em sua estrutura organizacional, como parte integrante do seu Departamento de Operações de Informação e, subordinadas àquela, a Seção de Proteção e a Seção de Exploração e Ataque. Dessa forma, o CoNavOpEsp incorpora capacidades e habilidades para atuar nos três campos da guerra cibernética – ofensivo, defensivo e exploratório[73] – aplicáveis em uma guerra naval.

No entanto, o emprego do espaço cibernético na MB não se limita à guerra naval, estando presente em complexos sistemas de informação empregados no dia a dia pelas diversas Organizações Militares (OM) que a compõem. Assim, para se proteger das ameaças que a interconectividade trouxe consigo, nesse outro campo de atuação, as OM orientam-se pela Doutrina de Tecnologia da Informação da Marinha (BRASIL, 2007).

Essa Doutrina, além de enunciar conceitos, princípios e diretrizes, estabelece atribuições visando à Governança de TI, bem como fomenta outras alçadas. Entre essas atribuições, algumas estão intimamente ligadas à cibernética.

---

[72] De acordo com a Doutrina de Operações de Informação, capacidades relacionadas à informação (CRI) são "aptidões requeridas para afetar a capacidade de oponentes ou potenciais adversários de orientar, obter, produzir e difundir informações, em qualquer umas das perspectivas da dimensão informacional – física, cognitiva ou lógica". A principais CRI são: operações psicológicas, ações de guerra cibernética, despistamento, segurança da informação, atividades de comunicação social e destruição física (BRASIL, 2018a, cap.2, p. 6).

[73] Tipos de ações cibernéticas aplicadas na defesa cibernética e na guerra cibernética, segundo a Doutrina Militar de Defesa Cibernética: ataque cibernético, proteção cibernética e exploração cibernética.

Compete à Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM):

> elaborar normas, instruções técnicas e procedimentos padronizados para áreas de conhecimento concernentes ao emprego da Tecnologia da Informação na MB, notadamente: 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 (BRASIL, 2007, v. 1, cap. 3, p. 3).

Cabe a ela, também, o estabelecimento de doutrinas e normas associadas às atividades de Segurança da Informação e Comunicações[74] (SIC) e à Defesa Cibernética (DC), bem como a coordenação, execução e análise dos projetos que impliquem atividades de SIC e de DC (BRASIL, 2019).

No que concerne à G Ciber, cumpre ao Centro de Tecnologia da Informação da Marinha (CTIM) operar os seus recursos tecnológicos, planejar os exercícios gerais e subsidiar a OM Orientadora Técnica (OMOT) para a capacitação técnica do pessoal relacionado com suas atividades específicas (BRASIL, 2007). Ao CTIM, compete, ainda, a gerência e a execução, sob a supervisão da DCTIM, das atividades de DC e de SIC (BRASIL, 2019) e a execução técnica das atividades de DC (BRASIL, 2019). Diante destas atribuições, depreende-se que cabem à DCTIM e ao CTIM atividades associadas à DC e à G Ciber. No que diz respeito à este último, o CTIM é a OM responsável pelo planejamento de exercícios gerais de G Ciber. No entanto, como exposto no Capítulo 2, considerando que em nível estratégico as ações cibernéticas devem ser denominadas Defesa Cibernética, observa-se uma disfunção, ou seja, a DCTIM e o CTIM não devem conduzir G Ciber.

Outro aspecto a ser considerado é a percepção baseada nos diferentes conceitos empregados na MB para a DC e para a G Ciber ao compará-los com os estabelecidos pelo Ministério da Defesa, reunidos no ANEXO – Quadro comparativo de definições para Defesa Cibernética e Guerra Cibernética.

Em relação à DC, torna-se evidente que as ações cibernéticas podem ser ofensivas (ataque cibernético), defensivas (proteção cibernética) e exploratórias (exploração cibernética). Portanto, em nível estratégico, a aplicação de tais ações estaria a cargo da DCTIM/CTIM. Contudo, não é o que ocorre na prática, pois, atualmente, em nível estratégico, a DCTIM/CTIM

[74] A Segurança da Informação e Comunicações é um conjunto de medidas para garantir os requisitos de sigilo, autenticidade, integridade e disponibilidade perante os riscos medidos em função do valor do ativo, das ameaças e das vulnerabilidades dos ambientes que a armazenam, a processam e a trafegam. A SIC é obtida por meio da contínua manutenção de normas, procedimentos e estruturas organizacionais empregadas para o tráfego de informação e comunicações (BRASIL, 2019).

atua na proteção e o CoNavOpEsp no ataque e na exploração, quando necessário e em conformidade com as orientações advindas do MD.

No tocante à G Ciber, como abordado no Capítulo 2, o MD enfatiza a atuação sobre o C^2; já a MB age de forma mais ampla e contemporânea, ao compreender que ação de G Ciber envolve atos ofensivos e defensivos, em sistemas de informação e redes de computadores, com o objetivo de explorar, danificar ou destruir informações digitais ou negar o acesso a informações (proteção cibernética) (BRASIL, 2007), não obstante a sua Doutrina de TI ter precedido a Doutrina Militar de Defesa Cibernética do MD. Nesse contexto, a MB insere exercícios de Guerra Cibernética em seus programas de adestramento, com o propósito de aperfeiçoar a execução das ações de G Ciber[75] e fortalecer a mentalidade de Defesa Cibernética da Força.

Em proveito da Força Naval, podemos citar o exercício de contraposição a ameaças cibernéticas[76] realizado em navios da Esquadra brasileira, por ocasião da Operação ADEREX-Anfíbia/Superfície 2021 (BRASIL, 2021d). Em nível estratégico, um exemplo de exercício de defesa cibernética é a Operação BALUARTE[77] que, em 2020, chegou a sua 11ª edição e cujo propósito é "avaliar a efetividade das estruturas organizacionais e dos instrumentos doutrinários da Marinha para realizar e se contrapor a ataques cibernéticos limitados[78]" (BRASIL, 2020f). Tais exemplos reafirmam o contemporâneo entendimento da Marinha, ao tratar de ações cibernéticas. Em nível operacional ou tático, tais ações estão a cargo do CoNavOpEsp. Em nível estratégico, a proteção é exercida pela DCTIM/CTIM, e as demais ações – ataque e exploração – mantêm-se por conta daquele Comando.

No entanto, para formalizar essa forma de operar no espaço cibernético, em caso de uma excepcionalidade, como o estado de guerra, faz-se necessário que o EMA formule e dissemine uma doutrina que circunscreva a atuação da MB nesse ambiente, particularmente para a DC, de modo a mitigar possíveis interferências ou disfunções entre o Setor Operativo e o Setor de Material da MB.

---

[75] Ações de G Ciber são classificadas em três tipos: ataque cibernético, exploração cibernética e proteção cibernética (BRASIL, 2014).

[76] O exercício consistiu em uma equipe de exploração e ataque nucleada no CoNavOpEsp, de realizar ações no Espaço Cibernético da Operação ADEREX-Anfíbia/Superfície, em busca de vulnerabilidades que permitissem degradar o Comando e Controle, assim como realizar ações nos meios navais componentes da Operação. Para opor-se a essa ameaça, um destacamento de proteção cibernética estava embarcado no Navio-Aeródromo Multipropósito Atlântico, em assessoramento direto ao Comandante do Grupo-Tarefa da Operação (BRASIL, 2021d).

[77] Operação conduzida pelo CoNavOpEsp com a participação da Diretoria de Comunicações e Tecnologia da Informação da Marinha e do Centro de Tecnologia da Informação da Marinha.

[78] Como aqueles perpetrados por grupos "hacktivistas" (uma junção de hack e ativista) e criminosos cibernéticos, sem apoio estatal.

4.3.1 Adequando-se ao presente e preparando-se para o futuro

A constante e cada vez mais célere evolução tecnológica tornou-se um desafio para a defesa cibernética. Por isso, a END brasileira elegeu o setor cibernético como estratégico para a Defesa Nacional, ao lado dos setores nuclear e espacial (BRASIL, 2020g). Diante disso e alinhada aos documentos condicionantes, a MB, para lidar com o paradoxo da tecnologia digital (os inúmeros benefícios gerados pela evolução tecnológica trazem consigo as ameaças) em face da inevitável crescente implementação de sistemas de informação associados à Marinha do amanhã e do futuro, empenha-se para acompanhar a evolução tecnológica relacionada ao setor cibernético. Em suma, defesa e segurança cibernética é uma das áreas temáticas de Ciência, Tecnologia e Inovação (CT&I) de interesse da MB (BRASIL, 2017b).

De acordo com o Plano Estratégico da Marinha (PEM 2040), um dos objetivos navais da MB é o desenvolvimento da sua capacidade cibernética (BRASIL, 2020b). Nesse sentido, uma de suas ações estratégicas navais (AEN) visa à criação de um Esquadrão de Guerra Cibernética (EsqdGCiber), que concentrará as capacidades e competências para realizar os três tipos de ações cibernéticas – proteção, exploração e ataque – isto é, reunirá os recursos humanos (guerreiros cibernéticos), as tecnologias e ferramentas necessários para assegurar a liberdade de ação da MB no ciberespaço. Ademais, será responsável pelo desenvolvimento de doutrina e procedimentos associados G Ciber.

Ao se pensar em G Ciber, hoje, o CoNavOpEsp atua nos níveis operacional e tático. Compreende-se, assim, que o EsqdGCiber seria subordinado àquele Comando e tornar-se-ia seu braço operativo. Logo, o EsqdGCiber atuaria em nível tático e o CoNavOpEsp passaria a pensar G Ciber e planejá-la em nível operacional. Cabe ressaltar que tal transformação há de ser ágil, em face da velocidade do avanço tecnológico na área de TIC.

Segundo a lei de Moore, cunhada em 1965, a capacidade de processamento (poder de processamento) dos computadores dobra a cada dois anos[79]. Já Nye Jr. (2011) ressaltou que, em trinta anos, essa capacidade dobrou a cada dezoito meses e passou a custar um milésimo mil vezes menos, entre 1970 e o início do século XXI. Tal incremento na capacidade computacional é decorrente da possibilidade de inserção de maior quantidade de transistores nos chips, graças à fabricação de transistores cada vez menores. No entanto, alguns estudiosos da computação, acreditam que a validade desta lei está terminando (MIT, 2020), o que não quer dizer que o poder de processamento estagnar-se-á. Segundo Vellante e Floyer (2021), a lei de Moore,

[79] Em 1965 o Gordon E. Moore, cofundador da Intel, previu que o número de transistores em uma mesma área (neste caso, processador) dobraria a cada dois anos. Esta é a definição estrita da lei de Moore.

conforme sua definição estrita, não está ocorrendo; entretanto, soluções inovadoras ainda permitirão a ampliação daquela capacidade. Contudo, do mesmo modo que a evolução tecnológica contribui para fortalecer a segurança cibernética, ela beneficia os *hackers*, que passam a ter acesso às mesmas tecnologias.

Portanto, ao se pensar em proteção cibernética, que engloba ações que buscam neutralizar ataques cibernéticos e a exploração cibernética sobre sistemas de informação – dispositivos computacionais e redes de computadores e de comunicações – é fundamental que sejam utilizadas ferramentas de segurança cibernética tecnologicamente atualizadas, de modo a suplantar os modernos sistemas maliciosos empregados para praticar ataques e invasões àqueles sistemas. Em suma, torna-se essencial acompanhar a evolução tecnológica relacionada ao setor cibernético para que as ações, nesse ambiente operacional, sejam efetivas, tanto na forma ofensiva – exploração e ataque – quanto na defensiva – proteção cibernética – que em nível estratégico é uma atividade de caráter permanente.

4.4 A maturidade cibernética das três Forças: EB, MB e FAB

Observada a capital importância do espaço cibernético para o Brasil, principalmente pelo fato de que atividades nesse domínio operacional podem gerar grandes danos ao Estado e, em maior proporção, impactar na Defesa Nacional, o país, na figura das Forças Armadas e de órgãos da Administração Pública Federal, busca o constante aprimoramento do seu SMDC, à medida que as ameaças cibernéticas se tornam mais frequentes e as armas cibernéticas[80] mais sofisticados.

Analisando-se as estruturas permanentes e temporárias de cada uma das FS, para atender às demandas impostas pela concepção do SMDC, constata-se que:

O EB, para a conformação de uma estrutura voltada à guerra cibernética – níveis operacional e tático – está organizado, de modo que cada uma de suas OM – BGE, B Com, B Com GE, BIM, Cia C^2 e as Cia Com – já detêm as atribuições que a elas serão confiadas, no caso de ativação da Etta Mi D, permitindo uma rápida transferência de parcela ou totalidade da capacidade instalada em cada OM, para a Etta de G Ciber, que será constituída em prol da F ter conjunta ou singular. Cabe ressaltar que na Etta de G Ciber da F ter, apenas o BGE apresenta as capacidades para realizar ações de ataque e, de forma plena, as ações de exploração.

Na MB, o CoNavOpEsp integra todas as capacidades voltadas à G Ciber, sendo

[80] Métodos de ataque cibernético.

responsável pelas ações de ataque, exploração e proteção em prol de uma força naval, aeronaval ou de fuzileiros navais.

A FAB, sem uma estrutura de G Ciber formalmente instituída, planeja reorganizar a Força até 2023, com a ativação do CDCAER que concentrará as capacidades para realizar os três tipos de ações cibernéticas. No entanto, até o momento, não há definição de como ela atuará em nível operacional ou tático, o que não descarta a possibilidade da atribuição de tal responsabilidade ao CDCAER.

Em nível estratégico, as três FS concentram a responsabilidade de coordenar a proteção cibernética em uma única OM, como a seguir: a DCTIM na MB, o CITEx no EB e o CCA-BR na FAB.

Ao se pensar na gestão do setor cibernético de cada força, observa-se que:

No que diz respeito ao EB, o ComDCiber, além de atuar como órgão central do SMDC, assumindo, assim, a gestão do setor cibernético no âmbito da Defesa do país, por estar inserido na estrutura regimental do Comando do EB[81], tem forte influência no planejamento, na execução e no controle das atividades desse setor no âmbito do próprio EB, facilitando o seu gerenciamento. A resolução de a FAB criar o CDCAER é pautada na necessidade de centralizar todas as ações relacionadas à DC no âmbito do COMAER. Em síntese, direta ou indiretamente, o EB conta com um órgão central e, a partir de 2023, a FAB disporá de um, também, para gerir todos os tipos de ações no domínio cibernético, isto é, o ataque cibernético, a proteção cibernética e a exploração cibernética. Na Marinha, observa-se uma segregação na governança realizada pelo Setor de Material e Setor Operativo, ou seja, ainda não há uma sistemática integrando as atividades do setor cibernético da Força.

4.5 A integração do setor cibernético da MB

Compreende-se que no setor cibernético a MB se organiza em três vetores de atuação:

– O CoNavOpEsp, responsável pelas ações de guerra cibernética: ataque, exploração e proteção. Suas tarefas são de natureza operativa e seguem um processo de planejamento militar, seja ele conjunto (processo de planejamento conjunto – PPC) ou singular (processo de planejamento militar – PPM).

[81] Na visão do autor, isto é um paradoxo, pois o ComDCiber, por ser um comando operacional conjunto, deveria estar na estrutura organizacional do MD.

– A DCTIM, responsável pela governança de TIC na MB e por implementar, por meio do CTIM, as ações de proteção cibernética, de natureza administrativa, na RECIM.

– O Centro de Inteligência da Marinha (CIM), responsável pela inteligência cibernética, podendo realizar ações de exploração cibernética em proveito de suas atividades.

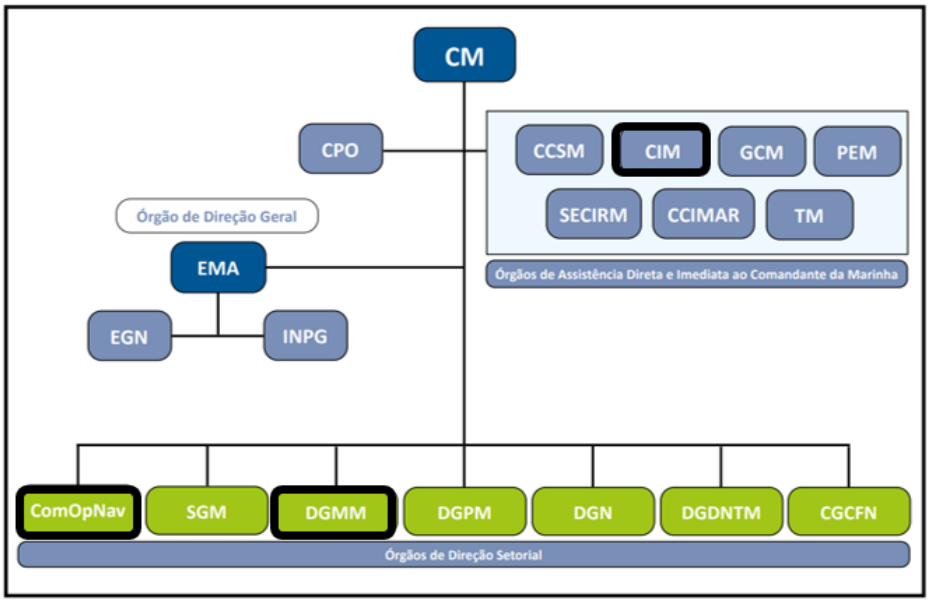


FIGURA 14 – Organograma resumido da MB.
Fonte: BRASIL, 2021c.

Pode-se observar que, cada um desses vetores se encontra inserido em um setor da Marinha. O CoNavOpEsp está estabelecido no setor operativo (ComOpNav), a DCTIM e CTIM fazem parte do Setor de Material (DGMM) e o CIM está diretamente ligado ao Comando da Marinha (CM). Dessa forma, a gestão do setor cibernético da MB sucede-se de forma descentralizada.

Chiavenato (2004) não aconselha nem desaconselha a descentralização da gestão, mas afirma que sua aplicação depende do contexto em que está inserida. Segundo ele, a descentralização traz vantagens como: autonomia para aqueles que estão na liderança, celeridade na tomada de decisão, menor interdependência entre setores e originalidade na solução de problemas. No entanto, apresenta como prejuízos: ausência de uniformidade nas decisões, dificuldade de controle e coordenação e tendência à duplicação de processos e tarefas. Tais desvantagens não são observadas na organização centralizada.

Segundo Chiavenato (2004), a estrutura organizacional centralizada traz, entre outras vantagens, o maior controle organizacional, a comunicação verticalizada e evita a duplicação de processos e tarefas. Ademais, Lacombe e Heilborn (2008) expõem como vantagens de

tal estrutura: proporcionar a especialização profissional, facilitar a uniformidade de procedimentos e técnicas dentro de uma determinada função, conferir flexibilidade para aumentar e reduzir pessoal e beneficiar a redução de custos.

Sob esse conceito e em harmonia com a Teoria Geral de Sistemas, em que pese o EMA formular a doutrina de defesa cibernética da MB, por meio de sua Subchefia de Logística (M-40) tratar da Defesa Cibernética, a implementação[82] de um sistema de defesa cibernética no âmbito da MB, que integre os três vetores (subsistemas) com um órgão central, ensejaria a homogeneidade de procedimentos, facilidade de controle e eficiência na comunicação vertical no setor cibernético da Força. Tal órgão seria responsável pela integração e coordenação das atividades diretamente associadas à guerra e à defesa cibernética. Considerando que o ComOpNav, por meio do CoNavOpEsp, atua de forma plena na G Ciber, ou seja, apresenta as capacidades necessárias para executar os três tipos de ações cibernéticas, o órgão central do sistema residiria no Setor Operativo.

Cabe ressaltar que a solução proposta não pretende alterar a sistemática de gestão dos três setores, mas sim, integrá-los em alto nível. Ela também não tenciona a criação de uma nova OM na estrutura organizacional do ComOpNav. Portanto, o CoNavOpEsp poderia ser o órgão central desse novo sistema.

Baseando-se no apresentado nos subcapítulos 4.4 e 4.5, são apresentadas sugestões para a MB.

4.6 Sugestões para a Marinha do Brasil

Com o propósito de aprimorar a estrutura voltada à defesa cibernética e G Ciber, sugere-se a implementação do sistema de guerra cibernética (SGC) da MB, cujo órgão central estaria na estrutura organizacional do ComOpNav. Nessa estrutura o EMA, por meio da M-40, permaneceria exercendo a função de harmonizar as atividades do setor cibernético no âmbito da Força, de acordo com as diretrizes provenientes do MD, por meio do ComDCiber.

[82] A criação de um sistema de defesa cibernética na MB encontra-se em estudo.

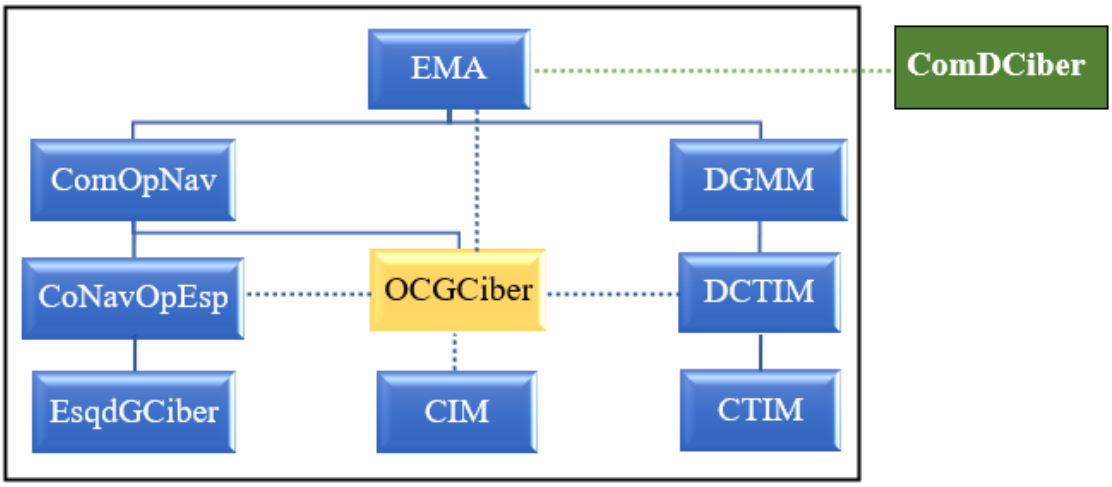


FIGURA 15 – Proposta de SGC da MB com um órgão central (OCGCiber).
Fonte: O autor.

Ao Órgão Central de Guerra Cibernética (OCGCiber) da MB, caberia a coordenação do SGC, utilizando-se da estrutura administrativa da MB, para alimentar com os insumos (recursos humanos, materiais e financeiros, educação etc.) necessários aos três vetores de ações cibernéticas, cada um, como já ocorre, com o seu instrumento, para levar a efeito as ações de interesse do Poder Naval brasileiro:

– CoNavOpEsp (futuramente o EsqdGCiber) – como instrumento de emprego da capacidade militar naval de natureza operativa, executando ações de ataque, exploração e proteção no domínio cibernético.

– CTIM – como instrumento de caráter administrativo, efetuando as ações de proteção cibernética da MB.

– CIM – como instrumento de inteligência, realizando ações de exploração.

A solução sugerida possibilitaria a padronização de procedimentos e a equalização de conhecimentos dos guerreiros cibernéticos da Força. Além disso, permitiria a troca de experiências, sob uma perspectiva diferenciada, entre os três vetores – CoNavOpEsp, DCTIM e CIM, contribuindo para a ampliação do poder cibernético da MB. Cabe destacar que, caso a equipe do CIM realize ações de exploração cibernética em proveito de suas atividades de inteligência, ela deve ser capaz de apagar seus rastros. Para tanto, necessitará de pessoal habilitado ou de empregar recursos do CoNavOpEsp.

Mapear, no âmbito da MB, a distribuição dos talentos em segurança e defesa cibernética, também poderia ser uma atribuição do OCGCiber, pois permitiria uma célere concentração de capital humano[83] necessário para reforçar as equipes do CoNavOpEsp, DCTIM ou CIM, se necessário.

Tal incumbência faz-se importante, em face da escassez de profissionais de segurança cibernética no mercado de trabalho brasileiro (GROSSMANN, 2021), o que impossibilita um rápido recrutamento de guerreiros cibernéticos do setor civil. Pesquisa realizada pelo *Enterprise Strategy Group* (ESG) e pela *Information Systems Security Association* (ISSA), entre o final de 2019 e início de 2020, relata que 70% dos membros da ISSA julgam que a carência global de talentos em segurança cibernética afetou sua organização (OLTSIK, 2020). Adicionalmente, sugere-se que o EMA crie uma doutrina ou atualize o EMA-416 (Doutrina de Tecnologia da Informação da Marinha), de modo a circunscrever a atuação coordenada dos setores operativo e material e das atividades de inteligência no ciberespaço, com base nas sugestões apontadas neste trabalho.

[83] Capital humano é o conjunto de conhecimentos, habilidades e atitudes que favorecem a execução de uma tarefa. São atributos obtidos por um trabalhador por meio de educação, qualificação e experiência.

5 CONCLUSÃO

Como consequência da transformação digital, Estados e organizações, definitivamente dependentes do espaço cibernético, se veem desafiados pelas crescentes ameaças cibernéticas nesse domínio facilmente acessível e sem fronteiras estabelecidas, o que torna a sua regulação complexa, elevando a instabilidade das relações internacionais, pois, mesmo em tempo de paz, a guerra cibernética se faz presente e o gerenciamento de riscos cibernéticos tornou-se essencial para os Estados.

Nesse cenário contemporâneo, ao zelarem pela Defesa Nacional, Estados e suas Forças Armadas passam a refletir sobre a necessidade de meios de defesa cibernética para atuarem, de modo a reconhecerem e a se contraporem a ataques cibernéticos direcionados a sistemas de informação estratégicos ou a infraestruturas críticas do país.

O espaço cibernético, como um domínio operacional, passou a exigir que os Estados atuem em duas vertentes: na defesa do país, contra possíveis ataques cibernéticos, cujas ações geralmente ocorrem de forma velada, ou seja, o autor intenciona que elas sejam praticadas sem deixar rastros, para impossibilitar a determinação da fonte do ataque. Em uma segunda vertente, voltada para o campo militar, em que a "weaponização" do ciberespaço fez nascer mais um campo de batalha. Nesse contexto, para o sucesso de uma operação militar, dois elementos indissociáveis, o ataque e a defesa, devem estar sempre presentes. Assim, de maneira análoga, operar no ciberespaço, com efetividade, requer capacidades ofensivas e defensivas nesse domínio operacional.

Os EUA, a China e a OTAN estruturam-se de modo a alcançar a liberdade de ação no espaço cibernético. Ambos os Estados têm por objetivo a superioridade nesse domínio operacional, pois entendem que isso lhes dá vantagem estratégica sobre os adversários, assim como, contribui para a estratégia dissuasória de cada um deles. A OTAN, sob o conceito de defesa coletiva, empenha-se para desenvolver uma consciência de que, para enfrentar as ameaças cibernéticas é essencial a conjugação coordenada de esforços de cada Estado membro, de modo transparente, interdependente e colaborativo.

Com esta compreensão, os EUA criaram, em 2010, o USCYBERCOM, um comando opercional conjunto permanente composto por elementos operacionais de cada uma das forças militares americanas (ARCYBER, AFCYBER, FLTCYBER e MARFORCYBER, para conduzirem e coordenarem o planejamento e as operações no ciberespaço, no intuito de defender e promover os interesses do EUA. Dada a relevância do domínio cibernético para o país, o USCYBERCOM foi elevado a comando combatente unificado em 2017, situando-se no

mesmo nível dos comandos regionais: USAFRICOM, USCENTCOM, USEUCOM USINDOPACOM, USNORTHCOM e USSOUTHCOM.

Com o entendimento de que a defesa cibernética é parte da tarefa central da OTAN, desde que reconheceu o ciberespaço como um domínio operacional, em 2016, essa Organização vem se reestruturando, para lidar com os novos desafios, contando, hoje, com: a NATO *Computer Incident Response Capability*, o NATO *Cyberspace Operations Centre* (CyOC) – em fase de implementação, com previsão de tornar-se totalmente operacional, em 2023 – o NATO *Cooperative Cyber Defence Centre of Excellence*, a NATO *School, a* NATO *Communications and Information Academy* e NATO *Defence College*.

No campo militar, os EUA e China, por entenderem que o êxito das operações militares está diretamente ligado à capacidade de atuação de cada Força no ciberespaço, reformulam suas FA, para serem capazes de atuar defensiva e ofensivamente nesse ambiente operacional. Em outras palavras, desenvolvem capacidades e competências para realizarem os três tipos de ações cibernéticas: proteção, exploração e ataque.

Para isso, a China conta com o *Network Systems Department*, também nominado força cibernética, subordinado ao *Strategic Support Force*, criado em 2015, que atua em prol de todo o Exército de Libertação Popular.

Os EUA conservam uma grande estrutura, cuja figura central é o USCYBERCOM, responsável, também, por sincronizar os esforços cibernéticos das forças militares americanas. No que diz respeito ao Poder Naval dos EUA, o FLTCYBER / Tenth Fleet – elemento operacional da Marinha americana junto ao USCYBERCOM – atua para garantir os efeitos operacionais e táticos desejados no ciberespaço e, por meio deste domínio, empregando seus guerreiros cibernéticos lotados no *Navy Cyber Defense Operations Command*, pertencente à estrutura organizacional da FLTCYBER / Tenth Fleet, que considera que as tecnologias emergentes moldarão o futuro das guerras. Portanto, faz-se necessário acompanhar o seu desenvolvimento, para incorporá-las como novos instrumentos a serem empregados no ciberespaço.

Voltando-se para o Brasil, constata-se que a preocupação com o espaço cibernético se deu com o estabelecimento da Política de Defesa Nacional (PDN) 2005. Em 2008, o setor cibernético do país foi alavancado com a publicação da Estratégia Nacional de Defesa (END) 2008. Marco para amadurecimento do setor, a END 2008 foi sucedida, desde então, de ações que revelam uma crescente preocupação do Brasil com o espaço cibernético.

Passados 15 anos desde a publicação da PDN 2005, a criação do Sistema Militar de Defesa Cibernética (SMDC), em 2020, tornou-se um marco expressivo para a Defesa Nacional. O estabelecimento de diretrizes para os órgãos envolvidos no SMDC, entre eles as FA,

proporciona que cada um deles determine estratégias, a fim de se aprestarem para a realização das atribuições a eles conferidas visando, de forma conjunta, a assegurar o uso indelével do espaço cibernético pelas FA e impedir ou dificultar a sua utilização contra os interesses do Brasil.

Inserida nesse grande sistema, a MB, por meio da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) e Centro de Tecnologia da Informação da Marinha (CTIM), protege sua rede de comunicações integradas da Marinha (RECIM), realizando, ininterruptamente, ações de proteção cibernética.

A rápida evolução tecnológica no setor cibernético exige um acompanhamento contínuo da evolução das ameaças cibernéticas que se multiplicam, dia a dia, pelas mãos de *hackers*. Logo, torna-se fundamental que a DCTIM e a CTIM possuam os recursos humanos (capital humano) e recursos materiais para se contraporem a tais ameaças e protegerem a Força, de ações de ataque e de exploração cibernéticas.

As OM responsáveis pelas ações de proteção cibernética da RECIM – DCTIM e CTIM – têm atuado satisfatoriamente no enfrentamento de ameaças que orbitam a borda daquela rede. Tais ações são de natureza administrativa e, portanto, desenvolvidas de acordo com processos administrativos inseridos na governança de TIC da MB.

Ao se pensar na guerra naval, a necessária atuação no espaço cibernético, para elevar a probabilidade de sucesso das ações na guerra cinética, requer a presença de guerreiros cibernéticos em sua força naval, aeronaval ou de fuzileiros navais, para a proteção de seus sistemas de informação, bem como para atuar sobre aqueles, empregados pelo inimigo. É nessa esfera que o CoNavOpEsp, criado em 2019, está inserido e, como detentor das capacidades voltadas para a G Ciber, é o braço operativo do ComOpNav para as ações ofensivas e defensivas, de caráter operativo, no ciberespaço.

Com tarefas de natureza operativa, seguindo o processo de planejamento militar, seja ele conjunto (PPC) ou singular (PPM), o CoNavOpEsp é, hoje, a OM responsável pelas ações de guerra cibernética na MB: ataque, exploração e proteção, em nível operacional e tático. No futuro, o EsqdGCiber passará a ser o braço operativo do CoNavOpEsp. Portanto, à luz das condicionantes de alto nível e com base na organização adotada pelos EUA, OTAN e China, conclui-se que a estrutura organizacional da MB é adequada, hoje em dia, para atuar nos três campos da defesa ou guerra cibernética (ofensivo, defensivo e exploratório).

No entanto, os documentos que orientam o setor cibernético na MB carecem de atualizações, de modo a abarcar a inserção do recém-criado CoNavOpEsp, que age como instrumento de emprego da capacidade militar naval de natureza operativa, executando ações de ataque, exploração e proteção no domínio cibernético.

A implementação do sistema de guerra cibernética da MB, com seu órgão central na estrutura organizacional do ComOpNav, certamente concorrerá para o aprimoramento das ações cibernéticas efetuadas pela Marinha, o que contribuirá para o desenvolvimento do poder cibernético, no âmbito da MB.

Por fim, cabe ressaltar que o êxito da Marinha no espaço cibernético, seja de forma defensiva ou ofensiva, requer o acompanhamento da evolução das ameaças cibernéticas e das novas TIC, a fim de que os recursos humanos sejam preparados para atuarem nesse domínio operacional, em proveito dos interesses da MB. Ademais, o perfeito conhecimento dos SDA e SDO que a Força vem adquirindo, torna-se fundamental, de modo que possíveis vulnerabilidades sejam eliminadas.

REFERÊNCIAS

ARAÚJO, Andréa Cristina Marques de; GOUVEIA, Luís Borges. **Uma revisão sobre os princípios da teoria geral dos sistemas.** Revista Estação Científica, Juiz de Fora, n. 16, 2016. Disponível em: < https://portal.estacio.br/media/3727396/uma-revisão-sobre-os-princípios-da-teoria-geral-dos-sistemas.pdf>. Acesso em: 18 jun. 2021.

ATECH. Site da Atech Negócios em Tecnologias S/A, 2021. **Atech, em atuação coordenada com o ComDCiber, participa do maior e mais complexo Exercício de Defesa Cibernética do mundo, Locked Shields 2021.** Disponível em: <https://atech.com.br/atech-em-atuacao-coordenada-com-o-comdciber-participa-do-maior-e-mais-complexo-exercicio-de-defesa-cibernetica-do-mundo-locked-shields-2021>. Acesso em 13jun. 2021.

BARROS, Renata Furtado de. **Guerra cibernética:** os novos desafios do Direito Internacional. Belo Horizonte: D`Plácido, 2015.

BRASIL. Comando da Aeronáutica. **Portaria n. 94/GC3, de 27 de janeiro de 2016.** Aprova a Concepção Estratégica – Força Aérea 100 - DCA 11-45. Disponível em: <https://www.fab.mil.br/Download/arquivos/DCA%2011-45_Concepcao_Estrategica_Forca_Aerea_100.pdf>. Acesso em: 15 jun. 2021.

_____. Comando do Exército. **Portaria n. 667, de 4 de agosto de 2010.** Ativa o Núcleo do Centro de Defesa Cibernética do Exército e dá outras providências.

_____. _____. Comando de Operações Terrestres. **Manual de Campanha EB70-MC-10.232 Guerra Cibernética.** Brasília: Comando de Operações Terrestres, 2017. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/1/631/3/EB70MC10232.pdf>. Acesso em: 16 jun. 2021.

_____. **Decreto n. 5.484, de 30 de junho de 2005.** Aprova a Política de Defesa Nacional e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 30 jun. 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5484.htm>. Acesso em: 01 jul. 2021.

_____. **Decreto n. 6.703, de 18 de dezembro de 2008.** Aprova a Estratégia Nacional de Defesa, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 19 dez. 2008. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: Acesso em: 27 jun. 2021.

_____. **Decreto n. 9.637, de 26 de dezembro de 2018.** Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto n. 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei n. 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 27 dez. 2018. Seção 1. p. 23. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm#art6i>. Acesso em: 13 fev. 2021.

_____. **Decreto n. 10.222, de 05 de fevereiro de 2020.** Aprova a Estratégia Nacional de Segurança Cibernética. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 6 fev. 2020. Seção 1. p. 6. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>. Acesso em: 13 fev. 2021.

_____. Estado-Maior da Aeronáutica. **Diretriz de implantação do Núcleo do Centro de Defesa Cibernética da Aeronáutica** (DCA 11-130). Brasília, DF, 2020a.

_____. Estado-Maior da Armada. EMA-305 – **Doutrina Militar Naval** (DMN). Brasília: 2017a. 143 p.

_____. _____. EMA-415 – **Estratégia de Ciência, Tecnologia e Inovação da Marinha do Brasil.** Brasília: 2017b.

_____. _____. EMA-416 – **Doutrina de Tecnologia da Informação da Marinha** (Volume I, 1ª rev.). Brasília: Estado-Maior da Armada, 2007.

_____. _____. EMA-335 – **Doutrina de Operações de Informação.** Brasília: Estado-Maior da Armada, 2018a.

_____. _____. 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: 18 fev. 2021. ISBN 978-65-991468-0-0.

_____. Diretoria-Geral do Material da Marinha. DGMM-0540 – **Normas de Tecnologia da Informação da Marinha** (3ª rev.). Rio de Janeiro: Diretoria-Geral do Material da Marinha, 2019.

_____. Exército Brasileiro. 1ª Divisão de Exército. 1 vídeo (4min 26s). **Exército participa de maior exercício de defesa cibernética do mundo.** Publicado pelo Canal do Exército brasileiro, 2021. Disponível em: <https://www.youtube.com/watch?v=2PzbOOHjfZA>. Acesso em: 12 jun. 2021.

_____. _____. Site do Centro Integrado de Telemática do Exército, 2021a. **Institucional.** Disponível em: <www.citex.eb.mil.br>. Acesso em: 20 jun. 2021.

_____. _____. Site do Exército Brasileiro. 7 ed. **Competição cibernética entre integrantes das Forças Armadas busca novos talentos na área.** 28 out. 2020c. Disponível em: <https://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/id/12363209>. Acesso em: 13 jul. 2021.

_____. _____. Site do Exército Brasileiro. **Setor estratégico para o Brasil ganha impulso com a ativação da Escola Nacional de Defesa Cibernética.** 08 fev. 2019a. Disponível em: <https://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/id/9524079>. Acesso em: 10 jun. 2021.

_____. Força Aérea Brasileira. Site da Força Aérea Brasileira. **FAB implanta Núcleo do Centro de Defesa Cibernética da Aeronáutica** (NuCDCAER), 02 dez. 2020d. Disponível em: <https://www.fab.mil.br/noticias/mostra/36606/TECNOLOGIA - FAB implanta Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER)>. Acesso em: 15 jun.2021.

_____. _____. Site da Força Aérea Brasileira. **Núcleo do Centro de Defesa Cibernética da Aeronáutica participa do Locked Shields 2021**. Rev. Capitão Oliveira Lima, 04 abr. 2021b. Disponível em: <https://www.fab.mil.br/noticias/mostra/37200>. Acesso em: 10 jun.2021.

_____. Marinha do Brasil. Comando de Operações Navais. **Portaria n. 19/CoNavOpEsp**, **de 6 de novembro de 2020e**. Aprova o Regimento Interno do Comando Naval de Operações Especiais (CoNavOpEsp) e dá outras providências.

_____. _____. **Portaria n. 232/MB, de 16 de agosto de 2019b**. Cria o Comando Naval de Operações Especiais (CoNavOpEsp) e dá outras providências. Disponível em: <https://www.jusbrasil.com.br/diarios/257292718/dou-secao-1-20-08-2019-pg-17>. Acesso em: 01 jun. 2021.

_____. _____. **Relatório de Gestão 2020.** Brasília, DF, 31 mar. 2021c. 234 p. Disponível em: <https://www.jusbrasil.com.br/diarios/257292718/dou-secao-1-20-08-2019-pg-17>. Acesso em: 23 jul. 2021.

_____. _____. Site da Marinha do Brasil. **Comando Naval de Operações Especiais conduz exercício de guerra cibernética**, 22 set. 2020f. Disponível em: <https://www.marinha.mil.br/noticias/comando-naval-de-operacoes-especiais-conduz-exercicio-de-guerra-cibernetica>. Acesso em: 09 jun. 2021.

_____. _____. Site da Marinha do Brasil. **Navios da esquadra realizam exercício de guerra cibernética durante a operação "ADEREX-Anfíbia/Superfície 2021**. 31 maio 2021d. Disponível em: <https://www.marinha.mil.br/noticias/navios-da-esquadra-realizam-exercicio-de-guerra-cibernetica-durante-operacao-aderex>. Acesso em: 09 jun. 2021.

_____. Ministério da Defesa. MD31-M-07 – **Doutrina Militar de Defesa Cibernética.** 1 ed. Brasília: Ministério da Defesa, 2014. 36 p. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_07a_defesaa_ciberneticaa_1a_2014.pdf>. Acesso em: 26 fev. 2021.

BRASIL. Ministério da Defesa. MD33-M-12 – **Manual de Operações Interagências.** 2 ed. Brasília: Ministério da Defesa, 2017c. 72 p. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/operacoes/md33a_ma_12a_opa_interagenciasa_2a_eda_2017.pdf>. Acesso em: 21 jun. 2021.

_____. _____. MD35-G-01 – **Glossário das Forças Armadas.** 5 ed. Brasília: Ministério da Defesa, 2015. 294 p. Disponível em: <https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf>. Acesso em: 26 fev. 2021.

_____. _____. MD51-M-04 – **Doutrina Militar de Defesa.** 2 ed. Brasília: Ministério da Defesa, 2007a. 48 p. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/o-estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes/md51-m-04-doutrina-militar-de-defesa-2a-ed-2007.pdf >. Acesso em: 15 maio 2021.

_____. _____. **Política Nacional de Defesa e Estratégia Nacional de Defesa encaminhadas ao Congresso Nacional em 2020g.** Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf>. Acesso em: 21 fev. 2021.

_____. _____. **Portaria Normativa n. 2.777-MD, de 27 de outubro de 2014a**. Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências. Disponível em: <https://www.resdal.org/caeef-resdal/assets/brasil----ordenanza-normativa-n---2.777---ministerio-de-defensa,-de-27-de-octubre-de-2014.pdf>. Acesso em: 22 fev. 2021.

_____. _____. **Portaria Normativa n. 3.389/MD, de 21 de dezembro de 2012.** Dispõe sobre a Política Cibernética de Defesa. Diário Oficial [da] República Federativa do Brasil, Poder Executivo - Ministério da Defesa, Brasília, DF, 27 dez. 2012. Seção 1. p. 11. Disponível em: <www.bdo3c.f-sc.org/archives/1107.pdf>. Acesso em: 15 maio 2021.

_____. _____. **Portaria n. 3.781/GM-MD, de 17 de novembro de 2020.** Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Poder Executivo - Ministério da Defesa, Brasília, DF, 19 nov. 2020h. Seção 1. p. 12. Disponível em: <https://www.in.gov.br/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860>. Acesso em: 22 fev. 2021.

BRENT, Laura. **NATO's role in cyberspace.** NATO Review, 12 fev. 2019. Disponível em: <https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html>. Acesso em: 20 maio 2021.

CASTELLS, M. **A galáxia da internet:** reflexões sobre a internet, os negócios e a sociedade (eBook Kindle). Rio de Janeiro: Jorge Zahar, 2003.

CCDCOE. Site do Cooperative Cyber Defence Centre of Excellence, 2021. **About us.** Disponível em: <https://ccdcoe.org/about-us>. Acesso em: 17 jun. 2021.

CHIAVENATO, Idalberto. **Introdução à teoria da administração.** 7 ed. São Paulo: Elsevier, 2004, 634 p. ISBN 978-85-352-1348-5.

CHINA. Gabinete de Informação do Conselho de Estado da República Popular da China. **China's Military Strategy** (2015), maio 2015, 27 p. Disponível em: <https://jamestown.org/wp-content/uploads/2016/07/China%E2%80%99s-Military-Strategy-2015.pdf>. Acesso em: 03 jun. 2021.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber war:** the next threat to national security, and what to do about it. New York: HarperCollins e-books, 2010.

CLAUSEWITZ, Carl von. **Da guerra**. Trad. Maria Teresa Ramos. 3ed. São Paulo: WMF Martins Fontes, 2017. [N. p.]

COSTELLO, John; McREYNOLDS, Joe. **China's Strategic Support Force:** a force for a new era. Washington, D.C.: National Defense University Press, 2018. 69 p. ISBN 978-0-16-094959-3. Disponível em: <https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf>. Acesso em: 13 maio 2020.

CRS. Congressional Research Service. **China's military:** the People's Liberation Army (PLA). 2021, 54 p. Disponível em: <https://www.everycrsreport.com/files/2021-06-04_R46808_848c9c293ea2f76c1b766d9174017md-eeefa03a5.pdf>. Acesso em: 25 jun. 2021.

EUA. Army Cyber Command. Site do U.S. Army Cyber Command, 2021. **Our Mission**. Disponível em: <https://www.arcyber.army.mil>. Acesso em: 03 maio 2021.

_____. Coast Guard. **Safety Alert 06-19**, jul. 2019. Disponível em: <https://safety4sea.com/wp-content/uploads/2019/07/USCG-Cyber-Incident-Exposes-Potential-Vulnerabilities-Onboard-Commercial-Vessels-2019_07.pdf>. Acesso em: 29 jun. 2021.

_____. Cyber Command. **Achieve and maintain cyberspace superiority** – Command Vision for US Cyber Command. 2018, 10 p. Disponível em: <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf>. Acesso em: 03 maio 2021.

_____. Cyber Command. Site do U.S. Cyber Command, 2021a. **Mission.** Disponível em: <https://www.cybercom.mil/About/Mission-and-Vision>. Acesso em: 03 maio 2021.

_____. _____. Site do U.S. Cyber Command, 2021b. **Our history.** Disponível em: <https://www.cybercom.mil/About/History/>. Acesso em: 03 maio 2021.

_____. Department of Defense. **Military and security developments involving the people's Republic of China 2020**. 2020, 173 p. Disponível em: <https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF>. Acesso em: 02 maio 2021.

_____. _____. **Cyber Strategy** – Summary. 2018a, 7 p. Disponível em: <https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF>. Acesso em: 03 maio 2021.

_____. Fleet Cyber Command / U.S. TENTH. **U.S. Fleet Cyber Command / U.S. TENTH Fleet Strategic Plan 2020-2025.** 2020a, 22 p. Disponível em: <https://www.fcc.navy.mil/Portals/37/FCC_C10F%20Strategic%20Plan%202020-2025.pdf?ver=qK9ai1Z8goc_8UrBWJp3oQ%3d%3d>. Acesso em: 17 jul. 2021.

_____. Fleet Cyber Command. Site do U.S. Fleet Cyber Command, 2021c. **Command description.** Disponível em: <https://www.fcc.navy.mil>. Acesso em: 03 maio 2021.

_____. _____. Site do U.S. Fleet Cyber Command, 2021d. **Mission & vision.** Disponível em: <https://www.fcc.navy.mil/ABOUT-US/MISSION-VISION >. Acesso em: 03 maio 2021.

_____. Marines. Site do Marines, 2021e. **Mission**. Disponível em: <https://www.marforcyber.marines.mil/About>. Acesso em: 03 maio 2021.

_____. Presidência da República dos EUA. **Memorandum for the Secretary of Defense:** elevation of U.S. Cyber Command to a Unified Combatant. Washington, 15 ago. 2017. Disponível em: <https://www.govinfo.gov/content/pkg/FR-2017-08-23/pdf/2017-17947.pdf>. Acesso em: 19 jul. 2021.

_____. Sixteenth Air Force. Site da Sixteenth Air Force. **Sixteenth Air Force (Air Forces Cyber)**, 27 ago. 2020b. Disponível em: <https://www.16af.af.mil/About-Us/Fact-Sheets/Display/Article/1957318/sixteenth-air-force-air-forces-cyber>. Acesso em: 03 maio 2021.

FRANÇA, Júnia Lessa; VASCONCELLOS, Ana Cristina de. **Manual para normalização de publicações técnico-científicas.** 8ed. rev. Belo Horizonte: UFMG, 2007. 255 p. ISBN 978-85-7041-560-8.

FRAVEL, M. Taylor. **China's new military strategy:** "Winning Informationized Local Wars". China Brief, v. 15, n. 13, 2015. Disponível em: <https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars>. Acesso em: 03 maio2021.

GARCIA, Antônio Carlos. **EMBRAER:** Fato relevante, 30 nov. 2020. Disponível em: <https://static.poder360.com.br/2020/12/Embraer-Fato-Relevante-30-nov-2020.pdf>. Acesso em: 17 maio 2021.

GILES, D. **Psychology of the media.** New York: Palgrave Macmillan, 2010. 230 p. ISBN 978-0-230-24986-8.

GOŹDZIEWICZ, Wiesław *et al*. **NATO road to cybersecurity**. The Kosciuszko Institute, 2016. 79 p. ISBN: 978-83-63712-29-7. Disponível em: <https://www.ik.org.pl/wp-content/uploads/nato_road_to_cybersecurity_the_kosciuszko_institute_2016.pdf>. Acesso em: 18 jul. 2021.

GROSSMANN, Luís Osvaldo. **Brasil é o país onde mais faltam profissionais de cibersegurança.** Convergência Digital, 11 jan. 2021. Disponível em: <https://www.convergenciadigital.com.br/Seguranca/Brasil-e-o-pais-onde-mais-faltam-profissionais-de-ciberseguranca-55860.html?UserActiveTemplate=site>. Acesso em: 01 jul. 2021.

HUREL, Louise Marie. **Cibersegurança no Brasil:** uma análise da estratégia nacional. Instituto Igarapé, Rio de Janeiro, n. 54, 39 p., abr. 2021, Disponível em: <https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf>. Acesso em: 16 jul. 2021

JINGHUA, Lyu. **What are China's cyber capabilities and intentions?** IPI GLOBAL OBSERVATORY, 22 mar. 2019. Disponível em: <https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions>. Acesso em: 03 maio 2021.

KANIA, Elsa B.; COSTELLO, John K. **The Strategic Support Force and the future of Chinese information operations**. The Cyber Defense Review, v. 3, n. 1, p. 105 – 121, 2018.

LACOMBE, Francisco José M.; HEIBORN, Gilberto Luiz J. **Administração:** princípios e tendências. 2 ed. rev. São Paulo: Saraiva, 2008. 544 p. ISBN 978-85-02-07244-2.

McREYNOLDS, Joe *et al*. **China's strategy for the cyber domain:** selected proceedings from the fourth annual China Defense and Security Conference (English Edition) (eBook Kindle). The Jamestown Foundation, 2014.

MIT Technology Review. **Nós não estamos preparados para o fim da lei de Moore**, 25 jul. 2020. Disponível em: <https://mittechreview.com.br/nos-nao-estamos-preparados-para-o-fim-da-lei-de-moore>. Acesso em: 01 jul. 2021.

NCSI. Site do National Cyber Security Index, 2021. Disponível em: < https://ncsi.ega.ee/ncsi-index>. Acesso em: 05 jul. 2021.

NYE Jr, Joseph S. **The future of power** (eBook Kindle). New York: PublicAffairs, 2011. [N.p.]

OLTSIK, Jon. **The life and times of cybersecurity professionals 2020.** Enterprise Strategy Group, jul. 2020. 49 p. Disponível em: <https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf>. Acesso em: 07 jul. 2021.

ONU. United Nations. **Report of Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security**, **2015.** 17p. Disponível em: <https://digitallibrary.un.org/record/799853>. Acesso em: 21 abr. 2021.

OTAN. **Brussels Summit Declaration**. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Councilin Brussels, 11 jul. 2018. Disponível em: <https://ccdcoe.org/uploads/2019/09/NATO-180711-Brussels-summit-declaration.pdf>. Acesso em: 01 jun. 2021.

_____. **Cyber defense** (*Last updated*: 02 jul. 2021). Disponível em: <https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en>. Acesso em: 05 jul. 2021.

_____. NATO Cyber Defense. **Factsheet**, ago. 2020. Disponível em: <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/8/pdf/2008-factsheet-cyber-defence-en.pdf>. Acesso em: 01 jun. 2021.

_____. NATO Standardization Office (NSO). **Allied Joint Publication (AJP-3.20):** Allied Joint Doctrine for Cyberspace Operations. 2020a, 28 p. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf>. Acesso em: 01 jun. 2021.

_____. **Statement by the North Atlantic Council concerning malicious cyber activities**. 03 jun. 2020b. Disponível em: <https://ccdcoe.org/uploads/2020/06/NATO-200603_News_-Statement-by-the-North-Atlantic-Council-concerning-malicious-cyber-activities.pdf>. Acesso em: 02 jun. 2021.

_____. **Warsaw Summit Communiqué** – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016. Disponível em: <https://www.nato.int/cps/en/natohq/official_texts_133169.htm>. Acesso em: 05 mar. 2021.

PENA, Rodolfo F. Alves. David Harvey. Brasil Escola. Disponível em: https://brasilescola.uol.com.br/geografia/david-harvey.htm. Acesso em: 06 ago. 2021.

POLLPETER, Kevin L.; CHASE, Michael S.; HEGINBOTHAM, Eric. **The creation of the PLA Strategic Support Force and its implications for Chinese Military Space Operations.** Califórnia: RAND Corporation, 2017, 46 p. Disponível em: <https://www.rand.org/pubs/research_reports/RR2058.html>. Acesso em: 03 jun. 2021.

RAND. Site da RAND Corporation, 2021. **Cyber warfare.** Disponível em: <https://www.rand.org/topics/cyber-warfare.html>. Acesso em: 20 abr. 2021.

SABBAT, Arthur. **Defesa Cibernética e Segurança Cibernética**: Diferenças e Semelhanças. Security Report, 16 jul. 2019. Disponível em: <https://www.securityreport.com.br/destaques/defesa-cibernetica-e-seguranca-cibernetica-diferencas-e-semelhancas/#.YRvsG3ySlPY>. Acesso em: 11 maio 2021.

SOMTOCHUKWU, Nnabuife Godfrey. **The significance and future of Network Security**. International Journal of Computer Science and Technology. Cranfield University, UK, v. 8, n.1, jan/mar. 2017. Disponível em: <http://www.ijcst.com/vol8/2/10-nnabuife-godfrey-somtochukwu.pdf>. Acesso em: 28 fev. 2021.

SYMANTEC. **Internet security threat Report, 2019.** Disponível em: <https://docs.broadcom.com/doc/istr-24-2019-en >. Acesso em: 03 maio 2021.

TECNOLOGIA & DEFESA. **Brasil participa do maior exercício de defesa cibernética do mundo**, 17 abr. 2021. Disponível em: <https://tecnodefesa.com.br/brasil-participa-do-maior-exercicio-de-defesa-cibernetica-do-mundo>. Acesso em: 12 jun. 2021.

TIDY, Joe. **Colonial hack:** how did cyber-attackers shut off pipeline? BBC News, 10 maio 2021. Disponível em: <https://www.bbc.com/news/technology-57063636>. Acesso em: 18 maio 2021.

TREND MICRO. **Trend Micro Annual Cybersecurity Report, 2020.** Disponível em: <https://documents.trendmicro.com/assets/rpt/rpt-a-constant-state-of-flux.pdf>. Acesso em: 02 maio 2021.

VELLANTE, Dave; FLOYER, David. **A new era of innovation:** Moore's law is not dead and AI is ready to explode, 10 abr. 2021. Disponível em: <https://siliconangle.com/2021/04/10/new-era-innovation-moores-law-not-dead-ai-ready-explode >. Acesso em: 01 jul. 2021.

WELCH, Larry D. **Cyberspace –** The fifth operational domain. Institute for Defense Analyses (IDA), 2011. 7 p. Disponível em: <https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx>. Acesso em: 19 jul. 2021.

ZHAO, Frank; HEATLEY, Jesse. **China's master plan for IT dominance:** China's top leadership has released a bold long-range blueprint for the country's Internet and technology strategy. The Diplomat, 11 ago. 2016. Disponível em: <https://thediplomat.com/2016/08/chinas-master-plan-for-it-dominance>. Acesso em: 18 maio 2021.

GLOSSÁRIO

Ataque Cibernético: “Ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente” (BRASIL, 2014, p. 23).

Exploração Cibernética: “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” (BRASIL, 2014, p. 23).

Marinha do amanhã: “Refere-se aos meios navais, aeronavais e de fuzileiros navais, assim como aos respectivos sistemas e subsistemas que estão sendo construídos e/ou obtidos pela MB” (BRASIL, 2017b, cap. 1, p. 2).

Marinha do futuro: “Reúne os estudos, as pesquisas, os desenvolvimentos tecnológicos, a análise da conjuntura em nível estratégico, a prospecção tecnológica e os primeiros passos para a concepção de futuros meios navais, aeronavais e de fuzileiros navais, bem como os respectivos sistemas, subsistemas e suprassistemas” (BRASIL, 2017b, cap. 1, p. 2).

Poder Nacional: “capacidade que tem o conjunto dos homens e dos meios que constituem a Nação, atuando em conformidade com a vontade nacional, de alcançar e manter os objetivos nacionais” (BRASIL, 2017a, p.15).

Poder Marítimo: é a projeção do Poder Nacional que “resulta 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 a manter os objetivos nacionais” (BRASIL, 2017a, p.15).

Proteção Cibernética: “Ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente” (BRASIL, 2014, p. 23).

ANEXO

Quadro comparativo de definições para defesa cibernética e guerra cibernética

Documento	Origem	Definição
Doutrina Militar de Defesa Cibernética	**MD**	GC é o "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" (BRASIL, 2014, p. 19).
		DC é 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 as finalidades 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" (BRASIL, 2014, p. 18).
Doutrina de TI da MB	**MB**	GC são "ações ofensivas e defensivas destinadas a explorar, danificar ou destruir informações digitais, ou negar o acesso às suas informações. Tais ações utilizam-se de sistemas de informação e de redes de computadores" (BRASIL, 2007, v. 1, cap. 1, p. 3).
Normas de TI da MB		DC é "conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento de nível estratégico, com as finalidades de proteger os interesses da Marinha e comprometer os sistemas de informação do oponente" (BRASIL, 2019, cap. 7, p. 2).