ESCOLA DE GUERRA NAVAL

CC (FN) MICHEL SILVA CAMELO

GUERRA CIBERNÉTICA:

A aderência à doutrina brasileira nas ações da segunda Guerra do Golfo em 2003.

Rio de Janeiro

2020

CC (FN) MICHEL SILVA CAMELO

GUERRA CIBERNÉTICA:

A aderência à doutrina brasileira nas ações da segunda Guerra do Golfo em 2003.

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF Alexander Thomaz Arruda

Rio de Janeiro

Escola de Guerra Naval

2020

AGRADECIMENTOS

À Deus, por sua graça e compaixão, por ser lâmpada para meus pés e luz para meus caminhos e por ter me concedido saúde e sabedoria para vencer as barreiras da vida em meio à pandemia COVID-19.

À minha esposa Renata pelo apoio, incentivo e cuidado durante o período em que me ausentei para dedicar-me a este trabalho e aos meus filhos Davi e Timóteo por me permitirem tempo para esta jornada e compreenderem sua necessidade.

Aos amigos do Curso de Estado-Maior para Oficiais Superiores do ano de 2020 formado, em sua maioria, pelos componentes da turma Almirante Maximiano, pelo ambiente amistoso e pela camaradagem. Em especial aos CF FN Leandro Marinho Moreira e CC FN Fernando Bellard Abdo pelo apoio durante este percurso.

Ao CF Alexander Tomaz Arruda, meu orientador, pelos ajustes, ensinamentos, experiência compartilhada, incentivos e paciência durante todas as fases deste trabalho acadêmico e aos CMG (RM1) Cláudio Marin e CF (RM1) Ohara Barbosa Nagashima, pelas orientações técnicas e auxílio na aplicação da normatização à pesquisa.

À Escola de Guerra Naval, através da direção, corpo docente e administração que facilitaram minha jornada a um degrau superior de conhecimento.

RESUMO

A evolução tecnológica tem forçado a mudança e a adaptação da guerra ao longo do tempo. Esses avanços geram novas oportunidades e vulnerabilidades que são aproveitadas antes, durante e depois dos confrontos. Cada experiência demanda observar conceitos e teorias que se não estiverem atualizadas, podem expor as forças envolvidas a tais vulnerabilidades. Assim, o objetivo desta pesquisa é analisar a aderência da doutrina de guerra cibernética brasileira em um cenário específico, os momentos iniciais da 2ª Guerra do Golfo em 2003, usando a doutrina brasileira estabelecida no manual de Doutrina Militar de Defesa Cibernética (MD-31-M-07), complementada pela doutrina conjunta dos Estados Unidos da América (EUA) presente no manual *Cyberspace Operations* (JP 3-12). O desenho de pesquisa utilizado foi o confronto da teoria com a realidade, usando como parâmetros os níveis de decisão, as ações da guerra cibernética e as funções operacionais. Concluiu-se que houve aderência parcial à doutrina, ficando pendente a interação com as funções operacionais presentes na doutrina estadunidense e como possibilidades para pesquisas futuras, surgem a possibilidade de se aprofundar na doutrina estadunidense ou em sua evolução ao longo do tempo, nas capacidades de pessoal e de material existentes nos dois países ou nas individualidades existentes nas Forças Armadas do Brasil.

Palavras-chave: Defesa Cibernética. Doutrina Militar de Defesa Cibernética. *Cyberspace Operations*. 2ª Guerra do Golfo. Iraque.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

C^2 –	Comando e Controle
DOD –	*Department of Defense,* Departamento de Defesa dos EUA.
DODIN –	*Department of Defense Information Network*, Rede de Informações do departamento de defesa dos EUA.
DOS –	Denial of Service, negação de serviço
EUA –	Estados Unidos da América
EMCFA –	Estado-Maior Conjunto das Forças Armadas
MD –	Ministério da Defesa do Brasil
OTAN –	Organização para o Tratado do Atlântico Norte
RU –	Reino Unido
SIC –	Segurança da Informação e Comunicações
$SISMC^2$ –	Sistema Militar de Comando e Controle
$STIC^2$ –	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle
TI –	Tecnologia da Informação
TIC –	Tecnologia da Informação e Comunicações

SUMÁRIO

1 INTRODUÇÃO

A guerra tem se transformado ao longo do tempo, adaptando-se às evoluções e às descobertas da humanidade. Todos esses progressos, ao se associarem à busca do ser humano pelo poder, levaram a conflitos internos em Estados, a disputas entre nações e até mesmo a contendas de proporções globais, como a Primeira Guerra Mundial (1914-1918) e a Segunda Guerra Mundial (1939-1945).

Computadores, veículos autônomos, internet das coisas[1] e outros desenvolvimentos são algumas das mais recentes tecnologias que podem ser alvo dessas contendas na atualidade. O ser humano vem se superando a cada dia na busca por novas tecnologias, muitas das quais pensadas inicialmente para serem empregadas no meio militar, e os desenvolvimentos cibernéticos[2] não são uma exceção.

Tais mudanças associadas à tecnologia geraram quebras de paradigma e novos estilos de relacionamento na sociedade. Pessoas deixam de ter rosto para ter várias identidades, atores internacionais deixam de ter bandeira ou Estado associado e fronteiras deixam de existir, a fluidez financeira aumenta e a facilidade comercial também, graças a propensão de tudo estar interligado pela rede de computadores.

Assim, com novos estilos, novos tipos de vulnerabilidades, de dominação e de poder surgem neste novo mundo: o espaço cibernético ou mundo virtual que, além de uma proteção específica, demanda também custódia para seus efeitos no mundo real.

Com o objetivo de observar a evolução desses acontecimentos, buscar mais

---

[1] Internet das coisas – do inglês, *internet of things* (IOT) – sistema interrelacionado de dispositivos computacionais, equipamentos digitais e mecânicos, e objetos aos quais são vinculados UIDs (identificadores únicos de usuário) e que possuem a habilidade de transferir dados pela rede sem a necessidade de interação do tipo pessoa-pessoa ou pessoa-computador. (BRASIL, 2019, p. 28, alterado pelo autor para melhor compreensão).

[2] Entenderemos por *cibernético* a definição do Ministério da Defesa: o termo que se refere à comunicação e ao controle, atualmente, relacionado ao uso de computadores, sistemas computacionais, redes de computadores e de comunicações e sua interação. (BRASIL, 2014, p. 18).

conhecimento sobre o tema e acolhimento na doutrina nacional, propomo-nos a analisar a Segunda Guerra do Golfo (2003 – 2011), especificamente o período que antecedeu o conflito e os seus momentos iniciais em 2003, para responder ao seguinte questionamento: as ações cibernéticas sofridas e executadas pelos Estados Unidos da América (EUA) durante o conflito têm aderência ao modelo teórico da doutrina brasileira de defesa cibernética no que tange aos níveis de decisão, às ações da guerra cibernética e às funções operacionais?

Para confirmar a hipótese de que há aderência, utilizamos como metodologia a comparação entre a teoria e a realidade, e o estudo foi dividido em cinco capítulos. Sucedendo esta introdução, o capítulo dois versará sobre o fundamento teórico imprescindível à pesquisa, cuja base se estabelece na doutrina de defesa cibernética do Ministério da Defesa do Brasil (MD), corroborado pelos fundamentos de operações conjuntas dos EUA no espaço cibernético, por se tratar do Estado líder da coalizão que esteve no conflito.

No capítulo três, descreveremos as principais ações da guerra cibernética planejadas e executadas ou não por atores envolvidos no conflito ou por atores externos que se envolveram e que contribuíram com o resultado das interações. No capítulo quatro, é realizada uma comparação entre o caso real e o modelo teórico doutrinário, buscando confirmar ou não a hipótese proposta através de similaridades ou de divergências. Finalmente, no capítulo cinco, evidenciaremos as principais conclusões e o que não foi possível encerrar neste trabalho, gerando novas possibilidades de linhas de pesquisa que poderão ser desenvolvidas futuramente.

O assunto abordado é relevante por ser uma ameaça complexa e relativamente nova se comparada a outros modais de conflito, sendo isso reforçado pelo fato de que quem o domina garante vantagem tanto em relação aos que possuem tal capacidade quanto em relação à possibilidade de surpresa em termos de força, espaço ou tempo.

2 CONCEITOS DE GUERRA CIBERNÉTICA

Neste capítulo nos apropriaremos de parcelas das doutrinas brasileira e estadunidense acerca da guerra cibernética. A primeira servirá de base teórica para chegarmos a uma resposta ao nosso questionamento inicial e a segunda, de reforço comparativo por ser a regra seguida pelo Estado líder da coalizão que se fez presente no conflito usado como exemplo.

Em geral, conceitos, teorias e leis cibernéticas variam de acordo com a alta política e as experiências de um país, que estabelece as leis as quais será submetido o ciberespaço, como descreve Mohan Buvana Gazula[3], em sua dissertação de mestrado para o *Massachussetts Institute of Technology* (MIT):

> [...] a aplicação de regras, conceitos e terminologia legais preexistentes a uma nova tecnologia pode acarretar certas dificuldades, tendo em vista as características específicas da tecnologia em questão. Aparentemente estamos nessa difícil janela deslizante de decisão de quais leis governamentais internacionais se aplicam à guerra cibernética e quanto dela realmente se aplica. O ciberespaço é agora considerado um assunto de alta política devido a questões como segurança nacional, instituições centrais e sistemas de decisão críticos para o Estado, seus interesses e seus valores subjacentes. (GAZULA, 2017, p. 14, tradução nossa[4]).

Por essa razão, balizaremos nossa pesquisa nos conceitos do MD. Como o objeto de estudo apresentado não contou com o emprego de tropas brasileiras, mas da coalizão dos dispostos[5], composta em sua maioria por países membros da Organização do Tratado do Atlântico Norte (OTAN) e liderada pelos EUA, alguns conceitos estadunidenses também serão acrescentados ao longo do trabalho, sendo objeto de comparação secundária nas seções

---

[3] Mohan Buvana Gazula, Mestre em Ciência da Computação pela Universidade de Boston, graduou-se em seu segundo mestrado pelo *Massachussetts Institute of Technology* (MIT) em 27 jun. 2017, tendo aprovada sua tese comparativa de estudo de casos intitulada *Cyber Warfare conflict Analysis and Case Studies* (Análise e Estudo de casos de conflitos da guerra cibernética). (GAZULA, 2017, p. 1, tradução nossa).

[4] No original: [...] *applying pre-existing legal rules, concepts and terminology to a new technology may entail certain difficulties in view of the specific characteristics of the technology in question. It seems apparent that we are in that difficult sliding window of deciding which international governing laws apply to cyber-warfare and how much of it really applies. Cyberspace is now considered a subject of high politics due to matters such as national security, core institutions and decision systems critical to the state, its interests and its underlying values.* (GAZULA, 2017, p. 14).

[5] *The Coalition of the willing*, termo original em inglês batizado pela administração do presidente dos EUA George W. Bush. (GORDON; TRAINOR, 2006, p. 54).

seguintes.

Assim sendo, a seção será subdividida em duas partes, sendo a primeira destinada aos conceitos brasileiros de defesa cibernética e a segunda aos conceitos estadunidenses.

2.1 CONCEITOS BRASILEIROS

Primeiramente, abordaremos cada um dos níveis de decisão e suas responsabilidades para posteriormente resumir os princípios de emprego mais relevantes, suas características, possibilidades e limitações, bem como as formas de atuação cibernética e os tipos de ações cibernéticas.

O Estado brasileiro, dependendo do nível de decisão, designa ações e responsabilidades para distintos setores subordinados, tendo até mesmo sua nomenclatura diferenciada. Porém, a título de padronização, usaremos o termo "defesa cibernética" durante a pesquisa, independentemente do nível, quando tratarmos de ações brasileiras, pois, segundo o Manual de Defesa Cibernética (BRASIL, 2014), é o mais abrangente e seus conceitos são aplicáveis no contexto de guerra cibernética.

O MD, no referido manual (BRASIL, 2014), adota a seguinte divisão de níveis decisórios: o político, o estratégico, o operacional e o tático, cujas responsabilidades, graficamente representadas na FIG. 1, são assim mencionadas:

a) Nível Político: sob coordenação da Presidência da República, os esforços se voltam para a Segurança da Informação e Comunicações[6] e Segurança Cibernética[7];

b) Nível Estratégico: os esforços do MD, do Estado-Maior Conjunto das Forças

---

[6] Segurança da Informação e Comunicações (SIC) – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e informações. (BRASIL, 2014, p. 19).

[7] Segurança Cibernética – arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas. (BRASIL, 2014, p. 19).

Armadas (EMCFA) e dos Comandos das Forças Armadas se voltam para a Defesa Cibernética[8];

c) Níveis Operacional e Tático: os esforços das forças componentes se concentram na Guerra Cibernética[9].

Estabelecidos os níveis e suas responsabilidades, abordaremos os princípios de emprego da defesa cibernética a seguir.

2.1.1 Princípios de Emprego de Defesa Cibernética

O tempo é um dos responsáveis pela evolução e as campanhas militares não escapam de sua ação. Seja na doutrina de defesa do Brasil ou nas doutrinas internas das forças armadas, os princípios seguiram estudos e evoluções propostas pelas lições aprendidas em combates próprios ou de outros países, buscando melhorar os resultados. O surgimento da tecnologia e dos meios cibernéticos pode não ter afetado os princípios de defesa militar, mas, como escrito no manual do MD (2014), alguns deles são relevantes na defesa cibernética:

a) Princípio do Efeito: as ações produzem efeitos que se convertem em vantagem que consequentemente afetam a realidade;

b) Princípio da Dissimulação: busca-se esconder os rastros de quem executou a ação;

c) Princípio da Rastreabilidade: as ações podem e devem ser rastreadas conforme

---

[8] Defesa Cibernética – conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, 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).

[9] Guerra Cibernética – corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle (C^2) 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 ($STIC^2$) do oponente e defender os próprios $STIC^2$. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2014, p. 19).

os registros nos sistemas de tecnologia de informação;

d) Princípio da Adaptabilidade: a capacidade de se adaptar à mutabilidade constante dos meios tecnológicos e do espaço cibernético.

Tais princípios nortearão os aspectos a serem analisados; e, uma vez citados, passaremos agora às características da defesa cibernética.

2.1.2 Características, possibilidades e limitações da Defesa Cibernética

Ainda na doutrina brasileira, o MD cita algumas características específicas que diferenciam o modal cibernético da atrição cinética dos conflitos, dentre as quais podemos destacar a insegurança latente, que afirma que nenhum sistema é totalmente seguro e que tem vulnerabilidades (BRASIL, 2014).

O alcance global e a vulnerabilidade das fronteiras geográficas são características ligadas e correlatas que versam sobre a possibilidade das ações ocorrerem simultaneamente em diversas frentes e locais no mundo, visto que as ações cibernéticas não se limitam a fronteiras geográficas. A mutabilidade mostra a imprevisibilidade das ações no meio cibernético, que se alteram constantemente para surpreender o alvo (BRASIL, 2014).

Além das anteriores, a incerteza e a dualidade, geradas pelas diversas variáveis que afetam os sistemas de computadores, nos quais a mesma ferramenta pode ser usada por atacantes e defensores para propósitos diversos, também afetam o ambiente operacional cibernético assim como o paradoxo tecnológico, ou seja, quanto mais tecnologia uma força possui mais dependente dos sistemas ela está e, consequentemente, uma maior quantidade de sistemas pode ser exposta a vulnerabilidades (BRASIL, 2014).

Ainda nessa linha das características, as ações levam o atacante a sofrer com o dilema da descoberta de uma vulnerabilidade, pois, ao mesmo tempo em que contribui com a segurança de seus sistemas ao divulgar a falha, perde a possibilidade de explorar o sistema

inimigo. Porém, não podemos esquecer que as ações cibernéticas não são um fim em si mesmas, prestando-se à assessoria e ao apoio a outros tipos de operações (BRASIL, 2014).

Por fim, uma característica também citada é a assimetria, a qual se destaca pela inserção de um método capaz de superar barreiras e obstáculos físicos que poderiam impedir o acesso às potências mais poderosas. A assimetria dá capacidade de vencer o desbalanceamento das forças no terreno ao causar danos em inimigos cujas ações simétricas não teriam efeito (BRASIL, 2014).

Tais características moldam as operações cibernéticas e as diferem das demais operações de atrição, delineando possibilidades de defesa cibernética bem como limitações. Entre as possibilidades temos: efetuar ações ofensivas, defensivas ou exploratórias; produzir conhecimento; atingir infraestruturas críticas remotamente; cooperar com a segurança cibernética nacional ou com a mobilização quando solicitado; obter a surpresa explorando vulnerabilidades; realizar ações assimétricas atingindo oponentes mais fortes com um custo baixo em relação aos outros modais (BRASIL, 2014).

Já entre as limitações temos a dificuldade de identificar e de acompanhar: a origem dos ataques; as vulnerabilidades nos sistemas; os talentos humanos; a evolução tecnológica (BRASIL, 2014). Por conta disso, somos surpreendidos e, por vezes, não contamos com a iniciativa nas ações por conta da evolução constante dos sistemas e da dificuldade de manter o recurso humano envolvido atualizado em relação às atividades cibernéticas. O conjunto de possibilidades e de limitações somados às características específicas de defesa cibernética nos levarão às formas de atuação cibernética que o Brasil optou por utilizar.

2.1.3 Formas de atuação e ações cibernéticas brasileiras

A atuação cibernética, assim como outras, é realizada em conjunto e em prol de um esforço maior da campanha. Os planejamentos em cada nível decisório e as ações vão variar

conforme contexto, tempo disponível para preparação, nível tecnológico empregado e a ser enfrentado, sincronização entre agentes, entre outros (BRASIL, 2014).

Ainda segundo a doutrina, as atuações cibernética, política e/ou estratégica ocorrem desde os tempos de paz buscando atingir os objetivos de seus respectivos níveis de decisão em apoio a outra operação, seja ela de informação ou de busca de dados de inteligência. Já a cibernética operacional ou a tática ocorrem em operações de nível decisório mais baixo contribuindo para atingir o efeito desejado (BRASIL, 2014).

O QUADRO 1, ANEXO D, correlaciona as formas de atuação e os critérios descritos anteriormente de acordo com os níveis de decisão, o que nos auxilia a compreender e a classificar os tipos de ações que ocorrem para, então, reagir prontamente de acordo com as técnicas mais atuais de defesa cibernética.

Conhecidas as formas de atuação cibernética brasileira, os princípios e as características, com suas possibilidades e limitações, passaremos a ressaltar o que a publicação nacional classifica como os tipos de ações cibernéticas, isto é: ataque cibernético, proteção cibernética ou exploração cibernética (BRASIL, 2014).

O ataque cibernético é a ação executada que degrada, interrompe, nega, corrompe ou destrói as informações dos opositores ou os sistemas que as contenham. A proteção cibernética, por sua vez, neutraliza ações cibernéticas contra nossas informações ou sistemas que as contenham, melhorando a segurança dos meios e das informações neles contidas, seja em tempos de crise ou de conflito, sendo necessário que se mantenha permanentemente no tempo. Já a exploração cibernética visa a busca ou a coleta de dados nos sistemas-alvo para produzir conhecimento ou identificar vulnerabilidades sem deixar rastros e contribuir para uma consciência situacional do espaço cibernético ou área-alvo (BRASIL, 2014).

A classificação por tipos contempla todas as ações conhecidas atualmente, mas, somadas as capacidades e limitações, ainda falta terem utilidade dentro do planejamento do

escalão superior. Por essa razão, faz-se necessário buscar os conceitos de funções operacionais e correlacioná-los às ações cibernéticas.

Face ao exposto, conseguimos expor os princípios, as características, as formas e as ações específicas da Defesa Cibernética adotados pelo governo brasileiro dentro de seus níveis de decisão para futuramente confrontá-los com uma ação real. No entanto, antes precisamos comprovar se esses conceitos têm amparo e similaridades com as teorias seguidas pelas tropas que executaram as ações do evento real. Por essa razão, seguiremos com o detalhamento de alguns dos seus conceitos.

2.2 CONCEITOS DA COALIZÃO

Como já mencionado, as tropas que foram empregadas na Segunda Guerra do Golfo não foram as brasileiras mas as participantes da coalizão dos dispostos, ou seja, as tropas da Austrália, Reino Unido (RU), Polônia e EUA, lideradas por este último. Sendo assim, cabe ressaltarmos os conceitos mais importantes para compreendermos melhor se as ações foram as previamente estabelecidas ou se foram ações inovadoras que geraram ou não alterações na doutrina, consequentemente verificar se há ou não aderência à doutrina brasileira.

Como a OTAN não possui um manual específico sobre guerra cibernética, utilizaremos nesta pesquisa o manual de operações conjuntas das forças armadas estadunidenses, uma vez que o país foi líder da coalizão.

2.2.1 Autoridades e Responsabilidades

Em sua dissertação, Gazula (2017) explicita que as responsabilidades e as autoridades na questão cibernética emanam do mais alto nível de decisão, assim como nas normas brasileiras. Da mesma forma, a Estratégia Cibernética Nacional estadunidense (THE

WHITE HOUSE, 2018) corrobora tal pensamento ao indicar um órgão atrelado ao nível político, o Conselho Nacional de Segurança dos EUA, como responsável por defender seu território ao proteger redes, sistemas, funções e dados; promover a segurança econômica e a crescente inovação; preservar a paz e a segurança aumentando a habilidade estadunidense em parceria com países aliados e detendo criminosos e terroristas virtuais; além de expandir uma doutrina conjunta de uso da internet que seja aberta, confiável, operável pelas forças e segura.

Além disso, o manual de operações conjuntas no espaço cibernético (EUA, 2018) diz que a autoridade para operações cibernéticas militares deriva da Constituição Nacional dos EUA. Já as autoridades específicas para operações cibernéticas militares são estabelecidas pelas políticas emanadas pelo Secretário de Defesa, incluindo instruções, diretrizes e memorandos do Departamento de Defesa dos EUA (DOD)[10], bem como diretivas de operações e exercícios, autorizados pelo Presidente da República ou pelo Secretário de Defesa, e ordens subordinadas emitidas por comandantes aprovados para executar as missões do assunto.

As missões militares e as ações relacionadas às forças que atuam no espaço cibernético também são listadas pelo manual de operações conjuntas, sendo nomeadas por este como atividades principais das operações no espaço cibernético, independentemente do tipo de autoridade sob a qual são executadas. Tais operações serão tema das próximas subseções.

2.2.2 Principais Operações no Espaço Cibernético

Toda operação cibernética tem um impacto que pode gerar oportunidades para aliados, fazendo com que ganhem ou mantenham vantagem operacional ou em questões financeiras e até mesmo afetando a segurança física do alvo. As operações cibernéticas não respeitam fronteiras geográficas, buscando sempre estruturas críticas que afetem o comércio,

[10] No original: "*Department of Defense*" (tradução nossa).

governo e defesas do alvo. Por isso, ao decidir pelo emprego de operações cibernéticas, os efeitos colaterais devem ser analisados e considerados pelo escalão político, mas as operações e táticas são desenvolvidas pelos níveis operacionais e táticos.

Apesar da possibilidade de terem resultados expressivos sozinhas, as operações cibernéticas são mais efetivas se ocorrerem sincronizadas e em proveito de uma operação principal. Somado a isso, o fato de não ser possível se obter superioridade cibernética e realmente saber se o ator cibernético é estatal ou não estatal exige que os comandantes se preparem para decisões complexas e planejamentos que talvez nunca serão executados por conta de decisões políticas e consequências que podem não ser aceitas por aquele nível de decisão (EUA, 2018).

Face ao exposto, a literatura divide o espaço cibernético em três camadas em que as operações ocorrem, a física, a lógica e a da pessoa cibernética, as quais podem ser mais bem visualizadas de maneira gráfica na FIG. 2 (EUA, 2018).

A Camada Física é composta pela infraestrutura e pelos equipamentos físicos de armazenamento, transporte e processamento de informação que requerem segurança física própria. Essa é uma parte que deve ser considerada, pois a localização desses equipamentos podem interferir no planejamento por envolverem entidades públicas ou privadas do Estado-alvo ou até mesmo de outros Estados (EUA, 2018).

A camada lógica é formada por componentes abstratos que não existem fisicamente, como aplicativos, dados, processos, entre outros que, por sua natureza de localização múltipla, só podem ser engajados com uma grande capacidade cibernética, ou seja, uma boa combinação de *software*[11], *firmware*[12] ou *hardware*[13] projetados especificamente para afetar o espaço

---

[11] *Software* – Qualquer programa de computador, especialmente para uso com equipamento audiovisual. (MELHORAMENTOS, 2020).

[12] *Firmware* – Conjunto de programas de computador que controla ou opera um dispositivo que já vem gravado na memória permanente e integrado àquele dispositivo. (MELHORAMENTOS, 2020).

[13] *Hardware* – Conjunto dos componentes físicos de um computador. (MELHORAMENTOS, 2020).

cibernético (EUA, 2018).

A camada da pessoa cibernética[14] é a rede ou a conta de usuário, seja ele humano ou automatizado em seus contatos cibernéticos. Nesse conceito, é possível que um indivíduo crie inúmeras pessoas cibernéticas, o que dificulta a atribuição de responsabilidade de ações do mundo virtual para o mundo real. Várias ações de inteligência e de análise desses dados são necessárias para identificar o usuário ou o autor real das ações.

Além dessas subdivisões do espaço cibernético, podemos observá-lo por meio da lente da propriedade ou da localização, no sentido de estar ou não sob sua proteção, facilitando o conhecimento dos protocolos utilizados aos planejadores. A literatura o divide em: *Blue Cyberspace, Red Cyberspace* e *Gray Cyberspace*[15] (EUA, 2018).

O *Blue Cyberspace* é representado por áreas cuja proteção é de responsabilidade dos EUA ou de países aliados. Nesse espaço se encontra a Rede do Departamento de Defesa, tanto a classificada quanto a não classificada, doravante chamadas de NIPRNET[16] e SIPRNET[17]. O *Red Cyberspace* é assim classificado por ser de propriedade ou controlado pela força adversária, enquanto o *Gray Cyberspace* é o conjunto de espaços que não se classificam nem como azul nem como vermelho (EUA, 2018).

Assim como as descrições dos tipos de espaços operacionais, há uma descrição dos tipos de ameaça no manual estadunidense: ameaças estatais; ameaças não-estatais; ameaças individuais ou de pequenos grupos; acidentes e perigos naturais (EUA, 2018).

As estatais se configuram como a maior ameaça, pois o Estado tem acesso a recursos, pessoal e tempo que podem não estar disponíveis a outros atores. Já as não-estatais

---

[14] Em inglês: *Cyber-persona layer*. (EUA, 2018, p. I-4, tradução nossa).
[15] Em português: Espaço cibernético azul, espaço cibernético vermelho e espaço cibernético cinza. (EUA, 2018, tradução nossa).
[16] *Non-classified Internet Protocol Router Network* (NIPRNET) – rede interna do Departamento de Defesa dos EUA não classificada. (EUA, 2018, p. I-4, tradução nossa).
[17] *SECRET Internet Protocol Router Network* (SIPRNET) – rede interna secreta do Departamento de Defesa dos EUA. (EUA, 2018, p. I-4, tradução nossa).

são representadas por organizações formais ou não, que não se limitam por fronteiras nacionais, entre as quais estão organizações não governamentais (ONG) e organizações criminosas, terroristas ou extremistas. Elas usam o espaço cibernético para levantar fundos, recrutar pessoal, organizar operações, comunicar-se, espionar, atacar a reputação de autoridades ou Estados, entre outras ações (EUA, 2018).

As individuais ou de pequenos grupos se referem às ameaças, que, como o próprio nome diz, são realizadas por pequenos grupos ou até mesmo por uma única pessoa devido à facilidade da tecnologia e dos equipamentos disponíveis; desse modo, aproveitam-se de vulnerabilidades para adquirir informações ou dados. Normalmente tais ameaças são usadas por organizações maiores para se esconderem como organização ou Estados (EUA, 2018).

Os acidentes ou perigos naturais são ameaças do cotidiano, pois as infraestruturas do espaço cibernético são afetadas constantemente por erros do usuário, problemas com a prestadora de serviços, acidentes industriais ou desastres naturais. Por serem imprevisíveis, têm um impacto maior e sua recuperação pode requerer uma maior coordenação ou a utilização de sistemas reservas (EUA, 2018).

Além das ameaças citadas acima, o manual dos EUA (2018) cita outras dificuldades que afetam as operações cibernéticas, entre as quais estão o desafio do anonimato, da geografia, da tecnologia e da dicotomia entre indústria privada e infraestrutura pública; pontos que podem ser equiparados às limitações previstas na literatura brasileira.

Sobre o anonimato ou a atribuição de responsabilidade, existe uma dificuldade quando não se pode atribuir a responsabilidade pela ação no espaço cibernético a um Estado, pessoa ou grupo. A incerteza demanda uma análise adequada e até mesmo coordenação internacional para identificar a autoria e, posteriormente, decidir como responder (EUA, 2018).

Já em se tratando da geografia, o ambiente virtual não se limita por ela e, como as ações são remotas, não há uma certeza da localização e, consequentemente, de um possível

dano colateral que pode afetar tanto uma zona azul quanto vermelha ou cinza (EUA, 2018).

Em termos de tecnologia, há a exploração de vulnerabilidades e a consequente atualização para evitar que se propague. Nos casos, dois pontos se contrapõem: a quantidade de tecnologia similar que facilita a exploração dessa vulnerabilidade enquanto ela existir e a dicotomia entre avisar sobre a vulnerabilidade e perder a possibilidade de explorá-la ou não a divulgar e manter uma possibilidade ao seu alcance (EUA, 2018).

Outro desafio é a terceirização de serviço e de capacidade tecnológica que leva à dicotomia entre serviço privado e infraestrutura pública, pois, ao se utilizar a estrutura de nuvem disponibilizada por empresas terceirizadas, existe uma perda de autoridade direta, que leva a um aumento no mapeamento de vulnerabilidades e de contingências (EUA, 2018).

Com base no exposto, a globalização gera uma dependência ainda maior de empresas para garantir uma confiabilidade e disponibilidade dos serviços, visto que a conectividade depende de fibra óptica, cabos submarinos, *backbones*[18] internacionais e outros aparelhos transmissores para conectar à rede mundial. Para mitigar tal dependência, uma atenção grande deve ser dispensada para assegurar as informações que trafegam no espaço cibernético, valendo-se de criptografia e de codificações para tráfego de mensagens.

Todos esses desafios e ameaças impostos às atividades cibernéticas levam a um planejamento complexo, que pode gerar várias possibilidades de operações. Por isso, para se atingir objetivos utilizando o espaço cibernético, é preciso considerar o máximo de variáveis possíveis e a pior hipótese dentre elas, evitando confrontar ameaças sem contingência prévia.

Uma vez que abordamos as operações, podemos prosseguir com as principais atividades que podem ser desenvolvidas por meio delas no ambiente cibernético, abordando suas classificações e relações com as funções operacionais.

---

[18] *Backbone* é um termo importado do inglês que significa espinha dorsal ou rede de transporte que, no espaço cibernético, refere-se à rede dielétrica ou subterrânea em fibra óptica, constituída por cabos que, em conjunção com equipamentos terminais adequados, permitem a disponibilização de canais de comunicação para serviços de transmissão de dados, voz e imagem. (MELHORAMENTOS, 2020).

2.2.3 Atividades Principais das Operações no Espaço Cibernético

O planejamento conjunto ou de coalizão segue um padrão estabelecido independentemente do tipo de operação, valendo-se de manuais de processo de planejamento combinado ou de conjuntos específicos[19], mas as atividades são definidas de acordo com cada país e com sua experiência.

As operações cibernéticas têm como propósito inicial alcançar objetivos no espaço cibernético ou por meio dele, porém, antes de executá-las, comandantes devem observar consequências, impactos ou danos colaterais que podem gerar. Na doutrina estadunidense (EUA, 2018), tais operações são orientadas por políticas do DOD para facilitar ou iniciar novas operações consideradas atividades virtualmente ativas[20], isto é, atividades complementares, não listadas entre as operações militares no espaço cibernético, que usam o ambiente virtual para operações logísticas via *internet*, envio de *e-mail*, treinamento pela *internet* (EUA, 2018).

As operações militares cibernéticas estadunidenses se dividem em missões do espaço cibernético, ações do espaço cibernético ou contramedidas no espaço cibernético (EUA, 2018). As missões do espaço cibernético são o conjunto de exercícios, operações ou atividades iniciadas por uma diretiva oficial que, dependendo do objetivo e da autoridade que ordena, são categorizadas como operações da Rede de Informação do Departamento de Defesa (DODIN)[21], operações Defensivas do Espaço Cibernético (DCO)[2121] e operações Ofensivas do Espaço Cibernético (OCO)[21] (EUA, 2018).

As operações da DODIN têm como objetivo configurar, operar, assegurar, manter ou estender o espaço cibernético do DOD dos EUA. As DCO são missões executadas para

---

[19] Para o processo de planejamento conjunto, os EUA utilizam o JP 5-0, *Joint Planning*. (EUA, 2018, p. IV-1).
[20] No original: *Cyberspace-enabled activities*. (EUA, 2018, p. II-1).
[21] No original: DODIN, OCO e DCO são acrônimos para *Department of Defense Information Network*, *Offensive Cyberspace Operations* e *Defensive Cyberspace Operations,* respectivamente. (EUA, 2018, p. II-2, tradução nossa).

defender a DODIN ou outro espaço cibernético que esteja sob a sua responsabilidade, podendo se subdividir em defesa interna, ações de resposta ou defesa do espaço cibernético não pertencente ao DOD (*Non*-DOD). Já as OCO são missões que projetam poder em um espaço cibernético externo à DODIN em apoio a objetivos nacionais ou a um comando de operações em campo. A FIG. 3 exemplifica os tipos de operações e ações empregadas (EUA, 2018).

Dentre as operações do espaço cibernético, ainda existe a necessidade de se executar tarefas complexas e específicas que requerem conhecimento técnico atualizado para gerar efeitos no espaço cibernético, são elas: a segurança cibernética, a defesa cibernética, a exploração cibernética e o ataque cibernético (EUA, 2018).

Segundo o manual dos EUA (2018), as tarefas de segurança cibernética são ações realizadas dentro de espaço cibernético próprio para evitar acesso não autorizado, exploração, dano ao material ou à informação, garantindo ao sistema de informação disponibilidade, autenticidade, integridade, confidencialidade e aceitação. Como exemplo, podemos citar políticas de senha forte, de dados criptografados, restrição de acessos indevidos pela rede interna, entre outros.

As operações de defesa cibernética são realizadas em espaço cibernético próprio para se contrapor a ações adversas que rompem ou ameaçam romper medidas de segurança estabelecidas no espaço cibernético e têm como objetivo detectar, classificar, conter e mitigar tais ameaças. Se necessário, são efetuadas ações para reestabelecer uma configuração segura (EUA, 2018).

Já as de exploração cibernética são atividades de inteligência, coleta de informação ou outros dados necessários fora do próprio espaço cibernético para preparar operações futuras. Obter acesso a um sistema oponente e mantê-lo, mapear espaços cinzas e vermelhos e descobrir vulnerabilidades de um sistema são exemplos desse tipo de ação (EUA, 2018).

As de ataque cibernético, por sua vez, geram ou manipulam sistemas para causar

efeitos danosos. Diferente da exploração, as ações de ataque não se preocupam em manter o sigilo e apagar os rastros, buscam resultados perceptíveis pelo usuário ou pelo sistema adverso (EUA, 2018). As ações de ataque são subdivididas em: negação (DoS), que degradam parte do sistema (*Degrade*), o sistema todo por um período de tempo (*Disrupt*) ou de forma irreparável (*Destroy*); e manipulação, que controlam e alteram dados no sistema para gerar danos físicos por meio do ambiente cibernético cinza ou vermelho (EUA, 2018).

Algumas vezes as ações adversas não podem ser classificadas de imediato tamanha a sua complexidade, por isso podem ser chamadas de atividades maliciosas ou *malware*[22] e as que se contrapõem são normalmente chamadas de contramedidas, no espaço cibernético, e assim serão classificadas caso ocorram no caso real a ser apresentado.

Um último ponto da doutrina estadunidense que merece destaque em nossa pesquisa, para relacionarmos à doutrina brasileira e aos fatos ocorridos no caso a ser detalhado, são as funções operacionais relativas às operações cibernéticas. Esse conceito é bastante empregado na doutrina estadunidense e sofre atualizações constantes, como a recente inclusão do fator informações em sua lista.

Cabe ressaltarmos que a doutrina brasileira possui tais conceitos registrados no manual da Escola de Guerra Naval, mas eles ainda não estão plenamente integrados aos manuais de planejamento conjunto nem aos de defesa cibernética do MD. Assim, caso necessário, utilizaremos somente os conceitos do manual estadunidense, detalhados a seguir.

A primeira função listada no manual dos EUA (2018) é o Comando e Controle (C^2). Quando em operações militares, o C^2 está relacionado ao planejamento, comando e comunicações no suporte às decisões, ou seja, atividades virtualmente ativas ou de apoio, que, em operações cibernéticas, estão relacionadas ao uso dos sistemas de C^2 em proveito de ações

[22] *Malwares* são *softwares* maliciosos projetados para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de *software* costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. (BRASIL, 2019, p. 29).

a serem executadas buscando vantagens operacionais e redução do tempo de decisão com o uso da tecnologia.

Outra relevante, e que pode gerar confusão se não definida claramente, é a função fogos, pois, em guerra cibernética, refere-se ao dano criado na rede ou por meio dela após ações de ataque cibernético, podendo ou não gerar a destruição física do *hardware*, sistemas ou instalações (EUA, 2018).

Já a função movimento e manobra se refere ao deslocamento de forças e ao posicionamento em terreno só que no espaço cibernético; a projeção da força independe de deslocamento físico no terreno, mas de execução de ações ou de mudança de dados para outros locais lógicos ou físicos sem a obrigatoriedade de se movimentar o *hardware* ou os meios (EUA, 2018).

A logística remete ao apoio de material e pessoal em operações comuns, mas no espaço cibernético, significa a proteção das redes da DODIN e de redes comerciais que suportam a estrutura da tecnologia de informação (TI) das forças (EUA, 2018).

Outras funções como inteligência, proteção e informação também constam na literatura (EUA, 2018) e dizem respeito, respectivamente: às informações de apoio às operações de inteligência no espaço cibernético ou fora dele; à segurança e à defesa do espaço cibernético; à gerência e aplicação de informações para influenciar as decisões.

Uma vez que abordamos os conceitos das doutrinas brasileira e estadunidense em operações de defesa cibernética, passaremos a abordagem do caso real para, então, analisarmos a sua aderência a tais doutrinas, particularmente a brasileira.

3 AÇÕES DE GUERRA CIBERNÉTICA NA GUERRA DO GOLFO

Versaremos agora sobre as ações de defesa cibernética observadas na Segunda Guerra do Golfo. Algumas delas foram planejadas e executadas, outras não, e isso gerou efeitos positivos e negativos que afetaram o rumo do conflito. Para compreendermos as ações e seus objetivos, portanto, devemos fazer uma contextualização do confronto, abordando aspectos do conflito anterior e da evolução da tecnologia da informação. Assim sendo, cremos ser importante relembrar fatos da Primeira Guerra do Golfo (1990-1991), bem como algumas evoluções históricas no período.

3.1 FATOS PRÉVIOS RELEVANTES

Conforme a afirmação de Gazula (2017), os EUA se aproximaram do Iraque após a Segunda Guerra Mundial por medo da influência soviética sobre o Oriente Médio e da disseminação do comunismo em uma região cujo potencial energético e econômico do petróleo era de seu interesse. Somado a isso, ele acrescenta que a tensão na região, que deu início à guerra entre Irã e Iraque (1980-1988), gerou uma demanda de apoio estadunidense que aproximou ainda mais os dois países. Essa relação, no entanto, deixou de existir quando Saddam Hussein (1937-2006) usou a força e invadiu o Kuwait, causando o rompimento dos laços entre os países quando houve a operação Tempestade no Deserto[23] (GAZULA, 2017).

Além de citar a guerra, Gazula (2017) abordou o primeiro caso de vírus em sistemas de computadores no *Ames Research Center*, também conhecido como incidente com o Morris Worm[24], pontuando que as brechas encontradas à época persistiram até o início da operação Tempestade no Deserto com poucas atualizações nos mecanismos de defesa, permitindo aos

[23] *Desert Storm* era o nome em inglês.
[24] D. Fisher, H. Finger, W. Kramer, J. Stanley. Report of Computer Virus Incident at Ames. November 2-5, 1988.

invasores cibernéticos a exploração das mesmas vulnerabilidades (GAZULA, 2017).

Já segundo Fred M. Kaplan (1954 -), os oficiais de inteligência da coalizão não faziam ideia das capacidades militares do Iraque, somente o suficiente para iniciar um bombardeio. Assim, segue afirmando que foi necessário buscar conhecimento cibernético para apoiar a inteligência, evento considerado por ele como o primeiro experimento de contra C^2 de ambiente cibernético realizado com sucesso em uma guerra (KAPLAN, 2016).

Nesse experimento, os analistas de inteligência entraram na rede C^2 de Saddam Hussein e descobriram que os militares tinham implementado comunicações via fibra ótica entre Bagdá e Basra. Assim, descobriram, nas bases de dados das empresas que prestaram o serviço, a localização exata dos "*switches*", que se tornaram alvos perfeitos para os bombardeios iniciais da guerra (KAPLAN, 2016).

Tal ação retirou as comunicações iraquianas nos momentos iniciais e os obrigou a utilizar os meios reservas. Nesse ponto, mais uma vez os estadunidenses os surpreenderam, pois, como sabiam que a alternativa era a comunicação por micro-ondas, apontaram um satélite de interceptação de micro-ondas para captar as comunicações iraquianas e obter informações que garantissem a surpresa em seus ataques (KAPLAN, 2016).

Esses fatos deram à coalizão a possibilidade de efetuar ações e manobras em terra sem ser observada eletronicamente bem como de conhecer com antecedência os movimentos da tropa inimiga. Como consequência, Saddam Hussein perdeu sua impulsão no ataque, uma vez que passou a utilizar mensageiros em motos para levar suas mensagens e ordens, perdendo muito tempo com isso.

Apesar do sucesso do novo experimento, o exército dos EUA não estava tão interessado em tal forma de manobra. Seus principais líderes tiveram pouco ou quase nenhum contato com um computador e estavam acostumados com a "velha escola". Para eles, somente destruindo ou matando o alvo é que se cumpria a missão, conforme versa Kaplan:

> [...] os principais civis do Pentágono também estavam desconfiados. Tudo isso era muito novo. Poucos políticos ou altos funcionários conheciam a tecnologia; nem o presidente Bush nem seu secretário de defesa, Dick Cheney, jamais usaram um computador. [25] (KAPLAN, 2016, p. [46], tradução nossa).

Outra confirmação sobre essa preferência pela guerra de atrição foi a disputa entre bombardear uma torre de comunicações ou invadir o sistema e atacá-lo por meio de uma negação distribuída de Serviço (DDoS)[26]. A necessidade era de inviabilizar as comunicações por meio da torre por um período de 24 horas, sem necessidade de destruí-la ou de gerar efeitos colaterais, como a morte de civis. No entanto, como disse Kaplan (2016), os planejadores, por falta de certeza sobre a efetividade da ação, preferiram o bombardeio e a destruição da torre.

A efetividade das ações cibernéticas gerou certa desconfiança, principalmente em termos de danos colaterais. Em outra ação descrita, uma instalação militar era alvo e os militares de comando e controle sugeriram desabilitar eletronicamente o gerador que o alimentava. A ação parecia perfeita para provar as ideias de menor letalidade propostas, mas, ao analisar os danos colaterais, perceberam que o gerador também alimentava um hospital e que, mesmo sem utilizar nenhum armamento, poderiam matar vários civis que ali se encontravam em tratamento (KAPLAN, 2016).

Tal ponto de vista foi muito contrastado com os danos colaterais das ações de atrição, como o lançamento de bombas, pois, como dito anteriormente, existia essa previsão nas ações cibernéticas, como no caso do gerador que alimentava o hospital. No entanto, após realizar os bombardeios, os danos não só foram concretizados, como também já partiam de uma certeza de suas consequências.

Essas dúvidas sobre emprego do meio cibernético ou de ações físicas presenciais somadas ao crescimento mundial da *internet* e da tecnologia geraram dúvidas e suposições por

---

[25] No original: *[...] the Pentagon's top civilians were also leery. This was all very new. Few politicians or senior officials were versed in technology; neither President Bush nor his secretary of defense, Dick Cheney, had ever used a computer.* (KAPLAN, 2016, p. [46], tradução nossa).

[26] DoS – *Denial of service,* termo em inglês que significa negar o serviço prestado por algum meio tecnológico por meio de bloqueio de suas funcionalidades. (CLARKE, 2015, posição [1153]).

parte da mídia, que passou a atribuir a intervenções cibernéticas estadunidenses alguns dos resultados positivos (KAPLAN, 2016).

Como exemplo, temos a falha no sistema de defesa antiaéreo iraquiano, publicada pela revista *U.S. News & World* (SMITH, 2013) como uma ação de forças especiais estadunidenses. Na matéria, mencionava-se que os EUA inseriram uma impressora infectada no aquartelamento iraquiano, o que inviabilizou o funcionamento dos sistemas de controle do seu espaço aéreo. Por outro lado, a revista *Infoworld* fez menção ao evento AF/91 como uma "piada de 1º de abril". Fato é que o sistema de defesa antiaéreo iraquiano não funcionou, permitindo um melhor desenvolvimento da operação Tempestade no Deserto (GANTZ, 1991).

A Guerra do Golfo pode ter sido o primeiro exemplo do emprego de ações tecnológicas típicas de uma guerra cibernética, como cita o general José Carlos Albano do Amarante (19-? - 2016), reforçando que a prioridade nesses casos seria gerar informações em tempo real e negar essa possibilidade a outra parte. Por meio desse ponto de vista, observarmos um crescimento do emprego da tecnologia atuando em prol da guerra cibernética e, consequentemente, da guerra de informação (AMARANTE, 2010).

Com base no que foi observado, podemos concluir sumariamente que, durante a Primeira Guerra do Golfo, as ações cibernéticas se limitaram à negação do uso dos sistemas de informação e de levantamento de dados de inteligência. No próximo item, abordaremos as ações cibernéticas na Segunda Guerra do Golfo, especificamente no início do conflito, em 2003, e como os fatos e ações da guerra anterior a influenciaram positiva ou negativamente.

3.2 AÇÕES CIBERNÉTICAS NA SEGUNDA GUERRA DO GOLFO

Neste tópico abordaremos as ações da guerra cibernética que ocorreram na Segunda Guerra do Golfo, mais especificamente antes e durante a Operação Liberdade do Iraque, a qual doravante chamaremos pelo seu nome em inglês, "*Iraqi Freedom*".

Como observado na subseção 3.1, as ações cibernéticas amplificaram os efeitos das operações de informação na Primeira Guerra do Golfo e, como consequência, bem antes do início oficial da Segunda Guerra do Golfo, a mídia já especulava quais seriam as possíveis ações dos EUA. Como o Pentágono não passava informações claras aos jornalistas, estes disseminavam várias notícias atraentes sobre formas incomuns de ataques, como argumentado em um artigo para o site *Security focus* (SMITH, 2013).

A incerteza que a mídia tinha e divulgava era a mesma de vários membros da força conjunta da coalizão. O sigilo sobre os meios e as ações possíveis, de ataque e de defesa, era tanto que seus componentes não faziam ideia das possibilidades disponíveis para contribuir em suas operações (KAPLAN, 2016).

Segundo David Fulghum[27], em seu artigo para a revista *Aviation Week & Space Technology*, os problemas na preparação para a guerra envolviam a logística tradicional e os caprichos em torno da guerra cibernética. No artigo, podemos observar que os EUA tinham clara intenção de que houvesse tentativas de ações cibernéticas frustradas e efetivadas, as quais serão mencionadas ao longo desta subseção para posteriormente serem confrontadas com a teoria apresentada na seção 2 (FULGHUM, 2003).

Uma ação descrita por Fulghum (2003) foi a tentativa estadunidense de invadir a rede de comunicações militares do Iraque. Essa foi uma tentativa frustrada marcada pela soberba, porque, em um primeiro momento, a coalizão cria ser muito fácil penetrar a rede militar de computadores, mas, durante as tentativas, foi constatado que ela estava interligada à rede de telefonia e que ambas estavam desorganizadamente entrelaçadas com as redes civis, gerando uma barreira para se alcançar os objetivos estabelecidos.

Ainda segundo Fulghum (2003), a ideia era invadir a rede e conseguir os planos de

[27] David A. Fulghum é um colunista técnico e muito conhecido nos EUA na área de informática e tecnologia. Escreve para a revista *Aviation Week & Space Technology* desde 1995.

voo e rotas de aeronaves, planejamento dos componentes terrestres, entre outros documentos que garantissem vantagem ao ataque vindouro, porém os danos colaterais causados por um possível ataque cibernético à rede de computadores civis poderia não ser aceitável pelo nível decisório naquele momento.

Já de acordo com James Andrew Lewis (1953-), quando os estadunidenses iniciaram a Segunda Guerra do Golfo, os iraquianos estavam com medo de expor seus sistemas de comando e de controle, o que tornou seu ciclo decisório mais lento. Lewis também reforça a ação de envio de *e-mails* ao alto comando iraquiano solicitando que se rendessem, e isso também contribuiu para abalar a resistência iraquiana (LEWIS, 2010).

Haja vista o seu uso na Primeira Guerra do Golfo, a mídia já noticiava a possibilidade de emprego de ações cibernéticas antes mesmo do início do segundo conflito, com base em informações de solicitações do presidente George W. Bush (1946 -) sobre as diversas formas de organizar tais ataques, divulgadas no *Washington Post* e no *Deutsh Welle* (ACIKGÖZ, 2003).

Por conta da experiência adquirida e de outras ações que ocorreram no interregno entre a Primeira e a Segunda Guerra do Golfo, a defesa cibernética foi se fortalecendo e sendo cada vez mais explorada pelos EUA. Um exemplo foi o caso *Solar Sunrise* (1998)[28] quando *hackers* invadiram, inicialmente, o sistema operacional da guarda nacional estadunidense na base aérea de Andrews, nos EUA, e depois invadiram outras bases aéreas. Tal evento foi citado por Kaplan como um movimento inicial de guerra cibernética, provavelmente realizado por iraquianos, principalmente após membros da equipe de inteligência confirmarem que as ações partiram de servidores dos Emirados Árabes Unidos conectados ao Iraque (KAPLAN, 2016).

O *Solar Sunrise*, evento que posteriormente foi reivindicado por um adolescente de

[28] Termo inglês que significa “Nascer do Sol do SOLAR”, onde SOLAR representava o sistema operacional SOLARIS da empresa SUN (Sol em inglês) que tinha como base o UNIX 2.4 e 2.6 e que era utilizado pelos militares dos EUA. (KAPLAN, 2016, p. [126]).

Israel e dois da Califórnia, foi um dos acontecimentos que colaborou com a mudança de postura em relação ao emprego de ações cibernéticas em apoio às operações de informação, navais, aéreas e terrestres (CLARKE; KNAKE, 2015).

Uma outra ação planejada e não executada foi o bloqueio das contas bancárias de Saddam Hussein e do governo iraquiano. O Pentágono e as agências de inteligência estadunidenses planejaram congelar os recursos por meio de ataque cibernético. A ideia por trás da ação era fazer com que o Iraque e o seu ditador não tivessem recursos para sustentar uma guerra nem pagar suas tropas (MARKOFF; SHANKER, 2009).

Todo o planejamento foi efetuado e todas as ferramentas estavam disponíveis à época, mas o nível de decisão e as fortes regras de engajamento impostas pela administração do governo Bush limitavam as ações, principalmente após receberem a informação de que os efeitos colaterais não se limitariam ao Iraque, podendo gerar uma crise econômica que afetaria todo o Oriente Médio, espalhando-se pela Europa e chegando até mesmo nos EUA (MARKOFF; SHANKER, 2009).

Corroborando com o fato acima, Clarke (2015) cita que a pressão dos banqueiros mundiais para manter a suposta sensação de confiabilidade em seus sistemas de segurança ao redor do mundo reforçou a ideia da negação política a qualquer tentativa de ataque aos sistemas financeiros, mesmo que isso implicasse em uma ocupação que levaria à morte de cem mil iraquianos.

Outra ação executada, durante a *Iraqi Freedom*, cooperou com as ações de operações de informação, especificamente com operações psicológicas. O objetivo conjunto era levar informações aos líderes iraquianos e encorajá-los a abandonar o apoio que davam a Saddam Hussein. A parte cibernética se encarregou de descobrir os contatos e de efetuar a distribuição em massa de *e-mails*, de mensagens por fax e até de facilitar ligações para todos esses líderes a partir de aeronaves e navios que operavam no Golfo Pérsico (WILSON, 2007).

Essa ação tinha uma grande concorrente, a rede *Al Jazeera*, que tinha a capacidade de distribuir mensagens a favor dos terroristas para até 35 milhões de telespectadores ao redor do mundo. Tal competição não reduziria o poder ou o espaço cibernético dos EUA, mas deixaria de influenciar nas informações, a menos que desenvolvessem uma estratégia combinada de comunicações contra a competitividade da mídia civil (WILSON, 2007).

Ainda durante a Operação *Iraqi Freedom*, os estadunidenses e as forças de coalizão, repetidas vezes, deixaram de executar ataques contra redes de computadores ou sistemas iraquianos. Mesmo havendo planos detalhados, havia a necessidade de aprovação por um nível elevado de decisão que, por sua vez, necessitava de garantias de que os efeitos colaterais se limitariam ao Iraque e que civis ou países neutros não teriam seus serviços interrompidos (WILSON, 2007).

A revista *Information Management & Computer Security* revelou que nas primeiras 48 horas de conflito, mais de 1000 sites da internet foram invadidos e reconfigurados para incorporar mensagens contra o conflito, um ataque comumente chamado de *Bait and switch*[29]. Na ação, os sites dos EUA foram os que mais sofreram, chegando a registrar 5.646 ataques contra 4.365 ao opositor, segundo reportou a empresa *mi2g* (CYBER, 2003).

A revista cita ainda que a rede *Al-Jazeera* também sofreu ataques do tipo DoS, prevenindo que tanto a sua versão em árabe quanto a em inglês fossem acessadas. A rede de notícias ainda passou por um ataque do tipo *hijack,* tendo seu domínio desviado para um computador que não pertencia à rede de notícias. Nesse segundo ataque, os usuários eram levados a uma página com a bandeira estadunidense e as palavras *Let freedom ring*, seguida da mensagem *hacked by patriot, freedom cyber militia*[30]. A ação não foi bem aceita pela coalizão,

---

[29] *Bait and Switch* – em português, propaganda enganosa. Ação que substitui o conteúdo de um site por informação não autorizada, mas que os atacantes querem divulgar. (NordVPN, 2019).

[30] *Let freedom ring, hacked by Patriot, freedom cyber militia* – em português, significa "deixe soar a Liberdade, invadido pela milícia cibernética livre Patriota. (Information Management & Computer Security, 2003, tradução nossa).

e o Centro de Proteção de Infraestruturas Nacionais (*National Infrastructure Protection Center* – NIPC) deixou claro que a atividade era ilegal e passível de punição (INFORMATION, 2003).

Essas ações deixam claro que houve um grande aumento em relação ao que ocorreu na guerra anterior e abrem uma porta para que os conflitos seguintes explorem bastante a nova forma assimétrica de conflito, uma vez que pode gerar consequências informacionais ou físicas sem envolver efetivo ou baixas.

Nesta seção, citamos as ações importantes na Segunda Guerra do Golfo e assim temos condições de seguir nossa metodologia, comparando a teoria apresentada na seção 2 com os fatos apresentados na seção 3.

4 ADERÊNCIA ENTRE A TEORIA E A SEGUNDA GUERRA DO GOLFO

Nas seções anteriores, selecionamos alguns aspectos teóricos da guerra cibernética: nível de decisão, princípios da guerra cibernética, ações da guerra cibernética e funções operacionais. Abordamos também as ações que ocorreram na Segunda Guerra do Golfo em seus momentos iniciais, em 2003.

Observamos ainda as principais ações realizadas ou planejadas e não executadas durante o conflito em foco. A seguir, compararemos essas ações com os conceitos teóricos apresentados para então confirmarmos ou não a aderência da doutrina no conflito.

4.1 NAS LENTES DOS NÍVEIS DE DECISÃO

Nesta subseção analisaremos as diferentes ações da guerra cibernética que ocorreram no conflito buscando verificar a aderência aos níveis de decisão da doutrina brasileira.

A primeira ação, que tinha como objetivo influenciar o sistema de comunicações do alto comando iraquiano, foi planejada no nível tático com facilidade por se considerar que existiam os meios necessários para tal, mas foi frustrada no nível político ao se constatar que as redes de comunicação militares estavam interligadas às redes civis e que, além disso, não eram independentes das redes de outros países.

Considerando os níveis de decisão descritos na doutrina brasileira, tais limitações também emanariam do nível político, pois os danos colaterais poderiam demandar coordenações diplomáticas posteriores. Por essa razão, podemos considerar que a relação de tal ação com o nível de decisão tem aderência com a doutrina brasileira.

No que tange à segunda ação, de tentativa de invasão às redes de comunicação iraquianas pelas forças estadunidenses, observamos, mais uma vez, o planejamento pelo nível

tático sendo limitado pelas determinações do nível político, que não queria que as comunicações civis fossem influenciadas. Tais negações nas comunicações e serviços de internet poderiam ter efeitos nos países vizinhos que compartilhavam de tais tecnologias, podendo também demandar coordenações diplomáticas ou até mesmo dificultar o apoio de países vizinhos durante a operação. Por corroborar as alegações da ação anterior, podemos considerar que essa também demonstra uma aderência à doutrina brasileira, em que o nível decisório é o mais alto, o político.

O *Solar Sunrise*, apesar de não ter ocorrido no período delimitado, contribuiu para a mudança no emprego das ações cibernéticas, principalmente no nível de decisão, o qual passou a ser empregado em apoio às operações de informação e centralizado em ações conjuntas, forçando um protocolo no qual decisões sobre o tema passaram ao nível mais alto em relação a momentos anteriores.

Mais uma ação que expressa o mesmo resultado foi o planejamento frustrado de bloqueio às finanças de Saddam Hussein. Como citado, o efeito colateral atingiria proporções significativas que poderiam prejudicar inclusive a coalizão, pois a economia de países da Europa poderia ser afetada e, consequentemente, a estabilidade entre os membros da coalizão seria afetada por um "fratricídio cibernético". Sendo assim, foi um ato em que a decisão no nível superior, o político, foi uma solução acertada. Seria muita pretensão afirmarmos que, pela doutrina brasileira, decidiríamos de maneira igual, mas podemos afirmar que o caso seria, da mesma forma, levado ao nível decisório mais elevado, o político. Concluindo que também haveria, nesse caso, aderência à doutrina nacional.

As demais ações não tiveram mais evidências que pudessem ser analisadas para contribuir com este tópico, no qual concluímos que, se a doutrina nacional brasileira, expressa no manual do MD, fosse utilizada como referência em termos de níveis de decisão, haveria aderência no conflito analisado.

4.2 NAS LENTES DOS PRINCÍPIOS DE EMPREGO

Quanto aos princípios de emprego listados no item 2.1.1, as ações ocorridas podem ser analisadas sem, contudo, terem todos os princípios presentes. Assim, analisaremos quais princípios se destacam para, com isso, definirmos a aderência à doutrina nacional.

Na aquisição da lista de correios eletrônicos das autoridades iraquianas, o princípio do efeito se destaca ao produzir a consequência informacional necessária para as operações de informação. Já a dissimulação, a rastreabilidade e a adaptabilidade não foram observadas, visto que havia a intenção de se revelar quem realizou a ação em um ambiente sem capacidade de reação ou rastreamento; havendo assim aderência ao modelo nacional.

No ataque planejado contra a rede de comunicações, o princípio da adaptabilidade e do efeito se destacam, pois a não aprovação da ação por meio cibernético levou a ações cinéticas que tiveram seus efeitos em ambos os espaços: o físico e o cibernético. Isso corrobora com a doutrina nacional, ou seja, há aderência.

No planejamento de bloqueio das finanças iraquianas, a dissimulação se destaca, pois, em que pese a ação não ter sido autorizada, a exploração foi bem sucedida, todos os dados foram levantados e seus riscos e consequências mapeados sem que os administradores dos espaços cibernéticos verificados pudessem perceber a presença dos invasores estadunidenses, que não deixaram indícios de sua ação. Assim, há aderência doutrinária.

Quanto às ações de propaganda enganosa sofridas pelas redes de computadores externas ao DODIN, destaca-se a rastreabilidade. Em que pese a carência de fonte bibliográfica que comprove que os autores foram encontrados, muitos deles foram rastreados e mitigados, pois a manipulação e a movimentação de dados pôde dar clareza aos analistas de como se contrapor aos ataques. Podemos ainda dar relevância ao princípio do efeito porque as consequências dos ataques produziram efeitos no mundo real traduzidas em desvantagem para os EUA, o qual passava à população, fragilizada pelos atentados do 11 de setembro, mais

insegurança em relação à sua crescente dependência dos sistemas tecnológicos. Esses dois princípios têm aderência em nossa doutrina.

4.3 NAS LENTES DAS AÇÕES CIBERNÉTICAS

Uma vez analisados os níveis de decisão e os princípios, discorreremos sobre as ações cibernéticas observadas no conflito, classificando cada uma conforme o manual do MD (2014) e, caso necessário, agregando detalhes referentes à doutrina estadunidense.

Cabe ressaltarmos que existe aqui uma diferença entre a doutrina dos EUA e a do Brasil. Conforme podemos observar, novamente, na FIG.3, os estadunidenses consideram a classificação das ações de acordo com o espaço cibernético, seja ele interno ao DODIN, externo defensivo, o DCO, ou externo ofensivo, o OCO, enquanto os brasileiros somente consideram as ações como ataque, proteção ou exploração cibernética.

Feito este enquadramento teórico, depreende-se que a aquisição da lista de correios eletrônicos das autoridades iraquianas se tratou de uma exploração cibernética para contribuir com operações psicológicas dentro de um contexto de operações de informação, o que possui aderência à doutrina brasileira.

Já o ataque planejado contra a rede de comunicações não foi executado por meios cibernéticos, mas por ações cinéticas. Dessa forma, podemos citar um emprego misto de ações cibernéticas do tipo exploração, no sentido de obter dados e locais necessários para interromper determinadas comunicações e, de posse dos dados, realizar um bombardeio que culminasse com a destruição dos meios físicos que proporcionavam tais comunicações. A integração não fica tão clara no manual de defesa cibernética, mas pode ser efetivada nos processos de planejamento conjunto e suas publicações basilares que, neste trabalho, não foram exploradas. Sendo assim, analisamos que há aderência parcial dada a falta de clareza do documento.

O planejamento de bloqueio das finanças iraquianas também se enquadra como

exploração cibernética que poderia evoluir para ataque cibernético caso fosse autorizado pelo nível político. Cabe a ressalva de que a autorização, na doutrina dos EUA, não ocorreu porque interferiria no *Gray Cyberspace*, ou seja, no espaço cibernético que não pertence às forças amigas nem às opositoras. Como essa classificação não existe na norma brasileira, podemos considerar que houve aderência parcial.

Referente aos ataques de propaganda enganosa, sofridos pelas redes de computadores externas ao DODIN, mas pertencentes ao *Blue Cyberspace* dos EUA, a doutrina nacional não contempla ações de proteção cibernética que podem ser realizadas em apoio a empresas nacionais ou mídias nacionais que sofram ataques e que comprometam indiretamente nossas operações de informações. No item 2.2.3, observamos que os EUA classificam tal espaço cibernético como *Non*-DOD, possuindo protocolos específicos para defesa e segurança desses meios, uma vez que, além do citado, o ataque poderia envolver empresas intermediárias nas comunicações, como os *backbones* internacionais. Assim, consideramos que nesse ponto não houve aderência na doutrina do Brasil.

Já a ação do grupo não estatal *Patriots* não foi uma ação oficial da coalizão tampouco aceita por ela, mas que lhe gerou benefícios ao bloquear notícias desfavoráveis da rede *Al-Jazeera*. Ações desse tipo, que contribuem com as ações das linhas de esforço das operações, não são contempladas em nenhuma das doutrinas, embora estejam se tornando cada vez mais comuns. Portanto, não possuem aderência em nossa doutrina.

4.4 NAS LENTES DAS FUNÇÕES OPERACIONAIS

Por fim, analisaremos as diferentes ações cibernéticas que ocorreram no conflito sob o enfoque das funções operacionais. Como bem discorremos na seção 2, a doutrina estadunidense é mais detalhada ao classificar as ações da guerra cibernética de acordo com as funções operacionais. A doutrina brasileira possui essa classificação nos conceitos internos de

cada força singular, mas não a correlaciona com as ações da guerra cibernética em nível conjunto. Por isso, faremos a comparação somente com base na doutrina estadunidense.

Para a aquisição da lista de correios eletrônicos das autoridades iraquianas, a função C^2, inteligência, fogos e informações foram mais bem aproveitadas. Na C^2, ressaltamos a aquisição de informações para tomada de decisão precisa no tempo, o que deu vantagem temporal no ciclo decisório da coalizão. Na inteligência, o êxito na obtenção de informações do oponente. Na fogos, os danos informacionais e psicológicos gerados ao contendor com efeito sobre seu tempo de C^2 e de decisão. E, na função informações, o uso de dados coletados para influenciar as decisões tanto do decisor quanto do oponente. Com base nisso, podemos dizer que houve aderência à doutrina estadunidense.

No ataque planejado contra a rede de comunicações, a função fogos ficou evidenciada não no espaço cibernético, mas sim nas ações de atrição no espaço físico, que geraram um dano no espaço cibernético e, consequentemente, contribuíram com as ações cibernéticas de negação de uso.

Ao destruir o *hardware* inimigo, o C^2 e o movimento e manobra também foram afetados: o C^2 pela perda das comunicações do oponente, o que gerou a necessidade de uso dos meios alternativos de transmissão de dados e de ordens por outros sistemas de comunicação; enquanto o movimento e a manobra pela não necessidade de deslocar meios para a área de operações para realizar tal ação, feita remotamente. Assim sendo, podemos analisar que houve aderência à doutrina dos EUA.

No planejamento do bloqueio das finanças iraquianas, destacamos as funções C^2, inteligência, fogos e informações. As informações obtidas na exploração cibernética facilitaram a tomada de decisão, pois os danos colaterais levantados poderiam ser maiores que os aceitáveis pelo nível político; assim, cremos que houve aderência à doutrina.

Os ataques de propaganda enganosa no *Blue cyberspace* dos EUA têm relação com

as funções C^2, fogos, manobra e movimento, proteção, logística e informações. Quanto ao C^2 e informações, as lições aprendidas influenciaram o nível político a vislumbrar a possibilidade de proteção do ambiente cibernético externo ao DODIN, mas que pertença ao *Blue cyberspace* estadunidense.

Em relação às funções fogos e logística, houve danos externos ao DODIN que afetaram a população dos EUA gerando um efeito de desaprovação, como ocorreu na guerra do Vietnã (1955-1975) e em outros conflitos influenciados pela mídia. Isso demandou ações inter-relacionadas à função logística por haver uma dependência dos meios civis e, por conseguinte, à função movimento e manobra, pois houve a necessidade de se alterar o posicionamento de alguns servidores desses meios durante a resolução de problemas. Quanto à proteção, fica evidente que não foi possível estabelecer a proteção adequada por se tratar de ambiente *Non*-DOD, ainda assim a necessidade dessa atuação ganhou relevância, principalmente se envolvesse *backbones* intermediários, o que não foi o caso. Assim, consideramos que houve aderência à doutrina estadunidense.

Já a ação do grupo não estatal *Patriots*, o C^2 se destaca na ação da coalizão de reprovar publicamente as ações do grupo na mídia e de não as reconhecer como parte das operações. Fossem elas oficiais ou não, ficou claro na função informações que não havia vínculo entre eles. Quanto à inteligência e informações, as operações foram afetadas positivamente, pois contribuíram com um dos objetivos da operação ao bloquear notícias desfavoráveis veiculadas pela rede *Al-Jazeera*. Na função movimento e manobra, os dados foram alterados de local e, por conta disso, estão relacionadas entre si, mesmo não tendo sido uma operação da coalizão. Tal ponto também teve aderência na doutrina dos EUA.

Em todas as ações que ocorreram, portanto, as funções estiveram presentes corroborando com a ideia de que elas acontecem independentemente do tipo de operação. Seja guerra de atrição, de manobra ou cibernética, elas estão presentes nos conceitos estadunidenses

e em algumas publicações nacionais.

Face ao exposto, podemos considerar que houve aderência das funções operacionais à doutrina estadunidense, como foi pormenorizado nos parágrafos anteriores, porém, como já mencionado, não existe uma doutrina nacional no MD que verse sobre o tema de forma a abranger todos as dimensões da guerra. Assim, podemos concluir, por meio dessas lentes, que a doutrina nacional não teve aderência, surgindo uma oportunidade de melhoria quanto a possibilidade de analisar o planejamento conjunto e, posteriormente, o planejamento da defesa cibernética a partir desse ponto de vista.

5 CONCLUSÃO

Instados a refletir sobre as ações de guerra cibernética em um mundo cada vez mais dominado pela tecnologia e pelos meios digitais, buscamos analisar as ações cibernéticas ocorridas na Segunda Guerra do Golfo, especificamente nos momentos iniciais do conflito e no período que o antecedeu. Como amparo teórico, baseamo-nos na doutrina do MD brasileiro e na doutrina conjunta de guerra cibernética dos EUA, por ser o país líder da coalizão que atuou no conflito citado.

A escolha por analisar o uso de ações cibernéticas na Segunda Guerra do Golfo, bem como suas consequências, decorreu do pouco conhecimento inicial sobre o tema e pelo fato de ter gerado uma expectativa muito grande na mídia à época, o que pode ser um grande incentivo para o uso de tecnologia nos conflitos seguintes.

Para atingir o objetivo estabelecido, a pesquisa foi estruturada em três seções de desenvolvimento: o primeiro voltado à apresentação dos pontos mais relevantes das doutrinas usadas como base teórica; a seção seguinte voltada às ações empregadas na Segunda Guerra do Golfo, contextualizando ações empregadas anteriormente na Primeira Guerra do Golfo e no restante do mundo e tendo em vista a dificuldade de se referenciar ações cibernéticas ao espaço geográfico; finalmente, dedicamos uma seção para discorrer sobre o objeto de pesquisa à luz da teoria sugerida, buscando uma conclusão sobre a aderência ou não por meio de comparação.

Ao nos aprofundarmos na doutrina de defesa cibernética brasileira, na segunda seção, abordamos seus conceitos importantes e os complementamos com conceitos da doutrina estadunidense por se tratar do estado líder da coalizão que atuou na guerra citada. Observamos nos modelos teóricos as responsabilidades, conforme os níveis de decisão, as ações da guerra cibernética e as funções operacionais, listando também algumas características específicas, as possibilidades geradas por elas e as limitações encontradas. Constatamos que as funções operacionais aplicadas à guerra cibernética não poderiam ser mais bem exploradas pela escassez

de literatura do MD brasileiro que abordasse o assunto relacionado à doutrina de defesa cibernética; assim, o ponto em questão demanda estudos futuros.

Na seção três, aprofundamos o conhecimento acerca das ações cibernéticas durante a Segunda Guerra do Golfo, em 2003, entre a coalizão dos dispostos e o Iraque. Para tal, foi necessário relembrar as ações empregadas no conflito anterior, a Primeira Guerra do Golfo, no Kuwait, bem como alguns aspectos do desenvolvimento da internet e das ameaças que essa nova tecnologia trouxe aos conflitos, como o ataque AF/91 e o *Solar Sunrise*.

Na seção quatro, confrontamos as doutrinas consideradas como teoria com a realidade citada no capítulo anterior, quando, então, verificamos a aderência total quanto aos aspectos relacionados aos níveis de decisão das ações de defesa cibernética; a aderência parcial à doutrina quanto às ações, limitações e possibilidades dos eventos que ocorreram durante o conflito; e a impossibilidade de se analisar a doutrina brasileira, em virtude da inexistência de referencial teórico, no que tange ao enquadramento das funções operacionais na guerra cibernética.

Cabe ressaltarmos que, de acordo com as evidências destacadas, não foi possível realizar um detalhamento completo de todos os aspectos analisados no modelo teórico apresentado por crermos na falta de uma integralização dos conceitos de funções operacionais em todos os níveis de decisão.

Assim, podemos retornar ao questionamento inicial: a doutrina de guerra cibernética brasileira atual teria aderência na Segunda Guerra do Golfo? Certamente poderíamos, inicialmente, pensar em um anacronismo, o que aumentaria a dificuldade de se responder tal pergunta. No entanto, no caso concreto estudado, não consideramos a divergência temporal e sim a evolução doutrinária dos dias atuais do nosso país, portanto é possível respondermos que houve aderência parcial, enfatizando que alguns pontos da doutrina nacional carecem de aperfeiçoamento com relação aos fatores operacionais.

Cabe ressaltarmos oportunamente que a pesquisa não teve como objeto o aprofundamento na doutrina estadunidense ou em sua evolução ao longo do tempo, nas capacidades de pessoal e de material existentes nos dois países, nas individualidades existentes nas Forças Armadas do Brasil, em ataques ou ações específicas da guerra cibernética em território nacional ou estrangeiro, que não o mencionado anteriormente, tampouco o detalhamento das doutrinas individuais de cada força, ficando em aberto essas e outras questões que podem gerar novas pesquisas.

Finalmente, depreendemos a relevante implicação para o MD e para a Marinha do Brasil consolidarem como lição aprendida a experiência estadunidense, que considera as funções operacionais já contempladas no conceito de Abordagem Operacional e o incorpora na doutrina de guerra nos diversos espaços cibernéticos, seja no *Blue cyberspace* (DODIN ou *Non-*DODIN*)*, no *Grey cyberspace* ou no *Red cyberspace*.

REFERÊNCIAS

ACIKGÖZ, Vedat. **Ciberguerra**: último ato de uma política malevolente. Deutsch Welle, 23 mar. 2003. Economia. Disponível em: https://p.dw.com/p/3Q1n. Acesso em: 29 Jun. 2020.

AMARANTE, José Carlos Albano do. **O alvorecer do século XXI e a ciência e tecnologia nas forças armadas**. *Military review*, Brasil, n. LXXXIII, p. 3-18, 1. tri. 2003. Disponível em: http://cgsc.contentdm.oclc.org/cdm/singleitem/collection/p124201coll1/id/1122/rec/1. Acesso em: 10 Abr. 2020.

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD-31-M-07**: Doutrina militar de defesa cibernética. 1ª Ed. Brasília, 2014. Disponível em: https://www.defesa.gov.br/forcas-armadas/estado-maior-conjunto/145-forcas-armadas/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/13188-publicacoes. Acesso em: 22 Mar. 2020.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação. **Glossário de segurança da Informação**. Brasília, p. 1-50, 2019. Disponível em: http://dsic.planalto.gov.br/arquivos/documentos-pdf/glossario_completo.pdf. Acesso em: 20 Jun. 2020

CABRAL, Isabel. **A história dos domínios de internet**. TechTudo, 2018. Disponível em: https://www.techtudo.com.br/noticias/2018/07/a-historia-dos-dominios-de-internet.ghtml. Acesso em: 02 Mai. 2020.

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

CYBER Attacks Accompany War in Iraq. Information Management & Computer Security, Bradford, v. 11, n. 4, p. 201, 2003. Disponível em: https://search.proquest.com/docview/212327920/7134604E61914316PQ/10. Acesso em: 20 Jun. 2020.

ESTADOS UNIDOS DA AMÉRICA. *Joint Chiefs of Staff*. **JP 3-12**: *Cyberspace Operations*. *Maryland*, p. 108, 2018. Disponível em: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf. Acesso em: 20 Jun. 2020.

FULGHUM, David A. ***Frustrations and backlog****: preparation for conflict in Iraq envolve complications of traditional logistics and vagaries of cyberwar.* Aviation Week, Washington, 10 mar. 2003. Disponível em: https://aviationweek.com/frustrations-backlogs. Acesso em: 12 Jun. 2020.

GANTZ, John. **Meta-Virus set to unleash plague on windows 3.0 users**. Infoworld, 01 abr. 1991. Disponível em: https://books.google.com.br/books?id=0FAEAAAAMBAJ&pg=PA39&lpg=PA39&dq=Virus+AF+91. Acesso em: 22 Mar. 2020.

GAZULA, Mohan Buvana. ***Cyber Warfare conflict Analysis and Case Studies***. 2017. 100 p. Tese (*Master of Science in Engineering and Management*) - *System Design and Management*

Program, Massachussetts Institute of Technology, 2017. Disponível em: https://dspace.mit.edu/handle/1721.1/112518. Acesso em: 20 Mar. 2020.

GORDON, MICHAEL; TRAINOR, BERNARD. **Cobra II**: *The Inside Story of the Invasion and Occupation of Iraq*. 1ªEd. New York: Pantheon, 2006. [530] p. Ebook.

KAPLAN, Fred M. ***Dark territory****: the secret story of cyberwar*. *NewYork*: Simon & Schuster, 2016. [666] p. Ebook.

LEWIS, James Andrew. ***Thresholds for Cyberwar***. *Center for Strategic and International Studies, Washington*, 01 out. 2010. Disponível em: https://www.csis.org/analysis/thresholds-cyberwar. Acesso em: 20 Mar. 2020.

MARKOFF, John; SHANKER, Thom. ***Halted '03 Iraq plan illustrates U.S. fear of cyberwar risk***. *The New York Times, New York*, 01 ago. 2009. Disponível em: https://www.nytimes.com /2009/08/02/us/politics/02cyber.html. Acesso em: 11 Abr. 2020.

MELHORAMENTOS. **Dicionário Michaelis**. 2020. Disponível em: https://michaelis.uol.com.br/moderno-portugues. Acesso em: 29 Jun. 2020.

NORDVPN. **As técnicas de ataque cibernético mais comuns**. NordVPN, 2019. Disponível em: https://nordvpn.com/pt-br/blog/tipos-comuns-hacking-internet/. Acesso em: 20 Jun. 2020.

SMITH, George. ***Iraqi Cyberwar****: an ageless Joke. Security Focus.* Disponível em: https://www.securityfocus.com/columnists/147. Acesso em: 22 Mar. 2020.

SMITH, George. ***One Printer, One Virus, One Disabled Iraqi Air Defense****. The Register,* Londres, 10 Mar. 2003. Disponível em: https://www.theregister.co.uk/2003/03/10/oneprinteronevirus. Acesso em: 22 Mar. 2020.

WILSON, Clay. ***Information Operations, Electronic Warfare, and Cyberwar:*** *Capabilities and Related Policy Issues. CRS Report for Congress.* 20 mar. 2007. Disponível em: https://www.everycrsreport.com/files/20070320RL317875334f1f80edb1fba74a6458 6fe64949014c2e7d8.pdf . Acesso em: 23 Abr. 2020.

ANEXO A

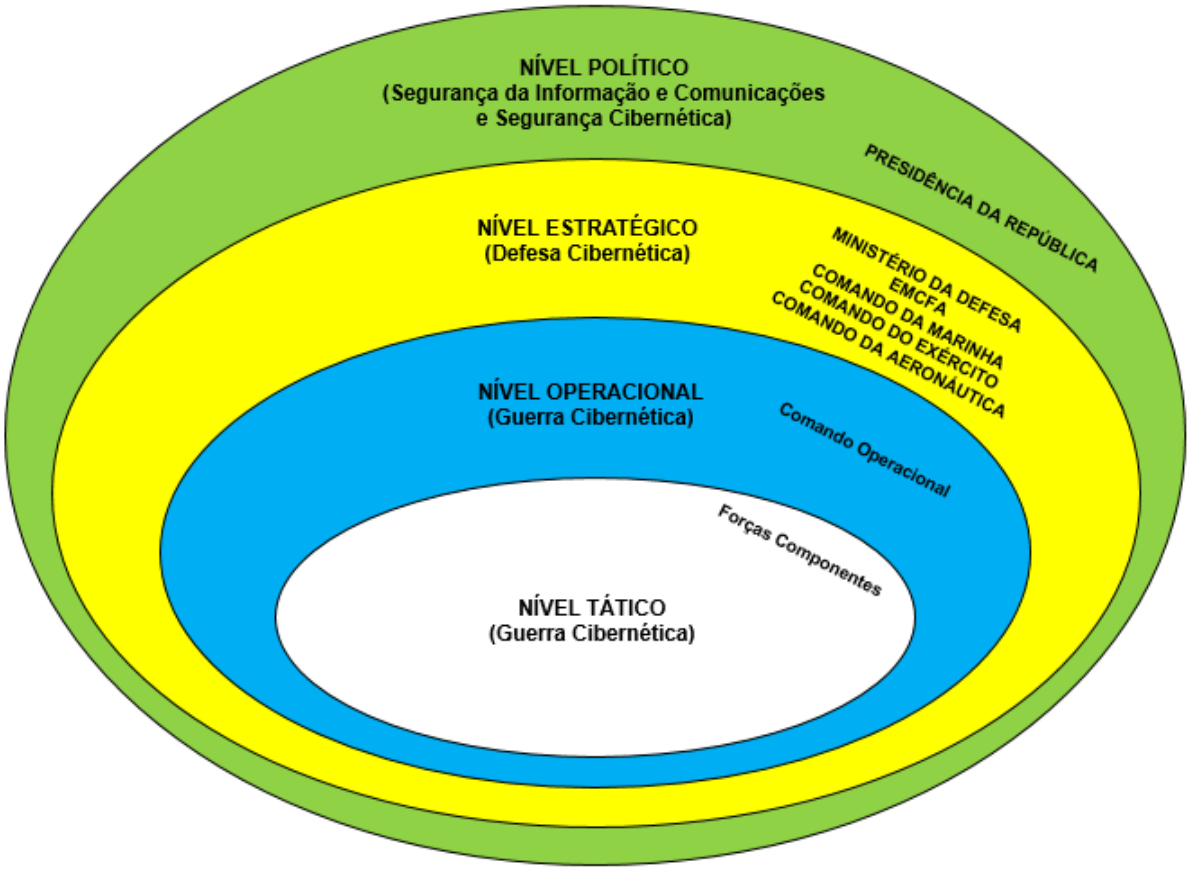

Figura 1 – Níveis de Decisão
Fonte: **MD-31-M-07**: Doutrina Militar de Defesa Cibernética, p. 17.

ANEXO B

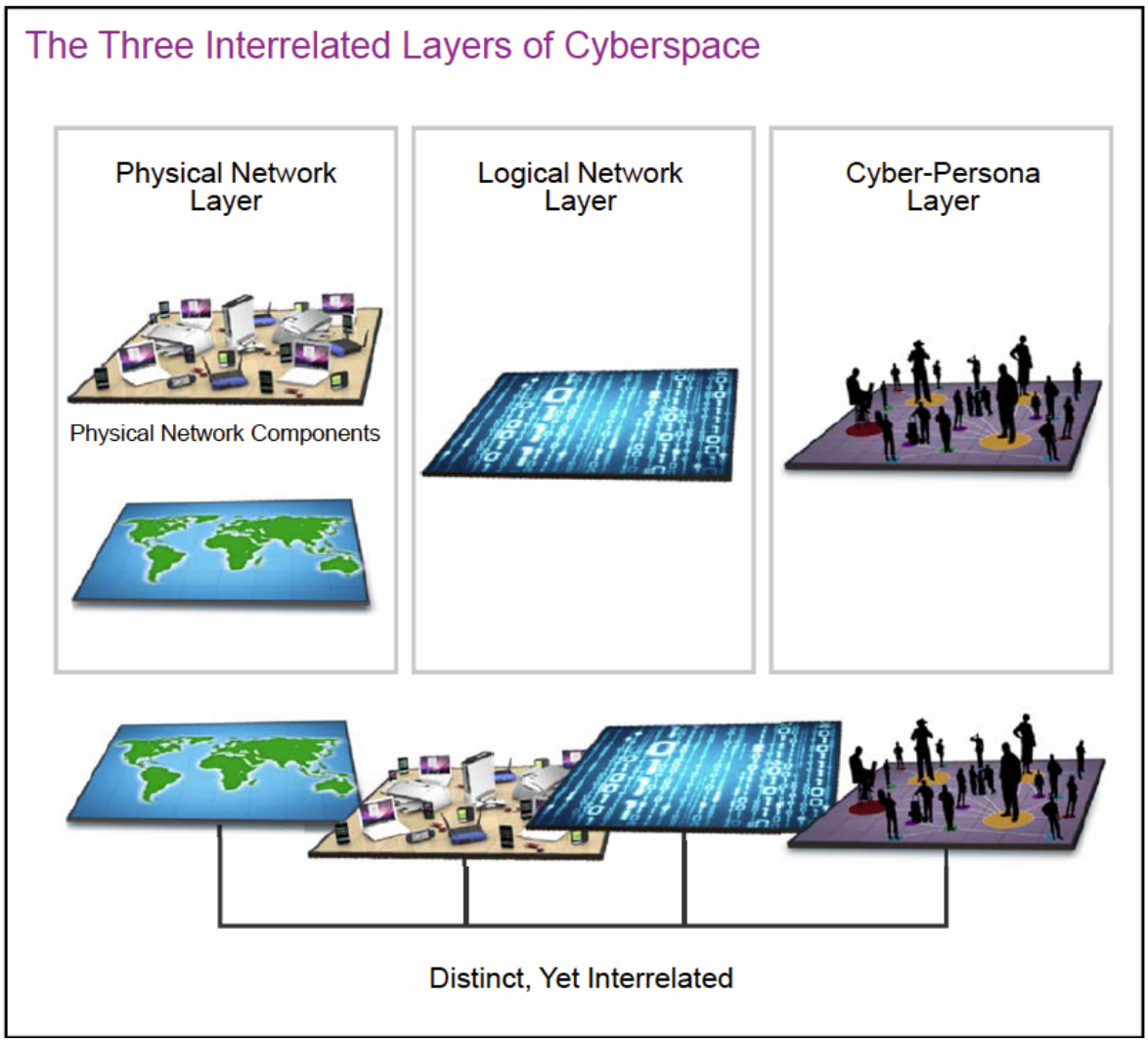

Figura 2 - A inter-relação entre as 3 camadas do espaço Cibernético
Fonte: **JP 3-12**, *Cyberspace Operations*, p. I-3.

ANEXO C

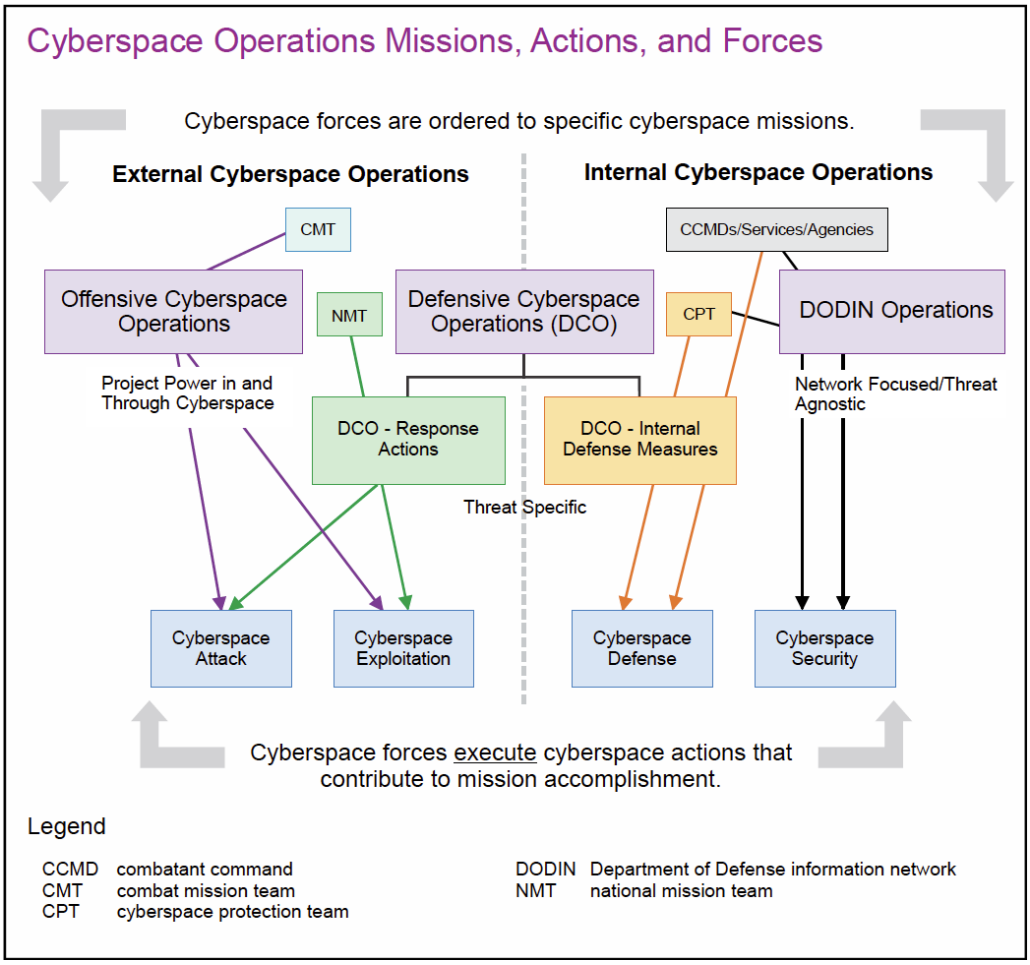

Figura 3 - Missões, Ações e Forças dos EUA empregadas no espaço Cibernético
Fonte: **JP 3-12**, *Cyberspace Operations*, p. II-3.

ANEXO D

QUADRO 1
Critérios e formas de atuação Possibilidades distribuídos segundo o nível de decisão

Critérios	Forma de atuação cibernética	
	Política / estratégica	Operacional / tática
Nível dos Objetivos	Políticos e/ou Estratégicos	Operacionais e/ou Táticos
Foco	Obtenção de Inteligência	Preparação do campo de batalha
Nível de envolvimento nacional	Normalmente interministerial, podendo requerer ações diplomáticas e de vários ministérios e agências (Defesa, Relações Exteriores, Ciência, Tecnologia e Inovação, GSI/PR, Agência Brasileira de Inteligência - ABIN, Agência Nacional de Telecomunicações - ANATEL etc.)	Normalmente no âmbito do Ministério da Defesa, podendo contar com apoio do Ministério das Relações Exteriores
Contexto	Desde o tempo de paz, podendo fazer parte de uma Operação de Informação ou de Inteligência	Em um ambiente de crise ou conflito, apoiando uma ação militar
Nível tecnológico empregado	Normalmente alto ou muito alto	Normalmente médio ou baixo
Sincronização	Dentro do contexto de uma sofisticada Operação de Inteligência, podendo requerer ações diplomáticas anteriores ou posteriores	Dentro do contexto dos sistemas operacionais de uma Operação Militar, sincronizado com a manobra
Tempo de Preparação e Duração	Duração prolongada, com tempo de preparação normalmente mais longo, com desenvolvimento e emprego de técnicas de difícil detecção	Duração limitada, normalmente com moderado ou curto tempo de preparação, utilizando conhecimentos já levantados e técnicas previamente preparadas

Fonte: **MD-31-M-07**-Doutrina Militar de Defesa Cibernética, p. 23. (Houve alteração para adequação ao MNPT)