ESCOLA DE GUERRA NAVAL

CC GUSTAVO ALMEIDA MATOS DE CARVALHO

A TEORIA DE BOYD APLICADA NA U.S. NAVY:

o ciclo de decisão OODA e a guerra de manobra no espaço cibernético

Rio de Janeiro

2019

CC GUSTAVO ALMEIDA MATOS DE CARVALHO

A TEORIA DE BOYD APLICADA NA U.S. NAVY:

o ciclo de decisão OODA e a guerra de manobra no espaço cibernético

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

Orientador: CF(RM1) Ohara Barbosa Nagashima

Rio de Janeiro
Escola de Guerra Naval
2019

AGRADECIMENTOS

À minha esposa Bia pelo amor, pela compreensão, pelo incentivo e pelo apoio incondicional.

Aos meus filhos Isabela e Matheus por terem entendido os momentos de ausência e por me fortalecerem nos momentos mais difíceis.

Ao meu orientador CF(RM1) Nagashima, pelo suporte, pelas suas correções e pelo incentivo.

RESUMO

O espaço cibernético é um ambiente desafiador para a condução da guerra. Novas tecnologias surgem para causar desequilíbrio no posicionamento de forças e alterar continuamente a percepção dos contendores nesse ambiente altamente volátil. Este estudo analisa a invasão cibernética à rede interna da Marinha dos Estados Unidos da América (EUA) que alterou sua forma de combater nesse espaço, conduzindo a Força a reorganizar seus procedimentos e mitigar a ocorrência de cenários desfavoráveis. Esse despertar cibernético mostrou que era necessário haver um planejamento mais detalhado e eficaz. A criação de um plano estratégico orientou as ações e o comportamento dentro de um contexto temporal, buscando alcançar um estado de consciência situacional superior a seus oponentes. Muitas iniciativas estratégicas listadas no plano pautavam-se na observação do espaço cibernético, e nas consequentes orientações, decisões e ações que auxiliam os tomadores de decisão a manobrarem tanto em ambientes administrativos comprometidos quanto no teatro de operações. Ao confrontar a teoria do Coronel John Boyd (1927-1997) com o plano estratégico, conclui-se que houve alta aderência às etapas do ciclo de decisão OODA e os princípios de guerra de manobra. Por fim, o trabalho ressalta a importância do assunto para a Marinha do Brasil ao expor a importância do processo cognitivo dos usuários e dos decisores e os impactos e prejuízos que a falta de percepção de uma ameaça podem causar para nossa Força Naval.

Palavras-chave: Boyd. Ciclo de decisão. OODA. Guerra Cibernética. Guerra de manobra.

LISTA DE ABREVIATURAS E SIGLAS

CMF	*Cyber Mission Forces*
CNO	*Chief of Naval Operations*
DoD	*Department of Defense*
DODIN	DoD *information network*
EUA	Estados Unidos da América
FBI	*Federal Bureau of Investigation*
FCC	*Fleet Cyber Command*
JCS	*Joint Chief of Staff*
NGEN	*Next Generation Enterprise Network*
NMCI	*Navy-Marine Corps Intranet*
NSA	*National Security Agency*
OC	Operações cibernéticas
OODA	Observação, Orientação, Decisão e Ação
SIGINT	*Signals Intelligence*
TFCA	*Task Force Cyber Awakening*
USCYBERCOM	*United States Cyber Command*
USMC	*United States Marine Corps*
USN	*United States Navy*

SUMÁRIO

1 INTRODUÇÃO

O mundo passa por uma grande transformação devida, em sua grande maioria, às novas tecnologias da informação. As mudanças incluem avanços na maneira em como a informação é coletada, armazenada, processada e disseminada. Enquanto a velocidade de processamento da informação aumenta progressivamente, os custos de seu armazenamento e disseminação diminuem. A implementação de tais capacidades aumentou incrementalmente as comunicações e, consequentemente, as conexões internacionais tendo em vista que mais pessoas e Estados ao redor do mundo adquirem acesso à Internet, à comunicações satelitais e a capacidades de reconhecimento.

Avançadas tecnologias de informação alterarão a forma como as pessoas e sociedades interagem, de uma forma que ainda não é possível predizer. Estados ao redor do mundo estão se adaptando e, simultaneamente, tentando moldar o desenvolvimento em curso das tecnologias da informação. Essas relações e interações são um dos fenômenos de nossa era.

Uma faceta observada em como o mundo se adapta às mudanças na tecnologia da informação é a maneira de condução dos conflitos. A produção de efeitos nas políticas de segurança nacional dos Estados e suas instituições é resultado da necessidade da inclusão de novas ameaças, da mudança na forma de combater e do avanço de interesses em um mundo cada vez mais incerto, complexo, volátil e ambíguo.

Na guerra, a evolução tecnológica e sua amalgamação com sistemas de armas, de comando e controle e organizacionais nos permite suspeitar que o uso da informação assume um patamar superior de importância em detrimento do emprego de medidas mais convencionais da força militar.

O domínio da guerra dependerá da dominância da informação e consequentemente, de um dos espaços em que ela trafega: o espaço cibernético. Considerado

como o quinto domínio da guerra, o cibernético é o ambiente onde adversários atacam em nanossegundos, sem exposição e mostram-se difíceis de serem identificados. Os métodos e processos empregados para atacar e defender os recursos de tecnologia da informação constituem uma nova forma de efetuar a guerra de manobra, inspirada pelas ideias do Coronel John Boyd.

Boyd estudou a guerra tanto taticamente quanto estrategicamente. Seu pensamento sempre foi buscar fazê-la de forma mais rápida e mais eficiente que seu oponente. Desempenhou vários papéis em sua vida: estudante, matemático, professor, engenheiro, projetista de aeronaves, historiador militar e piloto de caça. De sua experiência, elaborou conceitos que continuam ressonantes e inspiraram Forças Armadas a alterarem sua doutrina de emprego.

Baseado nas ideias de Boyd, analisaremos um recorte da mudança doutrinária vivenciada pela *U.S. Navy* (USN) após um ataque cibernético de grande escala em 2013, que alterou a percepção da Força quanto a seus oponentes. Os militares estadunidenses tiveram que combater durante alguns meses uma ameaça cibernética que se fez atuar em sua rede interna, ocasionando grandes prejuízos administrativos e financeiros. Apesar de os Estados Unidos da América (EUA) encontrarem-se em posição de vanguarda tecnológica e terem uma capacidade de transformar sistemas técnicos de grande complexidade em fatores de força, as mudanças tecnológicas correntes podem transformar rapidamente essa vantagem em uma vulnerabilidade através de inovação e disrupção conduzidas por novos atores globais.

De satélites que orbitam a Terra até o "Serviço Silencioso" abaixo dos mares, a USN depende do espaço cibernético para garantir comando e controle e fogo integrado, quando necessário. A plataforma cibernética se estende além dos sistemas tradicionais de tecnologia da informação e dos sistemas administrativos e almeja ampliar seu aparato de segurança cibernética para todas as capacidades em rede, incluindo o controle da guerra e de

seus sistemas de combate, de suporte de combate e outros sistemas de informação, enquanto fortalece as autoridades e responsabilidade de suas lideranças navais. Essa foi uma das maneiras encontradas para evitar que a tomada de decisões dos adversários seja mais rápida que a dos estadunidenses.

O propósito deste trabalho é verificar se a mudança doutrinária da USN, observando e analisando os objetivos e iniciativas estratégicos apresentados no Plano Estratégico 2015-2020 do *Fleet Cyber Command* (FCC) da USN, teve aderência à teoria do ciclo de decisão OODA do Coronel John Boyd e aos conceitos relativos à guerra de manobra.

No segundo capítulo, analisaremos a construção da arquitetura de uma das redes governamentais estadunidenses que possui o maior número de usuários e sistemas do mundo e o contexto situacional que levou à sua invasão, os atores envolvidos e as consequências que levaram a expedição do plano estratégico do FCC, que será o objeto de estudo desse trabalho.

No terceiro capítulo, examinaremos os principais conceitos da teoria de Boyd, enfatizando os princípios da guerra de manobra e como o espaço cibernético absorve essas influências.

No quarto capítulo, confrontaremos o plano estratégico do FCC com o modelo de guerra de manobra e a teoria do ciclo de decisão de Boyd e por fim, no quinto capítulo, exporemos as principais conclusões, bem como a relevância do estudo para a Marinha do Brasil (MB).

2 A OPERAÇÃO *ROLLING TIDE* E SUAS CONSEQUÊNCIAS

Neste capítulo, abordaremos os impactos do ataque cibernético que levou a USN rever alguns de seus procedimentos, técnicas e táticas para a defesa de suas redes internas e para esse fim, inicialmente, analisaremos os principais atores envolvidos no desenvolvimento da Operação *Rolling Tide*, utilizando conceitos dos termos utilizados na guerra cibernética em acordo com a Doutrina Conjunta Cibernética do *Joint Chief of Staff* (JCS) e as consequências dessa operação para a USN.

2.1 A *Navy-Marine Corps Intranet* (NMCI)

A rede interna da Marinha e do Corpo de Fuzileiros Navais estadunidense, conhecida pelo acrônimo NMCI, foi criada em 6 de outubro de 2000 com o propósito de consolidar cerca de 6 mil redes de computadores (NORTON, 2016). Algumas dessas redes não permitiam a troca de informação com outras e operavam isoladamente, denotando assim uma grande ameaça à segurança.

O então *Secretary of the Navy,* Gordon England (1937 -), afirmou que a rede era ineficiente e produzia resultados longe de serem considerados ótimos pois eram dezenas de *softwares* obsoletos, com múltiplas versões instaladas em servidores e computadores espalhados em todo o território estadunidense (WAIT, 2002).

A NMCI foi implementada através de um contrato de US$ 6,94 bilhões de dólares com a empresa *Electronic Data Systems Corporation* (EDS) para oferecer serviços de dados, vídeo e comunicações por voz, conectando as unidades de terra e realizando a interface com sistemas de computadores instalados a bordo de navios (WILSON, 2002). Em agosto de 2008, a EDS foi adquirida pela empresa *Hewlett-Packard* (HP). A USN descreveu esse contrato como o maior já executado na área de tecnologia da informação e inicialmente, o escopo do projeto era a conexão de mais de 360 mil computadores em única rede integrada, com

softwares, hardwares e telecomunicações padronizados.

Mesmo após o lançamento da NMCI, a USN tinha mais de 500 outras redes separadas. Em 2009, quando o contrato estava chegando ao fim – e com a preocupação com as "ameaças cibernéticas" contra as redes militares em ascensão – a Marinha estadunidense ainda planejava a aquisição de uma rede subseqüente que lhe daria maior controle sobre sua operação e defesa. Ao mesmo tempo, continuou a transferir mais seus usuários administrativos para a NMCI, na esperança de melhorar a segurança e tornar mais suave a transição para sua nova intranet chamada *Next Generation Enterprise Network* (NGEN) (GALLAGHER, 2014).

De acordo com a *Rear Admiral* Diane Weber do FCC, a NGEN para a Marinha representava uma oportunidade para a rede ser um recurso próprio do governo em detrimento de uma rede de posse de uma empresa, ganhando autoridade necessária para aumentar a capacidade de comando e controle, aprimorar a consciência situacional e a agilidade para manobrar a rede de acordo com as intenções do Comando.

Era previsto que o FCC operasse a rede em conjunto com técnicos da empresa HP, realizando a governança, o controle da gestão de configuração e a tomada de decisões de alto nível.

2.2 O *Fleet Cyber Command* e sua missão

O FCC é o comando operacional responsável pela operação das redes de informação da USN, pela condução de operações cibernéticas ofensivas e defensivas, operações espaciais e operações de *Signals Intelligence* (SIGINT)[1]. Sua missão é planejar, coordenar, integrar, sincronizar, dirigir e conduzir, no espaço cibernético, as atividades operacionais necessárias para assegurar liberdade de ação para a USN em todos os domínios

1 O termo *Signals Intelligence* ou SIGINT significa a inteligência derivada de sinais e sistemas eletrônicos, utilizados por alvos estrangeiros, como sistemas de comunicações, radares e sistemas de armas, fornecendo informação sobre capacidades, ações e intenções dos adversários.

da guerra, além de negar o uso desse espaço aos seus oponentes (ESTADOS UNIDOS DA AMÉRICA, 2015).

Foi criado em 29 de janeiro de 2010 em acordo com a visão do *Chief of Naval Operations* (CNO) de atingir a integração e inovação necessárias para obter a superioridade de combate no espectro das operações militares no domínio marítimo, no espaço cibernético e no domínio de informações (FLEET CYBER COMMAND PUBLIC AFFAIRS, 2010).

Durante sua cerimônia de criação, foi recomissionado o Comando da 10ª Esquadra (C10F), descomissionado desde 1945, com o objetivo de ser a Esquadra numerada do FCC e exercer controle operacional sobre as forças a ele atribuídas.

O FCC é o Comando Componente da USN subordinado ao *U.S. Cyber Command* (USCYBERCOM) e também se reporta diretamente ao CNO.

2.3 A invasão à *NMCI* em 2013

Nos anos seguintes à criação da NMCI, a defesa cibernética somente era um tema preocupante quando acontecia um incidente de segurança específico que nem sempre estava atrelado aos sistemas da USN ou ao *Departament of Defense* (DoD).

Em dezembro de 2014, o *Federal Bureau of Investigation* (FBI), a unidade de polícia do Departamento de Justiça estadunidense, havia alertado empresas norte-americanas que uma operação sofisticada de ataques cibernéticos estava sendo conduzida desde o Irã (FINKLE, 2014). De acordo com relatório realizado pela empresa de segurança cibernética *Cylance*, uma operação denominada *Cleaver* foi desencadeada por um grupo de 20 hackers iranianos nomeado "*Tarh Andishan"*[2]**,** objetivando atacar, estabelecer permanência e extrair dados sensíveis de redes de agências governamentais e de companhias responsáveis por administrarem instalações de infraestrutura crítica. Desde 2012 até 2014, o grupo foi responsável por cerca de 50 ataques em 16 Estados diferentes, sendo que 10 somente nos

2 No original iraniano, a tradução seria "Pensadores" ou "Inovadores".

EUA (CYLANCE, 2016).

Em conformidade com os pesquisadores da *Cylance*, os atacantes iranianos obtiveram acesso e roubaram dados em diversas organizações, variando desde dados pessoais e de pesquisa de alunos de universidades a informações confidenciais que permitiriam a sabotagem de sistemas de supervisão e controle industrial (CYLANCE, 2016).

O estabelecimento de um padrão de ataque possibilitou os pesquisadores identificarem que suas operações eram divididas em três fases: a primeira relacionada ao comprometimento inicial, a segunda fase levava ao escalonamento desse comprometimento, extraindo dados e obtendo posição de permanência dentro da rede e a terceira fase, que nem sempre foi evidenciada, era a execução da sabotagem ao assumir o controle de instalações para realizar ataques físicos (CYLANCE, 2016).

Dentre os ataques às organizações estadunidenses, um afetou diretamente as operações da maior rede corporativa militar do país e do mundo. Em setembro de 2013, o jornal Wall Street Journal acusou o Irã de ter invadido a rede *NMCI* e de acordo com o relatório da *Cylance*, essa invasão teria ocorrido em prol da Operação *Cleaver*. Devido a uma falha de segurança no servidor de hospedagem de um sítio voltado ao púbico externo, os invasores a puderam explorar e obtiveram acesso à rede privada da NMCI e se espalharam para outros sistemas (GALLAGHER, 2014).

2.4 A operação *ROLLING TIDE*

A reação da USN ao ataque cibernético na NMCI foi a condução da primeira operação voltada ao combate da atividade cibernética dirigida contra suas redes e capacidades de comando e controle, a Operação *Rolling Tide*.

De acordo com citação meritória do Secretário da Marinha estadunidense, o FCC, unido a outros órgãos governamentais de segurança cibernética, realizaram ações combinadas

que resultaram na execução sincronizada da maior e mais sofisticada manobra de rede na história da Marinha dos EUA. Os militares do FCC foram agraciados:

> Pelo serviço excepcionalmente meritório durante as missões atribuídas de 9 de agosto de 2013 a 23 de fevereiro de 2014. O pessoal do *U.S. Fleet Cyber Command* e *U.S. TENTH Fleet* se destacou na execução da Operação *Rolling Tide*, a primeira operação da Marinha dos EUA lançada especificamente para combater a **atividade cibernética dirigida contra nossas redes e capacidades de comando e controle**. As ações combinadas […], resultaram na **execução sincronizada da maior e mais sofisticada manobra de rede na história da USN** (ESTADOS UNIDOS, 2014, tradução nossa, grifo nosso).[3]

Embora a vulnerabilidade que permitia aos invasores obterem acesso fosse descoberta e encerrada em outubro de 2013 os *spywares*[4] instalados pelos invasores permaneceram na rede até novembro daquele ano. Autoridades informaram que nenhuma conta de e-mail foi comprometida e nenhum dado foi roubado no ataque, porém custou cerca de US$ 10 milhões para serem reparados os danos causados aos sistemas da rede – um processo que incluiu derrubar toda a rede, duas vezes, de forma a prover atualizações para sistemas e remoção de *malware*[5] (GALLAGHER, 2014).

A operação *Rolling Tide* revolucionou a estratégia de defesa cibernética da rede da USN, melhorando o comando e o controle, desenvolvendo um processo rápido para mitigar os riscos da rede e lançando as bases para defender suas redes contra futuras ameaças cibernéticas.

De acordo com a *Vice Admiral* Jan Tighe, houve uma mudança de paradigma no combate cibernético durante a invasão iraniana em 2013. Naquela época, a resposta geral a uma intrusão cibernética era "desligar tudo" para realizar a "limpeza". A NMCI, com aproximadamente 350.000 contas associadas, não era algo que pudesse simplesmente ser

---

3 No original: "*For exceptionally meritorious service during assigned missions from 9 August 2013 to 23 February 2014. The personnel os US Fleet Cyber Command and US TENTH Fleet distinguished themselves in execution of Operation Rolling Tide, the U.S. Navy´s first named operation launched specifically to counter cyber activity directed against our networks and command and control capabilities. The combined actions [...] resulted in synchronised execution of the largest and most sophisticated network manoeuvre in U.S; Navy history.*"

4 Programa espião que recolhe informações de usuários e o transmite a uma entidade externa, sem o conhecimento e o consentimento do usuário.

5 Programa malicioso que se infiltra em um sistema de computador alheio de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações sigilosas ou não.

"desligada" por um tempo indeterminado sem que afetasse a Marinha de alguma forma (CSIS, 2017).

E fazendo uma analogia ao funcionamento de um navio, não seria aceitável, tampouco seguro, que um sistema de propulsão, um sistema de navegação ou um sistema de comunicações fossem desalimentados enquanto estivesse sendo realizada a "limpeza" cibernética desses sistemas ou das redes, no caso da NMCI.

A noção de combater a ameaça cibernética durante a operação dessas redes se tornou primordial para o desenvolvimento da Operação *Rolling Tide* cujo objetivo principal era arquitetar e construir a capacidade de isolar diversos segmentos da rede para que, caso detectado algo anômalo, essa ameaça fosse prontamente isolada de forma a prevenir o oponente de acessar outras áreas críticas. A partir do isolamento dessa ameaça, a reação seria iniciada, a limpeza realizada e aquele segmento de rede comprometido seria restaurado.

Essa operação serviu como uma oportunidade de aprendizado para os militares estadunidenses haja vista que amadureceu a maneira de operarem e defenderem suas redes no espaço cibernético e, simultaneamente, evidenciou as falhas na postura de segurança cibernética e nas capacidades operacionais defensivas.

A invasão mitigada pela operação *Rolling Tide*, que foi encerrada em 23 de fevereiro de 2014, marcou o início de um "despertar cibernético" para a USN.

2.5 A *Task Force CYBER AWAKENING*

As autoridades navais estadunidenses perceberam sua falta de habilidade para holisticamente compreender a postura de segurança cibernética na USN, que deveria englobar aspectos muito além daqueles relativos às redes administrativas corporativas e incluir sistemas de combate e de controle industrial. Ademais, faltava à USN uma autoridade única e centralizada para gerenciar a segurança cibernética. As falhas de segurança que foram

evidenciadas na Operação *Rolling Tide* se manifestaram como explorações cibernéticas confirmadas, dados supostamente perdidos, vulnerabilidades conhecidas, consciência situacional de segurança cibernética limitada e salvaguardas inadequadas.

De forma a assumir uma nova postura e ganhar a perspectiva necessária, o *Admiral* John Greenert (1953 -), CNO, determinou a criação da *Task Force Cyber Awakening* (TFCA) em agosto de 2014. A TFCA foi um esforço de um ano, liderado pelo gabinete do Vice-Chefe de Operações Navais de Guerra da Informação, *Vice Admiral* Ted Branch e teve como objetivo formular uma base para a segurança cibernética na USN dentro de todos os sistemas, tanto a bordo quanto em terra, e determinar um rumo a seguir para aprimorar suas defesas.

A Força-Tarefa (FT) foi responsável por implementar mudanças na cultura organizacional, de maneira a empregar os recursos e determinar o nível de prontidão da Força, estendendo o uso do aparato de tecnologia da informação para sistemas de combate, suporte ao combate e outros sistemas de informação enquanto direcionava o processo de alinhamento e fortalecimento das autoridades competentes. Para esse fim, foram formados quatro Grupos-Tarefa (GT) com representação de toda a USN para organizar as ações.

O GT de capacidades analisou as ações e avaliações de segurança cibernética em andamento ou concluídas recentemente de forma a priorizar os investimentos para garantir que a Marinha estivesse no caminho correto em curto prazo (NORTON, 2016).

O GT denominado *CYBERSAFE* foi responsável por construir um programa baseado no programa SUBSAFE desenvolvido pelos submarinistas após a perda do USS Thresher em 1963[6]. O programa CYBERSAFE se aplicaria a um subconjunto limitado de componentes e processos robustos e incluiria rigorosos padrões técnicos, certificação e auditoria (NORTON, 2016).

6 De 1915 até 1963, a USN perdeu 16 submarinos por causas não relacionadas ao combate. Após o programa de qualidade SUBSAFE ser implementado para manter os padrões de segurança de operação de um submarino, nenhum navio certificado foi perdido em causa não relacionada ao combate.

O GT voltado à segurança cibernética da Marinha concentrou-se em avaliar as autoridades, os métodos e os recursos atuais necessários para melhor aplicar rigorosos padrões técnicos, certificações e avaliações por toda a USN (NORTON, 2016).

O GT técnico utilizou engenheiros experientes dos Comandos Operacionais de Sistemas da USN para assegurar que normas técnicas robustas fossem colocadas em prática de forma a impulsionar programas e sistemas cibernéticos (NORTON, 2016).

Mathew H. Swartz, Diretor da Divisão de Comunicações e Redes da USN, ressaltou a importância da busca de soluções para as vulnerabilidades encontradas após a Operação Rolling Tide:

> Nós queremos olhar para a integridade da instituição para prover às autoridades a habilidade de priorizar respostas e investimentos. Devido à interconectividade de nossos sistemas administrativos e de combate, a ameaça a um desses sistemas é uma ameaça a todos.[7](ANDERSON, 2014, tradução nossa)

Ao final de um ano, um dos objetivos da Força-Tarefa era desenvolver um plano estratégico robusto para aumentar a consciência de segurança cibernética na USN, estabelecendo a segurança cibernética como um "Negócio do Comandante"[8] e se tornando tão importante quanto um sistema de armas (ANDERSON, 2014).

Com o objetivo de compreender e priorizar as mais importantes ameaças e capacitar a USN a responder com senso de urgência, foi elaborado pelo FCC o Plano Estratégico 2015-2020.

2.6 O Plano Estratégico 2015-2020 do *FCC* e a obtenção do domínio da informação

A criação do Plano Estratégico 2015-2020 enfatizou os aspectos combatentes, ofensivos e defensivos, do FCC e também reconheceu que os responsáveis por conduzir a guerra nos demais domínios dependem da efetividade das ações do FCC na confluência do

7 No original: "*We want to look at the wholeness of the enterprise to provide leadership the ability to prioritize responses and investments. Because of the interconnectedness of our business and warfighting systems, a threat to one is a threat to all."*

8 Na Marinha do Brasil, são ordens disseminadas pelo Comando de cada organização militar através de um documento denominado "Voga do Comandante".

espaço cibernético, do espectro eletromagnético e do espaço.

O plano enunciou cinco objetivos estratégicos fundamentais que deveriam ser alcançados no espectro temporal estipulado, de forma a propiciar a USN a obtenção do domínio da informação e a consequente liberdade de ação e a superioridade na tomada de decisões. Cada objetivo estratégico foi abordado de forma ampla, acompanhado de um conjunto de iniciativas estratégicas como ações críticas para o atingimento desses objetivos e de um indicador de progresso de 18 meses para garantir o foco estratégico na obtenção do sucesso ao final dos cinco anos (ESTADOS UNIDOS DA AMÉRICA, 2015).

Analisaremos tais objetivos estratégicos conforme apresentados no plano estratégico apontando as mudanças de postura adotadas, as correlacionando ao observado nos eventos que antecederam e que ocorreram durante a Operação *Rolling Tide.* As lições aprendidas com essa operação contribuíram sobremaneira para a confecção das iniciativas estratégicas que conformam os objetivos.

O primeiro objetivo estratégico é a operação da rede como uma plataforma de combate, defendendo suas redes, comunicações e sistemas espaciais da USN, assegurando sua disponibilidade e, quando necessário, efetuando o combate para atingir os objetivos operacionais. Esse objetivo deverá ser alcançado por meio das seguintes iniciativas estratégicas (IE): assegurar comando e controle (IE 1.1); reduzir a superfície de intrusões de ataques (IE 1.2); aprimorar as Operações de Defesa em Profundidade (IE 1.3); diminuir o tempo do ciclo através do aumento da clareza organizacional (IE 1.4) e influenciar a agilidade e velocidade do planejamento, programação, financiamento e execução de processos no espaço cibernético (IE 1.5).

O segundo objetivo estratégico é a condução de operações de SIGINT adaptadas às evolutivas necessidades operativas, além de entregar as necessidades da *National Security Agency* (NSA)[9]. Utilizará as seguintes iniciativas estratégicas: institucionalizar a colaboração

9 É a Agência de Segurança Nacional dos EUA com funções relacionadas à SIGINT, criptoanálise e a

proposital (IE 2.1); expandir e robustecer as operações de SIGINT (IE 2.2) e manter a SIGINT atualizada e conduzir a Integração Nacional da SIGINT (IE 2.3).

O terceiro objetivo estratégico almeja entregar efeitos de combate no espaço cibernético por meio do avanço das capacidades de entrega de efeito para apoio de um espectro amplo de operações incluindo manobras cibernéticas e eletromagnéticas e operações de informação, adotando as seguintes iniciativas: liderar o entendimento e o uso dos efeitos cibernéticos pela USN (IE 3.1) e institucionalizar as capacidades de entrega cibernética (IE 3.2).

O quarto objetivo estratégico é a criação de uma consciência situacional cibernética compartilhada por meio da criação de um quadro operacional comum[10] cibernético que evolua para um quadro de consciência imediata da rede da USN e de tudo o que acontece nela. O alcance desse objetivo se dará por intermédio das seguintes iniciativas: estabelecer um conjunto de operações globais cibernéticas defensivas (IE 4.1); definir uma estratégia de dados unificados e criar ferramentas analíticas para alimentar a consciência situacional cibernética (IE 4.2) e direcionar os requisitos para ferramentas de visualização de forma a capacitar a consciência situacional cibernética compartilhada (IE 4.3).

O quinto e último objetivo estratégico do plano é o estabelecimento e robustecimento das *Cyber Mission Forces* da USN, formando 40 equipes de Missões Cibernéticas altamente qualificadas e planejando a sustentabilidade dessas equipes ao longo do tempo. Seriam utilizadas as seguintes iniciativas: desenvolver requisitos inovadores de seleção e recrutamento (IE 5.1); acelerar a geração de requisitos de adestramento (IE 5.2); direcionar requisitos para estabelecimento de capacidades de vanguarda (IE 5.3) e desenvolver capacidades e processos efetivos de Comando e Controle (IE 5.4).

Voltaremos a analisar tais objetivos estratégicos no quarto capítulo onde faremos

proteção das comunicações estadunidenses.

10 É uma apresentação única de informação operacional compartilhada por vários Comandos, preferencialmente em tempo real.

a verificação de sua aderência à teoria do Coronel John Boyd, que será discutida no próximo capítulo.

3 A TEORIA DO CICLO DE DECISÃO OODA DE JOHN BOYD APLICADA AO ESPAÇO CIBERNÉTICO

Neste capítulo, serão apresentados os conceitos do ciclo de decisão OODA em acordo com o modelo teórico elaborado pelo Coronel John Boyd (1927-1997), da Força Aérea dos EUA, que iniciou sua carreira como um piloto de combate extremamente proficiente na Guerra da Coreia (1950-1953).

O manual de táticas de caça, de sua autoria, modificou a maneira como toda Força Aérea no mundo voa e combate. Ele descobriu uma teoria física que modificou para sempre a forma com que aviões de caça são desenhados. E em uma das histórias militares mais surpreendentes da atualidade, o piloto Boyd ensinou ao *U.S. Marine Corps* (USMC) como combater uma guerra no solo. Por meio de suas ideias, surge o conceito de guerra de manobra que influenciou os EUA a obterem sua vitória na Guerra do Golfo (1990-1991) (CORAM, 2002).

Analisaremos também o conceito de Guerra em Três Blocos do General Krulak, fazendo um paralelo com a guerra cibernética.

Buscaremos compreender como os princípios e teorias de Boyd se aplicam ao espaço cibernético e como as características desse domínio podem alterar esses conceitos.

3.1 O ciclo de decisão OODA de John Boyd

John Boyd foi um estrategista que desenvolveu táticas de combate aéreo nas décadas de 1950 e 1960 e foi instrutor de voo na *Fighter Weapons School* na Base Aérea de Nellis nos EUA. Também foi responsável por elaborar o design das aeronaves F-15 e F-16 e foi para a reserva da Força Aérea estadunidense como Coronel em 1975. Suas ideias eram passadas por meio de apresentações orais ou ensaios sem que houvesse a publicação de uma obra que os compilasse.

A mais longa de suas apresentações, *Patterns of Conflict*, datada de 1986, forma o cerne de sua pesquisa relacionada aos conflitos, fazendo uma análise histórica de teorias e guerras para a obtenção da vitória. De acordo com as próprias palavras de Boyd "um compêndio de ideias e ações para ganhar e perder em um mundo altamente competitivo" (CORAM, 2012). Boyd também introduzira um conceito essencial para a compreensão de seus pensamentos: o modelo do ciclo de decisão OODA ou o Ciclo de Boyd (OSINGA, 2005).

O acrônimo OODA significa Observação, Orientação, Direção e Ação. O primeiro elemento, observação, é sentir a si mesmo e o mundo à sua volta. O segundo, orientação, é um complexo conjunto de filtros de herança genética, predisposição cultural, experiência pessoal e conhecimento. O terceiro elemento é a decisão, que revisa os rumos de ação e a seleção do rumo preferencial como uma hipótese a ser testada, e o quarto elemento é a ação, que seria o teste da decisão selecionada para implementação (HAMMOND, 2004).

Simplificando, Boyd reforça a ideia de que o sucesso na guerra, no conflito, na competição ou até mesmo na sobrevivência depende da qualidade e do ritmo dos processos cognitivos das lideranças e de suas instituições. A guerra pode ser interpretada como uma colisão de organizações em seus respectivos ciclos OODA (OSINGA, 2005).

Conforme exposto pelo Coronel Philip S. Meilinger, de acordo com Boyd:

> A chave para a vitória era agir mais rápido, tanto mentalmente quanto fisicamente, que o seu oponente. Ele expressou esse conceito em um processo cíclico chamado de Ciclo OODA. Tão logo um lado agisse, eram observadas as consequências e o ciclo começava novamente. […] O significado das teorias de táticas aéreas de Boyd é que ele mais tarde formulou a hipótese de que esse ciclo de operação contínua não estava em jogo somente em um duelo aerotático, mas também nos níveis mais altos da guerra. Ao traçar a história da guerra, Boyd viu a vitória consistentemente indo para o lado que poderia pensar de forma mais criativa e agindo rapidamente sobre essa percepção (MEILINGER, 1995, p.31, tradução nossa)[11].

11 No original: "*The key to victory was to act more quickly, both mentally and physically, than your opponent. He expressed this concept in a cyclical process he called the OODA Loop. As soon as one side acted, it observed the consequences, and the loop began anew. [...] The significance of Boyd's tactical air theories is that he later hypothesized that this continuously operating cycle was at play not only in a tactical aerial dogfight, but at the higher levels of war as well. In tracing the history of war Boyd saw victory consistently going to the side that could think the most creatively, and than acting quickly on that insight*."

Analisando-se essa visão, a teoria de Boyd afirma que a principal vantagem do sucesso no conflito é operar dentro do ciclo de decisão do oponente. Vantagens na observação e orientação permitem o estabelecimento de um ritmo para a tomada de decisões que supera a capacidade do inimigo de reagir efetivamente no tempo (GRAY, 1999). À medida que um indivíduo ou organização percorre continuamente seu ciclo OODA, iterativamente é observada uma melhora nesse processo que o capacita a tomar decisões de forma mais rápida.

Na interpretação mais popular da teoria boydiana, o ciclo OODA sugere que o sucesso na guerra depende da capacidade de ultrapassar o ritmo e o pensamento do adversário, ou em outras palavras, de fazer com que o nosso ciclo gire mais rápido que o do adversário, causando sua paralisia (OSINGA, 2005).

3.2 A guerra de manobra e o conceito da "guerra em três blocos"

Após uma análise da Guerra do Vietnã (1964-1968) onde a fricção não obteve o sucesso esperado, o USMC teve de responder a questões postadas pela sociedade estadunidense quanto a seu papel em conflitos vindouros. O dilema discutido era a manutenção da doutrina do combate baseado no atrito, tal qual conduzido durante a Segunda Guerra Mundial (1939-1945), arriscando assim ser uma força irrelevante no cenário mundial ou por outro lado, adotar uma nova postura, com a possibilidade de comprometer sua tradição em combates de mais de 200 anos (DAMIAN, 2008).

Esse debate se encerrou em 1989 quando o General Alfred M. Gray (1928 -), Comandante do USMC, assinou o novo manual doutrinário *Fleet Marine Force Manual* 1 (FMFM-1), *Warfighting*. Essa publicação descrevia a natureza, a teoria, a preparação e a condução da guerra sob aspectos inovadores e, fortemente influenciada pelas ideias de John Boyd, apresentou uma nova mentalidade conhecida como guerra de manobra (OSINGA, 2005).

Os *marines* encontraram na ênfase de Boyd em conceitos como velocidade, ritmo, variedade, surpresa, confiança, iniciativa, movimento, moral e mentalidade, inerentes ao ciclo de decisão OODA, uma alternativa a termos como superioridade em números e poder de fogo em massa. Boyd defendia táticas não-lineares, evitando e contornando posições inimigas, aventurando-se no território do adversário sem muita preocupação com os próprios flancos. Não buscava o espaço traduzido na conquista do território mas almejava surpresa, economia de tempo e choque. Tais táticas obrigariam a reação do adversário e criaria a impressão que os *marines* estavam em todos lugares e poderiam atacar qualquer lugar em qualquer momento. Em vez de ter o foco no terreno e no desembarque anfíbio, Boyd os fez focar no inimigo (OSINGA, 2015).

A guerra de manobra era uma maneira de pensar sobre como vencer qualquer conflito, desde insurgências como a guerrilha até conflitos convencionais contra grandes potências. Como teoria, a guerra de manobra se concentra em entrar na mente dos inimigos, descobrir suas fraquezas e com ênfase no alcance da desintegração, quebrar a coesão entre as unidades inimigas e suas ações (OSINGA, 2015).

A nova e sofisticada abordagem visava desenvolver sistemas nos quais uma unidade pudesse se adaptar mais rapidamente que o inimigo e responder com maior destreza às mudanças no campo de batalha. A capacidade de fazer a transição e pressionar o inimigo em um lugar e tempo decisivos fala dessa nova concepção (OSINGA, 2015).

A ampla influência das ideias de Boyd manifestada através do Ciclo OODA se tornou um símbolo instantaneamente reconhecido pelos militares em todo o mundo ocidental, tendo como principal marca a descrição da guerra de manobra em termos de ciclos de decisão competitivos (APPLEGATE, 2012).

Em 1997, o General Charles C. Krulak (1942 -) atualizou o FMFM 1 e expediu o *Marine Corps Doctrinal Publication* 1 (MCDP 1), expondo que o conceito de *Warfighting*

não “deveria ser somente uma guiagem para a ação e sim uma forma de pensar”. No primeiro capítulo da norma, a visão dos *marines* sobre a natureza da guerra é definida. Para descrever a guerra, a doutrina emprega conceitos fundamentais boydianos, como a difusão da não-linearidade, incerteza, risco, fluidez e desordem, apresentando a visão de que a guerra é um encontro de sistemas complexos e que a guerra é o surgimento do comportamento coletivo desses sistemas complexos em conflito uns com os outros. De acordo com Krulak, o aprimoramento do conceito na natureza da guerra e sua ênfase na complexidade e imprevisibilidade foi um dos objetivos almejados na revisão da publicação (ESTADOS UNIDOS DA AMÉRICA, 1997).

Através do conceito “Guerra em Três Blocos”, o General Krulak ilustrou um complexo espectro de desafios a serem enfrentados pelos *marines* em um moderno campo de batalha, onde ele foca no elemento humano em combate. No exemplo de Krulak, os militares podem ser obrigados a realizar uma ação militar em grande escala, operações de manutenção da paz e de ajuda humanitária dentro do espaço de três blocos contíguos de uma determinada cidade. O conceito demanda que forças armadas modernas devem ser treinadas para operar em todas as três condições simultaneamente, em um terreno limitado, e que, para isso, o adestramento de liderança nos níveis mais baixos precisa ser elevado.

Atualmente, as guerras modernas também são combatidas em um quarto bloco: o espaço cibernético.

3.3 A guerra de manobra no espaço cibernético

De acordo com a Doutrina Militar de Defesa Cibernética brasileira, o espaço cibernético é o espaço virtual, composto por dispositivos computacionais conectados ou não em redes, onde as informações transitam, são processadas ou armazenadas (BRASIL, 2014). Está presente em todas as redes computacionais do mundo e nos dispositivos a elas

conectados ou controlados. Essa característica global e sem delimitação tangível de fronteiras permite considerar o espaço cibernético como um campo de batalha onde existe a capacidade de invadir, controlar ou até mesmo de destruir tais redes. A informação administrada por redes de computadores que coordenam serviços públicos, como transportes, sistema financeiro e o meio militar, pode ser suscetível a ações cibernéticas do tipo exploração ou ataque a partir de qualquer localidade no exterior (CLARKE, 2016).

Falhas na arquitetura das redes, nos *hardwares* e *softwares* utilizados e a introdução crescente de sistemas *on-line* tornam possível a militarização do espaço cibernético, devido ao caráter difuso de ameaças virtuais que buscam manipular constantemente tais vulnerabilidades. Pela sua permeabilidade e influência nos demais domínios da guerra[12], considera-se o espaço cibernético como o quinto domínio da guerra (CAVELTY, 2012).

O conceito de manobra é descrito como a disposição de forças para conduzir operações assegurando uma vantagem de posição antes ou durante operações de combate. De acordo com Boyd, "a vitória em ciclos de decisão competitivos requer que um lado compreenda o que está acontecendo e aja mais rápido o que outro lado"[13] (WELLS II, 2010). A manobra em seus termos, pode ser descrita como operar dentro do ciclo de decisão do inimigo ou em outras palavras, conseguir sucesso em entrar nos aspectos que envolvem espaço, mente e tempo de forma a penetrar nos campos físicos, moral e mental do adversário. De acordo com o MCDP 1, o conceito da essência da manobra é então, tomar uma ação para gerar e explorar alguma forma de vantagem sobre o inimigo.

As operações militares no espaço cibernético são organizadas em missões executadas por meio de uma combinação de ações específicas que contribuem para o alcance do objetivo do Comando (ESTADOS UNIDOS DA AMÉRICA, 2018). Nesse domínio,

12 Os outros domínios da guerra são o marítimo, terrestre, aéreo e espacial.

13 No original: "*Victory in competitive decision cycles requires one side to understand what is happening and act faster than the other*."

quando um comandante operacional consegue manobrar com surpresa, despistamento, velocidade e agilidade, ele coloca o adversário em uma situação insustentável e sem a capacidade de obter a vitória (RULE, 2013). A aplicação do Ciclo OODA se torna uma ferramenta útil para a manobra no terreno cibernético.

A manobra na guerra cibernética pode ser conceituada como a aplicação de força para capturar, perturbar, negar, degradar, destruir ou manipular recursos de computação e de informação de modo a alcançar uma posição de vantagem em relação aos adversários. Pelo fato de ser um ambiente virtual, não há o movimento de forças na forma cinética e sim, a aplicação de forças em pontos específicos de ataque ou defesa. Tais forças seriam códigos computacionais especialmente escritos para alcançar os objetivos dos atacantes ou dos defensores e serem utilizados em um local ou no tempo que melhor convém (APPLEGATE, 2012).

De acordo com Duggan (2011), as forças não se movimentam no espaço cibernético e sim os pontos de ataque, dificultando a observação e a identificação, especialmente no que se refere à origem da fonte que ataca. Como em outros domínios da guerra, as operações ofensivas e defensivas não somente se completam, como são inseparáveis.

A guerra de manobra no espaço cibernético é utilizada para influenciar o processo cognitivo humano e o comportamento das máquinas de forma a atuar no ciclo de decisão OODA do adversário, explorando suas vulnerabilidades e obtendo uma posição mais favorável (BRANTLY, 2015).

Ao adentrar o domínio cibernético, a manobra adquire características únicas quando comparada à manobra nos outros domínios. Conforme Applegate (2012) explicita, é necessário compreender como o princípio da manobra se aplica às operações cibernéticas.

A velocidade nas operações cibernéticas é distinta quando comparada em termos

humanos e computacionais. Essa característica intrínseca ao espaço cibernético torna as ações virtualmente instantâneas e extremamente difíceis de serem contornadas após a condução de um ataque que obteve sucesso ou a alteração de postura perante a modificação de uma formação defensiva. No caso do ataque de sucesso, o tempo de deteção da ameaça não permitiria que o comprometimento das informações fosse evitado. Quanto a modificação das defesas durante a ocorrência de um ataque cibernético, é improvável que um atacante consiga alterar seu ataque com rapidez suficiente para continuar tendo êxito sem ser identificado. A velocidade favorece o lado que obteve a iniciativa das ações e ao trazer um paralelo com a teoria de Boyd, a manobra de sucesso é aquela onde o atacante ou o defensor entram no ciclo de decisão de seus adversários e se movimentem mais rápido do que eles podem reagir. As reações tendem a acontecer na velocidade de análise do ser humano tomador da decisão, enquanto as ações acontecem na velocidade das máquinas (APPLEGATE, 2012).

3.3.1 As operações militares no espaço cibernético

Conforme explicitado na *Joint Publication* 3-12 de 2018, as operações cibernéticas (OC) se traduzem como o emprego de capacidades do espaço cibernético onde o propósito principal é alcançar objetivos dentro ou através deste domínio. A doutrina militar busca estabelecer um modelo para o emprego de capacidades e forças do espaço cibernético. Tais forças são os recursos humanos designados a executar uma missão de OC.

Ações no espaço cibernético, com o devido cuidado de entrega de efeitos em cascata, podem permitir a liberdade de ação para atividades no domínio físico. Da mesma forma, atividades no domínio físico podem criar efeitos no espaço cibernético ao afetar o espectro eletromagnético ou alguma infraestrutura física.

O espaço cibernético pode ser dividido em três camadas inter-relacionadas: rede física, rede lógica e *cyber-persona*. Cada uma delas representa um diferente foco de como as

OC podem ser planejadas, conduzidas e avaliadas (ESTADOS UNIDOS, 2018).

A camada de rede física é composta por *hardware* e a infraestrutura computacional, que necessita de proteção para evitar o acesso indevido ou dano físico. Essa camada é o primeiro ponto de referência que as OC utilizam para determinar a localização geográfica e o ordenamento jurídico adequado (ESTADOS UNIDOS, 2018).

A camada de rede lógica é baseada na programação de códigos que auxiliam os componentes de rede a logicamente endereçar, intercambiar e processar dados. Para fins de seleção de alvos, planejadores podem saber a localização lógica de um objetivo, como máquinas virtuais ou sistemas operacionais, sem saber sua localização geográfica. Nos casos de alvos posicionados na camada lógica, somente podem ser engajados através de dispositivos ou programas designados para criar efeitos no espaço cibernético (ESTADOS UNIDOS, 2018).

A camada cyber-persona é a visão do espaço cibernético criada por uma abstração de dados da camada de rede lógica usando regras que se aplicam nessa camada para desenvolver descrições de representações digitais da identidade de um determinado ator ou entidade no espaço cibernético. Um indivíduo pode criar e manter múltiplas a *cyber-personas* através do uso de múltiplas identificações no espaço cibernético. Por outro lado, uma cyber-persona pode possuir múltiplos usuários utilizando uma mesma forma de acesso a um determinado serviço ou instrumento de rede. A localização de *cyber-personas* pode ser complexa e difícil, sendo necessário manter acompanhamento e monitoramento detalhado para efetuar a correta seleção do alvo nas camadas físicas e lógicas (ESTADOS UNIDOS, 2018).

As operações militares no espaço cibernético podem acontecer nessas camadas e são conduzidas por forças que cumprem três tipos de missões nesse domínio: as operações cibernéticas ofensivas, defensivas e as operações do DoD *information network* (DODIN). O

sucesso da execução dessas OC necessita da integração e sincronismo dessas missões (ESTADOS UNIDOS, 2018).

As operações DODIN incluem ações operacionais para dar segurança, configurar, operar, estender, manter e sustentar o espaço cibernético do DoD e criar e preservar o sigilo, a disponibilidade e a integridade do DODIN (ESTADOS UNIDOS, 2018).

As operações ofensivas são aquelas designadas para projetar poder em espaço cibernético estrangeiro através de ações em apoio a comandos operacionais ou a consecução de objetivos nacionais. É a missão que objetiva criar efeitos no domínio físico (ESTADOS UNIDOS, 2018).

As operações defensivas são executadas para defender o DODIN ou outros espaços cibernéticos do DOD de ameaças ativas. São missões orientadas para a proteção de dados, redes, dispositivos e sistemas contra atividades maliciosas correntes ou iminentes (ESTADOS UNIDOS, 2018). Se diferem das operações DODIN justamente por conta do posicionamento da ameaça à rede: as operações DODIN objetivam dar segurança ao espaço cibernético do DOD de todas as ameaças antes de qualquer atividade de ameaça.

Esses conceitos nos auxiliarão na comparação da teoria com a realidade, a ser realizada no próximo capítulo.

4 O PLANO ESTRATÉGICO DO FCC E SUA ADERÊNCIA À TEORIA DE JOHN BOYD

Nos capítulos anteriores, discorremos sobre as origens do plano estratégico do FCC 2015-2020 e numeramos seus objetivos estratégicos que objetivaram alterar a mudança de percepção dos militares quanto à segurança cibernética. Além disso, identificamos os elementos do Ciclo OODA que fazem parte do processo decisório em um conflito, assim como conceitos de guerra de manobra que nos auxiliaram a perceber que a guerra no espaço cibernético tem muitas similaridades com a doutrina militar utilizada pelos *marines* através dos conceitos de guerra de manobra.

Neste capítulo, analisaremos a mudança de paradigma ocorrida após a Operação *Rolling Tide* e identificar se há aderência entre a teoria de Boyd e as iniciativas estratégicas descritas no Plano Estratégico do FCC 2015-2020, comparando as ações decorrentes com as etapas do ciclo de decisão OODA, objetivando encontrar as semelhanças e as divergências.

4.1 Os objetivos estratégicos do FCC e sua aderência

Analisaremos nesta seção, os objetivos estratégicos em conjunto com as iniciativas estratégicas mais importantes e analisar sua aderência à teoria de Boyd. Conforme especificado em sua teoria, a chave para o sucesso no conflito é operar dentro do ciclo de decisão do oponente. As vantagens na observação e orientação habilitam maior tempo para a tomada de decisão e a execução da ação deve ultrapassar a capacidade do adversário para a reação.

O plano estratégico do FCC enfatiza o aspecto combatente do Comando, tanto ofensivo quanto defensivo. Conforme citado no plano, quando uma tecnologia alcança um nível onde é enquadrada como uma plataforma de combate, ela não abandona seu propósito inicial e alcança um patamar muito mais amplo e inclusivo. O estamento militar que

compreender este ponto de inflexão, mais brevemente será aquele que obterá vantagem. Após ser surpreendida pela invasão a NMCI em 2013, a USN buscou adaptar suas técnicas, táticas e procedimentos e aprimorar os processos conduzidos por seus militares, utilizando o espaço cibernético a seu favor e incrementando suas defesas de forma a obter um posicionamento vantajoso na guerra cibernética. Boyd reforça a ideia de que o sucesso na guerra, no conflito, na competição ou até mesmo na sobrevivência depende da qualidade e do ritmo dos processos cognitivos das lideranças e de suas instituições. Por esse motivo, há uma conectividade do plano à teoria.

4.1.1 A rede como plataforma de combate

O primeiro objetivo estratégico do plano é a operação da rede como uma plataforma de combate, e para alcançá-lo é necessário mantê-la sempre disponível, por meio de operações de defesa cibernética e DODIN e quando necessário, empregar operações de ataque. Entretanto, a arquitetura da rede possui vulnerabilidades inerentes à sua grandeza e seus usuários ainda não compreenderam como seu comportamento nas três camadas do espaço cibernético pode comprometer a segurança da rede. Tais fraquezas serão exploradas na etapa observação do ciclo de decisão do inimigo e deverão ser propriamente mitigadas na etapa de ação do ciclo de decisão do FCC, por meio de ações defensivas como o aprimoramento das operações de defesa em profundidade e a redução da superfície de ataque de intrusão.

A superfície de ataque é a soma da exposição ao risco de segurança de uma organização. É o conjunto de todas as vulnerabilidades e controles conhecidos, desconhecidos e potenciais em todos os *softwares*, *hardwares*, *firmwares* e redes (ESTADOS UNIDOS, 2015). Uma superfície de ataque menor pode ajudar a tornar uma organização menos explorável, reduzindo o risco. A iniciativa estratégia relativa à redução da superfície de ataque

deve ser realizada por usuários melhores adestrados, por inspeções de segurança cibernética, melhor certificação e credenciamento, dentre outras ações que buscam evitar que o adversário explore vulnerabilidades decorrentes do mau uso da rede. Essa iniciativa estratégica está diretamente relacionada à capacidade do adversário orientar sua decisão. Pelos princípios da guerra de manobra, a redução da superfície evitaria a liberdade de ação do adversário no âmbito do espaço cibernético.

As operações de defesa em profundidade, outra iniciativa estratégica que compõe esse objetivo, visam garantir a informação em ambientes altamente interligados por meio do aumento de inteligência, vigilância e reconhecimento almejando a deteção de atividade adversária dentro da rede da USN (ESTADOS UNIDOS, 2015). O uso coordenado de várias contramedidas de segurança é empregado para proteger a integridade dos ativos de rede da organização. Por intermédio do emprego de camadas de sensores, analistas e outras contramedidas, o objetivo a ser alcançado é a realização de manobras de defesa cibernética para a proteção de redes, comunicações e dados. Ao assumir uma forte postura defensiva, a USN almeja desencorajar o adversário na realização de ataques atuando em profundidade e distante do objetivo a proteger, modificando a etapa de observação do ciclo de decisão.

A interrupção da informação é incapacitante, ainda mais para uma Força da envergadura da USN. A arquitetura diversificada de rede, a transferência eficiente de dados e o gerenciamento de conhecimento operacional são algumas das capacidades que necessitam operar em conjunto para garantir o comando e controle e a habilidade para combater invasões.

Outra iniciativa estratégica descrita no plano destina-se à diminuição do tempo do ciclo por meio do aumento da clareza organizacional[14]. Em acordo com o plano, quando há a redução dos templos dos ciclos para deteção de intrusão nas redes, na resposta e compartilhamento da consciência situacional, a probabilidade de comprometimento é

14 De acordo com Kolb, a clareza organizacional é o sentimento de que as coisas são bem organizadas e os objetivos claramente definidos, em vez de serem desordenados, confusos ou caóticos.

reduzida e o processo de tomada de decisões é aprimorado.

Etapas essenciais são traçadas para ampliar a clareza e eliminar a ambiguidade organizacional[15]e dentre elas está o esclarecimento do uso de terminologias, de forma que os tomadores de decisão possam se comunicar melhor e para o benefício de todos os envolvidos nesse processo, que a comunicação seja realizada em inglês sempre que possível. Outra etapa é o esclarecimento dos papéis dos atores dentro e entre organizações, além dos processos e resultados intrínsecos a estas. Da mesma forma, ao melhorar a transparência dos dados vitais entre as organizações e ao realizar exercícios de forma interorganizacional, para combater tão bem quanto o treinamento é conduzido, busca-se atingir a clareza organizacional (ESTADOS UNIDOS, 2015).

Tal iniciativa estratégica está diretamente relacionada à teoria de Boyd ao atuar nos aspectos comportamentais das organizações e na inter-relação entre os decisores e os demais atores, abrangendo assim o aspecto da velocidade na troca de informações, que deve ser aprimorado, tendo em vista que a rapidez é um dos elementos-chave para as ações realizadas em prol do cumprimento do ciclo de decisão OODA.

A quinta e última iniciativa deste primeiro objetivo estratégico trata da influência da agilidade e velocidade do planejamento, programação, orçamento e execução de processos do espaço cibernético. No ambiente cibernético e espacial, adversários dos EUA exploram tecnologias a um ritmo acelerado. Diariamente, novas vulnerabilidades são descobertas e disseminadas, o que imediatamente expande a superfície de ataque e permite que agentes mal-intencionados penetrem potencialmente em suas redes. No domínio cibernético, que muda rapidamente e periodicamente, o grande desafio é manter-se na vanguarda.

Embora o FCC não seja encarregado de conduzir os processos de orçamento e execução de programação, de planejamento e de aquisição, ele pode os influenciar para garantir o delineamento de requisitos claros para o fornecimento de capacidades necessárias

15 São fatores que não permitem o avanço de uma organização.

ao sucesso neste domínio. A alteração dos processos de aquisição e governança de novos sistemas e tecnologias aliada a um investimento estratégico em gerenciamento e controle automatizado de inventário (*hardware*, *firmware* e *software*) e à aceleração do processo de aquisições são as formas encontradas pelo FCC para equiparar e ultrapassar os oponentes no desenvolvimento de novas tecnologias. Tais ações administrativas em sua essência parecem, à primeira vista, não terem aderência à teoria do ciclo de decisão de Boyd. Porém, se analisadas sob o prisma da guerra de manobra, o FCC busca alcançar um patamar superior e causar surpresa e choque nos adversários ao desenvolver e empregar novas tecnologias em suas ações no espaço cibernético. Consequentemente, atingiriam diretamente o ciclo de decisão do inimigo ao mudar sua percepção da situação, tornando suas reações mais lentas.

O indicador de progresso deste objetivo estratégico tinha como meta garantir que não haveria operações cibernéticas adversárias nas redes da USN durante os 18 primeiros meses da implantação do plano estratégico do FCC, aparelhando a defesa cibernética e modificando procedimentos para a operação da rede como plataforma de guerra.

4.1.2 As operações de SIGINT

A inteligência de sinais provê aos tomadores de decisão informações vitais sobre oponentes, incluindo suas capacidades, ações e intenções. O FCC conduz operações e implementa recursos de SIGINT em suporte a Comandantes de Forças da USN e Comandantes de Forças Conjuntas. Ademais, fornecem recursos e produtos de SIGINT para a NSA tanto como um provedor de força e um elemento operacional que suporta suas operações para detectar ameaças emergentes ou potenciais aos interesses dos EUA.

O FCC busca adaptar seu apoio às operações no domínio marítimo para incrementar o atendimento às necessidades que estão em constante evolução. Para esse fim, é importante que haja profunda especialização em SIGINT, além de uma estreita colaboração

com a NSA. Em acordo com o plano, a capacidade de personalização do suporte aumentará se criadas as condições para construir maior capacidade de compartilhamento de dados, maiores avanços técnicos em sensores e mais ferramentas de análise (ESTADOS UNIDOS, 2015).

Em virtude do caráter dual do FCC, a USN busca alcançar o equilíbrio entre o suporte militar às suas operações de inteligência de sinais e o suporte civil no apoio aos interesses da NSA que será traduzido por meio do indicador de progresso criado para esse fim. A demanda por operações de SIGINT mais adequadas às carências expostas é a característica principal do segundo objetivo estratégico do plano do FCC.

A primeira iniciativa estratégica desse objetivo é a denominada institucionalização da colaboração de propósitos, que consiste na expansão colaborativa de processos e cultura organizacional entre a NSA e a USN. A razão desse processo é impedir que oponentes explorem a falta de comunicação interna no âmbito governamental e usem essa vulnerabilidade como uma maneira de atingir o ciclo decisório, uma vez que o sucesso dessa iniciativa é pautado na rápida troca de informações, recursos e conhecimento que se encontram trafegando desde o nível estratégico/operacional até o nível tático, em unidades como navios, submarinos e aeronaves. Essa iniciativa tem maior aderência ao elemento observação do ciclo decisório de Boyd, tendo em vista que é nessa etapa que os adversários analisam as possibilidades de ação.

A próxima iniciativa estratégica desse objetivo se refere à expansão e ao robustecimento das operações de SIGINT, por meio da integração de centros de operações de informação regionais e de operadores e técnicos a bordo e os habilitando a operarem sensores remotos e orgânicos, conduzirem análise compartilhada de informação e dado e compilação de todas informações disponíveis para o assessoramento aos comandos apoiados. Conforme explicitado nos conceitos de manobra cibernética, a concentração de esforços nas operações de SIGINT visam à aplicação de forças em pontos específicos de ataque ou defesa, não

havendo necessariamente o movimento de forças cinéticas na camada física. Assim, tal iniciativa tem aderência aos conceitos de guerra de manobra derivados da teoria de Boyd ao permitir a condução de operações específicas para a obtenção de um posicionamento vantajoso no espaço cibernético.

As demais iniciativas estratégicas listadas para esse objetivo visam à manutenção de tecnologia de ponta na área de inteligência de sinais e ao atendimento das demandas operacionais da USN pelo sistema nacional de SIGINT. Tais iniciativas se complementam às duas anteriores e procuram agir no ciclo decisório do FCC ao entregar capacidades ampliadas para os tomadores de decisão.

Portanto, vimos que apesar de o FCC ser um comando da USN, seu plano estratégico procura o tornar mais integrado a uma rede de inteligência superior, contribuindo para o esforço do país na defesa cibernética.

4.1.3 A entrega de efeitos de combate no espaço cibernético

O FCC, em sua vertente operativa, se preocupa com a entrega de efeitos de combate pois tem como algumas tarefas de sua missão o planejamento, a coordenação, a direção e a condução das atividades no espaço cibernético. Por meio de um espectro abrangente de operações, incluindo as cibernéticas, as realizadas no espaço eletromagnético e as de informação, tais efeitos devem ser entregues de modo a ampliar o leque de opções cinéticas e não-cinéticas para os EUA.

Essa entrega de efeitos de combate constitui o terceiro objetivo do plano estratégico. O FCC identificou a necessidade de reforçar sua estrutura para robustecer a aptidão de entrega desses efeitos que acompanham a volatilidade e o dinamismo do espaço cibernético, além da crescente lista de necessidades operacionais. O crescimento da capacidade de combate, cada vez mais sofisticada, deverá ser disponibilizada para os

comandos operacionais em todas as fases da guerra, que atuarão como multiplicadores de força, atuando por meio de efeitos eletromagnéticos e cibernéticos.

De acordo com o plano estratégico do FCC,

> Nos próximos anos, devemos robustecer nossa organização e os processos que sustentam essa capacidade em evolução e torná-los repetitivos e previsíveis. Ao mesmo tempo, devemos facilitar a compreensão, o planejamento e o uso de nossos recursos por outros comandantes operacionais. (ESTADOS UNIDOS, 2015, p.17, tradução nossa)[16]

Esse objetivo possui apenas duas iniciativas estratégicas. A primeira, e mais importante dentre elas, versa sobre a liderança a ser assumida pelo FCC para que a USN compreenda e utilize os efeitos cibernéticos.

A Força Naval deve entender e adotar os efeitos cibernéticos como uma componente integrante do seu arsenal de guerra. Para isso, deve-se elevar o nível de conhecimento e confiança nos efeitos cibernéticos, nas operações e no meio ambiente.

No ciclo de decisão de Boyd, é necessário que durante a etapa de observação seja recolhido o maior número de informações para que estas sejam analisadas posteriormente na etapa de orientação. Para se ter uma análise apurada em todos os níveis, é necessário que se conheça as possibilidades de uso dessa informação. O domínio cibernético apresenta ameaças e oportunidades que não eram contemplados pela educação e treinamento militares. Portanto, a compreensão da dimensão desse domínio se faz primordial para que se possa rapidamente estabelecer os novos requisitos relacionados à formação, capacitação, certificação e qualificação e fornecer subsídios para a implementação destes nas organizações militares. Portanto, a importância do estudo da teoria de Boyd e sua correlação com o espaço cibernético.

O foco do FCC é auxiliar o processo decisório ao desenvolver requisitos para que os comandantes operacionais integrem o assunto cibernético aos seus centros de operações

16 No original: "*In the next few years we must mature our organization and the processes that underpin this evolving capability and then make them repeatable and predictable. At the same time, we must make it easy for other operational commanders to understand, plan for and use our capability."*

conjuntas e aos *maritime operations centers* (MOC)[17], que já possuem integrados a SIGINT e a guerra eletrônica (ESTADOS UNIDOS, 2015). Além disso, ajuda também os comandantes operacionais a utilizarem e integrarem efeitos cibernéticos na elaboração de seus planos operacionais.

A segunda iniciativa estratégica diz respeito a institucionalização da capacidade de entrega cibernética que deve ser realizada de forma previsível e em conjunto com outras capacidades, tornando-os mais fácil de empregar e consequentemente aumentando a velocidade na entrega desses efeitos que influenciam a guerra nos outros domínios.

4.1.4 A consciência situacional cibernética compartilhada

A vigilância proporciona sucesso no domínio cibernético, pois a disponibilidade, as vulnerabilidades e as atividades suspeitas ou maliciosas nos sistemas de informação da USN devem estar em constante monitoramento e análise. O quarto objetivo estratégico do plano é a expansão das atuais capacidades para a inclusão de um quadro operacional comum cibernético mais robusto, global e adaptado às missões.

O quadro operacional comum cibernético compilará o desempenho de sistemas cibernéticos, operações e ameaças em um quadro integrado, informando as operações de rede defensivas, além de apoiar outras operações da missão. Mostrará status, vulnerabilidades, ameaças, atividades suspeitas e impacto na missão, e será personalizável por missões e por região (ESTADOS UNIDOS, 2015).

O emprego de processos e doutrinas conjuntos permite que o quadro operacional comum seja utilizado com outras redes do DoD. Assim, fornecerá informações em tempo real, conforme necessário, para os tomadores de decisão táticos, operacionais e estratégicos, coadunando com as ideias de Boyd em respeito a todas as etapas do ciclo de decisão OODA.

17 O MOC fornece uma estrutura para o estabelecimento rápido e efetivo de apoio a um comandante marítimo de nível operacional.

A primeira iniciativa estratégica deste objetivo visa ao estabelecimento de um ambiente de computação controlado e altamente protegido, que permitirá que suas forças coletem e analisem dados e manobrem a rede da USN através de um quadro de consciência situacional cibernética compartilhada. Isso possibilitará o trabalho integrado entre as Forças no âmbito da USN, utilizando-se vários níveis de análise.

A definição de uma estratégia unificada de dados e a criação de ferramentas analíticas e de visualização para alimentar a consciência situacional cibernética complementam as iniciativas estratégicas deste objetivo.

O resultado esperado desse objetivo é tornar os tomadores de decisão do FCC aptos a monitorarem o status da rede e de comunicações e as atividades suspeitas ou maliciosas em todo o espectro das redes da USN e capazes de utilizarem essa informação para realizarem manobras na rede, conforme os conceitos teóricos de guerra de manobra de Boyd.

4.1.5 O estabelecimento das *Cyber Mission Forces* (CMF)

Em 2009, devido ao aumento das ameaças cibernéticas, foi estabelecido o USCYBERCOM, a maior autoridade militar para assuntos cibernéticos dos EUA. Foi determinada a necessidade de uma CMF, que complementaria as forças operacionais cibernéticas e defensivas existentes até então.

A CMF é composta pelas *National Mission Forces*, para defesa da infra-estrutura dos EUA contra ataques cibernéticos; pelas *Protection Forces*, para defesa e proteção da DODIN e pelas *Combat Mission Forces*, para apoiar o planejamento de comandantes para o combate e, quando autorizados, fornecer efeitos cibernéticos. O USCYBERCOM determinou que cada serviço deveria estabelecer equipes para compor a CMF. O FCC deveria compor e desenvolver 40 equipes em toda a USN (ESTADOS UNIDOS, 2015).

Visando alcançar esse objetivo, foram elaboradas quatro iniciativas estratégicas

que orientam requisitos para a seleção e o recrutamento de pessoal, que gerenciam os requisitos para sua qualificação, que deverá ser rápida e de acordo com os avanços tecnológicos observados, e por fim, que desenvolvam efetivo capacidades e processos de comando e controle para as equipes do CMF.

Tais iniciativas visam adaptar a mentalidade dos militares e civis às inovações percebidas e treinarem suas mentes para que incrementem seu processo cognitivo, permitindo assim que sua observação se torne mais acurada, contribuindo para que o ciclo de decisão gire mais rápido que o de seus oponentes.

Após analisarmos os cinco objetivos do plano estratégico do FCC e suas correspondentes iniciativas, em conjunto com a teoria de Boyd, encerramos o desenvolvimento do trabalho e passaremos a uma síntese a ser discutida no último capítulo de forma a concluirmos esta pesquisa.

5 CONCLUSÃO

Os avanços tecnológicos obtidos pelos Estados, no contexto do espaço cibernético, não podem ser considerados como fatores de força, haja vista que oponentes exploram a dependência exponencial da tecnologia da informação fruto desses avanços para alcançarem uma posição vantajosa. Aquele que possuir maior capacidade de observação, alcançará maior velocidade relativa no giro do ciclo de decisão e conquistará melhor posicionamento para terem a liberdade das ações. Por isso, a importância do estudo das teorias de Boyd quanto ao desenvolvimento do processo cognitivo dos responsáveis por manter o monitoramento da rede.

Boyd expressava a ideia de agir mais rápido que seus oponentes, levando à conceituação de guerra de manobra que tinha como essência manobrar mais rapidamente que o inimigo e responder mais rapidamente às mudanças no campo de batalha. A competição entre ciclos de decisão oponentes é a essência das guerras que são combatidas. Busca-se atuar e manipular o meio ambiente para que nosso ciclo seja o vencedor.

O espaço cibernético, considerado como uma nova dimensão desse campo de batalha, pode ser moldado pelas ações dos oponentes e tais mudanças acabam influenciando outros domínios. Por isso, existe a necessidade de conquistar espaço, posicionando-se de forma mais vantajosa para explorar as vulnerabilidades dos oponentes.

O caráter indissociável das operações defensivas e ofensivas na guerra de manobra acabe se estendendo ao espaço cibernético. A velocidade nesse domínio é instantânea e nossas defesas têm que se adaptar a esse caráter evolutivo. A velocidade favorece quem tem a iniciativa das ações e por isso é importante que as defesas estejam adaptadas.

No caso estudado neste trabalho, não podemos afirmar que houve falta de monitoramento ou falha na defesa cibernética da NMCI pela USN por ocasião de sua invasão

em 2013, porém é notório observar que as ações tomadas para a mitigação dessa ameaça levaram ao desencadeamento da maior operação cibernética da história da USN. A Operação *Rolling Tide* tornou-se um marco para a defesa cibernética da Força por ter mudado o paradigma no combate a um incidente dessa envergadura, isolando segmentos da rede NMCI e garantindo a continuidade de sua operação mesmo com o espaço comprometido.

O despertar cibernético que se seguiu após o fim da *Rolling Tide* buscava evitar a repetição de incidentes em curto prazo e preparava as fundações para a mudança da consciência situacional cibernética, que foi a razão de criação do plano estratégico elaborado pelo FCC para o quinquênio de 2015 a 2020.

Esse plano estratégico objetivou a superioridade no domínio da informação e a liberdade de ação em todos os domínios permeados pelo espaço cibernético. Era necessário concentrar esforços para a mudança da cultura organizacional da USN por meio de objetivos e iniciativas estratégicas que este trabalho demonstrou haver aderência com a teoria elaborada por John Boyd.

Dentre as 18 iniciativas estratégicas apresentadas, a conexão às ideias de Boyd se apresenta integralmente quando se almeja alterar a percepção do inimigo e girar nosso ciclo mais rápido que as capacidades de reação do oponente. No plano, ressalta-se a relevância da etapa observação do ciclo OODA possibilitando a coleta de informações necessárias para as outras etapas do processo de tomada de decisão.

O exercício constante do monitoramento também é importante para o aprimoramento da consciência situacional e conforme Boyd demonstra, evita-se que o ciclo de decisão do adversário gire mais rápido que o da USN. A maneira encontrada para atender esse requisito foi a criação de instrumentos de monitoramento em tempo real para que ameaças sejam identificadas prontamente e, assim como na etapa do ciclo de decisão de Boyd, serem imediatamente combatidas.

O FCC se pautou em vários princípios que orientaram a confecção desse documento. Baseado em sua excelência técnica e operacional, mostraram para o público interno e para a sociedade estadunidense, que seu papel para a defesa cibernética da USN e dos EUA é manter os resultados operativos favoráveis, reduzir os riscos operacionais e alcançar a superioridade no espaço cibernético. Assumindo uma posição de liderança, apontou a necessária direção de suas ações e esforços para a entrega de efeitos cibernéticos e iluminou o futuro de sua Força Naval, observando os acontecimentos presentes e aprendendo com o passado, confirmando assim a influência das ideias de Boyd.

Por fim, depreendemos a validade do estudo para a Marinha do Brasil de sua necessidade de estruturar-se para organizar e orientar suas ações no espaço cibernético, em conjunto com o Ministério da Defesa, conforme os conceitos de guerra de manobra e do ciclo de decisão OODA, especialmente quanto à necessidade de aprimoramento e desenvolvimento da consciência situacional cibernética. Meios não cinéticos têm a capacidade de gerar efeitos cinéticos em todos os domínios e é necessário compreender tais consequências para a guerra naval.

REFERÊNCIAS

ANDERSON, Sean. Task Force Cyber Awakening to create enduring cybersecurity resiliency. **CHIPS**, Washington, 15 outubro 2014. Disponível em: <https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=5702>. Acesso em: 05 mai 2019.

APPLEGATE, Scott D. **The principle of maneuver in cyber operations**. *In*: CZOSSECK, Christian, OTTIS, Rain, ZIOLKOWSKI, Katharina (Eds.) 2012 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2012.

BRANTLY, Aaron F. **Strategic cyber maneuver**. Small Wars Journal (online) Outubro de 2015. Disponível em <http://smallwarsjournal.com/jrnl/art/strategic-cyber-maneuver>. Acesso em: 05 jun 2019.

BRASIL. Ministério da Defesa. MD31-M-07: Doutrina Militar de Defesa Cibernética. 1. ed. Brasília, 2014.

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES. Cyber Warfare in the maritime domain. **Center for Strategic & International Studies**, Washington, 14 setembro 2017. Disponível em: <https://www.csis.org/analysis/cyber-warfare-maritime-domain>. Acesso em: 02 mai 2019.

CORAM, Robert. **Boyd:** The fighter pilot who changed the art of war. Nova York: Little, Brown & Company, 2002.

CYLANCE Inc. Operation Cleaver Report. **Cylance Inc.**, Irvine, 23 dezembro 2016. Disponível em: <https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Cylance_Operation_Cleaver_Report.pdf/>. Acesso em: 10 abr 2019.

DAMIAN, Fideleon. **The road to FMFM 1:** The United States Marine Corps and maneuver warfare doctrine, 1979–1989**.** Kansas, Kansas State University, 2008. (Tese de mestrado).

ENGLAND, Gordon. Remarks by the Honorable Gordon England to the NMCI Industry Symposium. **U.S. Navy**, Nova Orleans, 22 junho 2004. Disponível em: <http://www.navy.mil/navydata/people/secnav/england/speeches/england040622.txt>. Acesso em: 03 abr 2019.

ESTADOS UNIDOS DA AMÉRICA. Navy Unit Commendation to U.S. Fleet Cyber Command / U.S. TENTH Fleet. **Secretary of the Navy**, Washington, agosto 2014. Disponível em: <https://www.public.navy.mil/fcc-c10f/Fact%20Sheets/Navy%20Unit%20Commendation.2014.pdf>. Acesso em: 02 mar 2019.

ESTADOS UNIDOS DA AMÉRICA. **U.S. Fleet Cyber Command / TENTH Fleet Strategic Plan 2015-2020**. Fort Meade: U.S. Navy, 2015.

ESTADOS UNIDOS DA AMÉRICA. **FMFM 1: Warfighting**. Washington: U.S. Marine Corps, 1989.

ESTADOS UNIDOS DA AMÉRICA. **MCDP 1: Warfighting**. Washington: U.S. Marine Corps, 1997.

ESTADOS UNIDOS DA AMÉRICA. **JP 3-12: Cyberspace Operations**. Washington: Joint Chiefs of Staff, 2018.

FINKLE, Jim. Iran hackers may target U.S. energy, defense firms, FBI warns. **Reuters**, Boston, 13 dezembro 2014. Disponível em: <https://www.reuters.com/article/us-cybersecurity-iran-fbi-idUSKBN0JQ28Z20141213>. Acesso em: 25 abr 2019.

FLEET CYBER COMMAND PUBLIC AFFAIRS. Navy stands up Fleet Cyber Command, Reestablishes U.S. 10th Fleet. **U.S. Navy**, Meade, 29 janeiro 2010. Disponível em: <https://www.navy.mil/submit/display.asp?story_id=50954>. Acesso em: 21 abr 2019.

FRANÇA, Júnia L. VASCONCELLOS, Ana Cristina de. Manual para normalização de publicações técnico-científicas**.** 8. ed. Belo Horizonte: Ed. UFMG, 2007.

GALLAGHER, Sean. Iranians hacked Navy network for four months? Not a surprise. **ARS Technica**, Nova Iorque, 19 fevereiro 2014. Disponível em: <https://arstechnica.com/information-technology/2014/02/iranians-hacked-navy-network-for-4-months-not-a-surprise/>. Acesso em: 20 abr 2019.

GRAY, Colin. **Modern Strategy**. Nova Iorque: Oxford University Press, 1999.

HAMMOND, Grant T. **The Mind of War:** John Boyd and american security. Washington D.C.: Smithsonian Books, 2001.

KOLB, D. A. et al. **Psicologia Organizacional:** uma abordagem vivencial. São Paulo, Atlas, 1986.

MEILINGER, Philip. **Air Strategy**: Targetting for Effect. **Aerospace Power Journal**, Nova Iorque, 1999. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a515118.pdf>. Acesso em: 15 mai 2019.

NORTON, Nancy. **The U.S. Navy Evolving Cyber/Cybersecurity Story**. In: The Cyber Defense Review. West Point: Army Cyber Institute, 2016.

OSINGA, Frans. **Science, Strategy and War:** The strategic theory of John Boyd. 1. ed. Delft Eburon Academic Publishers, 2005.

PARKS, Raymond & DUGGAN, David. **Principles of Cyberwarfare**. IEEE Security & Privacy. Nova Jersey: IEEE, 2011.

RULE, Jeffrey N. **A Symbiotic Relationship**: The OODA loop, intuition, and strategic thought. Strategy Research Project. U.S. Army War College. Pennsylvania, 2013.

SECRETARY OF THE NAVY. Cybersecurity Readiness Review. **U.S. Navy**, Washington, 04 março 2019. Disponível em: <https://www.navy.mil/strategic/CyberSecurityReview.pdf>. Acesso em: 15 jun 2019.

WAIT, Patience. NMCI: Cleaning up Navy´s act. **Washington Technology**, Washington, 31

janeiro 2002. Disponível em: <https://washingtontechnology.com/Articles/2002/01/31/NMCI-Cleaning-up-the-Navys-act.aspx?m=2>. Acesso em: 30 abr 2019.

WELLS II, Linton. Maneuver in the global commons. **SIGNAL Magazine**. Dezembro, 2010. Disponível em <https://www.afcea.org/content/?q=node/2472>. Acesso em: 11 jun 2019.

WILSON, Noel. EDS grabs Navy contract worth $6.9 billion. **CNET**, Nova Iorque, 2 janeiro 2002. Disponível em: <https://www.cnet.com/news/eds-grabs-navy-contract-worth-6-9-billion/>. Acesso em: 15 abr 2019.