CMG (FN) **Jeferson** Barbosa Ramos
jeferson@marinha.mil.br

A Guerra Eletrônica nos GptOpFuzNav em Convergência com a Guerra Cibernética

O CMG (RM1-FN) Jeferson serve atualmente no Comando do Desenvolvimento Doutrinário do Corpo de Fuzileiros Navais (CDDCFN) como Assessor de Pesquisa e Desenvolvimento. É oriundo de Escola Naval; cursou o Curso de Altos Estudos de Política e Estratégia (CAEPE) da Escola Superior de Guerra, em 2003; o Curso de Comando e Estado-Maior da Escola de Guerra Naval, em 1998; e o Curso de Aperfeiçoamento de Oficiais de Engenharia da Escola de Aperfeiçoamento de Oficiais (EsAO) – Exército Brasileiro, em 1987. Serviu no Ministério da Defesa, como Analista de Inteligência Estratégica – Arco Amazônico; foi Comandante da Companhia de Guerra Eletrônica, em 1997, e Comandante da Companhia de Pioneiros no Batalhão de Engenharia de Fuzileiros Navais. Cursou também o Curso de Análise Prospectiva ministrado pela *Brainstorm* Assessoria de Planejamento e Informática, em 2001, e o *International Intelligence Director's Course pela Defence Intelligence and Security Centre School em Chicksands* – Londres, em 2002.

"Aqui a guerra é no espectro eletromagnético..."
(Autor Desconhecido)

1. Introdução

Muito se tem falado a respeito da Guerra Eletrônica[1] como ferramenta assessória às Operações de Guerra Naval. Todavia, a abordagem é mais ampla no sentido das Atividades Benignas e ao Emprego Limitado da Força. Nesse viés de pensamento, as questões aqui propostas vão além das fronteiras dos Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav).

Nesse sentido, o presente artigo perscruta os domínios da Guerra Eletrônica (GE) com sua concepção doutrinária e ato contínuo o qual trava uma dialética da convergência Guerra Eletrônica (GE) x Guerra Cibernética (GCiber). A partir dessa transversalidade, procura-se contextualizar a Operação em Redes (OR), ao ambiente cibernético e ao espectro eletromagnético, nos contornos do Sistema Naval de Comando e Controle (SisNC2[2]) e em decorrência no contexto do SIC2CFN[3]/SisC2DefNBQR/Combatente do Futuro[4].

Em complemento, o artigo propõe uma temática,"extra-borda", por intermédio de um excerto síntese da obra propedêutica, *Beyond Convergence – World Without Order*, remissivo à Doutrina Militar Naval (DMN), tendo como propósito suscitar ao leitor diversas reflexões sobre o assunto: "A Guerra Eletrônica nos GptOpFuzNav e a Convergência com a Guerra Cibernética" .

2. A Guerra Eletrônica / Concepção Doutrinária

No arcabouço doutrinário (CGCFN-62, Manual de Guerra Eletrônica nos GptOpFuzNav), conceitua-se Capacidade de Guerra Eletrônica (CGE) como o somatório de meios e recursos de toda ordem que permite a uma Força empreender

[1]Guerra Eletrônica (GE): parte do emprego militar da eletrônica que diz respeito às ações que envolvem o uso de energia eletromagnética para determinar, explorar, impedir, reduzir ou prevenir o uso efetivo pelo inimigo do espectro eletromagnético, e para assegurar o uso deste espectro pelas próprias Forças." (BRASIL, 2017b).

[2]O SisNC2 é um conjunto de instalações, de equipamentos e de comunicações, regido por princípios, normas e processos utilizados em Operações Navais com o objetivo de contribuir para a eficiência das forças envolvidas em combate

[3]O SIC2CFN, em fase de aquisição pelo CFN, é um sistema integrado de comando e controle, com objetivo de modernizar as capacidades de C2 do CFN, aprimorando a eficiência e eficácia operacional de um GptOpFuzNav. Possui uma arquitetura modular contando com os Módulos de Gestão de Batalha; de Comunicação; Módulo de Guerra Eletrônica; e Módulo de Artilharia.

[4]Sistema de Comando e Controle de Defesa NBQR com Integração ao Projeto Combatente do Futuro - SisC2DefNBQR - Combatente do Futuro. (Port Nr. 29/2019, do CGCFN). Estudo dos REM e RANS afetos à integração do "Projeto Combate do Futuro" com o Sistema de Comando e Controle de Defesa NBQR e ao SisGAAz.

eficazmente ações de GE em proveito de suas operações. A CGE é dividida em dois segmentos: as Atividades de Guerra Eletrônica (AGE) e Medidas de Guerra Eletrônica (MGE).

As AGE têm caráter estratégico, tático, logístico que contribuem para o estabelecimento, a reformulação ou verificação das capacidades operativas e estruturantes para o apoio ao planejamento nas operações dos GptOpFuzNav. São divididas em dois ramos: Reconhecimento Eletrônico (RETRON) e Aprestamento Eletrônico (APEL). O RETRON abrange o conjunto de atividades conduzidas, basicamente, com propósito estratégico ou em apoio ao planejamento de uma operação militar, que visa à obtenção e ao processamento sistemático e oportuno de obtenção de Conhecimentos sobre a CGE do inimigo. O RETRON pode ser de caráter tático, quando empregado em apoio ao planejamento de uma operação de um GptOpFuzNav, em que o valor das informações é diretamente proporcional à conjuntura.

O outro segmento das CGE, as MGE referem-se ao emprego da capacidade, em apoio direto a uma Operação Naval. Dividem-se em três ramos: Medidas de Apoio à Guerra Eletrônica (MAGE), Medidas de Ataque Eletrônico (MAE) e Medidas de Proteção Eletrônica (MPE)[5].

Conceitualmente, as ações de GE englobam o espectro eletromagnético[6], que vai desde o menor raio gama até a maior onda de radio frequência, incluindo as faixas visíveis, infravermelhas e ultravioletas. Assim, a atuação da GE varia com a frequência das emissões alvo. Além disso, a mudança de faixa de frequência exige outros tipos de técnicas e procedimentos, acarretando na necessidade de recursos humanos qualificados para atuar em cada faixa considerada.

Os efeitos desejados da GE são: determinação da presença, localização, disposição e ameaça representada por todos os sistemas de comunicações (SISCOM), de comando e controle, de armas e pelos sensores do inimigo que utilizem o espectro eletromagnético; negação do uso dos sistemas eletromagnéticos; exploração dos sistemas eletromagnéticos do inimigo, assegurando a Proteção de nossos sistemas, instalações, meios e equipamentos (...).

Desta forma, pode se depreender que é extremamente importante a coordenação das CGE com outros Sistemas, tais como: de armas, de Inteligência e com a manobra, cabendo, então, ao GptOpFuzNav a coordenação das ações na Área de Operação (Aop) afetas ao nível tático.

O Sistema de GE, normalmente, será de forma centralizada, e mediante o controle de um Centro de Coordenação de Guerra Eletrônica (CeCoGE) – nível tático e Centro de Guerra Eletrônica da Marinha (CGEM) – nível operacional.

Em síntese, para se obter maior eficiência e eficácia, a GE deve estar integrada dentro de um Sistema de Inteligência, o qual possua outras fontes de dados que possam verificar e ratificar as informações obtidas através da GE. Normalmente, no GptOpFuzNav, essa integração da GE com as demais fontes de dados será efetivada no Centro de Análise de Inteligência (CAI).

3. A Guerra Eletrônica no Contexto da Guerra de Manobra[7]

O uso intensivo das MGE (MAGE/MAE/MPE) faz parte do conceito de Guerra de Manobra, tornando o combate mais dinâmico. As MGE podem ser utilizadas, tanto para acelerar o ciclo OODA do GptOpFuzNav, quanto para retardar ou mesmo impedir a conclusão do ciclo OODA inimigo. As MAGE, por seu turno, podem ser empregadas para tornar mais rápida e precisa a fase da Observação.

Quanto maior for a informação sobre o inimigo, mais rápida e precisa será a Orientação dos Centros de GE. Com isso, os conhecimentos serão normalmente obtidos no nível estratégico, através das AGE, as quais são atividades estratégicas que podem facilitar a Orientação dentro de um quadro tático, tal como a confecção de um Banco de Dados (BD) com informações detalhadas sobre as forças inimigas e, paralelamente, prover a Proteção do SISCOM, já em tempo de paz.

Desta feita, o uso eficiente e eficaz das CGE pode desorganizar a liderança do oponente, além de provocar profundo estresse mental, aumentando o grau de incerteza nos coman-

[5] MAGE: conjunto de ações visando a busca, interceptação, identificação e localização eletrônica das fontes de energia eletromagnética irradiadas no ambiente eletrônico de um GptOpFuzNav, a fim de permitir a análise, o imediato reconhecimento de uma ameaça ou sua posterior exploração; MAE: conjunto de ações tomadas para evitar ou reduzir o uso efetivo do espectro eletromagnético pelo inimigo, bem como degradar, neutralizar ou destruir sua capacidade de combate por meio de equipamentos e armamentos que utilizem este espectro; e MPE: conjunto de ações tomadas para proteção de meios, sistemas, equipamentos, pessoal e instalações, a fim de assegurar o uso efetivo do espectro eletromagnético, diante do emprego de ações de GE por forças amigas ou inimigas.

[6] O espectro eletromagnético é a faixa contínua de frequências dentro da qual as ondas eletromagnéticas alteram as suas características de propagação.

[7] O conceito de Guerra de Manobra significa que as forças devem ser capazes de operar num ambiente confuso e caótico como é o Campo de Batalha. Significa também, que não só o GptOpFuzNav deve ser capaz de operar num ambiente assim, mas que é desejável que o GptOpFuzNav gere, também, confusão e desordem. Esta confusão e desordem podem ser criadas através do uso bem sucedido das ações de MAE.

dantes e seus EM. Assim, através da GE, é possível neutralizar ou prejudicar um processo de tomada de decisão, no contexto da Guerra de Manobra.

4. O Sistema Militar de Defesa Cibernética e a Doutrina Militar de Defesa[8] nos Domínios da GCiber

O Sistema Militar de Defesa Cibernética (SMDC) é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no espaço cibernético[9], assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional. Cabe, também, ao SMDC, assegurar a proteção cibernética do Sistema Militar de Comando e Controle (SISMC2[10]), garantindo às FA a capacidade de atuar em rede com segurança, bem como coordenar e integrar a proteção das infraestruturas críticas da informação de interesse da Defesa Nacional, definidas pelo MD.

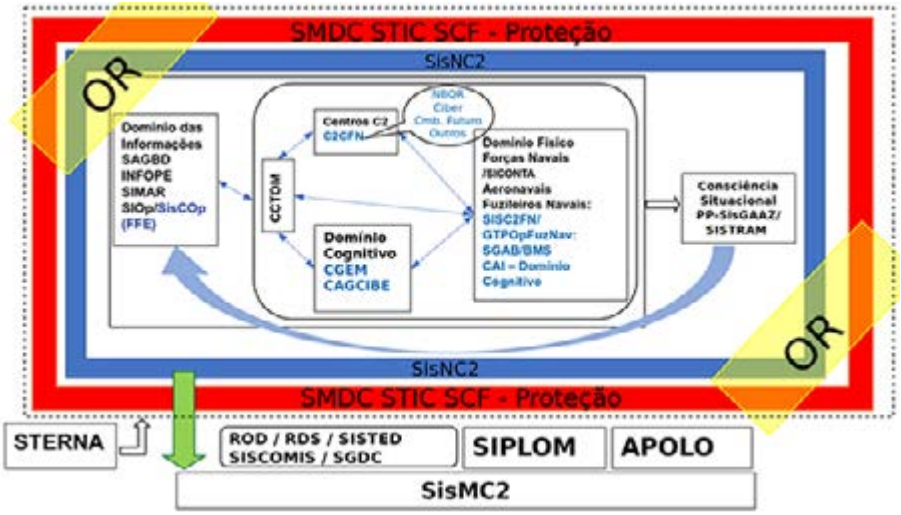
Para que o SMDC possa cumprir sua finalidade, faz-se necessário desenvolver, integrar e preparar, de modo contínuo e permanente, desde a situação de normalidade, as capacidades cibernéticas das FA e do MD, possibilitando o emprego operacional conjunto com o máximo de efetividade.

O EMCFA é o órgão responsável por assessorar o Ministro de Estado da Defesa na implantação e na gestão do SMDC, de modo a garantir, no âmbito da Defesa Nacional, a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança necessários.

O Centro de Defesa Cibernética (CDCiber) passa ao controle operacional do EMCFA/MD nas Operações Conjuntas e conta, permanentemente, com um Estado-Maior Conjunto para assessorar o Chefe do CDCiber na orientação, supervisão e condução das atividades de desenvolvimento, integração e preparo das capacidades cibernéticas das FA e do MD, levando em conta as particularidades de cada FA, de modo a obter uma atuação sinérgica.

De forma análoga, na MB, o Centro de Ações de Guerra Cibernética (CAGCiber - MB) é o centro de coordenação das ações cibernéticas nos níveis operacional e tático, incluindo o GptOpFuzNav no escopo do SISNC2 (ver Figura 1).

Figura 1: Mapa de visualização sistêmico.



Fonte: Autor.

Legenda:
SISTED – Sistema Tático de Enlace de Dados
STERNA – Sistema Tático de Enlace de Dados/MB
RDS – Rádio Definido por *Software*
SGDC – Satélite Geoestacionário de Defesa de Comunicação Estratégica
SCF – Sistema Ciber Físico
CISMAR – Centro Integrado de Segurança Marítima
SMDC – Sistema Militar de Defesa Cibernética
SGB/BMS – Sistema de Gerenciamento da Batalha/*Battle Management System.*

5. A Convergência GE x GCiber

Conforme o artigo *Ideas & Issues – GCiber / Informacion Operations*, a convergência é entendida como: "mistura de tecnologias, sistemas ou dispositivos, trata-se de um arranjo operacional, que objetiva criar uma estrutura para impedir/mitigar as ações do inimigo e estabelecer a Proteção de uma Força (ex: GptOpFuzNav), visando a sua eficiência, eficácia e efetividade." (RUSSEL, 2017, tradução nossa).

Sem uma estrutura sistêmica para empregar recursos de GCiber (*Cyberwarfare*) e GE (EW – sigla em inglês),

[8] A Doutrina Militar de Defesa Cibernética estabelece Guerra Cibernética (GC) como o uso ofensivo e defensivo de informação e sistemas de informação [...], no contexto de um planejamento ou operação militar de nível operacional ou tático, sendo desempenhada respectivamente por Comando Operacional e Forças Componentes. (BRASIL, 2014, p.19).

[9] O espaço cibernético é, por natureza, um espaço aberto desprovido de fronteiras tangíveis, onde tanto o setor público como o privado, civis e militares, atores nacionais e internacionais interagem de forma simultânea, interdependente e interligada. Por essas razões, não é um espaço seguro e protegido, sendo vulnerável a ataques cibernéticos, que podem ter como consequência perdas relevantes de ordem econômica e social ou constituir uma séria ameaça à Defesa Nacional, quer no plano da degradação ou destruição de infraestruturas críticas, quer no plano da neutralização ou negação ao acesso a recursos supranacionais.

[10] Sistema Militar de Comando e Controle - SISMC2 - (MD - 31 - 03, cap III, item 3,2). O SISMC2 é o conjunto de instalações, equipamentos, sistemas de informação, comunicações, doutrinas, procedimentos e pessoal essenciais ao C2, visando atender ao Preparo e ao Emprego das FA. Abrange os Sistemas Militares de C2 das FA, bem como outros sob a responsabilidade do Ministério da Defesa (MD).

o GptOpFuzNav corre o risco em desperdiçar a iniciativa das ações militares, deixando de responder às novas ameaças, tais como: terrorismo cibernético, pirataria.

Para estabelecer uma estrutura comum para a condução de operações do ciberespaço e do espectro eletromagnético, de modo que as vantagens tecnológicas possam ser utilizadas em proveito das nossas Forças, faz-se necessário concentrar os esforços na direção mais veloz do ciclo OODA.

A avaliação das necessidades futuras do Cyber e do EW e das capacidades técnicas individuais fornecem uma estrutura útil para descrever a convergência cibernética x EW para decisões políticas e programáticas/operativas. Essa abordagem *botom-up* é mais aceitável para descrever a convergência do que as abordagens teóricas e doutrinárias (*top-down*), e fornece a melhor oportunidade para "explorar" as competências individuais neste novo domínio.

As três principais ações dentro do ciberespaço são operações ofensivas, operações defensivas e operações de Rede de Informações (Operações em Rede - DMN). Quando comparado com as principais ações de guerra eletrônica (MAGE, MPE, MAE), um amplo alinhamento das ações e dos recursos *Cyber & EW* sugerem um possível modelo funcional de convergência Cyber x EW.

Isso, continua o artigo, faz com que *experts* sobre o assunto, em pauta, sejam frequentemente aprisionados pelas distinções paradigmáticas entre energia (EW) e código (*cyber*). Mas, como descreve o artigo referenciado, essas diferenças estão se tornando cada vez menores, particularmente no nível tático.

Uma revisão recente da Concepção Operacional dá pistas de que as ações no nível tático, tanto Cyber como EW, tornam-se opções atraentes também para as Forças Navais. Com isso, as capacidades operativas *Cyberwarfare* e do EW estão se tornando cada vez mais importantes para os escalões mais baixos de uma Força.

Conforme discutido no artigo em referência, o *cyber* e o *EW/EMS* são ferramentas fundamentais, desde o nível mais alto (estratégico), até os níveis mais baixos (Táticas, Técnicas, Procedimentos), que podem perfeitamente se organizar e operar sem prejuízo das atividades C2 e sem perda da Consciência Situacional.

Numa primeira leitura, pode-se inferir: o que distingue, a EW do *Ciberwafare*, nesta convergência, fundamentalmente, é que a primeira trata do controle da energia e a segunda cuida do controle de dados. Nesse sentido, visualiza-se a necessidade de formulação doutrinária para empregar as capacidades *Cyber*, em prol do GptOpFuzNav. Com isso, faz-se mister que se estabeleça um Sistema corporativo (SIC2CFN/SisC2DefNBQR / Combatente do Futuro) para a consecução de OR, no contexto do SMDC, em congruência ao SISCOMIS/SISMC2.

6. A Operação em Rede (OR) no Ambiente GE & GCiber

De acordo com a END, é necessário desenvolver as atividades de monitoramento e controle do espaço aéreo, do território, das Águas Jurisdicionais Brasileiras (AJB) e de outras áreas de interesse, aliados à capacidade de pronta - resposta a qualquer tipo de ameaça. Tais atividades demandam que, cada vez mais, as Forças possam operar em Rede, incrementando-se o intercâmbio de informações, o que, dadas as dimensões das AOp, exigirá a capacidade de se chegar, oportunamente, à região de interesse, de acordo com a capacidade de mobilidade estratégica.

A OR é uma concepção que remete às Forças (Navais, de Fuzileiros Navais e Aeronavais) a operarem no domínios da informação. Propicia condições para a interoperabilidade entre as Forças Singulares, contribuindo para a construção e a manutenção de uma Consciência Situacional (CS)e ao aprimoramento do ciclo OODA. Caracteriza-se pelo estabelecimento de um ambiente de compartilhamento, de modo a contribuir para a obtenção da superioridade de informação e da iniciativa das ações. (BRASIL, 2017b, p. 1-15 – 1-16).

Nesse sentido, o SISCOM/SISNC2 formata a estruturação de Rede da MB, indo ao encontro das premissas da Doutrina Militar de Defesa em consonância à DMN, incluindo-se a GE e GCiber nesse ambiente.

7. Impactos Operacionais da Operação em Rede nos GptOpFuzNav

A partir da conceituação de OR, avalia-se a necessidade de se ampliar as discussões sobre quais domínios de atuação serão adotados pela MB, em consonância à DMN.

Ainda para que sejam bem aplicados os conceitos de OR, de acordo com MD-31-M03, será necessário que as Forças Singulares estejam interconectadas nos domínios estabelecidos doutrinariamente, quais sejam: Domínios das Informações/Cognitivo/Físico – Tecnológico – o EB inclui o domínio social, que será adotado neste artigo (BRASIL, 2017a). A correta identificação e exploração dos domínios da OR permitem o entendimento mais aprimorado da Intenção do Coman-

dante; aumenta a velocidade do fluxo de informações; e, em decorrência, cadencia o ritmo das operações, contribuindo assim para que o ciclo decisório (OODA) seja mais ágil, em consonância ao conceito de "Guerra de Manobra".

Nesse viés de pensamento, o grau de interoperabilidade afetará a capacidade de conduzir as ações em terra. Por sua vez, uma acentuada interoperabilidade entre os sistemas C2 aumentará o fluxo das informações, proporcionando Consciência Situacional compartilhada, com uma visualização panorâmica do Campo de Batalha.

Dentre os impactos operacionais das OR, nos GptOpFuzNav, pode-se destacar os seguintes: ampliação da capacidade de planejamento, execução e controle de ações cibernéticas, seja de proteção, de exploração ou de ataque; incremento na capacidade de Inteligência; redução da vulnerabilidade cibernética dos equipamentos empregados em operações militares (ciberfísicos); e aumento da efetividade das operações em apoio às OpInfo e Opsico (domínio cognitivo e das informações).

A inserção do SIC2CFN e SisC2DefNBQR/Combatente do Futuro, nos GptOpFuzNav, incrementará a infraestrutura de TIC existente, permitindo a transmissão de voz e dados com relativa facilidade e segurança entre os componentes do GptOpFuzNav e o CAI. Desta forma, o Conhecimento será produzido de modo a permitir um salto qualitativo consciencial, em todos os níveis de C2 e, em decorrência, otimizar as práticas das técnicas, táticas e procedimentos (TTP).

Para cada nível de decisão e estabelecimento de uma Rede sustentada em recursos de TIC, torna-se imperativo a avaliação dos conceitos de Defesa Cibernética, GCiber e a consolidação doutrinária da Guerra Eletrônica nos GptOpFuzNav.

8. Além da Convergência

O livro "*Beyond Convergence – World Without Order*", editado por Hilary Matfess e Michael Miklaucic, do Center for Complex Operations, da Universidade de Defesa Nacional (NDU) trata da segurança internacional em um mundo caracterizado pela desordem, onde organizações criminosas (OCRIM), centradas em Redes, representam riscos substanciais aos interesses de segurança nacional. Além disso, as OCRIM desafiam os princípios fundamentais de soberania que norteiam o Sistema Internacional.

Os autores intitulam tais Redes como um verdadeiro "ecosistema criminal emergente", possuidor das seguintes tendências: convergência, hibridização e inflitração no Estado (...). Mais ainda, eles argumentam que embora o terrorismo, a insurgência e o crime organizado existam há muito tempo, no mundo atual, a ação destes atores é favorecida pelas ferramentas de TIC (...). Essas características permitiram aos atores ilegais se aproveitarem de tecnologia letal, armamento militar, informação em tempo real e diversos serviços de ordem jurídica, tecnológica, segurança, paramilitares.

A primeira seção / capítulo intitulado **"O desleixo em direção à distopia"** oferece uma visão de um mundo desamarrado dos princípios organizacionais (...). Essa parte prospecta os piores cenários mundiais de ataques ao Sistema Internacional. Inclui a discussão de Phil Williams sobre a crise da ordem internacional, argumentando que a governança global falhou devido à inabilidade dos Estados de se autogovernarem. Nils Gilman descreve o Estado, sob a pressão de "insurgências gêmeas", as redes dos plutocratas e as criminosas, ambas sem qualquer vinculo de lealdade para com o Estado. Scott Atran revela a profunda alienação em relação ao *status quo* global que leva ao extremismo que emerge como uma virtude redentora. Francis Fukuyama e Hilary Matfess examinam formas alternativas de governanças emergentes, que estão surgindo aleatoriamente (...).

Dessa temática, pode-se inferir que, no contexto do domínio cibernético evidencia-se a concepção de Defesa Cibernética como: "um conjunto de ações defensivas, exploratórias e ofensivas, realizadas no espaço cibernético, no contexto de um planejamento estratégico, com a finalidade precípua de proteger os sistemas de comunicações de um Estado-Nação; obter dados para a produção de Conhecimento/ Inteligência; e comprometer o STIC de forças assimétricas.

A segunda seção/capítulo, **"Uma Rede"**, examina a expansão das redes criminais existentes e explora suas características operacionais e implicações políticas. Descreve a extensão e interconectividade das redes criminais, grupos terroristas, e outros atores que permitem a corrosão externa do Estado (...). Discute a expansão da criminalidade e das normas anti - sistêmicas.

Nesta seção, pode-se observar que a OR perpassa as complexidades dos SISC2 em seus ambientes e conexões. No caso do GptOpFuzNav, pode-se inferir que torna-se requisito operacional, o estabelecimento de uma Rede de Informações, para cada nível de decisão (operacional, tático), visando fazer frente às ameaças assimétricas, nos domínios da GE e GCiber.

A terceira seção/capítulo **"Pandora"**: Descreve as recentes inovações que complicam o panorama da ameaça global. Discute a "mídia social", reforçando o papel dos atores antiestatais, permitindo a eles estabelecerem seguidores pseudocultos e facilitarem conexões com indivíduos (...). Mostra como as inovações tecnológicas produziram vulnerabilidades

no domínio cibernético, as quais estão sendo exploradas por OCRIM, terroristas e Estados hostis.

Neste viés de pensamento, as ações de GCiber tornam-se instrumentos nos três níveis de condução da guerra, seja político-estratégico, operacional e/ou indo mais além nas táticas, técnicas e procedimentos, no sentido amplo do Sistema de Gestão do Conhecimento (SGC- FN).

O último capítulo "**Uma caixa de ferramentas para o séc. XXI"**: Indica respostas aos novos desafios, com opções políticas tangíveis para mitigar as ameaças. Discute o papel crítico da estruturação do Estado como contraponto à ascensão dos atores ilícitos e ideologias atraentes (...). Detalha o apelo notável das ideologias destrutivas, as maneiras em que elas afetam a natureza do combate (...), e como as Forças Armadas podem se adaptar a este cenário. Apresenta uma solução organizacional do Estado, a partir da abordagem nominada *time to times*, do general Stanley McChrystal, tornando o processo de tomada de decisão mais ágil e efetivo, em face das ameaças.

Ainda, a obra evidencia que a ascensão da mídia social permitiu que grupos antiestatais atuem globalmente (...). Mais do que isso, as fraudes na Internet, tronaram-se campo para ação de "*hackers*" incorporados nos domínios da GCiber.

Disso tudo, pode-se abstarir que a GE e a Gciber, em convergência, podem ir além dos domínios sistêmicos convencionais, rompendo estruturas, tanto na base (infra) quanto no topo (supra). Que, em última análise, incorpora a dialética da tríade: desordem, caos, incerteza.

9. Conclusão

Assim, apoiado no trinômio desordem/caos/incerteza, evidencia-se a Guerra Eletrônica em suas dimensões multifacetadas, tanto nos contornos da Operação em Rede, como também na sua concepção meta situacional.

E, como resultado de uma análise sistêmica, o ponto de convergência com a Guerra Cibernética, identificado pelas interações no domínio social, e, pelo segmento terrestre e espacial, transborda as superestruturas governamentais, indo mais além, rompendo as barreiras supra - estatais.

Nesse cenário, as novas ameaças instrumentalizadas nas ferramentas de TIC, não somente reduzem os hiatos de capacidades entre forças convencionais e não convencionais, como também introduzem vulnerabilidades ao SISCOM/SISNC2 e em decorrência ao SIC2CFN/GptOpFuzNav.

Em síntese, a percepção operacional traz à tona um mundo complexo numa dinâmica disruptiva, na qual esta inserido o GptOpFuzNav como um ator coadjuvante tanto no sentido *top down* (Tomada de Decisão – Combatente do Futuro), como também *bottom up* (Combatente do Futuro – Tomada de Decisão).

Em suma: a Guerra Eletrônica em convergência à Guerra Cibernética tem que ser visualizada sob a panorâmica *lato sensu* dos níveis de condução da guerra (político – estratégico e operacional) e sob a ótica das estratificações das táticas, técnicas e procedimentos.

Referências

BRASIL. Exército. **EB70-MC-10.232**: 2017: Manual de Campanha de Guerra Cibernética. Brasília, 2017a.

BRASIL. Marinha. Estado-Maior da Armada. **EMA-305**: Doutrina Militar Naval. Brasília, 2017b.

BRASIL. Marinha. Corpo de Fuzileiros Navais. Comando-Geral. **CGCFN-60**: Manual de Comando e Controle dos Grupamentos Operativos de Fuzileiros Navais. Rio de Janeiro, 2008.

BRASIL. Marinha. Corpo de Fuzileiros Navais. Comando-Geral. **CGCFN-62**: Manual de Guerra Eletrônica dos Grupamentos Operativos de Fuzileiros Navais. Documento Reservado.

BRASIL. Marinha. Corpo de Fuzileiros Navais. Comando-Geral. **Portaria n. 29**, de 03 de abril de 2019. Designa os Oficiais que comporão o Grupo de Trabalho (GT), para estudar e apresentar a proposta dos Requisitos de Estado-Maior (REM) e dos Requisitos de Alto Nível de Sistemas (RANS) afetos à integração do "Projeto Combatente do Futuro" ao "Sistema de Comando e Controle de Defesa NBQR (SisC2DefNBQR)" e ao "Sistema de Gerenciamento da Amazônia Azul (SisGAAz)".

BRASIL. Ministério da Defesa. **END**: Estratégia Nacional de Defesa. Brasília, 2013,

BRASIL. Ministério da Defesa. **MD-31-M-03**: Doutrina do Sistema Militar de Comando e Controle. 3. ed. Brasília, 2015.

BRASIL. Ministério da Defesa. **MD-31-M-07**: Doutrina Militar de Defesa Cibernética. Brasília, 2014.

MATFLESS, Hilary; MIKLAUCIC, Michael. **Além da Convergência**: mundo sem ordem. Tradução Rudibert Kilian. Trasução de: Beyond Convergence: World Without Order.

RUSSEL, Brian. Cyberspace Operations and Eletronic Walfare Convergence, Part I: Skating to where the puck will be. **Marine Corps Gazette**. Quantico, VA, p. 67-71, july 2017.