ESCOLA DE GUERRA NAVAL

CC REINALDO LUÍS LOPES DOS SANTOS

A GUERRA CIBERNÉTICA EM UMA ESTRUTURA DE COMANDO E CONTROLE DE UMA FORÇA-TAREFA EM UMA OPERAÇÃO NAVAL

Rio de Janeiro

2012

CC REINALDO LUÍS LOPES DOS SANTOS

A GUERRA CIBERNÉTICA EM UMA ESTRUTURA DE COMANDO E CONTROLE DE UMA FORÇA-TAREFA EM UMA OPERAÇÃO NAVAL

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

Orientador: CF Fabiano Rebello Cantarino

Rio de Janeiro

Escola de Guerra Naval

2012

RESUMO

As guerras são acontecimentos que ocorreram ao longo dos anos por uma busca constante de poder entre povos e Estados. Como disse Thomas Hobbes em sua obra "O Leviatã", o "homem é o lobo dos homens", ele está em constante busca de poder. A história relata os diversos acontecimentos e as constantes evoluções das guerras ao longo dos anos. A fim de exemplificar, pode-se citar a criação do Estado-Maior, por von Moltke (1800 a 1891), que auxiliou a Prússia nas conquistas de diversas vitórias em diversas batalhas, dentre elas a guerra Franco-Prussiana ocorrida entre os anos de 1870 e 1871, contra França. O Estado-Maior servia para aperfeiçoar a guerra, para a execução dos planos de guerra e o assessoramento direto aos generais. De certa forma o Comando e Controle começava a ser empregado em batalhas. Os anos se passaram, e as evoluções da tecnológica e da telecomunicação aconteceram em uma velocidade assustadora. A internet foi criada, e como consequência, pessoas e Estados ficaram dependentes, fazendo com que ocorresse a perda de suas capacidades de controle e regulação dos fluxos globais de riquezas e informações estatais de interesse. Surge, desta forma, uma nova modalidade de guerra, a Guerra Cibernética, que passa a ser travada em um ambiente denominado de Ciberespaço, e que não pode ser mensurado, levando muitos autores a defender a tese de uma nova modalidade de guerra assimétrica, a guerra utilizada pelo Estado mais fraco contra o Estado mais forte. O estrategista SuntZu, em sua obra "A arte da guerra", quando citou os cinco fatores que governam a arte da guerra, não imaginou que o Ciberespaço iria surgir. Clausewitz, em sua obra "Da Guerra", que afirmou ser "a guerra é a continuação da política por outros meios", não podia imaginar que, com a evolução dos tempos, a Guerra Cibernética poderia ser um desses meios a ser utilizado por uma entidade Estatal. O Brasil, o Ministério da Defesa e a Marinha do Brasil, desde a publicação da Estratégia Nacional de Defesa, ocorrida no ano de 2008, estão se adequando e se estruturando a essa nova realidade. Finalizando, cabe destacar que a Guerra Cibernética pode ter consequências catastróficas para um Estado em seus diversos seguimentos, podendo ser executada desde os mais altos setores deste, até um segmento de Comando e Controle de uma Força Naval navegando em uma Operação Naval, colocando-o indisponível em sua utilização, cerceando ao Comandante a tomada de decisão. Destarte, o presente trabalho realiza uma análise sobre Guerra Cibernética em um Comando e Controle no âmbito de uma Força Naval em Operação e sugere algumas medidas para aperfeiçoar a sua capacidade no âmbito de uma Força em relação às novas ameaças surgidas no Espaço Cibernético.

Palavras-Chave: Guerra Cibernética; Espaço Cibernético; Comando e Controle; Força-Tarefa.

SUMÁRIO

1 INTRODUÇÃO

As relações entre os homens, e entre os Estados, desde a sua existência até os dias atuais, são marcadas pela busca constante de poder. Essa busca constante fica mais evidente ao longo da história quando desde o início os povos e os Estados guerreavam em busca de espaço e poder. Os diversos exemplos foram mostrados ao longo da história, e em especial no século XX, quando ocorreu a 1ª Guerra mundial (1914 - 1918) e a 2ª Guerra mundial (1939 - 1945), dois grandes acontecimentos globais militares que proporcionaram milhões de mortos e um rastro de destruição de diversos Estados participantes.

O surgimento da Guerra Fria (1947 - 1989), caracterizou uma etapa da história da humanidade marcada pelo conturbado relacionamento entre duas potências hegemônicas do momento, os Estados Unidos da América (EUA) e a ex-União das Repúblicas Socialistas Soviéticas (URSS). A "nova ordem mundial" surgiu, com a criação do conflito entre o capitalismo e o comunismo.

Com o sepultamento da Guerra Fria (1989)[1] os conflitos entre Estados sofreram profundas mudanças, não havendo mais a destruição em massa de cidades nem o massacre de populações, sendo as guerras conduzidas com ataques precisos a alvos determinados, fato esse exemplificado na condução da 1ª Guerra do Golfo, ocorrida em 1993.

Novas formas de conduzir a guerra foram introduzidas pelos Estados, como é o caso da Guerra Assimétrica, que é considerada por muitos autores renomados como a "a arte de guerrear que um Estado mais fraco usa contra um Estado mais forte".

Um novo cenário e percepção de novas ameaças e vulnerabilidades foram incrementadas, comprometendo a paz e a segurança internacional. Surgiu a internet. A partir

[1] Caracterizada pela derrubada do Muro de Berlim, em 9 de novembro de 1989, sendo considerada o seu marco em função de seu simbolismo.

de então, alterou-se profundamente o padrão das comunicações em escala mundial. O seu poder, juntamente com os novos progressos em telecomunicações e computação provocaram grandes mudanças tecnológicas, dos microcomputadores e dos mainframes descentralizados e autônomos à computação universal por meio da interconexão de dispositivos de processamentos de dados, existentes em diferentes formatos (CASTELLS, 2005).

A criação e o desenvolvimento da internet nas três últimas décadas do século XX foram consequências de uma fusão singular de estratégia militar, grande cooperação científica, iniciativa tecnológica e inovação cultural. A primeira rede de computadores, que na época foi denominada de ARPANET, entrou em funcionamento em setembro de 1969. (CASTELLS, 2005). Daquela época até os dias atuais, a internet mudou por meio do seu sistema de redes horizontais, da comunicação sem fio, do fácil acesso, pelo avanço ocorrido nas telecomunicações e na tecnologia, principalmente pela globalização ocorrida no mundo, que teve como uma das consequências à diminuição dos preços dos computadores e de seus periféricos.

A explosão da internet ocorrida nos últimos anos trouxe uma nova modalidade de ataques às redes de alguns órgãos estatais críticos. Ataques estes que vem aumentando significativamente ao longo dos anos, muitos encorajados pelos êxitos obtidos, pela relativa capacidade de ocultação do atacante, pelo baixo custo de seu ataque, e principalmente pela capacidade de ser realizada por qualquer tipo ou grupo de pessoa, sem discriminação de raça e sexo (CLARK; KNAKE, 2010). Uma nova modalidade de guerra foi originada após o fenômeno internet, a Guerra Cibernética (GCiber).

Com o avanço citado das telecomunicações a estrutura de Sistemas de Comando e Controle (C2), descrita como sendo o conjunto de instalações, equipamentos, comunicações, doutrinas, procedimentos e pessoal essenciais para auxiliarem ao Comandante (BRASIL, 2006), teve que sofrer alterações para se adaptarem a essas mudanças.

O Governo Federal, o Ministério da Defesa (MD) e a Marinha do Brasil (MB) estão se adaptando a essa nova realidade. No âmbito do MD, com a publicação da Estratégia Nacional de Defesa (END) no ano de 2008, o assunto passou a ser tratado com mais importância, ganhando o setor cibernético um destaque de maior valor nacional, cabendo ao Exército Brasileiro (EB) a sua gerência. No âmbito da MB pode-se considerar que o assunto foi iniciado no ano de 2008, quando o Centro de Tecnologia da Informação da Marinha (CTIM) passou a gerenciar o assunto referente a GCiber. Já no âmbito do Governo Federal, houve a criação do Grupo Técnico de Segurança Cibernética em 2009 (GT SEG CIBER).

Em virtude deste cenário que ora se apresenta, o propósito deste trabalho é identificar a influência da Guerra Cibernética sobre um Sistema de Comando e Controle de uma Força-Tarefa em uma Operação Naval, bem como identificar possíveis soluções para enfrentar essa nova modalidade de guerra atual.

O trabalho foi elaborado por meio de pesquisa bibliográfico-documental, fundamentada em livros, legislação, publicações doutrinárias, periódicos e artigos atinentes ao tema, e por meio da utilização de técnicas indiretas. Para alcançar o propósito pretendido, o trabalho compreende cinco capítulos: o segundo capítulo abrange as definições de guerra cibernética nos âmbitos internacional e do Brasil, no MD e na MB, pretendendo abordar nesse capítulo os conceitos de Guerra Cibernética e as suas ramificações, traçando um paralelo entre as doutrinas utilizadas no Brasil e fora dele; e comparar como a Estratégia Nacional de Defesa e o Livro Verde: Segurança Cibernética no Brasil, que balizam o assunto Guerra Cibernética está sendo adotado nas doutrinas utilizadas pela MB.

O terceiro capítulo aborda e pretende-se conceituar as definições de uma Força-Tarefa, C2 e os recursos de C2 em uma Força-Tarefa na MB; identificar, de acordo com a evolução tecnológica ocorrida ao longo dos anos, os recursos de C2 implementados pela MB;

identificar as possíveis vulnerabilidades na estrutura de C2 no tocante a Guerra Cibernética e o que se deve realizar para proteção de uma Força em Operação Naval.

O quarto capítulo aborda as consequências e soluções de uma Guerra Cibernética em uma estrutura de Comando e Controle de uma Força-Tarefa em Operação Naval. Nesse capítulo, pretende-se apresentar quais são as ações de Guerra Cibernética em um Comando e Controle; identificar as fragilidades em um sistema de Comando e Controle que está sendo utilizado pela MB nos dias atuais; identificar as possíveis soluções para que o ataque a uma Força-Tarefa em Operação Naval não seja realizado.

Ao final, no quinto capítulo, serão tecidos alguns comentários a título de conclusão.

2 DEFINIÇÕES DE GUERRA CIBERNÉTICA NOS ÂMBITOS INTERNACIONAL E DO BRASIL, NO MINISTÉRIO DA DEFESA E NA MB

Os avanços científicos e tecnológicos nos últimos trinta anos promoveram um aumento significativo por produtos e serviços baseados em tecnologia de informação, especialmente os relacionados a computação (BRASIL, 2010b).

Todos os dias, milhões de pessoas acessam a internet em busca e troca de informações e para efetuarem as mais diversas atividades de ordem pessoal e profissional. Com a vantagem nos acessos às atividades dos cidadãos e das organizações foram facilitadas, e, em contrapartida, trouxeram um risco que não foi vislumbrado na época da sua criação e que muitos utilizadores não possuem conhecimento da gravidade.

De acordo com o Instituto Brasileiro de Geografia Estatística (IBGE), o Brasil possuía 55,9 milhões de usuários de internet em 2008; e em 2009, 67,9 milhões. Assim, em 2008, os internautas representavam 34,8% da população e, em 2009, representavam 41,7%, o que demonstra uma curva significantemente crescente de acesso a rede, no país (BRASIL, 2010b).

Por trás destes acessos, um monitoramento realizado pelo Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CETIR Gov), órgão subordinado ao Gabinete de Segurança Instituicional da Presidência da República (GSI-PR), aponta que ocorrem cerca de duas mil tentativas de invasões maliciosas[2], por hora, nas 320 grandes redes do governo federal (BRASIL, 2010b).

Cabe ressaltar que atualmente muito se fala em GCiber. Devido às ameaças existentes no espaço cibernético, que será conceituado posteriormente, e de atos de diversos

[2] São invasões realizadas em computadores e redes, normalmente realizada por *hackers*, que são usuários avançados de computador que se dedicam a descobrir vulnerabilidades em sistemas de TIC, e que ilegalmente penetram em sistemas de computadores para danificá-los, obter informações ou para causar rompimento de redes, sendo ataques de autoria desconhecida, ou por curiosos e ataques de autoria desconhecida.

atores, o termo GCiber tende a vulgarizar-se. Com isso todo e qualquer incidente de ordem digital ocorrido em um computador, ou em uma rede de computadores têm sido tratado, equivocadamente e de forma generalizada. Para efeito deste trabalho, entende-se que os conflitos travados entre dois ou mais Estados no ciberespaço será tratado como GCiber. Já os assuntos inerentes a atividades desenvolvidas por atores não estatais, com danos a informações do ciberespaço serão tratados como incidentes cibernéticos, e que não serão abordados no presente trabalho (CLARK; KNAKE, 2010).

Assim, cabe ressaltar que como marco para o presente trabalho, faz-se mister a compreensão dos conceitos de *Cibernética*, *Guerra Cibernética*, de *Segurança Cibernética*, de *Defesa Cibernética* e *Espaço Cibernético* e *Tecnologia da Informação* (*TI*).

Ao observarmos as diferentes definições destacadas em diversas normas, publicações e livros no âmbito de Brasil e do exterior, obtêm-se diversos conceitos, dos quais podem-se destacar os seguintes.

Em se tratando de *Cibernética*, diz-se que o termo se refere ao uso de redes de computadores e de comunicações, e a sua interação dentro de sistemas utilizados por instituições públicas e privadas, de cunho estratégico, e exemplo do MD. No campo da Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC)[3], bem como os sistemas de armas e de vigilância (MELO DE CARVALHO, 2010).

A END destaca o fato de o setor cibernético ser decisivo para a defesa nacional, juntamente com o nuclear e o espacial, sendo os três setores considerados estratégicos para a defesa. Aponta também que diversos setores do Poder Executivo, dentre eles o GSI-PR, são responsáveis por lidar com ataques cibernéticos. A END enfatiza que os

[3] Conjunto de instalações, equipamentos, comunicações, doutrina, procedimentos e pessoal essenciais para o comando e controle, visando a atender as necessidades decorrentes do Preparo e do Emprego das Forças Armadas, consoante com a PDN e com a END. Abrange os sistemas de comando e controle da Forças, bem como os outros sob responsabilidade do Estado-Maior Conjunto das Forças Armadas (BRASIL, 2011).

setores cibernético e espacial devem permitir que as Forças Armadas, em conjunto, possam atuar em rede. No âmbito Forças Militares do Brasil, coube ao Exército Brasileiro gerenciar o assunto referente à Guerra Cibernética (BRASIL, 2008).

De acordo com a definição GCiber apontada por autor estrangeiro, um outro conceito que deve ser analisado é que indicam que são ações realizadas por um Estado para penetrar em computadores ou redes informatizadas de outro Estado, com a finalidade de causar danos ou perturbações nos mesmos (CLARK; KNAKE, 2010).

A definição de GCiber apontada no âmbito do MD na Doutrina de Operações Conjuntas, 1° volume (BRASIL, 2011) conceitua como:

> Guerra Cibernética é o conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informações e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil (BRASIL, 2011).

No âmbito da MB, dois conceitos são empregados sobre a GCiber. O primeiro retirado da Doutrina Básica da Marinha (DBM), que não conceitua o termo "Guerra Cibernética" propriamente dito, sendo utilizado o termo Ações de Guerra da Informação, e o segundo, retirado da Doutrina de Tecnologia da Informação da Marinha, fazendo sua referência direta ao termo "Guerra Cibernética". Assim a DBM aborda o tema:

> São aquelas que envolvem as ferramentas disponíveis no nível da informática e telemática para desestabilizar os sistemas operacionais e de comunicações do inimigo e, também, para possibilitar a defesa dos referidos sistemas amigos. Essas ações visam, principalmente, destruir, desativar, retardar ou confundir os sistemas de comando e controle pelo ataque deliberado à lógica operacional do sistema inimigo ou, no caso de sistema amigo, garantir a sua operacionalidade e confiabilidade (BRASIL, 2004).

Já a Doutrina de Tecnologia da Informação conceitua a GCiber:

> São ações ofensivas e defensivas destinadas a explorar, danificar ou destruir informações digitais, ou negar o acesso às suas informações. Tais ações utilizam-se de sistemas de informação e de redes de computadores (BRASIL, 2007a).

E como uma última definição de GCiber, são ações que são focadas em conflito interestatal. Independente de métodos e executantes, o que estará por trás das ações, de forma velada, ou não, será a agressão de um Estado a outro na busca da redução de poder nacional, que pode estar associada a outros métodos de ataque, inclusive físicos (ZUCCARO, 2011).

Ao analisar as definições extraídas de autor internacional, em normas no âmbito do MD e da MB, depreende-se que são bem similares, onde são apresentadas as expressões conflito ocorrido entre Atores Estatais; ações ofensivas e defensivas; incluem ambientes operacionais do oponente e do amigo; e ambas possuem propósitos comum que são a destruição das redes militares ou civil de um Estado para perda de informações.

Um outro conceito que deve ser analisado é que segundo a Política de Defesa Nacional (PDN), *segurança* é conceituada como sendo a condição que permite ao Estado Brasileiro a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais. (BRASIL, 2005).

Em um nível mais abaixo da PDN, podemos ressaltar os conceitos de *Segurança Cibernética* e *Defesa Cibernética*, que se confundem, mas na verdade possuem conceitos diferentes. De acordo com a norma do MD, *Segurança Cibernética* é a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas, estando diretamente relacionada a aspectos e atitudes tanto de prevenção quanto de repressão. Já a *Defesa Cibernética* compreende os conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com a finalidade de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de Inteligência e de causar prejuízos aos sistemas de informação do oponente (BRASIL, 2011).

No âmbito da MB, existem duas definições referentes à Segurança Cibernética que são: a) segurança do espaço cibernético, ou seja, a segurança das redes de computadores e de seus equipamentos de conectividade correlatos (BRASIL, 2007a); b) proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da Administração Pública Federal (APF) (MELO DE CARVALHO, 2011).

Já se tratando de Defesa Cibernética conceitua-se como sendo a defesa formada pelo conjunto das medidas de segurança de redes, proteção de informações sigilosas, segurança das estações de trabalho e servidores, políticas e procedimentos de segurança, capacidades e qualificação de pessoal, políticas de disseminação da cultura de segurança da informação, segurança física, adestramento, organização, desenvolvimento seguro de sistemas e criptografia de dados e voz (CLARK; KNAKE, 2010).

Depreende-se das citações que as definições de Defesa Cibernética no âmbito do Brasil possui um sentido bem direcionado, aonde se adotam ações defensivas, exploratórias e ofensivas, sempre com a finalidade de proteção e obtenção de dados para inteligência. Já na literatura do exterior tem um sentido mais amplo, porque aborda segurança de redes e periféricos, além de capacidades, pessoal envolvido e adestramentos, não sendo mencionadas as ações defensivas, ofensivas e de exploração.

De acordo com o I Workshop de Guerra Cibernética, organizado pela Diretoria de Ciência e Tecnologia da Informação (DCTIM), realizado na Escola de Guerra Naval nos dias 1 e 2 de junho de 2010, alguns conceitos são pertinentes e são extraídos do trabalho realizado:

a) *Ações Ofensivas de Guerra Cibernética*: são ações realizadas por meio de redes de computadores para interromper, negar degradar/corromper ou destruir a informação contida em computadores, redes e/ou sistemas de tecnologia da Informação (TI) inimigos;

b) *Ações Defensivas de Guerra Cibernética*: são ações realizadas por meio de redes de computadores para proteger, monitorar, analisar, detectar e responder à atividade não autorizada em computadores e/ou redes, de modo a garantir o uso continuado e a inviolabilidade dos nossos sistemas de TI; e

c) *Ações de Exploração de Guerra Cibernética*: são ações realizadas por meio de redes de computadores para a obtenção de informações sobre as vulnerabilidades dos sistemas de TI inimiga ou para a coleta de dados contidos nesses sistemas.

No tocante ao Espaço Cibernético, ou Ciberespaço, a nível das fontes internacionais, obtemos que é o espaço composto por centenas de milhares de computadores, servidores, "switches", e cabeamentos que permitem o funcionamento da infraestrutura da internet (CLARK; KNAKE, 2010); e que pode ser relatada como sendo um domínio global dentro de um ambiente de informação, cujo distintivo e único caráter é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar a informação através de redes interdependentes e interligadas através de tecnologias de informação e comunicação (KRAMER, 2009).

No âmbito do MD e adotada pela MB, o Espaço Cibernético é conceituado como o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas. Ações ofensivas no Espaço Cibernético podem impactar, inclusive, a segurança nacional (BRASIL, 2011) e (MELO DE CARVALHO, 2011).

Ao analisar as definições extraídas da MB da literatura estrangeira, depreende-se que são similares, onde são apresentadas as expressões redes conectadas, computadores e seus periféricos conectados em internet e sem fronteira física delimitada.

Verifica-se que o Setor Cibernético, na visão da END, não se restringe à Segurança e Defesa Cibernética, mas abrange, também, a Tecnologia da Informação e Comunicação (TIC), ferramenta básica para a implementação de redes de computadores (MELO DE CARVALHO, 2011).

Definimos que a Tecnologia da Informação (TI) é o conjunto de recursos tecnológicos empregados para a geração e o uso da informação (BRASIL, 2007a).

Outra definição de TI é o conjunto formado por pessoal técnico especializado, processos, serviços e recursos tecnológicos, incluindo equipamentos e programas que são utilizados na geração, no armazenamento, na veiculação, no processamento, na reprodução e no uso da informação (BRASIL, 2007b).

Portanto, embasado pelas referências e definições elencadas ao longo do capítulo, pode-se concluir que, para um ambiente militar e para a MB, há uma carência de documentos que defina os conceitos básicos relacionados à GCiber. Em relação às publicações já existentes, que possuem algum tipo de definição, há a necessidade de revisão e atualização de conceitos das referências doutrinárias para que contemplem e esgotem o assunto. Ressalta-se que os conceitos existentes relacionados direta ou indiretamente à GCiber, embora estejam alinhadas com os conceitos das fontes internacionais, estão distribuídos em diversas publicações e em livros didáticos no âmbito federal, demandando uma padronização desses conhecimentos, de modo a adequá-los ao emprego eficiente no âmbito da MB.

Conclui-se que a falta de conceitos estabelecidos e unificados em um documento doutrinário da MB impede que a Força se organize adequadamente para a organização, o planejamento e a execução das ações de GCiber. Com isso, para se efetuar um planejamento

em relação à GCiber no nível tático, há a necessidade de que a MB crie uma doutrina própria para emprego operativo da GCiber, através da edição de uma publicação que contemple as diretrizes emanadas do EB, que é quem coordena as ações de GCiber no âmbito do MD, para que tenha uma integração entre as três Forças Armadas (FA), quando operando em uma Operação Conjunta, ou operando isoladamente no âmbito operativo da MB, cabendo ressaltar ainda, que a norma, quando aprovada, deverá estar em sintonia com as exigências descritas na PDN, END e no Livro Verde: Segurança Cibernética no Brasil, livro este que foi organizado pelo Gabinete de Segurança Institucional da Presidência da República, no qual apresenta diretrizes básicas sobre a Segurança Cibernética no Brasil.

No próximo capítulo, serão abordados aspectos relacionados composição de uma Força-Tarefa (FT), definições de Comando e Controle (C2), os recursos utilizados pela MB para o emprego de C2 e a necessidade de seu eficiente emprego alinhados com as definições aqui abordadas.

3 DEFINIÇÕES DE UMA FORÇA-TAREFA, COMANDO E CONTROLE EM UMA FORÇA-TAREFA

A partir dos conceitos e definições apresentadas no capítulo anterior, destaca-se que a evolução da Era da Informação, e suas atividades no Espaço Cibernético encontram suas raízes remotas na construção dos primeiros computadores. Não resta dúvida de que o uso intensivo e indiscriminado do Espaço Cibernético, que não possui fronteiras, e que podemos considerá-lo o "Quinto Domínio da Guerra", após a terra, o mar, o ar, e o espaço exterior, somente se expandiu à velocidade espantosa com o advento da criação da internet.

A internet proporcionou a conectividade em tempo real, aumentando estrondosamente o volume e a rapidez na qual as informações tramitam e estão disponíveis para auxiliar os decisores. Isso fica cada vez mais latente nos dias atuais quando um Comandante de uma FT necessita de uma boa coordenação entre a emissão de ordens e suas diretrizes e o acompanhamento da evolução da situação e das ações desencadeadas durante uma operação. Essa coordenação depende diretamente de um fator chamado "informação". Para realçar, o Comandante de uma FT durante uma operação utiliza esse fator com as suas forças adjudicadas para repassar as suas orientações e ordens do comando; para coletar dados sobre o ambiente de guerra e sobre o seu oponente; para coletar dados sobre os seus meios adjudicados e para transmitir a maneira como a ação deve ser conduzida. O lado que possuir a melhor informação e utilizá-la mais eficazmente para obter a compreensão da cena de ação em questão terá maior vantagem sobre o seu oponente.

Para melhor entender o texto realçado acima, cabe à definição de alguns conceitos. Segundo a doutrina internacional, a Guerra de C2 consiste em uma das sete modalidades da Guerra de Informação, e que representa o conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as

informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos (CLARK; KNAKE, 2010). Já no âmbito do MD a Guerra de C2 é o uso coordenado de ações de segurança, despistamento, operações psicológicas, guerra eletrônica e destruição física, apoiadas por um sistema de inteligência, destinadas a negar informações, influenciar, degradar ou neutralizar capacidades de comando e controle do oponente, protegendo, ao mesmo tempo, a estrutura de Comando e Controle amiga (BRASIL, 2007a).

Depreende-se dos fatos citados de fonte internacional e da vigente no âmbito do MD que a Guerra de C2 procura negar o uso da informação pelo oponente e, ao mesmo tempo, proteger as informações da própria Força, de modo que não seja degradada e manipulada pelo oponente.

Para efeito deste trabalho cabe definir os conceitos de FT, C2 e os recursos utilizados em um C2 para uma FT.

Para a execução das operações, os meios alocados ao Comandante são agrupados por tarefas específicas, de acordo com o Processo de Planejamento Militar (PPM) da Marinha. A sua composição e a organização dos meios dependem da missão a ser cumprida pelo Comandante, da situação e das tarefas atribuídas aos vários componentes (BRASIL, 2004).

Uma FT está relacionada com uma organização por tarefa, que pode ser composta por três tipos de sistemas distintos, possuindo a finalidade de organizar as unidades operativas adjudicadas para os vários comandos, sendo denominadas de Organização por Tarefas, Organizações por Tipos e por Guerras. Para efeito do trabalho em questão só será abordado Organização por Tarefas (MTP-1D, 2002, tradução nossa).

A Organização por Tarefa, dependendo da sua tarefa, pode ser organizada em Grupos Tarefas (GT) que é uma Força Tarefa dividida em grupos, Unidades Tarefas (UT) que

é um Grupo Tarefa dividido em unidades, Elemento Tarefa (ET) que é uma Unidade Tarefa que pode ser dividida elementos tarefas (MTP-1D, 2002, tradução nossa).

Toda FT, quando designada para o cumprimento de uma missão, sempre terá um Comandante designado, que será uma autoridade que possui um poder individual nas forças armadas para direção, coordenação e controle das forças militares, e que, para cumprir a sua missão, possui uma Força Naval adjudicada a seu comando. A Direção é o processo de planejamento e tomada de decisões, estabelecendo prioridades, formulando políticas e impondo decisão; a Coordenação é o estabelecimento de operações, de acordo com mudanças de situações, com uma correlação coordenada no tempo e espaço das ações planejadas em ordem para um melhor resultado geral. No ambiente marítimo, termo coordenação pode incluir certas funções específicas de controle. Por último, o controle é a autoridade exercida por um comandante sobre parte das atividades de organizações subordinadas, ou outras organizações não normalmente sob seu comando, o qual inclui a responsabilidade de implementar ordens ou diretivas. Toda ou parte desta autoridade pode ser transferida ou delegada (MTP-1D, 2002, tradução nossa).

Depreende-se dos fatos citados que uma FT quando em uma Operação Naval poderá ser dividida em GT, UT e ET, onde os meios adjudicados são distribuídos em diversos grupos para realizarem tarefas específicas, para contribuir para o cumprimento da missão do Comandante, sendo todos esses meios subordinados ao Comandante da FT, que é investido no cargo para exercer Direção, Coordenação e Controle.

Para compreender o conceito de sistema de C2, faz-se mister compreender algumas definições, constantes da norma do MD que divide o conceito em componentes.

O MD definiu C2 como sendo a ciência e arte que trata do funcionamento de uma cadeia de comando e, nessa concepção, define-se que é uma atividade fundamental para o êxito das operações militares em todos os escalões de comando. Como atividade

especializada, sua execução será baseada em uma concepção sistêmica, com métodos, procedimentos, características e vocabulário que lhe são peculiares, envolvendo, basicamente, três componentes (BRASIL, 2011):

a) a autoridade legitimamente investida, decorrente das leis e regulamentos, atribuída a um militar para dirigir e controlar forças, sob todos os aspectos, apoiada por uma organização da qual emanam as decisões que materializam o exercício do comando e para onde fluem as informações necessárias ao exercício do controle (BRASIL, 2011);

b) a sistemática de um processo decisório que permite a formulação de ordens, estabelece o fluxo de informações e assegura mecanismos destinados à garantia do cumprimento pleno das ordens. Caracteriza-se pelo acompanhamento efetivo das ações em curso, confrontando-se os resultados da execução com o previsto no planejamento (BRASIL, 2011); e

c) o terceiro componente, e o mais importante para efeito desse trabalho, pois é por ele que uma FT pode sofrer um efeito adverso de GCiber pelo oponente, é representado por toda a estrutura, incluindo pessoal, equipamento, doutrina e tecnologia necessárias para a autoridade acompanhar o desenvolvimento das operações (BRASIL, 2011).

Depreende-se dos fatos citados acima que no tocante à GCiber, as atenções voltam-se para o terceiro componente do Comando e Controle que é o Sistema de C2, no qual inclui pessoal, equipamento, doutrina e tecnologia, e que é o caminho por onde uma FT pode sofrer influência da GCiber através de ações desenvolvidas por meio de um oponente.

Segundo foi depreendido da entrevista com o Capitão-de-Corveta Fernando Vidal Vianna Parente, 1° Adjunto da Seção de Inteligência/Operações do Comando da 1ª Divisão da Esquadra (ComDiv-1), com a evolução tecnológica ocorrida ao longo dos anos em que os meios navais da MB tiveram que se adaptarem, os recursos de C2 tornaram-se mais eficientes. A rapidez e o volume de informações aumentaram sobremaneira ao longo dos anos, tendo como consequência o significativo aumento da capacidade e do poder de tomada

de decisão do Comandante de uma FT. Para se adaptar essa realidade, vários recursos e sistemas foram implementados pela MB. Para facilitar o entendimento, os recursos de C2 adotados nos dias atuais por uma FT em uma operação, podem ser divididos em recursos que são gerenciados no âmbito de um FT, pelo próprio Estado Maior da FT, e os recursos que são gerenciados fora do âmbito da FT.

Para ilustrar, os recursos que são gerenciados no âmbito de uma FT são os seguintes: *Automatic Identification System (AIS)* que é um sistema de utilização obrigatória para toda a comunidade marítima internacional, em todas as classificações de navios, sendo utilizado para identificação automática dos dados dos navios que possuem o sistema, sendo composto por uma plataforma de software executada em computador, associado a um rádio transceptor marítimo da faixa de VHF (Very High Frequency); *Sistema de Análise de Exercícios Táticos da Esquadra - Auxílio à Navegação (SAETE-AN)* que foi desenvolvido pela MB, por intermédio do Centro de Apoio a Sistemas Operativos (CASOP), que tem a finalidade de auxiliar aos Comandos das Divisões da Esquadra na análise dos exercícios operativos realizados em uma comissão operativa, bem como para auxílio à tomada de decisão do Comandante da FT; *Rede Tática de Dados (RTD)* que foi desenvolvida pela MB, por intermédio do ComDiv-1, e que atualmente é gerenciada pelo CASOP, corresponde a uma Linha Tática para comunicação entre os meios componentes de uma FT, funcionando em forma de ferramenta no formato "chat" que tem como finalidade a comunicação entre navios e unidades de uma FT por meio de comunicação via VHF, ou por meio de comunicação via protocolo "IP", por meio de acesso a comunicação satelital através da Rede de Comunicações Integradas da Marinha[4] (RECIM). Essa rede sendo utilizada elimina a possibilidade de detecção da Força navegando, pois só utiliza transmissões na faixa de VHF; *Conexão de Dados e Telefônico com a RECIM através das Estações Móveis Navais das Bandas Ku e X*

[4] Conjunto de elementos computacionais, organizados em rede, que compõem a infraestrutura responsável pelo tráfego de informações (digitais e analógicas) no âmbito da MB (BRASIL, 2009a).

que foi considerado o maior avanço tecnológico implementado em um C2 dos meios navais, dos componentes terrestres, e de um Estado-Maior de um Comandante de FT. Navios e elementos de terra que possuem esta capacidade podem acessar ao sistema Lotus Notes, intranet, internet, a tecnologia *voice over IP*[5] (*VO-IP*) e ao sistema de vídeo conferência por meio do ambiente *web* que é disponibilizado pela Diretoria de Comunicação e Tecnologia da Informação (DCTIM) (VIANNA PARENTE, 2012).

Para ilustrar, os recursos que são gerenciados fora do âmbito de uma FT são os seguintes: *Sistema de Informação sobre o Tráfego Marítimo (SISTRAM)* que auxilia na busca de informações sobre o tráfego marítimo de interesse; *Sistema de Apresentação Gráfica de Banco de Dados (SAG-BD)* que foi desenvolvido pela MB, por intermédio do Comando de Operações Navais (ComOpNav), e tem como objetivo a apresentação da situação corrente na área de operação, através de uma plotagem gráfica dos fatores a serem acompanhados (Navios, Aeronaves, Conhecimentos Operacionais e Tropas de interesse) e dos Fatores Fixos (Pontos de Referência, Áreas Geográficas e Plataformas de Prospecção); *Sistema de Planejamento Operacional Militar (SIPLOM)* é o sistema de apoio à decisão prioritário dos CC² do SISMC², sendo empregado em Operação Conjunta a nível do MD, sendo utilizada como suporte a tomada de decisão e para comunicação entre as FA, sendo desenvolvida para acompanhar as operações e as atividades em uma Operação Conjunta, permitindo a manutenção da interoperabilidade entre as Forças. A responsabilidade sobre o sistema cabe ao MD.

Depreende-se dos fatos citados acima que por ser a GCiber uma atividade meio em uma guerra, os sistemas adotados pela MB, e mais precisamente em um Estado-Maior, que utiliza a conexão realizada pela RECIM para operar os seus sistemas, como por exemplo

[5] Internet Protocol é o conjunto de padrões e especificações que descrevem a forma pela qual os dados são divididos em pacotes. O endereço IP é um número único que identifica um computador ou dispositivo ligado a uma rede (LIBICK, 2009).

o SAG-BD,SISTRAM e SIPLOM, podem ser alvos de ataques cibernéticos pelo oponente, podendo ser considerado uma das fragilidades de um Comando e Controle, por se tratar do componente do C2 de maior alvo em uma guerra. Destaca-se que nesse trabalho a Conexão de Dados e Telefone com a RECIM através das Estações Móveis Navais (EMN) das Bandas Ku e X será abordada para efeito de proteção da FT em uma Operação Naval.

Como a MB só possui apenas uma rede a ser utilizada, não havendo uma diferenciação entre redes administrativa e operativa, sendo as duas utilizadas ao mesmo tempo, todos os meios componentes da FT que possuem as Estações Móveis instaladas a bordo, mesmo navegando em alto mar, e longe da costa, possuem a possibilidade de acessar a RECIM, dados via internet e suas caixas postais do sistema Lotus Notes, tendo a possibilidade de receber vários arquivos com potencial ofensivo, bem como sofrer uma invasão aos dados da FT, sendo considerados todos vulneráveis.

Assim sendo, com base nas referências citadas neste capítulo, este autor conclui que uma FT a qual possui meios adjudicados e um Comandante designado para o atingimento de uma missão, dependendo da complexidade da missão e da interação com diversos setores da MB, tem a sua execução realizada de maneira mais complexa. Para tal, com a evolução tecnológica ocorrida nos últimos anos, permitiu-se um o aumento da rapidez das informações trocadas entre o Comandante e seus meios adjudicados, bem como o volume de informações escoado pelos recursos de C2 existentes em uma Operação Naval, permitindo com isso que ocorresse uma redução na névoa da guerra[6], e o aumento da capacidade de sistemática de um processo decisório que permite a formulação de ordens, estabelece o fluxo de informações e

[6] É a falta de conhecimento que ocorre durante uma guerra. É a incerteza de cada lado sobre as capacidades e planos do inimigo. É também o caos que ocorre entre as forças aliadas quando ordens são mal interpretadas, por exemplo. A expressão é atribuída ao analista militar prussiano Carl von Clausewitz. Ele escreve: "A grande incerteza de todos os dados na guerra é uma dificuldade peculiar, pois toda ação deve, em certa medida, ser planejada na penumbra, a qual em adição freqüente - de um efeito de névoa ou luar - dá às coisas dimensões exageradas e aparência não-natural." (Revista Passadiço, 2007).

assegura mecanismos destinados à garantia do cumprimento pleno das ordens do Comandante durante a tomada de decisão; O sistema de C2 que é utilizado em uma guerra, depende diretamente do funcionamento de uma boa cadeia de comando e de seus recursos para que as informações e as decisões fluam para o exercício do controle; os sistemas utilizados em um C2 na MB podem ser alvos de ataques pelo oponente em uma GCiber e devem ter a sua proteção realizada durante toda a execução das ações; por não existir redes diferenciadas para tráfego administrativo e operativo, sendo utilizada a mesma rede, a capacidade de acesso a RECIM e a internet no mar por Navios que possuem Estações Móveis das Bandas X e Ku, tornam-se potenciais portas de para acesso de e-mails maliciosos e para invasão da rede de um C2 em plena operação naval.

Como consequência destas análises, o próximo capítulo tentará expor como são as formas de invasão de uma FT por um oponente, como a MB vem realizando a defesa de uma Força em uma Operação Naval, bem como da defesa é dependente de vários fatores para ser tornar eficiente.

4 CONSEQUÊNCIAS E SOLUÇÕES DE UMA GUERRA CIBERNÉTICA EM UMA ESTRUTURA DE COMANDO E CONTROLE DE UMA FORÇA-TAREFA EM OPERAÇÃO NAVAL

Como foi abordado no capítulo anterior, com a Evolução Tecnológica ocorrida ao longo do tempo, os meios navais da MB tiveram que sofrer mudanças para se adaptarem a essa realidade. Com a instalação de equipamentos de comunicação satelital pelos meios, houve uma melhora significativa nos fluxos de informação de um C2, facilitando sobremaneira nas tomada de decisões de um Comandante em uma Operação Naval. Destaca-se que toda facilidade gera uma reação contrária e que deve ser combatida. Uma FT que possui muitos meios com a possibilidade de acesso a recursos satelitais, possui inerente a essa capacidade o acesso à internet e a RECIM em plena operação no mar e a longas distâncias da costa, aumentando a possibilidade da Força sofrer um ataque cibernético em plena operação.

As fragilidades são muitas e para que elas sejam combatidas cabe ao Comandante da FT efetuar um rigoroso controle e impor uma série de restrições ao acesso pelos usuários durante a condução da comissão. Um simples acesso a um "e-mail" infectado com vírus[7] pode comprometer todo o C2 da FT, o que pode acarretar no comprometimento da missão do Comandante. O acesso à internet e ao correios Lotus Notes por intermédio da RECIM podem trazer riscos a irreparáveis a um C2. Para isso, deve-se ter a consciência de que as ações de exploração cibernética necessárias para a realização de uma ação ofensiva serão desenvolvidas desde o tempo de paz. A Defesa Cibernética começa pela conscientização de seus usuários. Os integrantes da MB devem entender que cada computador ligado a RECIM está, constantemente, na linha de contato da GCiber. Logo, o militar que estiver seu

[7] Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende de execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

computador “logado” na rede de sua OM, seja ele atracado ou no mar, deve ser considerado como um defensor cibernético. E os meios navais no mar também são considerados “logados” a RECIM por meio dos recursos satelitais que permitem esta facilidade. Assim é fundamental que cada um compreenda que a defesa cibernética da MB começa em sua estação de trabalho, sendo este pensamento o principal motivador para a criação de uma conscientização de segurança em todos os usuários. A internet e o correios Lotus Notes acessados do mar podem ser considerados portas de acesso a um ataque cibernético, principalmente por não ter a MB redes trabalhando de maneira independentes na área operativa e administrativas, e uma atenção especial devem ser dadas a essas facilidades.

A RECIM tem uma abrangência nacional, e alcança quase todos os continentes, interligando as Organizações Militares da MB em todo território brasileiro e no exterior (BRASIL, 2010). Como a MB só possui essa rede para atender as atividades administrativas e operativas, cabe ressaltar que dessa interação de atividades, a capacidade de acesso pelo oponente torna-se ainda maior, levando-se a se ter uma maior preocupação para defesa.

Conforme foi relatado na entrevista do Capitão-de-Corveta Fernando Vidal Vianna Parente, muitos dos recursos utilizados em um C2 necessitam dos recursos satelitais para sofrerem atualizações de seus sistemas. Dos recursos elencados, o SISTRAM, o SAG-BD, RTD-IP, SIPLOM, a Conexão de Dados e Telefônico com a RECIM através das estações móveis navais das bandas Ku e X e a Tecnologia VO-IP necessitam de internet e/ou acesso a RECIM para sofrerem atualização de seus sistemas. Somente o AIS e o SAETE-AN não necessitam de atualização por recursos satelitais, dependendo somente de equipamentos de comunicação na faixa de *VHF* (Very High Frequency). São por meio dos sistemas que sofrem atualizações por internet e/ou Lotus Notes que o oponente pode efetuar GCiber em relação a FT.

No mar, um sistema de C2 pode sofrer vários tipos de acessos ou ataques. Os ataques mais sofisticados começam com a pesquisa, dedicação e com a criatividade do ser humano. Descobrir suas vulnerabilidades em aplicações e sistemas operacionais e produzir códigos para explorá-las é a chave para o desenvolvimento do que chamaremos de artefato cibernético (CLARKE; KNAKE, 2010). Essas são as ações de Exploração Cibernética, que são realizadas por meio de redes de computadores para a obtenção de informações sobre as vulnerabilidades dos sistemas de TI do oponente ou para a coleta de dados contidos nesses sistemas. Pode-se constatar que se trata de uma atividade de Inteligência Cibernética.

Pode-se dizer que um sistema de C2 pode ser atacado por qualquer hacker, que pode ser contratado por um Estado, realizando este ataque de qualquer parte do mundo, e podendo ser realizado por meio de inúmeros recursos tecnológicos. Os estudiosos defendem que há uma sistematização nos ataques e que seguem cinco fases padrão. A primeira fase é o reconhecimento de quem se quer atacar; a segunda fase é a penetração; a terceira fase é a identificação dos recursos internos disponíveis, visando alterar o nível de privilégios de aplicativos de interesse do invasor; a quarta fase é que o invasor provoca danos e/ou subtrai as informações desejadas da vítima, ou seja, realiza ataque e exploração do oponente; a quinta fase é a que são incluídos mecanismos para remover as evidências da invasão, roubo ou outras ações ilícitas, aonde são editadas ou removidas informações dos registros de ocorrências (CLARKE; KNAKE, 2010). Nota-se que para obter sucesso num ataque e exploração algumas ações e elos devem ser explorados pelo oponente. É por isso que se pode afirmar que se uma FT possui uma eficiente Defesa Cibernética, o oponente deve empregar muitos recursos para obtenção de êxito no ataque. Dentre as ações que devem ser desencadeadas, buscar informações sobre a capacidade de C2 do oponente é fundamental para o sucesso do ataque. Observando-se as operações normais da vítima pelo oponente, podem-se obter informações tais como o tipo de “hardware” e “software” utilizados e comunicações

periódicas e regulares realizadas pelo oponente com os seus meios adjudicados para a realização da operação. Para que isso ocorra de forma eficiente, as ações de contra-inteligência e defensivas Cibernéticas tornam-se fundamentais para o sucesso do ataque. O Comandante de uma FT deve se preocupar na negação desses dados ao oponente para que dificulte o sucesso do ataque a Força.

Para que um ataque cibernético ocorra com êxito, são necessários alguns tipos de artefatos cibernéticos. Normalmente é utilizado um código malicioso (*malware*[8]), técnica ou um conjunto combinado de ambos que podem ser usados ofensivamente contra alvos inimigos. Existem vários tipos de códigos maliciosos como vírus, *worm*[9], *phishing*[10], *rootkits*[11], *trojan horse*[12], *spyware*[13] entre outros. Normalmente estes artefatos são introduzidos por meios de "e-mails" a quem for de interesse. Um Navio que possui acesso a Lotus Notes no mar pode ser considerado um alvo potencial para receber este tipo de artefato. Um militar desatento que abrir um "e-mail" contendo um desses códigos maliciosos pode infectar a sua estação de trabalho e a rede do seu Navio. Tais códigos devidamente adaptados ao ambiente alvo exploram as suas vulnerabilidades existentes nos sistemas operacionais, aplicações e ambientes de rede, afetando os serviços do oponente, capturando informações e/ou criando acessos remotos aos sistemas alvo. Destaca-se que os códigos maliciosos podem ser do tipo Conhecidos e Detectados por antivírus; ou Desconhecidos e não Detectados. Os objetivos de ataques podem as redes, sítios da internet e anexos de e-mail dentre outros.

---

[8] Palavra originária do inglês *Malicious software* (software malicioso).
[9] Programa capaz de se propagar automaticamente através de rede, enviando cópias de si mesmo de computador para computador. Diferente do vírus ele não embute cópia de si mesmo e não precisa ser executado.
[10] Mensagem não solicitada que passa por comunicação de uma instituição conhecida, como uma instituição bancária por exemplo, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. No início ele induzia ao usuário ao acesso a páginas fraudulentas na internet, atualmente, envia uma mensagem que induz ao usuário instalar códigos maliciosos nas máquinas acessadas.
[11] Programas que possui a finalidade de esconder e assegurar a presença de um invasor em um computador comprometido.
[12] Cavalo de Tróia.
[13] Expressão utilizada para se referir a uma grande categoria de software que tem como objetivo de monitorar atividades de um sistema e enviar informações coletadas para terceiros.

Diversos prejuízos a uma estrutura de C2 podem ocorrer com a realização de um ataque cibernético. Dentre eles, podem-se destacar o que é o principal objetivo de um ataque do oponente, que são as redes e o sistema de C2 do Comandante, o que acarretaria na perda da sua capacidade de tomar decisão e de coordenar as ações dos elementos subordinados. Outra capacidade que se pode destacar é a Negação de Serviço que é um ataque de negação de serviço que busca paralisar o acesso aos serviços de TI saturando-os com um alto volume de requisições. O sucesso dessa prática está no volume de requisições, e não na sua natureza, de forma que é muito difícil preveni-lo. Como exemplo de negação pode-se destacar o não recebimento das mensagens de atualização dos bancos de dados dos sistemas SISTRAM e SAG-BD, acarretando a não atualização do tráfego de navios mercantes e de pesca na área de interesse da Operação. O outro exemplo é o acesso pela RECIM do RTD por meio de IP, tendo o oponente nesse tipo de ação o acesso as mensagens geradas e trafegadas pelos meios e as posições dos Navios da FT por acesso as mensagens de posições dos meios que são geradas pelo AIS para envio ao SAETE-AN. Um exemplo mais crítico a ser citado seria a interrupção dos serviços satelitais, com o bloqueio do sinal do satélite. Com isso o Comandante perde toda a sua capacidade de acesso a RECIM, perdendo capacidades voz e dados, além da sua capacidade de atualização dos seus sistemas de C2 (VIANNA PARENTE, 2012).

Para que os fatos citados não ocorram, todo Comandante tem que se preocupar com a Defesa Cibernética de sua Força. Como foi destacado no segundo capítulo desse trabalho, a Defesa é formada pelo somatório das medidas de segurança de redes, proteção de informações sigilosas, segurança das estações, de trabalho e servidores, das políticas e dos procedimentos de segurança, das capacidades e das qualificações de pessoal, das políticas de disseminação da cultura de segurança da informação, da segurança física, do adestramento, da organização, do desenvolvimento seguro de sistemas e criptografia de dados e voz, enfim, é o somatório de utilizadores, dos processos, de material e de tecnologia para prover a segurança

de um FT, que visa contribuir para as garantias dos requisitos de disponibilidade, integridade, confidencialidade e autenticidade das informações digitais. Em um Comando e Controle, essa defesa se dará aos Sistemas de C2, local de maior fragilidade e por onde uma FT pode sofrer violações e ataques. Como a GCiber é uma atividade meio da guerra, é por essa subdivisão do C2 que se desenrolarão todas as ações de uma Operação. É por ela que um Comandante de FT deve ter total atenção para que a sua Força não sofrer ação de um oponente.

Para que a defesa de uma Força se torne eficiente, faz se mister a definição de "Defesa em Profundidade", que é a utilizada pela MB nos dias atuais, sendo a que é provida pelo somatório dos mecanismos de barreiras que são geradas entre o oponente e a rede aumentando a segurança como um todo (LIBICKI, 2009). Ou seja, nada mais é do que colocar diversas barreiras entre o sistema de C2 de uma FT e o oponente, para aumentar o esforço e os recursos empregados pelo oponente para o sucesso de um ataque, fazendo com que aumente as dificuldades no êxito do ataque a uma Força.

Ao se falar em defesa em profundidade, cabe destacar antes a estrutura de GCiber adotada pela MB, que desde o ano de 2008 vem sendo exercida pelo Centro de Tecnologia da Informação da MB (CTIM), que é o Órgão coordenador de TI da MB, sendo subordinado à DCTIM, que faz parte do setor de material[14] da MB, e é o órgão responsável por elaborar normas, instruções técnicas e procedimentos padronizados para as áreas de conhecimento concernentes ao emprego da tecnologia da informação na MB, inclui como atribuição a GCiber, ressaltando a tarefa de conduzir as atividades concernentes à GCiber, auditoria de

[14] Corresponde a toda a cadeia hierárquica da Diretoria-Geral de Material da Marinha e de suas Organizações Militares diretamente subordinadas. Disponível em: http://www.mar.mil.br/menu_h/organizacoes/organizacoes_mb.htm. Acesso em 20jun.2012.

segurança e forense computacional[15], sendo desempenhada através do Departamento de Guerra Cibernética (CTIM-20) constante em seu organograma[16] (BRASIL, 2010).

No que tange à GCiber no âmbito do setor operativo da MB, o Comando de Operações Navais possui um setor específico voltado para essa área desde o ano de 2006. Na palestra sob o título "As atividades de inteligência operacional desenvolvidas pelo Comando de Operações Navais" proferida ao Curso de Estado-Maior para Oficiais Superiores 2012, realizada na Escola de Guerra Naval, o Contra-Almirante Marcelo Francisco Campos, atual Subchefe da Subchefia de Inteligência Operacional (CON-20), apresentou a estrutura atual do ComOpNAv voltada para a área de GCiber. O CON-20 possui a Divisão de Contra-Inteligência (CON-23), que conta, como uma de suas seções, com a Seção de Segurança da Informação e Operações Cibernéticas (CON-23.2). Esta seção assessora o Comandante de Operações Navais nos assuntos afetos a GCiber, e nos assuntos concernentes à inteligência tecnológica voltada para a segurança da informação e da GCiber (CAMPOS, 2012).

Segundo a entrevista realizada ao Capitão-de-Corveta Fernando Vidal Vianna Parente, a estrutura de GCiber, ativada a nível tático, quando uma FT encontra-se em uma Operação Naval, é realizada com a CTIM passando a sua subordinação operativa ao ComOpNav (CON-20), que conduz todas as ações de GCiber durante a realização da Operação. No nível tático de FT, todo o assessoramento e suporte técnico é realizado pelo Centro Local de Tecnologia da Informação (CLTI-Mocanguê), que é subordinado ao ComemCh, que se encontra subordinado diretamente ao ComOpNav, atuando em conjunto com um dos Comandos de Divisão da Esquadra, que atua diretamente nos meios adjudicados para a realização da Operação (VIANNA PARENTE, 2012).

---

[15] É o emprego de técnicas e de procedimentos para a aquisição, preservação, identificação, extração, restauração, análise e documentação de provas computacionais armazenadas em mídias eletrônicas, a fim de atender demadas administrativas, jurídicas ou judicionais (BRASIL, 2007a).

[16] Estrutura administrativa do CTIM. Disponível em: http://www.ctim.mb/organograma.php. Acesso em 20jun.2012.

Antes do suspender dos Navios da FT para uma Operação Naval, o CLTI-Mocanguê realiza uma verificação na segurança das estações de trabalhos e servidores dos meios participantes da Operação, verificando os “antivírus”, “antispyware”, firewall pessoal, bem como as rotinas de atualização de sistemas operacionais e aplicações instaladas, com a finalidade de se detectar possíveis falhas para que não comprometam a segurança da FT e do C2 em uma Operação Naval, e durante toda a comissão ele fica responsável para servir de suporte para os meios no mar (VIANNA PARENTE, 2012).

Pelo que se depreende dos fatos citados, o procedimento de defesa em profundidade utilizado pela MB com ativação da estrutura de defesa de GCiber desde o ano de 2010, quando foi realizado o primeiro exercício de GCiber no âmbito da MB contra os meios de uma FT em Operação Naval, vem se demonstrando eficiente para atender os objetivos da Força.

Como a própria definição de Defesa diz, é importante abordar a capacitação de pessoal envolvido nessa guerra. Fica notório observar que a capacitação de pessoal é um fator preponderante para a estruturação da GCiber nas Forças Armadas, sendo este fato um motivo especial de destaque em diversas obras. O fato em questão é ressaltado quando Estados como o estadunidense, Rússia e China possuem escolas de formação para militares dedicados e GCiber, incluindo os hackers (CLARKE; KNAKE, 2010).

Para comprovar a importância de como o tópico capacitação de pessoal adquiriu grande importância, a END (2008) descreve que o futuro das capacitações tecnológicas nacionais de defesa depende mais da formação de recursos humanos de que do desenvolvimento de aparato industrial. Daí a primazia da política de formação de cientistas, em ciência aplicada e básica, já abordada no tratamento dos setores espacial, cibernético e nuclear (BRASIL, 2008a).

Segundo o Plano de Carreira para Praças da Marinha (PCPM), não há atualmente um quadro de formação específico voltado para a área de GCiber[17]. O Programa de Ensino da Marinha (ProEnsM), também não contempla um curso específico sobre GCiber voltados para oficiais e praças na MB[18].

De acordo com as tarefas listadas no anexo B deste trabalho, constata-se que os militares graduados nas especialidades de Comunicações Navais (CN), Eletrônica (ET), Sinais (SI), Administração (AD), técnico em Processamento de Dados (PD), Escrita (ES) e Técnico-Profissionais do curso de Qualificação Técnica Especial em Telemática (C-QTE-TL), que pelas suas áreas de atuação a bordo dos Navios, e que podem atuar na área de GCiber, pelos seus conhecimentos profissionais, não possuem em seus respectivos cursos tarefas relacionadas a GCiber (BRASIL, 2007).

Cabe ressaltar que os Navios não possuem em suas Tabelas de Lotação (TL) de bordo pessoal especializado em GCiber e nem filosofia de emprego assim como constatamos na guarnição de um canhão, ou na manutenção de um motor de combustão principal. Muitos Navios designam para exercer essa função militares que não possuem a devida qualificação técnica necessária para desempenho das funções exigidas. O militar, na maioria das vezes, tem a sua designação para esse tipo de função como encargo colateral, não permitindo uma dedicação integral a esse tipo de serviço em tempo integral (VIANNA PARENTE, 2012).

Depreende-se que mesmo com a devida importância dada pela END (2008) e diversas obras que tratam do assunto, a MB ainda não realizou significativas mudanças nos quadros e cursos para atenderem as demandas sobre o assunto. Os meios navais não possuem pessoal qualificado no assunto e a filosofia de emprego de GCiber, o que pode acarretar sérios problemas nos meios em operação naval. É recomendável que a MB identifique o quanto

[17] Publicação constante no site da DEnsM. Disponível em: http://www.dpmm.mb/site/indexn.html. Acesso em 20jun.2012.
[18] Publicação constante no site da DEnsM. Disponível em: http://www.dpmm.mb/site/indexn.html. Acesso em 20jun.2012.

antes se há recursos suficientes para a garantia da segurança de seus sistemas, planejando mudanças na formação e no treinamento de seu pessoal voltado para a área de GCiber.

Assim sendo, com base nas referências apresentadas, este autor conclui que a Defesa Cibernética é realizada pelo somatório da Conscientização do militares da MB no assunto GCiber e suas consequências para um FT, devendo a MB investir em todos os setores da instituição (Operativo e Administrativo) visando reduzir o risco do sucesso de um ataque e exploração por motivo de falta de consciência de um militar da MB. Muitos dos vírus que infiltram ataques não obterão sucesso, caso a conscientização dos militares seja efetiva. Na proteção de um C2, em seu componente de Sistemas de C2, que por seu somatório de pessoal, equipamentos, doutrinas e tecnologia, é considerada a porta por onde um oponente pode executar com êxito um ataque cibernético. Um Comandante de FT deve impor limites e restrições na utilização dos recursos dos sistemas de C2 durante a realização de uma Operação para que ocorra um controle efetivo e uma redução dos riscos de invasão e de ataque bem sucedido pelo oponente a sua Força; e na Capacitação dos Recursos Humanos, que fica evidente quando a MB ainda não apresentou nenhuma solução para mudança na formação de oficiais e praças na área de GCiber, destacando-se que faz se mister a necessidade de restruturação dos currículos dos cursos de formação de praças, tanto na fase de especialização como na fase de aperfeiçoamento, fazendo com que os militares graduados nas especializadas CN, ET, SI, AD/PD, ES e C-QTE-TL, que pelas suas áreas de atuação a bordo dos Navios, tenham capacitação relacionada aos fundamentos da segurança cibernética, tornando-se com isso um especialista na GCiber. No tocante ao oficial, temos como solução, o ingresso de oficiais do quadro Técnico, bacharel em engenharia da computação e ciência da computação, e que trabalhará exclusivamente na área de GCiber. No caso dos oficias oriundos da Escola Naval, faz se necessário à inclusão de uma disciplina voltada a GCiber nos diversos cursos de aperfeiçoamentos, seja ele de superfície, aviação, submarino, mergulhador de combate e

hidrografia, que são realizados como requisito de carreira no posto de primeiro-tenente, fazendo com que, assim como o oficial do Corpo da Armada, em seu curso de aperfeiçoamento de superfície aprende as diversas guerras, nos diferentes ambientes, tais como de superfície, anti-submarino, anti-aérea e eletrônica, inclua neste curso mais um ambiente de guerra denominado GCiber, permitindo que um oficial oriundo da Escola Naval, a medida que vai ficando mais antigo na carreira, independente do aperfeiçoamento realizado, possa assumir funções voltadas para GCiber nas diversas Organizações Militares da MB.

5 CONCLUSÃO

A Guerra Cibernética é um assunto considerado muito complexo e sua evolução nos dias atuais é notória. Todos os atores estatais possuem uma dependência dos recursos computacionais, bem como, a internet, para evolução e sobrevivência nos diversos setores, seja ele econômico, como nas transações bancárias e no comércio eletrônico, ou seja no controle de infraestruturas básicas, como o controle de distribuição de energia e água.

Fica notório, conforme demostrado no capítulo 2, que para um ambiente militar como o da a MB, há carência de uma norma que defina os conceitos básicos relacionados à GCiber. Ressalta-se que os conceitos empregados, embora estejam alinhados com os preconizados com nas literaturas internacionais, a falta de normatização impede a organização adequada da Força em um planejamento e na execução das ações de GCiber.

Dentro do exposto, para se efetuar um planejamento em relação à GCiber no nível tático há a necessidade de: 1- Criar uma doutrina própria para emprego operativo da GCiber no âmbito da MB quando operando isoladamente; 2-Editar de uma norma que contemple as diretrizes emanadas do EB, que é coordenador das ações de GCiber no âmbito do MD, a fim de obter a integração entre as três FA, quando operando em uma Operação Conjunta; e 3 - Garantir que a norma, quando aprovada, estará em sintonia com as exigências descritas na PDN, END e no Livro Verde: Segurança Cibernética no Brasil.

Conforme analisado no capítulo 3, a evolução tecnológica ocorrida nos últimos anos, permitiu o aumento na rapidez das informações compartilhada entre o Comandante e seus meios adjudicados, bem como o aumento do volume de informações escoado pelos recursos de C2 existentes em uma Operação Naval. Este aumento na rapidez da troca de informações e do volume da mesma, permite uma redução na névoa da guerra, e o aumento da capacidade sistemática de um processo decisório, onde se formula ordens, estabelece fluxo de

informações e assegura mecanismos que controla o pleno cumprimento das ordens do Comandante durante a tomada de decisão.

Conforme citado no capítulo 4, um sistema de C2 da MB podem ser alvos de ataques pelo oponente em uma GCiber e devem ter a sua proteção realizada durante toda a execução das ações. Por não existir redes diferenciadas para tráfego administrativo e operativo nos navios e sedes de comandos, a capacidade de acesso a RECIM e a internet por Navios quando no mar, tornam-se potenciais portas para acesso de e-mails maliciosos e para invasão da rede de Comando e Controle em plena operação naval. Sugere-se, desta forma, a criação de uma rede operativa para trabalhar de forma independente da administrativa já existente.

Destaca-se que a Defesa Cibernética é realizada pelo somatório da Conscientização do militares da MB no assunto GCiber e suas consequências para a FT. Recomenda-se que a MB investa em todos os setores da instituição (Operativo e Administrativo) visando reduzir o risco de ataque a rede interna por terceiros.

Na proteção de um sistema de C2, em sua subdivisão de Sistemas de C2, que é considerada a porta por onde um oponente pode executar com êxito um ataque cibernético recomenda-se, conforme analisado no capítulo 4, que o Comandante de FT deva: 1- Impor limites e restrições na utilização dos recursos dos sistemas de C2 durante a realização de uma Operação, a fim de que ocorra um controle efetivo deste sistema e uma redução dos riscos de invasão e de ataque bem sucedido pelo oponente; 2 - Capacitar os Recursos Humanos.

Porém fica evidente que a MB ainda não apresentou nenhuma solução para mudança na formação de oficiais e praças na área de GCiber, destacando-se que faz se mister a necessidade de restruturação dos currículos dos cursos de formação de praças, tanto na fase de especialização como na fase de aperfeiçoamento.

Neste contexto, o trabalho apresenta, conforme analisado no capítulo 4 a seguinte reestruturação de currículos: 1 - Os militares graduados nas especializadas CN, ET, SI, AD/PD, ES e C-QTE-TL, tenham adicionadas as suas formações matérias relacionadas aos fundamentos da segurança cibernética. 2 - Ao oficial, sugere-se o ingresso de militares do quadro Técnico, bacharel em engenharia da computação que se especializará exclusivamente na área de GCiber; e 3 - Aos oficias oriundos da Escola Naval, faz se necessário à inclusão da disciplina voltada a GCiber nos diversos cursos de aperfeiçoamentos, seja ele de superfície, aviação, submarino, mergulhador de combate e hidrografia. Desta forma, o curso de aperfeiçoamento de superfície incluirá a GCiber no contexto das diversas guerras, nos diversos ambientes, permitindo que este oficial possa assumir funções voltadas a GCiber nas diversas Organizações Militares da MB, independente do aperfeiçoamento realizado.

REFERÊNCIAS

BRASIL. Centro de Tecnologia da Informação da Marinha. **Organograma de 20 de junho de 2012**. Disponível em: < http://www.ctim.mb/organograma.php>. Acesso em 20 jun.2012.

BRASIL. Comando de Operações Navais. **Organograma de 20 de junho de 2012**. Disponível em: <http://www.con.mb/gabinete/gabinete.htm>. Acesso em 20 jun.2012.

BRASIL. Comando de Operações Navais. **RELATÓRIO DA MESA 01**: I Workshop de Guerra Cibernética da Marinha do Brasil. Rio de Janeiro, 2010.

BRASIL. Decreto n. 5.484 de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 1º jul. 2005, Seção 1, p. 5, Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm>. Acesso em 30 jul. 2012.

BRASIL. Decreto n. 6.703 de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 19 dez. 2008, Seção 1, p. 4, Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm>. Acesso em 30 jul. 2012.

BRASIL. Diretoria de Ensino da Marinha. **DEnsM-1001:** coletânea das relações de tarefas técnico-profissionais do corpo de praças da armada e do corpo auxiliar de praças. Rio de Janeiro, 2007.

BRASIL. Diretoria Geral de Material da Marinha. **DGMM-0540:** normas de tecnologia da informação da Marinha. Brasília, 2010.

BRASIL. Diretoria Geral de Material da Marinha. **Organograma de 20 de junho de 2012**. Disponível em: <http://www.mar.mil.br/menu_h/organizacoes/organizacoes_mb.htm>. Acesso em 20 jun.2012.

BRASIL. Estado-Maior da Armada. **EMA-305:** doutrina básica da Marinha. Brasília, 2004.

BRASIL. Estado-Maior da Armada. **EMA-410:** plano de desenvolvimento científico-tecnológico e de inovação da Marinha. Brasília, 2009.

BRASIL. Estado-Maior da Armada. **EMA-416:** doutrina de tecnologia da informação da Marinha. Brasília, 2007a.

BRASIL. **Livro Verde: Segurança Cibernética no Brasil**/Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Rafael Mandarino Junior – Brasília: GSIPR/SE/DSIC, 2010b. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em 30 jul. 2012.

BRASIL. Ministério da Defesa. **MD35-D-03**: Doutrina Militar de Comando e Controle. Brasília, 2006.

BRASIL. Ministério da Defesa. **MD35-G-01:** Glossário das Forças Armadas. Brasília, 2007b.

BRASIL. Ministério da Defesa. **MD35-M-01:** Doutrina de Operações Conjuntas, 1° volume. Brasília, 2011.

CAMPOS, Marcelo Francisco. **As atividades de Inteligência Operacional desenvolvidas pelo Comando de Operações Navais.** Rio de Janeiro:[s.n], 2012. Palestra proferida para o CEMOS na Escola de Guerra Naval em 12 de junho de 2012.

CANINAS, Osvaldo Peçanha. A Névoa da Guerra e a Fricção nos conflitos atuais: Pontos fundamentais na gestão dos conflitos modernos. **REVISTA PASSADIÇO**, Ed 27. 2007. Disponível na página na internet do *Centro de Adestramento Marques de Leão* em: < https://www.mar.mil.br/caaml/passadico2007portugues.htm>. Acesso em 30 jul.2012.

CASTELLS, Manuel. **A sociedade em rede**: A era da informação: economia, sociedade e cultura. 8 ed. São Paulo: Paz e Terra, 2005.

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

FRANÇA, Júnia Lessa; VASCONCELLOS, Ana Cristina. **Manual para Normatização de Publicações Técnico-Científicas**. 8. Ed. Belo Horizonte: Ed. UFMG, 2007.

LIBICKI, Martin C., **Cyberdeterrence and cyberwar**. RAND Corporation. 2009.

MELO DE CARVALHO, Paulo Sergio. Artigo **Conferência de Abertura: O Setor Cibernético na Guerra Cibernética**. Livro: Desafios Estratégicos para Segurança e Defesa Cibernética, organizado por RÊGO BARROS, Otávio Santana, GOMES, Ulisses de Mesquita, FREITAS, Whitney Lacerda de, Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

_____. ZUCCARO, Paulo Martino. Artigo **Tendência Global em Segurança e Defesa Cibernética – Reflexões sobre a Proteção dos Interesses Brasileiros.** Livro: Desafios Estratégicos para Segurança e Defesa Cibernética, organizado por RÊGO BARROS, Otávio Santana, GOMES, Ulisses de Mesquita, FREITAS, Whitney Lacerda de, Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

NATO, **Multinational Maritime Tactical Instructions and Procedures**, vol I , Change 4. U.S, 2008.

VIANNA PARENTE, Fernando Vidal. **Fernando Vidal**: inédito. Rio de Janeiro, 24 de maio de 2012. Entrevista concedida ao autor da monografia.

ANEXO A

O Capitão-de-Corveta Fernando Vidal Vianna Parente, exerce atualmente a função de 1° Adjunto da Seção de Inteligência/Operações do Comando da 1ª Divisão da Esquadra, que trata do assunto "Guerra Cibernética" no âmbito das comissões do Comando-em-Chefe da Esquadra (ComemCh).

1 – Quais são os recursos utilizados pelo ComDiv-1 em seu Comando e Controle (C2) em uma Comissão Operativa em Força-Tarefa (FT)?

R: **a)** SISTRAM (Sistema de Informação sobre o Tráfego Marítimo): O ComDiv-1 se utiliza da versão WEB (on line) do sistema para a busca de informações de interesse durante a realização de uma comissão operativa no âmbito da Esquadra.
b)SAG-BD: Sistema de Apresentação Gráfica – Banco de Dados;
c)AIS (Automatic Identification System) do navio Capitânia que é apresentado no programa SAETE-AN;
d)SAETE-AN (Sistema de Análise de Exercícios Táticos da Esquadra - Auxílio à Navegação);
e)RTD (Rede Tática de Dados);
f)SIPLOM (Sistema de Planejamento Operacional Militar): é um Sistema de suporte à decisão, desenvolvido para acompanhar as Operações Conjuntas e as atividades operacionais das Forças. É utilizado somente durante as operações combinadas, sob responsabilidade do MD;
g) Conexão de Dados e telefônico com a RECIM através das EMN (Estações Móveis Navais) das bandas Ku e X;
h) Tecnologia VO-IP (Voice over IP) Voz sobre IP;
i)Sistema de videoconferência via WEB disponibilizado pela DCTIM;
j) Rádio de VHF Marítimo com os canais MIKE;
k)Monitores para melhor visualização (apresentação) dos vários sistemas;
l) TV de LCD até 42" para melhor visualização do posicionamento dos navios através do SAETE-AN;
m) Equipamento de Comunicações Satelitais de uso comercial (Fleet Broadband – FBB 250/500) com acesso a voz, VO-IP e dados;
n)Notebooks para acesso aos vários sistemas; e
o) PRC para comunicações entre o Chefe de Operações e os Oficiais de Serviço no COC da Força.
Obs.: Embora a ComOpNavInst 32-01A (NORMAS PARA A TROCA DE INFORMAÇÕES DO SISTEMA NAVAL DE COMANDO E CONTROLE (SISN2)), dê uma idéia dos Sistemas que compõem o SISNC2, somente o SISTRAM (Sistema de Informação sobre o Tráfego Marítimo) através da versão on line (plataforma WEB) e o SAG-BD (Sistema de Apresentação Gráfica – Bando de Dados) são efetivamente utilizados como Sistema de Comando e Controle em uma Comissão Operativa.

2 – Quais são os recursos satelitais disponíveis na estrutura de C2 do Estado-Maior (EM) do ComDiv-1 em uma comissão Operativa em FT?

R.: O ComDiv-1 se utiliza dos recursos satelitais encontrados no Capitânia. Como não existe uma padronização dos equipamentos de comunicações satelitais utilizados pelos navios da Esquadra, podemos encontrar os seguintes recursos:

a) EMN das Bandas X ou Ku, permite voz e dados;
b) Equipamento de Telefonia do Sistema IRIDIUM, permite voz e dados;
c) Equipamento FleetBroadband de Comunicações Satelitais do Sistema INMARSAT, modelos 500 e 250, permite voz e dados;
d) Equipamento MINI-M de Comunicações Satelitais do Sistema INMARSAT, permite somente voz; e
e) Equipamento INMARSAT-C, permite somente dados.
Obs.: a) O ComDiv-1 possui um equipamento FleetBroadband (FBB) 250 que é instalado somente quando o navio Capitânia não possui um equipamento FBB-500 ou 250 instalado. Quando ele já possui o equipamento instalado e fins preservar o nosso equipamento, é feito somente a troca do SIM-CARD.

3 – O EM e os navios componentes da FT possuem a capacidade de acesso a internet durante uma comissão operativa em FT? Caso afirmativo, como é possível este acesso e como é realizado o controle de acesso à internet durante a comissão?

R.: Sim, quando o capitânia possuir comunicações satelitais das bandas X ou Ku. Porém os navios dotados deste recurso devem seguir o item 2.5 da DCTIMARINST 10-01 quanto ao quantitativo de usuários de correio eletrônico e acesso à internet. Para o EM de um Comando de Força no mar, o quantitativo fica a critério do 1ºAdjunto da Seção de Inteligência/Operações a quem cabe autorizar o acesso aos oficiais pertencentes ao EM (exceto Almirante, CEM e Chefe de Seção) do Comando de Força levando-se em consideração a necessidade funcional para o acesso.
Extrato da DCTIMARINST 10-01:
2.5-Agência postal para uso no SISCOMIS
Os terminais dos navios e as viaturas do CFN que possuem acesso ao sistema pela banda X ou Ku, poderão possuir uma agência de correio eletrônico específica para o tráfego operativo via satélite com a seguinte configuração:
a) número máximo de 15 (quinze) usuários de correio eletrônico;
b) número máximo de 5 (cinco) usuários com acesso a INTERNET;
c) agência postal com acesso via satélite segregada da agência administrativa;
d) cada agência postal terá no mínimo duas caixas postais obrigatórias, a saber:
ADMIN – para uso de mensagens relativas à administração do recurso, de uso dos administradores de rede;
MSG – para tráfego de mensagens.
Não está previsto o tráfego de documentos administrativos por esta agência, por tanto a mesma não deverá possuir caixa postal SECOM.
Os arquivos que trafegam por esta agência deverão possuir o tamanho máximo de 1MB.

4 – Existem programas ou sistemas utilizados em C2 do EM do ComDiv-1 que dependem da internet para atualização ou funcionamento durante uma comissão operativa em FT? Caso afirmativo, relacione-os.

R.: Não, nenhum sistema ou programa utilizado hoje para Comando e Controle necessita da internet para sua utilização, mas alguns sistemas necessitam de intranet e lotus notes para realizarem atualizações, como por exemplo SISTRAM, SAG-BD e vídeo conferência.

5 – Os navios participantes de uma FT utilizam-se de internet para realizar comunicação com o Comandante de uma FT (CFT)? Caso afirmativo relacioná-los?

R.: Em alguns casos, sim. Porém este canal só é utilizado nas comissões que envolvam meios estrangeiros como a UNITAS e FRATERNO entre outras. Nas comissões nacionais é proibido o uso da internet para comunicações entre os meios da FT.

6 – Em sua opinião os militares dos navios da Esquadra são conhecedores do assunto Guerra Cibernética?

R.: Não. Embora ultimamente tenham sido realizadas palestras para os OSID e ADMIN das OM da Esquadra, o assunto não tem sido levado por estes aos utilizadores finais, causando assim, um déficit de conhecimento sobre o assunto por parte da guarnição das OM da Esquadra.

7 – Qual é o procedimento adotado pelo ComDiv-1 na preparação antes do início da comissão e durante a comissão no tocante a Guerra Cibernética?

R.: Quando a Diretiva é expedida, fazemos uma solicitação ao CLTI-Mocanguê para que realize uma varredura nos meios envolvidos e no próprio ComDiv-1 a procura de falhas de segurança como portas abertas desnecessariamente, serviços ativos que comprometam a segurança como o compartilhamento de arquivos, pastas e impressoras, entre outros. A partir daí, o CLTI-Mocanguê mantém um acompanhamento através do Console ePO da McAfee de todas as estações de trabalho conectadas à rede dos navios da FT que possuam conexão da banda X ou Ku. Caso seja detectada qualquer anormalidade, como por exemplo o aumento expressivo de vírus detectados por uma estação de trabalho, o CLTI-Mocanguê avisa ao ADMIN do meio e ao ADMIN do Comando de Força que expediu a Diretiva.

8 – Em sua opinião os navios da Esquadra possuem militares habilitados para atuarem no assunto “Guerra Cibernética”?

R.: Não possuem pessoal qualificado para atuar no ramo da Guerra Cibernética. Quase a totalidade dos Navios da Esquadra não possuem militares qualificados para exercerem a função de guerra cibernética. Quem atualmente trata do assunto nos Navios são os administradores de rede dos meios.

9 – Caso a FT sofra um ataque Cibernético, qual é o procedimento adotado para combater este ataque?

R.: Não existe ainda um procedimento a ser adotado em caso de ataque cibernético. O ataque cibernético pode ocorrer da várias maneiras. O mais usual é o encaminhamento de “e-mail” contendo links maliciosos e arquivos anexos com vírus. Os ADMIN e OSID devem sempre disseminar as orientações para este tipo de ataque, seja através de adestramento ou em notas em plano do dia.

10 – Existe alguma estrutura especial ativada durante a realização de uma comissão operativa em FT no que diz respeito à “Guerra Cibernética”?

R.: Não existe. Atualmente, só é montada uma estrutura especial quando é programado um exercício de “Guerra Cibernética” concomitante com a realização de determinada operação. O CTIM passa a subordinação operativa do ComOpNav para tratar realizar o controle e as ações de GCiber durante toda a comissão.

11 – Caso uma FT sofra um ataque Cibernético, quais seriam as implicações no tocante a C2 para o EM e navios?

R.: A principal implicação poderia ser a negação de acesso (Access Denied) dos sistemas informatizados através do aumento de tráfego na rede e também a perda de dados sigilosos.

ANEXO B

Extrato da publicação **DEnsM-100:**Coletânea das Relações de Tarefas Técnico-Profissionais (RTTP) do Corpo de Praças da Armada e do Corpo Auxiliar de Praças:

QUADRO DE ESPECIALISTAS DO CORPO DE PRAÇAS DA ARMADA

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE COMUNICAÇÕES NAVAIS (CN):

1 - Cumprir os procedimentos adotados no Serviço de Comunicações da MB, relativos à utilização dos meios elétrico e postal, com o grau de sigilo desejado;
2 - Operar e auxiliar na manutenção dos equipamentos de comunicações, seus acessórios e quadros de distribuição de freqüências da OM;
3 - Cumprir a regulamentação da UIT para o Serviço Móvel Marítimo, com atenção ao tráfego de socorro e de emergência;
4 - Executar e registrar as rotinas do Sistema de Manutenção Planejada (SMP);
5 - Aplicar conceitos e procedimentos de Guerra Eletrônica (MAGE, CME, CCME) no que concerne à operação dos equipamentos de comunicações;
6 - Empregar o "software" para determinação de MUF / FOT;
7 - Empregar o código QUEBEC;
8 - Consultar e atualizar as publicações empregadas no serviço de comunicações;
9 - Operar o terminal de microcomputador da Rede de Comunicações Integradas da Marinha (RECIM);
10 - Efetuar digitação em microcomputador;
11 - Operar os "softwares" de comunicações, incluindo os de criptografia, em uso na MB;
12 - Identificar os procedimentos de destruição em emergência (equipamentos e publicações);
13 - Identificar os perigos para a vida humana inerente às atividades de comunicações navais (trabalho em locais altos, operações com equipamentos energizados, exposição à radiação eletromagnética e à fumaça), adotando as precauções de segurança preconizadas;
14 - Empregar as informações dos manuais técnicos, de modo a obter o máximo rendimento na operação dos equipamentos sob sua responsabilidade;
15 - Identificar, operar e auxiliar na manutenção das antenas existentes na OM;
16 - Identificar e operar os equipamentos de emergência utilizados pelo Sistema Marítimo Global de Socorro e Segurança;
17 - Cumprir as normas para processamento, tráfego e arquivamento de mensagens;
18 - Identificar as estruturas das redes de computadores utilizadas nas OM da MB; e
19 - Identificar itens pelo seu número de estoque nos diversos sistemas empregados pela MB, a partir de manuais técnicos, planos ou listas da dotação de sobressalentes para efetuar pedido de material.

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE ELETRÔNICA (ET):

1 - Empregar as informações de manuais técnicos na interpretação do funcionamento de equipamentos eletrônicos;
2 - Interpretar diagramas esquemáticos de circuitos eletrônicos;
3 - Interpretar a simbologia empregada para componentes eletrônicos;
4 - Utilizar medidores digitais e analógicos para verificar valores de tensão, corrente, resistência e outras variáveis;
5 - Utilizar o osciloscópio em suas diversas aplicações;
6 - Realizar pesquisa de avarias em unidades modulares;

7 - Realizar a operação e auxiliar na manutenção, testes, ajustes e reparos, ao nível de primeiro escalão, em equipamentos eletrônicos, componentes discretos e modulares, à vista das especificações disponíveis;
8 - Executar e registrar as rotinas do Sistema de Manutenção Planejada (SMP);
9 - Auxiliar na montagem, desmontagem e instalação de equipamentos eletrônicos;
10 - Avaliar o funcionamento de equipamentos de teste;
11 - Cumprir as precauções de Segurança relativas à operação ou reparo de equipamentos e componentes eletro-eletrônicos;
12 - Auxiliar na confecção dos pedidos de serviço e acompanhar o andamento do reparo junto às OM de apoio;
13 - Empregar as informações de publicações de sobressalentes e catálogos de componentes Eletrônicos;
14 - Fazer a manutenção de ferramentas e instrumentos de trabalho;
15 - Localizar e identificar unidades e partes componentes de radares, sonar, repetidoras, equipamento de IFF e equipamentos de CME / MAGE;
16 - Auxiliar na execução dos testes, ajustagens e reparos necessários à operação de servomecanismos, equipamentos eletro-mecânicos, eletro-eletrônicos e circuitos de controle com síncronos;
17 - Auxiliar na execução das medidas de sensibilidade, seletividade e alinhamento de circuitos de equipamentos eletrônicos, realizando, sob supervisão, os ajustes necessários;
18 - Aplicar os conceitos e procedimentos de Guerra Eletrônica (MAGE, CME e CCME) no que concerne à operação e auxiliar na manutenção dos equipamentos de CME/MAGE; e
19 - Identificar itens pelo seu número de estoque, nos diversos sistemas empregados pela MB, a partir de manuais técnicos, planos ou listas de dotação de sobressalentes para efetuar pedidos de material.

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE SINAIS (SI):
1 - Executar a vigilância, recepção, interpretação e transmissão de sinais de comunicação visual, com o navio em viagem ou no porto;
2 - Cumprir os procedimentos adotados no Sistema de Comunicações da MB, relativos à utilização dos meios ótico, postal e elétrico (dados e fax), com o grau de sigilo desejado;
3 - Cumprir as normas para processamento, tráfego e arquivamento de mensagens;
4 - Localizar um navio em seu grupamento operativo, utilizando o diagrama do dispositivo, e identificar a composição do grupamento da qual sua unidade faz parte;
5 - Codificar e decodificar mensagens, empregando o Código Internacional de Sinais e o Código Tático Naval;
6 - Identificar e utilizar sinais pirotécnicos, observando as precauções de segurança;
7 - Utilizar o prumo de mão;
8 - Inspecionar as luzes de navegação, de marcha, de cerimonial, de serviço e de comunicações visuais;
9 - Distinguir pavilhões nacionais de nações estrangeiras de interesse e as bandeiras dos estados;
10 - Identificar tipos de navios e aeronaves;
11 - Reconhecer os sinais de previsão de tempo;
12 - Cumprir, no que lhe competir, o Cerimonial da Marinha do Brasil;
13 - Identificar luzes, marcas e sinais sonoros e luminosos convencionados no RIPEAM;
14 - Identificar os procedimentos de destruição em emergência (equipamentos e publicações);
15 - Reconhecer ou transmitir sinais que se relacionam com avarias, homem ao mar, socorro; emergência (inclusive de aeronave) e mau tempo, utilizando os canais do meio ótico e acústico;

16 - Receber sinais horários;
17 - Executar rotinas de manutenção e reparos, dentro de suas atribuições dos equipamentos de comunicações visuais;
18 - Consultar e atualizar as publicações empregadas no serviço de comunicações;
19 - Cumprir as precauções de segurança na execução das tarefas pertinentes ao pessoal de sinais;
20 - Identificar o uso e limitações de holofotes, escotes, semáforas, bandeiras e demais recursos de comunicações visuais;
21 - Operar o terminal de microcomputador da Rede de Comunicações Integradas da Marinha (RECIM);
22 - Operar os "softwares" de comunicações, incluindo os de criptografia em uso na MB; e
23 - Identificar itens pelo seu número de estoque nos diversos sistemas empregados pela MB, a partir de manuais técnicos, planos ou listas da dotação de sobressalentes para efetuar pedido de material.

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE ADMINISTRAÇÃO (AD), TÉCNICO EM PROCESSAMENTO DE DADOS (PD):

HABILIDADES	TAREFAS
Monitorar sistemas	1- Monitorar recursos de rede; 2- Monitorar recursos de entrada, armazenamento e saída de dados; 3- Monitorar disponibilidade e desempenho de aplicativos; 4- Monitorar registros de erros; e 5- Monitorar consumo de CPU.
Administrar processamento de dados	6- Administrar cronograma de atividades planejadas; e 7- Administrar recursos disponíveis.
Assegurar funcionamento de hardware e software	8- Inicializar e desativar sistemas e aplicativos; 9- Configurar e reconfigurar hardware; 10- Realizar limpezas periódicas em equipamentos; 11- Requisitar manutenção preventiva e corretiva de hardware e software; 12- Reparar, recuperar e transferir arquivos, programas e relatórios; 13- Identificar e sanar falhas em hardware e software; 14- Assegurar funcionamento de equipamento reserva (contingência); 15- Assegurar funcionamento do cabeamento; e 16- Auxiliar na operação de computadores e periféricos.
Garantir segurança das informações	17- Fazer cópias de segurança (back up) e guardá-la em local prescrito; 18- Fazer rodízio de mídias; 19- Controlar acesso lógico do usuário; 20- Destruir informações sigilosas descartadas em meio magnético; e 21- Bloquear as máquinas para acesso de pessoas não autorizadas.
Atender ao usuário	22- Orientar o usuário na utilização de hardware e software; 23- Prestar suporte técnico disponibilizando recursos operacionais; 24- Auxiliar o analista nas definições e alterações dos sistemas; 25- Manter atualizado o cadastro de programas existentes; e

	26- Controlar arquivos do material de processamento de dados, de documentos normativos e técnicos da área.
Inspecionar ambiente físico de trabalho	27- Sugerir mudanças na disposição de equipamentos; e 28- Organizar cabeamento.

QUADRO DE ESPECIALISTAS DO CORPO AUXILIAR DE PRAÇAS

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE ESCRITA (ES):

1 - Executar trabalhos de digitação de documentos empregando o método de dez dedos;
2 - Elaborar documentos administrativos observando as regras estabelecidas nas normas sobre documentação na Marinha;
3 - Elaborar documentos relativos a controle de pessoal, controle de publicações e processos de concessão de condecorações;
4 - Elaborar documentos relativos a processos licitatórios e a atos e acordos administrativos conforme as normas competentes;
5 - Elaborar documentos e processos de comprovação, operar aplicativos específicos e exercer a função de agente subordinado ou de Fiel nas contas de gestão e de responsabilidade: Caixa de Economias, Execução Financeira, COPIMED, Pagamento de Pessoal e Civil, Material e SISBENF, Municiamento e Suprimento de Fundos;
6 - Manusear documentos ostensivos e sigilosos, observando as normas inerentes a documentos classificados, quando aplicáveis;
7 - Organizar coletâneas e arquivar documentos observando técnicas vigentes e de acordo com as normas competentes;
8 - Operar equipamentos básicos de suporte à execução dos serviços inerentes à SECOM, abrangendo scanner, fac-símile e copiadora reprográfica;
9 - Operar o sistema de correio eletrônico padronizado para uso na Marinha;
10- Operar programas de informática relacionados a assinatura eletrônica e criptografia autorizados no âmbito da Marinha;
11- Operar os aplicativos de informática referentes a automação de escritório, padronizados para uso na Marinha, constituídos de: sistema operacional para microcomputadores, editor de textos, planilha eletrônica, gerador de banco de dados, apresentação gráfica e software de navegação na INTERNET/INTRANET (browser);
12- Operar os aplicativos de informática adotados para uso geral na Marinha, desenvolvidos por Diretoria Especializada competente, no ambiente de computação para grupos de trabalho (workflow). Lotus Notes/SISDEM;
13- Operar dos sistemas corporativos da Marinha relacionados às áreas da Sistemática do Plano Diretor (SPD), do abastecimento, do pessoal e do pagamento de pessoal;
14- Operar os sistemas de informação padronizados da Marinha, de auxílio à administração geral, relacionados a pessoal, catálogos, boletins, legislação e documentação; e
15- Operar os sistemas de administração do Governo Federal: Sistema Patrimonial Imobiliário da União (SPIU), Sistema Integrado de Administração Financeira (SIAFI), Sistema Integrado de Administração de Pessoal (SIAPE), Sistema de Cadastramento Unificado de Fornecedores (SICAF), Sistema de Divulgação Eletrônica de Compras e Contratações (SIDEC) e demais sistemas implementados no âmbito do Sistema Integrado de Administração de Serviços Gerais (SIASG) aos quais tenha havido incorporação ou adesão da Marinha.

TAREFAS TÉCNICO-PROFISSIONAIS DO CURSO DE QUALIFICAÇÃO TÉCNICA ESPECIAL EM TELEMÁTICA (C-QTE-TL):

1 - Aplicar as técnicas e ferramentas de organização e métodos do trabalho;
2 - Aplicar os procedimentos adequados à realização de atividades de instrução;
3 - Aplicar os conhecimentos relativos à estrutura do Sistema de Comunicações da Marinha (SISCOM) e seu vínculo com a Agência Nacional de telecomunicações (ANATEL), em proveito das comunicações dos meios navais, aeronavais e de fuzileiros navais;
4 - Aplicar os conhecimentos relativos à estrutura da Rede de Comunicações Integradas da Marinha (RECIM) e seu relacionamento com a Tecnologia da Informação, em proveito das comunicações dos meios navais, aeronavais e de fuzileiros navais;
5 - Empregar softwares, principalmente de sistemas em tempo real, em proveito dos sistemas de telecomunicações utilizados pelos meios navais, aeronavais e de fuzileiros navais;
6 - Aplicar as técnicas de manuseio, operação e reparos em tecnologias de fibras óticas;
7 - Analisar o funcionamento e o comportamento dos diversos módulos componentes dos sistemas ópticos, elétricos e eletrônicos, afetos às comunicações analógicas e digitais;
8 - Executar, sob supervisão, tarefas de montagem, instalação, manutenção, diagnose, adaptação de hardwares e equipamentos de sistemas de comunicações digitais e analógicos aplicáveis nas Telecomunicações e Telemática**,** utilizados nos Sistemas Digitais Operativos (SDO) e Sistemas Digitais Administrativos (SDA), pertencentes aos meios navais, aeronavais e de fuzileiros navais, empregando as tecnologias utilizadas nas áreas de telecomunicações e redes, principalmente topologia das redes, arquitetura e protocolos, transmissão de sinais, gerenciamento, monitoração e segurança;
9 - Aplicar as técnicas de gravação de firmwares aos microprocessadores usados nos meios navais, aeronavais e de fuzileiros navais;
10 - Aplicar as técnicas relativas ao armazenamento, controle de versões de softwares e firmwares; e
11 - Elaborar relatórios, auxiliar na elaboração de normas técnicas e registrar informações sobre o desempenho de equipamentos de sistemas de telecomunicações.

QUADRO DE APERFEIÇOADOS DO CORPO DE PRAÇAS DA ARMADA

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE COMUNICAÇÕES NAVAIS (CN):

1 - Supervisionar as tarefas relacionadas à especialização em Comunicações Navais e executá-las nas condições compatíveis com seu grau hierárquico e situação funcional;
2 - Adestrar e supervisionar o pessoal subalterno no cumprimento da regulamentação da UIT para o Serviço Móvel Marítimo, com atenção ao tráfego de socorro e de emergência;
3 - Adestrar e supervisionar o pessoal subalterno na sintonia, operação e realização de rotinas de manutenção de equipamentos e no cumprimento dos procedimentos de comunicações;
4 - Efetuar a manutenção dos equipamentos de comunicações e antenas sob sua responsabilidade, no escalão de sua competência;
5 - Preparar pedido de serviço para correção de anormalidades em equipamentos de comunicações sob sua responsabilidade, em escalão superior ao de sua competência;
6 - Interpretar o Plano de Comunicações de uma diretiva e preparar as tabelas necessárias ao serviço de comunicações de sua OM;
7 - Empregar as informações dos manuais técnicos, de modo a obter o máximo rendimento na operação dos equipamentos sob sua responsabilidade;
8 - Supervisionar o cumprimento das normas de segurança inerentes às atividades de Comunicações Navais, incluindo o procedimento de destruição em emergência; e

9 - Efetuar a manutenção dos terminais de microcomputador da Rede de Comunicações Integradas da Marinha (RECIM).

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE ELETRÔNICA (ET):

1 - Supervisionar as tarefas relacionadas à especialização em Eletrônica e executá-las nas condições compatíveis com seu grau hierárquico e situação funcional;
2 - Supervisionar e executar os serviços de operação, teste, ajuste e reparo de equipamentos eletrônicos de sua responsabilidade;
3 - Identificar as características e a aplicação dos circuitos lógicos e da eletrônica digital;
4 - Executar os testes, ajustagens e os reparos necessários à operação de servo-mecanismos, equipamentos eletro-mecânicos, eletro-eletrônicos e circuitos de controle com síncronos;
5 - Executar medidas de sensibilidade, seletividade e alinhamento de circuitos de equipamentos eletrônicos, realizando os ajustes necessários;
6 - Pesquisar e detectar avarias, a nível de sistema;
7 - Supervisionar a execução e o registro das rotinas do Sistema de Manutenção Planejada (SMP);
8 - Supervisionar a instalação e a montagem de equipamentos eletrônicos de sua responsabilidade e acompanhar os respectivos testes de aceitação;
9 - Manter atualizados os Livros-Histórico dos equipamentos (testes, avarias, reparos, procedimentos e demais ocorrências dignas de registro);
10 - Aplicar os conceitos e procedimentos de Guerra Eletrônica (MAGE, CME e CCME) no que concerne à operação e executar a manutenção dos equipamentos de CME/MAGE;
11 - Elaborar relatórios conclusivos de avarias;
12 - Conduzir programas de adestramento sobre a atividade profissional e precauções de segurança;
13 - Operar, manter e reparar os equipamentos dos sistemas de aquisição de dados táticos e de direção de tiro; e
14 - Confeccionar os pedidos de serviço e acompanhar o andamento dos reparos junto às OM de Apoio.

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE SINAIS (SI):

1 - Supervisionar as tarefas relacionadas à especialização em Sinais e executá-las nas condições compatíveis com seu grau hierárquico e situação funcional;
2 - Adestrar e supervisionar o pessoal de sinais nos diversos serviços de comunicações visuais, incluindo a identificação de navios e aeronaves;
3 - Organizar o serviço de comunicações visuais no âmbito de uma força, navio ou OM de terra;
4 - Supervisionar a manutenção preventiva e corretiva dos equipamentos da navegação e sinais;
5 - Preparar pedidos de serviço para os equipamentos sob sua responsabilidade;
6 - Executar procedimentos da tabela de destruição de equipamentos em emergência;
7 - Cumprir as normas de segurança relativas à guarda e ao manuseio do material e das publicações que ficam sob sua responsabilidade; e
8 - Interpretar o Plano de Comunicações de uma diretiva e preparar as tabelas necessárias ao serviço de comunicações visuais de sua OM.

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE ADMINISTRAÇÃO (AD), TÉCNICO EM PROCESSAMENTO DE DADOS (PD):

HABILIDADES	TAREFAS
Administrar processamento de dados	1- Supervisionar tarefas relacionadas à especialização e executá-las nas condições compatíveis com seu grau hierárquico e situação funcional; 2- Conduzir planejamento e adestramento sobre as atividades profissionais; 3- Administrar cronograma de atividades planejadas; e 4- Administrar recursos disponíveis.
Monitorar sistemas	5- Monitorar recursos de rede; 6- Monitorar recursos de entrada, armazenamento e saída de dados; 7- Monitorar disponibilidade e desempenho de aplicativos; 8- Monitorar registros de erros; e 9- Monitorar consumo de CPU.
Assegurar funcionamento de hardware e software	10- Inicializar e desativar sistemas e aplicativos; 11- Configurar e reconfigurar hardware; 12- Realizar limpezas periódicas em equipamentos; 13- Requisitar manutenção preventiva e corretiva de hardware e software; 14- Reparar, recuperar e transferir arquivos, programas e relatórios; 15- Identificar e sanar falhas em hardware e software; 16- Assegurar funcionamento de equipamento reserva (contingência); 17- Assegurar funcionamento do cabeamento; e 18- Auxiliar na operação de computadores e periféricos.
Garantir segurança das informações	19- Fazer cópias de segurança (back up) e guardá-la em local prescrito; 20- Fazer rodízio de mídias; 21- Controlar acesso lógico do usuário; 22- Destruir informações sigilosas descartadas em meio magnético; e 23- Bloquear as máquinas para acesso de pessoas não autorizadas.
Atender ao usuário	24- Orientar o usuário na utilização de hardware e software; 25- Prestar suporte técnico disponibilizando recursos operacionais; 26- Auxiliar o analista nas definições e alterações dos sistemas; 27- Manter atualizado o cadastro de programas existentes; e 28- Controlar arquivos do material de processamento de dados, de documentos normativos e técnicos da área.
Inspecionar ambiente físico de trabalho	29- Sugerir mudanças na disposição de equipamentos; 30- Organizar cabeamento; 31- Supervisionar tarefas relacionadas à especialização e executá-las nas condições compatíveis com seu grau hierárquico e situação funcional; e 32- Conduzir planejamento e adestramento sobre as atividades profissionais.

QUADRO DE APERFEIÇOADOS DO CORPO AUXILIAR DE PRAÇAS

TAREFAS TÉCNICO-PROFISSIONAIS DA ESPECIALIDADE DE ESCRITA (ES):

1- Supervisionar as tarefas relacionadas à especialização em Escrita e Fazenda e executá-las nas condições compatíveis com seu grau hierárquico e situação funcional;
2- Exercer a função de escrivão em Sindicância, Processo de Deserção e Inquérito Policial Militar;
3- Exercer a função de Gestor das contas de gestão e de responsabilidade autorizadas, de acordo com as normas competentes;
4- Elaborar e supervisionar a confecção dos documentos administrativos observando as regras estabelecidas nas normas sobre documentação na Marinha;
5- Elaborar e supervisionar a confecção dos documentos relativos a controle de pessoal, controle de publicações e processos de concessão de condecorações;
6- Elaborar e supervisionar a confecção dos documentos relativos a processos licitatórios e a atos e acordos administrativos conforme as normas competentes;
7- Elaborar e supervisionar a confecção dos documentos e processos de comprovação, operar aplicativos específicos e exercer a função de agente subordinado ou de Fiel nas contas de gestão e de responsabilidade: Caixa de Economias, Execução Financeira, COPIMED, Pagamento de Pessoal e Civil, Material e SISBENF, Municiamento e Suprimento de Fundos;
8- Manusear e supervisionar a utilização dos documentos ostensivos e sigilosos, observando as normas inerentes a documentos classificados, quando aplicáveis;
9- Organizar e supervisionar a elaboração das coletâneas e arquivar documentos observando técnicas vigentes e de acordo com as normas competentes;
10- Organizar e supervisionar os serviços de SECOM;
11- Operar e supervisionar a utilização dos equipamentos básicos de suporte à execução dos serviços inerentes à SECOM, abrangendo scanner, fac-símile e copiadora reprográfica;
12- Operar e supervisionar a utilização do sistema de correio eletrônico padronizado para uso na Marinha;
13- Operar e supervisionar a utilização dos programas de informática relacionados a assinatura eletrônica e criptografia autorizados no âmbito da Marinha;
14- Operar e supervisionar a utilização dos aplicativos de informática referentes a automação de escritório, padronizados para uso na Marinha, constituídos de: sistema operacional para microcomputadores, editor de textos, planilha eletrônica, gerador de banco de dados, apresentação gráfica e software de navegação na INTERNET/INTRANET (browser);
15- Operar e supervisionar a operação dos aplicativos de informática adotados para uso geral na Marinha, desenvolvidos por Diretoria Especializada competente, no ambiente de computação para grupos de trabalho (workflow). Lotus Notes/SISDEM;
16- Operar e supervisionar a utilização dos sistemas corporativos da Marinha relacionados às áreas da Sistemática do Plano Diretor (SPD), do abastecimento, do pessoal e do pagamento de pessoal;
17- Operar e supervisionar a utilização dos sistemas de informação padronizados da Marinha, de auxílio à administração geral, relacionados a pessoal, catálogos, boletins, legislação e documentação;
18- Operar e supervisionar a utilização dos sistemas de administração do Governo Federal: Sistema Patrimonial Imobiliário da União (SPIU), Sistema Integrado de Administração Financeira (SIAFI), Sistema Integrado de Administração de Pessoal (SIAPE), Sistema de Cadastramento Unificado de Fornecedores (SICAF), Sistema de Divulgação Eletrônica de Compras e Contratações (SIDEC) e demais sistemas implementados no âmbito do Sistema Integrado de Administração de Serviços Gerais (SIASG) aos quais tenha havido incorporação ou adesão da Marinha;

19- Aplicar conhecimentos básicos de técnicos de contabilidade; e
20- Escriturar os documentos e modelos relativos a Conselho de Disciplina.