ESCOLA DE GUERRA NAVAL

CC LEANDRO FERRONE DEMÉTRIO DE SOUZA

A GUERRA CIBERNÉTICA NA MARINHA DO BRASIL:

desafios e aplicações.

Rio de Janeiro

2011

CC LEANDRO FERRONE DEMÉTRIO DE SOUZA

A GUERRA CIBERNÉTICA NA MARINHA DO BRASIL:

desafios e aplicações.

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

2011

RESUMO

A Internet mudou o padrão das comunicações, possibilitando a comunicação sem fio e transportando os movimentos sociais e estratégias geopolíticas para o plano global. Assim, as instituições dos Estados modernos, perderam suas capacidades de controlar e regular os fluxos globais de riqueza e informação. Com a diminuição destas capacidades, atores, estatais ou não, encorajados pela capacidade de ocultação e o baixo investimento requerido, passaram a aproveitar-se desta lacuna para realizar ações criminosas no Espaço Cibernético. Para se precaver contra essas ações foram criadas agências que irão conduzir a Segurança e a Guerra Cibernética no âmbito do Estado brasileiro e, por consequência, nas Forças Armadas. Faz-se necessário identificar as capacidades existentes e os desafios que a Marinha do Brasil enfrentará no âmbito da Guerra Cibernética, quando comparados ao estado da arte existente em outros Estados e em conformidade com o Livro Verde: Segurança Cibernética no Brasil e identificar a tecnologia necessária para enfrentar os novos desafios descritos neste Livro. A implantação do Centro de Defesa Cibernética atenderá apenas à finalidade de coordenar e integrar as ações de defesa cibernética do Exército Brasileiro, Marinha e Força Aérea Brasileira, sendo responsável apenas pela proteção das redes governamentais e militares, não contemplando as redes privadas que compõem os demais setores críticos brasileiros. A Marinha do Brasil está procurando estruturar-se em conformidade com as diretrizes de mais alto nível, alinhando-se com as metas desejáveis, apontadas por outros Estados com maiores capacidades de Guerra Cibernética que o Brasil, incluindo a nacionalização de itens e sistemas, a parceria com as indústrias de defesa e agências internacionais e a capacitação de pessoal, permitindo a garantia da segurança de seus sistemas e estruturas críticas. A capacidade de Guerra Cibernética que a Marinha do Brasil almeja não pode ser adquirida de uma forma individual, devendo dispensar especial atenção, além da capacitação do seu pessoal, à implantação de um órgão centralizador especializado em Guerra Cibernética que garanta a resiliência necessária, à parceria com o Estado e agências civis e à nacionalização de equipamentos, meios e vetores espaciais. A materialização desta capacidade deve ser feita através de um órgão centralizador, como um Centro ou Comando, com capacidades ofensivas e defensivas, que possa agir, em caso de um ataque cibernético, por interesse da Marinha do Brasil, com a devida autorização do Estado e conjuntamente com o Exército Brasileiro e a Força Aérea Brasileira. Desta forma estará sendo orientada para que se obtenha um domínio suficiente do espaço cibernético, permitindo sua utilização com as características de segurança, disponibilidade, integridade, confidencialidade e autenticidade fundamentais por ocasião de um conflito, assim como para o bom assessoramento aos Comandos Superiores no Teatro de Operações e a garantia do funcionamento dos seus sistemas críticos.

Palavras-chave: Espaço cibernético; Governança; Segurança Cibernética.

SUMÁRIO

1 INTRODUÇÃO

O advento da Internet[1] trouxe mudanças radicais no âmbito das comunicações. Seu sistema de redes horizontais, a possibilidade de comunicação sem fio, o acesso cada vez mais fácil e o preço cada vez menor dos equipamentos possibilitaram que movimentos sociais e estratégias geopolíticas se tornassem globais, agindo sobre fontes globais de poder e, desta forma, as instituições do Estado-nação, advindos da Era Moderna, foram gradualmente perdendo sua capacidade de controlar e regular os fluxos de riqueza e informação (CASTELLS, 1999).

Como consequência, encorajados pela relativa capacidade de ocultação e o baixo investimento requerido, indivíduos, comuns ou não, curiosos ou propositadamente preparados[2], perceberam a lacuna deixada pelos mecanismos reguladores e passaram a aproveitar-se desta incapacidade de efetivo controle pelos Estados, para realizar ações criminosas no Espaço Cibernético[3] (CLARKE; KNAKE, 2010).

Segundo o Glossário das Forças Armadas, publicação do Ministério da Defesa publicada em 2007, a Guerra Cibernética é definida como um 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

---

1 O embrião do que seria a Internet surgiu em 1969 através da ligação entre os dois primeiros elos daquele que viria a ser o ARPANET, interconectando a Universidade da Califórnia, em Los Angeles, e o *Stanford Research Institute* (SRI), em Menlo Park, Califórnia, dando início a uma nova fronteira na área de conhecimento e informação.

2 Segundo Clarke e Knake (2010), existem diferenças entre *hacker*, criminoso cibernético e guerreiro cibernético. *Hacker* é o indivíduo capaz de alterar determinadas instruções nos códigos dos programas com a finalidade de fazer com que o sistema realize novas tarefas para os quais não estava programado. Criminosos cibernéticos são os que realizam intrusões, por meio de computadores, em locais não autorizados. Guerreiros cibernéticos são os que trabalham para o Governo e realizam todas estas tarefas (CLARKE; KNAKE, 2010, pág.72).

3 Espaço Cibernético é definido como uma rede interdependente de infraestruturas de Tecnologias da Informação (TI), incluindo a Internet, as redes de telecomunicações e os sistemas de computadores. O termo também é usado para se referir ao ambiente virtual de informações e interações entre pessoas (EUA, 2009, pág1).

informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil (BRASIL, 2007b).

Neste trabalho, o conceito de Guerra Cibernética será utilizado com uma ressalva. Entende-se que as ações de Guerra Cibernética são caracterizadas por serem realizadas entre Estados e desenvolvidas no Espaço Cibernético. O consenso de autores de obras sobre o assunto indica que, mesmo que os ataques sejam realizados por indivíduos ou grupos não estatais, o Estado de origem dos ataques assumiria a responsabilidade pelos mesmos, pois deveria ter sido capaz de evitá-los ou controlá-los através de seus sistemas internos.

Para fazer frente à ameaça cibernética e desenvolver as capacidades necessárias, a Estratégia Nacional de Defesa [END] (2008) prevê que o setor cibernético, em conjunto com o setor espacial, deverá permitir que a capacidade nacional não dependa de tecnologia estrangeira e que as três Forças, em conjunto, possam atuar em rede, instruídas por monitoramento que se faça também a partir do espaço (BRASIL, 2008a, pág.12).

Nesse sentido, no ano de 2009 foi criado o Grupo Técnico de Segurança Cibernética (GT SEG CIBER), instituído no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), do Conselho de Governo, contando com representantes do Gabinete de Segurança Institucional da Presidência da República (GSIPR – DSIC e ABIN[4]), Ministério da Justiça (MJ e DPF), Ministério das Relações Exteriores (MRE), Ministério da Defesa (MD) e Comandos da Marinha, do Exército e da Aeronáutica, com a finalidade de propor diretrizes e estratégias de Segurança Cibernética para o país (BRASIL, 2010b, pág.12). Este grupo, no ano de 2010, elaborou e emitiu o Livro Verde: Segurança Cibernética no Brasil, um documento institucional do GSIPR, o qual balizará, em grande parte, este trabalho, uma vez que suas diretrizes contemplam as ações a serem desenvolvidas no âmbito do Governo e das Forças Armadas.

[4] As siglas DSIC e ABIN significam Departamento de Segurança da Informação e Comunicações e Agência Brasileira de Inteligência, respectivamente (BRASIL, 2010b, pág.7).

Assim, o propósito deste trabalho é identificar as capacidades existentes e os desafios que a Marinha do Brasil (MB) enfrentará na área de Guerra Cibernética (GC), comparadas ao estado da arte dos Estados que se utilizam da GC e em conformidade com o Livro Verde: Segurança Cibernética no Brasil, onde são apontadas diretrizes para os demais membros do GT SEG CIBER, bem como identificar a tecnologia de GC necessária para que a MB enfrente os novos desafios descritos nesse Livro.

A relevância deste estudo deve-se ao fato de que a identificação das capacidades, deficiências e tecnologias de Guerra Cibernética (GC) necessária à MB, para que haja o enfrentamento das novas ameaças no Espaço Cibernético, aumentará a segurança das redes, principalmente as de Comando e Controle (C^2), potenciais alvos de ataques.

O trabalho foi elaborado por meio de pesquisa bibliográfico-documental, com utilização de técnicas indiretas e fundamentada em livros, legislação, publicações doutrinárias, periódicos e artigos afetos ao tema.

Para alcançar seu propósito, o tema é desenvolvido em cinco capítulos. O segundo capítulo abrange a Segurança Cibernética e a Guerra Cibernética no Brasil. Nesse capítulo pretende-se apresentar um breve histórico da Segurança Cibernética, sua função estratégica de Estado e sua condição multidisciplinar e interinstitucional como condições fundamentais para seu desenvolvimento; abordar o que está sendo realizado nos Estados que desenvolveram capacidades de Guerra Cibernética; e comparar como a Estratégia Nacional de Defesa e o Livro Verde: Segurança Cibernética no Brasil definem as diretrizes para a Segurança Cibernética e a Guerra Cibernética para o Estado brasileiro e que servirão para orientar a estruturação e doutrinas de GC na MB.

O terceiro capítulo aborda as atuais capacidades e deficiências de Guerra Cibernética na Marinha do Brasil, incluindo o atual esforço de obter-se uma identidade própria, compatível com as tarefas a ela atribuídas, sem perder a característica de

interoperabilidade entre as Forças Armadas, uma vez que, pela END, o assunto Guerra Cibernética será coordenado pelo Exército Brasileiro (BRASIL, 2008a).

O quarto capítulo apresenta as metas necessárias à MB para que a ameaça cibernética seja mitigada e se obtenha um domínio suficiente do Espaço Cibernético de forma a garantir a utilização deste com segurança, disponibilidade, integridade[5], confidencialidade e autenticidade, capacidades definidas no Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (Guia SICI), documento emitido em novembro de 2010, o qual reúne métodos e instrumentos visando garantir a segurança desejada e que será abordado oportunamente nesse capítulo (BRASIL, 2010a).

[5] Incolumidade de dados ou conhecimentos na origem, no trânsito ou no destino (BRASIL, 2007b).

2 SEGURANÇA CIBERNÉTICA E A GUERRA CIBERNÉTICA NO BRASIL

> Vivemos em tempos confusos, como muitas vezes é o caso em períodos de transição entre diferentes formas de sociedade. Isso acontece porque as categorias intelectuais que usamos para compreender o que acontece à nossa volta foram cunhadas em circunstâncias diferentes e dificilmente podem dar conta do que é novo referindo-se ao passado (CASTELLS, 1999, p. I).

A Internet e tudo o que está ligado a ela fazem parte do nosso cotidiano. Serviços essenciais tornaram-se disponíveis através "da rede", facilitando as atividades do cidadão e das Organizações, oferecendo, como contrapartida, um risco impensável à época de sua criação (CASTELLS, 1999).

Como descrito no Livro Verde: Segurança Estratégica do Brasil, milhões de brasileiros acessam a Internet diariamente, trocando informações e utilizando diversos serviços, como os bancários, de comércio eletrônico, serviços públicos em geral, de pesquisa e de ensino, dentre outros (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 Institucional da Presidência da República (GSIPR), aponta cerca de duas mil tentativas de invasões maliciosas[6], por hora, nas 320 grandes redes do Governo[7] (BRASIL, 2010b, pág.34).

Nesse sentido, um dos novos desafios do século XXI é a Segurança Cibernética, definida pela Doutrina de Tecnologia de Informação da Marinha [EMA-416] (2007) como sendo a segurança do espaço cibernético, ou seja, a segurança das redes de computadores e de seus equipamentos de conectividade correlatos (BRASIL, 2007a) e tem como função, além de estratégia de Estado, manter as infraestruturas críticas, aí incluídas as de energia, defesa,

---

[6] Por *hackers*, curiosos e ataques de autoria desconhecida.

[7] Refere-se às redes que contemplam os sistemas de energia, transporte, água, telecomunicações e finanças (BRASIL, 2010a).

transporte, telecomunicações, finanças e de informações, para onde apontam, inclusive, esses acessos maliciosos descritos anteriormente.

Para este trabalho, adotar-se-á, adicionalmente ao conceito de Guerra Cibernética já definido no Glossário das Forças Armadas (2007), uma característica que, diferentemente da Segurança Cibernética, inclui 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).

Especificamente para efeito da Política de Defesa Nacional, 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).

Defesa Nacional é o conjunto de medidas e ações do Estado, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas (BRASIL, 2005).

Para garantir a segurança das infraestruturas críticas passíveis de ataques cibernéticos, Estados, como os Estados Unidos da América (EUA), França, Rússia, China, Israel, Canadá, Coreia do Sul e Coreia do Norte, dentre outros, já possuem capacidades de detectarem e realizarem ações de defesa ou ataques no campo cibernético (CLARKE; KNAKE, 2010).

Em sua obra, Clark e Knake atestam que os EUA, assim como os Estados supracitados, enfrentam dificuldades para organizar suas estruturas de Segurança Cibernética. Com o advento dos ataques cibernéticos, instituições governamentais e privadas realizaram ações individuais para fazer frente a essas ameaças. Atentos a essas ações isoladas, aqueles Estados perceberam que, estudos e ações realizadas dessa forma tanto aumentavam os

esforços, quanto os desperdiçavam. Assim, procuraram adotar um sistema em que uma única agência conduziria a Segurança e a Guerra Cibernética (CLARKE; KNAKE, 2010).

Existem problemas ainda maiores. Os EUA, por exemplo, limitados principalmente pelos Títulos 10 e 50[8] de seu Código de Leis, proíbe que agências civis conduzam ataques cibernéticos, permitindo às mesmas apenas a coleta de informações. Pela Lei, somente órgãos militares podem introduzir os códigos que afetariam sistemas informatizados inimigos (CLARKE; KNAKE, 2010).

Para contornar o problema, foi criada a *Defense Information System Agency* (DISA), subordinada ao Departamento de Defesa estadunidense, cujo diretor é um General de Divisão do Exército norte-americano. Essa agência emprega mais de 16.000 funcionários, dentre os quais, 35% são militares e 65% civis, possuindo um orçamento anual de 8,83 bilhões de dólares. Situada em Fort George G. Meade, Maryland, é o coração das ações cibernéticas defensivas e ofensivas dos EUA (CLARKE; KNAKE, 2010).

O Brasil, ao longo do tempo, procurou adequar sua estrutura de forma gradual, a fim de obter uma macrocoordenação nas atividades de Segurança e Guerra Cibernética.

Nesse sentido, verifica-se a evolução das ideias afetas a essa macrocoordenação através das ações realizadas ao longo do tempo.

No ano de 2004, uma deficiência importante no âmbito do Brasil e descrita por Domício Proença Júnior[9] em seu texto (PROENÇA JÚNIOR in PINTO; ROCHA; SILVA, 2004) era a ausência de organizações adequadas para gerenciar a Política Nacional. Domício escreve:

> A ausência de *organizações* adequadas abandona a política nacional a propostas parciais, mal-informadas e até simplesmente corporativas. Na ausência de estruturas e mecanismos atualizados, que permitam o exercício de direção política e a

[8] Os Títulos 10 e 50 do Código de Leis dos EUA referem-se, respectivamente, ás normas para as Forças Armadas e para a guerra e a defesa nacional estadunidense. Disponível em: http://uscode.house.gov/pdf/2010/2010usc01.pdf. Acesso em 10 jul. 2011.

[9] Professor da Coppe/UFRJ, Coordenador do Grupo de Estudos Estratégicos (GEE), membro do Instituto Internacional de Estudos Estratégicos (IISS, Londres) e da Associação Internacional de Chefes de Polícia (IACP, Leesburg, Va.), no ano de 2004.

> consideração técnica consistente, a dinâmica burocrática produz a tolerância para com a continuidade inercial e acrítica de entendimentos e práticas voluntaristas obsoletas (PROENÇA JÚNIOR in PINTO; ROCHA; SILVA, 2004, pág.101).

Na mesma obra, Proença Júnior afirma que: "[...] carecemos de organizações capazes de induzir, orientar e sustentar processos virtuosos e atuais em matéria de defesa e segurança" (PROENÇA JÚNIOR in PINTO; ROCHA; SILVA, 2004, p. 100).

Como contraponto, comprovando a evolução das ideias, em 2005 foi assinada a PDN e em 2008 a END. Esses decretos orientam, quando tratam do assunto, as diretrizes e ações que devem ser realizadas no sentido de se obter uma capacidade de Segurança e Guerra Cibernéticas compatíveis com as aspirações do Estado.

Pela Política de Defesa Nacional [PDN] (2005), os avanços da tecnologia da informação, a utilização de satélites, o sensoriamento eletrônico e outros aperfeiçoamentos tecnológicos trouxeram uma maior eficiência aos sistemas administrativos e de defesa. Como consequência, criaram-se vulnerabilidades que poderão ser exploradas, com o objetivo de inviabilizar o uso dos sistemas ou facilitar a interferência à distância (BRASIL, 2005).

Devido a esses avanços a PDN (2005) prevê, como orientação estratégica, que, para minimizar os danos de um possível ataque cibernético, é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que reduzam a vulnerabilidade[10] dos sistemas e permitam seu pronto restabelecimento (BRASIL, 2005).

Para atender a orientação estratégica citada, as políticas e ações definidas pelos diversos setores do Estado brasileiro deverão contribuir para a consecução dos objetivos da Defesa Nacional, seguindo diretrizes estratégicas, definidas na PDN, que alcancem as metas desejadas, contidas nessa orientação estratégica (BRASIL, 2005).

Como decorrência da PDN (2005), a Estratégia Nacional de Defesa [END] (2008) prevê, como princípio para que um projeto qualquer seja considerado um projeto forte de

[10] Situação de fraqueza de uma força, sistema, instalação ou equipamento, que pode ser explorada por um oponente para auferir vantagens (BRASIL, 2007b).

defesa e, por consequência, de desenvolvimento, a independência nacional, conseguida com uma capacitação tecnológica autônoma, inclusive nos assuntos estratégicos que contemplem os setores espacial, cibernético e nuclear. Afirma, ainda, que o Estado que não tem o domínio das tecnologias sensíveis não consegue a independência desejável tanto para a sua defesa como para o seu desenvolvimento (BRASIL, 2008a).

A END (2008) está organizada em torno de três eixos estruturantes. Tratar-se-á apenas do primeiro eixo, relacionado diretamente com este trabalho e que diz respeito a como as Forças Armadas devem se organizar e se orientar para melhor desempenharem sua destinação constitucional e suas atribuições na paz e na guerra (BRASIL, 2008a).

Ao lado da destinação constitucional das Forças Armadas e de suas outras atribuições, a END (2008) aborda, ainda, o papel de três setores decisivos para a defesa nacional, quais sejam o espacial, o cibernético e o nuclear. Inclui, como diretriz para que se atenda ao conceito de flexibilidade[11], o fortalecimento desses setores, descrevendo como as Forças Armadas devem operar em rede, tanto entre si quanto ligadas ao sistema de monitoramento do território, do espaço aéreo e das águas jurisdicionais brasileiras (BRASIL, 2008a).

Nesse sentido, o Estado brasileiro vem desenvolvendo uma cultura de governança única no setor público e de defesa, procurando adaptar-se às necessidades. O senso comum requer maior participação e sincronismo nas tarefas afetas à Segurança Cibernética, o que irá propiciar a construção de uma doutrina e de uma política nacional que serão traduzidas no Livro Branco: Política Nacional de Segurança Cibernética, decorrente das ações desencadeadas pelo Livro Verde: Segurança Cibernética no Brasil (BRASIL, 2010b).

---

[11] Característica de que deve dispor uma força militar, de modo a organizar-se para o cumprimento de uma missão específica, para atender tanto às diferentes fases de um plano ou ordem de operações, quanto de se adaptar às variações de situação que se possam apresentar, no desenrolar do combate ou missão recebida (BRASIL, 2007b).

Este autor concorda com o Livro Verde: Segurança Cibernética no Brasil quando o mesmo afirma que o estabelecimento de parcerias e ações colaborativas, tanto entre Estados, quanto entre os setores públicos e privados, sociedade e a academia, propiciariam a análise, coordenação e a integração de conhecimentos adquiridos por essas fontes (BRASIL, 2010b). Concorda ainda que este esforço deva atender a uma macrocoordenação e a uma governança bem estabelecida, para que não haja esforços distintos e que o conhecimento adquirido, contemplando métodos e capacidades de Guerra Cibernética, seja disseminado para as agências interessadas (BRASIL, 2010b).

Como descrito no Livro Verde: Segurança Cibernética no Brasil, esta coordenação da Segurança Cibernética será desenvolvida pelo Departamento de Segurança da Informação e Comunicação (DSIC), órgão do Gabinete de Segurança Institucional da Presidência da República, o qual possui a *expertise* necessária e uma "rede de contatos" dentro do território brasileiro e no exterior, facilitando a troca de informações entre as agências nacionais e internacionais (BRASIL, 2010b).

Ao observar a obra de Clarke e Knake (2010), onde se afirma que existe uma carência de uma agência norte-americana que gerencie a proteção das redes civis (CLARKE; KNAKE, 2010, pág.120), este autor analisa que o Brasil parece estar adotando políticas que não atenderiam em sua totalidade às necessidades de Segurança Cibernética. Em recente matéria para um grande jornal[12] eletrônico, o Coronel do Exército Brasileiro (EB) Luis Cláudio Gomes Gonçalves, coordenador da implantação do Centro de Defesa Cibernética (CDCiber), órgão do Ministério da Defesa que irá empregar cerca de cem militares da MB, EB e da Força Aérea Brasileira, com a finalidade de coordenar e integrar as ações de defesa cibernética das Forças Armadas brasileiras, afirmou que este Centro será responsável apenas

[12] Matéria do Jornal eletrônico Estadão.com.br, no dia 08 de junho de 2011, com o título: "Exército se arma para defender o espaço cibernético brasileiro". Disponível em: http://www.estadao.com.br/ noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro, 729291,0.htm. Acesso em: 12 jul. 2011.

pela proteção das redes governamentais e militares, nada tendo sido comentado sobre os sistemas críticos privados.

Desta forma, suportado pelas referências abordadas anteriormente, este autor conclui que, como aconteceu com os Estados citados, as agências brasileiras deveriam possuir uma capacidade de Guerra Cibernética alinhada com as exigências previstas na PDN (2005), na END (2008) e no Livro Verde: Segurança Cibernética no Brasil (2010), ou seja, buscarem uma cultura de governança única no setor público e de defesa, obter maior participação e sincronismo nas tarefas afetas à Segurança Cibernética, estabelecer parcerias e ações colaborativas entre Estados e outros setores públicos e privados, sociedade e a academia e atender a uma macrocoordenação e a uma governança bem estabelecida.

Analisa ainda que, quando da necessidade de um enfrentamento cibernético entre o Brasil e um contentor, a necessidade de uma agência militar faz-se necessária, pois a Guerra Cibernética, sendo realizada entre Estados, sugere ações desencadeadas por agências estritamente militares.

No próximo capítulo, serão abordados aspectos relacionados á capacidade de Guerra Cibernética no âmbito da MB e a necessidade de seu alinhamento com as diretrizes aqui abordadas.

3 A GUERRA CIBERNÉTICA NA MARINHA DO BRASIL

Uma vez abordados os documentos de mais alto nível que tratam do assunto Guerra Cibernética, enumeram-se as diretrizes que afetam a MB.

Para a Marinha do Brasil, a END (2008) aponta que o monitoramento da superfície do mar, a partir do espaço, deverá integrar as práticas e capacitações operacionais já disponíveis na própria MB, utilizando as doutrinas e sistemas atualmente em uso. Através do monitoramento, as forças navais, submarinas e de superfície terão fortalecidas suas capacidades de atuar em rede com as forças terrestre e aérea (BRASIL, 2008a).

Este autor prevê que, em caso de um ataque cibernético, esta capacidade de monitoramento e de conexão seriam alvos de grande valor a serem protegidos pela MB, assim como a rede que integra estes sistemas[13].

Para o Exército Brasileiro, a END prevê a existência de recursos espaciais de monitoramento e comunicações apoiados em vetores com total domínio nacional, podendo haver a participação de parceiros estrangeiros no projeto ou em sua implementação, incluindo as capacitações e os instrumentos cibernéticos necessários para assegurar as comunicações entre os equipamentos que realizam o monitoramento espacial e aéreo e a força terrestre (BRASIL, 2008a).

No contexto da interoperabilidade entre as Forças Armadas, este autor, ao analisar a END, conclui que, apesar da semelhança entre o previsto para o EB, especificamente citado na END, e o Corpo de Fuzileiros Navais (CFN) no tocante às suas tarefas como forças terrestres, o CFN não foi contemplado pela END, no âmbito da MB.

---

[13] Conexão de componentes de um sistema para reunir características técnicas e funcionais em um sistema interoperável, permitindo que dados existentes em sistemas diferentes possam ser compartilhados ou acessados mediante a definição de um protocolo de intercâmbio e a implementação de um componente que efetue a integração (BRASIL, 2007b).

Todas as orientações emanadas pela END (2008) para as Forças Armadas brasileiras contemplam a capacitação para a operação conjunta em rede (BRASIL, 2008a), o que atribui à interoperabilidade nos setores de comunicações e comando e controle (C^2), como exemplos, a probabilidade de se tornarem alvos em caso de ataques cibernéticos. A orientação para a obtenção desta capacitação é reforçada quando a END (2008) cita que:

> As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar (BRASIL, 2008a, pág.33).

A atividade de Guerra Cibernética na MB está a cargo do Centro de Tecnologia da Informação da MB (CTIM) e tem, como uma de suas tarefas, conduzir as atividades concernentes à Guerra Cibernética, auditoria de segurança e forense computacional[14], através do Departamento de Guerra Cibernética constante em seu organograma. Esse Departamento está subdividido em três Seções, quais sejam: Operações, Infraestrutura de Segurança da Informação Digital (SID) e Forense Computacional e Recursos Criptológicos (QUEIROZ, 2010).

Na palestra sob o título "Suporte de TI na MB", a qual contemplava as atividades realizadas pelo CTIM no ano de 2010[15], proferida durante o VI Simpósio de Tecnologia da Informação e Comunicações da Marinha, o Capitão-de-Mar-e-Guerra João Augusto Gomes de Queiroz, Diretor do Centro, afirmou que as atuais metas são implantar, monitorar e manter os ativos[16] da Rede de Comunicações Integradas da Marinha (RECIM) atinentes à segurança da

---

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

[15] Palestra disponível em http://www.informar.mar.mil.br/2010/pdf/palestra_encerramento_18_11_10.pdf. Acesso em: 12 jul. 2011.

[16] Ativos de informação são as bases de dados, os arquivos, a documentação de sistemas, os manuais de usuário, o material de treinamento, os procedimentos de suporte, de desenvolvimento, de manutenção ou de operação, os planos de continuidade e todos os meios digitais onde as informações trafegam, são processadas ou encontram-se armazenadas (BRASIL, 2007a).

informação digital, contemplando a proteção da borda[17] da RECIM, a proteção das redes locais (com o incentivo de um antivírus corporativo e a atualização dos aplicativos utilizados e dos sistemas operacionais) e os recursos criptológicos da MB (QUEIROZ, 2010). Durante o referido simpósio o Capitão-de-Mar-e-Guerra Queiroz apresentou uma ideia da abrangência dos sistemas da MB, e, por consequência, de sua vulnerabilidade.

No final do ano de 2010, a MB, através do CTIM, gerenciava 27.200 usuários de rede, 50.000 acessos diários e até 5.000 acessos simultâneos à Internet e disponibilizava 256 sítios eletrônicos de Intranet[18] e 163 de Internet (QUEIROZ, 2010).

A RECIM tem abrangência nacional, e alcança, ainda, quase todos os continentes e a Antártica. Quanto às redes móveis instaladas a bordo dos navios, o volume de tráfego diário (Internet) chega a 500 Gbytes de dados/voz (QUEIROZ, 2010).

A MB possui 670 sistemas em produção e o cumprimento da missão de muitas Organizações Militares (OM) seria comprometido pela indisponibilidade da RECIM e do Centro de Dados da MB (CD-MB), localizado nas dependências do CTIM (QUEIROZ, 2010).

O correio eletrônico da MB possui 32.000 usuários, enviando e recebendo 16.500 mensagens externas por dia, das quais 90% são filtradas como SPAM[19] (QUEIROZ, 2010). Este autor analisa que o problema das mensagens assim classificadas (SPAM) é o fato de oferecerem uma grande chance de invasão da RECIM por ocasião de um ataque cibernético.

Verifica-se, ainda, que esta abrangência dos sistemas da MB é um fator de vulnerabilidade, servindo como porta de entrada para eventuais ataques cibernéticos.

O CTIM procura, através da Central de Suporte da RECIM, alinhar a MB às práticas recomendadas de Governança de TI por meio do estabelecimento de um ponto único

---

17 Entende-se pela fronteira definida entre as redes internas da MB e as externas à mesma.

18 Rede de computadores privada que utiliza os mesmos protocolos da Internet. É considerada uma "versão privada da Internet", ou uma "mini-Internet", confinada a uma organização.

19 Envio em massa de mensagens não solicitadas pelos destinatários.

de contato entre seus clientes, quais sejam os Centros Locais de Tecnologia da Informação (CLTI), os Gerentes Operativos de Área (GOA), os Supervisores Operativos de Área (SOA) e os administradores de redes (ADMIN) com a gerência da RECIM, do CD-MB e de Segurança da Informação Digital[20] [SID] (QUEIROZ, 2010).

Com estas práticas, o que se busca é a diminuição dos tempos de resposta para tratamento de incidentes, com o consequente aumento da disponibilidade dos ativos de informação da RECIM (infraestrutura de conectividade e serviços) do CD-MB e de SID e uma atuação pró-ativa, a partir dos alarmes e monitores disponibilizados pelos *softwares* de gerência das redes (QUEIROZ, 2010).

Durante a 6ª Reunião do Conselho de Tecnologia da Informação da MB (COTIM)[21], realizada em 28 de outubro de 2010 nas dependências do Estado-Maior da Armada no Rio de Janeiro (EMA-RIO), foi aprovada a proposta do incremento da contingência geográfica, onde serviços críticos da MB serão disponibilizados, em forma de *backup*, em outras regiões do Brasil, garantindo a disponibilidade, melhor desempenho e segurança desses serviços, incluindo-se os da RECIM e do Centro de Dados da MB (QUEIROZ, 2010).

Como desafios a serem enfrentados, são enumeradas a evolução da TI, a formação e a capacitação do pessoal, a padronização de tecnologias, a homologação de sistemas digitais, a continuidade, o suporte local (através dos CLTI), a conscientização dos usuários, a segurança e o atendimento das necessidades futuras da Marinha (QUEIROZ, 2010).

Orientada pelas necessidades apresentadas na PDN (2005), a Doutrina de Tecnologia da Informação da Marinha [EMA-416] (2007) prevê que o desenvolvimento e a manutenção de Tecnologia da Informação na MB devem estar alicerçados em fundamentos,

---

[20] É o conjunto de conceitos, técnicas e medidas tecnológicas e/ou administrativas, utilizado para proteger a informação digital contra o uso indevido e oposto aos interesses da MB (BRASIL, 2007a).

[21] Órgão consultivo, deliberativo, de caráter permanente, em forma de colegiado, que tem como propósito assessorar o Comandante da Marinha no trato dos assuntos de alto nível relacionados á Governança de Tecnologia da Informação da MB (BRASIL, 2007a).

nos quais se inclui a capacitação dos recursos humanos envolvidos, constituída pela qualificação do pessoal e associada à aplicação do conhecimento adquirido, assumindo que esta capacitação é essencial para a eficácia das ações de TI (BRASIL, 2007a).

Como reforço da necessidade de capacitação de pessoal, a END (2008) prevê que:

> O futuro das capacitações tecnológicas nacionais de defesa depende mais da formação de recursos humanos do 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, pág.35).

Este autor verificou que, nas leituras realizadas abordando a Guerra Cibernética em outros Estados, é de comum acordo entre os autores que a capacitação de pessoal é fator preponderante para a estruturação da GC nas Forças Armadas. Estados como os EUA, Rússia e China possuem escolas de formação para *Hackers* e Guerreiros Cibernéticos (CLARKE; KNAKE, 2010), demonstrando essa preocupação.

Outros enquadramentos advindos da publicação Doutrina de Tecnologia da Informação da Marinha [EMA-416] (2007), atesta que competem: aos Órgãos de Desenvolvimento Tecnológico[22] acompanhar, em âmbito nacional e internacional, em consonância com a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), a evolução doutrinária e tecnológica das atividades inerentes à criptologia, à Guerra Cibernética e à Segurança da Informação Digital e assegurar a interoperabilidade entre os sistemas em desenvolvimento e os existentes na MB; e ao CTIM operar os recursos tecnológicos para a Guerra Cibernética, planejar os exercícios gerais de GC, subsidiar a Organização Militar Orientadora Técnica[23] (OMOT) nos aspectos de capacitação técnica do pessoal envolvido com as atividades específicas de GC, e mobilizar o pessoal qualificado,

---

[22] Compreendem o Centro de Análises de Sistemas Navais (CASNAV), o Instituto de Pesquisas da Marinha (IPqM), o Centro Tecnológico da Marinha em São Paulo (CTMSP) e o Instituto de Estudos do Mar Almirante Paulo Moreira [IEAPM] (BRASIL, 2007a).

[23] Neste caso, a Diretoria de Comunicações e Tecnologia da Informação da Marinha [DCTIM] (BRASIL, 2007a).

para o emprego em situações de conflito, de acordo com a doutrina estabelecida (BRASIL, 2007a).

Como fundamento, o que está previsto na publicação Doutrina de Tecnologia da Informação da Marinha [EMA-416] (2007), é o estabelecimento de uma infraestrutura de TI que permita a conectividade dos meios envolvidos em um Teatro de Operações (TO) e desses com as Organizações Militares de terra que os possam suprir de informações necessárias à execução das tarefas básicas do Poder Naval (BRASIL, 2007a). Essa infraestrutura é fundamental para a coordenação nas redes de Comando e Controle (C^2), possibilitando ao Comandante do Teatro de Operações (COMTOM) e aos Estados-Maiores receberem as informações que orientarão as futuras decisões.

No que tange à Guerra Cibernética no âmbito do Setor Operativo[24] da MB, o Comando de Operações Navais possui em sua estrutura uma Subchefia de Inteligência Operacional (CON-20). Subordinada a essa Subchefia está 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] (BRASIL, 2008b).

A esta Seção cabe assessorar o Comandante de Operações Navais, através do Subchefe de Inteligência Operacional (CON-20), nos assuntos concernentes à inteligência tecnológica voltada para a segurança da informação e Guerra Cibernética (BRASIL, 2008b).

Assim sendo, com base nas referências apresentadas, este autor conclui como pertinente que a Marinha do Brasil está se estruturando em conformidade com as diretrizes de mais alto nível, compreendidas na PDN, END e no Livro Verde: Segurança Cibernética no Brasil.

Como consequência desta analise, o próximo capítulo tentará expor os principais

---

[24] Compreende toda a cadeia hierárquica do Comando de Operações Navais, sendo constituído pelos Comandos de Distritos Navais, Comando-em-Chefe da Esquadra, Comando da Força de Fuzileiros da Esquadra e o Comando do Controle Naval do Tráfego Marítimo. Disponível em: http://www.mar.mil.br/ menu_h/organizacoes/ organizacoes_mb.htm. Acesso em: 20 jul. 2011.

desafios e metas a serem alcançadas pela MB, de forma a estar em um nível comparável ao estado da arte no setor de Guerra Cibernética.

4 DESAFIOS E METAS NECESSÁRIAS À MARINHA DO BRASIL

Como descrita no capítulo anterior, a atividade de Guerra Cibernética (GC) na Marinha do Brasil vem crescendo de forma sistematizada, seguindo as doutrinas atuais.

No ano de 2010, dois documentos relativos à Segurança Cibernética foram produzidos e distribuídos, como forma de orientar as diretrizes de alto nível que abordam o assunto. Apesar de tratarem sobre a Segurança Cibernética, afetam diretamente a Guerra Cibernética, pois essas duas atividades estão inegavelmente correlacionadas.

O Livro Verde: Segurança Cibernética no Brasil e o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação[25] [Guia SICI] (2010), outro documento institucional do GSIPR, podem ser considerados muito atuais, e, por consequência, a MB deveria procurar alinhar suas atividades conforme as orientações emanadas desses documentos.

De acordo com a análise deste autor, ambos os documentos baseiam-se fundamentalmente na ideia de capacitação das organizações. Esta capacitação abrange os recursos humanos e materiais, e deve ser objeto prioritário de estudo por parte da MB.

Com o advento desses documentos, a doutrina, as normas e as práticas usuais na MB deveriam ser revistas, para que sejam comparáveis às existentes nos Estados[26] com capacidades de GC consideradas no estado da arte, já abordadas anteriormente pelas referências deste trabalho.

O Guia SICI, ainda em sua primeira versão, trata de conceitos e práticas atuais para a identificação das Infraestruturas Críticas da Informação de uma organização, de forma

---

[25] Reúne métodos e instrumentos, visando garantir a Segurança das Infraestruturas Críticas da Informação, com relevantes aspectos destacados, dada a complexidade do tema nos dias atuais. É composto por estudos técnicos sobre a Segurança das Infraestruturas Críticas da Informação desenvolvidos por especialistas de diferentes órgãos da Administração Pública Federal, direta e indireta (BRASIL, 2010a).

[26] Como exemplos: Estados Unidos da América, França, China, Coreias do Norte e Sul, Rússia e Reino Unido, dentre outros (CLARKE; KNAKE, 2010).

a concentrar os esforços de segurança nessas infraestruturas. Para a análise deste autor serão abordados os conceitos mais visíveis para aplicação na MB. Outros conceitos e práticas estão incluídos no Guia, mas não serão objetos deste trabalho.

Segundo o Guia, para que uma organização identifique seus requisitos de segurança[27], ela deve basear-se em três pilares. O primeiro é o conjunto dos princípios, objetivos e necessidades para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações. O segundo é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender. E o terceiro, oriunda das duas anteriores, são os requisitos de segurança derivados da avaliação de riscos, processo responsável por identificar as ameaças aos ativos, as vulnerabilidades com suas respectivas probabilidades de ocorrência e os impactos ao empreendimento (BRASIL, 2010a).

Outro aspecto ressaltado pelo Guia prevê que, quando da formulação de estratégias para atender os requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação, devem ser considerados três fatores: segurança, resiliência e capacitação (BRASIL, 2010a).

A segurança da informação e comunicações descreve atividades que se relacionam com a proteção da informação e dos ativos da infraestrutura de informação contra riscos de perda, mau uso, divulgação indevida ou dano. Contempla a adoção de controles físicos, tecnológicos e humanos personalizados, que viabilizam a redução dos riscos a níveis aceitáveis, em conformidade aos requisitos de segurança exigidos pelo empreendimento (BRASIL, 2010a).

---

[27] Requisitos de segurança de um ativo de informação devem ser definidos por meio de critérios que atendam a disponibilidade, integridade, confidencialidade e autenticidade dessa informação (BRASIL, 2010a).

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT)[28], engenharia de resiliência é o processo no qual uma organização projeta, desenvolve, implementa e gerencia a proteção e a sustentabilidade de seus serviços críticos, relacionados com os processos de negócio e associados aos ativos de informação (BRASIL, 2010a).

O *Gartner Institute*[29] atesta que uma organização resiliente exige que haja um compromisso contínuo desta em relação ao acesso às informações, sistemas de conhecimento, mecanismos de comunicação, locais de trabalho e infraestruturas, de forma que possa rapidamente retornar à operação após um choque ou desastre (BRASIL, 2010a).

Este autor analisa que a resiliência é fundamental para a MB, pois uma vez que seja alvo de um ataque cibernético, sua pronta resposta e a capacidade de contornar os danos e retornar rapidamente às suas capacidades anteriores são necessidades primárias à tomada de decisão em caso de conflito ou desastres.

Para confirmar a importância da resiliência, o Guia SICI cita que:

> Segundo o Programa de Proteção da Infraestrutura Crítica da Austrália, existe uma preocupação no sentido de desenvolver a próxima geração de pensamento em relação à proteção das Infraestruturas Críticas, porquanto alguns estudos e pesquisas estão sendo conduzidas principalmente nos EUA, França, Nova Zelândia e na própria Austrália. Estes países já constataram que as ações atualmente adotadas para proteção das Infraestruturas Críticas não são suficientes e já buscam orientações para uma abordagem de resiliência. O fator primordial para este direcionamento não está associado apenas à questão das ameaças, mas também a forte interdependência entre os setores das Infraestruturas Críticas, que exige uma ação coordenada, integrada e efetiva.
>
> Considerar a resiliência sob uma perspectiva sistêmica apresenta-se com uma opção adequada para enfrentar este desafio: a proteção das Infraestruturas Críticas. A resiliência possibilita às organizações trabalharem, de forma independente e interdependente, para garantir a continuidade dos seus objetivos de negócio durante a interrupção de eventos, tais como: desastres naturais, acidentes industriais e atos terroristas, e para melhorar as parcerias com os serviços de gestão de emergência que visam assistir as comunidades (BRASIL, 2010a, pág85).

---

[28] Órgão estatal, mantido pelo Núcleo de Informação e Coordenação do Ponto Br (NIC.br), do Comitê Gestor da Internet no Brasil, atende a qualquer rede brasileira conectada à Internet, sendo responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato. Disponível em: www.cert.br. Acesso em 18 jul.2011.

[29] Instituto estadunidense, líder mundial em pesquisas sobre tecnologia da informação. Disponível em: http://www.gartner.com. Acesso em 18 jul. 2011.

Este autor verificou que, como deficiência que pode comprometer a capacidade de resiliência, hoje a MB possui apenas uma Intranet, não oferecendo uma alternativa em caso de ataques. As Forças Armadas dos EUA, como exemplo, utilizam ao menos três redes, uma não classificada, uma classificada como "secreta", a *SIPRNET*, e outra classificada como "ultra-secreta", a *JWICS* (CLARKE; KNAKE, 2010). Na analise deste autor, esta capacidade, além de "blindar" as informações trocadas nessas redes, oferece uma rápida alternativa por ocasião de um ataque a qualquer uma delas e atende à capacidade de resiliência.

Nesse sentido, apesar dos esforços em pesquisas e do desenvolvimento de recursos de segurança dos ativos de informação, dados como pesquisas, informações e projetos ainda são amplamente subtraídos de organizações norte-americanas (CLARKE; KNAKE, 2010).

Para a proteção dos ativos, existem recursos que podem parecer ortodoxos, porém são considerados o estado da arte em Segurança Cibernética. Mesmo indo de encontro ao conceito de globalização, são adotados por algumas organizações como a principal forma de proteção.

Como exemplo, o *Johns Hopkins University´s Advanced Phisics Laboratory* (APL), localizado nas proximidades de Baltimore, USA, recebe milhões de dólares por ano para aplicação em pesquisas, dentre as quais estão incluídas as pesquisas em projetos de segurança nacional estadunidense. Apesar de ser considerada uma *expert* em Segurança Cibernética, com contratos inclusive com a Agência Nacional de Segurança (NSA) norte-americana, em 2009 descobriu-se que algumas de suas pesquisas foram secretamente extraviadas de sua rede de computadores. A única forma que a APL encontrou para proteger as informações de suas pesquisas foi, efetivamente, desconectar sua rede (Intranet) da rede

mundial (Internet), isolando-se e mantendo-se como uma "ilha" no espaço cibernético (CLARKE; KNAKE, 2010).

Pela análise deste autor, esta prática só seria interessante caso a MB utilizasse um padrão como o norte-americano, ou seja, possuísse redes distintas para o tráfego de informações com diferentes classificações. Além do isolamento proporcionado por este padrão, o mesmo de nada adiantaria se não existisse um sério controle do pessoal envolvido nas demais práticas de segurança dos ativos, como a compartimentação de informações[30] e o veto ao uso de mídias pessoais de gravação, como CD, DVD, discos rígidos portáteis e dispositivos de memória removíveis (cartões de memória e *pen drives*).

Outro conceito apresentado por Clarke e Knake tenta medir a capacidade de Guerra Cibernética de um Estado e, na análise do autor deste trabalho, pode ser utilizado para uma instituição como a Marinha do Brasil, compara três fatores: a capacidade ofensiva de Guerra Cibernética, a capacidade defensiva em caso de ataques cibernéticos e a dependência cibernética do Estado, que significa a extensão de suas redes e sistemas. Quanto mais "informatizado" um Estado, mais dependente ele é e, por consequência, mais vulnerável (CLARKE; KNAKE, 2010).

Quando um Estado possui uma grande dependência cibernética, a quantidade de "alvos" oferecidos, por ocasião de um ataque cibernético, é grande. No caso contrário, quando essa dependência é pequena, há pouco o que atacar e as consequências de um ataque são mínimas (CLARKE; KNAKE, 2010).

Desta forma, segundo Clarke e Knake, o ideal seria que um Estado possuísse grandes capacidades ofensiva e defensiva e uma pequena dependência cibernética (CLARKE; KNAKE, 2010).

---

[30] Restrição do acesso com base na necessidade de conhecer, ou seja, na condição indispensável, inerente ao exercício funcional, para que uma pessoa, possuidora de credencial de segurança, tenha acesso a conhecimento ou dado sigiloso específico, compatível com o seu credenciamento. Desta maneira, a necessidade de conhecer constitui fator restritivo do acesso, independentemente do grau hierárquico ou do nível da função que a pessoa exerce (BRASIL, 2007b).

Ao estudar estes conceitos, em sua análise, este autor verificou que, como a tendência da MB tem sido informatizar cada vez mais seus sistemas, meios e redes, sua dependência e, por consequência, sua vulnerabilidade aumentam na mesma medida. Em caso de um ataque aos sistemas principais, os recursos reservas disponíveis na MB, além de escassos, não atenderiam ao conceito de resiliência, pois não permitiriam que fossem utilizados, em sua plenitude, os sistemas vitais de informações, monitoramento e comunicações, os quais atenderiam a uma grande operação em um Teatro de Operações (TO), por exemplo.

A MB demonstra seu alinhamento com as metas desejáveis de outros Estados com maiores capacidades de Guerra Cibernética que o Brasil, através da busca pela nacionalização de itens de *hardware, software* e sistemas, a parceria com as indústrias de defesa e agências internacionais e a capacitação de pessoal, claramente apontadas em outras obras estudadas para a construção deste trabalho.

Como exemplo, o Plano de Desenvolvimento Científico-Tecnológico e de Inovação da Marinha [PDCTM] (2009) tem por finalidade estabelecer as normas, os procedimentos e as orientações relativas ao planejamento, execução e controle das atividades de Ciência, Tecnologia e Inovação (CT&I) na Marinha, no horizonte temporal de 2010 a 2020 e aborda o planejamento estratégico da MB, estabelecendo as orientações e as ações que nortearão a aplicação da inovação e do conhecimento científico e tecnológico na Marinha (BRASIL, 2009).

O PDCTM cita, como alguns de seus objetivos estratégicos, a nacionalização de itens de *hardware*, *software* e dos sistemas, dos equipamentos e dos materiais, progressiva e seletivamente, com precedência para aqueles suscetíveis de restrição de fornecimento e a busca do domínio do conhecimento, incluindo a capacitação de recursos humanos, bem como

a atualização da infraestrutura tecnológica das Instituições de Ciência e Tecnologia (ICT) da MB (BRASIL, 2009).

As ações estratégicas a serem adotadas para que se alcancem os objetivos supracitados são, dentre outras, buscar o domínio tecnológico compatível com o estado da arte dos países desenvolvidos, buscar, sempre que possível, o incremento do índice de nacionalização dos meios operativos, sem prejuízo dos requisitos técnicos estabelecidos em projeto, com prioridade ao desenvolvimento de equipamentos e sistemas nacionais, principalmente para os novos meios em aquisição pela MB e desenvolver ações focadas na nacionalização de itens de *hardware*, *software*, de sistemas, equipamentos e itens sobressalentes considerados passíveis de serem fabricados pela indústria nacional, com prioridade para os itens de menor complexidade tecnológica e cuja dependência de fornecimento do exterior venha a comprometer a capacidade operativa dos meios da MB (BRASIL, 2009).

Como ponto fundamental, a capacidade de Guerra Cibernética que a MB almeja possuir não pode ser adquirida de uma forma individual. De nada adianta possuir esta capacidade, se outras áreas críticas no âmbito do Ministério da Defesa (Exército Brasileiro e Força Aérea Brasileira), do Governo Federal e do Estado brasileiro podem ser alvos de ataques das armas cibernéticas[31], servindo como fontes para intimidação, persuasão e uma possível imobilização dos meios da Marinha.

Desta forma, faz-se necessário que a capacidade de Guerra Cibernética em outras áreas críticas como a financeira, a nuclear e a energética, dentre outras, também seja encarada como fundamental e esteja em um patamar compatível com as aspirações do Estado.

Com a capacitação do seu pessoal, a implantação de um órgão centralizador especializado em Guerra Cibernética, uma estrutura que garanta a resiliência necessária, a

[31] Podem ser considerados como armas cibernéticas os códigos maliciosos, os *Trojans*, *spywares*, *keyloggers*, *botnets*, os vírus, *worms*, a propaganda na rede e o ataque distribuído de negação de serviço [*Distributed Denial Of Service* – DDOS] (CLARKE; KNAKE, 2010).

parceria com o Estado e agências civis e a nacionalização de equipamentos, meios e vetores espaciais (satélites e VANT[32], como exemplos), a MB estará sendo orientada para que se obtenha um domínio suficiente do espaço cibernético, garantindo a utilização desse com segurança, disponibilidade, integridade[33], confidencialidade e autenticidade, conceitos fundamentais, por ocasião de um conflito, assim como para o bom assessoramento aos Comandos Superiores no Teatro de Operações (TO) e a garantia do funcionamento dos seus sistemas críticos.

Este autor, sustentado pelos fatos apresentados, analisou que a materialização desta capacidade de Guerra Cibernética na MB deve ser feita através de um órgão centralizador, em forma de um Centro ou Comando, com capacidades ofensivas e defensivas, que possa agir, em caso de um ataque cibernético ou mesmo antecipadamente, por interesse da MB, com a devida autorização do Estado e conjuntamente com o Exercito Brasileiro e a Força Aérea Brasileira, garantindo o funcionamento dos sistemas e estruturas críticas. Este órgão deveria pertencer à Marinha do Brasil, atuando em seu âmbito interno. Externamente e de forma conjunta, a MB seria empregada junto ao CDCiber.

---

[32] Veículo aéreo não tripulado (VANT) é utilizado, dentre outras coisas, para monitoramento, busca, aerofotogrametria, direção de tiro de artilharia e patrulhamento urbano.

[33] Incolumidade de dados ou conhecimentos na origem, no trânsito ou no destino (BRASIL, 2007b).

5 CONCLUSÃO

A Internet mudou de forma contundente o padrão das comunicações, possibilitando, através de seu sistema de redes horizontais, da comunicação sem fio, do fácil acesso e da diminuição dos preços dos equipamentos, o transporte dos movimentos sociais e estratégias geopolíticas para o plano global. Desta forma, as instituições dos Estados modernos, foram gradualmente perdendo suas capacidades de controlar e regular os fluxos globais de riqueza e informação.

Com a diminuição destas capacidades, atores estatais ou não, encorajados pela relativa capacidade de ocultação e o baixo investimento requerido, passaram a aproveitar-se desta lacuna e realizam ações criminosas no Espaço Cibernético.

Como forma de se precaver dessas ações estão sendo criadas agências que irão conduzir a Segurança e a Guerra Cibernética no âmbito do Estado brasileiro e, por consequência, nas Forças Armadas.

Este trabalho procurou identificar as capacidades e deficiências de Guerra Cibernética (GC) existentes na Marinha do Brasil (MB), comparadas ao estado da arte de Estados que se utilizam da GC e em conformidade com o Livro Verde: Segurança Cibernética no Brasil, bem como identificar a tecnologia de GC necessária para que a MB enfrente os novos desafios descritos neste Livro.

Como descrito, a implantação do Centro de Defesa Cibernética (CDCiber), atenderá apenas à finalidade de coordenar e integrar as ações de defesa cibernética do Exército, Marinha e Aeronáutica, sendo responsável apenas pela proteção das redes governamentais e militares, não contemplando as redes privadas que compõem os demais setores críticos.

A orientação política aponta para que se busque uma governança na área de Segurança Cibernética. Desta forma, as agências brasileiras devem possuir uma capacidade de Guerra Cibernética comparável com as exigências prevista na PDN, na END e no Livro Verde: Segurança Cibernética no Brasil.

Para que se obtenha uma capacidade compatível com essas orientações, a Marinha do Brasil está procurando se estruturar em conformidade com as diretrizes de mais alto nível, observando essas orientações.

Essa estruturação está alinhada com as metas desejáveis, apontadas por outros Estados com maiores capacidades de Guerra Cibernética que o Brasil, incluindo a nacionalização de itens de *hardware*, *software* e sistemas, a parceria com as indústrias de defesa e agências internacionais e a capacitação de pessoal, permitindo à MB a garantia da segurança de seus sistemas e estruturas críticas.

A capacidade de Guerra Cibernética que a MB almeja possuir não pode ser adquirida de uma forma individual. Não adianta possuí-la, se outras áreas críticas do Estado brasileiro podem ser alvos de ataques das armas cibernéticas, servindo como fontes para intimidação, persuasão e uma possível imobilização dos meios da Marinha.

Pela análise do trabalho, a MB deve dispensar especial atenção à capacitação do seu pessoal, a implantação de um órgão centralizador especializado em Guerra Cibernética que garanta a resiliência necessária, a parceria com o Estado e agências civis e a nacionalização de equipamentos, meios e vetores espaciais (satélites e VANT). Desta forma a MB estará sendo orientada para que se obtenha um domínio suficiente do espaço cibernético, permitindo a utilização desse com as características de segurança, disponibilidade, integridade, confidencialidade e autenticidade fundamentais por ocasião de um conflito, assim como para o bom assessoramento aos Comandos Superiores no Teatro de Operações (TO) e a garantia do funcionamento dos seus sistemas críticos.

De acordo com a análise realizada, a materialização desta capacidade de Guerra Cibernética na MB deve ser feita através de um órgão centralizador, em forma de um Centro ou Comando, com capacidades ofensivas e defensivas, que possa agir, em caso de um ataque cibernético ou mesmo antecipadamente, por interesse da MB, com a devida autorização do Estado e conjuntamente com o Exército Brasileiro e a Força Aérea Brasileira. Este órgão deveria pertencer à Marinha do Brasil, atuando em seu âmbito interno. Externamente e de forma conjunta, a MB seria empregada junto ao CDCiber.

REFERÊNCIAS

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 12 jul. 2011.

_____. 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. 2008a, Seção 1, p. 4, Disponível em: <https:// www.defesa.gov.br/eventos_temporarios/2009/estrategia/arquivos/estrategia_defesa_nacional _portugues.pdf>. Acesso em 12 jul. 2011.

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

_____. *EMA-416 Doutrina de tecnologia da informação da Marinha*. Brasília, 2007a. v. I.

_____. *Portaria nº 115/EMA, de 30 de junho de 2008. Aprova o Regulamento do Comando de Operações Navais (ComOpNav)*. Brasília, 2008b.

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

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. *Guia de referência para a segurança das infraestruturas críticas da informação* / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010a. 151 p. Versão 01. Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/ 2_Guia_SICI.pdf>. Acesso em 09 jul. 2011.

_____. *Livro verde: Segurança Cibernética no Brasil/* Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010b. 63 p. Disponível em: <http://dsic.planalto.gov.br/documentos/ publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em 08 jul. 2011.

CASTELLS, Manuel. *A sociedade em rede* – volume I: A era da informação: economia, sociedade e cultura. 8 ed. São Paulo: Paz e Terra, 1999. 617 p.

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. 291 p.

ESTADOS UNIDOS DA AMÉRICA – EUA. *Cyberspace policy review:* Assuring a Trusted and Resilient Information and Communications Infrastructure. 2009. Disponível em <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. Acesso em 15 jul. 2011.

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

PROENÇA JÚNIOR, Domício. Contexto, ciência e desafios: o Brasil diante da defesa e segurança. In: PINTO, J. R. de Almeida; ROCHA, A. J. Ramalho da; SILVA R. Doring Pinho da (Org.). *Reflexões sobre defesa e segurança: uma estratégia para o Brasil*. Pensamento brasileiro sobre defesa e segurança, 1. Brasília: Ministério da Defesa, Secretaria de Estudos e de Cooperação, 2004, p. 85-106.

QUEIROZ, João Augusto Gomes de. *Suporte de TI na MB*. In: VI Simpósio de Tecnologia da Informação e Comunicações da Marinha, 2010, Rio de Janeiro. Disponível em <http://www.informar.mar.mil.br/2010/pdf/palestra_encerramento_18_11_10.pdf>. Acesso em: 12 jul. 2011.