GUERRA CIBERNÉTICA: A GUERRA NO QUINTO DOMÍNIO, CONCEITUAÇÃO E PRINCÍPIOS

Júlio Cezar Barreto Leite da Silva[1 2]

RESUMO

O presente artigo pretende apresentar uma definição abrangente para Guerra Cibernética. Para isso explora a gama de definições e significados afetos à matéria, pesquisando princípios, características, particularidades e emprego adequado dos termos, com o propósito de fundamentar a definição proposta. O artigo também aborda a situação do Brasil como ator no espaço cibernético comentando a partir de suas políticas e estratégias o momento atual. Ele apresenta e comenta a posição da Marinha do Brasil e sua atuação pioneira na segurança da informação, das comunicações e cibernética.

Palavras-chave: Cibernética; Guerra Cibernética; Quinto Domínio da Guerra.

1 Mestre em Ciências da Computação e Informática, na área de Inteligência Artificial, pelo Instituto Militar de Engenharia (IME), Rio de Janeiro, RJ, Brasil. E-mail: juliocezarbarretoleite@gmail.com

2 Doutor em Ciências Navais pela Escola de Guerra Naval (EGN), Rio de Janeiro, RJ Brasil.

CYBERNETIC WARFARE: THE FIFTH DOMAIN WARFARE, CONCEPTS AND PRINCIPLES

ABSTRACT

This article aims to present a comprehensive definition for Cyber Warfare. Therefore it explores the scope of concepts related to this matter, searching for principles, characteristics, peculiarities and proper use of words, in order to support the proposed definition. The article also addresses the situation of Brazil as an actor in the Cyberspace, commenting the country's current policies and strategies. It also presents the Brazilian Navy's position with pioneer action on informations', communications' and cybernetics' security.

Keywords: Cybernetics; Cyberwarfare; Fifth Domain Warfare.

INTRODUÇÃO

A Guerra Cibernética é hoje o mais novo domínio da guerra, juntamente com o domínio Terrestre, Marítimo, Aéreo e Espacial (Geoespacial). Constantemente ela apresenta sinais de que está em andamento e influencia cada vez mais os relacionamentos entre Nações e Estados.

Mas o que é a Guerra Cibernética? O presente artigo busca lançar luz sobre a polêmica existente em relação à definição desse domínio, suas características, conceitos e princípios. Aborda também as ações por parte do Brasil a fim de enfrentar a ameaça cada vez mais palpável que provém do Espaço Cibernético. Cita as políticas e estratégias, ligadas à Defesa Cibernética, implementadas e em implementação, apresentando o papel do Ministério da Defesa. O artigo também apresenta a Marinha no contexto da Guerra Cibernética, comentando seu pioneirismo, atuação e desenvolvimento.

DEFINIÇÕES ABRANGENTES

Cibernética

Em 1948, Norbert Wiener[3] cunhou o termo "Cibernética" para englobar o conjunto formado pela Teoria de Controle e a Teoria de Comunicação em uma máquina ou em um animal. Wiener visualizou que a ***informação***, como uma quantidade, era tão importante quanto à energia ou a matéria. Sua colaboração tornou possível a criação de um ambiente intelectual em que o funcionamento e o controle de computadores, sistemas de comunicação e controle, comandos eletromagnéticos, transmissões eletrônicas nas máquinas de calcular e nos autômatos modernos pudessem ser desenvolvidos. Dessa forma, podemos considerar a cibernética como o uso de sistemas de comunicação e consequentemente de seus componentes, que são vitais para troca de informações entre esses componentes, dentro de um mesmo sistema, e também entre o sistema e o ambiente.

Espaço Cibernético

Certamente o significado atribuído à Cibernética serviu para que William Gibson[4] criasse, em sua obra de ficção "Neuromancer" de 1982, o termo "Cyberspace" (Espaço Cibernético ou Ciberespaço), que servia para designar uma rede de computadores, roteadores, chaves e pessoas, que estava em constante mutação. O Departamento de Defesa dos EUA (Departament of Defense - DoD) define Espaço Cibernético como "um domínio global dentro do ambiente de informações que consistem das redes interdependentes de infra-estruturas de Tecnologia da Informação (TI), incluindo a Internet, redes de telecomunicações, sistemas de computador, processadores e controladores embutidos." [EUA. Departamento de Defesa (DoD)][5].

Cada vez mais computadores, seus equipamentos de interconexão, sistemas de comando, controle, comunicações e informação (C^3I) e sistemas de apoio à decisão compõem o espaço cibernético militar, em que a informação é o objetivo maior. Dessa forma, esse espaço se tornou fundamental na guerra, em decorrência da grande importância militar dos computadores e de suas redes para a circulação de ordens ou informações.

3 WIENER, Norbert. *Cybernetics: or the control and communication in the animal and the machine.* 1948.

4 GIBSON, William. Neuromancer. 2008.

5 ESTADOS UNIDOS DA AMÉRICA. Departamento de Defesa (DoD). *Department of Defense Dictionary of Military and Associated Terms*. 2008.

Hoje, as informações que trafegam nessas redes interligam aeronaves, embarcações, bases locais de apoio e centros estratégicos de controle localizados no país de origem, entre outros. Tentar invadir essas redes com o intuito de descobrir segredos ou para utilizá-los em proveito próprio é o objetivo do que hoje é denominado "Guerra Cibernética".

Guerra Cibernética

Não existe consenso em definir o que venha a ser Guerra Cibernética. Levando-se em consideração a definição da palavra "Cibernética" e aceitando a definição de Espaço Cibernético como o ambiente em que de ocorrerão conflitos entre diferentes atores, podemos imaginar que "Guerra Cibernética" seria o conflito travado entre dois ou mais Estados no Ciberespaço. As demais atividades desenvolvidas por atores não estatais, com potencial de dano à informação no Ciberespaço, devem ser tratadas como incidentes cibernéticos ou, usando um termo também já generalizado, como ataques cibernéticos, ligados à Segurança da Informação.

No Brasil, o Ministério da Defesa (MD) define Guerra Cibernética como sendo "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 informação e redes de computadores. Essas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil" [BRASIL, 2007c, p. 123][6]. Tal definição não contempla todos os tipos de ações comuns à Guerra Cibernética, deixando de contemplar a exploração de sistemas.

O DoD não tem uma definição específica para Guerra Cibernética, porém define Espaço Cibernético, como apresentado, e Operações no Espaço Cibernético. Essas operações são definidas como "o emprego de capacidades Cibernéticas onde o propósito principal está em alcançar objetivos ou bens militares dentro do espaço cibernético ou através dele." Juntas, as definições demonstram a compreensão do DoD sobre a Guerra Cibernética como sendo "o emprego de capacidades Cibernéticas onde o propósito principal está em alcançar objetivos ou bens militares em um domínio global dentro do ambiente de informações que consistem das redes interdependentes de infra-estruturas de Tecnologia da Informação (TI), incluindo a Internet, redes de telecomunicações, sistemas de computador, processadores e controladores embutidos ou através dele".

6 BRASIL. Ministério da Defesa. MD35-G-01: Glossário das Forças Armadas. 2007.

As conjecturas apresentadas, quando analisadas juntamente com as definições do MD e do DoD, e o entendimento de que o espaço cibernético é o ambiente operacional em que se dará o conflito, nos permitem chegar à compreensão e propor uma definição abrangente para Guerra Cibernética.

Guerra Cibernética é o conjunto de ações ofensivas, defensivas e ou exploratórias, realizadas no espaço cibernético, que buscam negar seu uso pelo inimigo e garantir o uso, a segurança, a confiança, a integridade, a rapidez e o sigilo das informações, existentes em computadores, redes e sistemas de informação, em proveito próprio, tanto na área militar quanto na área civil.

PRINCÍPIOS, CARACTERÍSTICAS, OBJETIVOS E AÇÕES

Princípios

Os Princípios da Guerra são matéria de estudo sempre associada a grandes pensadores da guerra como Sun Tzu[7], Clausewitz[8], Lydell Hart[9] e Caminha[10]. O valor desses estudos reside na formação de importantes padrões de referência tanto para uma análise estratégica quanto para as necessidades táticas. A partir deles estrategistas se orientam na elaboração dos planos e suporte para doutrinas. Para os comandantes em nível tático servem de orientação para as ações operacionais e seu desenvolvimento. Quando compreendidos e seguidos adequadamente, os estudos sobre os princípios da guerra indicam os caminhos de como chegar à vitória, apesar de não poderem ser considerados infalíveis.

São conhecidos pelos Estados Ocidentais nove Princípios da Guerra, são eles: Objetivo; Ofensiva; Massa; Economia de Forças; Manobra; Unidade de Comando; Segurança; Surpresa e Simplicidade. Nos Estados Orientais, destacando-se a Rússia e a China, são considerados: Ofensiva; Manobra e Iniciativa; Concentração e Economia de Forças; Avanço e Consolidação; Armas e Ações Combinadas; Aniquilamento; Ação de Comando; Qualidade e Quantidade das Forças; Reservas Adequadas; Moral; Estabilidade de Retaguardas e Surpresa.

Sun Tzu considerava cinco fatores fundamentais, que seguidos, definiriam quem seria vitorioso em um conflito. A Influência Moral – "Ter

7 SUN TZU, por CLAVELL, James. *A Arte da Guerra*., 1998.
8 CLAUSEWITZ, Carl V. *Da Guerra,* 1998.
9 HART, Liddell. *Estratégia:* Conceituação e emprego em 25 séculos. 1966.
10 CAMINHA, João C. G. *Delineamentos da Estratégia,* 1980.

o exército animado do mesmo espírito em todos os postos", o Clima – "Saber quando lutar e quando não lutar", Terreno – "Saber como manobrar tanto forças inferiores quanto superiores", Comando – "Ter capacidade militar e não ser influenciado pelo soberano" e a Doutrina – "Esperar preparado para surpreender o inimigo despreparado", sintetizam profeticamente todos os princípios, ocidentais e orientais. Esses, somados à arte do engodo ("atacar com estratagemas" Sun Tsu. *A arte da Guerra* – p. 25) definiam que.

> "A mais perfeita forma de comandar é impedir os planos do inimigo, evitar a junção de suas forças, atacar o exército inimigo no próprio campo e nunca sitiar cidades muradas" (SUN TSU, 1996 ,p.25)

Considerando a Guerra Cibernética, foram sugeridos por Parks e Duggan[11] oito princípios quando abordaram o tema em seu trabalho. São eles:

— Princípio do Efeito Cinético (Guerra Cibernética deve produzir efeitos no mundo cinético);

— Princípio da Mutabilidade (não existem leis de comportamento imutáveis no Mundo Cibernético, excetuando-se aquelas que necessitam de uma ação no Mundo Real);

— Princípio do Disfarce (alguma entidade no Mundo Cibernético possui a autoridade, acesso ou habilidade necessários para por em prática qualquer ação que um atacante deseje realizar; o objetivo do atacante é assumir a identidade dessa entidade, de alguma forma);

— Princípio da Dualidade do Armamento (as ferramentas – ou armamentos – da Guerra Cibernética são de natureza dual);

— Princípio da Compartimentação (tanto o atacante, como o defensor de um sistema, controlam uma pequena parcela do Ciberespaço que utilizam);

— Princípio da Usurpação (quem controlar a parte do Ciberespaço que o oponente utiliza, pode controlar o oponente);

— Princípio da Incerteza (o Ciberespaço não é consistente, nem confiável); e

— Princípio da Proximidade (limitações físicas de distância e espaço não se aplicam ao Mundo Cibernético).

A enumeração desses princípios específicos para a Guerra

11 PARKS, R.C. and DUGGAN, D.P. *Principles of Cyberwarefare*. 2001.

Cibernética deu-se a partir da crença dos autores de que os princípios clássicos da guerra não se adaptam ao Espaço Cibernético. Contudo, o presente artigo considera tais "princípios" mais afetos a características específicas do ambiente cibernético do que propriamente a características gerais de conflitos nesse mesmo ambiente.

Os Princípios da Guerra consagrados, clássicos, que se adequam à Guerra Cibernética de forma geral, são os seguintes:

— Princípio do Objetivo – O que atacar e onde atacar, destruir, conquistar, defender, manter, retardar, explorar etc;

— Princípio da Ofensiva – Manter ações ofensivas e defensivas que conduzam à vitória final. Consecução do objetivo almejado;

— Princípio da Massa – Maior concentração de esforços (software, hardware e operações de redes) ofensivos e defensivos sobre os principais sistemas do inimigo;

— Princípio da Manobra – O inimigo deve ser colocado em situação desfavorável através da aplicação flexível do poder de combate;

— Princípio da Unidade de comando - Para cada objetivo deve haver unidade de esforço sob a responsabilidade de um único comando;

— Princípio da Segurança – Não permitir jamais que o inimigo nos surpreenda. Manter doutrinas de Segurança da Informação e Defesa Cibernética fortes e atualizadas; e

— Princípio da Surpresa – Ser capaz de atuar no ponto e momento em que o inimigo não espere e seja apanhado despreparado.

Diante disso, Princípios da Guerra comumente aplicados às Guerras da Informação, Naval de Superfície, Eletrônica e outras. também são cabíveis ao ambiente cibernético, considerando suas características e objetivos peculiares.

Características

O Espaço Cibernético define algumas características aplicadas especificamente à Guerra Cibernética. O portal de análises de inteligência STRATFOR (2008)[12] enumera onze dessas características em seu trabalho: "necessidade de surpresa, necessidade de vulnerabilidades a explorar, dificuldade de realização do segundo ataque, efeito temporário dos ataques cibernéticos, limitação de danos físicos, uso dual das ferramentas, limitação do controle, vantagem do ataque sobre a defesa, existência de incertezas na Guerra Cibernética, presença de não combatentes no

12 STRATFOR. Portal de Análise. *CYBERWARFARE 101: The Internet Is Mightier Than the Sword*. 2008.

ciberespaço e o paradoxo cibernético".

Rattray[13], em seu artigo, enumera outras características da Guerra Cibernética, sendo as mais relevantes: Espaço Cibernético (campo novo e dinâmico); Anonimato; Quebra das barreiras físicas e geográficas e Assimetria.

Recorrendo aos "princípios" enumerados por Parks e Duggan e tendo em mente as características consideradas por Rattray e analisados no Portal STRATFOR, podemos concluir que a Guerra Cibernética ocorre no ambiente definido pelo Espaço Cibernético. Ela se aproveita do anonimato pela ocultação, surpresa, incerteza e o disfarce (engodo). Quebra as barreiras físicas e temporais devido à inexistência de limites, fronteiras ou distâncias físicas separando os atores. Suas operações são fundamentalmente assimétricas, sendo que os equipamentos, redes e sistemas do espaço cibernético possuem vulnerabilidades a explorar e a defender. Nela o primeiro ataque é decisivo, vigorando sempre o seguinte paradoxo cibernético:

> Quanto maior a capacidade em TI de um Estado, maior a sua fragilidade à ataques cibernéticos.

Observamos que as características consideradas no presente artigo levam ao entendimento de que a Guerra Cibernética é um instrumento de apoio para que as ações realizadas no mundo exterior ao espaço cibernético (mundo cinético) tenham eficácia na busca do sucesso da missão principal em atingir seus objetivos.

Objetivos

O objetivo básico, seja no nível estratégico, tático ou operacional, em uma guerra cibernética, é a informação.

Estrategicamente, a guerra cibernética tem como objetivo os sistemas relacionados à infra-estrutura nacional de energia (eletricidade, petróleo e gás), ao sistema financeiro e à infra-estrutura social (transportes, abastecimento e outros serviços públicos), contribuindo para a diminuição da capacidade de defesa e reação do Estado.

Taticamente, a guerra cibernética objetiva os sistemas de comunicação, controle e apoio à decisão, contribuindo para diminuir a

13 RATTRAY, Gregory J. *An environmental approach to understanding cyberpower*. 2009.

capacidade operacional e logística de uma Força Armada.

Operacionalmente, a Guerra Cibernética tem os sistemas de controle e a comunicação operacional como objetivo, contribuindo para a diminuição da capacidade de coordenação, apoio à decisão e manobra de um grupo ou fração da Força Armada.

Dessa forma observamos que a Guerra Cibernética esta presente nos campos estratégico, tático e operacional, desenvolvendo ações próprias do Espaço Cibernético.

Ações

Apresentados Espaço Cibernético, Guerra Cibernética, suas características e objetivos, necessitamos acrescentar as ações a serem desempenhadas no ambiente cibernético. As ações na Guerra Cibernética são divididas em três tipos básicos: Ações Ofensivas, Defensivas e de Exploração.

As ações ofensivas buscam destruir, impedir e ou dificultar a utilização de informação pelo inimigo e de suas capacidades cibernética, tanto por meio de ataques físicos como por ataques cibernéticos, pela rede, utilizando "armas cibernéticas".[14]

As ações defensivas buscam evitar ou minimizar ataques cibernéticos lançados pelo inimigo, protegendo a informação, e restaurar rapidamente os danos e limitações oriundas desses ataques, impingidas às capacidades cibernéticas, garantindo a utilização do Espaço Cibernético.

As ações de exploração buscam monitorar o inimigo na busca de informações sigilosas, detectar suas atividades cibernéticas e conhecer suas vulnerabilidades sistêmicas dentro da rede, buscando informações que proporcionem vantagem tanto no ambiente cibernético quanto no ambiente cinético.

ATORES CONTEMPORÂNEOS

Atores são os agentes do ato. São elementos facilmente identificáveis em um determinado ambiente, pois estão em constante interação com o ambiente e com outros atores, que podem ser externos ou internos. Suas ações influenciam outros atores, o ambiente em que se encontram e outros ambientes e atores externos. Os atores são agentes de

14 Armas Cibernéticas são dispositivos de hardware ou software empregados durante ações no Espaço Cibernético. As mais populares são as Chaves de Hardware, Firewalls (HW SW), Softwares Maliciosos (Malwares), vírus e outros programas (Bombas Cibernéticas) que atuam de forma predeterminada acionados externamente ou por comandos de software, sempre com intuito de garantir a utilização da informação no meio Cibernético ou causar dano ao inimigo.

modificações que podem alterar características e relacionamentos do meio.

Entre os atores existentes no ambiente cibernético encontramos os Estados, as Instituições, as Corporações Industriais/Empresariais, o Setor Financeiro, o Setor de Serviços, Grupos de ativistas políticos/religiosos, "*hackers*", criminosos digitais ("*crackers*", "*banckers*", etc.) e pessoas comuns.

Esses atores têm como característica comum estarem ligados a uma rede que se conecta mundialmente, a Internet. Todos eles realizam interações dentro do Espaço Cibernético, utilizando serviços, trocando informações, comunicando-se, movimentando a economia, desenvolvendo serviços/facilidades, cometendo crimes e fazendo a guerra.

Os atores cibernéticos existem e se multiplicam, em número e variedade, na medida em que avança a tecnologia da informação e aumenta o acesso, da humanidade, às facilidades da computação.

EMPREGO DA GUERRA CIBERNÉTICA: CAMPOS DE UTILIZAÇÃO (SOFTWARE, HARDWARE E REDE)

Como citado anteriormente, o principal objetivo na Guerra Cibernética é a informação. Tal informação deve possibilitar efeitos capazes de ultrapassar o domínio cibernético. A utilização de softwares e hardwares com a finalidade de controlar redes de dados só possui algum sentido se afetarem atores também fora desse campo, daí o emprego da Guerra Cibernética ser possível em diversos campos da atividade humana desde que dependam de recursos de computação e informática para se desenvolverem e tenham alguma influência na consecução de um propósito final.

Ataques à estruturas sensíveis de um país com a consequente paralisação ou destruição de seus sistemas são os efeitos desejados nos domínios físico e cognitivo da guerra. Domínio cognitivo entende-se ser aquele em que encontram as percepções e a compreensão sobre o significado da informação, bem como os modelos mentais, preconceitos e valores que influenciam como a informação é interpretada, compreendida e utilizada. (ALBERTS; HAYES, 2003).[15]

BRASIL NA GUERRA CIBERNÉTICA: PND, END, PCD, GSI E EXÉRCITO BRASILEIRO

A crescente presença dos Estados no espaço cibernético e as

15 ALBERT, David S.; Hayes Richard E. *Power to the Edge:* Command and Control in the Information Age. 2003.

atividades dos atores não estatais, incluindo entidades comerciais, criminosos cibernéticos e grupos terroristas, tornam o ciberespaço um ambiente cada vez mais complexo e vulnerável. Essa vulnerabilidade tem influenciado políticas Estatais para garantir a proteção das estruturas nacionais. O Brasil estabeleceu na Política Nacional de Defesa (PND), na Estratégia Nacional de Defesa (END) e na Política Cibernética de Defesa (PCD) os parâmetros de atuação necessários à preparação do País para atuar no domínio cibernético.

A END define o Setor Cibernético como um dos três setores estratégicos nacionais, sendo uma de suas prioridades a implantação do Comando de Defesa Cibernética, que a partir de dezembro de 2012 passou a coordenar o Sistema Brasileiro de Defesa Cibernético (SBDC).

O SBDC esta dividido em três níveis de atuação: político, estratégico e operacional e tem como finalidade atender os objetivos da END referentes à defesa cibernética, coordenando os diversos órgãos do Estado no que se refere a esse tema. O quadro abaixo apresenta a distribuição das instituições pelo SBDC:

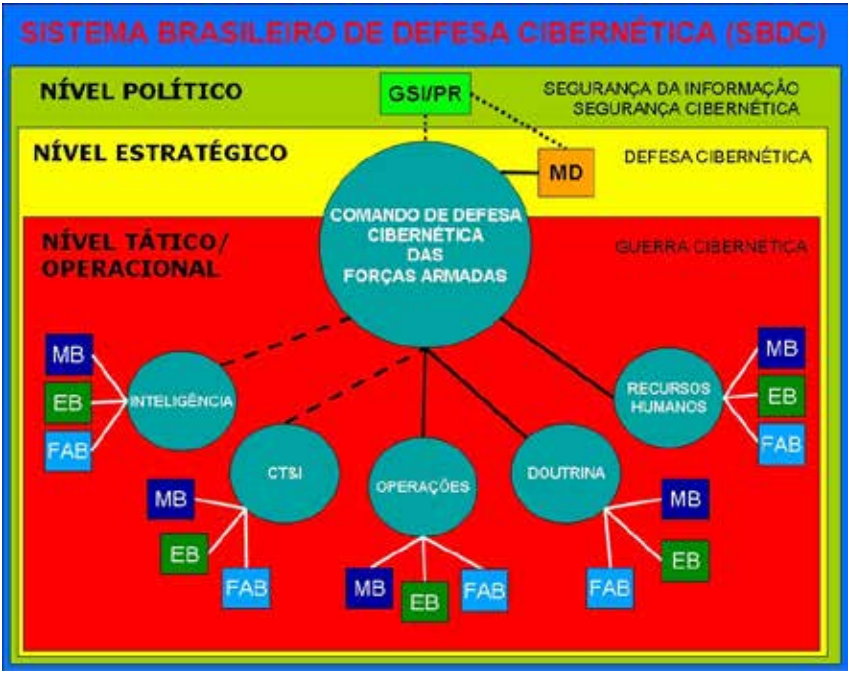

Figura 1 – Quadro com os níveis de abrangência do SBDC.

O Gabinete de Segurança Institucional da Presidência da República

(GSI/PR) é o coordenador da segurança de informação e comunicação (SIC) e cibernética (SC) zelando pela segurança dos sistemas afetos à infra-estrutura nacional de energia (eletricidade, petróleo e gás), o sistema financeiro e a infra-estrutura social (transportes, abastecimento e outros serviços públicos).

O GSI/PR age de forma coordenada com o MD que é o coordenador da defesa cibernética, a nível estratégico, e da guerra cibernética, a nível tático/operacional.

O Comando de Defesa Cibernética das Forças Armadas, dentro da estrutura do SBDC exerce papel de assessoria executiva ao MD e ao GSI/PR sendo responsável pela parte executiva das ações de defesa cibernética, a nível estratégico, e pela coordenação das três forças armadas, Marinha, Exército e Aeronáutica, à nível tático/operacional, no que se refere aos aspectos logísticos, operacionais, doutrinários, de CT&I e recursos humanos afetos a guerra cibernética propriamente dita.

A coordenação do SBDC a nível nacional cabe ao Exército Brasileiro, que é responsável pelo Comando de Defesa Cibernética das Forças Armadas.

No Brasil a Guerra Cibernética prioriza a segurança de informação e comunicação, segurança cibernética e defesa dos ativos de informação da Administração pública Federal. O MD, por meio da END e da PCD mostra excessiva preocupação com os níveis político e estratégico do SBDC, deixando a desejar, porém, no que diz respeito à Defesa Cibernética de nível tático-operacional, que é deixada a critério de cada força singular, e à Guerra Cibernética propriamente dita, parecendo menosprezar os efeitos de ataques cibernéticos fora do âmbito das estruturas críticas nacionais.

MARINHA DO BRASIL NA SEGURANÇA DA INFORMAÇÃO E GUERRA CIBERNÉTICA

A Marinha do Brasil (MB) é a pioneira na utilização de recursos de informática na administração pública federal desde o final dos anos 1960. Foi a primeira força armada a empregar sistemas de armas computadorizados adquiridos com as fragatas da classe "Niterói" na década de 1970. Esse pioneirismo continua com a criação de centros de excelência para apoio à sistemas operativos (CASOP) e de análise de sistemas navais (CASNAV).

A chegada da END encontrou a MB preparada para agir nos

campos da SIC e da SC. Na MB, esses campos são coordenados pela Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM). A DCTIM tem implementado, por meio de projetos em andamento no CASNAV, diversos sistemas de apoio à segurança digital da informação e das comunicações na MB.

No setor cibernético, o CASNAV desenvolve projetos de segurança voltados para a certificação digital no contexto de Chaves-Públicas desde os anos 90. Seus programas serviram de modelo para a implementação da Infra-estrutura de Chaves - Públicas da Defesa (ICP-Defesa) e inspiram a implementação de um sistema de chaves - públicas de segurança para ser utilizado em toda administração pública federal. Dentre os projetos em implementação pelo CASNAV destacam-se três: o Volume Criptografado (VolCript), destinado a gerenciar e proteger arquivos digitais para reduzir o risco de sabotagem e adulteração, o Metodologia para Avaliação e Homologação de Aplicações de Sistemas Criptográficos, para garantir a qualidade e a segurança do software criptográfico e do Projeto Guerra Cibernética Objetiva (GUERCIB). Tal projeto busca minimizar ataques praticados nos sistemas de informações digitais da Marinha, sendo composto por softwares inteligentes.

Dessa forma, podemos verificar que a MB se mantém pioneira no desenvolvimento de soluções em TI aplicada a Defesa Cibernética e Segurança da Informação e Comunicação, porém ainda não se desenvolve no campo da guerra cibernética propriamente dita, sendo um espelho do estágio em que o país se encontra no setor.

CONCLUSÃO

O mundo tem testemunhado o surgimento de diversos resultados de ações relacionadas ao setor cibernético. A maior incidência é de crimes cibernéticos atribuídos a "*crackers*" e "*banckers*". Recentemente a constatação de que outros atores vêm agindo sob o manto do anonimato confirma a existência de uma guerra cibernética em andamento. A sabotagem do programa nuclear iraniano por ataque de vírus[16], a paralisação dos serviços

16 O Mossad, agência de inteligência estrangeira de Israel, atacou, em julho de 2010, o programa nuclear iraniano com um vírus de computador altamente sofisticado chamado Stuxnet. A primeira arma digital de importância geopolítica, que pode mudar a forma como as guerras são travadas - e não será o último ataque de seu tipo.

essenciais e o corte das comunicações com o mundo sofrido pela Geórgia durante a crise com a Rússia e, recentemente, a espionagem de diversos países realizada pelo Serviço Secreto Americano (NSA) e denunciada por Edward Snowden, comprovam que o espaço cibernético é certamente um domínio global.

A definição de Guerra Cibernética apresentada no presente artigo se aproxima dos fatos constatados e apresentados acima. Esta nova modalidade de conflito é o conjunto de ações ofensivas, defensivas e ou exploratórias, realizadas no espaço cibernético, que buscam negar seu uso pelo inimigo e garantir o uso, a segurança, a confiança, a integridade, a rapidez e o sigilo das informações, existentes em computadores, redes e sistemas de informação, em proveito próprio, tanto na área militar quanto na área civil.

Dentro desse contexto, constatamos que o SBDC não engloba todos os níveis em que se realizam as ações em uma guerra cibernética. O sistema vem se preparando para a defesa contra ações de exploração, enquanto deixa a desejar em ações de ataque e defesa cibernéticas. O Brasil enfatiza a segurança da informação das comunicações (SIC) e cibernética (SC), porém está vulnerável no que se refere à Defesa e Guerra Cibernética propriamente dita.

Essa vulnerabilidade permanecerá enquanto não houver uma vontade política mais forte, aporte financeiro adequado, investimento em pessoal, material e pesquisa e principalmente uma conscientização coletiva da Nação sobre os resultados que podemos esperar quando não se está preparado para uma Guerra Cibernética.

REFERÊNCIAS

ALBERT, David S.; HAYES, Richard E. *Power to the Edge:* Command and Control in the Information Age. DoD Command and Control Research Program CCRP. Washington, DC: Library of Congress Press, 1942, reimpressão 2003. Disponível em: <http://www.dodccrp.org/files/Alberts_Power.pdf>. Acesso em: 20 maio 2014.

BRANDÃO, Antônio Cesar C. Novos paradigmas para o campo de batalha do século XXI: guerra cibernética. Rio de Janeiro: Academia Militar das Agulhas Negras (AMAM). EPESM, 2., 2010. Anais... 2010. Disponível em <http://www.aman.ensino.eb.br/index2.php?option=com_docman&task=doc_view&gid=497&Itemid=60 >. Acesso em: 04 out. 2011.

BRASIL. Comandante do Exército. Portaria nº. 666, de 4 de agosto de 2010. Cria o Centro de Defesa Cibernética do Exército e dá outras providências. *Boletim do Exército*, n. 31, de 6 de agosto de 2010. Site DefesaNet 2011. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/1633/CDCIBER---Portaria-de-criacao-do-Centro-de-Defesa-Cibernetica-do-Exercito>. Acesso em: 29 set 2012.

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, 1 jul. 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm>. Acesso em: 20 maio 2014.

BRASIL. Ministério da Defesa. *Estratégia Nacional de Defesa*: paz e segurança para o Brasil. Brasília, DF, 2008. Disponível em: <http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_portugues.pdf>. Acesso em: 20 maio 2014.

BRASIL. Ministério da Defesa. *MD35-G-01*: glossário das forças armadas. 4. ed. Brasília, DF: Publicação do Ministério da Defesa, 2007.

CAMINHA, João C. G. *Delineamentos da Estratégia*. Escola de Guerra Naval (EGN), Rio de Janeiro: EGN, 1980, 598 p.

CHINA confirma cyber blue team. *DefesaNet*, maio 2011. Seção Tecnologia. Disponível em: <http://www.defesanet.com.br/tecnologia/noticia/1167/China-confirma—Cyber-Blue-Team>. Acesso em: 29 set. 2012.

CLAUSEWITZ, Carl V. *Da Guerra*. 2. ed. São Paulo: Editora Martins Fontes, 1996.

CRESCE número de ciberataques. *DefesaNet*, mar. 2011. Seção Cobertura especial, cyberwar, tecnologia. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/286/Cresce-numero-de-ciberataques>. Acesso em: 29 set. 2012.

CUNHA, Diogo. *Introdução à Guerra Cibernética*: a necessidade de um despertar brasileiro para o assunto!. Rio de Janeiro: Forense Computacional, 2011. Disponível em: <http://guerracibernetica.wordpress.com/category/forense-computacional/>. Acesso em: 04 out. 2011.

CYBERWARFARE 101: the internet is mightier than the sword. Stratfor Global Intelligence, 15 Apr. 2008. Disponível em: <http://www.stratfor.com/memberships/114720/analysis/cyberwarfare_101_internet_mightier_sword>. Acesso em: 27 abr. 2010.

EUA querem estratégia de cibersegurança mundial. *DefesaNet*, maio. 2011. Seção Cobertura especial, cyberwar, tecnologia. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/1066/EUA-querem-estrategia-de-ciberseguranca-mundial>. Acesso em: 29 set. 2012.

EXÉRCITO dos Estados Unidos lança app para blogs de soldados. *DefesaNet*, mar. 2011. Seção Cobertura especial, cyberwar, tecnologia. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/124/Cyberwar---Exercito-dos-Estados-Unidos-lanca-app-para-blogs-de-soldados>, Acesso em: 29 set 2012.

GIBSON, William. *Neuromancer*. 4. ed. São Paulo: Editora Aleph, 1991.

HART, Liddell. *Estratégia:* Conceituação e emprego em 25 séculos. Rio de Janeiro: Editora Biblioteca do Exército, 1966.

HUAWEI desafia governo dos EUA a investigá-la. *DefesaNet*, mar. 2011. Seção Cobertura especial, cyberwar, tecnologia. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/136/Cyberwar---Huawei-desafia-governo-dos-EUA-a-investiga-la>. Acesso em: 29 set. 2012.

KEITH, B. Alexander. *A Guerra no ambiente cibernético.* Washington D.C.: National Defense University Press, Joint Force Quarterly, MILITARY Technology (MILTEC), mar. 2011. p. 41-44.

MOON, Peter, Cyberwar: em contexto: Internet não é garantia de democracia. *DefesaNet*, abr. 2011. Seção Tecnologia. Disponível em: <http://www.defesanet.com.br/tecnologia/noticia/715/Cyberwar---Em-contexto--Internet-nao-e-garantia-de-democracia>. Acesso em: 29 set. 2012.

MOTTA, Severino, CDCiber: na guerra cibernética, Brasil adota estratégia do contra-ataque. *DefesaNet*, jun. 2011. Seção Cobertura especial, cyberwar, tecnologia. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/1632/CDCiber---Na-guerra-cibernetica--Brasil-adota-estrategia-do-contra-ataque>. Acesso em: 29 set. 2012.

PARIZ, Tiago; SILVEIRA, Igor. PLANALTO responde: Forças Armadas contra hackers. *DefesaNet*, jun. 2011. Seção Cobertura especial, cyberwar, tecnologia. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/1624/Cyberwar---Planalto-Responde--Forcas-Armadas-contra-hackers>. Acesso em: 29 set.;2012.

PARKS, Raymon C.; DUGGAN, David P. Principles of Cyber-warfare. *IEEE Security & Privacy*, v. 9, n. 5, p. 30-35, Sept./Oct. 2011. Disponível em: <http://www.periwork.com/peri_db/wr_db/2004_May_11_11_30_41/DOCS%20WEBREVIEW/PrinciplesCYBER%20WARFARE.pdf >. Acesso em: 1 set. 2011.

RATTRAY, Gregory J. An environmental approach to understanding cyberpower. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry K. (Ed.). *Cyberpower and national security*. Washington: Center for Technology and National Security Policy, 2009. cap. 2.

SAMPAIO, Fernando G. *Ciberguerra guerra eletrônica e informacional*: um novo desafio estratégico. Brasília: Escola superior de Geopolítica e Estratégia (ESGE), 2001. Disponível em: <http://www.defesanet.com.br/esge/ciberguerra.pdf>. Acesso em: 29 set. 2012.

SORG, Letícia. Evgeny Morozov: 'A internet acelera o fim de regimes fracos'. *DefesaNet*, mar. 2011. Seção Cobertura especial, cyberwar, geopolítica. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/112/Cyberwar---Evgeny-Morozov---A-internet-acelera-o-fim-de-regimes-fracos>. Acesso em: 29 set. 2012.

STARK, Holger. Mossad's miracle weapon: stuxnet virus opens new era of cyber war. *Spiegel on Line*, Berlim, Alemanha, Aug. 2011. Disponível em: <http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html>. Acesso em: 01 set. 2011.

SUN TZU. *A Arte da Guerra.* 17. ed. Rio de Janeiro: Editora Record, 1996. 111 p. Tradução de José Sanz.

UNITED STATES. Departament of Defense. *Strategy for operating in cyberspace*. Washington D.C.: DoD Press, July 2011.

UNITED STATES. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington D.C., July, 2011. Disponível em: <http://www.defense.gov/news/d20110714cyber.pdf>. Acesso em: 20 maio 2014.

UNITED STATES. Department of Defense. *Dictionary of Military and Associated Terms*. Washington D.C.: DoD Press, Nov. 2010. (Joint Publication 1-02). Disponível em: <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf>. Acesso em: 20 maio 2014.

UNITED STATES. The White House. *International Strategy for Cyberspace:* prosperity, securityu, and openness in a networked world. Washington D.C., may 2001. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: 04 out. 2011.

WALLER, Michael. China revisa a Arte da Guerra. *DefesaNet*, set. 2000. Seção Geopolítica. Disponível em: <http://www.defesanet.com.br/geopolitica/noticia/1166/China-Revisa-a-Arte-da-Guerra>. Acesso em: 29 set. 2012.

WIENER, Norbert. *Cybernetics or Control and Communication in the Animal and the Machine*. 2. ed. Nova Yorque: John Wiley & Sons Inc., 1965. 232p.

Recebido em: 05/06/2014
Aceito em: 16/12/2014