ESCOLA DE GUERRA NAVAL

CMG MARCELO LUIS SEABRA PINTO

GUERRA CIBERNÉTICA NA MB:

desafios e perspectivas para a próxima década

Rio de Janeiro

2009

CMG MARCELO LUIS SEABRA PINTO

GUERRA CIBERNÉTICA NA MB:

desafios e perspectivas para a próxima década

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CMG (RM1) Antonio José NEVES de Souza

Rio de Janeiro

Escola de Guerra Naval

2009

RESUMO

O controle da informação sempre fez parte das operações militares, porém os avanços tecnológicos e a situação das sociedades totalmente interligadas economicamente e através da internet têm imputado aos comandos militares uma nova visão sobre a Guerra Cibernética, com nova ênfase para controlar ou desabilitar os computadores inimigos com o propósito de reduzir a capacidade de reação do adversário. As redes de computadores hoje são meio, alvo e arma da guerra. Com o domínio da tecnologia digital de ataque e defesa, forças militares capacitadas poderão agir diretamente nos computadores inimigos, alterando os bits armazenados e comprometendo a informação dentro dos computadores ou paralisando as comunicações nas redes de dados dos adversários. O presente trabalho apresenta um resumo histórico dos perigos da evolução tecnológica dos sistemas computacionais. Em seguida, se apresenta como alguns Estados e organizações internacionais têm abordado o assunto, principalmente, no aspecto da segurança da informação. A situação atual em órgãos do governo brasileiro e a legislação já existente sobre o assunto também são apresentados. Como resultado do trabalho pretende-se apresentar os desafios e as perspectivas para a Marinha do Brasil enfrentar nos próximos anos, a fim de se preparar para as novas ameaças do espaço cibernético.

Palavras-chave: Guerra Cibernética, Marinha do Brasil, Segurança da Informação.

ABSTRACT

The control of information has always been part of military operations, but technological advances and the situation of the companies fully interconnected economically and through the Internet have accused the military commands a new vision on the Cyberwarfare, a new emphasis to control or disable enemies with computers the purpose of reducing the capacity of reaction of the opponent. The computers networks of today are way, target and weapon of war. With the field of digital technology for attack and defense, military forces may act directly trained on computers enemies, changing the bits and compromising the information stored within computers or paralyzing the communications networks of data from opponents. This work presents a historical summary of the dangers of technological evolution of computer systems. It then shows how some states and international organizations have addressed the issue, especially in the aspect of information security. The current situation in bodies of the Brazilian government and the existing legislation on the subject are also presented. As a result of the work aims to present the challenges and prospects for the Brazilian Navy face in coming years in order to prepare for the new threats of cyberspace.

Keywords: Cyberwarfare, Brazilian Navy, Information Security.

LISTA DE ABREVIATURAS E SIGLAS

APF – Administração Pública Federal
CCripto – Coordenadoria de Criptologia
CGSI – Comitê Gestor de Segurança da Informação
COeM – Coordenadoria de Organização e Métodos
COM – Comando de Operações Navais
COpS – Coordenadoria de Operações Cibernéticas e Análises de Segurança
CTIM – Centro de Tecnologia da Informação da Marinha
DCT – Departamento de Ciência e Tecnologia
DCTIM – Diretoria de Comunicações e Tecnologia da Informação da Marinha
DGMM – Diretoria Geral do Material da Marinha
DIPNAV – Diretrizes para o Planejamento Naval
DTM – Diretoria de Telecomunicações da Marinha
DoS – Negação de Serviço
DSIC – Departamento de Segurança da Informação e das Comunicações
EB – Exército Brasileiro
EMA – Estado Maior da Armada
EMD – Estado Maior de Defesa
END – Estratégia Nacional de Defesa
EUA – Estados Unidos da América
FAB – Força Aérea Brasileira
GC – Guerra Cibernética
GCR – Guerra Centrada em Redes
GED – Gerenciamento Eletrônico de Documentos
GRI – Grupo de Resposta a Incidente
GSI-PR – Gabinete Segurança Institucional da Presidência da República
ICP-Brasil – Infraestrutura de Chaves Públicas Brasileira
IME – Instituto Militar de Engenharia
ITA – Instituto Tecnológico da Aeronáutica
MB – Marinha do Brasil
MD – Ministério da Defesa
NGCSI – Núcleo de Guerra Cibernética e Segurança da Informação
NuPDGI – Núcleo de Pesquisa e Desenvolvimento em Guerra da Informação
OM – Organização Militar
ONU – Organização das Nações Unidas
OTAN – Organização do Tratado do Atlântico Norte
PDN – Política de Defesa Nacional
PEM – Plano Estratégico da Marinha
PLA – People´s Liberation Army
RAM – Revolução em Assuntos Militares
RIP – Regulation of Investigatory Powers
SERPRO – Serviço Federal de Processamento de Dados
SIC – Segurança da Informação e Comunicações
SICGov-2008 – Congresso de Segurança da Informação e Comunicações do Governo Federal
SID – Segurança da Informação Digital
TI – Tecnologia da Informação
VAL – Verificação Automática de Locutor

SUMÁRIO

1 INTRODUÇÃO

O conflito cibernético se caracteriza pelo uso da informática para ações ofensivas a fim de negar, corromper, explorar ou destruir valores do adversário, com o objetivo de através do acesso às redes de computadores de alvos estratégicos enfraquecer o inimigo nas suas defesas convencionais, arruinar sua coesão e diminuir sua capacidade de controle, comunicações, reação e ainda de condutas defensivas, visando restringir a atividade do atacante na infraestrutura de redes.

As ações ofensivas de uma Guerra Cibernética (GC) iniciam-se usando a infraestrutura da internet e, de acordo com seu caráter transnacional, podem ter origem no estado inimigo ou em outros estados em que existam grupos que simpatizem com a causa do inimigo ou ainda que possuam redes que possam ser usadas como escravas num ataque. Isso significa que, em muitas ocasiões, não se pode identificar a origem de um ataque ou seus responsáveis, pois suas ações, vítimas e autores extrapolam as fronteiras físicas estabelecidas entre as nações, dificultando a ação do direito público em virtude da dificuldade de se caracterizar as responsabilidades e os responsáveis.

Neste tipo de conflito, o levantamento de informações nas redes, o roubo de arquivos confidenciais e a identificação de possíveis alvos que possam vir a permitir a conquista do poder sobre um inimigo são importantíssimos. O uso dos recursos computacionais em um ataque tem como intuito, em uma ação de surpresa, impedir ao inimigo do uso do seu potencial de comando e controle, bem como infligir baixas em setores críticos de sua infraestrutura nacional, não permitindo a ele uma reação e causando em sua população incerteza, desconfiança e desapontamento, diante de um inimigo invisível e incógnito.

É claro que todos os setores da infraestrutura nacional dependem das telecomunicações para a operação eficiente e, também é conhecido que o presente nível de dependência da tecnologia da informação (TI) e sistemas baseados em computadores representam, para alguns aspectos da infraestrutura dos serviços críticos, a base da informação para que possam também funcionar. Da mesma forma, a energia elétrica é definitivamente essencial para as facilidades e funções dos equipamentos de todos os serviços críticos, e atualmente também, muito dependente da TI.

Tomando por base esses dados, pode-se inferir como alvos vantajosos para uma guerra cibernética, as redes de computadores e sistemas que gerenciam e controlam os serviços críticos de:

a. Redes de Telecomunicações;

b. Redes de Comando e Controle;

c. Saúde Pública, Emergência e Água potável;

d. Controle de Matriz Energética;

e. Sistema Financeiro.

Estes são somente os cinco alvos que considera-se mais críticos. Pode-se e deve-se, numa análise mais ampla, visando a futura construção de um Plano Nacional de Segurança da Informação, identificar outros sistemas que são críticos ao país e à população, tais como aeroportuários, distribuição de combustíveis, sistemas dos programas assistenciais, judiciário etc.

Atualmente no Brasil, não existe concretamente uma política de segurança das informações que se preocupe com esta modalidade de guerra que é a GC. Não é um assunto apenas de governo e Forças Armadas, mas sim um projeto que envolve todos os setores da sociedade, pois todos são e estão dependentes da infraestrutura das redes de computadores.

Até agora, o governo e a Marinha do Brasil (MB) adotaram poucas ações para identificar quais seriam nossos serviços críticos, suas vulnerabilidades e as medidas que permitem a redução ou a eliminação dessas vulnerabilidades. Nesse tipo de conflito, a preocupação com a segurança das informações passa a ser essencial para fornecer capacidade de lutar, mas também para fornecer a capacidade de se preparar e reagir diante de um possível ataque. Tem que se preocupar com a proteção dos nossos sistemas e também com a formação de recursos humanos para o gerenciamento da segurança da informação sob todos os aspectos.

Um excelente exemplo de atividade cibernética atual é uma reportagem publicada no jornal O Globo do dia 29 de março, em que relata a descoberta de uma operação de espionagem eletrônica em 103 países com pelo menos 1.295 computadores infiltrados:

> Uma vasta operação de espionagem eletrônica infiltrou-se em computadores e roubou documentos de centenas de escritórios governamentais e particulares em todo o mundo, inclusive máquinas do Dalai Lama. [...] A investigação descortinou uma operação mais ampla que, em menos de dois anos, infiltrou-se em pelo menos 1.295 computadores em 103 países, inclusive muitos pertencentes a embaixadas, ministérios das Relações Exteriores e outros departamentos governamentais, assim como os dos centros tibetanos no exílio do Dalai Lama em Índia, Bruxelas, Londres e Nova York. [...] Esta nova operação de espionagem é, de longe, a maior a vir à tona em termos do número de paises afetados (MARKOFF, 2009, p.42).

A reportagem nos aponta claramente a necessidade imperativa de se preparar adequadamente para esta possibilidade real de ataque cibernético, não só aos sistemas da MB, como também aos serviços críticos da infraestrutura nacional.

Dessa forma, este trabalho pretende abordar a situação em que se encontra a MB em matéria de segurança de sistemas e redes, os desafios a enfrentar, as perspectivas para os próximos anos e, a partir daí, procurar apresentar propostas de melhoria para que se possa estar preparado, não apenas para a defesa, mas também para ataques cibernéticos.

2 HISTÓRICO

> "Lutar e vencer todas as batalhas não é a glória suprema; a glória suprema consiste em quebrar a resistência do inimigo sem lutar."
>
> Sun Tzu

Na década de 80, o mundo era um lugar mais simples. A economia parecia saudável, não havia muitos canais de TV e, nos filmes do cinema americano, a maior ameaça à segurança mundial era um adolescente com um computador.

No filme "Jogos de Guerra"[1], um *nerd* desajuizado penetra acidentalmente no sistema de computadores que controlam o arsenal atômico dos Estados Unidos da América (EUA) e coloca o mundo à beira de uma guerra nuclear. Esse filme não ganhou muitos prêmios, mas introduziu o estereótipo do *hacker* precoce. Hoje, será que existe alguma chance de um jovem *hacker*, sozinho, iniciar uma GC? Na opinião de diversos estudiosos, as ações de um único indivíduo com motivos pessoais não podem ser consideradas como GC, embora também possam ser bastante prejudiciais. Para ocorrer uma GC, é necessário o patrocínio do Estado.

Apesar do receio pelo acontecimento de uma guerra computadorizada ser bem antigo, somente quando a internet começou a se popularizar, no início dos anos 90, foi criado o termo "Guerra Cibernética". Em 1993, cientistas do núcleo pensante do Pentágono, através de um documento, intitulado "Cyberwar is Coming!" (a Guerra Cibernética está chegando), argumentam que uma batalha on-line travada entre duas nações seria quase inevitável, entretanto, não seria tão destrutiva como um conflito real.

O livro, "The Science of Military Strategy", publicado pela primeira vez em língua inglesa pelo PLA (People´s Liberation Army) da China em 2001, mostrou que o uso de alta tecnologia não-nuclear pode trazer efeitos estratégicos similares aos das armas nucleares e, ao mesmo tempo, pode evitar o grande risco político, possivelmente causado pelo uso de Informação Digital. Entre outros efeitos, seguindo o advento da Era da informação digital, a Guerra da Informação[2] e a estratégia da Guerra da Informação são duas áreas da ciência que devem receber o máximo de atenção por todos os Países e que devido as suas características,

---

[1] Filme "Jogos de Guerra", produzido em Hollywood, com o ator Matthew Broderick.

[2] Guerra da Informação é um conceito de guerra entendido como sendo o resultado da composição de sete formas de guerra, que traduzem o conceito de proteção, manipulação, degradação e negação da informação, incluindo-se entre elas a GC.

nos coloca em uma situação de estarmos muito mais próximos de uma GC do que de uma Guerra Nuclear.

Atualmente, as implicações de uma GC são, cuidadosamente estudadas pelos serviços de inteligência dos principais Estados democráticos. Um ataque coordenado a alvos da sua infraestrutura crítica como bancos, usinas elétricas, empresas de telefonia e telecomunicações, serviços de transporte e logística, serviços de emergência e segurança pública, agências governamentais, entre outros, seria um pesadelo para todos.

Nos dias de hoje, a maior parte dos principais sistemas de informação, necessários para o funcionamento de qualquer nação moderna, estão interligados por meio de redes de computadores. Desse modo, passou a se desconsiderar limites geográficos. Um pequeno ataque iniciado num sistema bancário em qualquer lugar do planeta, rapidamente poderia se espalhar, não só através do sistema financeiro, mas também, para outros sistemas críticos, podendo levar uma nação inteira à capitulação, sem que seja realizada qualquer manobra política ou militar para isso.

Como exemplo, pode-se citar o ataque cibernético à Estônia, em maio de 2007, que alguns descrevem como a primeira guerra no espaço cibernético.

Logo após, a retirada do centro da capital do país, de uma estátua de bronze que homenageava os soldados soviéticos que combateram na 2ª Guerra Mundial, o governo da Estônia afirmou que seus sites na internet começaram a ser atacados, afetando a vida de toda a pequena nação, uma vez que o país é um dos mais informatizados do mundo. Tudo é feito pela internet, ela é quase tão vital quanto a água potável.

Apesar dos estonianos afirmarem que os ataques foram originados por ordem da Rússia, em retaliação à retirada da estátua, nada foi confirmado e os russos negam qualquer participação (LANDLER E MARKOFF, 2007).

A economia mundial hoje, ainda se recuperando de uma crise, é um excelente alvo para se iniciar qualquer conflito cibernético.

Outro bom exemplo de ataque cibernético foi o que ocorreu em pelo menos 35 sites dos Estados Unidos e da Coréia do Sul, em junho do corrente ano.

Durante uma semana, diversos sites governamentais nos dois países, foram atingidos, entre eles, o da Casa Branca, dos Departamentos de Defesa, de Estado, e do Tesouro, da Bolsa de valores de Nova York e do jornal “Washington Post”, nos EUA e da Presidência, do Ministério da Defesa, do Parlamento, de bancos e do jornal “Chosun Ilbo”, na Coréia do Sul. A maioria dos órgãos conseguiu reagir aos ataques.

O Serviço Nacional de Inteligência da Coréia do Sul afirmou, que:

> Este não é um ataque simples feito por um único *hacker*, mas parece que foi cuidadosamente planejado e executado por uma organização específica ou no nível de um Estado (JORNAL O GLOBO, 2009, p 29).

A agência de espionagem da Coréia do Sul disse que o principal suspeito é a Coréia do Norte. O especialista em Coréia do Norte da Universidade Dongguk, Kim Yong-byun, disse:

> Se for descoberto que a Coréia do Norte está por trás destes ataques, pode significar que ela tentou mostrar para os EUA e para o Sul que possui não só armamento militar, mas também a capacidade cibernética de paralisar agências-chave (JORNAL O GLOBO, 2009, p 29).

Num exercício, chamado de "Cyber Storm II"[3], pôde-se confirmar as sérias conseqüências para a sociedade que podem ser ocasionadas pelas atividades de GC. Nele mais de 2,5 mil pessoas, responderam a cenários que incluíam desde a desativação dos serviços telefônicos e de internet, à ataques a companhias de infraestrutura críticas. Este evento contou com representantes de agências governamentais e mais de 40 empresas privadas de quatro países, inclusive o Brasil.

Um conflito "sem-contato" é um exemplo de situação cada vez mais estudada por estrategistas da guerra assimétrica[4]. Vários exemplos são vistos como totalmente factíveis, incluindo-se a GC contra alvos da população civil e redes militares de comunicações e logística, além da infraestrutura financeira e das operações de inteligência.

Seguindo esta tendência, no dia 17 de dezembro de 2008, foi sancionada a Estratégia Nacional de Defesa (END) (BRASIL, 2008, p 24) que coloca o setor cibernético como estratégico para o Brasil, ao lado dos setores nuclear e espacial.

Neste documento também é definido que:

---

[3] Cyber Storm II, exercício simulado de um grande e coordenado ataque cibernético, dirigido e monitorado a partir de um centro de controle em Washington, EUA, realizado em março de 2008.

[4] Guerra assimétrica é um tipo de guerra que deriva-se de uma força empregando novas capacidades que o oponente não percebe, nem compreende, nem espera: capacidades convencionais que sobrepujem as do adversário ou que representem novos métodos de ataque e defesa.

> "a END é inseparável de Estratégia Nacional de Desenvolvimento. Esta motiva aquela. Aquela fornece escudo para esta. Cada uma reforça as razões da outra. Em ambas, se desperta para a nacionalidade e constrói-se a Nação. Defendido, o Brasil terá como dizer não, quando tiver que dizer não. Terá capacidade para construir seu próprio modelo de desenvolvimento" (END, 2008, p 2).

Nos dias de hoje tem-se definido como realizar a defesa do Mar, Terra e Ar e suas respectivas responsabilidades, porém um novo e importante espaço surge, o espaço cibernético.

Hoje não há regulamentação suficiente em relação ao espaço cibernético, tão pouco a definição de suas responsabilidades. Porém, em seu item 4, a END define como estratégico que "projeto forte de defesa favorece projeto forte de desenvolvimento" (END, 2008, p 2).

Acrescenta que forte é o projeto de desenvolvimento que, sejam quais forem suas demais orientações, seja guiado pelo princípio de independência nacional, alcançada pela capacitação tecnológica autônoma, inclusive no estratégico setor cibernético. "Não é independente quem não tem o domínio das tecnologias sensíveis, tanto para a defesa como para o desenvolvimento" (END, 2008, p 2).

Esta END prima pelo alinhamento ao princípio supracitado e foca nas ações estratégicas relacionadas à defesa do espaço cibernético. Numa destas ações: "Contribuir para o incremento do nível de Segurança Nacional", é definido que:

> o aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do GSI-PR (END, 2008, p 56 e 57).

Juntamente com os cenários de destruição em massa, surgem os cenários de uma GC, onde os filmes "Hollywoodianos" já desenham os mais nefastos cenários. A realidade é que devido a suas características silenciosas, de anonimato e por não ser, em um primeiro momento letal, a GC já é uma realidade em todos os novos conflitos, tais como Guerra do Iraque, invasão da Geórgia pela Rússia e em diversos conflitos menores. Com o crescimento da economia brasileira e com o aumento de importância no cenário mundial, certamente vamos ser alvo deste tipo de ataque "não beligerante", pois o mesmo pode causar sérios danos, sem declaração de guerra, ou mesmo, assunção de responsabilidades.

Outra dura realidade é que as instituições militares e governamentais estão pouco preparadas e coordenadas para reagir a um ataque cibernético em escala nacional e, infelizmente, os nossos adversários políticos, militares ou comerciais estão, cada vez mais, buscando as nossas fraquezas digitais.

A MB e as demais Forças Armadas estão cada vez mais dependentes da informação em suas operações militares. Cresce também a necessidade e a dependência na infraestrutura crítica de dados e esta infraestrutura crítica está cada dia mais interconectada na economia global.

Os avanços tecnológicos do setor comercial dão aos oponentes um incrível poder computacional e uma mobilidade nunca antes vista. No campo de batalha cibernético, muitas táticas e estratégias podem ser importadas dos campos de batalha convencionais. Porém, baseado no fato de que o campo de batalha cibernético é um teatro de operações totalmente criado pelo homem e possui um dinamismo intenso e uma grande capacidade de incorporar avanços tecnológicos existem outros fatores que devem ser analisados que tornam o combate cibernético totalmente diferente de outros campos de batalha:

- É necessário vencer a primeira batalha:

Na guerra convencional, o país que vence a primeira batalha não necessariamente, vence a guerra. Veja Pearl Harbor. Mas com a GC, precisa-se vencer a primeira batalha porque poderá não haver a segunda. O inimigo pode afetar nossas infraestruturas críticas com ataques cibernéticos coordenados, não teremos como montar uma defesa efetiva e seremos forçados a nos render.

- A primeira batalha pode durar alguns segundos:

Ao contrário de Pearl Harbor, ataques cibernéticos são invisíveis. O inimigo penetrou em nossas redes de computadores, atacou nossos sistemas e destruiu ou manipulou nossos dados, antes de detectar-se algo errado. Quando se descobre um ataque cibernético, tem-se que descobrir quem realizou e porquê. Hoje, os tipos de forense computacional podem levar dias ou semanas. Por isso, pode-se perder a guerra.

- A GC pode envolver ações difíceis de serem detectadas por parte de quem se defende:

Muitas pessoas podem realizar GC com maciços ataques tipo negação de serviço (DoS) como os ativistas russos fizeram na Estônia em 2007. Mas a GC não precisa ser realizada em larga escala. Em vez de tomar toda a rede elétrica, um *hacker* poderia entrar em uma subestação que suporte um determinado sistema de defesa aéreo. Da mesma forma que se

tem precisão nos mísseis guiados na guerra convencional, também se tem ataques cibernéticos altamente precisos.

- A missão do inimigo pode ser causar o caos e não destruição:

Tende-se a pensar em um inimigo explodindo edifícios e sistemas de transporte durante a guerra. Mais o objetivo político da GC pode ser gerar o caos entre os cidadãos e não destruir infraestruturas. Por exemplo, o que acontece se o inimigo lançou um ataque cibernético contra o sistema financeiro de um país, e parece que todo o dinheiro foi deslocado de seus bancos? Esse tipo de ataque não exige qualquer bombardeamento de edifícios bancários para gerar o caos.

- Uma das missões do inimigo pode envolver a manipulação de dados e não o roubo ou a destruição:

Durante a Guerra do Golfo, um grupo de *hackers* holandeses propositadamente penetrou em dezenas de sistemas de computadores militares americanos e se ofereceram para prestar ajuda para Saddam Hussein. Quando as violações foram descobertas, os militares americanos tiveram que parar o envio de ordens e verificar se os dados em suas bases estavam corretos e se não tinham sido manipulados pelos *hackers*. Este incidente demonstra como desinformação dentro de sistemas de computadores *hackeados* poderia prejudicar a capacidade de um país para responder um ataque cibernético.

- As redes privadas de dados e voz serão um dos alvos:

A maioria de nossa infraestrutura crítica – energia, transporte, telecomunicações e financeira – é de propriedade privada. As empresas que operam essas redes têm de compreender que eles serão alvos certos na GC, e precisam gastar dinheiro para garantir a segurança em suas redes, sistemas e dados. Esta é uma das razões porque peritos militares recomendam que operadores de infraestruturas críticas se comuniquem com funcionários do governo e criem procedimentos e protocolos antes de serem atacados.

- Quando as redes do setor privado forem atingidas, o Ministério da Defesa (MD) deve estar preparado para assumir o controle da situação:

Há um equívoco em se pensar que os proprietários e operadores das infraestruturas críticas são responsáveis, sozinhos, pela segurança cibernética. Esta perspectiva não vai suportar a GC, especialistas predizem. Assim como os militares são responsáveis pela segurança do espaço aéreo e do solo em torno de uma empresa de energia, também deverá assumir a co-responsabilidade pela segurança cibernética da empresa se um ataque cibernético tiver ocorrido, eles advertem.

- As redes privadas podem ser usadas para lançar um ataque cibernético:

Se as empresas não proverem segurança nas suas redes, os sistemas podem ser tomados por um *botnet* e utilizados em um incidente de GC. Por exemplo, dois terços dos computadores usados para lançar os ataques contra a Estônia estavam dentro dos Estados Unidos, apesar de terem sido controlados por ativistas russos, dizem especialistas. Normalmente, as máquinas utilizadas em um ataque cibernético não são de propriedade do atacante. A maioria das empresas não percebe que estão vulneráveis a terem seus ativos de rede utilizados para a GC.

- A maior ameaça pode ser o inimigo interno:

Uma das maiores vulnerabilidades em redes é do pessoal interno com acesso legítimo a computadores e dados. O mesmo perigo existe na GC. Uma forma de ameaça que pode ocorrer é quando o inimigo rapta um membro da família de um operador de rede e, em seguida, o força a instalar um *malware*. Esse é um motivo para as agências governamentais e empresas privadas que cuidam das infraestruturas críticas terem um adequado controle de segurança com seus empregados.

- A GC é uma modalidade de Guerra:

Olhar a GC separada da guerra tradicional é um erro, ela deve estar vinculada à guerra física, dizem especialistas. Por exemplo, um inimigo pode explodir um prédio no solo que desativa um satélite, que por sua vez desativa o acesso à internet. Em uma GC, ataques à redes, provavelmente serão combinados com ataques físicos. Portanto, a proteção contra GC deve ser considerada como parte de uma estratégia militar mais ampla.

3 A GUERRA CIBERNÉTICA NO MUNDO

Este capítulo pretende ser exemplificativo de alguns dos principais atores no palco da GC. Em geral, algumas visões são comparáveis à dos Estados Unidos, incluindo o Reino Unido, Alemanha, e da Organização do Tratado do Atlântico Norte (OTAN). A França, no entanto, pode ser uma exceção, porque muitos observadores concluíram que um francês pode ver um papel legítimo do ponto de vista econômico da GC na consecução dos objetivos nacionais. O pensamento do russo retrata a GC como um ato de guerra para a qual qualquer resposta, convencionais ou com armas de destruição em massa, é considerada justificada. A China vê a GC como uma legítima forma de guerra assimétrica e está preparando especialistas profissionais em computação para esta tarefa. Estas visões serão apresentadas abaixo de forma mais particular.

3.1 ESTADOS UNIDOS DA AMÉRICA

“Os Estados Unidos não contam com uma política militar clara que defina como as autoridades responderiam a um ataque cibernético contra suas redes de comunicações, energia ou serviços financeiros”, foi alertado durante um painel de cientistas e consultores realizado no dia 29 de abril (CONVERGÊNCIA DIGITAL, 2009).

O Almirante William Owens, antigo chefe do Estado-Maior Conjunto das Forças Armadas norte-americanas, durante coletiva de imprensa, em Washington, declarou que a idéia de "domínio unilateral duradouro do espaço cibernético pelos Estados Unidos não era realista, em parte devido ao baixo custo das tecnologias requeridas para montar um ataque”. Ele também disse que “a idéia de que operações ofensivas desse tipo eram uma opção militar "sem riscos" não estavam corretas” (CONVERGÊNCIA DIGITAL, 2009).

A GC não seria tão mortal quanto a guerra nuclear, ou tão claramente dramática. Mas Mike McConnell, ex-diretor de inteligência nacional, alertou no ano passado que ataques cibernéticos com "capacidade de ameaçar o suprimento monetário americano equivalem a uma arma nuclear" (THE NEW YORK TIMES, 2009).

O General da Força Aérea Kevin Chilton, que dirige o Comando Estratégico, disse que "altos conselheiros do Pentágono não excluem um ataque físico com qualquer força contra um ataque aos Estados Unidos através da internet. Atualmente, as redes militares são analisadas milhares de vezes ao dia, mas a meta dos atacantes parece ser a espionagem, e não tomar as redes críticas" (LAMOS, 2009).

Após inúmeros ataques as redes do Pentágono, com os adversários copiando terabytes de dados militares, os EUA têm aumentado seu foco em bloquear as redes e formular uma doutrina militar para o ciberespaço. Muitos dos ataques as redes nos EUA são lançados de servidores na China, levando funcionários a culpar o governo chinês de financiar os *hackers* para os ataques (LAMOS, 2009).

O Presidente Barack Obama e o Secretário de Defesa Robert M. Gates ainda não decidiram qual o tipo de organização militar irá prosseguir no domínio cibernético. A administração Obama está atualmente revendo a política cibernética dos Estados Unidos. O **p**residente irá criar um novo posto na Casa Branca que terá a responsabilidade de proteger as redes de computadores do país, consideradas críticas.

O governo dos EUA já cogita a criação de um Comando Cibernético, inicialmente como uma divisão do Comando Estratégico. O Pentágono argumenta que as estratégias de defesa e ataque cibernético exigem uma infraestrutura semelhante à montada nos anos 1940 e 1950 em torno do armamento nuclear (ZERO HORA.com, 2009).

3.2 REINO UNIDO

A visão do Reino Unido com relação a GC é semelhante à dos Estados Unidos. Basicamente, considera que a GC se refere a ações que afetam outros sistemas de informação, enquanto defendem os seus próprios sistemas em apoio aos objetivos nacionais.Além disso, o Reino Unido utiliza um sistema jurídico forte, em torno de um grande número de leis, e acredita que grande parte pode ser aplicada às atividades do espaço cibernético. Isto sugere que o Reino Unido vê ataques cibernéticos contra indivíduos e sociedades civis como uma questão criminal que será tratada conforme as leis.

Em 2000, o Regulamento das Competências de Investigação (*Regulation of Investigatory Powers-RIP*), permitiu ao governo do Reino Unido interceptar e ler e-mail, e exigir decriptografia de arquivos pessoais suspeitos. Governo britânico diz que o RIP coloca

"pela primeira vez, técnicas de investigação intrusivas em um documento, e fornece novos poderes para ajudar a combater a ameaça representada pelo aumento da utilização de encriptação, por força penal, e garante que a supervisão independe aos poderes do regulamento" (EUA, 2001).

3.3 RUSSIA

Muitos russos afirmam que o perigo de uma GC está atrás apenas de uma guerra nuclear. Os russos vêem um papel militar para as atividades de GC, onde a competição entre lados opostos tem o objetivo de ganhar e manter informações vantajosas sobre os outros. Isto é realizado por meio de capacidades específicas de tecnologia da informação para afetar sistemas de informação, processos de tomada de decisão, sistemas de comando e controle, e mesmo a população de um adversário. Alguns russos acreditam que, após o começo do conflito, "lutar contra os vírus e outras informações relacionadas ao mesmo, podem ser utilizadas como poderosa força multiplicadora". A Rússia mantém o seu direito de usar armas de destruição em massa como primeiro sinal de força na GC, e em seguida contra o próprio Estado agressor.

Em 12 de setembro de 2000, o Presidente russo Vladimir Putin adotou a Doutrina Russa de Informações de Segurança, que tinha sido aprovada, em 23 de junho, na reunião do Conselho de Segurança Russo. A nova doutrina, ostensivamente, prevê o Governo com um sistema jurídico forte para lidar com crimes de informática e garantindo segurança no espaço cibernético. De certa forma, o que representa uma tentativa parcial por parte da Rússia para lidar com as ameaças cibernéticas, esconde as dificuldades para enfrentar os problemas domésticos e externos (EUA, 2001).

3.4 CHINA

A China está se movendo agressivamente para a GC incorporando em seus militares sua organização, formação e doutrina. De fato, se uma Revolução em Assuntos Militares (RAM) é definida como uma mudança significativa na tecnologia aproveitada para

realizar comparáveis mudanças na doutrina, organização e formação militar, então, talvez a China, de todas as nações, é a que está enfrentando uma verdadeira RAM no espaço cibernético. Além disso, o desenvolvimento da GC na China deve causar preocupação em alguns líderes militares americanos. Como exemplo, o General Eberhart, que liderava o Comando Espacial Americano, em 2001, disse que os militares americanos estão preocupados com as intenções da China e com o desenvolvimento dos seus meios para levar a cabo ataques a redes de computadores (EUA, 2001).

O conceito chinês de GC incorpora pontos de vista muito próprios, sobre como fazer a guerra aos níveis estratégico, operacional e tático.A China também é fortemente influenciada pela ideologia marxista-leninista, quanto a guerra. Muito da sua abordagem tem a ver com uma ênfase no conhecimento do estilo da guerra, e buscando vantagens assimétricas em relação ao adversário. A GC é vista como uma "transformação da guerra mecanizada da era industrial para uma guerra de decisões e controle, uma guerra do conhecimento e uma guerra do intelecto" (EUA, 2001).

A China está formando novas unidades militares compostas de especialistas em computação treinados em inúmeras de universidades, academias e centros de formação. Vários grandes exercícios de formação anual já foram realizados desde 1997. Os chineses têm dado ênfase significativa na formação de pessoas mais jovens para estas funções. A China parece estar preparando um exército de *hackers* para uso em ataques cibernéticos.

Em março, foi divulgado um relatório onde pesquisadores canadenses revelaram a descoberta de uma vasta operação de espionagem eletrônica, na qual, pelo menos 1.295 computadores foram invadidos e infectados em 103 países, inclusive muitos pertencentes a ministérios, embaixadas ou organizações internacionais. Afirma-se que a maioria dos computadores que controlavam o sistema estavam localizados na China, embora não se possa confirmar que o governo chinês esteja envolvido (MARKOFF, 2009).

Os pesquisadores da Universidade de Toronto trabalharam durante 10 meses, a pedido do escritório do Dalai Lama no exílio, que teve vários computadores invadidos (MARKOFF, 2009).

3.5 ALEMANHA

Na maior parte dos casos, a perspectiva alemã em relação a GC é comparável a dos Estados Unidos e do Reino Unido. Ela reconhece como regra legítima a GC ofensiva e

defensiva para consecução dos Objetivos Nacionais. No entanto, a Alemanha tende a ser um pouco mais sistemática do que os Estados Unidos. Para fins de entendimento sobre ameaças cibernéticas e respostas cibernéticas, Estados-nação são considerados separadamente de atores não-estatais (como ativistas políticos, organizações internacionais, e os meios de comunicação) criminosos (crime organizado, *hackers*, etc) e atores individuais (incluindo os fanáticos religiosos e forças especiais).

De duas maneiras, no entanto, o ponto de vista do alemão para GC pode ser diferente. A Alemanha pode incluir a gestão dos meios de comunicação como um elemento da GC. Isto pode acontecer por várias formas: a Alemanha tem avaliado o potencial de dano econômico que pode atingir as empresas alemãs e sua economia; a Alemanha pode ter causado perdas econômicas significativas para a França em mais de um caso envolvendo espionagem industrial no espaço cibernético e a Alemanha pode estar procurando formas de atenuar as consequências de potenciais ataques cibernéticos (EUA, 2001).

3.6 FRANÇA

O francês aparentemente vê a GC como tendo dois elementos principais: o militar e o econômico. O conceito militar prevê um papel limitado para as atividades de GC. Seu conceito militar vê as atividades de GC tendo lugar em grande parte no contexto de conflito de baixa intensidade ou outras operações de não guerra, geralmente realizadas sob a égide da OTAN e das Nações Unidas (muitas vezes sob o controle dos EUA). Neste contexto, aliados não são considerados adversários.

Em contrapartida, o conceito econômico ou civil inclui um leque mais vasto de potenciais aplicações de GC. O francês parece assumir uma perspectiva muito mais ampla e profunda para o conflito na esfera econômica; paz econômica não existe, é muito mais como um ambiente no qual os concorrentes prosseguem num mercado de vantagens de soma-zero. Os franceses não se vêem obrigados a aprovação pela OTAN, ONU, ou Estados Unidos. Na perspectiva para um conflito econômico permite ser tanto aliado como adversário, ao mesmo tempo. Os franceses têm uma escola econômica para a GC.

A França também pode ter uma perspectiva diferente para a monitoração dos seus cidadãos no espaço cibernético. Relatórios que vêm a tona dizem que os franceses têm a sua

própria versão do Echelon[5] (declaradamente um esforço dos Estados Unidos - não oficialmente confirmado - destinado a interceptar praticamente todas as comunicações globais), Frenchelon, como alguns o chamam, é declaradamente utilizado para acompanhar e analisar as comunicações francesas, especialmente na região de Paris (EUA, 2001).

3.7 PALESTINA E ISRAEL

Em 1999, começou o conflito entre *hackers* palestinos e israelenses, mas aumentou drasticamente em setembro de 2000, quando jovens *hackers* israelenses realizaram ataques constantes e bloquearam seis sites do Hezbollah e do Hamas no Líbano e também da Autoridade Nacional Palestina. Este evento que parecia de pouca importância, gerou uma GC. Os palestinos clamaram por uma Guerra Santa Cibernética. No início, foram atacados sites do governo e do setor financeiro de Israel, incluindo os serviços de internet, que quase foi colocado totalmente fora do ar.

Até início de 2002, o conflito já havia desconfigurado quase 200 sites israelenses e um pouco menos de 50 palestinos, incluindo até um site americano.

A GC Palestina-Israel nunca causou séria ameaça física a qualquer uma das nações e seus efeitos a longo prazo podem ser considerados irrelevantes. Entretanto, os ensinamentos colhidos durante o conflito, podem servir de exemplo para futuros conflitos cibernéticos (ALLEN E DEMCHAK, 2004).

3.8 ORGANIZAÇÃO DO TRATADO DO ATLÂNTICO NORTE

De acordo com informação publicada no jornal britânico "The Guardian", do dia 7 de março de 2008, a OTAN passou a considerar a GC um perigo tão grande quanto o de um ataque com mísseis.

[5] Echelon é um sistema de interceptação de comunicações com duas características muito importantes: a capacidade praticamente global de vigilância e o sistema funciona a nível mundial graças a uma cooperação entre vários países (Reino Unido, EUA, Canadá, Austrália e Nova Zelândia).

Ainda segundo a reportagem, o encarregado pela defesa da organização contra ataques baseados em computadores, Suleyman Anil, afirmou que "a luta cibernética está agora num nível de prioridade tão grande quanto nossas defesas contra mísseis estratégicos. Nós temos visto cada vez mais ataques e não achamos que eles vão parar" (THE GUARDIAN, 2008).

O terrorismo cibernético[6] está entre as principais ameaças temidas pela OTAN, pois apesar de alertas sobre esse perigo existirem desde o começo do uso da internet, somente nos últimos anos o assunto passou a ser discutido pelos Estados.

3.9 ATORES NÃO-ESTATAIS

Há indícios consideráveis de que alguns atores não-estatais e forças anti-governo utilizam o espaço cibernético como uma outra ferramenta para lutar contra diferentes nações. Como exemplo, o movimento Zapatista no México usa a Internet para obter apoio para sua causa. A milícia Talibã do Afeganistão - um movimento que controla a maior parte do Afeganistão - mantém um site com uma gama de materiais e até mesmo solicita contribuições a partir do estrangeiro. Do mesmo modo, existe um sitio na internet do Movimento de Libertação Nacional Basco[7] (EUA, 2001).

[6] Terrorismo cibernético é realizado através de tentativas de derrubar redes de comunicação on-line ou de usar a internet para atacar instituições oficiais.
[7] Movimento de Libertação Nacional Basco é um movimento separatista na região entre a Espanha e a França.

4 A LEGISLAÇÃO NO BRASIL

Neste capítulo pretendemos apresentar o que existe na legislação do Governo Federal e da MB, e que já pode ser usada para se apresentar propostas para o estabelecimento de doutrinas a serem seguidas na GC.

4.1 GOVERNO FEDERAL

A Política de Defesa Nacional (PDN) foi aprovada em 30 de junho de 2005, pelo Decreto nº 5.484, em seu texto, no capítulo 6. Orientações Estratégicas, item 6.19, já orienta nossa política de defesa sobre a necessidade de se melhorar nossa segurança contra possível ataque cibernético: "para minimizar os danos de possível ataque cibernético, é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento" (PDN, 2005, p.8).

Em 17 de dezembro de 2008, foi aprovada a END, ela está centrada em ações estratégicas de médio e longo prazo e tem por objetivo modernizar a estrutura nacional de defesa, atuando em três eixos principais: reestruturação da indústria brasileira de material de defesa, reorganização das Forças Armadas e política de composição dos efetivos das Forças Armadas.

A END está dividida em duas partes: Parte 1- Formulação sistemática e Parte 2- Medidas de Implementação. Na parte 1, são definidos os três setores estratégicos essenciais para a defesa nacional: o espacial, o cibernético e o nuclear.

No setor cibernético é dito:

> 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 (END, 2008, p.24).

Pode-se notar na END que o governo coloca o setor cibernético como primordial para a Defesa Nacional.

4.2 MARINHA DO BRASIL

O Plano Estratégico da Marinha (PEM) foi aprovado em 13 de março de 2008, na sua 2ª revisão. Em seu capítulo 6, são definidos os objetivos navais da MB, um destes objetivos aborda a necessidade de manter a segurança de nossos sistemas digitais de tecnologia da informação (TI) e de comunicações no Estado da Arte, a fim de se evitar ataques cibernéticos. No capítulo 11, em suas Diretrizes para o Planejamento Naval (DIPNAV), no setor de Ciência e Tecnologia e TI, é dito: "estabelecer ações para garantia do uso da informação de interesse da MB e negar a sua utilização de forma contrária". Nesta DIPNAV, está implícito a necessidade de manter a segurança de nossos sistemas para garantir o uso da informação pela MB.

A Diretoria Geral do Material da Marinha (DGMM), possui publicações que tratam de segurança de sistemas digitais, segurança criptológica e de comunicações na MB. São elas:

DGMM-0520 – Normas para a Gestão de Segurança das Informações Digitais em Redes Locais (2004).

DGMM-0510 – Normas para Criptologia da Marinha (2000).

DGMM-0500 – Manual de Comunicações da Marinha (2006).

Na DGMM-0510, em seu capítulo 1, são enunciados alguns conceitos básicos, tais como:

> Criptologia – é a ciência que trata tanto dos princípios, meios e recursos não só empregados para emprestar às mensagens portadoras de conhecimentos sigilosos um relativo grau de segurança, como também para revelar o verdadeiro significado de uma linguagem ininteligível ou imperceptível. Destina-se a negar ao oponente o acesso a tais conhecimentos, ainda que consiga interceptar a mensagem (DGMM-0510 1ª revisão, 2000, p.1-1).

A criptologia se divide em:

> a) Criptotecnia – consiste em aplicar às linguagens faladas ou escritas um tratamento que torna seus textos ininteligíveis, representados por criptogramas,

> mediante modificações na natureza ou na posição de seus componentes, segundo convenções preestabelecidas; a forma inteligível é restaurada pela aplicação inversa, ou seja, convertendo os criptogramas em textos claros;
>
> b) Esteganotecnia – consiste no uso de recursos capazes de dar aos textos das mensagens uma forma imperceptível aos sentidos humanos da visão e audição. Com a utilização de tais recursos se pretende impedir que o oponente conheça o conteúdo dessas mensagens, mesmo quando por ele interceptadas; e
>
> c) Criptoanálise – instrumento necessário para se descobrir (ou "quebrar") o conteúdo de criptogramas, transformando-os em texto claro, sem o prévio conhecimento das operações que os produziram (DGMM-0510 1ª revisão, 2000, p.1-1 e 1-2).

Esses conceitos são importantes para o entendimento do tema segurança da informação que será tratado mais adiante, e também, quando nos prepara-se para ações defensivas e ofensivas na GC.

O Estado Maior da Armada aprovou em 18 de dezembro de 2007, a 1ª revisão da Doutrina de Tecnologia da Informação da Marinha (EMA-416), nesta norma constam vários conceitos e definições, como: Forense Computacional, Governança de TI, Guerra Centrada em Redes (GCR), segurança da informação e segurança da informação digital (SID).

Também é definido GC, como sendo;

> ações ofensivas e defensivas destinadas a explorar, danificar ou destruir informações digitais, ou negar o acesso às suas informações. Tais ações utilizam-se de sistemas de informação e de redes de computadores (EMA-416 1ª revisão, 2007, p.1-3).

E Segurança Cibernética, como:

> é a segurança do espaço cibernético, ou seja, a segurança das redes de computadores e de seus equipamentos de conectividade correlatos (EMA-416 1ª revisão, 2007, p 1-4).

Em outro capítulo trata das ações de proteção dos sistemas de informação digital, que englobam as seguintes atividades:

> **a) planejamento**: visam à preparação para prevenção de possíveis ameaças ou riscos às informações digitais;
>
> **b) histórico:** registro de ocorrências que possam vir a ocorrer no ambiente onde se processam ou trafegam informações digitais;

> **c) análise:** auditorias e avaliações de vulnerabilidades, de riscos ou de incidentes que possam ocorrer no ambiente onde se processam ou trafegam informações digitais;
>
> **d) correção**: correções e reparos no ambiente onde se processam ou trafegam informa-ções digitais, para pronto restabelecimento de suas condições operacionais e dos requisitos básicos de SID; e
>
> **e) adestramento:** visam adestrar o pessoal quanto aos documentos, aos procedimentos e às demais instruções de SID. (EMA-416 1ª revisão, 2007, p 5-1 e 5-2).

A norma também aborda a conscientização do pessoal e coloca como fatores importantes para a SID, a mentalidade de segurança e o adestramento.

Pelo que foi mostrado pode-se avaliar a necessidade da apresentação de propostas para criação de doutrinas que permitirão a MB estar preparada para se defender contra possíveis ataques cibernéticos.

5 A SITUAÇÃO NO GOVERNO E FORÇAS SINGULARES

Este capítulo abordará como órgãos do Governo Federal e as demais Forças Armadas estão atuando na área de GC.

5.1 GABINETE DE SEGURANÇA INSTITUCIONAL-PR

O Gabinete de Segurança Institucional (GSI-PR) é um órgão subordinado diretamente à Presidência da República que possui em sua estrutura organizacional, uma secretaria-executiva com um Departamento de Segurança da Informação e das Comunicações (DSIC).

Este departamento possui tarefas que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da Informação e das Comunicações, no âmbito do governo federal.

O GSI-PR atua em 37 ministérios, com mais de 6.000 entidades governamentais, 320 redes relevantes, onde trabalham mais de 900.000 servidores federais. Além disso no Brasil, 40% da população possui computador, 38% acessam a internet, existem 8,1 milhões de conexões em banda larga e 27,3 milhões de usuários bancários de internet (MANDARINO, 2008).

Dentre as ações realizadas estão:

- a assinatura de acordos internacionais com Portugal, Espanha, Rússia e França e em fase de negociação com Luxemburgo, Israel, Itália e EUA, que tratam de credenciamento de segurança de pessoas e organizações e troca de informações sigilosas;
- a criação de várias Normas sobre segurança da informação;
- a capacitação de recursos humanos;
- criação de Centros de Tratamento de Incidentes em Redes, na Administração Pública Federal (APF); e
- atuação na área da segurança cibernética.

O Decreto nº 3.505 de 23 de junho de 2000, instituiu a Política de Segurança da Informação na APF e o Comitê Gestor de Segurança da Informação (CGSI), integrado por representantes de diversos Ministérios e coordenado pelo GSI-PR.

A estratégia usada para capacitação de recursos humanos na APF é tentar sensibilizar todos os servidores, conscientizar 10%, capacitar 1% e especializar 0,1% em segurança da informação e comunicações (SIC) (MANDARINO, 2008).

Em outubro de 2008, foi realizado o Congresso de Segurança da Informação e Comunicações do Governo Federal (SICGov-2008) com os objetivos de sensibilizar autoridades de alto escalão do governo brasileiro e discutir temas de interesse para o aprimoramento da SIC na APF. Participaram do evento 420 pessoas.

Foram identificados diversos problemas a serem atacados (MANDARINO, 2008):

- ausência de uma cultura padronizada em segurança da informação;
- ausência de coordenação nas ações conjuntas e do estabelecimento de padrões e normas nacionais;
- ausência de legislação adequada;
- indefinição das Fronteiras (Redes de Comunicações Transnacionais);
- dificuldade em estabelecer princípios de jurisdição territorial; e
- necessidade emergente de repensar e rever o conceito de segurança das infraestruturas críticas – em especial da segurança cibernética.

O GSI-PR conta com um número reduzido de servidores e com um orçamento anual ainda pequeno para poder realizar todas as ações necessárias para garantir a integridade nos sistemas da APF.

O estabelecimento de uma infraestrutura nacional com atuação no ramo de segurança da informação deve ser composta por diferentes setores do governo, como o GSI-PR, bem como por diversas organizações da iniciativa privada, o que proporcionaria um maior grau de integração nacional no assunto, e atenderia a diferentes expectativas.

5.2 EXÉRCITO BRASILEIRO

De acordo com o ofício nº 178/2 SCh/SI-3, de 15 de abril de 2004, do Estado Maior do Exército, encaminhado ao MD, a situação dos Projetos de Guerra Cibernética e Segurança da Informação no âmbito daquela Força, encontrava-se da seguinte forma:

Em termos de vulnerabilidades existentes, eram as seguintes:

1) Diversos sistemas de uso corporativo no Exército Brasileiro (EB), relativos à gestão de pessoal e financeira, são vulneráveis a acessos por pessoas não autorizadas, utilizando-se apenas técnicas e ferramentas livremente disponíveis na Internet. Alguns desses sistemas são operados pelo Serviço Federal de Processamento de Dados (SERPRO) e atendem a toda a APF. Nesses sistemas, verificou-se que é possível, no mínimo, a obtenção de informações confidenciais ou sensíveis.

2) Devido às restrições de ordem legal, não são realizados testes visando à verificação da possibilidade de se alterar informações armazenadas nesses sistemas. Entretanto, em alguns desses sistemas, já é possível especular com razoável probabilidade de acerto que a alteração de dados é possível.

3) A falta de embasamento legal, para evitar que atividades decorrentes da utilização de técnicas, táticas e procedimentos, típicos de GC sejam caracterizadas como ações criminosas.

4) De forma análoga aos sistemas corporativos em uso no Exército, e pela experiência das vulnerabilidades encontradas em estudos semelhantes conduzidos pelo Departamento de Defesa norte-americano, acredita-se que diversos sistemas de comando e controle da infraestrutura crítica nacional sejam vulneráveis a operações de GC.

Em relação, às necessidades e carências para a efetivação dos projetos em desenvolvimento, eram as seguintes:

- **OBJETIVO 1:** Obter soluções criptográficas, em *software* e *hardware,* próprias do Exército, visando à preservação do sigilo das informações transmitidas ou armazenadas em meios de TI.
    - **1) Ação 1.1**: Obter, por desenvolvimento próprio, algoritmos criptográficos para uso no EB.
    - **2) Ação 1.2:** Implementar, em *software* e *hardware*, os algoritmos obtidos.

- **OBJETIVO 2:** Estruturar o Núcleo de Pesquisa e Desenvolvimento em Guerra da Informação (NuPDGI), constituído de recursos humanos e materiais destinados ao cumprimento das seguintes atribuições:
    - acompanhamento permanente da evolução das técnicas que visam ao comprometimento da segurança de redes de comunicações e sistemas computacionais;
    - prestar assessoramento às organizações militares, aos órgãos governamentais e às empresas que operem redes e sistemas computacionais de interesse para a defesa nacional, quanto aos procedimentos e ferramentas a serem adotados para a defesa contra ataques cibernéticos;
    - colaborar na formação de recursos humanos na área de guerra de informação, capazes de atuar em proveito de operações de inteligência e contra-inteligência;
    - desenvolver ferramentas de hardware e/ou software visando à proteção das redes e sistemas computacionais contra ações adversas de guerra de informação;

- desenvolver ferramentas de hardware e/ou software visando ao ataque cibernético de redes e sistemas computacionais de forças adversas; e
- atuar, quando determinado, como força adversa simulada, realizando tentativas de ataques cibernéticos contra redes e sistemas computacionais da infraestrutura de interesse da defesa nacional.
    1) **Ação 2.1:** Capacitar integrantes do NuPDGI em segurança da informação, mediante obtenção de certificação nos principais sistemas e equipamentos em uso no EB e em gestão da segurança segundo as normas NBR/ISO 17799.
    2) **Ação 2.2:** Avaliar técnicas e ferramentas de proteção de redes e sistemas computacionais.
    3) **Ação 2.3:** Analisar técnicas e ferramentas de ataque cibernético.
    4) **Ação 2.4:** Desenvolver técnicas e ferramentas de ataque cibernético.
    5) **Ação 2.5:** Especializar oficiais engenheiros de telemática / computação /comunicações / eletrônica, da arma de comunicações e da área de inteligência em técnicas de guerra de informação.
    6) **Ação 2.6:** Especializar oficiais engenheiros de telemática /computação /comunicações / eletrônica, e oficiais das armas, quadros e serviços portadores de diploma de curso de nível superior nas áreas de computação, engenharia elétrica ou de matemática para desempenhar atividades de planejamento, direção, assessoria e execução na área de segurança da informação;
    7) **Ação 2.7:** Perpetrar, com autorização das autoridades competentes, ataques cibernéticos "não-destrutivos" contra redes e sistemas computacionais de interesse da defesa nacional, atuando como força adversa simulada (*red team*);
- **OBJETIVO 3:** Desenvolvimento de processos alternativos de autenticação de usuários de sistemas de informação.
    1) **Ação 3.1:** Aperfeiçoar sistema de verificação automática de locutor (VAL) desenvolvido no Instituto Militar de Engenharia (IME).
    2) **Ação 3.2:** Incorporação do sistema VAL em um sistema de autenticação de usuário de sistema de informação.

Desde então, pouco foi realizado para se reduzir as vulnerabilidades e atingir os objetivos elencados, acima. Os motivos não se sabe ao certo, mas entre eles devem estar os reduzidos recursos recebidos durante os anos, para manutenção das Forças.

O EB possui um setor que atua na área de GC, no Centro de Desenvolvimento de Software, localizado em Brasília.

Em 31 de janeiro de 2007, através da Portaria nº 063 do Departamento de Ciência e Tecnologia (DCT), foi criado o Estágio Setorial de Guerra Cibernética, que tem como objetivo: "habilitar os oficiais intermediários e subalternos de carreira para empregar judiciosamente técnicas e ferramentas de GC, visando a preservação do sigilo das informações transmitidas ou armazenadas em meios que utilizam a tecnologia da informação".

Cada curso matricula no máximo 10 alunos, entretanto, não se têm informação de quantos alunos cursaram até este ano.

5.3 FORÇA AÉREA BRASILEIRA

De acordo com o ofício nº 3/6SC1, de 15 de abril de 2004, do Estado Maior da Aeronáutica, encaminhado ao MD, os projetos previstos ou que estavam em execução, eram os seguintes:

- implantação de uma estrutura de gerenciamento para coordenar a implantação da segurança das informações dentro das organizações;
- capacitação de recursos humanos na área de segurança da informação;
- gerenciamento Eletrônico de Documentos – GED, que deverá estar de acordo com a Infraestrutura de Chaves Públicas Brasileira (ICP – Brasil);
- instalação e manutenção de salas-cofre;
- telefone seguro;
- celular seguro;
- certificação digital;
- ativação de grupos de resposta a incidentes de segurança;
- capacitação de recursos humanos na área de segurança da informação;
- adequação das normas para aquisição, desenvolvimento e manutenção dos projetos e sistemas;
- aquisição ou desenvolvimento de ferramentas de software capazes de identificar, alertar e responder automaticamente ao surgimento de problemas importantes; e
- estabelecimento, de um grupo com capacitação específica para executar ações ofensivas contra um inimigo declarado.

Da mesma forma que no EB, pouco se evoluiu nesses projetos, em parte também, devido a falta de recursos alocados. A Força Aérea Brasileira (FAB) possui um setor de GC no Instituto Tecnológico da Aeronáutica (ITA), localizado em São José dos Campos.

6 DESAFIOS

Para ter vantagens em um cenário de crise no espaço cibernético ou onde o espaço cibernético possa ser utilizado em conjunto com outras ações nos espaços convencionais, a MB deve estabelecer procedimentos de defesa, ataque e alarme cibernético. Para tanto, a Marinha deve entender os riscos do espaço cibernético e criar uma doutrina que defina mecanismos para operações cibernéticas, como nas operações navais. Em uma visão mais holística do complexo problema do combate cibernético, os procedimentos criados devem atender a, basicamente, três demandas:

a. reduzir os benefícios que grupos contrários ao Estado brasileiro, criminosos, terroristas possam encontrar no espaço cibernético para perpetrar suas atividades maliciosas que atinjam a infraestrutura crítica da Marinha;

b. se beneficiar de oportunidades no espaço cibernético melhorando a segurança das redes de comunicações da Marinha e aumentando a resistência a um possível ataque; e

c. melhorar o conhecimento e a capacitação dos técnicos e dos decisores e dar às autoridades o poder de decisão diante de situações de crise ou conflito no espaço cibernético.

Doutrinariamente, também é imperioso definir os limites das ações e da responsabilidade das três forças e do MD.

Desta forma, o propósito das atividades de GC é reduzir o risco e explorar as oportunidades, melhorando o conhecimento, a capacitação e o poder de decisão, a fim de garantir a vantagem estratégica da Marinha e contribuir para a vantagem estratégica do Brasil no espaço cibernético.

Para garantir a vantagem estratégica da MB no espaço cibernético e contribuir para a vantagem do Brasil no mesmo espaço, as seguintes tarefas devem ser perpetradas:

a. reduzir a ameaça de operações cibernéticas adversárias por meio da redução da motivação e da capacidade do oponente de atuar no espaço cibernético administrado pela Marinha e pelo Governo Brasileiro;

b. reduzir as vulnerabilidades do espaço cibernético de interesse da MB ou do Estado Brasileiro;

c. reduzir o impacto das operações cibernéticas no espaço cibernético brasileiro ou controlado pela MB.

6.1. VULNERABILIDADES DA MB ANTE ÀS AMEAÇAS CIBERNÉTICAS

Em relação às ameaças cibernéticas, o conjunto de vulnerabilidades que se encontra na MB e seus sistemas de informação e controle é decorrente de diversos fatores, dos quais cabe destacar:

- falta de conscientização quanto ao problema, suas ameaças e riscos;

- escassez de incentivos à pesquisa e desenvolvimento de tecnologia própria nacional em dispositivos e procedimentos voltados à Segurança da Informação;

- escassez de suporte em pesquisa acadêmica na área de defesa cibernética, incluindo pesquisa nacional em criptologia;

- utilização de sistemas totalmente importados e com tecnologia proprietária tipo "caixa-preta";

- falhas de segurança nos protocolos, sistemas operacionais e aplicativos utilizados e que não são devidamente corrigidos;

- privatização total, sob o controle de empresas estrangeiras, da infraestrutura crítica nacional de telecomunicações;

- inexistência de políticas, normas e certificações voltadas à defesa ante as ameaças de GC; e

- inexistência de procedimentos de segurança e planos de contingência devidamente testados, mostrando que a cultura de segurança é heterogênea e incipiente.

Dentro do contexto nacional, a MB deve garantir que as suas redes de comando e controle, seus sistemas de informação e, consequentemente, suas respectivas redes de comunicações, sigam procedimentos e normas de segurança estabelecidos, como também sejam testadas quanto à manutenção dos requisitos básicos de Segurança da Informação (sigilo, integridade, disponibilidade e autenticidade). A falta de procedimentos e normas estabelecidas não permite a realização de testes periódicos das redes e seus sistemas integrantes, como também dificulta a realização de análises de vulnerabilidades e riscos iminentes.

Além disso, não está formalizada uma política central para desenvolvimento de dispositivos, procedimentos, formação e manutenção de pessoal voltado especificamente à área de Segurança da Informação, abrangendo, principalmente, as áreas de segurança de redes e criptologia. Todas estas vulnerabilidades são decorrentes do próprio fato de não se conhecer a si próprio, o que pode ser proporcionado a partir de auditorias periódicas e regulares de segurança. Contudo, estas auditorias específicas requerem o estabelecimento de normas e procedimentos a serem seguidos por todos aqueles que acessam algum sistema de propriedade da MB. A não existência de normas e procedimentos torna os usuários impossibilitados de criar uma cultura de segurança e de executar suas tarefas de forma orientada, aumentando exponencialmente o conjunto de vulnerabilidades.

No caso de proteção e defesa do Estado Brasileiro em relação a ameaças cibernéticas, sugere-se também uma prioridade diferenciada em relação aos alvos preferenciais que podem ser penetrados e desvirtuados para provocar caos na sociedade.

As novas tecnologias que são criadas para a realização de operações militares, também criam novas vulnerabilidades de Segurança Nacional e novas questões de Política de Segurança Nacional, que devem ser atacadas pelo governo:

- possibilidade de se realizar o controle de armas cibernéticas;
- necessidade de cooperação internacional para a defesa contra ataques cibernéticos;
- considerar que as atividades centradas em rede podem atingir nações amigas ou neutras no conflito;
- necessidade de ajuda da população civil que deve estar treinada contra ataques cibernéticos; e
- possível acusações de crimes de guerra se a ofensiva militar através de armas cibernéticas causar severos danos a sistemas computacionais críticos de empresas civis ou de sistemas de outros países não beligerantes.

6.2. ACORDOS INTERNACIONAIS DE COOPERAÇÃO NA ÁREA DE GUERRA CIBERNÉTICA

Muitos países tratam o espaço cibernético como um novo teatro de operações e as atividades de GC como estratégia de Estado, incluindo a formação específica de grupos de

“guerreiros cibernéticos” como tropa de elite. Destes países, cabe destacar os avanços e casos reais publicados por especialistas chineses e russos, bem como os respectivos apoios governamentais para execução das atividades de GC. De forma a assessorar os assuntos de GC que possam fazer parte de algum acordo de cooperação internacional, sugere-se a abordagem e cooperação nos seguintes temas:

- conhecimento da estrutura oficial ou de organização governamental voltada às atividades de GC;

- conhecimento da doutrina básica para as atividades de GC;

- conhecimento sobre procedimentos e normas para as atividades de GC e segurança da informação;

- conhecimento da formação e recrutamento de pessoal, civil ou militar, para atuar nas áreas de GC, segurança da informação e segurança de redes de comunicações;

- possibilidade de realização de visitas, cursos ou estágios por brasileiros na organização voltada à atividades de GC e segurança da informação, principalmente na área de defesa de redes de comunicações e auditorias de segurança da informação; e

- possibilidade de intercâmbios ou estágios por brasileiros em atividades de criptologia e criptoanálise.

7 PERSPECTIVAS PARA A PRÓXIMA DÉCADA

Atualmente, a MB não possui doutrinas específicas para a GC. A Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) foi criada a partir de um estudo realizado por um grupo de trabalho, com o objetivo de centralizar em uma única Organização Militar (OM) da MB, todos os assuntos que envolvessem a TI, que se encontrava espalhada por várias OM.

A DCTIM foi criada em 16 de janeiro de 2008, através de uma reorganização da Diretoria de Telecomunicações da Marinha (DTM), para poder realizar todas as novas atribuições relacionadas à TI. A Diretoria possue uma Superintendência de TI, a qual está subordinado o Departamento de Segurança da Informação Digital, com três divisões, a Divisão de Auditorias de SID, a Divisão de Projetos de SID e a Divisão de Criptologia, que possuem, dentre outras tarefas, o estabelecimento de doutrinas, normas e procedimentos na área de Segurança da Informação, incluindo a GC.

O Centro de Tecnologia da Informação da Marinha (CTIM), criado em 16 de abril de 2008, é subordinado diretamente à DCTIM, e também possui um Departamento de Segurança da Informação Digital, com quatro divisões, sendo uma delas, a Divisão de GC. Entretanto, esta divisão ainda não esta operando, devido a falta de pessoal qualificado na área. O CTIM é a OM de execução, que dará a realimentação da monitoração das redes de comunicações utilizadas pela MB sobre possíveis ataques.

A DCTIM terá que capacitar o CTIM, para que possa executar as atividades de GC, de monitoramento, configuração das redes e centralização do gerenciamento das redes.

No Comando de Operações Navais (CON), existe uma Divisão de GC, dentro da Subchefia de Inteligência, que ficará responsável pela GC no campo operacional, como já realiza com a guerra convencional.

No EMA, na Subchefia de Comando e Controle, existe a Divisão de Comunicações e TI, que tratará da GC no campo estratégico.

Para que as perspectivas para os próximos anos sejam alvissareiras, todas essas OM, com a participação de todos os servidores civis e militares da MB, do mais moderno ao mais antigo, devem trabalhar com um único pensamento, reduzir as nossas vulnerabilidades ante as ameaças cibernéticas, para que se possa enfrentar a possibilidade crescente de sermos atingidos por uma GC.

O primeiro passo já foi dado, com a criação da DCTIM e do CTIM, agora a MB têm que proporcionar os meios materiais e humanos para o avanço nessa área.

Outro passo importante, é a integração com as Forças Singulares e com o MD. Através do compartilhamento das atuais atividades com as demais Forças, podemos alcançar resultados muito melhores.

Seguem-se algumas sugestões para essa possibilidade de integração entre as Forças e o MD:

- entende-se como necessária a integração das Forças e do MD, nos trabalhos de pesquisa e desenvolvimento de projetos nas áreas de criptologia, segurança da informação e GC. O assunto cresce de importância à medida que aumentam as vulnerabilidades decorrentes da expansão do processo de informatização, tanto no ambiente militar como no civil.

- realizar estudos para o desenvolvimento de uma doutrina de GC, aproveitando o conhecimento das três Forças, já existente nessa área, com vistas à formação e capacitação de recursos humanos.

- é desejável, a exemplo das atividades de sistemas estratégicos de guerra eletrônica e de inteligência, que coletam informações em tempo de paz para emprego em caso de conflito, a estruturação de uma Força Operacional para, em tempo de paz, coletar dados sobre vulnerabilidades de sistemas de forças adversas, contribuindo para a superioridade informacional de nossas forças.

- há necessidade de novos instrumentos legais que legitimem as atividades nessa área, visando ao levantamento de vulnerabilidades, sem incorrer em prática de crime.

- as ações na área de GC, exceto aquelas específicas, tendo como alvos os sistemas de C2 militares, são de natureza estratégica, isto é, pertencem à chamada infraestrutura crítica nacional e sua defesa deveria estar a cargo de uma "Força Combinada", com integrantes das três Forças, numa unidade operacional de GC.

A nossa estratégia de atuação contra as atividades de GC pode contemplar ações tanto defensivas quanto ofensivas. Deve-se estar preparado para realizar ataques cibernéticos, caso sejam necessários para a defesa de nossos sistemas críticos.

Dessa forma, vislumbram-se cinco etapas básicas para se atingir níveis aceitáveis de segurança contra atividades de GC e de segurança da informação:

1ª ETAPA: Criação de um Sistema de Segurança contra atividades de GC e de Segurança da Informação, com as seguintes tarefas:

- estabelecer uma arquitetura para responder às atividades de GC contra os sistemas críticos da MB;
- prover o desenvolvimento de táticas e assessoramento de análise estratégica das nossas vulnerabilidades ante atividades de GC;
- incentivar o desenvolvimento da capacidade do setor privado para fazer frente a ameaça de atividades de GC, para atuarem como contingência, aos nossos sistemas;
- disseminar os níveis de alarmes adequados frente à ameaça de atividades de GC e de comprometimento de Segurança da Informação;
- implantar o gerenciamento das redes para o caso de incidente nacional;
- coordenar planos de operacionalidade básica da arquitetura dos sistemas críticos e planos contingentes para os casos de incidente nacional;
- elaborar planos de exercício de segurança contra atividades de GC e de Segurança da Informação; e
- disseminar informações ao setor público-privado que envolvam ameaças a vulnerabilidades nacionais conhecidas.

2ª ETAPA: Estabelecimento de um Programa de redução de vulnerabilidades identificadas e proteção contra ameaças de atividades de GC e Segurança da Informação, com as seguintes metas:

- proposição de artifícios legais para prevenir e punir ataques cibernéticos em fórum nacional;
- criação de processos para assegurar que os setores apontados como vulnerabilidades estejam conscientes das conseqüências das ameaças potenciais;
- redução ou eliminação das vulnerabilidades dos *software* e aplicativos utilizados nos sistemas;
- priorização das ações de segurança contra atividades de GC e de Segurança da Informação e desenvolvimento de uma agenda própria.

3ª ETAPA: Estabelecimento de um Programa de capacitação e treinamento de segurança contra atividades de GC e de Segurança da Informação, com a seguinte meta:

- continuidade em capacitação, treinamento e educação de todos os setores, na MB, para atender às necessidades de Segurança contra atividades de GC e de Segurança da Informação.

4ª ETAPA: Estabelecimento da segurança contra atividades de GC e de Segurança da Informação da MB, com as seguintes metas:

- estabelecimento de área de segurança para utilização de rede de comunicações de dados local da MB; e
- incentivo aos Estados e Municípios para que adotem um Programa de Segurança da Informação em consonância com o da MB.

5ª ETAPA: Participação de acordos de cooperação com outros países em Sistemas Internacionais de segurança contra atividades de GC e de Segurança da Informação.

A participação da MB e também do País em acordos de cooperação internacional certamente contribuirá, por meio da troca de informações, para o aperfeiçoamento de nossa estrutura organizacional, das normas elaboradas e das técnicas empregadas. Além disso, uma participação ativa pode servir como fator dissuasório e de confiança mútua.

Para que o cumprimento dessas etapas sugeridas tenha maior êxito, será importante a criação de um Núcleo/Departamento inserido na estrutura do Estado Maior de Defesa (EMD)/MD, que será responsável especificamente por:

1. desenvolver um plano Estratégico a nível nacional para assegurar a integridade da infraestrutura crítica do País e segurança da informação;
2. prover o Gerenciamento de Crise em resposta a ocorrência de atividades de GC (prover os principais meios para facilitar e coordenar o impacto de um ataque, a investigação da ameaça e a monitoração dos trabalhos de restabelecimento operacional);
3. prover assessoria ao setor privado e outras entidades governamentais/não-governamentais, atinentes a implementação de planos de restabelecimento de operacionalidade aceitável da infraestrutura crítica do País, decorrentes de atividades de GC; e

4. coordenar com outras agências do Governo Federal o provimento de estudos científicos e informações afetos às atividades de GC e segurança da informação. Adotar medidas e contramedidas apropriadas sobre o assunto, voltadas para assessorar à União, Estados, Municípios, organizações não-governamentais, setor privado, acadêmico e público.

A concentração das atividades de defesa e ataque à sistemas informatizados em um único núcleo ou departamento, constitui-se numa forma de alcançar o preparo adequado para a GC, organizando as atividades de forma integrada. Portanto, esse núcleo visa implementar uma evolução doutrinária, operativa e tecnológica dessa área de interesse, concentrando esforços na capacitação de pessoal especializado para realização e desenvolvimento das atividades de GC e de Segurança da Informação.

Propõe-se que o Núcleo de Guerra Cibernética e Segurança da Informação (NGCSI), como pode ser chamado, seja composto por três Coordenadorias:

- Coordenadoria de Criptologia (CCripto);
- Coordenadoria de Organização e Métodos (COeM); e
- Coordenadoria de Operações Cibernéticas e Análises de Segurança (COpS).

Além dessas Coordenadorias, deve existir ainda um grupo “ad-hoc”, voltado às respostas aos incidentes que porventura venham a ocorrer, sendo composto, de acordo com a natureza do incidente, por membros das três Coordenadorias. Voltado, portanto, à ações reativas, este Grupo de Resposta a Incidentes (GRI) será guarnecido e desguarnecido de acordo com os procedimentos estabelecidos pela COeM. A ativação ou desativação do GRI será sempre por ordem do Coordenador-Geral do NGCSI.

A Coordenadoria de Criptologia (CCripto), voltada as atividades de coordenação dos recursos criptológicos para uso pelas três Forças integrantes do MD, deve ser composta por dois setores:

- Códigos e Chaves: responsável pela gerência, desenvolvimento e manutenção de códigos criptográficos que possam ser de uso comum pelas três Forças e MD, proporcionando realizar, de forma integrada, comunicações seguras, bem como processamento e armazenamento de informações. Além disso, a guarda adequada dos códigos-fonte das cifras e respectivas chaves também estão sob a responsabilidade deste setor; e

- Criptoanálises: responsável pelas atividades de certificação e validação de códigos utilizados (criptoanálise certificacional) e pelas atividades de quebra de cifras (criptoanálise operacional) ou deciframento de mensagens criptografadas interceptadas.

A Coordenadoria de Organização e Métodos (COeM), voltada às atividades de organização e métodos do NGCSI, deve ser composta por três setores:

- Normas e Procedimentos: responsável pela elaboração e manutenção de normas e procedimentos para as atividades a serem executadas e desenvolvidas pelo NGCSI, bem como suas adequações doutrinárias e legais, quando aplicável;

- Formação de Pessoal: responsável pela seleção de pessoal, manutenção e planejamento da capacidade técnica dos integrantes do NGCSI, como também adestramento contínuo do grupo de resposta a incidentes; e

- Coordenação de Atividades e Exercícios: responsável pela integração das atividades do NGCSI de acordo com a doutrina estabelecida, bem como planejamento de exercícios gerais de GC e de ativação do grupo de resposta a incidentes.

A Coordenadoria de Operações Cibernéticas e Análises de Segurança (COpS), voltada às atividades de operação e desenvolvimento de recursos tecnológicos para GC, deve ser composta por quatro setores:

- Operações e Auditorias de Segurança: responsável pela realização efetiva das operações de GC, e por auditorias de Segurança da Informação em setores definidos pelo MD e de acordo com as normas e procedimentos estabelecidos;

- Análises de Riscos e Dispositivos: responsável pela realização de análises de vulnerabilidades e riscos em sistemas definidos pelo MD, bem como avaliação técnica de dispositivos voltados às atividades de reação e defesa de GC;

- Desenvolvimento de Recursos e Projetos: responsável pelo desenvolvimento e manutenção de aplicativos específicos voltados às atividades de ataque em GC, bem como assessorar projetos e arquiteturas voltadas à proteção das redes de comunicações definidas pelo MD; e

- Sensores e Alertas: responsável pelo posicionamento, manutenção e monitoramento de sensores de dispositivos de alertas em redes ou pontos definidos pelo MD, mantendo seus registros e análises de forma a possibilitar estudos e ativação adequada do grupo de resposta a incidentes. Além disso, também é responsável pela manutenção de uma página de alertas em relação a incidentes, possibilitando que ações pró-ativas sejam iniciadas.

8 CONCLUSÃO

O espaço cibernético possui hoje milhões de usuários aumentando exponencialmente a cada minuto. As pessoas estão ligadas à internet e, na maioria das vezes, sem nenhuma política de segurança, onde não existe um mínimo de controle. Esta falta de políticas, processos e controles, facilitam a disseminação de atos criminosos no espaço cibernético.

A preocupação com a disponibilidade, confidencialidade, integridade e autenticidade não deve estar restrita apenas à MB, mas também aos governos onde esta preocupação deve estar associada às Políticas Nacionais de Segurança da Informação. Estas devem ser escritas baseadas em contínuos levantamentos de vulnerabilidades e análises de risco, buscando sempre a máxima eficiência.

O estabelecimento da capacidade tecnológica para reagir ou se defender contra atividades de GC pode, a um baixo custo, contribuir para a redução do chamado "fosso digital" que os países do Primeiro Mundo impõem aos países menos desenvolvidos. O estabelecimento desta capacidade está diretamente relacionado à organização, formação e preparo do pessoal para este fim e depende, também, de uma Política de Estado, devido à atual integração e dependência que os sistemas críticos nacionais possuem em relação à TI.

Cada vez mais a complexidade e dimensão das atividades comerciais, do governo e da população, levam a uma dependência dos sistemas corporativos, que armazenam informações não mais disponíveis de outra forma. Muitos sistemas de comando e controle privados, governamentais e militares estão automatizados e dimensionados para velocidades de resposta muita acima da humana, para reagir a ataques ou dar apoio às decisões, que virão com antecipação de minutos, ou até mesmo segundos, quando o homem não teria condições de dirigir seu sistema de defesa. Os meios sofisticados e de alta velocidade e, mais recentemente, as técnicas ditas invisíveis, tornam a dependência de sistemas automatizados de previsão de ataque/defesa, cada vez mais uma necessidade, o que é confiado aos sistemas computacionais. A penetração nesses sistemas pode inviabilizar, portanto, toda uma estratégia de defesa e levar um país ao caos pela sua total paralisia estratégica.

Por fim, a maior vulnerabilidade da MB reside na dependência externa de sistemas corporativos, na pesquisa incipiente na segurança da informação, na falta de procedimentos para respostas a incidentes e na falta de uma cultura de Segurança da Informação. Assim, para se buscar a redução dessas vulnerabilidades deve-se reduzir a dependência externa e

intensificar pesquisas nas áreas de: Segurança de Redes, Procedimentos de Segurança, Vírus, Topologias de Segurança, *Firewalls*; Sistemas de Detecção de Intrusos (IDS), Análises de Risco; e Criptografia/Criptoanálise (Operacional e Certificadora).

Um ponto importante que deve ser observado, é que a GC não deve ser uma preocupação apenas da MB ou das Forças Armadas, outros órgãos e instituições também devem estar comprometidos, pois como foi abordado, os alvos de GC não são apenas militares, mas principalmente, os serviços de infraestrutura crítica, que afetam toda a nação.

A capacitação de pessoal especializado, a normatização do assunto e a melhoria dos meios (físicos, técnicos e de software) para levar a segurança aos níveis adequados requerem a dotação de recursos financeiros em montante elevado.

A palavra de ordem é se preparar adquirindo conhecimento, antecipar com o levantamento e análise, e agir o mais rápido possível como o momento atual exige.

REFERÊNCIAS

ALLEN, Patrick D. DEMCHAK, Chris. **A Guerra Cibernética entre a Palestina e Israel**, Military Review, 2004.

BRASIL. Departamento de Ciência e Tecnologia. **Portaria nº 063**, Brasília, DF, 2007.

_____. Diretoria Geral do Material da Marinha. **Normas para Criptologia da Marinha:** DGMM-0510 – 1ª revisão, Rio de Janeiro, RJ, 2000.

_____. Estado Maior da Aeronáutica. **Ofício º 3/6SC1**, Brasília, DF, 2004.

_____. Estado Maior da Armada. **Plano Estratégico da Marinha:** EMA- 2ª revisão. Brasília: DF, 2008.

_____. Estado Maior da Armada. **Doutrina de Tecnologia da Informação da Marinha:** EMA-416 – 2ª revisão, Brasília, DF, 2007.

_____. Estado Maior do Exército. **Ofício nº 178/2 SCh/SI.3**, Brasília, DF, 2004.

_____. Ministério da Defesa. **Estratégia Nacional de Defesa**, Brasília, DF, 2008.

_____. Presidência da República. **Política de Defesa Nacional**, Brasília, DF, 2005.

CONVERGÊNCIA DIGITAL. **Guerra Cibernética: Especialistas querem política nacional nos EUA**, Brasil, 30abr2009.

DUTRA, André Mello Carvalhais. **Introdução à Guerra Cibernética: a necessidade de um despertar Brasileiro para o assunto**, ITA, São José dos Campos.

ESTADOS UNIDOS DA AMÉRICA. Department of Defense. **The Implementation of Network-Centric Warfare**, Washington, DC, 2005.

_____. Congressional Research Service. **Report for Congress**, Washington, DC, 2001.

FÉLIX, Jorge Armando. **O Gabinete de Segurança Institucional**, Rio de Janeiro, RJ, Palestra em 19mar2009.

LAMOS, Robert. **Ataque cibernético poderia trazer resposta militar dos EUA**, Security Focus, 13mai2009.

LANDLER, Mark; MARKOFF, John. **The New York Times**, Nova York, 3jun2007.

MANDARINO, Raphael. A Segurança da Informação em Instituições Governamentais, Rio de Janeiro, RJ, Palestra em 12nov2008.

MARKOFF, John. **O Globo**, Rio de Janeiro, 29mar2009.

O GLOBO. **Uma declaração de guerra cibernética**, Rio de Janeiro, 9jul2009.

TEIXEIRA, Duda. **Veja**, Brasil, 23mai2007.

THE GUARDIAN. Londres, 7mar2008.

THE NEW YORK TIMES. **EUA planejam táticas de ataque e defesa em Guerra Cibernética**, New York, 2009.

ZENTGRAF, Maria Christina. **Introdução ao estudo da metodologia científica**. Rio de Janeiro. COPPEAD/UFRJ, 2009. Módulo de ensino.

ZERO HORA.com, 2009.