ESCOLA DE GUERRA NAVAL

CC (FN) TULIO ALVAREZ DE SOUZA

A GUERRA CIBERNÉTICA E A MARINHA DO BRASIL:

as ameaças cibernéticas e a defesa da MB

Rio de Janeiro

2012

CC (FN) TULIO ALVAREZ DE SOUZA

A GUERRA CIBERNÉTICA E A MARINHA DO BRASIL:

as ameaças cibernéticas e a defesa da MB

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

Orientador: CF Fabiano Rebello CANTARINO.

Rio de Janeiro

Escola de Guerra Naval

2012

RESUMO

A evolução da sociedade moderna com o advento da Tecnologia da Informação (TI) vem proporcionando benefícios, principalmente quanto à integração social e econômica, conferidos pela agilização de processos e circulação de informações em tempo real. Ao mesmo tempo em que a TI agrega valores, torna as pessoas, organizações e Estados vulneráveis a um novo tipo de ameaça, a cibernética. Este paradoxo da maior vulnerabilidade do mais forte é característica da assimetria cuja principal ameaça é a Guerra Cibernética (GCiber). Compreendê-la tem sido um dos grandes desafios para este novo milênio, tendo em vista que as ações cibernéticas envolvidas são reais, rápidas, complexas e não se limitam em fronteiras físicas e geopolíticas. Seus atores podem ser estatais ou não, envolvendo uma vasta gama de vetores e riscos. Criminosos, espiões, terroristas, ativistas e até mesmo Estados, em conflito ou não, podem atuar neste cenário causando grandes prejuízos financeiros, paralisando infraestruturas críticas, e, até mesmo, indiretamente, ceifando vidas. Recentes eventos comprovam a vulnerabilidades dos sistemas e demonstram a velocidade e complexidade que as ameaças se desenvolvem. Estados têm se preocupado com esta fragilidade e empenhado recursos a fim de desenvolver capacidades de defesa cibernética, seja nos níveis político, estratégico ou operacional/tático. O Brasil se encontra dentro daqueles que buscam soluções de segurança e defesa com o propósito de garantir a soberania e integridade nacional. A Marinha do Brasil (MB), como parcela integrante do Poder Nacional, também é dependente da TI e investe para suprimir as vulnerabilidades e ampliar sua capacidade de GCiber. Este trabalho busca analisar de forma sucinta as ameaças cibernéticas, suas características (atores, ações, efeitos desejados etc.), enumerando casos concretos e seus aprendizados, e a maneira de como se encontra estruturada a MB para enfrentar os novos desafios, com a finalidade de contribuir para a melhora da percepção da necessidade de busca contínua do aperfeiçoamento das capacidades operacionais da força naval.

Palavras-chave: defesa, guerra, ameaças, ataque, exploração e proteção cibernéticas, riscos, capacidade, emprego, infraestrutura crítica, tecnologia, informação, vírus, Marinha do Brasil.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A marcante evolução experimentada a partir da segunda metade do século passado devido à Tecnologia da Informação (TI) vem proporcionando inquestionáveis avanços na sociedade, principalmente quanto à integração social e econômica. Não obstante, estes benefícios conferidos pela agilização de processos e circulação de informações em tempo real tornam as pessoas, organizações e Estados vulneráveis a um novo tipo de ameaça, a cibernética.

Este paradoxo da maior vulnerabilidade do mais forte é característica marcante da assimetria proporcionada pelas ações cibernéticas, que são reais, rápidas, complexas e não se limitam em fronteiras físicas e geopolíticas. Seus atores podem ser estatais ou não, envolvendo uma difusa variedade de vetores e riscos. Crimes, espionagem, terrorismo, ativistas e até mesmo Estados, em conflito ou não, podem atuar causando grandes prejuízos financeiros, paralisando infraestruturas críticas, e, até mesmo, indiretamente, ceifando vidas. Tais fatos indicam que as ameaças cibernéticas devam ser tratadas com prioridade para a defesa dos Estados, sendo este um dos principais desafios da sociedade moderna.

No âmbito militar não há como tratar o assunto de maneira diferente. A defesa da soberania e integridade territorial são tarefas atinentes ao setor e, para cumpri-las, particularmente quanto às novas ameaças como a cibernética, faz-se necessário o entendimento de como elas atuam e de seus efeitos desejados e riscos.

Casos reais ocorridos recentemente, como por exemplo o do vírus STUXNET no Irã em 2010, demonstram a fragilidade dos sistemas e a aplicação de ações cibernéticas em prol de determinados efeitos desejados. Tem sido observado que as ações cibernéticas podem ocorrer isoladamente ou em apoio a ações cinéticas num campo de batalha. A Guerra do Golfo (2003), a Geórgia (2008), a Coreia do Sul e Coreia do Norte (2009), o Irã (2010) e o

Oriente Médio (2012), foram palco de ações cibernéticas e indicam ensinamentos que merecem estudos a fim de permitir uma visão mais holística desta conjuntura.

O Brasil e a Marinha do Brasil (MB) tem se aperfeiçoado, investindo em tecnologia, processos e conhecimento para, não somente se proteger das ameaças cibernéticas, mas também empregar as técnicas e metodologias da Guerra Cibernética (GCiber) como um recurso disponível em sua capacidade operacional.

Neste sentido, visando ampliar a discussão em torno do tema GCiber, esta monografia tem o propósito de analisar de forma sucinta as ameaças cibernéticas, suas características (atores, ações, efeitos desejados etc.), enumerando casos concretos e seus aprendizados, e na maneira como a MB encontra-se estruturada para enfrentar os novos desafios, contribuindo para melhorar a percepção da necessidade de busca contínua do aperfeiçoamento das capacidades operacionais da força naval.

O trabalho está fundamentado em pesquisa bibliográfico-documental, baseada em publicações doutrinárias, obras, artigos atinentes ao tema, e da utilização de técnicas indiretas, sendo que, para alcançar o propósito visualizado, encontra-se estruturado em três capítulos.

O primeiro apresenta e analisa os conceitos e definições da GCiber, enquadrando-a em uma nova dimensão de um conflito criada pelo homem, a cibernética; classificando as ações decorrentes quanto ao seu emprego. As ameaças cibernéticas são destacadas com suas principais características, atores, efeitos desejados, com o intuito de proporcionar uma perspectiva singular sobre os riscos envolvidos.

No segundo capítulo são apresentados e analisados exemplos históricos enumerando aspectos e ensinamentos que podem contribuir para a melhoria das condições de proteção adotadas pela MB. No último capítulo são comentadas as iniciativas do nível estratégico brasileiro, e como a MB encontra-se estruturada para fazer frente às ameaças cibernéticas e uma conclusão que reúne as principais ideias desenvolvidas ao longo do texto.

2 GUERRA CIBERNÉTICA

Este capítulo apresenta e analisa os conceitos e definições da GCiber, enquadrando as ações cibernéticas no contexto das dimensões de um conflito e na classificação quanto ao seu emprego conforme definição no âmbito do Ministério da Defesa (MD). As características principais das ameaças cibernéticas são destacadas com o intuito de proporcionar uma perspectiva singular sobre os riscos envolvidos.

2.1 Conceitos e definições

A crescente utilização das tecnologias englobando atividades em diversas áreas, como o controle de sistemas de infraestruturas críticas (matrizes energéticas, finanças, telecomunicações, transportes, saúde e *internet*), torna as sociedades modernas cada vez mais dependentes e vulneráveis às ameaças e incidentes existentes em torno do uso dos computadores, das redes e dos sistemas de TI (LIBICKI, 2009).

Um dos termos que constantemente aparecem em livros, filmes, artigos e noticiários, para tentar apresentar os problemas de segurança relativos aos ataques e incidentes nas redes, é a GCiber.

O autor Richard Clarke[1] (2010), conceitua que GCiber se refere às ações realizadas por Estados para penetrar em computadores e redes de outro Estado com a finalidade de causar dano ou de neutralizá-la. Afirma ainda que é real, rápida, global, extrapola o campo de batalha e já começou (CLARKE, 2010).

Na mesma linha, o Departamento de Defesa dos Estados Unidos da América (EUA) propôs a seguinte definição para GCiber: "conflitos armados conduzidos total ou

[1] Richard Clarke serviu como coordenador nacional de segurança dos EUA entre os governos de Ronald Reagan (1980-1989) e Bill Clinton (1993-2001) e foi autor do livro *CyberWar – The next threat to national security and what to do about it.*

parcialmente por meio da cibernética. Operações militares conduzidas a negar uma força adversa o uso eficiente de sistemas do espaço cibernético[2] e armas durante um conflito. A GCiber inclui ataques e defesa cibernéticos." (EUA, 2010).

Outra perspectiva sobre GCiber é a de Daniel Ventre (2011), um pesquisador francês que a apresenta como sendo uma matriz complexa, coberta de incertezas, e que deve ser entendida como uma relação de dupla interpretação, uma ontológica[3] e outra topológica. Na ontológica deve ser questionado se o que está acontecendo é realmente uma guerra ou não. A definição dos limites entre categorias encontradas nos incidentes precisariam ser definidos, como crimes, conflitos etc. Sob o ponto de vista topológico, deve-se repensar como podem ser transportados os conceitos de guerra, normalmente vinculados a território e aos Estados, para um campo onde as fronteiras não são tão definidas assim. Ventre (2011) defende que as ações ofensivas e defensivas devem fazer parte das capacidades militares cujos esforços devem ser direcionados para fazer frente a um oponente (VENTRE, 2011).

O mesmo autor ainda esforça-se para delimitar melhor o conceito de GCiber, citando e definindo o que ela não é: a GCiber não pode ser simplificada a conceitos de espionagem cibernética da mesma forma que uma guerra não pode ser reduzida a ações de espionagem; acima de tudo, GCiber não é um conceito fixo, um objeto definido com precisão e imutável; não pode ser simplificada a ações diversas encontradas na *web*[4], como pichações de páginas entre Estados rivais, organizações ou movimentos políticos; não pode ser comparada a ações realizadas por *hackers*[5] ou *hacktivistas*[6], como encontrado na mídia; e, que, não é guerra fria (VENTRE, 2011).

---

[2] Espaço Cibernético é o espaço virtual, composto por dispositivos computacionais conectados em redes ou não, nos quais as informações digitais transitam, são processadas, e/ou armazenadas.
[3] Ontologia é a parte da filosofia que trata da natureza do ser. Teoria metafísica do ser.
[4] Entende-se por *web* o sistema de documentos reunidos de várias mídias num suporte computacional, implementado por sistemas eletrônicos de comunicação que são interligados e executados na *internet*.
[5] *Hackers* são os usuários com alto conhecimento que se dedicam a descobrir novas vulnerabilidades em sistemas, seja por motivações pessoais, ganhos financeiros etc.
[6] *Hacktivistas* são uma combinação de *hackers* e ativistas.

Os autores citados divergem quanto aos conceitos de GCiber em seu contexto. Clarke (2010) explora uma definição mais tradicional afirmando que seria um conflito entre Estados. Por outro lado, Ventre (2011) é mais abrangente, considerando outros tipos de incidentes e conflitos como parcela do contexto.

Os documentos de doutrinas militares consideram a GCiber como uma das formas ou componentes das Operações de Informação[7] e pode ser definida como ataques computadorizados acompanhados de operações militares físicas para destruir as forças militares inimigas ou que se originarem de conflitos políticos entre Estados (DANG 2011).

A GCiber pura, na qual somente armas cibernéticas são usadas, é praticamente improvável. As guerras do futuro serão efetivadas por meio de ações convencionais (cinéticas) e cibernéticas, estas utilizadas para ampliação da força ou subversão do oponente. (SOMMER, 2011).

As definições e conceitos sobre o tema são importantes, mas não tão relevantes quanto o uso estratégico da aplicação do poder envolvido. A GCiber é um instrumento do poder que não substitui a força física, mas a complementa, podendo ser trabalhada isolada ou em combinação com as demais dimensões de um conflito (mar, ar, terra e espaço).

No Brasil, o MD identificou os conceitos e metodologia de emprego da GCiber no Manual de Doutrina de Operações Conjuntas. Neste manual encontra-se a definição de Defesa Cibernética (DC):

> É o conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com a finalidade de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de Inteligência e de causar prejuízos aos sistemas de informação do oponente (BRASIL, 2011).

[7] Entende-se por Operações de Informação as ações coordenadas que concorrem para a consecução de objetivos políticos e militares. Executadas com o propósito de influenciar um oponente real ou potencial, diminuindo sua combatividade, coesão interna e externa e capacidade de tomada de decisão. Atuam sobre os campos cognitivo, informacional e físico da informação do oponente, e, também, sobre os processos e os sistemas nos quais elas trafegam, ao mesmo tempo em que procuram proteger forças amigas e os respectivos processos e sistemas de tomada de decisão (BRASIL, 2007).

E de GCiber, que é o:

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

As definições acima confirmam a tese de que não é necessário haver um conflito entre Estados para a configuração da GCiber. Ademais, na Doutrina Militar Conjunta do Estado brasileiro, as ações no espaço cibernético brasileiro são denominadas conforme o nível de planejamento:

−Nível político: Segurança da Informação e Comunicações (SIC) e segurança cibernética, coordenadas pelo Gabinete de Segurança Institucional da Presidência da Republica (GSI/PR) e abrangendo a Administração Pública Federal (APF), direta e indireta, bem como as infraestruturas críticas da informação nacionais dos setores público e privado;

−Nível estratégico: DC, a cargo do MD, interagindo com o GSI/PR e APF; e

−Níveis operacionais e tático: GCiber, denominação restrita ao âmbito interno das Forças Armadas (BRASIL, 2011).

As ações cibernéticas são classificadas conforme seu emprego em exploração cibernética, ataque cibernético e proteção cibernética. A exploração cibernética atende aos fins de Conhecimentos de Inteligência; o ataque cibernético para fins ofensivos, seja para interromper, negar, degradar, corromper ou destruir informações armazenadas em dispositivos e redes computacionais e de comunicações do oponente; e a proteção cibernética aos fins defensivos, cuja abrangência é focada na neutralização de ataques e exploração realizados pelo oponente, incrementando as ações de segurança cibernética em face de uma situação de crise ou conflito armado (BRASIL, 2011).

Segundo Ventre (2011), uma ação cibernética pode ser realizada diversas vezes, em vários períodos de tempo. O impacto pode ser enorme, dependendo do vulto das ações e

da criticidade do alvo. Ao mesmo tempo em que podem ser percebidas, também podem ocorrer em silêncio (VENTRE, 2011).

Depreende-se que a GCiber é um recurso significativo que pode ser utilizado como um excelente método para alcançar objetivos estratégicos. Outro aspecto relevante é a importância do motivo da ação realizada, independente do oponente. Caso seja contra as estruturas do Estado, afetando a soberania nacional, é legítimo enquadrar a GCiber como recurso ou ameaça. No caso de sua utilização como um recurso disponível para o Estado, as ações cibernéticas podem ser realizadas durante a preparação do campo de batalha de forma a reduzir o poder de influência do oponente e conquistar uma maior liberdade para a manobra. Quando considerada como ameaça, faz-se mister compreender seu funcionamento, possibilidades e limitações, tema a ser abordado a seguir.

2.2 Ameaças cibernética

Conhecer as ameaças que circundam o mundo cibernético é fator crucial e fundamental para minimizar os impactos dos riscos envolvidos no processo de utilização do meio digital. Atores estatais e não estatais fazem parte deste jogo, no qual sistemas de TI podem ser atacados, incluindo-se os de infraestrutura crítica de um Estado. Neste caso, ações podem ser executadas contra sistemas de energia, telecomunicações, transportes, saúde e de abastecimento, pois vulnerabilidades existem e podem ser exploradas a qualquer momento. Outra possibilidade é a interferência nos sistemas bancários e nos instrumentos do mercado financeiro, causando um impacto enorme sobre a economia (NYE, 2009).

No entendimento do escritor Joseph Nye (2009) existem quatro ameaças à segurança nacional, cada uma com um diferente horizonte de tempo e distintas soluções: o crime, a espionagem econômica, o ciberterrorismo e a GCiber. A partir dessa categorização,

cada Estado, por meio de análise de riscos e percepção de vulnerabilidades, adotará qual tipo de ameaça deverá ser enfrentada com prioridade. Arquilla e Ronfeldt (2001) ainda acrescentam os *hackers* e *hacktivistas* como ameaças (ARQUILLA, 2001).

As ações cibernéticas dos atores estatais e não-estatais listados acima são executadas no espaço cibernético criado pelo homem representado como mais uma das dimensões de um conflito, porém transversal às quatro outras tradicionalmente consideradas como marítima, terrestre, aérea e espacial. No cruzamento entre as dimensões cibernética e as demais encontram-se o domínio Real (denominado "R") e o domínio Virtual (denominado "V"). Este encontro é onde se encontra o espaço cibernético (ou, eventualmente, espaço da informação). Ao imaginar quais as ações poderiam ser conduzidas em "V" que afetam "R" e vice-versa é que se define qual tipo de operação será realizada. As ações cibernéticas estão aí delimitadas (FIG. 1) (VENTRE, 2011).

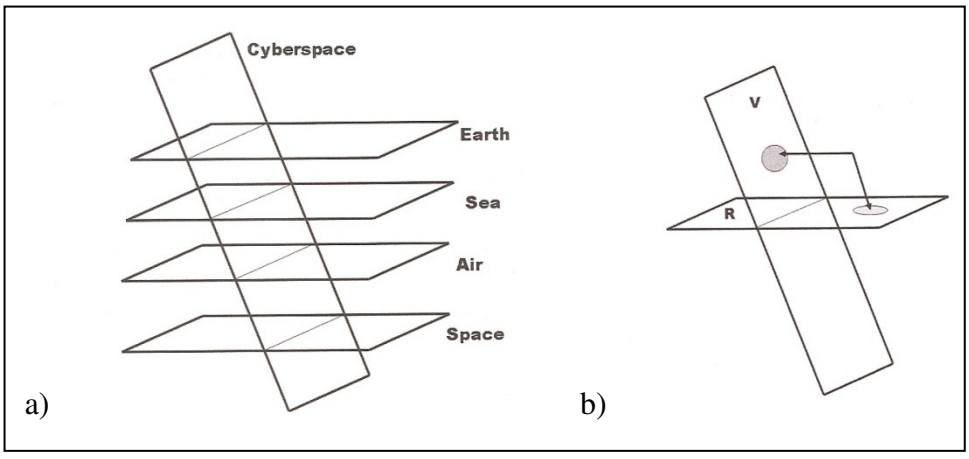

FIGURA 1 – Dimensões de um conflito.
a) Interseção do Espaço cibernético com demais dimensões.
b) Local das operações cibernéticas. Encontro do Domínio Virtual com o Real.
Fonte: VENTRE, 2011, p. 162,163.

Considerando-se as interações entre a dimensão cibernética e as demais, vislumbra-se que os efeitos desejados das ações realizadas pelas ameaças cibernéticas abrangeriam quatro áreas: perda de integridade, de disponibilidade, de confidencialidade e destruição física. A perda da integridade está relacionada diretamente com a modificação indesejada de dados dos sistemas de informação, resultando em imprecisão, fraude ou

decisões equivocadas. A perda de disponibilidade é tornar indisponível para usuários autorizados a informação necessária naquele momento. A perda de confidencialidade ocorre quando há acesso não autorizado a sistemas de informação, podendo ameaçar até a segurança nacional conhecida por comprometimento. Já a destruição física refere-se à habilidade de criar dano físico real a determinado sistema por meio da utilização da TI. Neste último, citam-se os sistemas que operam as infraestruturas críticas de um Estado, nos quais dispositivos físicos são controlados por programas de computador nomeados como *Programmable Logic Controllers* (PLCs) (SYMANTEC, 2010). Estes sistemas são conhecidos como *Supervisory Control and Data Acquisition (*SCADA*),* que podem ser atacados causando mau funcionamento de serviços críticos, como controle de voo ou de trens (EUA, 2006).

Compreende-se que as ameaças cibernéticas podem afetar os sistemas da infraestrutura de um Estado. Dentre as estruturas, as de Comando e Controle (C2), Sistemas de Armas, e outros sistemas militares incluem-se como possíveis alvos, cujo mau funcionamento causaria impactos negativos relevantes nas forças militares que os utilizam.

Com o aperfeiçoamento dos ataques, os Estados têm investido em mecanismos de defesa para garantir o funcionamento e segurança em tempo de paz e de conflitos. As forças militares estão se aperfeiçoando, criando doutrinas, por vezes incipientes, pela falta de ações práticas na história. Os ataques podem gerar hipóteses de emprego e ameaçar a estabilidade das relações internacionais. Podem até ser considerados como atos de guerra, sendo que a dificuldade em se identificar o autor é enorme. Os computadores ou dispositivos identificados como vetores de ataques podem ter sido comprometidos anteriormente, e até mesmo estar sendo utilizados como uma ação de dissimulação. As ações cibernéticas podem ser silenciosas e invisíveis até que o "gatilho seja puxado" (CLARKE, 2010).

Corroborando com a idéia de que o risco das ameaças cibernéticas é inerente às sociedades modernas, observou-se pela primeira vez na história a inclusão da ação de ataque

cibernético na lista dos cinco principais riscos à economia global, conforme Relatório Global de Riscos de 2012 do Fórum Econômico Mundial (DAVOS, 2012).

Para a realização de um ataque cibernético é necessário um programa ou código, que normalmente pode ser encontrado na *internet*. Entretanto, programas mais sofisticados estão sendo construídos por especialistas, grupos e por Estados, e podem causar vastos impactos. Observa-se no geral, que a eficiência de um ataque não é necessariamente relacionada ao mecanismo ou ferramenta mais moderna, complexa e poderosa, mas sim ao efeito desejado alcançado (VENTRE, 2011).

Rússia, China, EUA, Israel, Irã e Coreia do Norte são Estados que se encontram em pleno desenvolvimento de suas capacidades de GCiber, sejam ofensivas e defensivas. Em consequência, há o risco de que tais artefatos possam cair em mãos de terroristas e criminosos. Esta ameaça de terrorismo cibernético é esperada para os próximos anos (CLARKE, 2010).

Sob outra perspectiva, a empresa de segurança *McAfee*[8] afirma que as ações de ataques cibernéticos, mesmo as mais complexas, avançadas e persistentes conhecidas como *Advanced Persistent Threats* (APT)[9], deixam rastros que podem ser estudados com detalhes, possibilitando a identificação de informações importantes sobre suas características. Dados como a metodologia utilizada, assinatura dos códigos, dentre outros, são altamente relevantes e devem ser acompanhados. Estas capacidades devem ser desenvolvidas pela inteligência cibernética de um Estado e são fundamentais para sua defesa (MCAFEE, 2012).

Conclui-se que existe uma gama de variáveis envolvidas nas ameaças cibernéticas. Os atores podem ser estatais ou não e as ações cibernéticas realizadas encontram-se no espaço cibernético, uma nova dimensão de um conflito criada pelo homem e

---

[8] A *McAfee* é empresa de segurança situada nos EUA.

[9] *Advanced Persistent Threat* - APT é a ameaça cibernética persistente e avançada que pode realizar um ataque, altamente segmentado, bem pesquisado, amplamente financiado, e adaptado a uma organização particular, que geralmente emprega múltiplos vetores e que pode implementar técnicas para evitar sua detecção.

que permeia as tradicionais dimensões marítima, aérea, terrestre e espacial. Os efeitos desejados das ameaças podem abranger a perda da disponibilidade, integridade, confidencialidade e até a destruição física. Os mecanismos utilizados podem ser facilmente encontrados e utilizados por qualquer pessoa.

Outros pontos relevantes apresentados indicam a evolução constante das ações de ataque e exploração, cada vez mais complexas e sofisticadas. A dificuldade em se identificar a autoria de um ataque pode ser encarada como um fator limitador para a defesa. Desta forma, pressupõe-se uma tendência de desequilíbrio entre ataque e defesa, exigindo mudanças na capacidade de defesa, como a necessidade de se implementar sistemas dotados de inteligência artificial.

Os riscos envolvidos são cada vez mais percebidos pela sociedade, uma vez que as ameaças cibernéticas podem afetar os sistemas de infraestrutura de um Estado, fazendo com que fossem incluídas entre um dos cinco principais riscos à economia mundial.

A fim de melhor exemplificar estes conceitos, o próximo capítulo enumera casos concretos de conflitos cibernéticos recentes de nossa sociedade, cujas experiências colhidas podem contribuir para a melhoria da condição de defesa da MB.

3 EXEMPLOS HISTÓRICOS

Este capítulo tem como objetivo apresentar e analisar casos e exemplos históricos de ocorrência de ataques cibernéticos ao longo do mundo. O entendimento das ameaças citadas no capítulo anterior aplicadas em exemplos reais pode elucidar e contribuir para a melhoria da capacidade de GCiber da MB.

3.1 Guerras do Golfo (1991-2003)

Uso da tecnologia nos campos de batalha do século XX, como na Primeira Guerra do Golfo (1991), seja para conduzir e gerenciar a logística, seja para prover o acompanhamento da situação e até mesmo para o lançamento de bombas inteligentes guiadas por satélite é uma tendência que não há como voltar atrás. Apesar de não ter sido utilizada nenhuma arma cibernética específica para neutralizar as redes de defesa do Iraque, a coalizão liderada pelos EUA estava pronta para atacar as redes de computadores adversárias. É de se observar que, ao mesmo tempo em que se cria uma grande vantagem tática no uso da tecnologia em combate, ela também aponta para várias vulnerabilidades que podem ser exploradas, seja por uma força militar semelhante, ou por outra menor e considerada mais fraca. Aqui, as características da Guerra Assimétrica se acentuam e fazem das redes de C2 um alvo compensador para ambas as partes, principalmente contra aquela que mais detém o uso da tecnologia (CLARKE, 2010).

Já na Segunda Guerra do Golfo (2003), as redes militares do Iraque foram comprometidas e diversas ações cibernéticas realizadas. Centenas de Oficiais iraquianos receberam *e-mails* do sistema de dados do Ministério de Defesa Iraquiano contendo textos

com ideias-forças trabalhadas pelas Operações Psicológicas[10] (OpPsi) das forças aliadas, instruindo aos iraquianos de que haveria uma invasão ao Iraque e que somente as forças que se opusessem ao ataque seriam destruídas. A intenção da invasão era depor o regime de Saddam Hussein (1979-2003). A instrução era para que as tropas se desarmassem e não engajassem, pois após a retirada de Saddam Hussein as tropas poderiam voltar a seus postos para serem reconstituídas (CLARKE, 2010).

Percebe-se que as redes de dados das forças militares oponentes são alvos importantes a serem considerados em um conflito. Trabalhos de inteligência prévios realizados pela exploração de acesso à rede e sistemas do oponente, como por exemplo, o de *e-mails,* são ações que podem contribuir para a Guerra de Informação. A utilização destes dados, alinhados às técnicas de OpPsi, fez chegar aos "corações e mentes" ideias para desmoralizar e manipular a opinião interna das tropas iraquianas. A combinação destes vetores e o alinhamento com os objetivos estratégicos podem desbalancear o poder de combate dos beligerantes.

Atenção especial deve ser dada à utilização da *internet*, como por exemplo, o uso de redes sociais que passam a ter importância no cenário quando se referem às ações de Exploração Cibernéticas. Elas são fontes de informações e de desinformações que devem ser analisadas e utilizadas em prol da defesa.

No caso da Segunda Guerra do Golfo (2003), verificou-se o emprego de ações exploratórias, ligadas à inteligência, mesmo antes da realização das ações cinéticas no Teatro de Operações.

[10] Operações Psicológicas - Operações que incluem as ações psicológicas e a guerra psicológica e compreendem ações políticas, militares, econômicas e psicossociais planejadas e conduzidas para criar em grupos - inimigos, hostis, neutros ou amigos - emoções, atitudes ou comportamentos favoráveis à consecução de objetivos nacionais (BRASIL, 2007).

3.2 Estônia (2007)

Durante os 52 anos de ocupação soviética, após o término da Segunda Guerra (1939-1945), muitos movimentos de insurgências e até de guerrilha se formaram na Estônia, porém foram suprimidos pelo governo de Moscou. Apenas em 1991, com o desmembramento da antiga União das Repúblicas Socialistas Soviéticas (URSS), iniciou-se a estruturação dos ex-Estados soviéticos como a Estônia, que obteve independência em 1992. Após a saída do exército russo em 1994, a Estônia aumentou seus laços comerciais com o resto do leste europeu, obtendo um alto crescimento econômico nos anos 2000. Teve seu ingresso aceito na Organização do Tratado do Atlântico Norte (OTAN) em 29 de março de 2004, e na União Europeia (UE) em primeiro de maio de 2004.

A Estônia é citada como um caso de estudo de ataques cibernéticos, pois sofreu uma série destes ataques a partir de 27 de abril de 2007, deixando vários sítios do governo inoperantes. O governo estoniano acusou a Rússia, de ter se motivado a realizar os ataques por conta da remoção de uma estátua que marcava a vitória russa contra o nazismo, a estátua do Soldado de bronze de Tallinn (CARR, 2010).

O ataque sofrido foi do tipo Negação de Serviço Distribuído (DDoS)[11], realizado por redes de computadores controladas pelos atacantes. Estas redes são conhecidas como *botnets*. Para marcar a capilaridade da ferramenta, qualquer computador pode ser utilizado no ataque, bastando estar infectado por um software malicioso. Um usuário de qualquer parte do globo pode acessar um sítio ou receber um *email* com o programa de ataque e fazer parte do processo sem mesmo ter consciência disto. Esta técnica é barata e não exige grandes pesquisas e nem mesmo sofisticação no método, podendo se alastrar e ganhar um enorme vulto horas após ser disponibilizado o programa na *internet.* No ataque realizado contra a

[11] *Distributed-Deny-of-Services* (DDoS) – ataques de negação de serviços distribuído realizado com o uso de uma rede de computadores sob controle do atacante (*botnet*).

Estônia, foram identificadas diversas *botnets* que atingiram não somente os sítios do governo, mas também servidores de telefonia, sistemas de cartões de créditos e diretórios de negócios, bancos e de setores das comunicações da *internet*. Os efeitos dos ataques tiveram proporções extraordinárias fazendo o país ficar sem rede de dados confiável e estável por cerca de três semanas (CARR, 2010).

Mesmo com a utilização de técnicas de defesa de rede implementadas como uso de antivírus e *firewall*[12] os ataques eram mantidos e constantemente burlavam as defesas criando novas frentes de ataques. Uma equipe da OTAN foi chamada para auxiliar na resposta a estes incidentes tentando minimizar os danos sofridos pela Estônia. Com *softwares* de varreduras para tentar identificar as fontes dos ataques, os especialistas conseguiram mapear os ataques e chegaram à conclusão que os computadores que controlavam as *botnets* encontravam-se na Rússia e os códigos fontes dos programas de ataque estavam escritos em alfabeto cirílico. Mesmo com tais indícios, o governo Russo negou veementemente a participação nos ataques e assinou um acordo de cooperação para identificar os atacantes que estivessem em seu território. Respostas foram apresentadas como sendo ações de pessoas nacionalistas, mas nada de concreto foi alcançado nas investigações. Permanecem suspeitas sobre a participação de elementos do crime organizado como atores não estatais ligados aos ataques. O envolvimento da Rússia não foi comprovado, mas a suspeita ainda paira como possível facilitador dos ataques, até mesmo como coordenador dos atores não estatais (CLARKE, 2010).

Após este evento, foi criado um Centro de Defesa Cibernética em 2008 na Estônia, que funciona até hoje como um órgão de DC da OTAN, protegendo as redes dos Estados que fazem parte daquela organização (NATO, 2011).

---

[12] *Firewall* é um dispositivo de rede de computadores que visa aplicar uma política de segurança a um determinado ponto da rede.

A criação deste órgão integrado para responder aos incidentes de redes da OTAN confirma a dificuldade de se combater isoladamente os ataques cibernéticos. A origem dos ataques é dúbia e o impacto devastador. Faz-se necessário que a proteção contra este tipo de ameaça deva ser realizada por meio de cooperação e integração, sejam de pessoas, empresas ou governos.

3.3 Geórgia (2008)

Situada mais a sul, a Geórgia era vista como área de influencia de Moscou. Em agosto de 2008, a Geórgia e Ossétia do Sul iniciaram um sério conflito. Os georgianos intensificaram os ataques militares e, no dia seguinte a este ataque, a Rússia interveio no conflito a favor da Ossétia do Sul, declarando guerra contra a Geórgia, deslocando rapidamente seu exército e expulsando os georgianos da Ossétia do Sul. Precisamente no mesmo dia do ataque terrestre russo, houve uma grande movimentação de ataques cibernéticos contra a Geórgia (CLARKE, 2010).

As técnicas envolvidas nas ações cibernéticas inicialmente eram de ataque, com efeitos desejados de: perda de disponibilidade (com a interrupção dos serviços nos sítios do governo e da imprensa); e de perda de integridade (com a invasão de páginas da *internet* e modificação de seus conteúdos - *defacement*[13], nos quais eram inseridos, por exemplo, fotos do líder da Geórgia, Mikheil Saakashivili, comparado-o com o premier alemão durante a 2ª Guerra Mundial (1939-1945), Adolf Hitler). A partir de então, os ataques foram crescendo em intensidade e sofisticação até o momento em que a batalha terrestre chegou ao seu fim (CLARKE, 2010).

[13] *Defacement* - Também chamada de pichação. Técnica que consiste em alterar o conteúdo da página *web* de um sítio.

Os efeitos destes ataques foram devastadores. Os roteadores que demandavam às redes da Geórgia, com dados oriundos dos tráfegos da Rússia e Turquia, praticamente pararam devido à inundação de pacotes nas redes criada pelos ataques DDoS com utilização de *botnets* (modelo de ataque similar ao utilizado contra a Estônia) (CLARKE, 2010).

Além disso, os atacantes assumiram os controles de roteadores da *internet* situados na Geórgia, fazendo com que a população ficasse sem comunicação com o mundo externo, sem receber notícias, *e-mails* e sem acesso à rede de dados. As tentativas de defesa eram ineficazes. Novos ataques eram realizados a partir de qualquer tentativa de bloqueio. Uma das ações de proteção cibernética foi a de bloquear o tráfego oriundo da Rússia, mas os ataques foram redirecionados e passaram a chegar pela China. As investigações apontaram para a existência de várias *botnets* controladas por servidores situados na Rússia, no Canadá, na Turquia e, ironicamente na Estônia (CLARKE, 2010).

A Geórgia transferiu seus servidores do governo para as redes do *Google*[14] na Califórnia (EUA) para que pudessem voltar a operar, mas mesmo assim, os servidores foram alvos de ataques contínuos. A rede bancária foi praticamente neutralizada, além das redes de cartões de crédito e sistemas de telefonia móvel (CLARKE, 2010).

Foram empregadas pelo menos seis grandes *botnets* que utilizavam computadores espalhados pelo globo de usuários da *internet*, cujos computadores estavam infectados com os programas maliciosos. Também foi observada grande adesão voluntária de usuários que se interessaram em fazer parte dos ataques, bastando que baixassem os programas maliciosos criados especialmente para realização dos ataques contra a Geórgia. Eram ferramentas simples, disponibilizadas em sítios da *internet* em que qualquer pessoa poderia baixar, instalar e executar ataques com um simples aperto de um botão chamado "*Start Flood*" do próprio programa malicioso. Esta variação do método de se conseguir novos vetores para o ataque

[14] *Google* é uma empresa multinacional com sede dos EUA de serviços *online* e *software*.

criou um verdadeiro exército de voluntários, que dificultou ainda mais a contenção do ataque (CLARKE, 2010).

A coordenação dos ataques utilizou listas de alvos previamente selecionados, entre os quais os sítios do governo da Geórgia, bem como outros sítios de valor estratégico, incluindo-se os das embaixadas estadunidense e britânica. Para as ações deflagradas foram usados grupos nacionalistas de *hackers* civis, coordenados por um fórum técnico e de mobilização, conhecido como *StopGeorgia.ru*, que era hospedado em um provedor de *internet* do Texas, nos EUA (CARR, 2010).

O governo russo negou a participação e citou que acreditava ser uma resposta popular. Para este caso, há fortes indícios de que alguns sítios que foram utilizados como origens dos ataques estavam hospedados em *links* do aparato de inteligência russo. Cabe aduzir que as ações orquestradas nos ataques não seriam possíveis de serem realizadas por uma cruzada patriótica cibernética somente baseada no clamor popular (CLARKE, 2010).

Estes ataques refletem uma parcela das possibilidades de utilização do espaço cibernético para a condução da GCiber. O espaço cibernético considerado para as ações de ataque extrapolou o Teatro de Operações com a utilização das redes existentes e disponíveis em outras partes do globo. Verifica-se que a dimensão cibernética influencia e afeta diretamente outras dimensões de um conflito, comprovando a relação citada no capítulo anterior.

Constata-se que não foram utilizadas armas cibernéticas sofisticadas e inéditas nos ataques contra a Geórgia. Pautaram-se em simples ferramentas disponíveis na *internet*, e foram supostamente coordenados para atingir um propósito específico que acabou por apoiar outras ações no campo de batalha físico. Evidencia-se a utilização de ações cibernéticas para limitar e reduzir a capacidade de C2 do oponente e também da infraestrutura crítica do Estado alvo, de modo a garantir maior liberdade de ação.

Ressalta-se a participação de atores não estatais nestes conflitos. Este fato deve ser levado em consideração na realização das ações de GCiber da MB, pois amplia a dificuldade de gestão neste tipo de conflito.

3.4 Coreia do Norte x Coreia do Sul (2009)

Na Coreia do Norte são percebidas grandes iniciativas nas capacidades de GCiber. Como exemplo, cita-se a criação de unidades especiais de *hackers* do Exército Popular da Coreia, que possui elementos de Guerra Psicológica e Cibernética como a Unidade 204 com cerca de cem *hackers*. Possuem também outra unidade somente focada em GCiber com cerca de seiscentos *hackers*, a Unidade 121. Elas foram consideradas suspeitas da participação de ataques cibernéticos realizados contra a Coreia do Sul, em julho de 2009 (CLARKE, 2010).

Durante estes ataques foram utilizadas técnicas de DDoS, com uso de *botnets,* com efeitos desejados de perda de disponibilidade e de integridade. Os ataques ocorreram com a atuação da OpPsi, explorando o apoio dos EUA à Coreia do Sul, como medida de retaliação e demonstração de poder durante a comemoração da independência dos EUA, no dia 4 de julho de 2009. O sucesso destes ataques contra a Coreia do Sul é uma prova clara das graves deficiências dos sistemas de defesas atuais. As ferramentas utilizadas desta vez eram mais sofisticadas, possuindo características de autodefesa. Sua defesa era o lançamento de um ataque DDoS contra qualquer computador que a identificasse (COLEMAN, 2011).

Para fazer frente a esta tecnologia, é necessário trabalhar com inteligência artificial à base de modelagem comportamental. É uma das poucas técnicas que tem demonstrado eficácia contra as versões mais recentes dessas armas cibernéticas, porém ainda

carece de disponibilidade comercial. Uma estratégia de defesa em profundidade[15] é necessária para tentar se defender contra *botnets*. Em uma análise mais detalhada deste ataque verificou-se que vetores de dezesseis Estados foram utilizados (FIG.2).

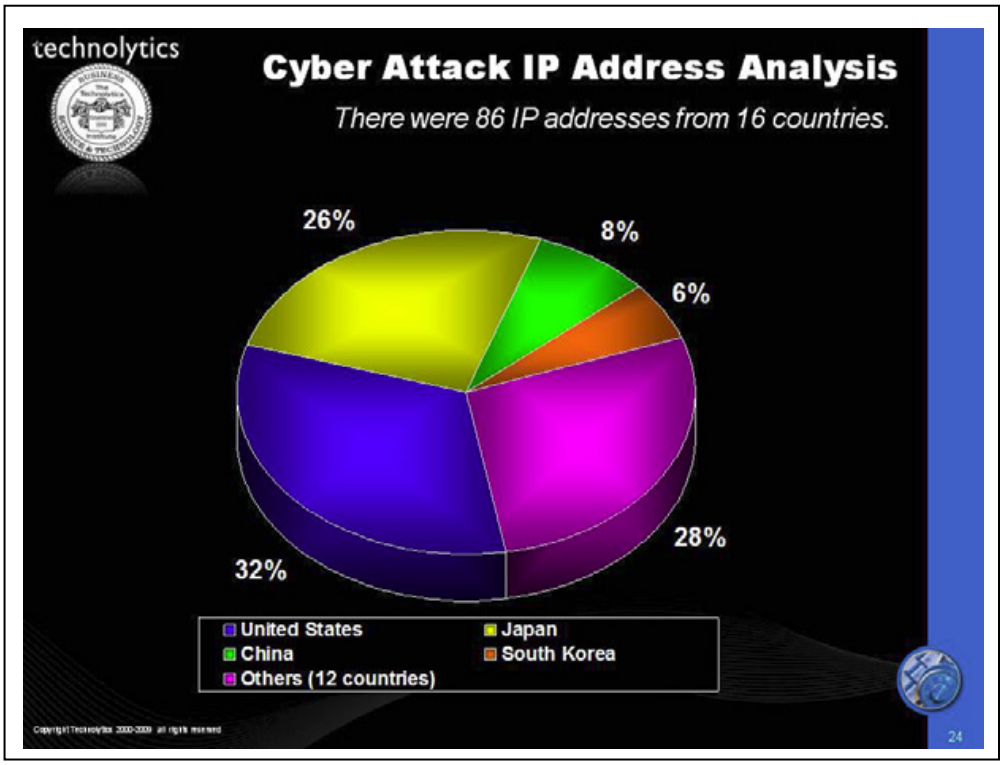

FIGURA 2: Análise dos endereços de ataque e países de origem
Fonte: COLEMAN, 2011, p.211.

A integração das equipes de GCiber com a OpPsi permite impulsionar e catalisar o resultado dos ataques cibernéticos e confirmam que estas ações se enquadram nas Operações de Informação conforme citado no capítulo 2. Outra característica importante é a sofisticação das armas de ataque que continham mecanismos de autodefesa, dificultando ainda mais a defesa. A preparação da proteção cibernética contra este tipo de ação deve ser realizada com investimento em pessoal e tecnologia, empregando inteligência artificial, a fim de minimizar o impacto.

[15] Defesa em profundidade: técnica de defesa onde são utilizados diferentes mecanismos de segurança e de controle em uma rede de computadores que se complementam aumentando o grau de segurança.

3.5 Irã (2010)

O *Stuxnet* é um programa de computador malicioso descoberto em 2010 e destinado a destruir as centrífugas de enriquecimento de urânio na usina nuclear de Natanz, no Irã, atuando no sistema SCADA que as controla. Este programa demonstrou na prática a possibilidade de infectar um sistema de computador e prejudicar o funcionamento de um sistema industrial físico. O *Stuxnet* é altamente complexo, direcionado para atacar um sistema específico, com uso de vulnerabilidades de *software* desconhecidas, chamadas de *Zero-Days*[16], e certificados digitais[17] falsos e com um código enxuto e eficiente.

O efeito físico de ataques em sistemas *SCADA* é uma preocupação real, particularmente quando se observam os possíveis danos sobre as infraestruturas críticas (petróleo, energia, abastecimento, transportes etc.). Concretiza-se aqui um artefato cibernético criado especialmente com o efeito desejado de perda da disponibilidade, pela neutralização ou destruição do alvo.

Outro esclarecimento sobre este ataque é o de que as redes de controle das centrífugas de enriquecimento de urânio do Irã não estavam ligadas na *internet*. Supõe-se que a técnica utilizada para inserção do código *Stuxnet* nos computadores alvos foi por meio de um dispositivo de mídia removível (*pen-drive*) trazido por um dos funcionários internos. A infecção extrapolou o objetivo e o código malicioso foi encontrado em outros Estados (FIG. 3) (SYMANTEC, 2010).

[16] Vulnerabilidades *Zero-Day* – são vulnerabilidades existentes em sistemas que ainda não possuem correção.

[17] Certificado Digital é o documento eletrônico ou arquivo de computador que contém um conjunto de informações referentes a entidade para o qual o certificado foi emitido (seja uma empresa, pessoa física ou computador) mais a chave pública referente a chave privada que acredita-se ser de posse unicamente da entidade especificada no certificado.

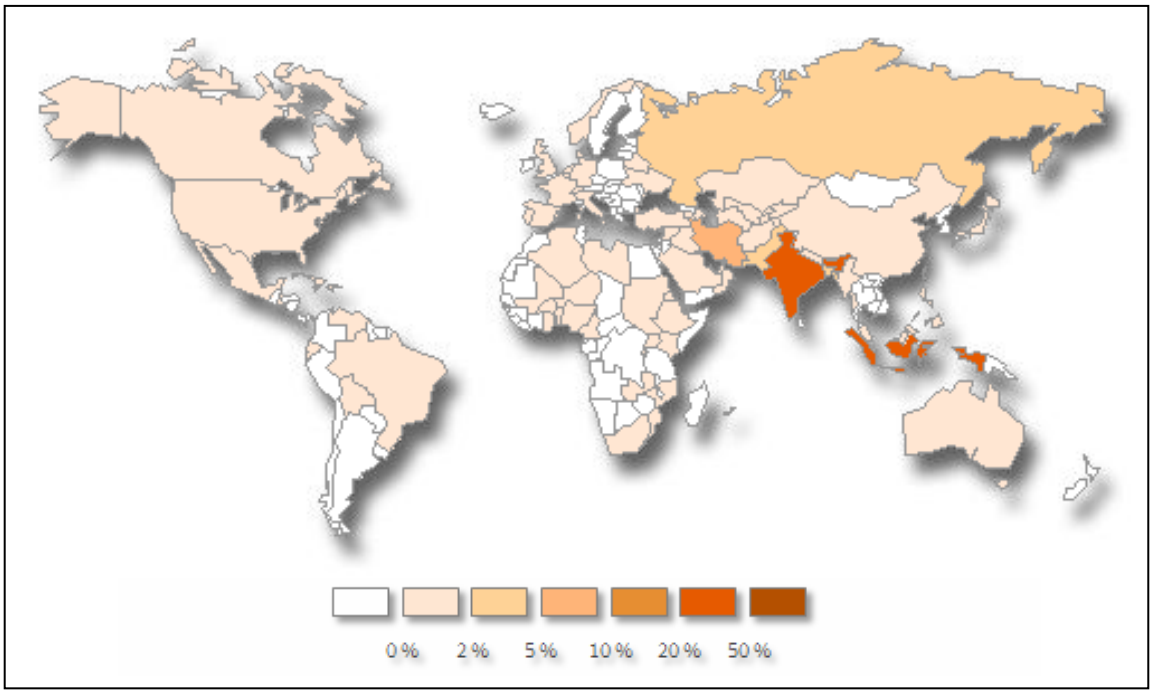

FIGURA 3 - Distribuição geográfica do STUXNET (% de computadores da rede com vírus).
Fonte: SYMANTEC, 2010.

Mesmo adotando procedimentos de segurança e de controle nas organizações na tentativa de isolar o sistema, basta uma brecha ou falha de segurança para que um ataque cibernético tenha sucesso. O problema é que podem existir falhas nos sistemas que foram descobertas pelo oponente sem que qualquer outro a conheça. Estas falhas podem fazer parte de um banco de dados de um atacante de modo a escolher qual vetor de ataque poderá utilizar. É importante lembrar que a partir de sua descoberta, a vulnerabilidade pode ser corrigida e medidas de segurança implementadas, diminuindo a eficácia e/ou neutralizando o ataque ao longo do tempo. Conclui-se que o constante monitoramento e adoção de políticas de segurança não são suficientes para a garantia da proteção das redes e dados.

Neste caso também se observa a utilização de uma ação de ataque cibernético, mas sem qualquer relação direta com ataques cinéticos. O Irã não se encontrava em conflito declarado com nenhum outro Estado durante a descoberta do *Stuxnet*. Existem pressões internacionais contra o desenvolvimento de seu projeto nuclear, citam-se as realizadas pelos EUA e por Israel, e o uso da GCiber com ações de ataque com efeitos desejados de destruição

ou neutralização podem vir a retardar seu projeto, contribuindo para a consecução de objetivos estratégicos da política externa de outros Estados.

O papel da Contra-inteligência ganha importância, pois apresenta mais uma camada da segurança ativa em busca da neutralização de possíveis ameaças antes mesmo de suas concretizações. Reforça-se a necessidade de se manter efetivas as ações de proteção cibernéticas.

3.6 Oriente Médio (2012)

Um programa malicioso até então inédito foi descoberto recentemente pela empresa russa de antivírus Kaspersky[18]. Denominado *Flame*, este programa é considerado um "canivete suíço" das ações de exploração e ataque. Nos dispositivos infectados ele grava o áudio, coleta os dados digitados, monitora o tráfego da rede, coleta *screenshots* (imagens de tela) e interage com dispositivos *bluetooth*[19] que estejam próximos da máquina alvo. Trata-se de várias funcionalidades modulares e de um código que pode ter até 20 *Megabytes*[20] se estiver instalado com todos seus módulos (GOSTEV, 2012).

Em sua análise, Gostev (2012) afirma que partes do código possuem similaridades com o código do *Stuxnet,* pois entre outras semelhanças, os dois se aproveitam da mesma vulnerabilidade em sistemas operacionais *Windows* para ativarem suas funcionalidades. No entanto, ainda não foram constatados elementos determinantes para ligar os desenvolvedores de um *software* malicioso ao outro.

Todos os dados trabalhados pelo *Flame* estão disponíveis para os operadores por meio de acesso remoto no *link* de C2 que se conecta a equipamentos servidores ao redor do

[18] A *Kaspersky Lab* é uma empresa multinacional, cuja matriz encontra-se em Moscou.
[19] *Bluetooth*: tecnologia de rede sem fio de curto alcance.
[20] *Megabyte* é uma unidade de medida de informação equivalente a 1000000 *bytes*. Sendo que um *byte* equivalente a 8 *bits*.

globo. O problema agora não é somente a exploração em si, mas a complexa maneira de como as informações são capturadas (MAHER, 2012).

Os principais Estados afetados pelo *Flame* encontram-se no Oriente Médio: Irã, Israel, Palestina, Síria, Líbano, Arábia Saudita. A FIG. 4 apresenta com uma melhor contextualização.

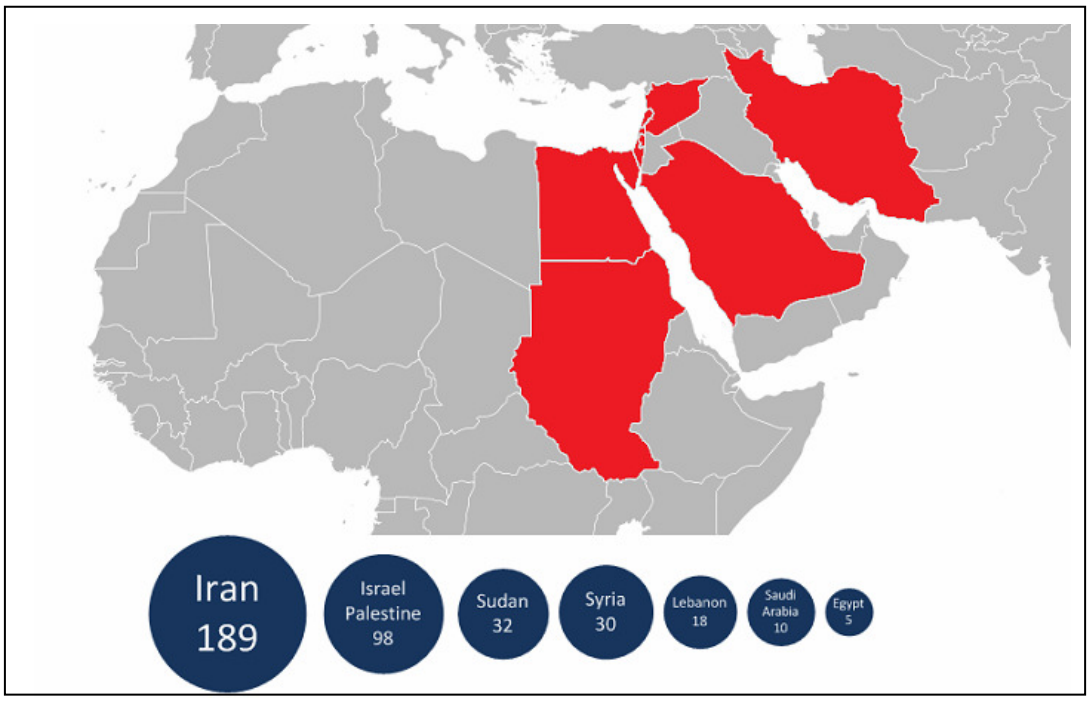

FIGURA 4 - Estados mais afetados pelo programa malicioso Flame.
Fonte: GOSTEV, 2012b.

Não foram observados sinais de indicação de um alvo específico, como o caso do *Stuxnet*, mas a ameaça deste conjunto de ferramentas é enorme. A flexibilidade para implantar módulos de ataque específicos, que podem ser direcionados a dispositivos SCADA, à infraestrutura crítica, às redes de C2 militares, e assim por diante, apresenta uma forma de ataque cibernético difícil de ser combatida isoladamente. Mais do que nunca, a integração dos órgãos de inteligência, de defesa e segurança, faz-se necessária para uma resposta à altura destes ataques.

Apesar do foco atual do *Flame* se encontrar no Oriente Médio, o Brasil e a MB não podem se furtar de estarem prontos para enfrentar este tipo de ameaça. A busca constante do conhecimento e integração dos mecanismos de segurança e defesa deve ser alvo das metas traçadas para a garantia da nossa soberania.

Dos exemplos citados neste capítulo conclui-se que os ataques cibernéticos podem ser utilizados para apoiar ações convencionais, neutralizando estruturas de C2 para ampliar e garantir liberdade de ação; para apoio às OpPsi, como na divulgação de propaganda para desmoralizar o adversário, distribuição de *e-mails* e outro tipo de mídia na i*nternet,* no lugar de panfletos em meio físico; e até mesmo para ações exclusivamente cibernéticas, com efeitos desejados de destruição ou neutralização de alvos.

A preocupação com o surgimento de novas tecnologias e na maneira como são tratadas as informações deve ser constante. Ações de exploração cibernéticas relacionadas ao levantamento e coleta de dados de inteligência podem ser realizadas de uma maneira ostensiva, particularmente quando se referem às redes sociais. Estas informações podem ser trabalhadas e utilizadas a fim de maximizar o impacto no caso de ataques cibernéticos.

A velocidade e capilaridade das redes vão além das capacidades de qualquer mecanismo de defesa cinético que possa ser implementado para a defesa de um Estado. As vulnerabilidades devem ser tratadas rapidamente com investimentos em capacitação de pessoal e tecnologia, fazendo com que os usuários e sistemas de TI não venham a ser surpreendidos no caso de um conflito cibernético, ou, caso ocorra desta forma, que as respostas sejam rápidas e a resiliência[21] das redes seja mantida.

Quanto maior a dependência tecnológica de um Estado, maiores serão os riscos e impactos de um ataque cibernético. A possibilidade de uma suposta coordenação de atores não estatais em ações cibernéticas e a dificuldade da confirmação da identidade de quem está

[21] Resiliência: É o poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.

patrocinando ou operando o ataque durante um conflito contribuem para ampliar a dificuldade da defesa.

Os códigos maliciosos como o *Stuxnet* e o *Flame* demonstram a evolução e sofisticação no desenvolvimento de artefatos e permitem a execução de um amplo espectro de ações exploratórias ou de ataques.

Para tentar resolver a questão são necessários acordos de cooperação, de inteligência e de interoperabilidades nacionais e internacionais, de modo a somar forças para criar uma eficiente e eficaz estrutura para fazer frente a estes ataques. Isto posto, serão elencadas no próximo capítulo as ações que a MB vem adotando em prol de sua segurança e defesa cibernética.

4 A GUERRA CIBERNÉTICA NA MARINHA DO BRASIL

Este capítulo apresenta e analisa as ações que estão sendo realizadas no âmbito do Brasil e da MB relativas à defesa e GCiber com a finalidade de contribuir para a melhoria da percepção dos riscos e da necessidade de busca contínua do aperfeiçoamento das capacidades operacionais da MB para enfrentar as ameaças cibernéticas citadas e daquelas que futuramente surgirão.

4.1 Defesa Cibernética no Brasil

Os temas segurança e DC vêm sendo discutidos e construídos no Brasil, no âmbito da APF, pois são assuntos de importância para a segurança do Estado. Como visto nos capítulos anteriores, as novas exigências para a proteção tornaram-se um grande desafio para os atores governamentais. A manutenção e preservação das infraestruturas críticas, tais como energia, transporte, telecomunicações, abastecimento, finanças, informação, dentre outras fazem parte deste contexto, bem como a atuação das Forças Armadas, nos casos de ameaça à soberania, previstos em lei (BRASIL 2010).

Na legislação brasileira e nos documentos atinentes aos temas já existem definições de responsabilidades e competências a órgãos federais para o trato com a segurança cibernética, como por exemplo a Estratégia Nacional de Defesa (END), que atribuiu ao MD o fortalecimento dos setores essenciais para a Defesa Nacional: o cibernético, o nuclear e o espacial, cujos responsáveis são o Exército Brasileiro (EB), a MB e a Força Aérea Brasileira (FAB), respectivamente (BRASIL, 2008).

O Livro Verde - Segurança Cibernética no Brasil, produzido pelo GSI/PR e lançado em 2010, reúne propostas de diretrizes básicas, visando iniciar amplo debate social,

econômico, político e técnico-científico sobre o tema, dada a complexidade do cenário mundial (BRASIL, 2010).

Para atender ao solicitado na END, ações no nível estratégico estão sendo tomadas. A criação Centro de Defesa Cibernético (CDCIBER)[22] do Comando do Exército é um exemplo. Trata-se de um órgão de nível estratégico que atua em prol da defesa cibernética nacional. O CDCIBER participou ativamente de sua primeira missão no monitoramento de rede da Rio+20, Conferência da Organização das Nações Unidas (ONU) para Desenvolvimento Sustentado que ocorreu de 20 a 22 de julho de 2012, reunindo cerca de cem chefes de Estado e de governo. O foco do trabalho permaneceu na ação colaborativa entre vetores de defesa, envolvendo setores como os de Segurança Pública, Ministério das Relações Exteriores (MRE), SERPRO[23], dentre outros. A atuação do Centro também ocorrerá nos grandes eventos como Copa do Mundo (2014) e Olimpíadas (2016)[24].

O primeiro comandante do CDCIBER, General-de-Divisão José Carlos dos Santos (2012), define a estratégia operacional do Centro como sendo a de atuar em defesa-ativa para fazer frente às ameaças do mundo moderno, alinhada à política de relações internacionais brasileira, citando:

> Nossa política é de defesa-ativa. Não buscamos atacar outras nações, o que queremos é proteger nossos sistemas. Quem sabe fazer a defesa, sabe que arma foi usada e também pode atacar, mas só pensamos nisso dentro de uma estratégia de neutralizar uma fonte de ataque, não fora dela (SANTOS, 2012).

A MB tem atuações firmes relacionadas à DC que colaboram para a segurança da instituição e do governo, o que será abordado nas próximas páginas.

---

[22] As normas relativas ao CDCIBER encontram-se dispostas em: <http://200.20.16.3/guardiao/controle.php?modulo=consulta&tela=legislacoes&acao=consultar&menu=0&rodape=0&idTipoLegislacao=&idAreaAtuacao=&idAssunto=242&idOrg=19&idFunc=3>. Acesso em: 15 de junho de 2012.

[23] SERPRO - Serviço Federal de Processamento de Dados - Serpro é uma empresa pública vinculada ao Ministério da Fazenda. Foi criada no dia 1º de dezembro de 1964, pela Lei nº 4.516, com o objetivo de modernizar e dar agilidade a setores estratégicos da Administração Pública brasileira. A empresa, cujo negócio é a prestação de serviços em Tecnologia da Informação e Comunicações para o setor público, é considerada uma das maiores organizações públicas de TI no mundo.

[24] Disponível em: <http://www.exercito.gov.br/c/journal/view_article_content?groupId=18107& article Id=1663967&version=1.0>. Acesso em: 10 de maio de 2012.

4.2 A Marinha do Brasil e a Guerra Cibernética

A MB possui uma rede de dados própria, institucional, chamada de Rede de Comunicações Integradas da Marinha (RECIM) que é a infraestrutura responsável pelo tráfego de informações digitais e analógicas no âmbito da MB. É constituída por vários enlaces e linhas de comunicação interligando as redes locais e metropolitanas dos Distritos Navais. O tráfego de acesso à *internet* utiliza essa malha de comunicações, compartilhando-a com o tráfego de aplicações consideradas mais relevantes da rede corporativa, tais como: o tráfego de sistemas operativos de C2, o acesso aos sistemas e serviços na rede do SERPRO, os sistemas digitais administrativos, os sistemas de Voz sobre IP (VoIP), o gerenciamento da RECIM e outras aplicações comuns da *intranet* (BRASIL, 2009).

A RECIM possui dispositivos de conexão e barreiras de segurança que permitem sua interligação segura à *internet* e a outras redes de interesse da MB. Inclui-se neste aspecto, o Sistema de Comunicações Militares por Satélite (SISCOMIS), que tem por finalidade atender a Estrutura Militar de Defesa (EMiD) (BRASIL, 2009).

A fim de melhor se organizar para a gestão da TI, tendo em vista a complexidade do mundo moderno e dos problemas relativos às novas ameaças cibernéticas, a MB se reestruturou em 2007, criando a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) e o Centro de Tecnologia da Informação da Marinha (CTIM).

A DCTIM é o Órgão de Direção Especializada, coordenador da TI no nível estratégico da MB, e tem dentre suas funções a competência na elaboração, na revisão e no gerenciamento das normas gerais para a Segurança das Informações Digitais (SID). Exerce dentro de suas atividades: a coordenação, a execução e a análise dos projetos que impliquem atividades de SID e de GCiber (BRASIL, 2009).

O CTIM é o órgão de execução no nível operacional, cuja competência, dentre outras, é a de executar as atividades técnicas de GCiber, sob coordenação da DCTIM. Encontram-se em seu escopo de trabalho as atividades de manutenção de registros de acesso aos recursos de TI da RECIM e de incidentes de segurança; realização de auditoria de SID; analise de vulnerabilidades de sistemas de TI; avaliação técnica dos recursos de SID (antivírus, *firewalls*, proteção contra intrusos etc.); gerenciamento e manutenção dos recursos criptográficos; dentre outras. Possui uma Equipe de Tratamento e Respostas a Incidentes de Redes (ETIR-MB), que atua frente às ameaças cibernéticas provendo uma camada de segurança alinhada às melhores práticas internacionais (BRASIL, 2009). Constata-se que grande parcela das ações executadas são as do tipo proteção cibernética, com fins defensivos, cuja abrangência é focada na neutralização de ataques e exploração realizados pelo oponente, incrementando as ações de segurança cibernética.

Na estrutura administrativa encontram-se os Centros Locais de Tecnologia da Informação (CLTI) que são elementos organizacionais de apoio com tarefas como a de efetuar o controle operacional e administrativo das redes (dados, voz e vídeo) de sua área de jurisdição, apoiando, por solicitação da Organização Militar (OM), ou caso considere necessário, na resolução de incidentes, de forma a garantir a operação adequada da RECIM e dos seus serviços. É o CLTI que apoia o CTIM na resolução de todo e qualquer tipo de incidente relativo às redes (BRASIL, 2009).

Em cada OM ainda existem os Oficiais de Segurança das Informações Digitais (OSID) e os Administradores de Redes Locais (ADMIN), que atuam nas camadas mais baixas da organização. Quando ocorrem incidentes sem condições de resolução no âmbito local, os ADMIN concentram as solicitações de usuários, e encaminham ao suporte da RECIM, no CTIM, que aciona, em caso de necessidade, o CLTI da respectiva área de jurisdição.

Fazem parte da estrutura de TI da MB o Conselho de Tecnologia de Informação da Marinha (COTIM) e a Comissão Técnica de TI (COTEC-TI), que atuam no âmbito da gestão e tomada de decisões. Na figura abaixo se visualiza a estrutura de Gestão de Segurança da Informação e Comunicações da MB (FIG 5) (BRASIL, 2009).

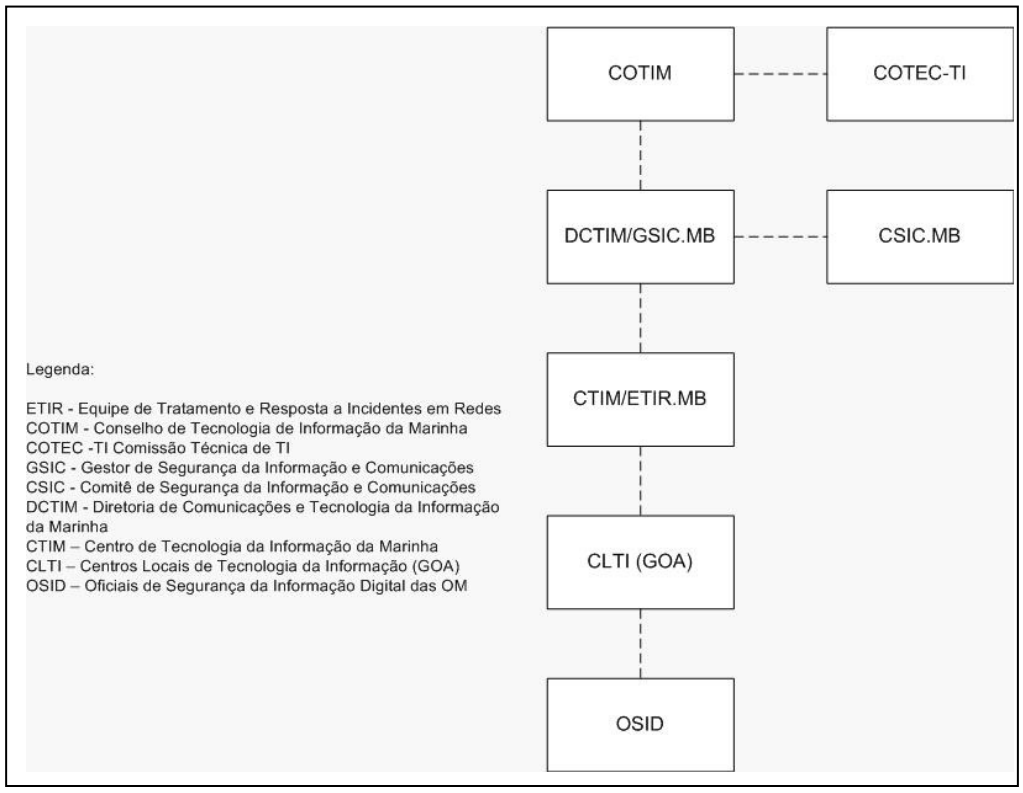

FIGURA 5: Estrutura de Gestão de Segurança da Informação e Comunicações na MB.
Fonte: (BRASIL, 2009).

Quando se trata do setor operativo, as Comunicações Navais (CN) são gerenciadas pelo Comando de Operações Navais (ComOpNav), cuja dependência e ligação com a RECIM para a execução desta tarefa é plena. As redes de C2 estabelecidas com os tropas, navios, aeronaves e forças, propiciam a troca de informações e facilitam a tomada de decisões dos comandantes participantes, porém, cabe ressaltar que, mesmo quando se utilizam redes extra-MB, faz-se necessária sua interligação com a RECIM. É a RECIM que proverá as CN e a interconexão com os sistemas da MB, sendo um importante ativo a ser preservado.

Apesar das forças envolvidas serem subordinadas ao ComOpNav, a responsabilidade pelo controle e monitoramento da RECIM é do CTIM.

O assessoramento ao Comandante de Operações Navais (CON) nos assuntos concernentes à inteligência tecnológica voltada para a segurança da informação e assuntos relativos à GCiber cabe à Subchefia de Inteligência Operacional (CON-20). Subordinada a essa Subchefia encontra-se a Divisão de Contra-inteligência (CON-23) que atua na área empregando a Seção de Segurança da Informação e Operações Cibernéticas (CON-23.2) (BRASIL, 2008b).

A MB participa ativamente de reuniões e simpósios para discussão e aprimoramento das questões ligadas ao tema DC. Durante o Simpósio com o tema "Segurança e Defesa Cibernética", realizado na Escola de Comando e Estado Maior do Exército (ECEME), em maio de 2012, no IX Ciclo de Estudos Estratégicos, a MB apresentou os conceitos e definições, princípios, estabelecimento de ações, condutas, situações de C2, bem como as áreas de pesquisa e desenvolvimento e capacitação do pessoal que fazem parte da doutrina de GCiber da instituição. Seja em situação de paz ou de crise envolvendo ameaças cibernéticas faz-se necessário o monitoramento do *status quo* das redes da MB. Com este fim, emprega-se um sistema de alarmes, divididos em cinco níveis (branco, azul, amarelo, laranja e vermelho), sendo que estes identificariam a situação ou condição de defesa da RECIM. Em situação cotidiana e administrativa, os alarmes estariam nas cores branco, azul e amarelo e a DCTIM seria a responsável pelas ações de defesa. Para o caso de eventos de maior magnitude e impacto na segurança da RECIM, os alarmes se alterariam para as cores laranja e vermelho, conforme criticidade, e as ações de GCiber entrariam numa fase operacional sob coordenação do ComOpNav (VIANNA, 2012).

Com a finalidade de aumentar a segurança da informação nos sítios e sistemas da MB, o Centro de Análises de Sistemas Navais (CASNAV) vem desenvolvendo sua capacidade, investindo em novos processos, tecnologias e treinamento de pessoas nas áreas de Criptologia, Análise de Vulnerabilidade de *Softwares*, Técnicas de Varredura e Desenvolvimento Seguro. Para apoiar as ações de proteção cibernéticas, o projeto Guerra Cibernética Objetiva (GUERCIB) desenvolve *softwares* inteligentes para minimizar ataques praticados nos sistemas de informações digitais da MB[25]. Todos esses relevantes projetos e ações de Ciência, Tecnologia e Inovação têm como meta contribuir na estratégia da GCiber que a MB está adotando para proteger com eficiência as fronteiras digitais do Estado brasileiro.

Ademais, a busca contínua de conhecimento e o desenvolvimento de sua capacidade de GCiber da MB pode ser ressaltada no investimento realizado em seu capital intelectual, cujo planejamento[26] da capacitação do pessoal da MB nas áreas de conhecimento de TI é estruturado em razão das dificuldades que se apresentavam nos cenários tecnológicos e econômicos do país (BRASIL, 2009)

Em relação ao setor operativo, a MB tem realizado exercícios internos, planejamento conjuntos em âmbito nacional e internacional a fim de aprimorar a capacidade operacional da força. O relacionamento com outras forças e a simulação de eventos tem propiciado um melhor entendimento dos métodos de emprego da GCiber, englobando as ações previstas na Doutrina Militar Conjunta do MD, cuja construção do conhecimento se encontra em plena atividade (VIANNA, 2012).

Pelo exposto, existem na estrutura de TI da MB, mecanismos que atuam em prol das ações de GCiber. É perceptível a grande dependência da TI nas tarefas rotineiras, o que torna o espaço cibernético da MB vulnerável à atuação das ameaças cibernéticas.

---

[25] Disponível em: <http://casnav.mar.mil.br/casnav/site/index.php/noticia/12>. Acesso em: 18 de junho 2012.
[26] Os dados encontrados no Plano de Capacitação do Pessoal de Tecnologia da Informação e Comunicações da Marinha (PLACAPE-TIC).

Entretanto, a MB tem atuado de maneira pró-ativa e significativa para minimizar os riscos das ameaças cibernéticas, e também na ampliação de sua capacidade de GCiber, seja na busca contínua de conhecimento, no investimentos em sua infraestrutura, e na participação de exercícios operativos, reuniões e simpósios. É fato que estes esforços são louváveis, mas ainda não são plenamente suficientes para enfrentar as ameaças cibernéticas que crescem em volume e sofisticação.

Os desafios modernos e futuros dos campos de batalha tornam a GCiber é uma realidade e, mesmo que parte considerável dos esforços esteja nas ações defensivas, a MB não pode abrir mão do contínuo desenvolvimento de suas capacidades ofensivas para executar ações de exploração e de ataque.

5 CONCLUSÃO

No decorrer deste trabalho foram analisados e apresentados os conceitos e definições da GCiber e das ameaças cibernéticas. As ações cibernéticas podem ser realizadas por atores estatais ou não, e encontram-se no espaço cibernético, uma nova dimensão de conflito (cibernética), criada e controlada pelo homem que interage com as demais dimensões clássicas: marítima, aérea, terrestre e espacial. Seus efeitos desejados podem variar de acordo com a motivação e abrangem a perda da integridade, disponibilidade, confidencialidade e destruição. Percebe-se claramente o paradoxo da maior vulnerabilidade do mais forte, característica marcante da assimetria, proporcionada pelas ações cibernéticas, que são reais, rápidas, complexas e não se limitam em fronteiras físicas e geopolíticas.

As ações cibernéticas são classificadas conforme seu emprego: de exploração, de ataque e de proteção; e os riscos envolvidos são cada vez mais percebidos pelas sociedades, pois podem afetá-las severamente, seja no âmbito da segurança ou economicamente, como por exemplo: a possibilidade de afetar as infraestruturas críticas de um Estado.

Depreendeu-se então que a GCiber não pode ser considerada como somente uma ameaça, mas também como um recurso significativo dos Estados para alcançar seus objetivos estratégicos. No caso de seu emprego como um meio disponível para o Estado, as ações cibernéticas podem ser realizadas durante a preparação do campo de batalha de forma a reduzir o poder de influência do oponente e conquistar uma maior liberdade para a manobra.

Ao analisar as ameaças cibernéticas, verificou-se que existe uma grande dificuldade de se identificar a autoria de um ataque. Outra característica marcante é que as ações cibernéticas podem extrapolar o Teatro de Operações e as fronteiras físicas do Estado.

Reconheceu-se a constante evolução das ações de ataque e exploração, cada vez mais complexas e sofisticadas. O emprego da GCiber em conjunto com a OpPsi, confirmaram

a idéia de que ambas fazem parte das Operações de Informações, impulsionando e catalisando os efeitos desejados.

Existe uma tendência de desequilíbrio entre ataque e defesa, exigindo mudanças na capacidade de defesa, particularmente nas ações de proteção, como a necessidade de se implementar sistemas dotados de inteligência artificial, e de ampliar as ações de Contra-inteligência.

No Brasil, iniciativas louváveis têm surgido para enfrentar as ameaças cibernéticas. Citam-se a criação do CDCiber e a produção do Livro Verde, ambos em 2010. Aquele atua no nível estratégico coordenando as ações da DC do Estado, enquanto que este atua no nível político, abordando a segurança cibernética, reunindo propostas e ampliando o debate social, econômico, político e técnico científico sobre o tema.

Ao analisar a estrutura de GCiber da MB, identificou-se que parcela considerável dos recursos de TI atuam em prol das ações de proteção cibernética. Entretanto, a MB não pode abrir mão do contínuo desenvolvimento de suas capacidades ofensivas para executar ações de exploração e de ataque. A atuação da instituição de maneira pró-ativa e significativa na busca contínua de conhecimento, nos investimentos em infraestrutura, na participação de exercícios operativos, reuniões e simpósios, contribuem para minimização dos riscos, e principalmente, na ampliação de sua capacidade operacional.

Portanto, com base nas considerações tecidas e nas análises efetuadas no desenvolvimento deste trabalho, estima-se ter atingido o propósito de ampliar a discussão, de forma sucinta, em torno do tema GCiber, considerando os aspectos relativos às ameaças cibernéticas, como suas características (atores, ações, efeitos desejados etc.), enumerando casos concretos e seus aprendizados, e na maneira como a MB encontra-se estruturada para enfrentar os novos desafios, contribuindo para melhorar a percepção da necessidade de busca contínua do aperfeiçoamento das capacidades operacionais da força naval.

REFERÊNCIAS

ARQUILLA, John; RONFELDT, David. **Networks and Netwars**: The Future of Terror, Crime, and Militancy. Santa Monica: RAND, 2001. 288p.

BRASIL. Decreto n. 6.703 de 18 de dezembro de 2008. **Aprova a Estratégia Nacional de Defesa, e dá outras providências.** Diário Oficial [da República Federativa do Brasil], Brasília, DF, 19 dez. 2008, Seção 1, p. 4, Disponível em: <https:// www.defesa.gov.br/eventos_temporarios/2009/estrategia/arquivos/estrategia_defesa_nacional _portugues.pdf>. Acesso em: 15 mai. 2012.

BRASIL. Diretoria-Geral do Material da Marinha. **DGMM-540**: Normas de Tecnologia da Informação da Marinha. 1 rev. Rio de Janeiro, 2009.

BRASIL. **Livro verde**: Segurança Cibernética no Brasil/ Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010. 63 p. Disponível em: <http://dsic.planalto.gov.br/documentos/ publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 08 maio de 2012.

BRASIL. Ministério da Defesa. **MD30-M-01**, Doutrina de Operações Conjuntas. 1 vol. Brasília, 2011.

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

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

CARR, Jeffrey. **Cyber Warfare**. 1 ed. Sebastopol, CA: O'Reilly Media inc., 2010. 205p.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber war**: the next threat to national security and what to do about it. New York: Harper Collins, 2010. 290p.

COLEMAN, Kevin; FAVERO, Randy. **Cyber Commander´s eHandbook**: The weaponry & strategies of digital conflict. 2 ed. EUA: Technolytics, 2011. 236p.

DANG S. T. **The Prevention of Cyberterrorism and Cyberwar.** Issue one for the GA First Committee: Disarmament and Internacional Security (DISEC). Vietnam: Old Dominion University, 2011.

DAVOS. **Fórum Econômico Mundial**: Relatório de Riscos Globais de 2012. Davos, 2012. Disponível em: <http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf>. Acesso em: 20 mar. 2012.

EUA, **Joint terminology for cyberspace operations**, Joint Chiefs of Staff, Department of Defense, USA, 2010. Disponível em:<http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>. Acesso em: 20 de maio de 2012.

EUA. **US Army Training and Doctrine Command Deputy Chief of Staff for Intelligence. Handbook No. 1.02**, Critical Infrastructure Threats and Terrorism. EUA, 2006. Disponível em: <http://fas.org/irp/threat/terrorism/sup2.pdf >. Acesso em: 11 maio de 2012.

GOSTEV, Alexander. **Back to Stuxnet**: the missing link. Moscou, 2012. Disponível em: <http://www.securelist.com/en/blog?weblogid=208193568> Acesso em: 20 de junho de 2012.

GOSTEV, Alexander. **The Flame**: questions and answers. Moscou, 2012b. Disponível em: <http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers>. Acesso em: 20 de junho de 2012.

LIBICKI, Martin C. **Cyberdeterrence and cyberwar**. Santa Monica: RAND Corporation, 2009. 214 p.

MAHER. **Identification of a New Targeted Cyber-Attack**. Iran Computer Emergency Response Team – MAHER, 2012. Disponível em: < http://www.certcc.ir/index.php?name =news&file=article&sid=1894>. Acesso em: 10 de março de 2012.

MCAFEE. **Joint Extend McAfee Total Protection for Endpoint with HBGary Digital DNA and Responder.** USA, 2012. Disponível em:<http://www.mcafee.com/us/ resources/solution-briefs/sb-hbgary.pdf>. Acesso em: 20 de maio de 2012.

NATO. **Novas ameaças:** a dimensão cibernética. Bruxelas, 2011. Disponível em: <http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/PT/index.htm>. Acesso em: 20 junho de 2012.

NYE JR., Joseph. **Cooperação e conflito nas relações internacionais**. Tradução de Henrique Amat Rego Monteiro. São Paulo: Gente, 2009. 400 p.

SANTOS José C. **Entrevista sobre Guerra Cibernética**. Brasil, 2011. Disponível em: <http://www.exercito.gov.br/c/journal/view_article_content?groupId=18107&articleId=732319&version=1.0>. Acesso em: 15 de junho de 2011.

SYMANTEC. **W32.Stuxnet**. USA, 2010. Disponível em: < - http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>. Acesso em: 02 de junho de 2012.

SOMMER P., BROWN I., **Reducing systemic cybersecurity risk**, Report for OCDE, Information Systems and Innovation Group, London School of Economics. London: 2011. Disponível em: < http://www.oecd.org/internet/46894657.pdf>. Acesso em: 15 de março de 2012.

VENTRE, Daniel. **Cyberwar and Information Warfare**. London: Ed Wiley, 2011. 412p.

VIANNA, Nilson R. **A defesa cibernética na visão da MB**. Palestra proferida no IX Ciclo de Estudos Estratégicos da Escola de Comando e Estado Maior do Exército (ECEME). Rio de Janeiro, 2012. Disponível em: < http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/ index.php/CEE/XICEE >. Acesso em: 12 de julho de 2012.