GUERRA CIBERNÉTICA: RESPONSABILIDADE DO EXÉRCITO, DEVER DE TODOS

Abner Alves de Melo[1], George Gustavo da Costa Barbosa[1], Jorge Vagner Vieira da Cruz[1], Edson Barbosa de Souza[1], Larissa Lima Ferreira[1], Liliane Correa de Oliveira Klaus[1], José Carlos dos Passos[1], Luiz Rosado Costa[1], Victor Sardinha Bexiga[1], Nilo Sérgio de Lima Barros e Silva[2]

Resumo**:** A guerra do século XXI não conhece fronteiras: os conflitos são interconectados na velocidade de um clique. A disputa é pelo controle dos sistemas informatizados, que hoje são essenciais para o modo de vida de boa parte da população, como por exemplo os responsáveis pela distribuição de energia elétrica, de água, transporte e pelos serviços de urgência. No contexto da guerra cibernética, cresce a importância de uma nação desenvolver sistemas de defesa visando assegurar a manutenção desses serviços e impedir que as ameaças virtuais se transformem numa realidade caótica. O Exército Brasileiro recebeu a missão constitucional de estruturar a defesa do País para esse novo campo. Este trabalho, a partir de revisão bibliográfica que considerou trabalhos desde as origens do termo "cibernética" até as mais recentes produções científicas, tem o objetivo de contribuir para a difusão do tema, tanto nas Forças Armadas como para o público civil. Desta maneira, foram abordados tanto os aspectos técnicos, que baseiam a discussão sobre a guerra cibernética, quanto os elementos legais internacionais e nacionais envolvendo o tema. Concluiu-se que, apesar de a legislação atual sobre crimes cibernéticos e o papel do governo serem extremamente escassos e abstratos, o Exército tem se empenhado em desenvolver regulamentos próprios e oferecer subsídios para que o Poder Legislativo nacional cumpra o seu papel.

1 1º Tenentes do Quadro Complementar de Oficiais e do Serviço de Saúde (turma de 2011). Escola de Formação Complementar do Exército. Salvador, Brasil. sisdefesa@googlegroups.com

2 Maj QCO/Informática, Mestre em Ciência da Computação pela UNB, Instrutor da EsFCEx nilosergiob@gmail.com

Palavras-chave: Guerra Cibernética. Crimes Cibernéticos. Sistemas de Defesa.

Abstract**:** The twenty-first century war knows no borders, conflicts are instantaneously interconnected. The dispute is about obtaining control over computer systems that are now essential to the way of life of considerable part of the population, for example, involving electricity and water distribution, transport systems and emergency services. In the context of cyber war, a nation is now supposed to develop its defense systems in order to ensure the maintenance of these services and to avoid that cyber threats become a chaotic reality. The Brazilian Army was given the legal task to structure the country's defense within this context. This work, based on a literature review considering studies carried out from the origins of the term "cybernetics" to the most recent scientific research, aims to contribute in presenting the issue, both to the military and to the public audience. Thus, both technical aspects that underlie the discussion of cyberwar and the international and national legal elements involving the subject, were addressed. We came to the conclusion that, despite the extremely scarce and abstract current legislation on cybercrimes and the role of government, the Army has been engaged in developing their own regulations and in providing help for the national legislative power to fulfill its role.

Key-words: Cyber War. Cybercrime. Defense Systems.

1 Introdução

As ações de hackers e os ataques a sites oficiais do Governo Brasileiro motivaram, num ritmo cada vez mais frenético, manchetes no noticiário em 2011. As notícias nomeiam de "guerra cibernética" qualquer uma dessas atividades e colocam em xeque a preparação dos órgãos de defesa diante dessas ameaças.

A defesa da soberania nacional é dever constitucional das Forças Armadas. Numa guerra cibernética que envolvesse o Brasil, alvos cruciais seriam as "infraestruturas críticas", ou seja, os setores energéticos, financeiro, bancário, de transportes, telecomunicações, fornecimento de água, órgãos de defesa, segurança pública e polos tecnológicos.

Diante desse contexto, cabe ao Exército Brasileiro a responsabilidade específica sobre a Guerra Cibernética, segundo a Estratégia Nacional de Defesa.

Como procedimentos metodológicos, realizou-se os seguintes levantamentos como passos interdependentes para a realização de nossa pesquisa: referências científicas relevantes para contextualizar a Guerra Cibernética; legislação nacional existente sobre o assunto; legislação internacional existente sobre o assunto; legislação e regulamentos existentes nas Forças Armadas sobre o assunto; casos mais atuais; aspectos técnicos importantes; e estratégias de comunicação social que possam ser relacionadas com o assunto.

Como objetivos específicos, a pesquisa se propôs a registrar discussões sobre o próprio conceito de Guerra Cibernética, resgatar a legislação nacional e internacional que envolve o tema e contextualizar os conflitos de guerra cibernética com casos recentes. O trabalho pretende apontar a necessidade de uma estratégia de comunicação social para que o Exército se relacione de forma eficiente com seu público de interesse, especialmente os usuários de sistemas informatizados. Para tanto propôs-se atingir os seguintes objetivos específicos:

2 Guerra Cibernética: Definições e Técnicas

No âmbito das ciências militares, a guerra cibernética pode ser considerada um objeto recente de situar as ameaças com as quais

se deparam os estrategistas de segurança. Fazendo uma analogia, a cibernética pode ser relacionada com o comando e o controle de informações em máquinas ou seres vivos.

Para definir uma guerra por vias cibernéticas, é preciso que ela esteja inserida na disputa entre nações. Apesar da diversidade de definições, é notória a existência de um aspecto consensual, onde, para ocorrer uma Guerra Cibernética, é necessário um patrocínio estatal, pois as ações oriundas de um indivíduo com motivações pessoais, não podem ser consideradas como Guerra Cibernética, embora possam ser igualmente prejudiciais. (STOPATTO, 2009, p. 215)

Uma peculiaridade da guerra no mundo cibernético seria o princípio da proximidade. No mundo virtual, ela não precisa existir para que uma ação seja bem sucedida, pois do outro lado do mundo, é possível assumir o controle de um sistema de vital importância para a defesa do inimigo. Algumas medidas preventivas podem ser adotadas pelo Exército Brasileiro no que se refere à prevenção de ataques cibernéticos. Uma delas é a adoção de um sistema periódico de auditoria (logs), possibilitando verificar, a todo o momento, como andam as defesas do Exército Brasileiro em face às ameaças existentes.

Internacionalmente, também há estudos e cada vez mais institucionalização de ações de preparo para a guerra no ciberespaço. O Estado também pode comandar um ciber-ataque interno, conseguindo que um operador infiltrado introduza formas de "enganar" o sistema, tornando-o mais vulnerável. O interesse estatal também pode originar uma ameaça interna interagindo com a parte física da rede, ou seja, os computadores. Basta vender máquinas ou aparelhos eletrônicos a outros países com componentes programados para causarem determinadas vulnerabilidades.

2.1 Vulnerabilidades

O termo "vulnerabilidade" pode ser definido como um problema ou ponto fraco que pode ser explorado ou atacado. Em Tecnologia da Informação, significa "haver brecha em um sistema", em que se aproveita das falhas de outros programas, a fim de se obter acesso não autorizado aos

sistemas. Ela também é definida como falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, pode resultar na violação da segurança de um sistema computacional. Uma vulnerabilidade pode ser uma simples falha ou uma série de pontos fracos que acabam permitindo uma ou várias ameaças. Existem ferramentas específicas para se explorar as vulnerabilidades, cada qual para uma respectiva vulnerabilidade a ser explorada. Normalmente, para que uma "brecha no sistema" ocorra é necessário que alguns passos sejam negligenciados pelo fator humano. A maioria das vulnerabilidades apresentadas pelos principais sistemas operacionais pode ser descoberta ou detectada por ferramentas automatizadas especialmente desenvolvidas para esse fim. Essas ferramentas são chamadas de Softwares de Varredura, ou simplesmente *Scanners*. Para evitar que cibercriminosos explorem as vulnerabilidades, as organizações precisam se concentrar em diminuir a janela de tempo entre a descoberta da

2.2 Ataques cibernéticos

De acordo com o Glossário das Forças Armadas (BRASIL, 2007), defesa é entendida como "o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança", ou ainda, como "reação contra qualquer ataque ou agressão real ou iminente". O mesmo glossário define "ataque" como "ato ou efeito de dirigir uma ação ofensiva contra o inimigo" e GC (Guerra Cibernética) como "Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores".

2.3 Crimes de Informática

É importante delimitarmos o que hoje é considerado crime no meio virtual. Podemos caracterizar alguns tipos de cibercrimes, tais como acesso indevido aos sistemas de computador ter acesso ou tentar ganhar acesso, indevidamente, a um sistema de

computador ou a uma rede de computadores, fazendo o sistema produzir alguma função. O agente deve estar ciente, no momento do crime, que ele não estava autorizado a ter acesso ao sistema. O agente pode cometer tal crime fisicamente ou remotamente. Como crime, podemos citar:

- violação de sistemas de processamento de dados através de senha de outrem: utilizar senha de outrem sem a devida autorização com o intuito de ganhar acesso ao computador ou a rede de computadores.

- fraude através do uso do computador: apropriar-se indevidamente de valores através da manipulação de qualquer sistema de processamento de dados, obtendo assim vantagem econômica para si ou para outrem.

- furto de informações contidas no computador: apropriar-se indevidamente de informações contidas em qualquer sistema de processamento de dados, seja temporária ou permanentemente.

- sabotagem: impedir ou prevenir o funcionamento de um computador ou de um programa de computador, temporária ou permanentemente, interferindo no sistema de forma a causar distúrbios no mesmo.

2.4 Criptografia, cidadania e o ciberterrorismo

A história mostra que o homem, desde a antiguidade, busca o aprimoramento contínuo no processo de comunicação. Após o surgimento da escrita, as relações humanas e o convívio em sociedade foram extremamente facilitados. Esse processo evolutivo da comunicação tem sido acompanhado pela preocupação com a segurança da informação. Informações, muitas vezes vitais a uma instituição ou indivíduo, são sempre alvos de adversários de natureza política ou militar que buscam vingança, poder e sabedoria ou, até mesmo, alvos de simples curiosos.

A criptografia surgiu a cerca de 2000 anos a.C. como uma área especializada em produzir meios para escrever de forma secreta. As maneiras de criptografar escritas evoluíram com o tempo, conforme necessidade de se aprimorar essas técnicas, evitando-se que fossem "quebradas" e descobertas por intermédio da criptoanálise. Criptoanálise pode ser definida

como a arte de desenvolver técnicas que permitam decifrar uma mensagem codificada com finalidades diversas, como descobrir seu conteúdo ou até mesmo modificá-lo.

Os sistemas criptográficos são utilizados pelos cidadãos, em suas transações, em larga escala, no intuito de propiciar sigilo, protegendo a informação contra ataques passivos que pretendem conhecê-las; autenticidade, assegurando que a comunicação seja autêntica; integridade, garantindo que o conteúdo da informação não seja alterado; não repúdio, impedindo o transmissor ou receptor de negar a mensagem; controle de acesso, restringindo o acesso aos sistemas informatizados e disponibilidade, evitando perda ou redução da disponibilidade da informação.

Independentemente do desenvolvimento da tecnologia ou de batalhas travadas numa guerra do medo, o que importa é fazer valer a liberdade civil lutando na defesa contínua pelos preceitos da cidadania.

3 Casos Recentes de Ataques Cibernéticos

A realidade da Guerra Digital ultrapassou um nível mais profundo de aperfeiçoamento. Existem armas invisíveis que podem atingir qualquer ponto do planeta e, com apenas um "click", causar um blackout, uma enchente, uma pane completa nos sistemas de controle de vôo ou de navegação, até mesmo o acionamento involuntário de reatores nucleares. Ataques a redes de computadores são cada vez mais comuns, causando diversos danos e milhões de dólares em prejuízos financeiros.

Esta ameaça está se desenvolvendo rapidamente como uma ferramenta de guerra em todo o mundo.

3.1 A gênese: o primeiro vírus de computador

Criado por Bob Thomas em 1971, o primeiro vírus de computador invadia o sistema e postava uma mensagem inocente na tela, dizendo "*I´m the Creeper, catch-me IF you can*! (Eu sou assustador, pegue-me se for capaz). Conjuntamente ao primeiro vírus foi criado o primeiro anti-vírus chamado "*The Reaper*" que tinha como serventia eliminar o *The*

Creeper. O primeiro vírus da história não roubava ou destruía dados, nem mesmo sobrecarregava o sistema.

3.2 Estônia, abril de 2007

Após a retirada de um monumento em homenagem aos soldados russos que combateram os nazistas na segunda guerra, as relações entre Estônia e Rússia ficaram profundamente abaladas e, segundo o governo estoniano, foram o estopim de um grande ataque cibernético sofrido por este país. O ataque foi um bombardeamento de informações que sobrecarregaram o sistema digital da Estônia. Para isso, os hackers espalharam programas invasores em milhares de computadores pelo mundo, que, com um simples comando, entupiram com lixo eletrônico as máquinas estonianas, que pifaram sem conseguir atender à avalanche de informação.

3.3 Irã, 2007 e 2011 - *Stuxnet*

Apesar de ter se revelado poucos detalhes sobre o vírus, o Stuxnet atacou o sistema de controle de uma usina nuclear no Irã. Segundo o embaixador da Rússia à OTAN, o vírus tinha atingido o sistema de Computação em Bushehr, colocando o risco de uma catástrofe nuclear de dimensão idêntica a do acidente de Chernobyl em 1986, na Ucrânia, então parte da União Soviética. Alguns analistas de defesa dizem que o alvo principal seria provavelmente o enriquecimento de urânio do Irã - o processo que gera combustível para usinas nucleares e que pode fornecer material para o processamento de bombas.

Embora nenhum país ou facção tenha assumido a autoria, apenas Israel e EUA teriam tecnologia para desenvolver um vírus tão elaborado.

4 Ferramentas de Segurança

Existem diversas ferramentas de segurança atualmente, cada qual com suas peculiaridades e finalidades específicas. Abaixo estão relacionadas algumas ferramentas de segurança mais conhecidas e utilizadas por administradores de redes.

NMAP: É uma ferramenta conhecida como *Scanner* de portas, ou seja, ela faz uma

varredura das portas e lista o estado das mesmas. Através dela é possível descobrir falhas e fraquezas na rede da instituição.

Nessus: O *Nessus* é uma ferramenta de varredura remota de vulnerabilidades para sistemas *Linux, BSD, Solaris*. Possui uma *interface GTK* e efetua mais de 1200 verificações remotas de segurança.

Snort: É uma ferramenta muito eficiente conhecida como sistema de detecção de intrusões, capaz de efetuar análises em tempo real de tráfego capturado e registo de datagramas em redes *IP*. Permite a análise de protocolos, procura de conteúdos e pode ser usado para detectar diversos ataques como transbordamentos de memória (*buffer overflows*), levantamentos furtivos (*stealth*) de portos de transporte, ataques usando *CGI*, sondas para *SMB*, tentativas de identificação de sistemas operativos etc.

***Tcpdump*:** É uma ferramenta não gráfica bem conhecida e muito apreciada para análise de tráfego em redes. Pode ser usada para apresentar os cabeçalhos dos datagramas que passam por uma interface de rede e que validam uma regra imposta, e também para detectar problemas de rede ou para monitorar a atividade na rede.

O ***SSH*** (*Secure Shell*) é um programa para iniciar sessões em computadores remotos e neles executar comandos. Fornece um canal de comunicação seguro (cifrado) sobre uma rede insegura entre duas máquinas sem confiança mútua. Foi também concebido para substituir o *rlogin, rsh e rcp* e pode ser usado para fornecer *rdist e rsync* com um canal de comunicação seguro.

5 Princípios do Direito Internacional Humanitário e Guerra Cibernética

Não há regulação específica para a guerra cibernética no âmbito do Direito Internacional Humanitário (DIH) e nem parece ser viável, tendo-se em vista que a velocidade dos avanços tecnológicos não permitiria que fossem criadas convenções específicas precisas e duradouras, sob pena de, se criadas, tornarem-se, em pouco tempo, obsoletas. A novidade dos ataques cibernéticos e a

consequente falta de regulamentação específica, todavia, não podem servir de óbice à aplicação do Direito Internacional Humanitário, levando-se em conta sua imprescindibilidade na ordem internacional por possuir a função primordial de proteger a pessoa humana (e reflexamente os bens) em áreas de conflito.

Estabelecida a aplicação dos princípios de DIH à guerra cibernética, devem os operadores do Direito levar em consideração para sua aplicação a seguinte situação: ao mesmo tempo em que a guerra eletrônica reduz o número de baixas civis, aumenta o potencial de violação a princípios e codificações do DIH, vez que estas violações não gerariam um desgaste político nas proporções do que seria causado com a morte e destruição física direta de alvos civis.

5.1 Legislação Nacional e Atuação do Exército Brasileiro

Em meados de 2005 foi aprovada a Política de Defesa Nacional, pelo Decreto 5.484/05, que dispensou especial atenção à questão da guerra eletrônica envolvendo o Estado Brasileiro, a ponto de reconhecer que os avanços na área de TI (Tecnologia da Informação), dentre outras searas, foi a que mais se destacou e causou preocupação, uma vez que muitas vulnerabilidades foram criadas, com o escopo primordial de inviabilizar o uso de sistemas ou provocar interferência à distância (BRASIL, 2005).

É importante destacar que, antes mesmo de se estabelecer a Política de Defesa Nacional, a Portaria Normativa nº 333 do Ministério da Defesa, de 24 de março de 2004, já instaurava a Política de Guerra Eletrônica, definindo seus objetivos e determinando suas diretrizes. De lá para cá, a importância dada às atividades de guerra eletrônica estão numa crescente constante, a todo tempo, na guerra ou na paz, sempre em busca da prevenção de ataques e, se preciso, derrotando o oponente sem o uso de armas convencionais, preservando-se a defesa e segurança nacionais.

Uma das medidas preliminares do Exército Brasileiro foi a criação, em fevereiro de 2009, do Centro de Comunicações e Guerra Eletrônica (CCOMGEX). Em seguida, precisamente em

agosto de 2010, criou-se o Centro de Defesa Cibernética do Exército (CDCiber). Tais fatos foram seguidos de treinamentos, em parceria com países europeus, principalmente a Espanha, no sentido de que fossem apresentadas aos militares brasileiros as ameaças existentes, a maneira como funcionam, de onde partem e o modo como são construídas.

Em setembro de 2009, a Portaria PR/GSI 45 instituiu o Grupo Técnico de Segurança Cibernética, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), do qual participam integrantes das três Forças. Esse grupo tem o objetivo de propor diretrizes e estratégias para a Segurança Cibernética, no âmbito da Administração Pública Federal.

No que diz respeito à legislação nacional, segundo o Livro Verde (BRASIL, 2007), elaborado pelo Gabinete de Segurança Institucional da Presidência da República, cujo tema é "SEGURANÇA CIBERNÉTICA NO BRASIL", é fato que o ordenamento jurídico brasileiro não dispõe de normas específicas para regular as condutas típicas de uma Batalha Cibernética.

Finalmente, percebe-se que o Estado Brasileiro, em sendo representado pelo Exército Brasileiro, na problemática em discussão, que é a Guerra Cibernética, ainda está em fase de amadurecimento e que muitos projetos ainda estão por se concretizarem. Contudo, certo é que o EB, como visto acima, já está definindo doutrina e tropa especializada para lidar com o tema. Além disso, estabelece o Livro Verde (BRASIL, 2007), que uma das diretrizes a serem contempladas pelo Brasil, no Plano Nacional de Segurança Cibernética, é "protagonizar a articulação e elaboração de Convenção global, sobre crime cibernético, no âmbito da ONU, no curto e médio prazo." A finalidade é estabelecer um marco legal na legislação internacional.

6 Estratégias de Comunicação Social

Com a crescente utilização da informática e a interligação de sistemas em redes, corporações e governos em geral têm obtido inúmeros benefícios quanto à dinamização dos processos de

comunicação, ocasionando aumento de produtividade e disponibilidade tempestiva de acesso à informação impactando de forma direta e decisiva na competitividade e, consequentemente, na evolução e desenvolvimento de uma nação.

Diversos órgãos de pesquisas revelam que a maior parte dos incidentes vinculados às redes de computadores advém da falta de conscientização dos usuários de TI – Tecnologia da Informação.

A segurança associada a TI e a programas de conscientização tem como um de seus objetivos finais a garantia do sucesso dos negócios e interesses institucionais e envolve práticas que resultam em maior qualidade. Isso exige o engajamento de todos os seguimentos da sociedade e serve como anteparo ao fracasso.

A boa comunicação pode ser vista como termo indispensável ao comprometimento de usuários de TI quanto à observação de requisitos de segurança e, consequentemente, à obtenção do sucesso nos negócios e continuidade de processos de infraestrutura crítica, que contam cada vez mais com a TI para suas operações.

6.1 Estratégias de relações públicas

Dentre os campos da Comunicação Social, podemos destacar o de Relações Públicas como possuidor de ferramentas específicas que podem ser aplicadas no momento de planejamento do Exército Brasileiro para adotar políticas e ações que envolvem o tema da guerra cibernética. Relacionar-se com públicos não é uma escolha que empresas e organizações diversas fazem. É uma condição social.

O trabalho de um administrador de relações públicas começa com planejamento estratégico. O objetivo é fazer uma análise que resulte num diagnóstico organizacional externo e interno, indicativo de ameaças e oportunidades, pontos fracos e fortes. Por fim, é preciso traçar um perfil completo da organização em seu contexto econômico, político e social.

As relações públicas podem abrir canais de comunicação entre os públicos para construir uma relação de

confiança mútua e credibilidade, com ênfase nas missões e nos propósitos e princípios da instituição. Essa função estratégica precisa ser considerada, tendo em vista que a emergência das ameaças cibernéticas envolve todos os setores da sociedade e exige do Exército Brasileiro um relacionamento eficaz com esses segmentos. Bancos públicos e privados, usinas de energia ou de tratamento de água, serviços essenciais à sociedade, trabalham em rede e podem, portanto, ser alvos de hackers numa situação de ataque cibernético. Assim precisam ser guardados pelo Exército. Num contexto de guerra ou não, a interação do Exército com esses setores pode ajudar a guiar as ações desses setores num momento crucial. Ou mesmo prevenir que esse momento chegue.

7 Conclusão

A partir de uma revisão bibliográfica e pesquisa exploratória, identificou-se os grandes prejuízos que os ataques cibernéticos podem causar. Como resultado amplo, pontuou-se o que já existe sobre o tema Guerra Cibernética, tanto em termos técnicos como legais, para facilitar o trabalho dos futuros estudiosos e orientar os militares do Exército na continuação do desenvolvimento de trabalhos sobre o assunto. Adicionalmente, no que diz respeito à Comunicação Social, concluiu-se que o Exército precisa investir no gerenciamento de relacionamentos estratégicos com públicos de interesse para o desenvolvimento da segurança cibernética, especialmente na área privada e no público interno.

Analisando o material existente sobre o assunto, percebe-se, portanto uma nova filosofia de defesa: A Defesa Cibernética, possuindo como missão a responsabilidade de impedir o sucesso de ataques virtuais que visam como alvo os sistemas públicos e militares do país. Nesse contexto, observa-se, através do estudo das bibliografias, que o Exército Brasileiro foi designado a criar a Estratégia Nacional de Defesa (END). Surge, então, o CDCiber, Centro de Defesa Cibernética. Além da aquisição de novas tecnologias verificou-se, através desta pesquisa, a grande importância de desenvolver a

mentalidade de preocupação com a segurança e difundir a importância da defesa cibernética para a segurança nacional e o funcionamento eficiente dos sistemas públicos e militares. Ainda dentro deste preceito, é fundamental que o Congresso crie leis visando punir os crimes digitais e que toda sociedade brasileira se engaje neste desafio.

Referências

BRASIL. Constituição da República Federativa do Brasil. Brasília: 1988.

_____. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências.

_____. Decreto nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional. Disponível em: <https://www.defesa.gov.br/pdn/index.php?page=home>. Acesso em: 21 ago 2008.

_____. Decreto nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional. Disponível em: <https://www.defesa.gov.br/pdn/index.php?page=home>. Acesso em: 21 ago 2008.

_____. Portaria nº. 45 PR/GSI, de 8 de setembro de 2009. Instituiu o Grupo Técnico de Segurança Cibernética, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN).

_____. Portaria Normativa nº 196/MD, de 22 de fevereiro de 2007. Dispõe sobre o Glossário das Forças Armadas.

_____. Portaria Normativa nº 333/MD, de 24 de março de 2004. Dispõe sobre a Política de Guerra Eletrônica de Defesa.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde: segurança cibernética no Brasil**. 2010.

SANTOS, José Carlos dos. Na guerra cibernética, Brasil adota estratégia do contra-ataque: depoimento. [21 de junho, 2011]. Brasília: Portal IG. Entrevista concedida a Severino Motta.

STALLINGS, William **Criptografia e segurança de redes**. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

STOPATTO, Sérgio Luiz. A Guerra Cibernética e a Mobilização Nacional. In: **Cadernos de Estudos Estratégicos de Logística e Mobilização Nacionais.** Divisão de Assuntos de Logística e Mobilização Nacionais. Rio de Janeiro: Escola Superior de Guerra, 2010.