O POSICIONAMENTO DAS FORÇAS ARMADAS BRASILEIRAS NOS CONFLITOS DA GUERRA CIBERNÉTICA

POSITIONING OF BRAZILIAN ARMED FORCES IN THE CONFLICTS OF CYBER WARS

doi.org/ 10.29327/4127120

Marcel de Macedo Lima Giffoni[1]

RESUMO: A internet, que é um dos maiores avanços tecnológicos da área de comunicações, trouxe diversas vantagens para a sociedade, já que proporciona uma maior interação entre pessoas das mais variadas partes do mundo sem a necessidade de um deslocamento físico. Com o passar dos anos, a sociedade foi se tornando cada vez mais dependente dessa tecnologia, já que grande parte dos serviços usados pela população encontra-se na rede mundial de computadores. O lado negativo dessa revolução tecnológica se deve pela exploração, por intermédio de *hackers,* das falhas existentes nessa extensa rede de dados, logo incidentes de segurança foram aparecendo no decorrer de sua utilização. Com isso, conflitos que afetam diretamente a sociedade foram surgindo, por tal, motivo o termo guerra cibernética surgiu, pois, recursos tecnológicos são usados com os mesmos objetivos de uma guerra convencional. As Forças Armadas brasileiras possuem estratégias de atuação na prevenção de ataques para uma melhor defesa cibernética no Brasil.

Palavras-chave: Defesa e Forças Armadas . Guerra Cibernética. Internet. Tecnologia.

ABSTRACT: The internet, which is one of the greatest technological advances in the area of communications, has brought several advantages to society, as it provides greater interaction between people from the most varied parts of the world without the need for physical displacement. Over the years, society has become increasingly dependent on this technology, since most of the services used by the population are found on the world wide web. The negative side of this technological revolution is due to the exploitation, through hackers, of the flaws in this extensive data network, so security incidents started to appear in the course of its use. As a result, conflicts that directly affect society have arisen. For this reason, the term cyber war emerged, because technological resources are used for the same purposes as conventional warfare. The Brazilian Armed Forces have strategies for preventing attacks for a better cyber defense in Brazil.

Keywords: Defense and Armed Forces. Cyber War. Internet. Technology.

[1] Graduado em Engenharia da Computação. Universidade ENIAC – São Paulo e Sistemas de Informação. Universidade Castelo Branco – Rio de Janeiro, pós-graduado em Banco de Dados. Faculdade Cidade Verde – Maringá - Paraná, pós-graduado em Gerenciamento de Projetos. Universidade Cândido Mendes – Rio de Janeiro, pos- graduado em Gestão de Tecnologia da Informação e da Comunicação. Universidade Cândido Mendes – Rio de Janeiro. Militar e especialista em Cybercrime e Cibersecurity: Prevenção e Investigação de Crimes Digitais. Faculdade Cidade Verde E- mail: marcelgiffoni@hotmail.com.

INTRODUÇÃO

A modalidade de conflito conhecida como guerra cibernética utiliza armas virtuais que são usadas para atacar o oponente em um ambiente virtual. Há malefícios existentes nesse campo de batalha, já que os ataques causam prejuízos a quem os sofre. Nas últimas décadas, os ataques cibernéticos no Brasil aumentaram sete vezes mais que a média mundial, já que o país sofreu 274% de ataques contra apenas 38% da média restante do mundo. As perdas financeiras que foram causadas pelos ataques no Brasil teve um valor médio de US$ 2,45 milhões conforme mostrado na pesquisa global de segurança da informação elaborada pela *PricewaterhouseCoopers* Brasil LTDA em 2016.

Diante do cenário mundial de ataques cibernéticos, os países vêm se preparando com formas de defesa contra essas ameaças. O Brasil está tentando reduzir os riscos desse novo campo de batalha criado, já que os impactos podem ser danosos como de uma guerra convencional. Nessa perspectiva, a preocupação com a defesa cibernética engloba instituições dos setores privados, públicos e militares. O objetivo do trabalho é conceituar a guerra cibernética, mostrar a probabilidade dos riscos de incidentes de segurança da informação e apresentar as formas de defesa utilizadas pelas Forças Armadas do Brasil, o qual uma de suas missões é tornar o mundo virtual brasileiro mais seguro.

Para o desenvolvimento do trabalho foram utilizadas pesquisas bibliográficas baseadas em publicações e livros a respeito de guerra cibernética. As informações pesquisadas são oriundas das Forças Armadas. As análises foram retiradas de casos relacionados com o tema.

1 Ciberguerra

Hoje, os meios computacionais são essenciais para a sociedade. A utilização da tecnologia é uma forma competitiva para a obtenção de superioridade perante o inimigo durante as guerras. Com a atual era da informação isso não muda, já que grandes potências mundiais vêm sofrendo inúmeros ataques cibernéticos. A retirada de um serviço hospedado na internet que seja essencial para a população ou a propagação de códigos maliciosos em uma rede de dados do governo são exemplos que ocorrem no ambiente cibernético. Ações ilícitas que são realizadas através de equipamentos eletrônicos no ciberespaço podem definir o conceito de guerra cibernética, mas pode ser compreendido de maneira mais detalhada com o que o Exército Brasileiro define. Para o Manual de Campanha n.º 10.232 do Exército Brasileiro (p. 18, 2017).

> Guerra cibernética é uma ação que corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de comando e

> controle do adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático, ou de uma operação militar. Compreende ações que envolvem as ferramentas de tecnologia da informação e computação para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sistemas de Informação. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às tecnologias da informação e computação.

Órgãos privados também sofrem dos efeitos de ações criminosas como os órgãos públicos, com isso em uma ciberguerra não ocorre distinção entre alvos militares e civis, então o conhecimento da probabilidade de riscos emanada de incidentes de segurança da informação é essencial por causa da exposição de informações na rede mundial de computadores.

Com a dependência dos sistemas de informação e o avanço tecnológico, o combatente que possuir a soberania do espaço cibernético estará com vantagem perante seus inimigos. Com a complexidade existente nesse campo de batalha, as estratégias de defesa se modificam a todo, estante para a adaptação nesta nova realidade de guerra, já que a difícil identificação de quem ataca e a utilização de armas que não convencionais pode destruir uma nação inteira. Logo, mecanismos de defesa no âmbito de um país são criados para que a soberania nacional não esteja ameaçada.

Muitos países não dão a devida importância a essa realidade virtual. O que ocorre nesses locais é o baixo investimento na área de segurança de dados, e consequentemente espionagens e sabotagens a estruturas estratégicas ocorrem a todo instante, o que compromete a segurança nacional de uma nação.

1.2 Probabilidade de riscos

Um ataque cibernético pode impactar negativamente na vida de muitas pessoas. Os serviços essenciais da sociedade encontram-se em infraestruturas de sistemas de distribuição de energia, gás ou água, sistemas de telecomunicações, comércio eletrônico, jornais virtuais que mostram notícias a população em tempo real, dentre outros. Os ataques a esses serviços podem ser mais destrutivos do que os danos causados em uma guerra convencional. O *Stuxnet*, por exemplo, é um vírus que foi criado em 2010 para atrasar o programa nuclear do Irã, já que ele tomava o controle das operações da infraestrutura industrial utilizada, com isso diversas centrífugas de enriquecimento de urânio foram danificadas. O vazamento de documentos em 2013 que comprovavam o monitoramento de pessoas em qualquer parte do mundo foi descoberto por um ex-agente da CIA. Instituições brasileiras como Petrobrás, a embaixada brasileira em

Washington, milhares de ligações telefônicas, milhões de e-mails, dentre outros foram espionados pela Agência de Segurança Nacional dos Estados Unidos (NSA).

Há três modalidades de ataque na guerra cibernética, que não são novidades em uma guerra convencional. A espionagem, que detecta informações sigilosas do inimigo e é utilizado para obter superioridade militar e política. A sabotagem, que é uma ação direta como a paralisação do sistema energético de uma região com o objetivo de prejudicar a prestação de serviços de hospitais para que mortes ocorram sem a necessidade do lançamento de uma bomba. Por último, existe a subversão que tenta desestruturar a ordem social ou até a derrubada de um governo. A divulgação de notícias falsas são rumores dessa modalidade de ataque. Para o Manual de Campanha n.º 10.232 do Exército Brasileiro (2017, p. 19) "risco cibernético consiste na probabilidade de ocorrência de um incidente associado ao tamanho do dano por ele provocado."

1.3 Defesas Cibernéticas das Forças Armadas do Brasil

O rastreamento de um ataque é muito difícil, o que dificulta o rastreamento do atacante. Assim, é necessário o contínuo monitoramento dos sistemas de informação mais críticos. A defesa da segurança nacional é uma preocupação dos setores privados e públicos, tanto civis como militares, sendo a prevenção a melhor forma de defesa existente.

O Brasil é um país pacífico no âmbito cibernético, logo não há intenção de lançar ataques a outros países. Já na defesa de ameaças, o país possui o Programa de Defesa Cibernética Nacional que tem como objetivo incrementar as atividades de capacitação, ciência, doutrina, tecnologia e inovação, inteligência e operações no âmbito da defesa nacional. A capacidade de defesa cibernética e combate aos crimes virtuais aumentaram após a criação do programa.

O Programa de Defesa Cibernética na Defesa Nacional classifica as atribuições ao espaço cibernético com base em três níveis fundamentais: (1) Nível Político, que é de responsabilidade da Presidência da República, (2) Nível Estratégico, que é responsabilidade do Ministério da Defesa e Comandos das Forças Armadas e o (3) Nível Operacional e Tático, cuja responsabilidade é própria das Forças Armadas, é acionado em casos de Guerra Cibernética.

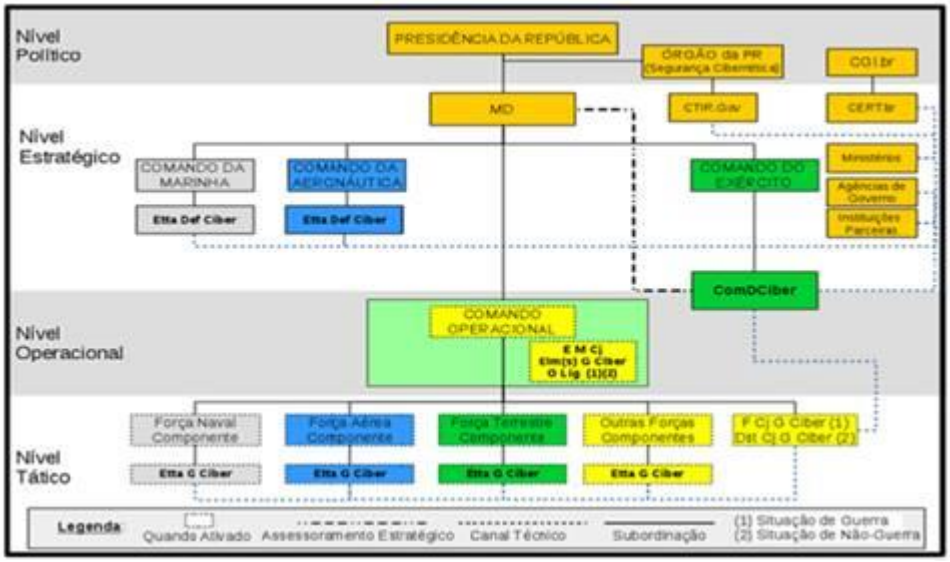
1.4 Defesas Cibernéticas das Forças Armadas do Brasil

O rastreamento de um ataque é muito difícil, o que dificulta o rastreamento do atacante. Assim, é necessário o contínuo monitoramento dos sistemas de informação mais críticos. A defesa da segurança nacional é uma preocupação dos setores privados e públicos, tanto civis como militares, sendo a prevenção a melhor forma de defesa existente.

O Brasil é um país pacífico no âmbito cibernético, logo não há intenção de lançar ataques a outros países. Já na defesa de ameaças, o país possui o Programa de Defesa Cibernética Nacional que tem como objetivo incrementar as atividades de capacitação, ciência, doutrina, tecnologia e inovação, inteligência e operações no âmbito da defesa nacional. A capacidade de defesa cibernética e combate aos crimes virtuais aumentaram após a criação do programa.

O Programa de Defesa Cibernética na Defesa Nacional classifica as atribuições ao espaço cibernético com base em três níveis fundamentais: (1) Nível Político, que é de responsabilidade da Presidência da República, (2) Nível Estratégico, que é responsabilidade do Ministério da Defesa e Comandos das Forças Armadas e o (3) Nível Operacional e Tático, cuja responsabilidade é própria das Forças Armadas, é acionado em casos de Guerra Cibernética.

Figura 1- As atribuições ao espaço cibernético com base em três níveis fundamentais



Fonte: Manual de Campanha Guerra Cibernética, 2017

Segundo o Manual de Campanha n.º 10.232 do Exército Brasileiro (p. 23, 2017),

> O Sistema de Guerra Cibernética do Exército (SGCEx) é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de guerra cibernética, assegurando o seu uso efetivo pelo Exército Brasileiro, bem como impedindo ou dificultando a utilização do espaço cibernético pelo oponente.

As capacidades do Sistema de Guerra Cibernética do Exército (SGCEx), que são as aptidões para o cumprimento de uma determinada missão, englobam a proteção, o ataque e a exploração cibernética. A proteção conduz ações para neutralizar ataques, o ataque desenvolve

ações para interromper, negar, degradar, corromper ou destruir informações, ou sistemas computacionais e explorar faz a coleta de dados, de modo sigiloso, nos sistemas de informação de interesse.

O governo brasileiro estabeleceu que o setor cibernético é um dos três setores que mais possuem importância estratégica no país, assim o Exército Brasileiro instituiu o setor cibernético no âmbito de defesa por determinação do Ministério da Defesa. A existência de um órgão que colaborasse para a implantação da governança da defesa no ambiente virtual brasileiro foi necessária e com isso foi criado o Centro de Defesa Cibernética (CDCiber), que tem o objetivo de inibir ataques digitais, neutralizar fontes de ataque e proteger sistemas de informações. O órgão desenvolve simuladores de guerras cibernéticas, sistemas e segurança da informação, como antivírus e programas de detecção de intrusão, além de dar treinamentos a respeito de segurança da informação para civis e militares. Grandes eventos como os jogos olímpicos e copa do mundo tiveram a participação do centro que atuou em coordenação com os setores privados e públicos na defesa cibernética do país. O recebimento de informações de inteligência e a colaboração entre todos os órgãos participantes permitiram o sucesso das realizações dos eventos. Militares das três forças armadas, agentes da Polícia Federal e técnicos da Agência Nacional de Telecomunicações compõe o efetivo dessa organização militar focada na defesa do ambiente virtual brasileiro.

No que concerne à Marinha do Brasil, existe o Centro de Ações de Guerra Cibernética (COMOPNAV) para coordenação dos recursos e ações preventivas contra a Guerra Cibernética da MB. Há o Centro de Inteligência da Marinha (CIM) e o Centro de Análises de Sistemas Navais (CASNAV) que ajudam nas investigações de casos de ataques cibernéticos.

Na Força Aérea, os órgãos centrais responsáveis pelo controle de ameaças cibernéticas são: o Centro de Computação da Aeronáutica (CCA), o Centro de Inteligência Aeronáutica (CIAER), a Diretoria de Tecnologia da Informação da Aeronáutica (DTI) e o Centro de Estudo e Avaliação da Guerra (CEAGAR).

Além das Forças Armadas, há outros órgãos envolvidos com a defesa cibernética no Brasil, como o Centro de Tratamento de Incidentes de Redes do Governo (CTIR), que atende aos incidentes de redes dos Órgãos da Administração Pública Federal (APF) e fornece informações para a criação de normas e políticas nas áreas de segurança. A Agência Brasileira de Inteligência (ABIN) é outro órgão que também está envolvido com a segurança da informação.

1.5 Considerações Finais

A nova modalidade de guerra que não necessita de um combate físico para causar prejuízos financeiros pode ser mais danosa que uma guerra convencional, já que um país inteiro pode se desestabilizar sem saber a origem do ataque realizado. Logo, percebe-se que a segurança da informação é tão importante quanto à segurança das fronteiras de um país ou uma defesa antimíssil.

O setor de defesa cibernética brasileiro já coleta bons resultados do trabalho conjunto das Forças Armadas com órgãos da Administração Pública Federal. A atuação bem sucedida do país nos grandes eventos ocorridos no país exemplifica o sucesso do setor no Brasil, mas em um contexto mundial ainda possui atraso se comparado com países desenvolvidos como os Estados Unidos.

O Programa de Defesa Cibernética na Defesa Nacional que faz com que as Forças Armadas trabalhem juntas para a utilização efetiva do espaço cibernético brasileiro, bem como o uso de ações que dificultam ou impeçam sua utilização contra os interesses de defesa nacional é fundamental para o país. Com isso, órgãos civis e militares especializados nessa área foram criados para defender a soberania do Brasil.

De acordo com o trabalho, pode se afirmar que ações como treinamento de profissionais, integração de órgãos civis e militares, investimento em tecnologia, conscientização da população sobre segurança da informação, criação de planos de defesa cibernética em âmbito nacional, criação de políticas de segurança e proteção de serviços críticos hospedados na rede mundial de computadores são as melhores formas de defesa para a guerra cibernética.

Referências

atalha invisível: estamos prestes a ver uma Guerra Mundial Cibernética? Disponível em ‹https://www.tecmundo.com.br/seguranca-de-dados/111932-batalha-invisivel-estamos-prestes-ver-guerra-mundial-cibernetica.htm›. Acesso em: 20 nov. 2020.

EB70-MC-10.232: **Manual de campanha Guerra Cibernética.** Brasília, 2017.

FROTA. Francisco. **Guerra Cibernética**. Disponível em: ‹https://jornalggn.com.br/tecnologia/defesa-tecnologia/guerra-cibernetica›. Acesso em: 18 nov. 2020.

Liberdade de ação no Espaço Cibernético. Disponível em: ‹http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica›. Acesso em: 07 nov. 2020.

NETTO. Oscar Rocker. **Ataque Cibernético no Brasil cresce 7 vezes mais que média mundial**. Disponível em: ‹http://riscosegurobrasil.com/materia/ataque-cibernetico-no-brasil-cresce-7-vezes-mais-que-media-mundial›. Acesso em: 10 nov. 2020.

Por dentro do CDCiber, o Centro de Defesa Cibernética do Exército Brasileiro. Disponível em: ‹https://medium.com/brasil/por-dentro-do-cdciber-o-centro-de-defesa-cibernetica-do-xercito-brasileiro-40ce637d119›. Acesso em: 01 nov. 2020.

Política Nacional de Defesa. Disponível em: ‹https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf›. Acesso em: 11 nov. 2020.

Programa de Defesa Cibernética na Defesa Nacional. Disponível em: ‹https://www.gov.br/defesa/ptr/arquivos/ensino_e_pesquisa/defesa_academia/cadn/palestra_cadn_xi/xv_cadn/programaa_daa_defesaa_ciberneticaa_naa_defesaa_nacional.pdf/view›. Acesso em: 29 out. 2020.

Você já ouviu falar do Stuxnet, o maior vírus da história? Disponível em: ‹https://viga.com.br/voce-ja-ouviu-falar-do-stuxnet-o-maior-virus-da-historia›. Acesso em: 25 out. 2020.