ESCOLA DE GUERRA NAVAL

CC MARCELO PINTO GOMES

UMA COMPARAÇÃO ENTRE A CAPACIDADE DE DEFESA CIBERNÉTICA BRASILEIRA E A ESTADUNIDENSE ENTRE 2010 E 2018

O surgimento do quinto domínio

Rio de Janeiro

2018

CC MARCELO PINTO GOMES

UMA COMPARAÇÃO ENTRE A CAPACIDADE DE DEFESA CIBERNÉTICA BRASILEIRA E A ESTADUNIDENSE ENTRE 2010 E 2018

O surgimento do quinto domínio

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.
Orientador: CMG (FN-RM1) William

Rio de Janeiro

Escola de Guerra Naval

2018

AGRADECIMENTO

Aos meus filhos que puderam compreender um período tão longo de dedicação e à minha esposa pelo contínuo incentivo e apoio durante todo o processo de realização desse trabalho.

Ao Capitão de Fragata Eugênio Huguenin e Capitão de Mar e Guerra (FN-RM1) William, meus orientadores, pelas orientações precisas e necessárias que foram fundamentais para a concisão, elaboração de idéias e desenvolvimento do trabalho.

Ao Capitão de Fragata (RM1) Ohara Barbosa Nagashima pela dedicação e orientação costumeira dada a mim e a toda a turma do Curso de Estado Maior para Oficiais Superiores (CEMOS-2018).

RESUMO

O propósito da pesquisa é comparar a capacidade de Defesa Cibernética dos Estados Unidos da América (EUA) e do Brasil, diante da crescente ocorrência de assuntos relacionados na última década. Para realizar essa análise foi escolhida a teoria do alemão Ratzel onde prega que as sociedades com maior grau de desenvolvimento devem ampliar seu espaço para sua população, incluindo aí os recursos naturais e humanos. Juntamente com essa teoria será observado o conceito de Defesa Cibernética, muito importante para auxiliar a teoria a enquadrar os fatos observados na pesquisa. A relevância do tema consiste na oportunidade em proporcionar a percepção da consciência de segurança cibernética que é uma excelente ferramenta para se enfatizar um assunto tão importante e subempregado pelo lado brasileiro como será visto ao decorrer do trabalho. Para alcançar esse objetivo, realizou-se uma pesquisa exploratória, bibliográfica e documental, adotando-se um estudo comparativo entre as capacidades de defesa cibernética dos Estados em questão no período entre 2010 e 2018. Foram pesquisadas as doutrinas, as estruturas e algumas ações praticadas e após inter-relacioná-las com a teoria de Ratzel, com a definição de guerra cibernética, com os dados e evidências, concluiu-se que os EUA possuem uma capacidade de Defesa Cibernética mais desenvolvida. Essa supremacia estadunidense é proporcionada por maiores investimentos e por uma maior consciência cibernética comprovando seu caráter extremamente ativo em ações defensivas decorrentes de um grande número de ataques que sofre regularmente e em ações ofensivas e exploratórias pelo seu caráter cultural e dominador.

Palavras-chave: Defesa Cibernética. Estados Unidos da América. Brasil. Teoria de Ratzel.

LISTA DE TABELAS

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABIN – Agência Brasileira de Inteligência

CAGC - Centro de Ações de Guerra Cibernética

CDCiber – Centro de Defesa Cibernética

CGEM – Centro de Guerra Eletrônica da Marinha

CIA – *Central Intelligence Agency*

CMF – *Cyber Mission Force*

ComOpNav – Comando de Operações Navais

ComDCiber – Comando de Defesa Cibernética

DCTIM – Diretoria de Comunicações e Tecnologia da Informação da Marinha

DGE – Departamento de Gestão de Ensino

DGMM – Diretoria Geral de Material da Marinha

DoD – *Department of Defence*

DoDIN – *Department of Defence Information Network*

DOU – Diário Oficial da União

EB – Exército Brasileiro

EMA – Estado Maior da Armada

EMAER – Estado Maior da Aeronáutica

EMCj – Estado Maior Conjunto

ENaDCiber – Escola Nacional de Defesa Cibernética

END – Estratégia Nacional de Defesa

EUA – Estados Unidos da América

FBI – *Federal Bureau of Investigation*

FAB – Força Aérea Brasileira

FFAA – Forças Armadas

GCHQ - *Government Communications Headquarters*

JAPEC – *Joint Acquisition and Protect Cell*

MB – Marinha do Brasil

MD – Ministério da Defesa

MRE – Ministério das Relações Exteriores

NSA – *National Security Agency*

NuENaDCiber – Núcleo da Escola Nacional de Defesa Cibernética

NuComDCiber – Núcleo do Comando de Defesa Cibernética

OM – Organização Militar

OTAN – Organização do Tratado do Atlântico Norte

PEECFA – Plano Estratégico de Emprego Conjunto das Forças Armadas

SMDC – Sistema Militar de Defesa Cibernética

TI – Tecnologia de Informação

TIC – Tecnologia de Informação e Comunicações

USCYBERCOM – *United States Cyber Command*

US SOUTHCOM – *United States South Command*

SUMÁRIO

INTRODUÇÃO

A partir do século XXI, houve um rápido crescimento na área de tecnologia de informação e comunicação (TIC), destacando-se em especial a evolução da Internet. Sendo assim, pessoas e até Estados passaram a confiar suas informações, de todas as naturezas, ao espaço cibernético[1]. Em virtude da crescente importância do assunto, este espaço também chamado de ciberespaço passou a ser estudado e monitorado por elementos com intenções variadas, desde usuários comuns até a programadores especializados em atuar, neste campo, anonimamente.

Diante dessas mudanças trazidas pelas novas tecnologias digitais, os Estados buscam interação com esse novo ambiente, pois os cidadãos estão cada vez mais conectados e dependentes das redes sociais. As empresas, por sua vez, realizam seus negócios "on-line" e as Forças Armadas (FFAA) conduzem suas estratégias com o auxílio dessas novas ferramentas. A evolução trazida pelas conquistas do mundo conectado, onde se destacam a facilidade, a rapidez e a redução de custos na comunicação, trouxe os ataques cibernéticos[2] que visam afetar sistemas, extrair dados ou, até mesmo, anteceder a ataques das FFAA em caso de conflitos.

Sistemas de armas de plataformas como navios, aeronaves e radares fixos, componentes de sistemas de defesa antiaéreo já são acionados por meio de softwares que são os elementos mais sensíveis e visados por poderem controlar um lançamento, efetuar um disparo ou ser cegado durante uma ação. Tudo isso graças ao aumento em potencial do alcance e da velocidade das comunicações satelitais.

---

[1] De acordo com a Doutrina Militar de Defesa Cibernética, é espaço virtual, composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam, são processadas e/ou armazenadas (MD31-M-07, 2014, p.18).

[2] De acordo com a Doutrina Militar Naval são ações de guerra cibernética enquadradas quanto ao tipo de modo a degradar, corromper, destruir ou manipular informações em ativos de informação de interesse (EMA 305, 2017, p.3-26).

Esse novo século é acompanhado pelo desenvolvimento cada vez mais acelerado dos componentes tecnológicos, propiciado pelas indústrias de ponta que produzem atualizações de seus produtos, que se tornam cada vez mais leves, menores e mais rápidos. Muitos deles são utilizados em computadores, robôs e sistemas de vigilância e monitoramento.

Um grande número de Estados já demonstraram interesse e preocupação com esse novo e desconhecido campo de atuação, por terem sofrido ataques sem autoria comprovada. Mesmo não existindo formalmente uma guerra cibernética declarada, existem exemplos de ataques realizados recentemente, de acordo com Clarke e Knake (2015): (i) ataque realizado por aeronaves israelenses à Síria em 2007 possibilitado por uma investida prévia junto ao seu sistema de defesa antiaéreo que foi cegado; (ii) a campanha psicológica realizada pelos EUA contra o Iraque 13 anos após a primeira investida que resultou no envio de centenas de e-mails para dentro do sistema do Ministério da Defesa (MD) iraquiano; (iii) ainda em 2007, ataques realizados à Estônia por russos nacionalistas, em decorrência da retirada de uma estátua da ex-União Soviética do território estoniano, que tiveram servidores inundados de pedidos de acesso ficando, com isso, sobrecarregados e por fim impossibilitados de responder a requisições legítimas; e (iv) em 2008, o ataque cibernético russo à Geórgia.

Levando em consideração este cenário, movido pelo avanço da tecnologia e pelos novos desafios que surgem e são impostos à Defesa Cibernética dos EUA e do Brasil, o presente trabalho se propõe a realizar uma pesquisa exploratória, bibliográfica e documental para compor um estudo comparativo entre a capacidade de Defesa Cibernética dos Estados em questão na era digital[3], para identificar e citar algumas singularidades e similaridades. Para alcançar tal objetivo, foi escolhida a teoria do “Lebensraum”, em português: Espaço Vital de Friedrich Ratzel que diz: ”Toda a sociedade, em um determinado grau de

[3] É um termo frequentemente utilizado para designar os avanços tecnológicos iniciados na Terceira Revolução Industrial e que reverberaram na difusão de um ciberespaço, um meio de comunicação instrumentalizado pela informática e pela Internet. Disponível em: <https://mundoeducacao.bol.uol.com.br/geografia/era-informacao.htm>. Acesso em 27 Jun. 2018.

desenvolvimento, deve conquistar territórios onde as pessoas são menos desenvolvidas". No contexto da nossa análise, entenderemos essa questão territorial como uma luta pela conquista e manutenção do espaço cibernético.

Para se realizar a análise comparativa, buscaremos respostas para as seguintes questões: Qual Estado tem a capacidade de Defesa Cibernética mais desenvolvida? Qual Estado realiza mais investimentos na área?

Para responder às questões formuladas, a hipótese estabelecida neste trabalho é de que os EUA, em relação ao Brasil, estão na vanguarda nos assuntos relacionados ao espaço cibernético e que não tem interesse em realizar acordos de cooperação na área.

E, por fim, o presente estudo está dividido em seis seções: a introdução; uma seção explanando sobre a teoria escolhida e a definição do conceito chave do estudo; duas seções contendo a abordagem e a amplitude da capacidade de defesa cibernética dos EUA e do Brasil; uma seção onde serão apresentadas algumas singularidades e similaridades entre os citados Estados; e, finalmente, uma seção concluindo o trabalho.

2 – O REFERENCIAL TEÓRICO E A DEFINIÇÃO DE GUERRA CIBERNÉTICA

Abordaremos neste capítulo, o referencial teórico a ser utilizado no trabalho, assim como o conceito de Guerra Cibernética. A apresentação desses conteúdos é necessária, pois eles servirão de base para o entendimento e análise de toda a pesquisa realizada.

Este capítulo será dividido em duas seções, a primeira apresentará a teoria do Espaço Vital de Ratzel, enquanto a segunda abordará o conceito de Guerra Cibernética segundo a Doutrina Militar de Defesa Cibernética. Ambos os conceitos serão utilizados para analisar os aspectos da pesquisa apresentados neste trabalho.

2.1 – Espaço Vital ou "Lebensraum"

Espaço vital ou Lebensraum, segundo Friederich Ratzel[4], é o direito que uma nação possui de aumentar o espaço para sua população, levando em conta todos os recursos naturais e humanos que vierem a ser encontrados nas áreas reivindicadas como seu espaço vital, de acordo com Tosta (1984).

O desenvolvimento de um Estado, segundo Ratzel, está vinculado à conquista de novos territórios e também, consiste na ambição máxima de um povo, em um direito para sua população e, afirma também, que as lutas entre os povos são condicionadas pela busca por espaço.

[4] (1844-1904), Geógrafo e etnólogo alemão, pensador, considerado pai e precursor da Geopolítica, e como um dos principais teóricos clássicos da Geografia e do Determinismo Geográfico. Sua principal obra publicada foi a Antropogeografia. Disponível em: <https://brasilescola.uol.com.br/geografia/friedrich-ratzel.htm Acesso em 27 Jun. 2018.

Desde a antiguidade, podemos verificar que os povos lutavam entre si, com seus exércitos, pelo domínio terrestre, enquanto outros, mais visionários, progrediam com suas embarcações e alcançavam terras mais distantes, exercendo o controle do domínio marítimo.

A partir do início do século XX, durante a segunda revolução industrial[5], vemos com o advento do avião, o surgimento do terceiro domínio operacional, e as nações lançam mão dessa ferramenta para conquistar o espaço aéreo. No final desse mesmo século, com a aceleração do desenvolvimento científico-tecnológico, deparamo-nos com a corrida espacial, a conquista da lua, o desenvolvimento e o lançamento de satélites por diversos países do mundo e, desta forma, a conquista do quarto domínio operacional.

Com a intensificação do desenvolvimento tecnológico, as empresas, indústrias e fábricas em todo o mundo se tornaram computadorizadas e integradas. Com o tempo, as pessoas também passaram a ter acesso a essa tecnologia e a navegar nesse novo espaço. Surgiu, o quinto domínio operacional, que abrange as comunicações, a Internet, a tecnologia de informação, a robótica, os sistemas de informação em geral e que, atualmente, pode ser explorado sem grandes investimentos, o chamado domínio cibernético.

Sendo assim, os Estados que mais se desenvolverem nesse caminho terão uma grande vantagem por ter a possibilidade de, dominar os demais. O quinto domínio operacional, equipara-se a um território a ser conquistado e aquele que melhor conhecer e dominar esse território se sobressairá frente a outros Estados. Esse se tornou o desejo de muitos que, mesmo com poucos recursos financeiros, se lançam nessa corrida. Tanto os EUA, quanto o Brasil, se desenvolvem nessa área, cada um segundo a sua realidade e possibilidades.

2.2 – Definição de Defesa Cibernética segundo a ótica do Brasil

[5] Surgiu com o progresso científico e tecnológico observado na Inglaterra, França e Estados Unidos, em meados da segunda metade do século XIX. Disponível em <https://www.todamateria.com.br/segunda-revolucao-industrial/> Acesso em 08 jul. 2017.

O Domínio cibernético vem sendo explorado tanto para o ataque, quanto para a defesa, desde indivíduos até governos com grandes infra-estruturas. Então, diante de ataques cibernéticos inesperados e de diversas origens, é necessário possuir uma capacidade de Defesa Cibernética que apresenta a seguinte definição:

> Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo MD, com as finalidades de proteger os sistemas de informação (Sist Info) de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e comprometer os sistemas de informação do oponente. (DOUTRINA MILITAR DE DEFESA CIBERNÉTICA DO MD, 2014, p.18).

Sendo assim, segundo Oliveira (2011), embora muitas fontes associe a definição à defesa simplesmente, vimos que esse é um conceito mais abrangente que envolve medidas de resposta ativa e até atitudes ofensivas de caráter preventivo, empregados principalmente no contexto de ações em prol da Defesa Nacional. São atividades preventivas ou reativas de responsabilidade do MD e das FFAA em prol da soberania nacional.

Muitas são as possibilidades de se interagir em um novo espaço cibernético, seja pelo seu monitoramento apenas, seja realizando intencionalmente a exploração de seus recursos. Nesse processo, uma conquista pode se tornar possível. Os Estados atuantes nesse novo domínio que são possuidores de diferentes recursos de TIC, buscam seu aperfeiçoamento e devido à inexistência de fronteiras físicas, tendem a se aprofundar na atuação que não precisa ser diretamente proporcional aos seus recursos financeiros como ocorre numa guerra convencional. Os motivos podem ser os mais variados desde que levem a alguma vantagem particular, financeira ou política.

A ampliação do espaço, conforme a teoria do Espaço Vital, pode levar à conquista dos recursos materiais encontrados na área reivindicada e também à conquista de recursos humanos, quando necessário. Aos recursos materiais corresponderiam os informacionais: planejamentos, segredos, códigos e similares. Os recursos humanos são as pessoas (curiosos,

técnicos em informática, hackers[6] ou crackers[7]) que se especializam e se aprofundam em conhecimentos específicos na área de TIC, fundamentais nesse processo. Esses indivíduos não necessariamente precisam estar na área explorada. Podem ser recrutados em qualquer parte do mundo, doutrinados e treinados para garantir a supremacia do lado do explorador. O contexto analisado nesse trabalho é o nível estratégico cujo ator principal é um Estado. As ações serão no sentido de monitorar o próprio espaço, de se proteger e ao mesmo tempo explorar o espaço do oponente, produzindo conhecimentos relevantes de interesse que tragam alguma supremacia.

Mesmo que uma ação na esfera cibernética não parta diretamente de um governo ou agência diretamente ligada ao governo, a origem dela poderá ser, por exemplo, o recrutamento e a cooptação e, vir a ser útil posteriormente. Por isso, será levado em conta até mesmo as ações mais isoladas como pertinentes a este estudo e, portanto, considerada como recurso a disposição do Estado.

[6] Quem invade sistemas computacionais ou computadores para acessar informações confidenciais ou não autorizadas, apontando possíveis falhas nesses sistemas Disponível em: <https://www.dicio.com.br/hacker/> Acesso em 01 Ago. 2018.

[7] Indivíduo com grande conhecimento na área informática que invade computadores ou sistemas computacionais com propósitos ilegais, especialmente para roubar códigos, senhas pessoais ou bancárias. Disponível em: <https://www.dicio.com.br/cracker/> Acesso em 01 Ago. 2018.

3. CAPACIDADE DE DEFESA CIBERNÉTICA BRASILEIRA

Será vista neste capítulo a participação das três FFAA na estrutura de guerra cibernética brasileira e seus graus específicos de envolvimento. Suas contribuições para o Estado e o envolvimento do Brasil no cenário cibernético também serão apresentados.

3.1 Estrutura de Defesa Cibernética Brasileira

A Estratégia Nacional de Defesa (END), elegeu três setores como fundamentais para modernizar a estrutura de defesa nacional por meio da Diretriz Ministerial número 14 de 9 de novembro de 2009, pela qual coube ao Exército Brasileiro (EB) a responsabilidade pela coordenação e a liderança no setor Cibernético, diferentemente do que ocorre nos EUA, que fizeram uma distribuição de responsabilidades mais uniforme entre as forças, como será mostrado no capítulo 4.

Na END, na primeira fase, foi determinado que o EB analisasse e definisse a abrangência do tema e propusesse os objetivos setoriais, o que foi cumprido ainda em 2009. Na segunda fase, após aprovação dos objetivos setoriais que propusesse estratégias setorais e estudasse a adequabilidade das estruturas existentes. O MD aprovou as propostas em outubro de 2010, que estabeleceram nove objetivos estratégicos, com suas respectivas ações estratégicas correlatas e, a partir daí, foi criado o Comando de Defesa Cibernética das Forças Armadas (Com D Ciber) encarregado de executar os objetivos em questão. Dentre esses nove, convém destacar os seguintes, de acordo com Política Cibernética de Defesa (2012):

a) Assegurar com exatidão o uso do Espaço Cibernético pelas FFAA e impedir o uso por outrem que ameace a integridade do país de acordo com a Política de Defesa Cibernética em vigor sendo fiel à estrutura de defesa cibernética criada com o levantamento de riscos a gestão quanto ao impacto e ocorrências de ameaças cibernéticas;

b) Recrutar, treinar e capacitar pessoal de forma continuada com cursos, estágios ou seminários para as atividades no setor cibernético criando cargos e funções específicas, com sólido plano de carreira, cadastrando e controlando inclusive, tomando ciência de potenciais técnicos extra FFAA com critério para mobilização e desmobilização de pessoal e, por fim, realizando parcerias estratégicas ou intercâmbio com instituições de interesse;
c) Criar uma Doutrina de Defesa Cibernética com desenvolvimento e atualização constante de conteúdo promovendo o intercâmbio em instituições nacionais e estrangeiras de interesse e gerando um banco de dados de conhecimento na área;
d) Adequar as estruturas das FFAA de TIC à utilização em atividades correlatas ao setor cibernético;
e) Se utilizar da capacidade dissuasória e operacional do setor cibernético para cooperar com o esforço em caso de mobilização nacional com levantamento de informações sobre pessoal e equipamentos, formulando o plano mais adequado; e
f) Promover a realização de campanhas de conscientização em segurança e defesa cibernética.

De acordo com o General de Divisão Angelo Kawakami Okamura (2016-2018), ex-comandante da Defesa Cibernética do Exército Brasileiro:

> O Comando de Defesa Cibernética (Com D Ciber) foi criado em 02 de janeiro de 2015 e ativado em 15 de abril de 2016. É um Comando Conjunto, pertencente à estrutura regimental do EB, responsável pela coordenação e integração das atividades de Defesa Cibernética no âmbito do Ministério da Defesa (MD), atuando como órgão central do Sistema Militar de Defesa Cibernética (SMDC) e está estruturado da seguinte forma:
>
> – Estado-Maior Conjunto (EMCj), que é chefiado por um Contra Almirante é voltado para a doutrina e planejamento estratégico de emprego conjunto das Forças Armadas em Defesa Cibernética, participando da elaboração dos Planos Estratégicos de Emprego

> Conjunto das Forças Armadas (PEECFA);
> – Centro de Defesa Cibernética (CDCiber), é chefiado por um General de Brigada. Teve seu núcleo ativado em Agosto de 2010 e sua criação em Setembro de 2012. É o órgão operacional para as ações de Defesa Cibernética;
> – Departamento de Gestão e Ensino (DGE), que é chefiado por um Brigadeiro cujo objetivo é observar as atividades de Gestão estratégica, ensino e capacitação de recursos humanos; e
> – Escola Nacional de Defesa Cibernética (ENaDCiber) como centro polarizador de ensino e pesquisa de Defesa Cibernética (TECNOLOGIA E DEFESA, 2018).

Em 21 de julho de 2015, o EB ativou dois núcleos de Defesa Cibernética, no Comando Militar do Planalto (CMP). As instalações representam um passo importante para o Setor. O Núcleo do Comando de Defesa Cibernética (NuComDCiber) e o Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber**)** passam a contar com militares das três FFAA trabalhando no mesmo ambiente físico.

O NuComDCiber está subordinado ao CDCiber, definido por meio da Portaria Normativa nº 2777, de 27 de outubro de 2014, publicada no dia 28 de outubro de 2014 no Diário Oficial da União (DOU).

Em relação ao NuENaDCiber, foi publicado em portaria do MD em outubro de 2014. O projeto foi encomendado à Universidade de Brasília (UnB) e entregue em julho de 2015. A capacitação e treinamento pessoal para atuação no setor cibernético a favor da defesa do país, que anteriormente era destinado ao CDCiber, agora é papel do ENaDCiber. Diferentemente de outros centros de estudos do EB, como o Instituto Militar de Engenharia, o ENaDCiber tem uma sede física, mas os cursos são espalhados por todo o território brasileiro, em parcerias com universidades e centros técnicos.

3.2 Marinha do Brasil, Força Aérea Brasileira e a ABIN na Guerra Cibernética

Como foi visto anteriormente, de acordo com as responsabilidades que lhe foram atribuídas, o EB desenvolveu uma ampla estrutura para conduzir, coordenar e integrar as

atividades cibernéticas com as demais forças, onde para elas foi designada uma participação menos efetiva. Mas as participações da Marinha do Brasil (MB), da Força Aérea Brasileira (FAB) e de outros setores também devem ser mencionadas e serão vistas nos subitens abaixo.

3.2.1 – Marinha do Brasil na Guerra Cibernética

Todas as Organizações Militares (OM) da MB, como de praxe, tomam suas medidas cautelares no que diz respeito à segurança de suas informações o que dificultam ataques cibernéticos. Porém, existem algumas que lidam mais diretamente com o assunto em questão, sendo responsáveis por disseminar e supervisionar o cumprimento da Doutrina de Defesa Cibernética e o correlato estabelecimento pelas OM da Força das medidas de segurança como as citadas logo abaixo:

No Estado Maior da Armada (EMA) existe a Subchefia de Comando e Controle e internamente a Divisão de Tecnologia de Informação e Comunicações, que trata do assunto no nível estratégico;

No Comando de Operações Navais (ComOpNav) existe a Divisão de Guerra Cibernética subordinada à Subchefia de Inteligência Operacional que trata do assunto no nível operacional; e

Na Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), em seu Departamento de Segurança da Informação Digital também existe uma Divisão de Guerra Cibernética, responsável pela contínua proteção cibernética dos ativos informacionais da MB.

Convém citar também algumas publicações que tratam do assunto, são elas: o Plano Estratégico da Marinha, que inclui objetivos como os de segurança digitais e TI, e a Diretoria Geral de Material da Marinha (DGMM), que possui publicações que tratam da segurança de sistemas digitais e de criptologia.

Mais recentemente foi criado o Centro de Ações de Guerra Cibernética (CAGC), com o propósito de realizar o planejamento, condução e controle das atividades operacionais de Guerra Cibernética no ComOpNav. Está em estudo sua transferência para o Centro de Guerra Eletrônica da Marinha (CGEM) ou a criação de uma OM que inclua assuntos cibernéticos, de guerra eletrônica e operações de informação;

E, por fim, a MB realiza anualmente os exercícios Baluarte, em ambiente real, de dupla ação que visa identificar as vulnerabilidades na interface da Rede Integrada de Comunicações da Marinha (RECIM) com a Internet, e o Cyber Securitas, em ambiente virtual que utiliza parte da estrutura adquirida para emprego futuro no, CAGC. Além de participar de exercícios conjuntos e combinados com outros Estados.

3.2.2 – Força Aérea Brasileira na Guerra Cibernética

Para modernizar a estrutura de defesa brasileira, a END atribuiu à FAB a gerência do programa espacial, mas como a MB, não deixou o setor cibernético desamparado. Destaca-se o Estado-Maior da Aeronáutica (EMAER) que trata do assunto no nível estratégico, cabendo à Seção de Comando e Controle da Subchefia de Operações a Defesa Cibernética, de acordo com Veiga (2012);

3.2.3 – ABIN

Um importante setor que não deve ser negligenciado é a Agência Brasileira de Inteligência (ABIN). É um órgão que pertence à Presidência da República, vinculado ao Gabinete de Segurança Institucional. É o órgão central do Sistema Brasileiro de Inteligência (SISBIN), que congrega unidades de inteligência de 38 órgãos da Administração Pública Federal. Muitos são os fóruns em que ela participa, mas dois são relacionados à atividade de Inteligência: a Rede Nacional de Segurança e Criptografia (RENASIC) e o Comitê Gestor da Segurança da Informação (CGSI). (ABIN, 2018).

3.3 Atuações expressivas do Brasil em Defesa Cibernética

O Brasil, principalmente diante dos grandes eventos esportivos mais recentes, pode-se dizer que cumpriu com suas responsabilidades em garantir a defesa do ciberespaço brasileiro, fazendo com excelência seus serviços nos eventos listados a baixo:

a) O I Seminário de Defesa Cibernética do MD de 21 a 24 de Junho de 2010, conduzido pelo EB com a primeira fase aberta ao público convidado, composto de acadêmicos e representantes de infraestruturas críticas nacionais, dos setores público e privado, das FFAA e do MD e a segunda fase com participações restritas ao MD e FFAA, com palestras específicas sobre a situação do Setor Cibernético em cada Força e incluindo a realização de debates distribuídos em quatro salas temáticas;

b) Rio +20 (2012); Primeiro grande evento sob a responsabilidade do CDCiber que estabeleceu um Destacamento de Defesa Cibernética no pavilhão 1 do Riocentro com a participação de diversos parceiros externos, dentre eles, representantes das três FFAA e da ABIN;

c) Copa das Confederações da FIFA e Jornada Mundial da Juventude (2013): O primeiro contou com um destacamento central em Brasília mais seis destacamentos de defesa remotos contando com a participação de militares das três FFAA em todos os destacamentos e no segundo foi feito um esforço para garantir o fornecimento regular de serviços à população e fiscalizar movimentações suspeitas em fronteiras, nos espaços aéreos ou marítimos onde para isso as FFAA montaram um esquema de atuação em dez setores estratégicos de defesa do Estado dentre eles o de Defesa Cibernética de acordo com o MD[8];

d) Copa do Mundo da FIFA (2014): Vários esforços foram feitos para o fortalecimento da segurança, a produção de respostas a incidentes de redes, a incorporação de lições

[8] Disponível em: <https://www.defesa.gov.br/noticias/4355-15-07-2013-defesa-a-participacao-da-defesa-na-jornada-mundial-da-juventude> Acesso em 01 Jul 18.

aprendidas e a proteção contra ataques cibernéticos, além da atualização doutrinária. Cerca de 100 militares das três FFAA atuaram em conjunto ao Centro de Coordenação e Defesa de Área (CCDA) e ao Centro Integrado de Comando e Combate Regional (CICCR) nas 12 cidades-sede da Copa o que garantiu o sucesso da segurança do evento[9];

e) Jogos Olímpicos e Paralímpicos Rio (2016): Com base nos ataques cibernéticos sofridos nas olimpíadas de Londres (2012) o Brasil deu uma alta prioridade ao evento e por conta disso além do CDCiber contou com a participação da ABIN. Este último mapeou os principais hackers em potencial capazes de atuar em eventos de grande importância, mas infelizmente não foi capaz de impedir a ação do grupo Anonymous que foi responsável por diversos ataques nos Governos Estadual e Municipal no Rio de Janeiro, derrubando diversos sites do Brasil sobre os Jogos Olímpicos. (O GLOBO, 2016);

f) O Com D Ciber promoveu, entre os dias 23 e 27 de outubro de 2017, o I Exercício Ibero-Americano de Defesa Cibernética, reunindo militares da Argentina, Brasil, Colômbia, Espanha, México e Portugal, além de observadores do Peru; e

g) O Com D Ciber com a finalidade de envolver seus participantes no treinamento e na proteção de ataques virtuais realizou, entre 3 a 6 de julho de 2018, no Forte Marechal Rondon, Distrito Federal o Exercício Guardião Cibernético, utilizando o Simulador de Operações de Guerra Cibernética (Simulador Virtual – SIMOC), no qual foram inseridos eventos cibernéticos, como uma grande quantidade de ações de hackers no setor financeiro, no setor de defesa e no setor nuclear. O exercício de nível nacional contou com a participação dos representantes do MD, do MRE, do Gabinete de Segurança Institucional da Presidência da República, da MB, do EB, da FAB, do Banco Central do Brasil, de bancos públicos e privados, das empresas do setor nuclear e das entidades do setor cibernético.

[9] Disponível em: <http://www.brasil.gov.br/editoria/seguranca-e-justica/2014/07/defesa-cibernetica-tem-obtido-exito-em-atuacao-durante-a-copa> Acesso em 01 Jul 18.

Apesar de nos eventos citados não terem ocorrido registros de ações ofensivas e exploratórias a luz da teoria, concorrendo para a conquista de novos espaços, o Brasil cumpriu sua missão nesses eventos importantes não permitindo que o espaço cibernético nacional fosse explorado e os grandes eventos esportivos fossem prejudicados.

3.4 Atuação brasileira em ataques cibernéticos

O Brasil, apesar de não ter uma participação tradicional na realização de ataques, ocupou a oitava posição, segundo a Symantec Spam[10], no ranking de países que são origens de ataques cibernéticos, entre 2014 e 2015, embora a pesquisa realizada em 2016 não informe se os ataques tiveram alguma procedência estatal. Os dados podem ser observados na tabela contida no anexo A. Os EUA ocupam a primeira posição, seguidos da China e da Índia, países que possuem um grande contingente populacional.

Já em outra pesquisa, realizada no segundo trimestre de 2015, de acordo com a figura 1 do anexo B, dessa vez realizada pela empresa estadunidense *Akamai Technologies*, mostrou o Brasil em uma posição mais a frente quando se trata de ataques a aplicações Web. Dessa vez, ocupando o terceiro lugar, sendo responsável por 11% dos ataques cibernéticos no mundo, ficando atrás dos EUA, com 15% e da China, com 51%.

Por fim, agora em 2017, nova pesquisa realizada pela mesma fonte, mostra os números um pouco semelhantes, havendo uma troca de posição entre a China e os EUA, de acordo com a figura 3 do anexo D. Dessa vez os EUA passaram a ocupar a primeira posição com 33,8%, a China com 10,2% e o Brasil com uma leve alteração com 8,2% das autorias em termos de ataques cibernéticos.

[10] Relatório Anual de Segurança na Internet número 21 publicado em 2016 pela Symantec Spam. Disponível em: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf> Acesso em 01 jul. 2018.

3.5 Ataques mais expressivos sofridos pelo Brasil e ameaças correntes

Em 2014, houve uma série de ataques por hackers aos sistemas do Ministério das Relações Exteriores, que incluíam também suas embaixadas pelo mundo. A invasão foi realizada por meio de inúmeras tentativas de skimming[11] o que lhes permitiu acesso a informações e mensagens sigilosas, comprometendo cerca de mil e quinhentos diplomatas brasileiros. Não foi identificada a procedência dos ataques, mas ficou constatada a vulnerabilidade da estrutura diplomática brasileira.

No final de 2015, hackers invadiram o sistema do EB durante uma madrugada de domingo e exporam na Internet dados pessoais de mais de sete mil militares. Neste caso, a motivação foi conhecida: uma represália às técnicas utilizadas pelo EB em jogos de guerra cibernética. Os *hackers* que realizaram o ataque afirmaram que essas ações eram uma lição para o CDCiber, pois em uma dessas competições, os militares brasileiros teriam trapaceado para ganhar o jogo. Tal caso demonstrou a fragilidade brasileira em defesa cibernética na ocasião, pois em uma guerra a possibilidade de neutralizar o oponente é fundamental. (OLIVEIRA, et al, 2017).

Segundo Edward Snowden[12], houve hackeamento da rede privada da Petrobrás e espionagem à ex-presidente Dilma Roussef durante seu governo (2011 a 2013) que era realizado por meio de inúmeras escutas telefônicas, inclusive durante as viagens de avião, com auxílio de criptografia. (HARDING, 2014).

Hackers realizaram um ataque em 22 de Junho de 2011 a sites do Governo Brasileiro, onde o site da Petrobrás ficou fora do ar naquela tarde. Um representante relatou que recebeu um volume grande de acessos ao mesmo tempo, embora não tenha sofrido dano

[11] Captação de informações de acesso de uma pessoa ou grupo específico de pessoas por meio de correios eletrônicos falsos.
[12] É um analista e ex-administrador de sistemas da CIA e da NSA que tornou públicos por meio dos jornais inglês The Guardian e Washington Post estadunidense detalhes de vários programas que constituem o sistema de vigilância global da NSA. (HARDING, 2014).

nas informações disponibilizadas em sua página na Internet. A maioria teria partido de computadores localizados na Itália, se iniciando de madrugada. Eles acessaram, na sequência, os sites da Presidência da República, Portal Brasil e Receita Federal. O Serviço Federal de Processamento de Dados (Serpo), responsável pela segurança dos sites, informou que não houve invasão nem comprometimento nos dados, no entanto, o episódio ficou marcado como um dos maiores ataques até então (JORNAL NACIONAL, 2011).

Em 2014, e-mails e sistemas de dados do Itamaraty por todo o mundo sofreram ataques. Nesse evento, foram hackeados documentos do *Intradocs*, tipo de intranet que contém todas as comunicações diplomáticas, mesmo as reservadas. O Itamaraty reportou que não aconteceu a ruptura do sistema, mas sim do conteúdo *Intradoc* anexado aos *e-mails*. Segundo foi apurado, conteúdo da visita do vice-presidente estadunidense durante a Copa do Mundo daquele ano, assim como o resumo da participação do Estado numa Cúpula de segurança nuclear na Holanda, em março de 2014, foram expostos. Os ataques mostraram a vulnerabilidade da capacidade de defesa cibernética do governo naquela ocasião, onde cerca de 1.500 diplomatas brasileiros em todo mundo tiveram seus correios eletrônicos efetados, sem contar com os funcionários da chancelaria e funcionários locais da embaixada (FOLHA DE S. PAULO, 2014).

Levando em consideração a TIC, que faz parte do contexto cibernético, devemos lembrar das eleições presidenciais que ocorrerão no Brasil em outubro de 2018 e que as *fake news*[13] podem influenciar em seu resultado. O STF deverá agir de formas preventiva e punitiva em oposição a quaisquer movimentos de disseminação de notícias falsas e, se for

[13] Notícias falsas ou incompletas utilizadas para dissimular informações e influenciar grupos de pessoas, principalmente as que se restringem unicamente às redes sociais como fontes de informação. Também são ameaças à democracia e ao livre debate. Disponível em: https://www.telegraph.co.uk/technology/0/fake-news-exactly-has-really-had-influence/ Acesso em 01 Ago. 2018.

comprovado que algum candidato foi beneficiado, ele poderá ter a candidatura cassada e a eleição, nessas condições, anulada.

O TSE neste ano formou comitês de inteligência de imprensa em parceria com a ABIN, o EB e a Polícia Federal, acompanhado pelo Ministério Público, para monitorar o processo eleitoral, com foco na disseminação de *fake news*. Segundo seu ministro, ele está convidando uma empresa estrangeira acusada de disseminá-las no Brasil para prestar esclarecimentos. O TSE estará de prontidão para identificar robôs virtuais propagadores de notícias falsas, que é um grande percalço que vem crescendo de forma contínua. Um segundo problema visualizado, é a baixa confiabilidade na transparência do processo eleitoral uma vez que no Brasil serão usadas como forma de apuração urnas eletrônicas que podem ser potencialmente manipuladas.

Em primeira análise, é necessário mencionar que o Brasil, é em geral, um dos países onde os ataques cibernéticos mais tem aumentado. De acordo com Alves e D'Andrea (2016), mundialmente os ataques aumentaram 38% e, no caso do Brasil, eles aumentaram 274%. Como mostra a Figura 2 do anexo C, dados do segundo trimestre de 2017, que corroboram com dados da mesma fonte de anos anteriores, um estudo realizado na *Akamai*, o Brasil é o terceiro local que mais tem sofrido ataques cibernéticos e, o primeiro, os EUA. Isto, com certeza, é consequência da maior participação brasileira no cenário internacional.

A mesma pesquisa realizada pela empresa estadunidense *Akamai Technologies* revelou também que o Brasil está entre os maiores alvos de ataques cibernéticos. Recebendo 7% de todos os ataques cibernéticos do mundo, atrás apenas dos EUA, que é a vítima em 81% dos casos, como também mostra a figura 2 do anexo B. A pesquisa mostrou que os principais alvos desses ataques são jogadores e empresas de jogos online, que têm suas contas hackeadas normalmente por hackers chineses. Esse tipo de ocorrência perfaz 35% do total.

A busca pelo Brasil em cumprir os objetivos estratégicos estabelecidos pelo MD o levou a realizar a busca pelo domínio do espaço cibernético, de acordo com uma política previamente estabelecida, levando em consideração a quantidade, a qualidade e o posicionamento dos recursos humanos disponíveis. Tais objetivos estão de acordo com a teoria de Ratzel e em sintonia com o objetivo de grande parte das nações do mundo na atualidade.

O Com D Ciber, que é um comando conjunto, criado em 2015, é a concretização desse processo onde é levado a cabo com base na Doutrina já mencionada. Mesmo estando a cargo do EB ele tem uma participação colaborativa das três Forças singulares que estão representadas no seu Estado Maior e nos Núcleos localizados no CMP.

O Brasil, de acordo com as pesquisas, está ativamente posicionado no espaço cibernético principalmente pela sua grande quantidade de usuários e sua crescente e natural evolução tecnológica no setor. Isso é caracterizado pela expressiva colocação no cenário mundial atuando das duas formas: tanto realizando ataques, quanto sofrendo. Cabe ressaltar que o governo brasileiro, representado pela figura do próprio presidente, pelo MRE, embaixadas e FFAA sofrem ataques de forma rotineira e, assim, podemos ver a importância do desenvolvimento da capacidade defensiva da Defesa Cibernética Brasileira.

Analisando a teoria de Ratzel, exercendo o direito de buscar a conquista de novos territórios cibernéticos, o Brasil vem ganhando experiência defensiva com a organização dos grandes eventos esportivos e objetiva adquirir treinamento no campo ofensivo e exploratório por meio da ABIN e da criação do NuComDCiber e do NuENaDCiber.

Infelizmente, as *fake news* são uma realidade e representam uma ameaça real. Se não forem monitoradas e reprimidas poderão exercer influência negativa no processo eleitoral. Da mesma forma, as urnas eletrônicas deverão ser monitoradas para trazer a confiabilidade necessária ao processo.

Realizou-se uma pesquisa em diversas fontes e não foi encontrado nada que de maneira governamental se referisse a realização de algum tipo de espionagem cibernética ou processo de obtenção de conhecimentos de inteligência de forma mais ostensiva que se tivesse tornado público por meio do governo brasileiro como foi o caso explicitamente conhecido que vinha sendo realizado pelas agências estadunidenses de segurança (NSA) e de inteligência (CIA) apresentadas no capítulo 4, seja por falta de capacitação, manutenção da ética ou por recursos insuficientes.

4 – CAPACIDADE DE DEFESA CIBERNÉTICA ESTADUNIDENSE

Este capítulo está dividido em três seções, nas quais serão apresentados dados relevantes para a visualização do comprometimento dos EUA com a guerra cibernética. Começaremos o estudo, então por sua espinha dorsal.

4.1 – Estrutura de Defesa Cibernética dos EUA

Os EUA possuem um Comando de Defesa Cibernética (USCYBERCOM), subordinado ao Departamento de Defesa (DoD), que foi criado em 2009 no Quartel General da Agência Nacional de Segurança (NSA) e foi elevado ao status de comando combatente e unificado em 04 de maio de 2018. Ele é composto de 133 equipes cibernéticas, as *Cyber Mission Force Teams* (CMF), que já atingiram a sua completa capacidade operacional. São 41 equipes pertencentes ao Exército, 40 equipes pertencentes à Marinha, 39 equipes pertencentes à Força Aérea e 13 aos Fuzileiros Navais. Essas 133 equipes se distribuem entre 4 setores distintos: As equipes de Missão Nacional (*National Mission Teams*), com 13 equipes que tem o propósito de defender os EUA e seus interesses contra ataques cibernéticos significativos; as equipes de Proteção Cibernética (*Cyber Protection Teams*), com 68 equipes com a missão de defender as redes e sistemas do DoD contra ameaças cibernéticas; as equipes de Missão de Combate (*Combat Mission Teams*), com 27 equipes que tem a atribuição de fornecer apoio aos Comandos Combatentes, gerando efeitos integrados no ciberespaço em apoio a planos operacionais e operações de contingência; e as Equipes de Apoio (*Support Teams*); com 25 equipes que fornecem apoio analítico e de planejamento para as equipes da Missão Nacional e Missão de Combate. (*U.S DEPARTMENT OF DEFENSE*, 2018).

4.2 – Estratégia de Defesa Cibernética dos EUA

Alguns anos depois do Brasil, somente em 2015, o governo dos EUA divulgou um documento, por meio do DoD, que expõe sua estratégia para a segurança e defesa cibernética, fruto da necessidade de se posicionar contra ataques diversos que vinha sofrendo, seja de

hackers ou de outros governos. Sua estratégia é ampla e consistente o bastante para preocupar e desestimular ataques de atores internacionais experientes no assunto como a Rússia, a Coréia do Norte e a China e utilizar armas ofensivas para desestruturar a rede adversária, se necessário. O programa contará com mais de 6.200 pessoas entre civis, militares e as equipes CMF nos próximos anos e custará bilhões de dólares anualmente.

No que tange ao setor privado, como as companhias controlam 90% das redes cibernéticas, o monitoramento e resposta aos ataques de rotina a bens privados, bem como roubo de propriedade intelectual, serão de responsabilidade delas, cabendo ao DoD a atuação em casos mais complexos.

O governo, desta forma, terá um papel específico na defesa contra os ataques mais sérios (estimados em cerca de 2%), referidos na estratégia anunciada com as seguintes características: como envolvendo "perda de vida, danos significativos à propriedade, consequências adversas graves para a política externa estadunidense ou sério impacto econômico para os EUA". A resposta inicial a esses ataques começará por meio de um conjunto de agências especializadas – a NSA, o Departamento de Defesa Interna, a CIA, o FBI e o Pentágono. Em seguida, por ordem presidencial, os militares poderão realizar operações em resposta a um "ataque iminente ou em andamento contra o território dos EUA ou a seus interesses no espaço cibernético". De acordo com Barbosa (2015), com tantas agências governamentais envolvidas, o potencial de duplicação de esforços é provável e é grande a probabilidade de conflitos e descoordenação, como se viu no início do combate ao terrorismo, depois do ataque às torres gêmeas em Nova York.

O DoD estabeleceu cinco objetivos estratégicos para suas missões no espaço cibernético, de acordo com o documento já citado:

1 º Objetivo- Criar e manter preparadas forças e capacitações para operar no espaço cibernético

Para atingir tal objetivo, o DoD vai se empenhar em treinamento persistente de pessoal no mais alto padrão, para estar pronto e dispor dos melhores recursos. Desde 2013, ele vem investindo em seu pessoal, em tecnologias, desenvolvendo as CMF; em sistemas de comando e controle, e desenvolvendo os recursos necessários para operar no ciberespaço. Esta estratégia estabelece objetivos específicos para o DoD se estabelecer, enquanto equipa suas forças e pessoal até pelo menos 2020 e, para atingir essa meta, as seguintes ações serão necessárias:

1) Garantir uma força de trabalho, e para isso deverá:

a) Desenvolver uma força pronta de Missão Cibernética e uma força de trabalho cibernética associadas e construídas sobre três pilares fundamentais: treinamento aprimorado, aperfeiçoamento no recrutamento militar e civil e sua retenção e apoio do setor privado mais forte;

b) Promover fluxos de carreira viáveis a partir de decisões das CMF para todos os militares que realizam e apoiam operações cibernéticas;

c) atrair especialistas oriundos da Guarda Nacional e da Reserva para promover soluções criativas para problemas de segurança cibernética, para apoiar as missões e para engajar a base industrial de defesa e o setor comercial;

d) Além da preocupação com os militares, o Departamento de Defesa deve recrutar e manter pessoal civil altamente qualificado e técnico oferecendo um bom plano de carreira, para sua força de trabalho cibernética total;

e) O DoD, para complementar sua força de trabalho cibernética civil, deverá utilizar programas de intercâmbio para empregar especialistas das melhores empresas de

cibersegurança e tecnologia da informação do setor privado do país para desempenhar funções exclusivas de engenharia, análise e construir benefícios mensuráveis; e

f) O DoD desenvolverá políticas para apoiar a Iniciativa Nacional para a Educação em Cibersegurança, realizando parcerias com interagências, instituições de ensino, bem como os setores estatal e privado.

2) Garantir uma capacitação técnica e para isso, deverá:

a) Desenvolver uma Plataforma Unificada com base nos requisitos de planejamento; e

b) Continuar a acelerar o desenvolvimento cibernético para construir capacidades cibernéticas utilizando parcerias no setor de pesquisa e investimentos para o desenvolvimento de tecnologias avançadas para defender os interesses dos EUA no ciberespaço buscando a expansão da capacidade das CMF.

Em 2013, o DoD desenvolveu um modelo para alcançar a prontidão das CMF e para desenvolver opções militares cibernéticas viáveis para apresentar ao Presidente e Secretário de Defesa. Também passou a se preocupar em obter as ferramentas técnicas disponíveis para conduzir operações de apoio às missões dos comandos combatentes.

3) Validar e refinar continuamente um mecanismo de comando e controle adaptável para operações cibernéticas.

4) Estabelecer uma capacidade de simulação e modelagem cibernética com a criação de algorítimos para avaliar a eficácia das operações cibernéticas. e

5) Avaliar a capacidade da Força Missão Cibernética.

Para avaliar essa capacidade, o Estado-Maior Conjunto, com o apoio de USCYBERCOM e outros componentes do DoD, proporão, coletarão, analisarão e relatarão um conjunto apropriado de métricas para o Principal Consultor Cibernético medir a capacidade operacional das CMF. Essas métricas incluirão atualizações sobre o status de USCYBERCOM e de suas capacidades de contingência para promover o desenvolvimento de

capacidades e proficiência, bem como acessos e ferramentas que podem ser requerido em uma contingência.

2º Objetivo - Defender sua rede de informações, tornando seguros seus dados e mitigando os riscos nas missões do Pentágono;

O DoD deve tomar medidas para identificar, priorizar e defender suas redes mais importantes, uma vez que a totalidade de ataques a seus dados é muito grande para que possa realizar suas missões de forma eficaz. Também deve planejar e realizar exercícios em um ambiente cibernético degradado e interrompido no caso de um ataque às suas redes de dados e finalmente, deverá elevar o nível de tecnologia e inovação para se manter à frente das ameaças, sem deixar de trabalhar com o setor privado para ajudar a proteger os dados do comércio de base industrial de defesa e estar preparado para ajudar outras agências a fortalecer as redes e dados dos EUA contra ataques cibernéticos e espionagem cibernética.

A estrutura de segurança única do Ambiente Conjunto de Informações (JIE) permitirá uma defesa de rede robusta e mudará o foco de proteger redes e sistemas específicos de serviços para proteger o empreendimento do DoD de forma unificada se desenvolvida com uma conscientização cibernética aprimorada, implantada em resposta a requisitos validados e capaz de acomodar futuras medidas defensivas.

Para atingir tal propósito, deverá:

a) Garantir a eficácia da sede da Força Conjunta para as operações da rede de informações do DoD (DoDIN). Operando subordinadamente à USCYBERCOM, a Sede da *Joint Force* - DoDIN coordenará a defesa da rede e mitigará os riscos cibernéticos para as operações e missões do DoD, que por sua vez avaliará, validará e implementará totalmente o conceito do *Joint Force Headquarters*-DoDIN;

b) Implementar uma capacidade para mitigar todas as vulnerabilidades conhecidas, principalmente as de alto risco passíveis de serem exploradas por adversários;

c) Otimizar o atual Serviço de Defesa de Rede de Computadores DoD *Provider* (CNDSP) verificando se os atuais processos do CNDSP são suficientes para defender as redes contra ameaças conhecidas e projetadas no ciberespaço e se as atuais forças do CNDSP estão adequadamente treinadas e equipadas para se defender contra ameaças avançadas;

d) Avaliar e iniciar melhorias para a segurança cibernética dos sistemas de armas atuais e futuros, baseando-se nos requisitos operacionais. Para todos os futuros sistemas de armas que o DoD adquirir ou desenvolver, será exigido padrões específicos de segurança cibernética para sistemas de armas. A política e a prática de aquisição serão atualizadas para promover uma cibersegurança efetiva ao longo do ciclo de vida de um sistema;

e) O DoD criou equipes chamadas de Equipes Vermelhas para testar e monitorar redes vitais e sistemas de missão na deteção de vulnerabilidades e para melhor monitorar as redes no Centro de Operações da Unidade de Missão Cibernética. Como parte deste trabalho, todos os principais exercícios devem incluir uma equipe de *cyber* vermelho para testar as suas defesas cibernéticas em um cenário realista em que o Departamento poderia ter suas operações interrompidas por um adversário; e

f) O DoD estabelecerá uma Célula de Proteção e Exploração Conjunta (JAPEC) para vincular agentes de inteligência, contrainteligência e policiais a gerentes de programas de aquisição para prevenir e mitigar a perda de dados e roubo. Também conduzirá avaliações de riscos, danos de espionagem cibernética e roubo para informar sobre os requisitos, aquisição, cursos de ação programáticos e de contra-inteligência.

Não menos importante, os Departamentos Militares e o Subsecretário de Defesa para Inteligência, em consulta com o Principal Conselheiro Cibernético, desenvolverão uma

estratégia para a aprovação do Secretário de Defesa que maximiza as capacidades e autoridades das agências de contrainteligência dos departamentos militares para identificar, atribuir e defender contra espiões cibernéticos.

E, por último, deve-se lembrar que as autoridades de contra-espionagem estão posicionadas para combater a espionagem cibernética. A estratégia especificará como as agências de inteligência do DoD colaborarão mais efetivamente com as comunidades de inteligência e aplicarão a lei em investigações e operações para impedir o furto de propriedade intelectual contra os EUA, seus aliados e parceiros.

3ºObjetivo: Estar preparado para defender o território e os interesses vitais estadunidenses contra ataques cibernéticos de consequência significativa.

O DoD deve trabalhar com seus parceiros estatais, o setor privado e e as nações parceiras para deter e, se necessário, derrotar um ataque cibernético de conseqüências significativas em seu território. Também deve desenvolver sua inteligência, e capacidades operacionais para mitigar ataques cibernéticos antes que eles possam causar impacto em ativos sensíveis.

Ele trabalhará com a comunidade de inteligência mais ampla para desenvolver capacidades de inteligência sobre atividades adversárias e debelar ataques cibernéticos antes que eles possam impactar os EUA e seus interesses. E, para atender aos requisitos de contingência do Comando Combatente, deverá expandir sua inteligência, redes adversárias humanas e técnicas. Assim como para operar efetivamente no ciberespaço é preciso requerer inteligência cibernética, alerta antecipado e conscientização situacional compartilhada por meio de todas as fases de uma operação potencial. Toda coleta de inteligência seguirá a lei e a orientação delineada nos pedidos do executivo.

A CMF e outros componentes relevantes do DoD formarão parcerias com organizações-chave interinstitucionais.Além disso, irá praticar procedimentos de emergência por meio de exercícios regulares em todos os níveis e apoiar exercícios interagenciais para praticar emergências e deliberar procedimentos de ação cibernética.

O DoD proverá uma estrutura a fim de cooperar com outras agências governamentais para conduzir as operações nacionais, fazendo parcerias com o FBI, a CIA e DHS para construir relacionamentos e integrar capacidades para fornecer ao Presidente o amplo leque de opções disponíveis para responder a um ataque de conseqüências significativas aos EUA.

Para desenvolver ferramentas automatizadas de compartilhamento de informações e assim, melhorar a consciência situacional compartilhada, o DoD fará parceria com o Departamento de Segurança Interna (DHS) e outras agências para desenvolver mecanismos padronizados, contínuos e automatizados para compartilhar informações com cada um de seus parceiros críticos como forças-chave aliadas, parceiras militares, governos estaduais, municipais e o setor privado. Além disso, o DoD trabalhará com outras agências do governo dos EUA e com o Congresso para apoiar a legislação que permite o compartilhamento de informações entre o governo dos EUA e o setor privado.

4º Objetivo - Disponibilizar opções viáveis de planos e operações cibernéticas para utilizar essas opções a fim de controlar escaladas de conflitos em todas as etapas

Durante períodos de tensões ou hostilidades, o DoD deverá poder fornecer ao Presidente uma ampla gama de opções para gerenciar a escalada do conflito. Se direcionado, também deve ser capaz de usar operações cibernéticas para interromper as redes de comando e controle de um adversário, infra-estrutura crítica e capacidade de suas armas.

Como parte de toda a gama de ferramentas disponíveis para os EUA, o DoD deve desenvolver opções cibernéticas viáveis e integrar essas opções aos planos departamentais.

Ele, da mesma forma, desenvolverá capacidades cibernéticas para atingir os principais objetivos de segurança com precisão, e para minimizar a perda de vida e dano à propriedade. E, finalmente, para garantir a unidade de esforço, permitirá que comandos combatentes planejem e sincronizem operações cibernéticas em todos os domínios das operações militares.

5ºObjetivo - Construir alianças e parcerias internacionais para conter ameaças comuns e para aumentar a segurança e a estabilidade internacionais.

Todas as três missões cibernéticas do DoD exigem colaboração próxima com aliados e parceiros estrangeiros. Sendo assim, dentro do seu engajamento cibernético internacional, busca construir uma parceria em segurança, defesa cibernética, e busca aprofundar parcerias operacionais, quando apropriado.

Dada a alta demanda e relativa escassez de recursos cibernéticos, o DoD deve fazer escolhas difíceis e concentrar suas iniciativas de capacidade de parceria em áreas onde os interesses dos EUA estão em jogo. Nos próximos cinco anos, seus esforços se concentrarão em parcerias com o Oriente Médio, com a Ásia-Pacífico e os principais aliados da OTAN. Ao longo desta estratégia, ele avaliará constantemente o ambiente internacional e desenvolverá parcerias inovadoras para responder a desafios e oportunidades emergentes.

O DoD permanecerá flexível e ágil à medida que constrói alianças e parcerias para melhor responder às mudanças no ambiente estratégico, e para isso deverá:
a) Desenvolver soluções para combater a proliferação de malware destrutivo qua atores estatais e não estatais procuram adquirir. A disseminação descontrolada de *malware* destrutivo para atores hostis representa um risco significativo para o sistema internacional.
b) Fortalecer o diálogo cibernético dos Estados Unidos com a China para melhorar a estabilidade estratégica. Ao longo desta estratégia, como parte das conversas consultivas de defesa EUA-China e diálogos relacionados, como o *Cyber Working Group*.

c) Continuar a manter discussões com a China para trazer maior compreensão e transparência à doutrina militar, política e governo de cada nação.

O DoD apoiará os esforços do governo dos EUA para fortalecer a confiança no relacionamento EUA-China. Além disso, o DoD continuará a levantar dúvidas sobre o roubo de propriedade intelectual, segredos comerciais e informações comerciais confidenciais por parte da China.

4.3 Capacidade estadunidense de realização de espionagem e produção de conhecimento de inteligência (Caso Snowden)[14]

De acordo com Harding (2014), por meio de suas atividades, a Agência Nacional de Inteligência dos EUA (NSA)[15] trabalhando em conjunto com a Agência de Inteligência Britânica (GCHQ), a CIA[16] e suas agências de interceptação em bases militares estadunidenses e embaixadas, realizavam irrestritamente diversas ações de coleta de informações de inteligência e espionagem[17] por meio da interceptação de dados em cabos submarinos de telecomunicações, de acesso à informações oriundas de satélites em conluio com o Reino unido e de rastreio de dados em aplicativos e dispositivos utilizados em todo o mundo e totalmente confiáveis até então como *Google*, *Skype*, telefones celulares, GPS, *YouTube*, Tor, e-commerce. A NSA também era capaz de receber informações das maiores empresas de telecomunicações dos EUA, inclusive de operações bancárias em uma vasta quantidade de Estados no mundo como a Coréia do Norte, China, Japão, Suíça, Oriente

[14] Ex-contratado da CIA e NSA que expôs as atividades principalmente dessas companhias entre outras em primeira mão ao jornal britânico: The Guardian, em 2013 segundo Harding (2014);
[15] Órgão subordinado ao Departamento de Defesa dos Estados Unidos (DoD) que realiza atividades de inteligência e de segurança das comunicações daquele Estado segundo Harding (2014);
[16] Agência Central de Inteligência estadunidense é uma agência de inteligência responsável por investigar assuntos de segurança nacional e por tomar parte em assuntos secretos quando necessário segundo Harding (2014);
[17] É uma ação realizada por um agente adverso que busca, de maneira clandestina, acesso a informações sensíveis ou sigilosas de instituições nacionais ou internacionais para beneficio específico de grupos de interesse ou empresas. Disponível em:< http://www.abin.gov.br/atuacao/fontes-de-ameacas/espionagem/>. Acesso em 06 jul. 2018.

Médio, Brasil e inclusive o próprio EUA no intuito idealista de se defender contra ameaças de terrorismo e por outro lado, realista de realizar vigilância em massa com excessos comprovados que violavam inclusive a constituição dos EUA, o que motivou as denúncias de Eduard Snowden.

Uma grande variedade de dispositivos podiam ser monitorados desde que fossem eletrônicos como rádio, usassem microondas, tramitassem informações via satélites ou por cabos submarinos ou que pudessem ser interceptados. Além de informações colhidas por meio da Internet, a NSA já fazia um processo de engenharia social mesmo antes da existência da rede social *Facebook.*

As ações estadunidenses ainda eram potencializadas com o apoio do acordo de partilha de inteligência firmado entre os EUA e outros quatro Estados anglófonos como o Canadá, Nova Zelândia e Austrália além do Reino Unido já citado. O programa de espionagem, que era chamado de *Stellar Wind*, se tornou parcialmente público por meio do *New York Times* em 2005. Por esse motivo, o então ex-presidente George W. Bush (2001-2009) confirmou apenas o que a imprensa noticiou, e de forma astuta, o chamou de Programa de Vigilância Terrorista. Como a quarta emenda da constituição dos EUA proíbe buscas e apreensões sem justificativas contra cidadãos estadunidenses, interceptações de comunicação, se tornam ilegais e só são aceitas somente contra um suspeito específico, apoiadas por uma "causa provável" e mediante emissão de um mandado judicial. O que tinha começado de forma ilegal passou a ser aprovado pelo congresso sem que muitos entendessem sua real motivação. A política de espionagem não só continuou, como foi ampliada no governo Barack Hussein Obama (2009-2017), e agora as investigações passaram a estar reforçadas e legalizadas com mandados judiciais. (HARDING, 2014).

Em relação à teoria de Ratzel, os EUA, favorecidos pela sua posição tecnológica e financeira desenvolveu uma capacidade cibernética consistente e mais profunda que o Brasil

como é demonstrado pela composição das 133 equipes cibernéticas distribuídas pelas FFAA, pela aliança com os países francófonos, pela NSA e CIA, agências mundialmente atuantes, pelas tecnologias informacionais de origem nacional como o *Google, facebook e skipe* e pelos programas de espionagem. Essa capacidade permite a atuação dos EUA de forma ofensiva e exploratória permitindo a conquista de novos espaços, mais eficazmente, satisfazendo melhor a ambição de seu povo.

5- SINGULARIDADES E SIMILARIDADES ENTRE BRASIL E EUA

Nesse capítulo será comparado mais efetivamente como se comporta a atuação dos EUA e a brasileira no espaço cibernético verificando em ambos os Estados, suas atuações concretas, a busca por parcerias e suas atuações como protagonista de ataques ou como alvo deles.

5.1- Singularidades dos EUA e do Brasil

5.1.1 - Recursos comparados dispendidos em Guerra Cibernética

A expectativa é de que o CDCiber tenha recebido R$ 400 milhões de reais em investimentos até 2015, oriundos de sua fonte que é o Programa de Defesa Cibernética na Defesa Nacional. Segundo o general José Carlos dos Santos, chefe do CDCiber em 2012, a previsão é que cerca de dez projetos receberam esses recursos. De acordo com Matsuura (2016), criado oficialmente em 2012, este Comando gastou somente R$ 190 milhões do orçamento previsto até 2015. Apesar das restrições em geral, o CDCiber aprovou as operações em grandes eventos como a Rio+20, a Jornada Mundial da Juventude, a Copa das Confederações e a Copa do Mundo, porém, o Estado ainda não possui capacidade de se proteger de armas cibernéticas como o " Great Canon"[18].

De acordo com Fleck (2013), a previsão dos investimentos previstos para a Defesa Cibernética para pelo menos as próximas duas décadas é de menos de 0,5% dos R$ 208 bilhões a serem gastos em ações consideradas prioritárias pelo EB. Com a projeção de gastos de apenas R$ 840 milhões até 2035, o valor não chegaria a R$ 40 milhões anuais até 2035. Fazendo uma comparação com os esforços cibernéticos dos EUA, o investimento brasileiro na

[18] "Grande Canhão" é uma arma cibernética desenvolvida pela China que consegue redirecionar o tráfego de internautas estrangeiros que visitam seus sites para um alvo. Até agora, o "canhão" só foi usado para a censura, mas ele pode derrubar servidores estratégicos de um Estado.

área é relativamente inferior, só em 2014 o orçamento estadunidense foi de US$ 4,7 bilhões (cerca de R$ 18 bilhões de reais). Os gastos brasileiros incluem operações de capacitação, criação dos núcleos de defesa cibernética, a construção da sede definitiva do Centro de Defesa Cibernética e o desenvolvimento de um rádio definido por software.

Infelizmente, no Brasil estamos muito incipientes nos esforços e estabelecimento de prioridades quanto aos recursos alocados e destinados à proteção da segurança das comunicações governamentais e privadas. Os recursos destinados ao CDCiber, estão muito aquém de suas possibilidades.

5.1.2 – Detalhes relevantes da estratégia estadunidense:

a) Utilização de algoritmos para testar a eficácia das operações cibernéticas;

b) Avaliação e implantação de melhorias quanto à segurança cibernética em seus atuais e futuros sistemas de armas que serão adquiridos ou desenvolvidos;

c) Atração de especialistas da Guarda Nacional e da reserva para atuação na área;

d) Política de realização de exercícios em ambiente cibernético degradado e interrompido em nível nacional;

e) Utilização de equipes para testar e monitorar as redes vitais e sistemas para a detecção de vulnerabilidades; e

f) Desenvolvimento e atualização constante de uma rede de comando e controle cibernética e a partir de operações cibernéticas, interromper as redes de comando e controle do adversário;

É interessante mencionar que nos EUA dentro do setor privado onde as companhias controlam 90% do setor cibernético, o DoD atua em casos mais complexos, cabendo a elas o

monitoramento e resposta em casos de rotina e, no Brasil, cada empresa exerce e é responsável pela sua política de segurança cibernética.

5.2 – Similaridades entre o Brasil e os EUA

5.2.1 – Acordos de cooperação no campo cibernético

Em consonância com seu quinto objetivo estratégico, os EUA demonstram uma clara intenção em realizar alianças e parcerias internacionais, embora uma de suas ações seja o interesse específico em manter um diálogo cibernético com a China, o Brasil não ficou de fora. O setor cibernético tornou-se um fator de proximidade entre ambos os Estados. [19]Dois meses após ser divulgado o resultado da Chamada Conjunta para Projetos de Pesquisa e Desenvolvimento em Segurança Cibernética, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), em Brasília, foi visitado pelo diretor de Ciência da Computação da *National Science Foundation*[20] (NSF), Jim Kurose, para discussão do desenvolvimento de projetos afins entre os Estados.

Foi realizado um balanço a respeito dos dois workshops bilaterais em segurança cibernética já realizados, que reuniram pesquisadores e acadêmicos dos dois Estados, além de empresas do setor. O primeiro, em 2015, foi sediado no Brasil e o segundo, em 2016, nos EUA.

A visita do representante dos EUA mostrou seu entusiasmo e confirmou seu interesse em continuar investindo em pesquisas e soluções relacionadas à segurança cibernética, e em manter a parceria com o Brasil. Jim Kurose afirmou que existem cinco equipes mistas com integrantes dos dois Estados realizando pesquisas a serem desenvolvidas em dois anos com um orçamento disponível de US$ 3 milhões, pagos metade por cada Estado.

---

[19] Disponível em: <https://www.rnp.br/noticias/brasil-e-estados-unidos-alinhados-relacao-seguranca-cibernetica> Acesso em 06 jul. 18.

[20] É uma agência federal independente criada pelo congresso dos EUA em 1950, para entre outras coisas promover o progresso da ciência. Disponível em: <https://www.nsf.gov/about/> Acesso em 06 jul. 18.

O Brasil, nesse processo de cooperação, apresentou ideias para novas parcerias com os EUA, inclusive em outras áreas como TIC e de inteligência artificial e mostrou-se interessado em lançar uma nova chamada conjunta sobre segurança cibernética, aspecto importante na sua estratégia de transformação digital.

De acordo com o Departamento de Estado dos Estados Unidos (DoS)[21], foi realizado entre 25 e 26 abril do corrente ano, um acordo bilateral[22] de cooperação cibernética e política de uso da Internet. Representantes dos EUA e do Brasil compuseram um grupo de trabalho de TIC para reforçar o compromisso de manutenção de um espaço cibernético interoperável e seguro. O grupo de trabalho focou em segurança na Internet, proteção e livre fluxo de dados assim como foi discutido recentes desenvolvimentos na área para aplicações regionais e internacionais. Foi realizado um acordo de Defesa Cibernética e de combate aos crimes cibernéticos. O acordo também inclui o compartilhamento de boas práticas em proteção de dados, de cruzamento de informações de interesse e de cooperação militar.

Entre 2015 e 2016, foram realizados em duas etapas, uma em Brasília e a segunda na Flórida um *workshop* em Segurança e privacidade Cibernética[23] onde Brasil e EUA formalizaram um acordo para lançar chamada pública conjunta para pesquisas em segurança cibernética. Após a segunda etapa, o Ministério da Ciência, Tecnologia e Inovação (MCTI) e a *National Science Foundation* (NSF) dos EUA assinaram memorando de entendimento para avançar na cooperação em cibersegurança.

[21] É o departamento responsável pelas relações internacionais. É um equivalente a um ministério das relações exteriores em outros Estados.
[22] Disponível em: < https://www.state.gov/r/pa/prs/ps/2018/05/282074.htm>. Acesso em 04 Jul.18.
[23] Disponível em: <http://www.brasil.gov.br/editoria/educacao-e-ciencia/2016/04/parceria-entre-brasil-e-eua-reforca-pesquisas-em-seguranca-cibernetica>. Acesso em 04 jul. 18.

De 14 a 25 de maio de 2018, o Com D Ciber realizou no Centro de Instrução de Guerra Eletrônica (CIGE), em Brasília, o "3º Estágio Internacional de Defesa Cibernética[24] para Oficiais das Nações Amigas". O Estágio teve como finalidades compartilhar os conhecimentos na área de Cibernética e estreitar os laços de amizade e cooperação entre as Forças Armadas do Brasil e de outros 16 Estados, dentre eles os EUA.

Também não poderíamos deixar de mencionar que ocorrerá na Flórida (EUA) de 01 a 10 AGO, o exercício combinado PANAMAX 2018 dirigido pelo Comando do Sul Estadunidense (US SOUTHCOM) que contará com a participação de representantes brasileiros. É um exercício multinacional com foco na segurança do Canal do Panamá e arredores incluindo operações conjuntas, combinadas e interagências para galgar uma resposta integrada diante de uma variedade de ameaças internacionais.

5.2.2 – Estratégias desenvolvidas no campo cibernético

Tanto o Brasil quanto os EUA estão alinhados nos seguintes aspectos relativos ao espaço cibernético:

a) A busca pela liberdade em usufruir do espaço cibernético como um todo e negar o uso do seu próprio espaço;
b) A criação de uma doutrina regulamentadora como base para a imersão nessa área;
c) A preocupação em recrutar pessoal civil ou militar, capacitar ou selecionar pessoal já capacitado para atuação responsável e objetiva, inclusive com plano de carreira;
d) A adequação de suas FFAA aos recursos disponíveis em TIC para utilização no setor;
e) A utilização de seus recursos na dissuasão, em incremento à capacidade operacional, na utilização quando possível em esforço de guerra; e

[24] Disponível em: < http://www.forte.jor.br/2018/05/14/3o-estagio-internacional-de-defesa-cibernetica-para-oficiais-das-nacoes-amigas/ Acesso em 06 jul.2018.

f) Desenvolvimento de uma iniciativa nacional para educação em cibersegurança;

Ambos os Estados possuem um Comando de Defesa Cibernético desde 2009, o USCYBERCOM, do lado estadunidense e o Com D Ciber, nacional. Analisando os comandos citados vemos que o Brasil concentrou seus esforços no EB, enquanto os EUA distribuíram em equipes cibernéticas dentre suas FFAA, de forma equilibrada.

6 – CONCLUSÃO:

O século XXI começou repleto de novidades, principalmente na área tecnológica e, dentre elas, as trazidas pela informática, onde podemos afirmar que transformaram o mundo principalmente por acelerar as comunicações, por reduzir o tempo de desenvolvimento de muitos processos e por alterar o rumo dos conflitos e a percepção de Estado mais forte.

O potencialmente mais forte, com certeza, passou a se preocupar em conhecer o domínio cibernético para operar em sua plenitude e se manter nessa posição. Esse ambiente passou a ser desenvolvido, frequentado e explorado e nele os recursos financeiros não são o aspecto determinante, o que pode permitir um grande número de nações a ter algum envolvimento relevante e vir a oferecer alguma ameaça a Estados que gozavam até então de grande supremacia, protegidos por sua capacidade tecnológica, por seus recursos bélicos ou insularidade.

Na Guerra Cibernética, nenhum dos fatores citados representa motivos de intimidação por si só. O conhecimento de TIC e de informática, que não requerem investimentos maciços, transformam um cidadão comum em um indivíduo especializado que pode ser recrutado para contribuir na proteção dos sistemas de uma nação ou para realizar ações de espionagem ou de ataque em Nações de interesse, como foi o caso do estadunidense Edward Snowden.

O domínio do Espaço Cibernético passou a representar a conquista de novos territórios, pelo aumento do alcance na área das comunicações, pelo encurtamento de distâncias, pelo processamento mais acelerado pelas empresas de suas atividades e, por fim, pelos sofwares desenvolvidos, que passaram a controlar muitos equipamentos, inclusive os militares, utilizados pelas FFAA no transcurso dos conflitos.

A teoria escolhida, desenvolvida por Ratzel, legitima as nações à busca pelo desconhecido, à ampliação do espaço e leva em consideração os recursos humanos. Nesse

contexto, Brasil e EUA exploram o campo cibernético de forma organizada, cada qual com a sua doutrina desenvolvida.

A teoria do Espaço Vital é reinvindicada pelo Brasil e pelos EUA. Ambos lutam pela conquista de novos espaços cibernéticos. OS EUA vão mais longe impulsionados pela sua TIC mais desenvolvida e por investimentos financeiros muito maiores o que denota uma maior ambição de seu povo nessa área.

Em relação à definição, os EUA atuam de forma mais ofensiva, em virtude da expressiva quantidade de ataques que sofre e pelos recursos financeiros substanciais atribuídos a esse setor. O Brasil pelo contrario, atua mais defensivamente, devido aos menores investimentos e também por sofrer ataques em menor vulto. Outro aspecto importante é a preocupação demonstrada por ambos os Estados em proteger seus sistemas de informação com as estruturas criadas e a preocupação na produção de conhecimentos de inteligência, tanto pela CIA e a NSA, estadunidenses, quanto pelo EMA e o ComOpNav, no Brasil, nas Subchefia de Comando e Controle e Subchefia de Inteligência Operacional, respectivamente.

As estruturas de defesa cibernética de ambos, como são hoje, foram criadas em 2009. Coube ao EB, no caso do Brasil, concentrar a maior parte do esforço cibernético e às FFAA estadunidenses receber parcelas bem distribuídas deste esforço. De forma similar, foram elencados objetivos estratégicos no campo cibernético, mostrando que são similares desde o preparo de pessoal qualificado, a defesa do Estado contra ataques cibernéticos, até a realização de parcerias estratégicas.

Enquanto o Brasil de forma eficiente manteve a segurança no campo cibernético dos grandes eventos realizados entre 2012 e 2016 com as limitações financeiras que impedem o CDCiber de atuar de forma ofensiva, os EUA trabalhavam em outro patamar como foi averiguado pela denúncia de Snowden. A partir de suas agências foi possível explorar o

espaço cibernético de forma ampla com total liberdade desde os próprios estadunidenses até outras Nações de interesse por todo o mundo, e seus chefes de Estado inclusive.

Apesar de ambos os comandos cibernéticos receberem recursos limitados, a limitação brasileira chega a ser mil vezes maior e sua atuação passa a ser modelada com base nisso. O estadunidense como vimos tem um alcance global e o Brasil praticamente interno ao seu território.

Cabe destacar algumas atuações atribuídas somente ao USCYBERCOM que mostra seu potencial como a capacidade de possuir dispositivos para verificar a eficácia de suas operações cibernéticas, a rotina em realizar exercícios em ambiente cibernético degradado ou interrompido e de verificar e corrigir constantemente suas vulnerabilidades. A iniciativa em aumentar a segurança cibernética dos atuais e futuros sistemas de armas das FFAA estadunidenses que serão adquiridos ou desenvolvidos e por fim a iniciativa de desenvolver e atualizar constantemente uma rede de comando e controle cibernética e a partir de operações cibernéticas, interromper as redes de comando e controle do adversário.

É interessante mencionar que nos EUA dentro do setor privado onde as companhias controlam 90% do setor cibernético o DoD atua em casos mais complexos cabendo a elas o monitoramento e resposta em casos de rotina e no Brasil cada empresa exerce e é responsável pela sua política de segurança cibernética.

Vimos que dentro da teoria os EUA e o Brasil ocupam seus lugares dentro do espaço cibernético que é determinado pelo grau de investimento e determina seu desenvolvimento e consequentemente amplia seu território cibernético no caso dos EUA e tenta impedir de ter seu território explorado no caso do Brasil.

Concluímos a partir das análises prévias que os EUA possuem a capacidade de defesa cibernética mais desenvolvida e que também realiza mais investimentos na área, e que a hipótese considerada estava incorreta onde apesar dela confirmar a posição brasileira

ocupando um patamar muito inferior na área, os EUA mesmo buscando prioritariamente realizar acordos de cooperação com Estados mais desenvolvidos ele não despreza Estados como o Brasil.

7 - REFERÊNCIAS BIBLIOGRÁFICAS

1) ABIN**. Cooperação Nacional.** Disponível em: <http://www.abin.gov.br/atuacao/ cooperacao/cooperacao-nacional/ > Acesso em 01 jul. 2018**.**

2) ALVES, Fernando**.** D'ANDREA, Edgar, **Inovando e Transformando em Segurança Cibernética. Disponível** em: < https://www.pwc.com.br/pt/publicacoes/servicos/ assets /consultoria-negocios/2016/tl-gsiss16-pt.pdf> Acesso em: 01 jul. 2018.

3) AMORIM, Celso. **Doutrina Militar de Defesa Cibernética.** DOU, 2014. 38p.

4) BARBOSA, Rubens. Defesa NET. EUA: **Cinco objetivos estratégicos para as missões de defesa cibernética**. Disponível em: <http://www.defesanet.com.br /cyberwar/noticia /20151/EUA--cinco-objetivos-estrategicos-para-as-missoes-de-defesa-cibernetica/>. Acesso em 20 mai. 2018.

5) BRASIL. Ministério da Defesa. **Defesa Cibernética obtém êxito em atuação durante a Copa**. Disponível em: <http://www.brasil.gov.br/editoria/seguranca-e-justica/2014/07/ defesa-cibernetica-tem-obtido-exito-em-atuacao-durante-a-copa>. Acesso em: 01 jun. 2018.

6) _____. Ministério da Defesa. JMJ 2013: **A participação da Defesa na Jornada Mundial da Juventude.** Disponível em: https://www.defesa.gov.br/noticias/4355-15-07-2013-defesa-a-participacao-da-defesa-na-jornada-mundial-da-juventude>. Acesso em 01 jul. 2018.

7) _____. Portaria n˚2777/MD, de 27 de outubro de 2014. **Núcleo de Comando de Defesa Cibernética**. Diário Oficial da União (DOU), Brasília, n. 208, 28 out. 2014. Seção 1, p.7.

8) _____. Portaria n˚2777/MD, de 27 de outubro de 2014**. Núcleo da Escola Nacional de Defesa Cibernética**. Diário Oficial da União (DOU), Brasília, n. 208, 28 out. 2014. Seção 1, p.7.

9) _____. Portaria n˚ 3.389/MD, de 21 de dezembro de 2012. **Política Cibernética de Defesa.** Diário Oficial da União (DOU), Brasília, n. 249, 27 dez. 2012b. Seção 1, p. 11-12.

10) CARVALHO, Paulo Sérgio Melo**, Desafios Estratégicos para a segurança e Defesa Cibernética, O Setor Cibernético nas Forças Armadas Brasileiras**. Brasília. Secretaria de Assuntos Estratégicos da Presidência da República. 2011. 22p.

11) CLARKE e KNAKE, Richard A. e Robert K, **Guerra Cibernética, A próxima ameaça à segurança e o que fazer a respeito**. Rio de Janeiro. Brasport. 2015. 241p.

12) DICIONÁRIO ONLINE DE PORTUGUÊS. **Dicio**. Disponível em: <https:// www.dicio. com.br/ cracker/ hacker/> Acesso em 01 Ago. 2018.

13) FLECK, Isabel. Folha de São Paulo. Mundo. **Investimento brasileiro para defesa cibernética representa 0,5% de orçamento do Exército para os próximos 20 anos.** Disponível em: <https://www1.folha.uol.com.br/mundo/2013/07/1310924-investimento-brasileiro-para-defesa-cibernetica-representa-05-de-orcamento-do-exercito-para-os-proximos-20-anos.shtml Consultado em 24/06/2018> Acesso em 06 jul. 2018.

14) FOLHA DE SÃO PAULO, **Itamaraty sofre onda de ataques de hackers.** Disponível em: <https://www1.folha.uol.com.br/mundo/2014/05/1460646-itamaraty-sofre-onda-de-ataques-de-hackers.shtml> Acesso em 02 jul. 2018.

15) HARDING, Luke. **Os arquivos Snowden**. São Paulo. Texto Editores LTDA. 2014. 192p.

16) JORNAL NACIONAL, **Sites do governo sofrem maior ataque hacker da história,** Disponível em: < http://g1.globo.com/jornal-nacional/noticia/2011/06/sites-do-governo-sofrem-maior-ataque-hacker-da-historia.html> Acesso em 02 jul. 2018.

17) LANDES, David. S, **Riqueza e a Pobreza das Nações**, Rio de Janeiro, Editora Elsevier LTDA, 1998, 760 p.

18) MATSUURA, Sergio. O Globo Sociedade e Tecnologia. **Brasil terá Escola Nacional de Defesa Cibernética**. Disponível em: <https://oglobo.globo.com/sociedade /tecnologia /brasil-tera-escola-nacional-de-defesa-cibernetica-15914957> Acesso em 24 Jun. 2018.

19) O GLOBO, **Anonymous diz que roubou dados de sites do governo e da prefeitura do RJ.** Disponível em: < http://g1.globo.com/rio-de-janeiro/olimpiadas/rio2016/noticia/2016/08/anonymous-brasil-diz-que-roubou-dados-de-seis-sites-do-governo-do-rj.html. Acesso em 01 jul. 2017.

20) OLIVEIRA, João Roberto**, Desafios Estratégicos para a segurança e Defesa Cibernética, Sistema de Segurança e Defesa Cibernética Nacional: Abordagem com Foco nas Atividades Relacionadas à Defesa Nacional**. Brasília. Secretaria de Assuntos Estratégicos da Presidência da República. 2011. 24p.

21) OLIVEIRA M. et al. **Guia de Defesa Cibernética na América do Sul**, Recife. UFPE. 2017, 85p.

22) OLIVEIRA, Paulo Humberto Cesar. **Manual de Campanha de Guerra Cibernética**. Boletim do EB nr 25 de 23 Jun. 2017. 2017. 45p.

23) SYMANTEC, **Internet Security Threat Report (ISTR) Volume 21, abril 2016**. Disponível em:< https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf> Acesso em 01 jul. 2018.

24) TEC MUNDO, **Brasil é o terceiro país que mais realiza ataques cibernéticos no mundo.** Disponível em: <https://www.tecmundo.com.br/ataque-hacker/85053-brasil-terceiro-pais-realiza-ataques-ciberneticos-mundo.htm> Acesso em 02 jul. 2018.

25) TECNOLOGIA E DEFESA. **10 perguntas para o general Okamura, comandante da Defesa Cibernética do Exército Brasileiro.** Disponível em: <http://tecnodefesa.com.br/10-perguntas-para-o-general-okamura-comandante-da-defesa-cibernetica-do-exercito-brasileiro/> Acesso em 27 Jun. 2018.

26) TECHNOLOGY E INTELLIGENCE: **Fake News, o que é exatamente**. Disponível em: https://www.telegraph.co.uk /technology/0/fake-news-exactly-has-really-had-influence/ Acesso em 01 Ago. 2018.

27) TODA MATÉRIA. **Segunda Revolução Industrial**. Disponível em: https://www.todamateria.com.br/segunda-revolucao-industrial/>. Acesso em 08 jul. 18.

28) TOSTA, Octavio, **Teorias Geopolíticas**, Rio de Janeiro. Biblioteca do Exército. 1984. 103p.

29) U.S Department of Defense, **Cyber Mission Force Achieves Full Operational Capability**. Disponível em: <https://www.defense.gov /News/Article /Article/ 1524747/cyber-mission-force-achieves-full-operational-capability17/MAI/2018>. Acesso em 19 mai. 2018.

30) VEIGA, Ricardo**. A Defesa Cibernética (Def Ciber) Na Visão da Força Aérea Brasileira (FAB).** FAB. 2012.

ANEXO A

2015 País/Região	2015 Bots (%) no Mundo	Porcentagem de Mudança dos Bots por País/Região	2014 País/Região	2014 Bots (%) no Mundo
1 China	46.1%	+ 84.0%	1 China	16.5%
2 Estados Unidos	8.0%	- 67.4%	2 Estados Unidos	16.1%
	5.8%	-54.8%	3 Taiwan	8.5%
4 Turquia	4.5%	+29.2	4 Itália	5.5%
5 Itália	2.4%	- 71.2 %	5 Hungria	4.9%
6 Hungria	2.2%	- 69.7%	6 Brasil	4.3%
7 Alemanha	2.0%	- 58.0%	7 Japão	3.4%
8 Brasil	2.0%	-70.1%	8 Alemanha	3.1%
9 França	1.7%	-57.9%	9 Canadá	3.0%
10 Espanha	1.7%	- 44.5%	10 Polônia	2.8%

TABELA 1 – Top 10 de países origem de ataques cibernéticos. Fonte Symantec Spam ISTR 21(2016), p. 60.

ANEXO B

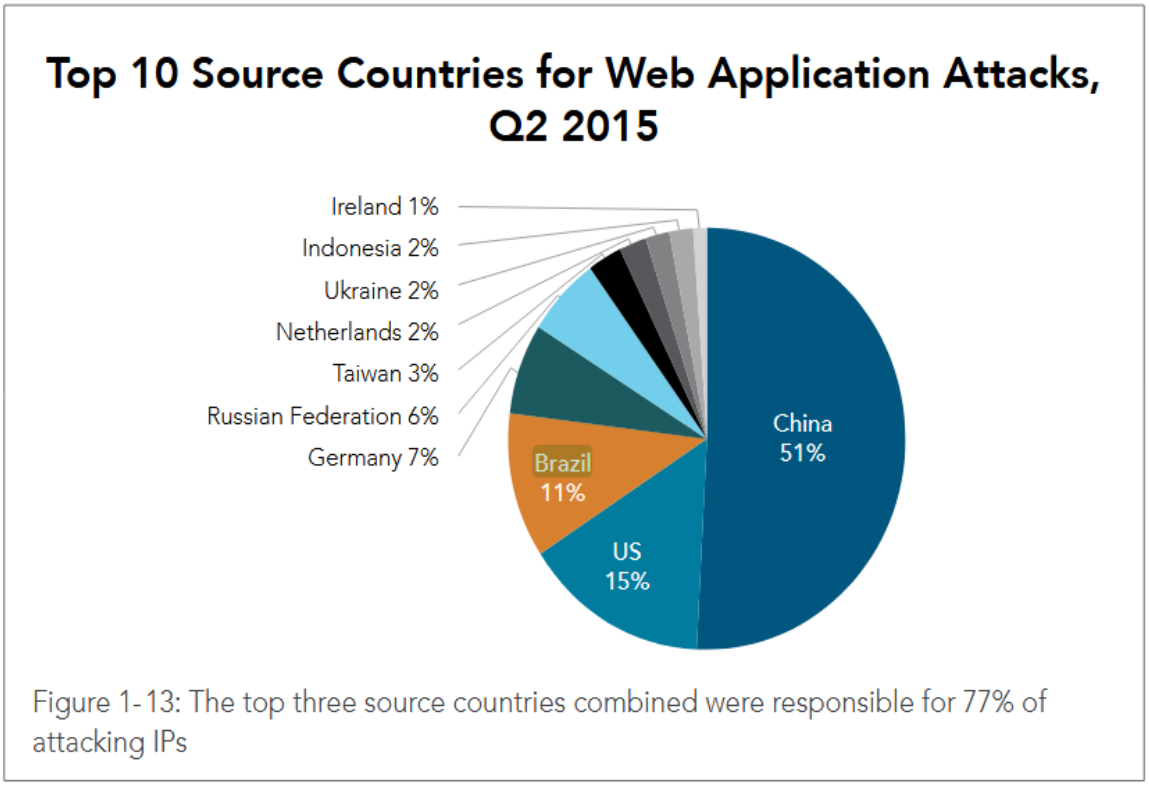
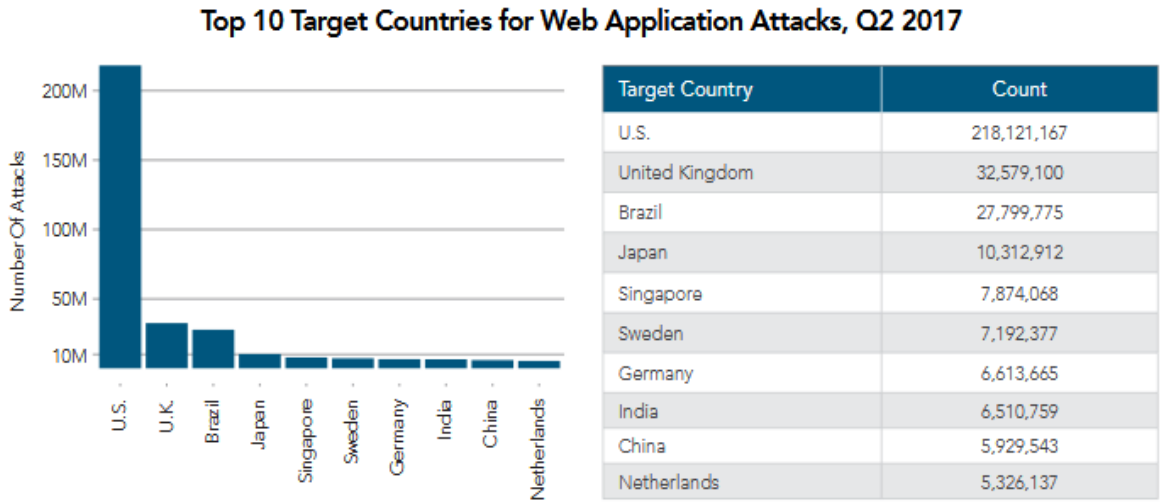


Figura 1: Relatório de segurança de ameaça na Internet. Top 10 países fontes de ataque na Web, 2º trimestre de 2015. Disponível em <https://www.akamai.com/kr/ko/multimedia/documents/state-of-the-Internet/2015-q2-cloud-security-report.pdf> Acesso em 15 jul. 2018.

ANEXO C

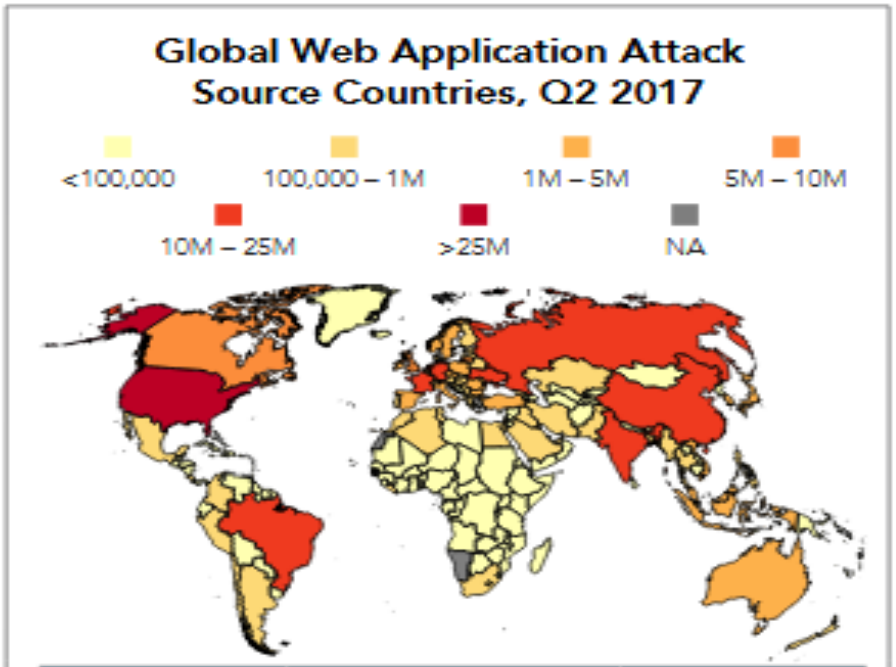


Target Country	Count
U.S.	218,121,167
United Kingdom	32,579,100
Brazil	27,799,775
Japan	10,312,912
Singapore	7,874,068
Sweden	7,192,377
Germany	6,613,665
India	6,510,759
China	5,929,543
Netherlands	5,326,137

Figure 3-6: The U.S. dominated as the primary target for attackers again in Q2

Figura 2: Relatório de segurança de ameaça na Internet. Brasil como alvo de ataques WEB, 2º trimestre de 2017. Disponível em: <https://www.akamai.com/de/de/multimedia /documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf> Acesso em 15 jul. 2018.

ANEXO D



Country	Attacks Sourced	Percentage
U.S.	122,425,660	33.8%
China	37,048,489	10.2%
Brazil	29,613,511	8.2%
Netherlands	23,003,848	6.4%
India	11,874,529	3.3%
Ukraine	11,791,345	3.3%
Russia	11,401,965	3.1%
France	10,605,255	2.9%
Germany	10,365,340	2.9%
Canada	7,892,141	2.2%

Figura 3: Relatório de segurança de ameaça na internet. Brasil como fonte de ataques WEB, 2º trimestre de 2017. Disponível em:< https://www.akamai.com/de/de/multimedia /documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf> Acesso em 15 jul. 2018.