CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA

CURSO DE BACHARELADO EM RELAÇÕES INTERNACIONAIS

CIBERDEFESA: ESTRUTURA DE DEFESA CIBERNÉTICA BRASILEIRA

DANIELLY ALCINA FREITAS DE SENA

Caruaru

2016

CENTRO UNIVERSITÁRIO TABOSA DE ALMEIDA

CURSO DE BACHARELADO EM RELAÇÕES INTERNACIONAIS

CIBERDEFESA: ESTRUTURA DE DEFESA CIBERNÉTICA BRASILEIRA

Monografia apresentada por Danielly Alcina Freitas de Sena, ao curso de Relação Internacionais do Centro Universitário Tabosa de Almeida, como exigência para obtenção do grau de bacharel em Relações Internacionais, sob a orientação da Profª Ma. Mariana Lyra

Caruaru

2016

BANCA EXAMINADORA

Aprovada em: 06/12/2016.

Presidente: Profª Ma. Mariana Lyra

Primeiro Avaliador: Prof. Dr. Saulo Miranda

Segundo Avaliador: Prof. Dr. Saulo Souza

CARUARU

2016

AGRADECIMENTOS

Gostaria de agradecer, primeiramente, aos meus pais que sempre me apoiaram no decorrer de minha formação e me encorajaram em todos os momentos da minha vida, aos meus irmãos Ítalo e Drielly que sempre estiveram presentes, me incentivando e apoiando para que eu conseguisse terminar essa etapa da minha vida.

Agradeço também aos meus amigos Daiane, Priscila, Silvia, Everton, Juliene, Michael, Jorzelia, que me acompanharam em toda graduação, pelo apoio e ajuda nos diversos momentos, pelos momentos de descontração e as viagens que sempre foram as mais divertidas. Também a minha amiga Nathalia que sempre esteve disposta a ajudar nas mais diversas coisas. A minha amiga Andrya que apesar de não me acompanhar durante todos os anos de formação me incentivou muito.

A minha professora orientadora Mariana Lyra que me ajudou muito no desenvolvimento desse trabalho, sempre disponível e aumentando os prazos para entrega dos capítulos, por toda contribuição e dedicação.

Gostaria de agradecer também ao professor Fábio que me deu várias referências e me incentivou na criação do meu projeto. A Gills Lopes (UFPE) que me ajudou fornecendo estudos sobre o tema.

RESUMO

O ciberespaço é um ambiente que ainda é desconhecido seu limite, por essa razão não se sabe ao certo todas as ameaças que podem surgir. O avanço cada vez mais rápido da tecnologia permite o desenvolvimento das chamadas “armas cibernéticas”, cada vez mais sofisticadas, dificultando as manobras defensivas dos Estados e atingindo suas infraestruturas críticas. Esse cenário é o mais novo campo de atuação de diversos atores das Relações Internacionais. Assim, a presente pesquisa busca definir o ciberespaço e esclarecer como é o funcionamento e da Defesa Cibernética brasileira, suas ofensivas e defensivas e como é gerada a influência do Brasil na Governança da Internet. Com esse intuito será necessário usar a teoria concebida pela Escola Copenhague para explicitar o processo de securitização do espaço cibernético, utilizando-se da abordagem descritiva e de instrumentos, como a análise bibliográfica e documental, que visa uma melhor demonstração sobre os órgãos que estruturam a defesa cibernética nacional — assim, como os ataques originados e sofridos, pelo Estado brasileiro. Para que dessa forma se possa ter uma visão mais ampla de como encontra-se a Defesa Cibernética brasileira atualmente, tornando possível uma futura análise sobre o desenvolvimento da Ciberdefesa nacional. Dessa forma concluísse que a ciberdefesa brasileira deve ser constantemente melhorada para alcançar a demanda criada nos últimos anos.

Palavras Chaves: Ciberespaço. Segurança Nacional. Defesa Cibernética. Brasil.

ABSTRACT

Cyberspace is an environment that is still unknown its limit, for that reason is not known for sure all the threats that can arise. The rapidly advancing technology allows the development of increasingly sophisticated so-called "cyber weapons", hampering the defensive maneuvers of states and reaching critical infrastructures. This scenario is the new field of action of several actors of International Relations. Thus, the present research seeks to define cyberspace and clarify how the Brazilian Cyber Defense is functioning and its offensive and defensive and how the influence of Brazil in Internet Governance is generated. With this in mind, it will be necessary to use the theory conceived by the Copenhagen School to make explicit the process of securitization of the cybernetic space, using a descriptive approach and instruments, such as bibliographical and documentary analysis, aimed at a better demonstration of the organs that structure the National cyber defense — as well as the attacks originated and suffered by the Brazilian State. So that a broader view of how the Brazilian Cyber Defense can be found today, making possible a future analysis on the development of national cyber defense. In this way, it is concluded that Brazilian cyber-defense must be constantly improved to meet the demand created in recent years.

Key words: Cyberspace. National Security. Cyber Defense. Brazil.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ABIN	Agência Brasileira de Inteligência
BRICS	Brasil, Rússia, Índia, China, África do Sul
CASIC	China Aerospace Science & Industry Corporation
CGI	Comitê Gestor da Internet
CLTI	Centro Local de Tecnologia de Informação
COMAER	Comando da Aeronáutica
COTEC-TI	Comissão Técnica de Tecnologia de Informação
COTIM	Conselho de Tecnologia da Informação da Marinha
CSEC	Communications Security Establishment of Canadá
CTIM	Centro de Tecnologia de Informação da Marinha
CTIR	Centro de Tratamento de Incidentes de Segurança de Redes de Computadores
CTIR.AER	Centro de Tratamentos de Incidentes de Redes da Aeronáutica
DCTIM	Diretoria de Comunicação e Tecnologia de Informação da Marinha
DSIC	Departamento de Segurança de Informação e Comunicação
EMA	Estado Maior da Armada
EMAER	Estado Maior da Aeronáutica
END	Estratégia Nacional de Defesa
EUA	Estados Unidos
GGE	Group of Governmental Experts
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IANA	The Internet Assigned Numbers Authority
IBAS	Fórum de Diálogo Índia, Brasil e África do Sul
ICANN	Assigned Name and Number
IGF	Internet Governance Forum
ITU	International Telecommunication Union
NASA	National Aeronautics and Space Administration

NSA	National Security Agency
OCDE	Organização para a Cooperação e Desenvolvimento Económico
ODG	Órgão de Direção Geral
ODS	Órgão de Direção Setorial
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
PNI	Política Nacional de Inteligência
SCTIC	Seção de Comando de Tecnologia e Comunicação
SI	Segurança Internacional
TIC	Tecnologia de Informação e Comunicação

SUMÁRIO

INTRODUÇÃO

A partir da década de 1980 o mundo passou por transformações nunca antes vistas com o advento da internet, trazendo um cenário em que não havia delimitações de fronteiras e muito menos de sua total extensão. A criação do espaço cibernético fez com que as relações internacionais se modificassem, como um todo, pois todas as noções territoriais não seriam aplicadas no ciberespaço.

Junto com o desenvolvimento cada vez mais rápido das tecnologias de informação e comunicação (TIC), fez com que as ameaças em sua dimensão também se ampliassem. Essas ameaças à soberania tornam-se cada vez mais presentes graças à espionagem cibernética; ataques a órgãos de vital importância para a sobrevivência e manutenção do Estado estão muito mais recorrentes nos últimos anos. A ocorrência de ataques cibernéticos tende a aumentar, devido aos constantes avanços de tecnologias voltadas à espionagem cibernética e ao desenvolvimento de vírus cada vez mais eficazes

Logo o objetivo desse trabalho é definir o espaço cibernético e seus impactos no espaço físico, observar a questão brasileira em sua estrutura de Defesa Cibernética: suas ofensivas e defensivas do Estado. A problemática abordada, trata-se de como se encontra a estrutura de Defesa Cibernética Nacional.

Nesse trabalho é usado o método de pesquisa bibliográfica e documental para um estudo de caso do Brasil, identificando qual é a situação atual do Estado no que se diz respeito à estrutura de Defesa Cibernética. A abordagem utilizada é a descritiva, através da coleta e análise dos dados. Os instrumentos para coleta de dados será a análise bibliográfica e documental, por meio de trabalhos científicos conceituados na área, também serão analisadas as leis, que determinam a utilização ciberespaço no Brasil.

Para melhor compreender o fenômeno, será utilizada a Escola de Copenhague, para descrever o espaço cibernético e sua securitização; o discurso sobre as ameaças cibernéticas; e as reais consequências que elas podem trazer para o território físico do Estado. É observado que não se pode separar a dimensão física da cibernética, já que elas reagem como reflexos uma da outra.

No entanto, apesar de estudos nessa área de pesquisa terem progredido muito, ainda há poucas pesquisas especificas da área de relações internacionais a respeito do tema, acarretando dificuldade, teórica, e analítica, para abordar a temática.

Esse estudo está estruturado em três capítulos, além da introdução e considerações finais. O primeiro capítulo apresenta o embasamento teórico, a partir da Escola de Copenhague e das definições de ciberespaço e defesa cibernética, ademais, também aborda a guerra cibernética e casos de confrontos que a demonstram. No segundo capitulo será visto a Estrutura de Defesa Cibernética brasileira e os principais órgãos responsáveis por ela. E por fim no terceiro capitulo será tratado da atuação do Brasil no ciberespaço por meio de casos de ataques realizados contra o país e ataques originários do Estado, além disso, também vai tratar do papel brasileiro para governança da internet.

1 CIBERESPAÇO NA SEGURANÇA INTERNACIONAL

O estudo da Segurança Internacional (SI), em suas raízes mais tradicionais, tem como base os conflitos entre Estados, Porem, com o passar dos anos foram surgindo conflitos que não se adequavam ao padrão estabelecido — conforme será explicado no item 1.1 deste trabalho. Dentre essas novas problemáticas enfrentadas pelo Estado, encontram-se as ameaças cibernéticas que em nenhum momento podem ser desconsideradas, dado o seu amplo grau de utilização em um mundo globalizado. Tratando-se de um ambiente em que perpassam um grande número de informação em alta velocidade e em amplitude, não é de se surpreender que tal cenário deixaria os seus usuários vulneráveis em relação aos outros usuários da rede.

Para melhor entendimento da evolução das ameaças cibernéticas, serão citados casos que demonstrem a evolução dos ataques cibernéticos. O primeiro caso abordado será o Morris, ocorrido em 1988 — ele foi um dos primeiros vermes reconhecidos por afetar a infraestrutura nascente do mundo — o verme se espalhou em torno de computadores em grande parte dos EUA, ele utilizava fraquezas do sistema UNIX. O programa era capaz de se propagar numa rede 8 horas após ser liberado, nesse tempo já havia infectado milhares de computadores. Dessa forma vários computadores foram danificados em poucas horas, porque o "verme" se reproduzia tão rapidamente que era impossível apagá-lo da rede, além do mais, esses vermes saturaram tanto a banda larga que a NSA [1]foi obrigada a desligar todas as conexões durante um dia inteiro.

Em 2006, quando a rede intranet da China *Aerospace Science & Industry Corporation* (CASIC) foram pesquisados, *spywares* foram encontrados nos computadores de departamentos classificados e líderes empresariais. No entanto só em 2007 o Ministério de Segurança de Estado declarou que 42% dos hackers vinham de Taiwan e 25% dos EUA, este ataque foi definido como roubo de informações nas áreas-chaves chinesas.

Em 2007, a NASA foi forçada a bloquear e-mails com anexo antes do lançamento do ônibus espacial com receio de ser hackeado. *A Business Week* relatou que os planos de novos ônibus espaciais dos EUA foram obtidos por intrusos estrangeiros desconhecidos.

[1] National Security Agency

Israel sofreu um ataque a sua infraestrutura de internet, em janeiro de 2009, durante a ofensiva militar a Faixa de Gaza. O ataque foi direcionado a sites do governo e foi executado em pelo menos 5.000.000 computadores. As autoridades do país acreditam que a culpa do ataque foi de uma organização criminosa baseada em um antigo estado soviético e financiado por Hamas ou Hezbollah.

Em 2010, um grupo denominado de *"Iranian Cyber Army"* interrompeu o serviço do navegador chinês Baidu. Os usuários eram redirecionados para uma página que mostrava uma mensagem política iraniana, o mesmo grupo que havia invadido o Twitter em dezembro do ano anterior, com uma mensagem semelhante.

No ano de 2011, o governo canadense notificou um grande ataque cibernético contra suas agências, incluindo *Defence Research and Development of Canada*, uma agência de pesquisa do Departamento de Defesa Nacional do país. O ataque forçou o Departamento de Finanças e do Conselho do Tesouro, principais agências econômicas do Estado, a se desconectarem da rede.

Em 2012, a empresa russa Kaspersky descobriu um cyber ataque global chamado de Outubro Vermelho — que teria sido utilizado pelo menos desde 2007 — ele era operacionalizado por meio de vulnerabilidades dos programas da Microsoft Word e Excel. Os principais atingidos foram os países da Europa Oriental, da antiga União Soviética e da Ásia Central. O vírus coletava informações das embaixadas dos governos, empresas de pesquisa, instalações militares, fornecedores de energia, nucleares e de outras infraestruturas críticas.

A partir dos eventos citados acima concluísse que o desenvolvimento cada vez mais rápido das tecnologias de informação e comunicação (TIC) fez com que as ameaças nesse espaço também se ampliassem. Consequentemente, os Estados têm se preocupado cada vez mais com o crescimento das ameaças no ambiente virtual e procurado maneiras de fortalecer suas defesas cibernéticas eficientemente, assim, como desenvolver ofensivas cibernéticas.

1.1 Securitização do Espaço Cibernético

Os Estudos de Segurança Internacional — em seu princípio e, sobretudo, as teorias ligadas ao Realismo Clássico — definia o Estado como único participante de

conflitos. Afinal, a maioria dos conflitos ocorria entre Estados.Todavia, após o fim da Segunda Guerra mundial, foi visto uma forma diferente de conflito que começou a ganhar atenção, as guerras interestatais e ataques terroristas, emergindo a necessidade de teorias que dessem conta dessas novas ameaças[2].

Levando em consideração tais fatos o presente trabalho utilizará a Teoria da Escola de Copenhague — que buscou reorganizar o sistema internacional no pós-Guerra Fria, ampliar e redefinir os temas a serem tratados pelos estudos de Segurança Internacional — os teóricos dessa corrente consideram a definição de segurança depende de sua colocação discursiva como uma ameaça existencial. Buzan, Weaver e Wilde apoiam que segurança é uma prática auto referencial, assim, a ameaça não seria objetiva, mas sim definida em um procedimento intersubjetivo (ACÀCIO, 2016, p.50).

A maneira de se instrumentalizar esta estrutura de análise dos temas de segurança na agenda pós-Guerra Fria, se dá pela definição das Unidades de Análise de Segurança, no qual o Objeto de Referência é definido como a coisa existencialmente ameaçada; o Ator Securitizador é aquele que securitiza a questão através do discurso, indicando que o Objeto de Referência está sendo ameaçado; Ainda existe também o Ator Funcional que utiliza de sua influência no processo de securitização. Partindo da visão de Buzan et al (1998) a respeito da securitização podem ser definidas três categorias para a demarcação de uma real ameaça: 1) não-politizado em que o Estado não vai lidar com a questão; 2) politizado, o tema torna-se parte da agenda política do governo e consequentemente requerendo decisões governamentais sobre diversos tipos de atribuições; 3) securitizado é a face extrema da politização, quando a ameaça é vista como existencial e demanda medidas emergenciais.

Como argumentado por Acácio (2016), apesar de Buzan e seus colaboradores, descreverem como é construída uma ameaça, não chegarem a argumentar especificamente a respeito do ciberespaço, ressalta-se que Hasen, Nissenbaum e Hart (2009) aplicam a teoria desenvolvida na Escola de Copenhague ao ciberespaço, que propõem — dada a relevância que o tema de Segurança Cibernética ganhou na agenda internacional — a adoção indutiva de um Setor Cibernético, com Unidades de Análise em Segurança e dinâmicas próprias, mostrando dessa maneira que a literatura de Relações internacionais está caminhando para aplicação operacionalizada da Escola de Copenhague na questão de Segurança Cibernética.

[2] Para detalhes da discussão sobre novas ameaças e novas guerras, ver Kalyvas (2001).

Dessa maneira, para melhor operacionalizar as categorias de securitização no cenário cibernético, Hansen e Nissenbaum (2009), retomam Buzan et al (1998) e seus colaboradores, na questão de que existe uma gramática de segurança específica – para aquele setor chamado de setor cibernético: a) hipersecuritização tem o pressuposto maior a colocação do tema como ameaça existencial em função da possibilidade de danos a serem causados por ataques cibernéticos nas esferas social, econômico e militar, atraindo, assim, os objetos de referência desses respectivos setores; b) práticas diárias de segurança, onde a gramática dos Estudos de Segurança é usada para aceitação da audiência, uma vez que os discursos englobam constantemente aspectos de Segurança Cibernética que atingem o cidadão, os objetivos que os Atores de Securitização possuem as características no Setor Cibernético, assegurando a parceria dos indivíduos para protegerem as redes e, principalmente, deixar a hipersecuritização mais aceitável, seguindo o princípio que os indivíduos passariam a ligar elementos catastróficos de ataques cibernéticos as atividades que realizam em seu cotidiano; c) tecnificações onde ocorre a despolitização da questão, já presente na agenda de Segurança do Estado, restringindo-a a opinião dos especialistas em Segurança da Informação e fazendo com que seja usada no discurso político.

Dessa maneira, o espaço cibernético passa a enquadrar-se no processo de securitização proposto pela escola de Copenhague, seguindo o princípio de que toda ameaça é construída, através do discurso e passam por processos de securitização como foi visto no último parágrafo. As ameaças cibernéticas passaram por esse processo e foram se consolidando cada vez mais, por causa dos ataques cibernéticos que se tornam cada vez mais frequentes, e deixando danos cada vez maiores nas partes vitais dos Estados. Assim, se fez necessário implementar na agenda de segurança a Defesa Cibernética.

1.2 Definição de Ciberespaço

Antes do seguimento da discussão a respeito da cyber defesa, é importante pontuar o que seria o ciberespaço. Cavelty (2012) o define como: In popular usage, we tend to use the terms cyberspace and internet almost interchangeably, even though the

internet is just one part of cyberspace, though certainly the most important one nowadays" (CAVELTY, 2012, p. 4).

Enquanto Rettray, Evans e Healey (2010) levantam que, em suas origens, na década de 1980, o espaço cibernético[3] primeiramente foi tratado como um ambiente eminentemente separado do mundo físico, dessa forma, ocorria à revelia das fronteiras nacionais e geográficas e, portanto, não era submetido às restrições subsequentes das bases da soberania e da segurança nacional. Entretanto, o ciberespaço possui bases em estruturas físicas, provenientes da conexão de sistemas e redes controlados por protocolos contidos nas fronteiras dos Estados. Tal sistema é propicio a mudanças frequentes, mas não de forma irrestrita.

Nesse contexto, é primordial que os países desenvolvam instituições e protocolos mutáveis, facilmente adaptáveis e sujeitos à aprendizagem, para aproveitar seu potencial da melhor maneira possível.

> Cyberspace, a concept coined in the 1980s, was viewed initially as a space fundamentally separate from the physical world. Some theorists went so far as to assert that cyberspace transcends geographic and national boundaries, and therefore strains traditional notions of sovereignty and security. Yet cyberspace is fundamentally a physical environment, created by connecting physical systems and networks, and managed by rules setin software and communications protocols — all of which are located in the sovereign boundaries of nation-states (RATTRAY; EVANS; HEALEY, 2010, p. 140).

Singer e Friedman (2014) observam a evolução da definição do que seria exatamente o ciberespaço e a partir dela definem que o ciberespaço é em sua essência em primeiro lugar e acima de tudo um ambiente de informação, ou seja, constituído por dados digitalizados que são criados, armazenados, e, o mais importante, compartilhados, assim, o ciberespaço perpassa o ambiente virtual, fazendo parte do mundo físico.

Para reforçar a ideia de espaço cibernético, Kuehl (2009) argumenta que o "cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store modify and exchange information via networked information systems and physical infrastructures" (KUEHL, 2009, s/p).

A partir do que foi apresentado, pode ser observado que o ciberespaço não se limita apenas à internet. Tais termos não podem ser intercambiáveis como sinônimos, assim como o fato do espaço cibernético não é apenas um espaço virtual, ele possui suas bases na estrutura física. Por encontrar-se nessas estruturas é considerada uma parte do

[3] No texto espaço cibernético e ciberespaço são utilizados como sinônimos.

sistema geográfico, uma geografia real não apenas um espaço virtual, composta por servidores, cabos, computadores, satélites e etc.

Assim pode ser analisado no caso do *Wikileaks*, que interfere diretamente na soberania estatal divulgando dados secretos de diversos países, que como consequência gera grande desconforto aos Estados. No entanto, o dilema territorial permanece; afinal não se sabe onde estaria a base física do *Wikileaks* e nem qual ator soberano teria o controle sobre ele. Esse dilema é uma consequência do desenvolvimento do espaço cibernético, pois nele existem ainda muitos espaços não explorados e outros como o caso *Wikileaks* que não podem ser reconhecidos ou controlados por Estados-nações em si.

1.3 Defesa Cibernética

Antes de aprofundar as questões ligadas à defesa nacional cibernética, faz-se necessário diferenciar o conceito de Defesa e de Segurança Cibernética. A Ciberdefesa enquadra-se na atuação do setor militar responsável por garantir a sobrevivência do Estado no que diz respeito a suas Forças Armadas. Normalmente todos os seus três componentes — a Aeronáutica, o Exército e Marinha — que são as principais fontes de defesa dos Estados, mesmo que algumas nações como os EUA incorporem mais forças a sua defesa (LOPES, 2013).

No caso da Segurança Nacional, Buzan et al (1998), classifica-a como procedimento para tratar a ameaça domestica como uma alegação, cuja finalidade reivindica poder para manobrar sem muito controle ou restrição democrática. Dessa forma, pode ser concluído que a Defesa Nacional combate ameaças de natureza normalmente externa que necessita a mobilidade das forças em domínio do Estado. Enquanto a Segurança Nacional, normalmente, requer resoluções internas como por parte da polícia ou até mesmo ministérios.

Em relação ao caso cibernético, a Defesa Cibernética é o conjunto de práticas defensivas, exploratórias e ofensivas em uma conjuntura de planejamento militar efetivadas no espaço cibernético. Isto é, uma tentativa de ressalvar a segurança nacional contra as cyber ameaças (LOPES, 2013).

Por outro lado, a Segurança Cibernética refere-se ao combate e à prevenção dos denominados crimes cibernéticos no campo da segurança pública, ou seja, segurança cibernética é um tema de investigação policial ou até mesmo por parte de ministérios públicos. Segundo a ITU, Segurança Cibernética trata-se de uma forma mais ligada a política e ao desenvolvimento de boas práticas:

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. (ITU, 2008, p. 2)

Dessa maneira, a segurança cibernética busca defender os usuários do ciberespaço dos chamados crimes cibernéticos, que segundo o Tratado do Conselho Europeu sobre Crimes Cibernéticos (2001): "classifica atividades como fraude e promoção de pedofilia na rede como ilegais; esclarece algumas questões de jurisdição e específica o que a polícia pode fazer para pegar e punir os criminosos." Já o Manual de Prevenção e Controle de Crimes Informáticos das Nações Unidas (1995) inclui fraude, falsificação e acesso não autorizado em sua definição de cybercrime.

Assim, o antivírus Norton (2016) observa que o cybercrime pode englobar uma gama muito ampla de ataques. Compreender essa ampla variedade de crimes cibernéticos é importante visto que os diferentes tipos de crimes cibernéticos requerem atitudes diferentes.

Conclui-se dessa forma, que diferentemente da Defesa Cibernética — que normalmente ocorre contra um ataque de origem estrangeira, com objetivos de espionagem, danificar ou inviabilizar partes da estrutura sensível nacional — os ataques tratados pela Segurança Cibernética inclui crimes cibernéticos que podem atingir diretamente usuários da rede como em casos de fraudes, pirataria ou acessos a dados restritos de outros usuários.

Tais crimes podem ter origem tanto nacional como internacional como em casos de redes de promoção a pedofilia e a pirataria. Esses delitos normalmente são resolvidos por órgãos do Estado como a polícia federal e demais órgãos mas não incluem necessariamente a participação do Exército como nos casos de Defesa Cibernética.

1.4 Guerra Cibernética

Para a priorização das questões de defesa, é necessário que existam ameaças externas. Quando se relaciona à questão da cibernética, elas são ainda maiores que as usuais — teorias tradicionais — afinal elas podem acarretar em ataques tanto no ciberespaço, como também podem causar destruição no espaço físico. Todos os ataques ao espaço cibernético resultam em danos na infraestrutura física, mas alguns deles — como será explicado na próxima seção — podem causar prejuízos muito maiores.

É importante considerar que desde seu preludio as Relações Internacionais basearam-se nas guerras e em relações comerciais. Como expõe Gonçalves (2016):

> Desde os primórdios da história da humanidade, as relações internacionais se fundamentam em dois alicerces: o comércio a guerra. E no mundo globalizado do século XXI, onde o comércio entre os povos alcança patamares nunca antes vistos, a guerra pelas defesas das riquezas e pela garantia desse comércio se vê também diante de uma nova dimensão. Assim, enquanto o século XX testemunhou o advento de uma terceira dimensão no fenômeno da guerra (a aeroespacial), o conflito no século XXI defronta-se com outra nova: o espaço cibernético. (GONÇALVES, 2016, p. 19-20).

Diferenciando-se dos conflitos ocorridos nos primórdios do século XX, surge um novo modelo de conflito, que Cruz Junior (2013) denomina de Guerra Fria Cibernética como está explicitado abaixo:

> A guerra fria cibernética vivida hoje apresenta uma diferença básica do período em que vigorou a guerra fria tradicional. Naquela época, havia um efeito "demonstração" de tecnologias militares que não se vê mais – pelo menos não abertamente como era feito. Praticamente todos os ataques cibernéticos ocorridos até então são apócrifos (CRUZ JUNIOR, 2013, p.10).

Pode ser notado que com os ataques cibernéticos é muito difícil atribuir a responsabilidade a outros países, pois o ambiente virtual utilizado de forma inteligente favorece o anonimato, Enquanto os avanços tecnológicos em tais áreas não possui grande visualização como ocorria nos conflitos do início do século XX. Nesse sentido, a maioria dos ataques não foram reconhecidos oficialmente, apenas há suposições e muitos ataques que permanecem sem autoria.

Como observa Clausewitz (2007), levando-se em conta que um dos principais instrumentos que determina uma guerra é a informação e a inteligência (estratégia), colocando-se tal afirmação em análise, incorporando ao ambiente do ciberespaço, pode ser notado que ele recebe grandes fluxos de informações a cada segundo, inclusive

informações de vital importâncias para os Estados. Então, o Estado ou grupo que possuir os recursos de filtrar as informações coletadas e a inteligência de utilizar estas informações estrategicamente ao seu favor conseguiria uma alta vantagem em relação ao país atingido. Assim, podemos observar que para conseguir defender-se adequadamente dos ataques cibernéticos externos, torna-se necessário investir cada vez mais no desenvolvimento das infraestruturas de base do ciberespaço e da tecnologia.

Para melhor compreender a guerra cibernética em sua complexidade, deve-se tomar casos concretos de ataques cibernéticos que tiveram grandes reflexos em estruturas estatais. Um dos ataques mais famosos e de grande proporção foi o vírus *Titan Rain*, descoberto em 2004, nos Estados Unidos. Os investigadores federais norte-americanos descobriram uma série contínua de ataques às redes dos departamentos de Defesa, Estado, Energia e Segurança Interna, bem como aqueles de empreiteiros da defesa, e *terabytes* de download de dados. Acredita-se que o vírus tenha entrado no sistema em 2003, com objetivo de espionagem. A culpa foi atribuída à China, além disso, tal ataque não limitou-se apenas aos EUA, também foi detectado no *British Foreign Office.*

O *Shady RAT* foi descoberto em 2011, pela empresa de antivírus *MacAfee*, que revelou a existência de uma companhia de pirataria que já contava com cinco anos de idade. Ela funcionav através do envio de um e-mail para um funcionário de uma organização visada, que, em seguida, instala um "Cavalo de Tróia[4]" no computador depois de haver clicado em um anexo aparentemente inofensivo.

As 49 vítimas incluem: o Comité Olímpico Internacional, as Nações Unidas, a Associação das Nações do Sudeste Asiático, empresas no Japão, Suíça, Grã-Bretanha, Indonésia, Dinamarca, Singapura, Hong Kong, Alemanha e Índia, e os governos dos Estados Unidos — Taiwan, Coreia do Sul, Vietnã e Canadá. Pelo menos 13 empresas de defesa dos EUA também foram atingidas — com base dos destinatários desses ataques muitos analistas passaram suspeitar de envolvimento chinês. Esse caso tem sido chamado o maior ataque cibernético de todos os tempos.

Em 2009, foi descoberta no Canadá uma rede de espionagem maciça, chamada de *Ghost Net*, que já havia se infiltrado em 103 países e mais de 1.295 computadores.

[4] Cada vez mais, os Cavalos de Tróia são o primeiro estágio de um ataque, e o seu objetivo principal é manterem-se ocultos enquanto fazem o download e a instalação de uma ameaça mais robusta, como um bot. Diferente dos vírus e worms, os Cavalos de Tróia não se propagam sozinhos. Eles normalmente são levados às suas vítimas através de uma mensagem de e-mail, na qual é mascarado como uma imagem ou piada, ou por um site malicioso, que instala o Cavalo de Tróia em um computador através de vulnerabilidades de navegadores da Web, como o Microsoft Internet Explorer. (NORTON BRASIL).

Entre os afetados também estavam o Ministério dos Negócios Estrangeiros e as embaixadas no Irã, Bangladesh, Indonésia, Índia, Coreia do Sul, Tailândia, Alemanha e Paquistão também foram afetados. Essa rede foi alegada ao Estado chinês, mas ele nega envolvimento.

Outro evento característico da guerra cibernética é, como explica Sandroni (2013), o verme *Stuxnet*. Ele infectou o sistema tecnológico da Siemens instalado em quatorze empresas iranianas e tinha como finalidade realizar espionagem e interrupção de operações. Especialistas observaram que a infestação do verme ocorreu via USB.

Entretanto, ainda não se sabe quando exatamente o *Stuxnet* entrou no sistema, alguns acreditam que desde 2009. A culpa deste ataque foi atribuída aos EUA e a Israel, com o objetivo de ataque as centrais nucleares iranianas.

Especialistas em segurança cibernética relataram que o *Stuxnet* seria a primeira superarma cibernética designada para destruir um alvo real, um alvo fora do mundo cibernético, diretamente no mundo físico – uma fábrica, uma refinaria, ou talvez uma usina nuclear. De acordo com o site de notícias do *website* "Poder Aéreo", o aparecimento do *Stuxnet* criou uma onda de espanto entre os especialistas de segurança informática. O *malware* é muito grande, muito codificado, complexo para ser compreendido instantaneamente. Ele tem em seu desenho, incríveis truques novos, como a tomada de controle de um sistema de computador sem o usuário tomar qualquer ação ou clicar em qualquer botão, apenas inserindo um *pendrive* infectado, ou seja, diferente de outros vírus que normalmente necessitam que o usuário clique em uma confirmação normalmente disfarçada, instala-se automaticamente.

O caso de espionagem mais recente e com maior envolvimento da mídia foi o caso Snowden de 2013, revelado em uma publicação do The Guardian. Edward Snowden apontou que a NSA coletou dados de ligações telefônicas de milhões de cidadãos americanos a partir do programa de monitoramento chamado de *PRISM*. Ainda afirmou que à Casa Branca acessava fotos, e-mails e videoconferências de quem usava os serviços de empresas como Google, Skype e Facebook, monitorava cidadãos em outras nações, além da descoberta de seu monitoramento diretamente ao chefe de Estado de países como o Brasil, França e Alemanha.

A operação *PRISM*, revelado no caso Snowden teve uma das maiores repercussões, pois se tratou de uma denúncia direta, diferenciando-se dos outros casos de espionagem que dificilmente se consegue acusar oficialmente uma Estado, pois os rastros deixados são muito poucos para fundamentar tal ato.

Além de ataques destinados à espionagem, ocorreram diversos ataques que influenciou diretamente na estrutura física dos Estados. Como o caso dos ataques a Estônia em 2007, o ataque distribuído de negação de serviço, que normalmente envolve o uso de computadores remotamente requisitados - conhecidos coletivamente como uma *botnet* - sobrecarregar um servidor web alvo, deixando-o *offline*. Que causou muitos prejuízos ao Estado já que ele é extremamente conectado, consequentemente muito dependente da rede. Este ataque foi atribuído a Rússia já que os ataques começaram depois de um dos símbolos ser movido.

Outro ataque também atribuído à Rússia ocorreu em 2008, durante a guerra Rússia-Geórgia, em que os principais sites georgianos, incluindo as páginas do Presidente Mikheil Saakashvili, do Ministério das Relações Exteriores e do Ministério da Defesa, bem como numerosos sites corporativos e de mídia, foram derrubados por ciberataques. Apesar de ter menor proporção, comparado aos ataques a Estónia, ele deixou o Estado georgiano em problemas deixando o site do líder do Estado inoperável por cerca de vinte quatro horas, através dos ataques distribuídos de negação de serviço (DDOS).

E mais recentemente, após o *Stuxnet,* foi descoberto o Flame. "Trata-se de um *cyberweapon*[5] *c*omplexo que forçaram o Irã a cortar suas plataformas Ministério do Petróleo a partir da Internet - teria sido escrito usando a mesma língua que jogos como o *Angry Birds* (TSUKAYAMA, 2012). O Flame é considerado vinte vezes mais potente que o *Stuxnet*. Além disso, o jornal Washington Post observa que o vírus foi encontrado também em computadores em todo o Estado Iraniano e ao que parece estaria relacionado ao *Stuxnet* e ao *Duqu* — ele é um sofisticado Trojan que parece ter sido escrito pelos mesmos autores do worm Stuxnet.

O Estado Iraniano novamente acusa os EUA e Israel. Nesse sentido, o Irã foi acusado da criação do vírus Shamoon que poderia ser uma resposta ao Flame, infectando os computadores da Saudi Aramco apagando parte de suas informações vitais em 2012.

Como demonstrado nesses exemplos, pode ser identificado que realmente está ocorrendo uma guerra cibernética em diferentes proporções, avançando conjuntamente com a evolução da tecnologia.

[5] Arma Cibernética.

O ciberespaço tem sido usado como auxílio nas estratégias nos tipos de ataques e guerras mais tradicionais, como, no caso do ataque a base nas margens do rio Eufrates, na guerra do golfo, e até mesmo na guerra do Iraque, por meio, da pirataria, e ainda há os casos de ataques de *drones*[6], comandados via satélite.

O caso ocorrido na margem do rio Eufrates no território Sírio em 2007 foi a destruição por meio de caças israelitas de uma base que seria responsável por tentar criar armas nucleares — a Síria havia adquirido recentemente um sistema de defesa aérea da Rússia, que não conseguiu detectar a presença dos aviões caça de Israel. Então, restou a dúvida de como os israelenses cegaram o sistema russo, por meio de uma ação direta no sistema de redes da Síria ou por um vírus instalado a distância por especialistas do governo israelita.

No episódio dos *drones*, como diz Padilha (2015), atualmente tais objetos são utilizados frequentemente não apenas como armas, trazendo mudanças significativas no setor civil. Com essa tecnologia seria mais fácil e em certa medida menos arriscado ganhar uma guerra. Tratando-se da sua utilização nos EUA, os ataques que normalmente utilizam *drones* em países em que ainda não foi declarado guerra formalmente, normalmente uma medida contra terroristas e também em casos de salvaguardar seu território por meio da vigia das suas fronteiras.

Clark e Knake (2010) consideram que a guerra cibernética existe e os casos que ocorreram até agora estão longe de demonstrar o potencial real do poder cibernético dos Estados.

> Cyber war is real. What we have seen so far is far from indicative of what can be done. Most of these well-known skirmishes in cyberspace used only primitive cyber weapons (with the notable exception of the Israeli operation). It is a reasonable guess that the attackers did not want to reveal their more sophisticated capabilities, yet. What the United States and other nations are capable of doing in a cyber-war could devastate a modern nation. (CLARK; KNAKE, 2010, p. 29-30).

Os mesmos autores observam, que pelo fato do espaço cibernético, tudo ocorre na velocidade da luz a guerra cibernética está acontecendo em uma velocidade tão alta que nenhum confronto de tamanha estatura havia sido visto antes. Observa-se sua amplitude, já que qualquer confronto na esfera do ciberespaço pode rapidamente se

[6] Drone é um apelido informal para todo e qualquer objeto voador não tripulado. Palavra de origem inglesa, drone significa "zangão" ou "zumbido". A palavra é uma associação ao som realizado pelo aparelho durante um voo. Se diferencia dos Veículos Aéreos Não Tripulado (VANT), por seus fins.

tornar global, pois os sistemas são totalmente interligados. Além de que a guerra cibernética não teria um campo de batalha, pois envolve todo o ciberespaço, mas ainda não se sabe até onde ele se estende, nem sua profundidade.

> Cyber war has begun. In anticipation of hostilities, nations are already "preparing the battlefield." They are hacking into each other's networks and infrastructures, laying in trapdoors and logic bombs—now, in peacetime. This ongoing nature of cyber war, the blurring of peace and war, adds a dangerous new dimension of instability. (CLARK, KNAKE, 2010, p.30).

Por outro lado, Bruce Schneier (2013), especialista em segurança cibernética, questiona todas as definições existentes de guerra cibernética. Ele garante que muitas vezes a definição de guerra cibernética não está bem aplicada, por que, ainda não se sabe como é de fato uma guerra no ciberespaço, quando uma guerra cibernética inicia-se e tampouco se sabe como fica o espaço cibernético quando a guerra termina. Ele também observa que há uma grande dificuldade em definir o que seria uma guerra cibernética, existindo uma confusão ou associação com táticas de guerra.

Assim, levando em consideração o que os autores propõem a respeito da guerra cibernética, sendo de vital importância que a defesa cibernéticas esteja bem desenvolvida para prevenir ataques cibernéticos, que possam danificar as nossas infraestruturas nacionais. Para isso é importante pesquisar, investir e desenvolver tecnólogos nas áreas que influem em nossa defesa cibernética.

2 ESTRUTURA BRASILEIRA DE DEFESA CIBERNÉTICA

Nesse seguimento será tratado das estruturas de defesa brasileiras e suas políticas de implementação. Para isso é importante primeiramente se observar o histórico de desenvolvimento da ciberdefesa no Estado. Como observa Celso Amorim em âmbito governamental, foi tratado inicialmente a partir do desenvolvimento da Segurança de Informação caracterizando-se com a criação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), por meio da Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001.

Assim, ela foi evoluindo gradativamente por sua necessidade cada vez mais frequente. Em 2006, por meio do Decreto nº 5.772, foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), dentro do GSI/PR, para coordenar atividades de Segurança de Informação e Comunicação SIC, na instância da Administração Pública Federal.

As divisões estratégicas de defesa do país, segundo a Estratégia Nacional de Defesa (END), que foi aprovado pelo decreto de nº 6.703, em 18 de dezembro de 2008, considera três setores estratégicos de Defesa que são o nuclear, o cibernético e o espacial. Desde esse momento a defesa cibernética passou a ser considerada como prioritária para o exército brasileiro.

É importante notar que mesmo que no decreto citado acima ter deixado o Exército Nacional a cargo de tais setores, em 9 de novembro de 2009, por meio da Diretriz Ministerial nº0014, a responsabilidade pela coordenação e integração desse Setor, cabe à Aeronáutica conceber, planejar e executar as ações necessárias à Def Ciber e dos seus ativos.

Em cumprimento as diretrizes citadas acima, em 2 de agosto de 2010, foi ativado Núcleo do Centro de Defesa Cibernética. E, em 29 de dezembro do mesmo ano, foi explicitado nas atribuições do DSIC - GSI/PR a sua competência de planejar e executar e coordenar a execução das atividades Segurança Cibernética e de Segurança da Informação e Comunicações na Administração Pública Federal.

Dessa maneira, podemos observar que a Defesa Cibernética Nacional, utiliza-se das principais áreas de Defesa do Estado. Além de mobilizar esses dois setores ela também faz uso da Agência de Inteligência Brasileira (ABIN) responsável assim como o exército e a aeronáutica em salvaguardar o Estado brasileiro da espionagem e sabotagem cibernéticas, protegendo suas infraestruturas vitais.

No contexto de mapeamento e tratamento de incidentes ocorridos na rede da APF é feito no Centro de Tratamento de Incidentes de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR). Ele está subordinado ao Departamento de Segurança de Informação e Comunicações (DSIC), e do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). O CTIR, por diversas vezes trabalha em parceria com diversos setores ligados a Defesa Cibernéticas em eventos em grande escala nacional.

Seguindo na linha dos decretos que firmam as políticas de estrutura cibernética nacional, ocorreu em 20 de setembro de 2012 o Decreto Presidencial nº 7.809, entre outras medidas, incluiu, na Estrutura Regimental do Comando do Exército e o Centro de Defesa Cibernética. Em seguida em 21 de dezembro do mesmo ano o Ministério da Defesa, por meio da Portaria nº 3.405/MD. Atribuiu ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e pela integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa, consoante o disposto no Decreto nº 6.703, de 2008 (END).

Assim, foi aprovada a Política Cibernética de Defesa prevista na portaria normativa nº 3.389, que tem entre seus objetivos desenvolver e de manter atualizada a doutrina de emprego do Setor Cibernético. Dessa é dada uma grande prioridade para o setor de Defesa Cibernética Nacional. No dia 12 de setembro de 2013, ocorreu a atualização da Estratégia Nacional de Defesa e a aprovação do Livro Branco de Defesa Nacional, por meio do decreto nº 373.

Além disso, é importante lembrar, como é observado no livro Verde de Segurança Cibernética no Brasil, organizado por Mandarino Junior e Canongia (2010), o Brasil sempre teve um caráter participativo e até mesmo protagonista nos fóruns internacionais como, por exemplo, na adoção pela OEA, desde 2004, “Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética. Assim vale observar quais são as estratégias nacionais que o Brasil adota para melhor entender seu protagonismo em eventos ligados ao espaço cibernético”.

O Brasil tem tido um grande protagonismo na governança da internet, tanto que é uma das mais reconhecida internacionalmente, possuindo um modelo pluriparticipativo centralizado no Comitê de Gestor da Internet (CGI). O CGI demonstra sua força de participação da governança na rede a partir do decálogo adotado em 2009. Deixando mais uniforme o que seriam os princípios básicos da rede.

A adoção do decálogo fez com que o Brasil elaborasse o Marco Civil para a Internet no país. Tal projeto deu origem à Lei 12.965 de 23 de abril de 2014 deve ser entendido como reação dos diversos *stakeholders* da Internet em todo país à uma série de propostas legislativas que foram propostas nas duas casas do Congresso Nacional destinadas a criminalizar condutas relacionadas direta e indiretamente à Internet (CANABARRO; WAGNER, 2014). Além disso, nesse mesmo ano, ocorreu em São Paulo o Encontro Multissetorial Global sobre o Futuro da Governança da Internet (NetMundial), que contou com a presença de representação de mais de noventa países, demostrando mais uma vez a grande participação do país nesse fenômeno.

A respeito das estratégias adotas pelo Estado brasileiro em Ciberdefesa, a Estratégia Nacional de Defesa (2012), define os seguintes objetivos:

> (a) Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;
>
> (b) Aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à certificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;
>
> (c) Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética;
>
> (d) Desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;
>
> (e) Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais;
>
> (f) Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;
>
> (g) Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e
>
> (h) Estruturar a produção de conhecimento oriundo da fonte cibernética. (END, 2012, p. 95).

A partir desses objetivos podemos ter uma ideia como vem progredindo as questões de Defesa Cibernética Nacional. E que diversos setores de capacitação, pesquisa científica, doutrina, preparo e emprego operacional; e gestão de pessoal e inteligência. No próximo seguimento será mostrado como as áreas da Defesa Nacional compreendem e realizam atividades na Ciberdefesa.

2.1 Divisão de Papeis da Defesa Cibernética da Aeronáutica

A visão da Defesa Cibernética no nível de Segurança Nacional se estabelece como de vital importância para todas as forças envolvidas. Para a Aeronáutica, o investimento nas áreas de Ciberdefesa é essencial principalmente após um ataque cibernético realizado por hackers, ocorrido em 2008, que resultou na desfiguração do Portal Eletrônico Oficial da Aeronáutica, na noite anterior a um evento de *software* livre patrocinado pelo Comando da Aeronáutica (COMAER). Tal ataque foi atribuído a um grupo brasileiro conhecido por "*Fatal Error Group*".

Após esse incidente, medidas foram tomadas como a adoção do Centro de Tratamento de Incidentes de Rede (CTIR.AER) para monitorar a rede da Aeronáutica em busca de vulnerabilidades conhecidas e responder aos incidentes que ocorrerem. Além do ataque mencionado, a Aeronáutica também considera a influência que a Defesa Cibernética toma em Estados de grande importância como os EUA, nas suas políticas e estratégias de defesa.

Tratando-se de sua divisão de tarefes internas, como esclarece Veiga (2012) "no âmbito da Aeronáutica, cabe ao seu Estado-Maior (EMAER) realizar o planejamento estratégico e estabelecer políticas e diretrizes para a coordenação dos setores de interesse". Com esse intuito, a EMAER é dividido em Subchefias e Seções, organizadas por áreas de atuação. Nesse contexto a Defesa Cibernética na Aeronáutica está sob a responsabilidade da Seção de Comando e Controle da Subchefia de Operações.

Porém, essa Seção também é responsável por diversas áreas informacionais, por essa razão com o aumento continuo da importância e da operações realizadas, gerou a necessidade de separar as áreas de Def Ciber e a TI em uma nova Seção dedicada às duas, dentro da Subchefia de Operações. De acordo com Veiga (2012), governança da Def Ciber é realizada pela Subchefia de Operações, que tem sua base nos pilares da

definição das responsabilidades, com a clara divisão de quem vai realizar o que, do alinhamento estratégico e da conformidade no cumprimento das legislações e normas legais, internas e externas ao COMAER.

A Força Aérea define as operações ligadas a Def Ciber em três partes: 1. Proteção Cibernética, são as atividades de Def Ciber defensivas que consistem em utilizar Meios da Força Aérea para neutralizar ataques cibernéticos e explorações cibernéticas realizados contra os SCTIC das forças amigas; 2. Exploração Cibernética são as atividades exploratórias que consistem em empregar Meios de Força Aérea para coletar dados de interesse nos SCTIC inimigos e para identificar as vulnerabilidades desses sistemas; 3. Ataque Cibernético são as atividades ofensivas que consistem em aplicar Meios de Força Aérea para neutralizar ou destruir os SCTIC inimigos.

2.2 Divisão de Papeis da Defesa Cibernética da Marinha Brasileira

No caso da Marinha brasileira, assim como a Aeronáutica, divide as táticas de Def Ciber em proteção cibernética, exploração cibernética e ataque cibernético. A principal diferença é que na Marinha são adicionados mais duas que são a de Operação que consiste em Conjunto de táticas, técnicas e procedimentos ofensivos e defensivos usados pelos militares, a fim de alcançar o domínio da informação no espaço cibernético, ou seja, todas as atividades realizadas no âmbito de Defesa Cibernética. E a Resiliência Cibernética Capacidade de manter as infraestruturas críticas operando sob ataque cibernético ou de restabelecê-las após uma ação adversa, nesse caso seria o princípio de salvaguardar as estruturas que mantem o Estado.

A Marinha Nacional divide as áreas em domínios, em que a Defesa Cibernética se enquadra no nível político estratégico e a Guerra Cibernética no tático e operacional. Tratando-se da Governança da TI, que primeiramente passa pelo Estado Maior da Armada (EMA), vai para COTIM, representado pelo Conselho (ODG + ODS +DCTIM: Assessor), COTEC-TI Comissão Técnica (Rep. Técnicos dos ODS), segue para a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), responsável pelo Planejamento, Orientação, Supervisão, Assessoria e Projetos, que tem que estar em conformidade com a Segurança, Infraestrutura, Sistemas digitais (homologação), e por fim passa para Centro de Tecnologia da Informação da Marinha

(CTIM), responsável pela execução e gerenciamento operacional. Depois de todo esse processo a execução é feita no Centro Local de Tecnologia da Informação (CLTI).

Após a análise da visão da marinha e da aeronáutica a respeito da Def Ciber, pode ser concluido que, apesar de haver uma grande divisão de tarefas em todas as forças estatais, com o intuito de manter as estruturas vitais a salvo, os princípios e definições do que seria a Defesa Cibernéticas e seus intuitos permanecem os mesmos por causa de sua determinação na Política e Estratégia Nacional de Defesa e a ligação ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

2.3 Divisão de Papeis da Defesa Cibernética do Exército Brasileiro

O Exército brasileiro tem papel fundamental na Ciberdefesa pois possui o Centro de Defesa Cibernética que é o órgão responsável por coordenar e integrar os esforços dos vetores vocacionados para compor a defesa. Com a Estratégia Nacional de Defesa (END), ainda em 2008, o setor cibernético foi colocado entre as três áreas de importância estratégica para a Defesa Nacional. De acordo com a END, foram implementadas suas diretrizes e, em 2009, foi instituído o Setor Cibernético no âmbito da força terrestre.

Com o Projeto de Estratégia de Defesa Cibernética e logo foi visto a necessidade da criação de órgão com capacidade de exercer a governança de maneira colaborativa, entre os vetores naturalmente vocacionados para compor a defesa no campo cibernético. Para atender tal proposito foi criado em 2010 Centro de Defesa Cibernética (CDCiber), por decisão do Comando do Exército. As premissas de trabalho deste novo órgão são coordenar e integrar os esforços dos vetores da defesa cibernética. Nesse sentido, é possível afirmar que:

> Em virtude desse conjunto de ações, o Projeto Estratégico de Defesa Cibernética incluiu o Exército Brasileiro no restrito grupo de organizações, nacionais e internacionais, que possuem a capacidade de desenvolver medidas de proteção e mitigar ataques no campo cibernético (EPEX, 2016, s/p)

Além disso, em 21 de julho de 2015, foram ativados dois núcleos de Defesa Cibernética, no comando militar do planalto, o Núcleo do Comando de Defesa Cibernética (NuComDCiber) e o Núcleo da Escola Nacional de Defesa Cibernética

(NuENaDCiber) passaram a contar com militares das três Forças Armadas trabalhando no mesmo ambiente físico. Essas estruturas integram o Sistema Militar de Defesa Cibernética brasileiro, que atua em cinco áreas de competência: Doutrina, Operações, Inteligência, Ciência e Tecnologia e Capacitação de Recursos Humanos. Sua finalidade é proteger e explorar o Setor Cibernético (Exército Brasileiro, 2015).

O Núcleo do Comando da Defesa Cibernética (NuComDCiber), foi prevista pela portaria nº 2.777/MD, de 27 de outubro de 2014, que determinou que o NuComDCiber está na estrutura regimental do Comando do Exército, subordinado ao CDCiber e contará, na forma da legislação, com o exercício de militares das três forças. E que está sob responsabilidade do Estado-Maior junto as Forças Armadas as atividades de coordenação nos episódios de operações conjuntas, se especificando, em atos próprios, os aspectos inerentes ao controle operacional.

Nessa portaria também encontra-se a criação da Escola Nacional de Defesa Cibernética na Estrutura Regimental do Comando do Exército, subordinada ao CDCiber e contará, na forma da legislação, com o exercício de militares da Marinha, do Exército e da Aeronáutica. A Escola terá como meta capacitar para o exercício de atividades de interesse do Setor Cibernético. Inicialmente, seus cursos serão realizados na modalidade de Ensino a Distância (EAD).

2.4 Agência Brasileira de Inteligência (ABIN)

No caso da Agência Brasileira de Inteligência (ABIN), os atos mais utilizados nessas questões são as de Inteligência e contrainteligência, que são as denominadas atividades de inteligência. Que de acordo com a Política Nacional de Inteligência (PNI) define a Inteligência como atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, referentes a fatos e ocorrências dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e da nação. Já as atividades de contrainteligência são definidas pela PNI como atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à

proteção de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado.

Entre as ameaças que ABIN enfrenta para proteger o Estado brasileiro a cibernética está definida como a ações deliberadas com o emprego de recursos da tecnologia da informação e comunicações que objetiva a interrupção, penetração, adulteração ou destruição das redes utilizadas por setores públicos e privados fundamentais à sociedade e ao Estado em especial referentes a sua infraestrutura crítica. Vale destacar que dentre as ameaças destacadas na PNI também encontra-se a espionagem, sabotagem, interferência externa e ações contrarias a soberania, que de certa forma dispõe em sua maioria de auxilio ou se utiliza de ataques diretamente no espaço cibernético.

A partir desse seguimento, pode ser notado que os setor de Defesa Cibernética no Brasil é bem amplo e dividido entre diversos setores apesar de ter pontos de referência como o Centro de Defesa Cibernética e seus objetivos serem determinados pela Política e Estratégia Nacional de Defesa. Pois o espaço cibernético é uma área fundamental para um Estado e no país não existe um setor restrito apenas a tal área, como pode ser visto abaixo na Figura 1.

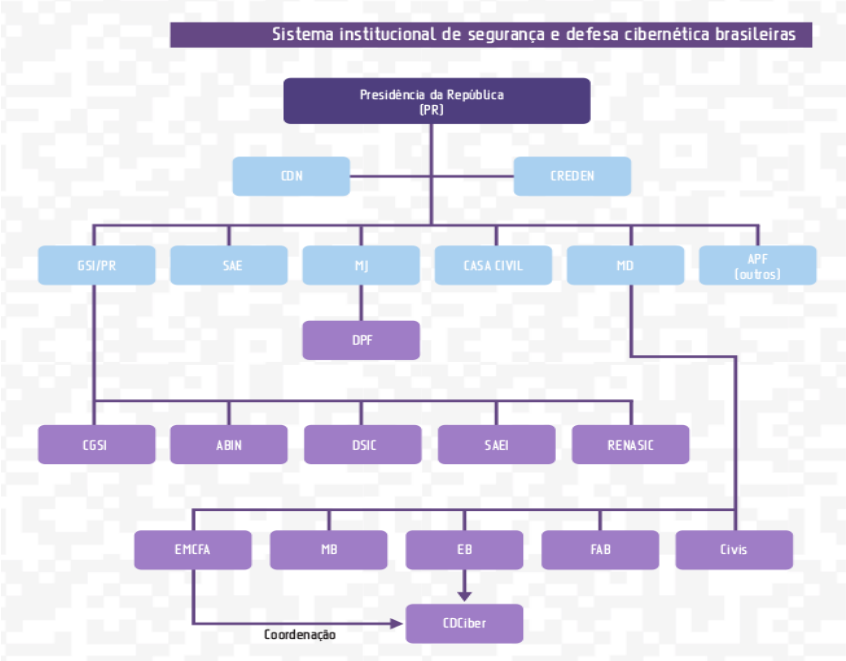


Figura 1 – Organograma do sistema institucional de segurança e defesa cibernética brasileiras.
Fonte: Brasil-Ciberseg (2015).

Um dos motivos que leva a defesa cibernética brasileira a ser tão ampla pode ser que os poderes responsáveis pela Defesa Nacional são os mais propensos aos ataques cibernéticos assim cada um deles tem que ter maneiras de defender-se para que esses ataques não cheguem a causar danos ao Estado.

3 ATUAÇÃO DO BRASIL NO CIBERESPAÇO

Nesse capítulo será tratado mais especificamente da atuação do Estado brasileiro nos ataques cibernéticos seja sendo alvo deles ou sendo designado como a fonte deles. Assim como a sua grande atuação para promover a governança da internet para diminuição dos crimes cibernéticos. Com esse intuito serão utilizados casos de ataques concretos realizados contra o país ou por ele, assim como reuniões que participou para a promoção da governança na rede.

Primeiramente, é importante notar que o Estado brasileiro em geral é um dos países onde os ataques cibernéticos mais têm crescido nos últimos anos, segundo a Pesquisa Global de Segurança de Informação de 2016 observa que globalmente tais ataques tem avançado 38%, mas no caso do Brasil ele cresce em 274%, ao todo foram 8.695 casos que se dividiam em diferentes setores. No que se diz respeito ao setor financeiro as perdas chegaram a US$ 2,45 milhões. Dessa maneira o tema de Defesa Cibernética para o Brasil deve se encontrar em primeiro plano visto que ele é um dos países que possui um dos maiores crescimento de ataques cibernéticos do mundo, através desses dados pode ser observado que esse tema no Brasil já encontra-se securitizado na agenda de segurança nacional e deve ser tratado com medidas emergenciais

Ainda segundo o Mapa de Ameaças Digitais elaborado pela empresa de segurança digital *PSafe*, durante o mês de agosto de 2016, um total de mais de 10 milhões de ataques cibernéticos foram feitos no Estado brasileiro. Além disso, no último ano o país registrou um aumento de 254% do número de ataques sofridos em redes brasileiras. Para tentar reverter esse quadro o investimento em Defesa Cibernética tem crescido nos últimos anos. Tal tema veio à tona no fórum da FIEMG, na tentativa de prepara setores fundamentais para a Economia Nacional.

Como bem exemplificado na Figura 2 abaixo, produzido em um estudo realizado na *Akamai*, o Brasil é o segundo local que mais tem sofrido ataques cibernéticos está apenas abaixo dos Estados Unidos.

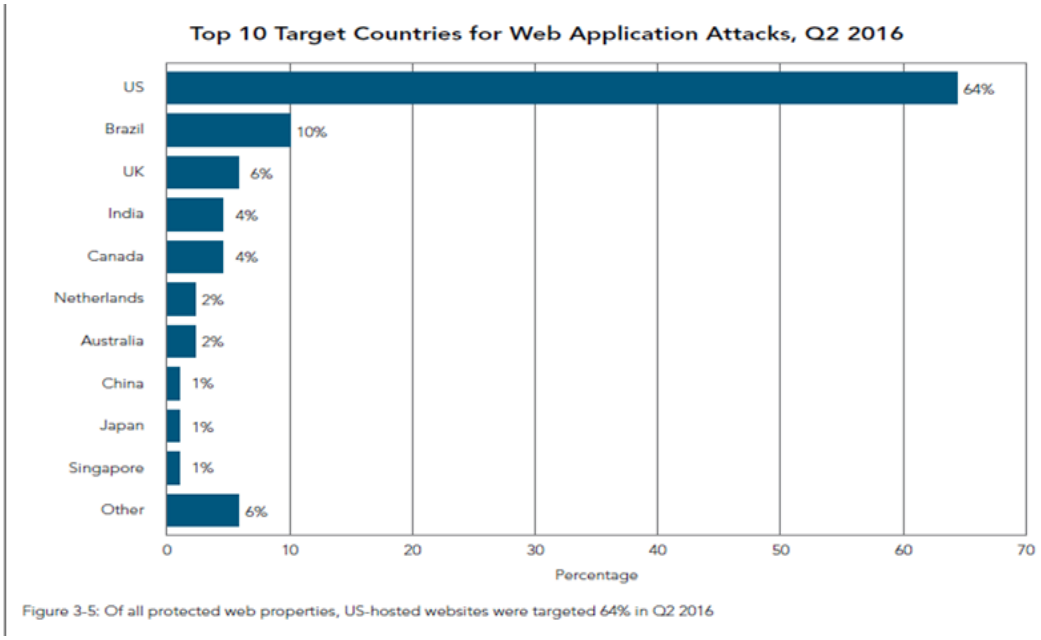


Figura 2 –Top 10 Países-Alvos De Ataques De Aplicativos Da Web , Q2 2016.
Fonte: Akamai (2016, p. 30).

Então é possível notar que entre o ano de 2011 á 2016 os ataques cibernéticos direcionados ao país têm crescido cada vez mais, tanto por causa de sua maior aparição no cenário internacional representado pela realização de eventos de escalas globais como no caso da Copa do Mundo, das Olimpíadas e de seu amplo grau de participação para promover a governança da internet, mais representado por meio do Encontro Multissetorial Global sobre o Futuro da Governança da Internet (NetMundial).

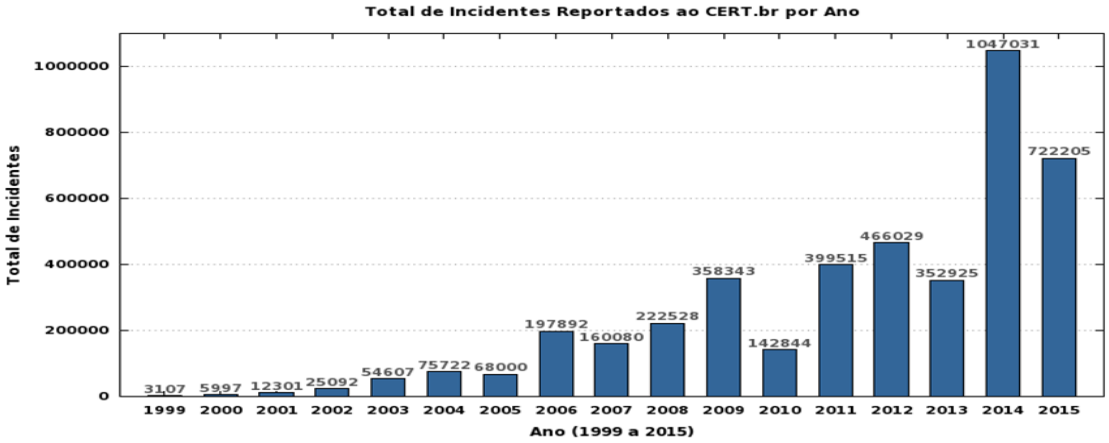


Figura 3 –Total de Incidentes Reportados ao Cert.Br Por Ano (2015)
Fonte Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil (2016).

Assim, como explicitado na figura 3, fornecido pelo Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança, durante o período de 2011, o Brasil registrou diversos ataques a algumas estruturas fundamentais no Estado, alcançou o auge em 2014 em que o país sedeava a Copa do Mundo, além do evento da NetMundial em abril.

Tratando-se das ameaças existentes no setor de Defesa Cibernética foi levantado do Seminário Internacional de Defesa Cibernética (2015), a respeito das infraestruturas críticas observando a Itaipu como se não a maior uma das infraestruturas fundamentais para o Estado, já que abastece 17% do Brasil e 80% do Paraguai, a preocupação se instaura pois a usina também está sob o comando digital, e observando os fatos que estão ocorrendo nos últimos anos em que usinas nucleares de abastecimento são atingidas por ataques cibernéticos que tentam impedir seu funcionamento. E como declara Carlos Sucha (2015, s/p) “A segurança da informação é um aspecto central. Sem energia, comunicação ou informação não há segurança”.

Em relação aos ataques cibernéticos de acordo com um relatório elaborado pela Trend Micro em parceria com a Organização dos Estados Americanos os ciberataques estão cada vez mais direcionados as infraestruturas críticas. Assim mais de 40% dos entrevistados alegaram terem enfrentado ataques destrutivos, e 40% teriam sofrido tentativas de desligamento do sistema. Esses números são essenciais, uma vez que apenas 60% dos 575 consultados no estudo relataram ter detectado tentativas de roubos de dados, considerados há tempos o principal objetivo dos ataques cibernéticos (Under-Linux, 2015).

Dessa forma, percebe-se que o Estado está exposto a diversas ameaças no Espaço Cibernético por seu protagonismo na promoção de eventos internacionais e está preocupando-se com a proteção de suas infraestruturas críticas que podem vir a ser alvos a ataques desse tipo. No próximo seguimento serão relatado alguns casos de ataques cibernéticos contra o Brasil.

3.1. Ataques Recebidos Pelo Brasil

Excetuando-se os ataques que repercutiram na mídia e geraram comoção como no caso de Edward Snowden e casos de eventos com grandes visualizações como a Copa do Mundo e as Olimpíadas, as informações de ataques que atingiram diretamente

o Brasil como Estado são poucos vistos nas notícias e artigos, por essa razão a Pesquisa aqui realizada utiliza apenas poucos sites de notícias.

Em 22 de Junho de 2011, o Governo Brasileiro sofre um dos maiores ataques de hackers até então. O site da Petrobras ficou fora do ar no começo da tarde. A empresa relatou que recebeu um volume grande de acessos ao mesmo tempo, mas que não houve dano nas informações disponíveis na página da internet. Os ataques começaram de madrugada. A maioria teria partido de computadores localizados na Itália. Os hackers fizeram acessos em sequência aos sites da Presidência da República, Portal Brasil e Receita Federal. O Serviço Federal de Processamento de Dados, responsável pela segurança dos sites, proferiu que não houve invasão nem danificação dos dados, no entanto, o episódio ficou marcado como um dos maiores ataques a essas redes da história (G1, 2011).

No ano de 2014, *e-mails* e sistemas de dados do Itamaraty em todo o mundo foram alvos de ataques. Nesses ataques foram hackeados documentos *Intradocs*, espécie de intranet que reúne todas as comunicações diplomáticas, inclusive as reservadas. A instituição afetada disse que não ocorreu a violação do sistema em si mas sim do conteúdo *Intradoc* anexado a E-mails. Conteúdo da visita do vice-presidente americano durante a Copa do Mundo, assim como o resumo da participação do Estado numa Cúpula de segurança nuclear na Holanda em março de 2014. Os ataques duraram cerca de duas semanas, o número de correios eletrônicos afetados foi desconhecido mas estimasse cerca de 1.500 diplomatas brasileiros em todo mundo, sem contar com os funcionários da chancelaria e funcionários locais da embaixada (Folha de S. Paulo, 2014).

O Estado brasileiro foi determinado em um estudo em 2014 como um dos três países que mais recebe ataques por vírus bancários no mundo. Nos três países analisados foram detectados e bloqueados 126,6 mil tentativas de infecção só no período de um mês.

Além dos fatos mencionados, foi descoberta a atuação do 5-eyes em espionagem cibernética mirando o Ministério de Minas e Energia por atuação direta da Agência Canadense de Segurança em Comunicação (Csec). O 5-eyes nasceu durante a segunda guerra mundial, oficiais de inteligência da Grã-Bretanha e dos EUA buscavam decodificar transmissões de rádios de inimigos por meio da troca de inteligência. Nos anos que se seguiram, a tecnologia das comunicações mudou drasticamente – e a coleta de informações é muito mais fácil na era digital. Essa troca de inteligência continua até

os dias de hoje incluindo os EUA e Reino Unido, o Canadá, a Austrália, e a Nova Zelândia. A espionagem cibernética do Canadá foi apoiada pela NSA e o 5-eyes.

Depois do estudo, realizado em 2015, o Brasil foi o único país da América Latina afetado pelo *Carbanak*. Para se infiltrar na intranet do banco, os atacantes utilizaram e-mails direcionados (*spear phishing*) – atraindo os usuários a abri-lo e infectando máquinas com *malware.* Uma *backdoor*, baseada no código malicioso *Carberp*, foi instalada no PC da vítima. Depois de obter o controle sobre a máquina comprometida, os cibercriminosos usaram-na como um ponto de entrada; investigaram a intranet do banco e infectaram outros PC para descobrir qual deles poderia ser usado para acessar sistemas financeiros críticos. Os criminosos então estudaram os instrumentos financeiros utilizados pelos bancos, utilizando *keyloggers* (*malware* que registra a digitação) e vírus que capturam a imagem de tela. E na conclusão os criminosos furtaram os fundos da maneira que mais convinha (B!T, 2015).

Por meio desses ataques cibernéticos, ocorridos nos últimos anos, pode ser notado que ataques contra estruturas governamentais em busca de inviabilizar serviços ou a espionagem propriamente dita, além disso o setor financeiro do Estado tem sido um dos mais atacados tanto no país como em outras regiões do mundo como no caso de Bangladesh ocorrido ainda em março desse ano, questões de espionagem e de quebra de soberania representado pelo caso de Edward Snowden e o da invasão dos E-mails no Itamaraty. Para fora do Brasil ainda ocorreu o caso a invasão do E-mail da candidata à presidência estadunidense Hillary Clinton, atribuído a Rússia até então. A partir do que foi discutido fica nítida a importância de ter um sistema de Defesa Cibernéticos desenvolvido para proteger as infraestruturas críticas nacionais e preservar a soberania estatais.

2.3.1 Operações das Olimpíadas

Um evento de repercussão mundial, como as Olimpíadas, chama a atenção de diversas operações de ataques cibernéticos. As Olimpíadas de Londres, em 2012, sofreram uma tentativa de ataque ao seu fornecimento de energia no dia de sua cerimônia de abertura, o que iria causar um grande distúrbio já que tal evento é transmitido para o mundo todo. Felizmente, o objetivo desse ataque não foi alcançado, graças à equipe de

segurança digital do evento. No entanto, os Jogos de Londres registraram cerca de seis ataques graves de invasão digital, em um total de 97 ataques (Forças Terrestres, 2016).

As ocorrências em Londres fez com que o Brasil tratasse a segurança cibernética desse evento como prioridade. Em virtude dos 97 ataques, em 2012, somados ao avanço cada vez mais rápido da tecnologia, as ameaças ficaram ainda maiores. Em 2015, foi posto em funcionamento um laboratório de testes de integração de sistemas, que pode fazer 200 mil horas de avaliações para assegurar a confiabilidade da estrutura digital dos Jogos, seguindo o exemplo bem-sucedido em Londres. Entre os objetivos está barrar ataques cibernéticos. Com esse intuito A Agência Brasileira de Inteligência (ABIN) mapeou os grupos de *hackers* com maior possibilidade de atuar em grandes eventos. A ABIN ainda observa que apesar de Londres detectar 97 ataques o aparato de defesa digital ainda detectou quase 200 milhões de incidentes que poderiam indicar ameaças. Para impedir que tais incidentes ocorram os jogos do Rio, o evento contou com a ABIN, a força-tarefa conta com a colaboração do Centro de Defesa Cibernética do Exército e do Comitê Gestor da Internet no Brasil.

No entanto, apesar de todos os preparos, grupos de hackers como o Anonymous foram responsáveis por diversos ataques nos Governos Estadual e Municipal no Rio de Janeiro, derrubando os sites do *Brasil 2016*, sobre os Jogos Olímpicos, o das Olímpiadas do Rio, o site de Esportes do Brasil e diversos outros. Através de DDoS, além desses sites outros relacionados as Olímpiadas do Rio foram derrubados (El País, 2016).

Apesar dos ataques citados, os Jogos do Rio terminaram sem nenhum grande ataque cibernético que pudesse interferir diretamente na competição, claro que não foi por falta de tentativa. De acordo com a Cisco, responsável pelos equipamentos de rede e serviços corporativos dos jogos, foram registrados 4,2 milhões de eventos de segurança e 731.607 tentativas de ataques de DDoS foram bloqueadas. (O Globo, 2016).

Neste seguimento pode ser notado o grande esforço e capacitação do Estado Brasileiro para impedir que grandes incidentes ocorressem nos Jogos Olímpicos, assim como o grande número de ataques cibernéticos que eventos desse porte estão expostos. Tal situação reforça a ideia de que é necessário um maior investimento em áreas ligadas a Defesa e Segurança Cibernética.

3.1.2 Ataques Atribuídos ao Brasil

O Estado Brasileiro, apesar de não ser tão aclamado e conhecido por seus ataques cibernéticos em diversos relatórios ele aparece 8º lugar no ranking de origem de ataques cibernético no relatório anual da *Symantec Spam.* Dessa forma o Estado brasileiro também conquista o posto de Estado que mais ataca na América Latina. Como pode ser notado abaixo na tabela 1.

Tabela 1 – Top 10 de Países de Origem de Ataques Cibernéticos (bots).

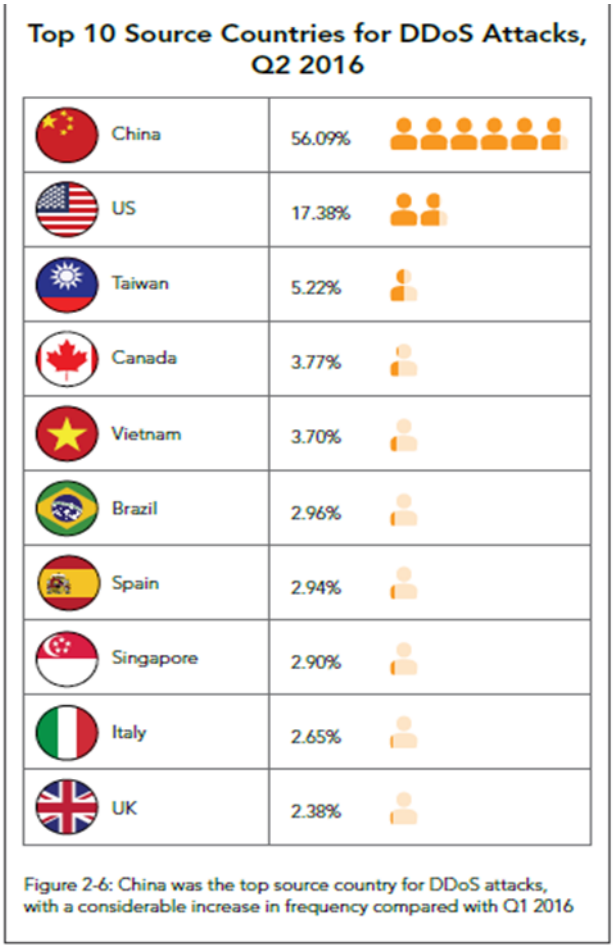
2015 País/Região	2015 Bots (%) no Mundo	Porcentagem de Mudança dos Bots por País/Região	2014 País/Região	2014 Bots (%) no Mundo
1 China	46.1%	+ 84.0%	1 China	16.5%
2 Estados Unidos	8.0%	- 67.4%	2 Estados Unidos	16.1%
	5.8%	-54.8%	3 Taiwan	8.5%
4 Turquia	4.5%	+29.2	4 Itália	5.5%
5 Itália	2.4%	- 71.2 %	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%

Fonte: Symantec Spam (2016).

Observando a tabela 1 fornecida pelo *Symantec Spam*, pode-se observar que houve uma diminuição dos ataques oriundo das maiorias dos países, e um crescimento de Estados como China que teve um crescimento de cerca de 30%. Assim como pode ser observado a aparição de Estados que, até 2014, não faziam parte da lista de maior origens de ataques como no caso da Turquia que foi classificada em quarto lugar na lista. Certamente, grandes ataques foram realizados e alcançaram visibilidade, como o

ataque a sites do Governo da Armênia, em abril de 2016. Além disso, houve ataques às instituições financeiras globais por parte de hackers Turcos. Que mostra o crescimento desse Estado em ataques cibernéticos globais. Da mesma maneira que outros países como nos casos do Canadá, Polônia e Japão que não encontram-se mais na lista dos dez responsáveis pelos *bots* no mundo, graças a uma maior fiscalização na rede, em casos principalmente de ataques promovidos por indivíduos e grupos.

Outro estudo promovido pela *Akamai* (2016), coloca o Brasil em sexto lugar nos ataques cibernéticos de tipo DDos. Que são um dos tipos de ataques mais utilizados de negação de serviços em sites financeiros e públicos dos Estados. Como pode ser analisado no Quadro 1 apresentado abaixo:



Quadro 1 – Top 10 dos Países de Origem de Ataques (ddos), q2 2016.
Fonte: Akamai (2016, p. 16).

Por meio das informações aqui demonstradas a respeito dos ataques cibernéticos realizados pelo Brasil, pode-se perceber que além de ser um dos grandes alvos de

ataques cibernéticos, o Estado também é um uma grande fontes de ataques cibernéticos de diferentes tipos. Apesar de dificilmente se encontrar muitos relatos de ataques cibernéticos promovidos pelo Brasil, ele ainda possui um grade ranking tratando-se de realizar ataques cibernéticos.

2.4 Governança da Internet

O Brasil tem tido uma postura protagonista em diversos fóruns internacionais entre eles encontra-se em dialogo a questão da promoção da governança da internet. Para melhor se compreender a importância do Estado brasileiro na busca pela governança da internet, se faz necessário ver a crescente participação do país em discursões e acordos internacionais a respeito da Segurança e Defesa Cibernética.

Segundo a Escola de Copenhague, necessita-se de um ator securitizador que declara que o objeto de referência está sendo ameaçado, nesse contexto o Brasil em parceria com outros Estados colocam a necessidade da Governança da Internet. Partindo do pressuposto que o domínio da internet seria facilmente manipulado pelos EUA, já que todos os órgãos oficiais da Governança que existe hoje encontram-se no território estadunidense, logo, o objeto de referência seria o domínio da Internet. Depois do caso Snowden, o caráter emergencial de criação de uma nova Governança da Internet se torna essencial.

O Estado Brasileiro tomou diversas iniciativas para fomentar o combate as ameaças cibernéticas, entre elas estão a Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética, adota pela OEA desde 2004, que visa a criação de uma cultura de Segurança cibernética para proteger os cidadãos e os serviços essenciais, cujo alcance não poderia ser feito através da atuação de apenas um Estado. Em 2009, o Workshop Hemisférico Conjunto da OEA sobre o Desenvolvimento de uma Estrutura Nacional para Segurança Cibernétic,a de 16 a 20 de novembro, contando com a presença do Brasil, representado pelo GSIPR.

No período de 2009 a 2010, o Brasil participou como observador *ad hoc* no *Working Party on Information Security and Privacy - WPISP*", e do "*Comittee for*

Information, Computer and Communications – ICCP, promovidos pela Organização para Cooperação e Desenvolvimento Econômico (OCDE), realizados na França. No encontro de 2010, o Brasil propôs a realização de um estudo comparativo das estratégias nacionais de segurança cibernética; a qual foi inteiramente aceita e, para tanto, foi criado um grupo de trabalho com participação de países voluntários com esse objetivo. O Grupo é presidido pelo representante de Portugal na OCDE.

É importante mencionar a *Meridian Conference* de alto nível, com a participação de especialistas e tomadores de decisão de governo, voltadas para questões de segurança das infraestruturas críticas da informação e correlatas, que vem explorando os benefícios e oportunidades de cooperação entre governos, e promovendo fórum de excelência para compartilhamento das melhores práticas mundiais, no tema. O livro verde de Segurança Cibernética aborda a criação do conceito de Meridiano pelo Reino Unido e promoveu a primeira conferência em 2005. Desde então a conferência acontece todo ano em diferentes localidades. A *Meridian Conference,* realizada em 2009, nos Estados Unidos, foi marcante para o Brasil, pois foi a primeira vez que contou com a presença de Estados latino-americanos. Em 2015, tal conferência ocorreu na Espanha.

O Estado Brasileiro por meio do Ministério da Defesa integra o "*Group of Governmental Experts" (GGE) on "Developments in the Field of Information and Telecommunications in the Context of International Security"* no âmbito da ONU e alcançou reconhecimento internacional no tema. O Livro Verde de Segurança Cibernética dá ênfase na construção de bases para o entendimento internacional de segurança cibernética, principalmente a respeito do crime cibernético; já que a convenção de Budapeste não atende mais o nível de complexidade dos crimes cibernéticos, dado aos crescentes avanços tecnológicos, assim como não é suficiente em termos de cooperação internacional. Dessa forma, o Brasil procurou definir consensos de entendimento de Segurança e Crimes Cibernéticos. Por meio da Convenção do Crime Cibernético, ocorrida no ano de 2010, em Salvador, foi emitida a Declaração que permitiu a criação de um grupo para tratar globalmente a matéria – crime cibernético, condessado pelos 158 países, sobre tal aspecto.

Tratando-se agora da Governança da Internet propriamente dita, que é definida pela Cúpula Mundial da Sociedade de Informação promovida pela ONU, em 2005, como:

> Desenvolvimento e aplicação, por governos, pelo setor privado e pela sociedade civil – em seus respectivos papéis – de princípios, normas, regras e procedimentos de tomada de decisão, bem como de programas, que devem

> determinar a evolução e o uso da Internet (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2005, s/p).

Tal definição leva em consideração um grande rol de atores que deveriam ser refletidos na governança da rede; É perceptível a complexidade pois, como já foi abordado anteriormente, no mundo cibernético não há fronteiras visíveis, assim a governança internacional da internet se faz necessária.

Ao observar-se o histórico da governança da internet, nota-se que apesar da internet em si ser uma rede aberta que agrupa uma série de redes computacionais autônomas. Ela passou por várias modificações que acabaram criando diversas ramificações responsáveis pelo controle da rede. Basicamente, durante toda década de 1990, a Governança da Internet por assim dizer permaneceu nas mão dos Estados Unidos, seja pela forma mais técnica pelo controle do IP e DNS, por parte da academia, ou na criação de organizações para melhor regula-la já que a rede permanecia crescendo a cada dia. Foi por esse motivo que surgiu na Califórnia em 1998 a Internet Corporation for *Assigned Name and Number* (ICANN), para servir como ponto focal para governança da raiz da internet. A ICANN trabalha junto do *The Internet Assigned Numbers Authority* (IANA), que gerencia os parâmetros dos protocolos, recursos de números da Internet e nomes de domínio, ele é regulado pela ICANN.

Foi apenas no início dos anos 2000 que a Cúpula Mundial para a Sociedade da Informação foi comissionada pelos membros da Organização das Nações Unidas (ONU) à União Internacional das Telecomunicações com o intento de fomentar a reflexão a respeito a respeito das oportunidades e dos desafios - especialmente aqueles vinculados às Metas do Milênio da ONU - inerentes ao avanço da digitalização e das TIC pelo mundo (CGI, 2005).

Assim, temas como exclusão digital, a própria governança da rede, tentativa de criação de princípios fundamentais, o plano de ação para a sociedade de informação, trabalho perspectivos. Em sua pauta assuntos de infraestrutura, direitos fundamentais, diversidade linguística, políticas públicas a respeito da internet, além das questões de segurança e crime cibernético.

Em 2006, nasce o *Internet Governance Forum* (IGF), um espaço destinado a diálogo de atores que tenham interesse, no entanto o fórum não tem poder decisório, apena emitem mensagens importantes que devem ser levados a principal organização de comando (ICANN), como mandatos.

O fato dos maiores instrumentos de governança da internet ainda encontrar-se nos Estados Unidos, deixa diversas nações desconfortáveis principalmente com os casos de espionagem que o Estado está envolvido. Como o caso de Edward Snowden, em 2013, revelados pelo *Wikileaks*, em que chegou a utilizar a operação de monitoramento diretamente com chefes de Estado - como foi o caso do Brasil -, além da empresa estatal Petrobras também ter sido alvo de espionagem. A partir desse caso, o Brasil e a Alemanha demonstram um grande desconforto em relação aos EUA. Dessa forma esses Estados procuram manter seu protagonismo na temática de Governança da Internet para conseguir constituir e manter princípios fortes da utilização da rede.

O Brasil tem tido um grande protagonismo na governança da internet, tanto que é uma das mais reconhecida internacionalmente, possuindo um modelo pluriparticipativo centralizado no Comitê de Gestor da Internet (CGI). O CGI demonstra sua força de participação da governança na rede a partir do decálogo adotado em 2009. Deixando mais uniforme o que seriam os princípios básicos da rede.

A adoção do decálogo fez com que o Estado elaborasse o Marco Civil para a Internet no Brasil. tal projeto deu origem à Lei 12.965 de 23 de abril de 2014 deve ser entendido como reação dos diversos *stakeholders* da Internet em todo país à uma série de propostas legislativas que foram propostas nas duas casas do Congresso Nacional destinadas a criminalizar condutas relacionadas direta e indiretamente à Internet (CANABARRO; WAGNER, 2014). Além do que nesse mesmo ano em São Paulo ocorreu o Encontro Multissetorial Global sobre o Futuro da Governança da Internet (NetMundial), que contou com a presença de representação de mais de noventa países, demostrando mais uma vez a grande participação do país nesse fenômeno.

Ainda tratando-se de Governança da Internet, o ano de 2013 foi decisivo no tocante ao aumento dos esforços para a criação de uma nova governança da internet. Brasil e Alemanha - países vítimas do grande esquema de espionagem estadunidense- conseguiram elevar as atenções para a governança desta área sensível. Os casos de espionagem foram levados à Assembleia Geral da ONU, em que além de ter o apoio do BRICS e do IBAS, também conseguiu o apoio da Alemanha sobre a possibilidade de juntar esforços na área de defesa da privacidade na internet no âmbito do Conselho de Direitos Humanos. Angela Merkel a chanceler alemã da época, também declarou que:

> Ainda temos que construir muito esse caminho, mas há um entendimento de vários países que é um tema novo, é uma agenda que se abre para as relações internacionais, um tema que seguramente ocupará a ONU nos próximos anos e portanto há, sim, um interesse crescente (MERKEL apud O GLOBO, 2013, s/p).

No entanto, mesmo depois de todos os esforços para a criação de uma nova governança da internet, o tema vem se apagando do discurso brasileiro. No período de 2014, a ex-presidenta Dilma Rousseff, em seu discurso na abertura da Assembleia Geral da ONU, abordou as questões dos direitos humanos no mundo real e virtual e a privacidade na era digital. Entretanto, em 2015, o tema não foi abordado pela presidente em seu discurso. Além disso, Canabarro (2016) também argumenta que:

> Uma outra crítica que poderia ser apontada à manifestação de 2015 diz respeito à ausência de manifestação de apoio, pelo Brasil, à renovação do mandato do Fórum de Governança da Internet. Pode ser que isso se justifique pelo fato de que essa renovação corria em um processo paralelo, com espaço pertinente para o país firmar sua posição. Ainda assim, poucos meses depois do discurso, o Brasil sediou a 10a edição do Fórum, em João Pessoa, na Paraíba, tendo sido o único país do mundo a contar com o privilégio de sediá-lo por duas ocasiões (a anterior foi em 2007). Apesar de o tema ser granular, a diplomacia brasileira perdeu uma oportunidade relevante de intensificar a promoção do modelo brasileiro de governança da Internet (capitaneado pelo CGI.br) como inspiração para os demais países (que tem servido como elemento de *soft power* para a diplomacia brasileira no setor correspondente); e – com isso – pressionar, ainda mais, pelo avanço da democratização da governança global da Internet, da qual o IGF é o principal símbolo há dez anos (CANABARRO, 2016, s/p).

Assim pode ser notado que mesmo o Brasil sediando o Fórum duas vezes, no ano de 2015 provavelmente por seu contexto político o Estado não procurou destacar-se no evento. Em 2016 o presidente repetiu a lacuna do ano anterior, baseado na mesma justificativa do governo anterior o contexto político turbulento em que o Estado se encontra então como explicado por Canabarro (2016) ele procura

> Criar uma narrativa de normalidade institucional que faça sentido do ponto de vista dos cidadãos no contexto pós-impeachment e que sirva à busca de legitimidade internacional, mantendo um perfil protocolar e sem grandes direcionamentos e proposições, como explica em uma nova avaliação feita pelo mesmo Guilherme Casarões. Mas se a conjuntura de 2015 desabona a lacuna de então, o mesmo não vale para 2016, pelo simples fato de ser o ano crucial para que saibamos como se encerrará o "longo 2014 da governança da Internet", inaugurado precocemente ainda em 2013, em grande medida, pela ação do Brasil. (CANABARRO, 2016, s/p).

Nesse sentido, a Alemanha tem se destacado mais na promoção da Governança da Internet, enquanto o Brasil tem mantido certa distância do tema por causa de sua instabilidade política. A Alemanha continua seu discurso e ações de promoção a uma no Governança da Internet. Apesar de o Brasil não está participando tão ativamente dessa

promoção como no período de 2013-2014, o Estado continua com a parceria com o Estado Alemão que é muito bem demonstrada na realização da I Reunião de Consulta Brasil-Alemanha sobre temas Cibernéticos, que teve como objetivo o debate do atual cenário de tecnologia, seus desafios e oportunidades dentro da esfera mundial. Assim se pode observar que mesmo o Estado demonstrando uma interação menor com o tema ele ainda representa uma grande atuação em conjunto com a Alemanha em relação a criação da nova Governança da Internet.

4 CONSIDERAÇÕES FINAIS

Esse trabalho mostrou a importância do espaço cibernético nas Relações Internacionais, principalmente na área de Segurança Internacional através da análise dos casos e estruturas apresentados. Por meio da discursão é possível observa a estrutura de Defesa Cibernética brasileira e sua evolução através das leis que determinam sua importância além da Estratégia Nacional de Defesa, assim como o país demostrou um grande protagonismo em matéria da criação de uma nova dinâmica de governança da internet.

No primeiro capítulo, se discutiu a respeito da securitização do espaço cibernético a partir da visão da escola de Copenhague, assim como foi definido o que seria o ciberespaço, a diferenciação entre segurança e defesa cibernética utilizando a perspectiva de que a primeira é responsabilidade da polícia e a segunda como ameaça a segurança nacional faz parte do meio militar. Também foram abordadas as questões de guerra cibernética demonstrada por conflitos realizados por meio de ataques cibernéticos, que chegaram a influenciar as infraestruturas críticas de Estados de diferentes maneiras.

No segundo capítulo, foi discutida a estrutura brasileira para a Defesa Cibernética que se divide em diversos órgãos. Focando-se nas Forças Armadas, aeronáutica, marinha e ABIN, que demonstram a visão nacional da Defesa Cibernética, além de observar as leis que determinam a Defesa Cibernética Nacional. Em que podemos ver o avanço perspectivo da Def Ciber no país principalmente a partir de 2013.

No capítulo três foi demonstrado a atuação do Brasil como alvo e origem dos ataques cibernéticos sendo perspectivo que os ataques ao país tem tido um grande crescimento principalmente entre 2013 e 2016, coincidido com o período em que o país ganha um maior protagonismo através das realizações de grandes eventos internacionais. Também foi tratado do protagonismo que o Estado apresentou a respeito da governança da internet incorporado principalmente nos discursos da presidente na ONU entre o período de 2013 e 2014, que nos dois últimos anos não foi abordado em seu discurso.

Dessa forma, a partir desse estudo, pode ser concluído que o cibernético influencia diretamente nas infraestruturas vitais do Estado e é necessária uma defesa que se desenvolva rapidamente para acompanhar a tecnologia.

No caso do Brasil, possuidor de uma grande estrutura de Defesa Cibernética, exige-se a necessidade de contínuo avanço, desenvolvimento e uma melhor articulação entre os órgãos responsáveis pela ciberdefesa nacional, isso significa mais eficiência na defesa, para se defender e contra-atacar os ciberataques que estão cada vez mais recorrentes.

O Estado deveria está buscando seu posto como influenciador internacional da governança da internet, que foi fundamental para colocar o Brasil como um dos principais global player na temática, entretanto, a participação do país vem demonstrando enfraquecimento nos últimos anos, pode-se notar a diminuição da aparição do tema em seu discursos oficiais.

As motivações para o enfraquecimento da posição internacional do Brasil na governança da Internet, se dá por tensões políticas e restruturação das relações internacionais do país para um novo alinhamento, deixando certa dúvida em qual caminho o país está seguindo — em relação as suas interações internacionais — a respeito da temática da governança da internet e qual será sua posição nesse aspecto.

A área de Segurança Internacional no ambiente cibernético é recente caracterizado por sua emergência no final do século XX e sua maior ampliação no século XXI. Assim ainda é um espaço pouco explorado e rico em informações fundamentais para as Relações Internacionais, demandando novos estudos direcionados a esse tema.

REFERÊNCIAS

AMORIM, CELSO. **Doutrina Militar de Defesa Cibernética.** Ministério da Defesa. Publicado no D.O.U. nº 224 de 19 nov. 2014.

AKAMAI. **Q2 2016 State of the Internet Security Report.** 2016. Disponível em < https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf >. Acesso em 9 nov. 2016.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

_____. **Decreto Legislativo nº 373, 25 de setembro de 2013** (aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa).

_____. **Decreto nº 7.276, de 25 de agosto de 2010 (**aprova a Estrutura Militar de Defesa e dá outras providências).

_____. **Decreto nº 7.411, de 29 de dezembro de 2010** (define as competências do DSIC – GSI/PR, dentre outras).

_____. **Decreto nº 7.809, de 20 de setembro de 2012** (altera a estrutura regimental da Marinha, do Exército e da Aeronáutica).

_____. **Diretriz Ministerial nº 14/2009 do Ministério da Defesa, de 9 de novembro de 2009** (dispõe sobre integração e coordenação dos setores estratégicos da Defesa).

_____. **Diretriz Ministerial 0014 Integração e Coordenação dos Setores Estratégicos da Defesa.** Brasília, 2009.

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

_____. **Instrução Normativa nº 1/GSI/PR, de 13 de junho de 2008** (disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências) e suas Normas Complementares.

_____. **Instrução Normativa nº 001/EMCFA/MD, de 25 de julho de 2011** (aprova as Instruções para Confecção de Publicações Padronizadas do Estado-Maior Conjunto das Forças Armadas – EMCFA - MD20-I-01, 1ª Edição/2011).

_____. **Lei Complementar (LC) nº 97, de 9 de junho de 1999, alterada pelas LC nº 117, de 2 de setembro de 2004, e nº 136, de 25 de agosto de 2010** (dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas).

_____. **Lei nº 12.965, de 23 de abril de 2014** (estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil).

_____. **Política Nacional de Defesa Estratégia Nacional de Defesa**. Ministério da Defesa. BRASÍLIA, 2012.

————. **Política Nacional de Inteligência. Agência Brasileira de Inteligência**. 2016.

_____. **Portaria nº 400/SPEAI/MD, de 21 de setembro de 2005** (aprova a Política Militar de Defesa - MD51-P-02).

_____. **Portaria Normativa nº 578/SPEAI/MD, de 27 de dezembro de 2006** (aprova a Estratégia Militar de Defesa - MD51-M-03).

_____. **Portaria Normativa nº 113/DPE/SPEAI/MD, de 1º de fevereiro de 2007** (aprova a Doutrina Militar de Defesa - MD51-M-04).

_____. **Portaria Normativa nº 196/EMD/MD, de 22 de fevereiro de 2007** (aprova o Glossário das Forças Armadas - MD35-G-01, 4ª Edição).

_____. **Portaria Normativa nº 513/EMD/MD, de 26 de março de 2008** (aprova o Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas - MD33-M-02, 3ª Edição/2008).

_____. **Portaria Normativa nº 3810/MD, de 8 de dezembro de 2011**(aprova a Doutrina de Operações Conjuntas - MD30-M-01, Volumes 1, 2, e 3 - 1ª Edição/2011).

_____. **Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012** (aprova a Política Cibernética de Defesa - MD31-P-02 - 1ª Edição/2012).

_____. **Portaria nº 3.405/MD, de 21 de dezembro de 2012**, (atribui ao Centro de Defesa Cibernética, do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa, consoante o disposto no Decreto nº 6.703/08).

_____. **Portaria Normativa nº 229/MD, de 28 de janeiro de 2013** (aprova a publicação Operações Interagências - MD33-M-12, 1ª Edição/2012).

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap. **Security: A New Framework for Analysis.** Lynne Rienner, Londres, 1998.

CANABARRO, Diego; WAGNER, Flávio. **A Governança da Internet: Definição, Desafios e Perspectivas, In: Encontro da ABCP, 9.,** 2014, Brasília. Anais, 2014. Disponível em < http://www.encontroabcp2014.cienciapolitica.org.br/resources/anais/14/140 >. Acessado em 9 ago. 2016.

CANABARRO, Diego. **Onde foi parar a Internet nos discursos do Brasil na Assembleia Geral da ONU em 2015 e 2016.** Observatório da Internet no Brasil, 2016. Disponível em < http://observatoriodainternet.br/post/onde-foi-parar-a-internet-nos-discursos-do-brasil-na-assembleia-geral-da-onu-em-2015-e-2016 >. Acesso em 14 nov.2016.

CAVELTY, Myriam Dunn. Cyber (Un) Sicherheit: Grundlagen, Trends und Herausforderungen. **Polit Bild,** v. 1, n. 2012, p. 66-87, 2012.
CASTELLS, Manuel. **A Ciberguerra do Wikileaks.** La Vanguardia, 2010. Disponível em: <http://www.bresserpereira.org.br/Terceiros/2010/10.12.A_ciberguerra_do_Wikileaks.pdf>. Acesso em 16 ago. 2016.

CCM. **Vermes Informáticos**. 2016. Disponível em < http://br.ccm.net/contents/756-vermes-informaticos >. Acesso em 18 set. 2016.

CERT.BR. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em < http://www.cert.br/stats/incidentes/ >. Acesso em 15 de agosto de 2016.

CGI.br/RES/2009/003/P. 2009. Disponível em < http://www.cgi.br/resolucoes/documento/2009/003 >. Acessado em 20 set. 2016.

CHACRA, Gustavo. **Vírus usado contra o Irã usa linguagem feita na PUC-Rio.** Estadão, 2012. Disponível em <http://www.estadao.com.br/blogs/jt-radar/virus-usado-contra-o-ira-usa-linguagem-feita-na-puc-rio/>. Acesso em 13 de set. 2016.

CLARKE, Richard; KNAKE, Robert. **Cyber War The Next Threat to National Security and What to Do About It.** HarperCollins, 2012.

CLAUSEWITZ, Carl Von**. Da Guerra: Livro Um.** Tradução Para o Inglês Michael Howard e Peter Paret. Tradução do inglês para o português Luiz Carlos Nascimento e Silva Valle, 2007.

COMANDO DA AERONAÚTICA. Aviso Interno nº 2, Brasília, 2012.

CRYPTOID. **Brasscom participa da I Reunião de Consulta Brasil-Alemanha sobre temas Cibernéticos.** CRYPTOID, 2016. Disponível em < https://cryptoid.com.br/banco-de-noticias/brasscom-participa-da-i-reuniao-de-consulta-brasil-alemanha-sobre-temas-ciberneticos/>. Acesso em 15 nov.2016.

CÚPULA MUNDIAL PARA A SOCIEDADE DA INFORMAÇÃO (2005a). Tunis Agenda for the Information Society. Documento n. WSIS- 05/TUNIS/DOC/6(Rev. 1)-E. Disponível em: < http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>. Acesso em 23 set. 2016.

DA CRUZ JÚNIOR, Samuel. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual,** Texto para Discussão, Instituto de Pesquisa Econômica Aplicada (IPEA), No. 1850, 2013.

DE LUCA, Isabel. **Brasil diz ter apoio da Alemanha para nova governança da internet.** G1, 2013. Disponível em < http://oglobo.globo.com/mundo/brasil-diz-ter-apoio-da-alemanha-para-nova-governanca-da-internet-10171492>. Acesso em 14 nov. 2016.

EL PAÍS. **Novos ataques do Anonymous no Rio marcam início dos jogos digitais**. Disponível em: <http://brasil.elpais.com/brasil/2016/08/15/opinion/1471267832_175141.html>. Acesso em: 23 nov. 2016.

EXTRA. **Olimpíada no rio registra 4,2 milhões de ataques cibernéticos**. Disponível em: <http://extra.globo.com/noticias/celular-e-tecnologia/olimpiada-do-rio-registra-42-milhoes-de-ataques-ciberneticos-20061377.html>. Acesso em: 23 nov. 2016.

FEDERAÇÃO NACIONAL DE SEGUROS EM GERAIS. **Brasil na rota de crimes cibernéticos. 2015.** Disponível em < http://www.cnseg.org.br/fenseg/servicos-apoio/noticias/brasil-na-rota-de-crimes-ciberneticos.html>. Acesso em 13 out. 2016.

FIRMINO, Rodrigo. **Território e Materialidade: Wikileaks e o Controle do Espaço Informacional.** Contemporânea comunicação e cultura - vol.09 – n.02 – agosto de 2011. Disponível em < https://portalseer.ufba.br/index.php/contemporaneaposcom/article/view/5091/3880>. Acesso em 12 set. 2016.

FORÇAS TERRESTRES. **Defesa cibernética nas olimpíadas rio 2016**. Disponível em: <http://www.forte.jor.br/2016/04/26/exercito-abin-e-cgi-br-farao-defesa-cibernetica-nas-olimpiadas-rio-2016/>. Acesso em: 23 nov. 2016.

GALANTE, Alexandre. '**Malware' Stuxnet foi desenvolvido para destruir usina nuclear iraniana**. Poder Áereo, 2010. Disponível em < http://www.aereo.jor.br/sobre-2/>. Acesso em 14 set. 2016.

G1. **Sites do governo sofrem maior ataque hacker da história.** 2011.Disponível em < http://g1.globo.com/jornal-nacional/noticia/2011/06/sites-do-governo-sofrem-maior-ataque-hacker-da-historia.html>. Acesso em 13 out. 2016.

HANSE, Lene; NISSENBAUM, Helen. **Digital Disaster, Cyber Security and Copenhagen School.** International Studies Quarterly, n. 53, 2009, 1555-1575.

ICANN, **As Funções da IANA.** 2015. Disponível em < https://www.icann.org/pt/system/files/files/iana-functions-18dec15-pt.pdf>. Acesso em 21 set. 2016.

ISMAIL, Shaharudin; YUNOS, Zahri Hj. **Cyberspace the new war frontier.** The Star InTech. On, v. 21, 2005.

ITU-T. **Overview of cybersecurity Recommendation.** 2008. Disponível em < https://www.itu.int/rec/T-REC-X/e>. Acesso em 03 set. 2015.

KEATING, Joshua E. **Shots Fired.** Disponível em: <http://www.foreignpolicy.com/articles/2012/02/24/shots_fired>. Acesso em 04 set.2016.

KUEHL, Daniel T. **From cyberspace to cyberpower: Defining the problem. Cyberpower and national security,** 2009. Disponível em <

http://ctnsp.dodlive.mil/files/2014/03/cyberpower-i-chap-02.pdf>. Acesso em 03 set. 2016.
LOPES, Gills. **Reflexos da digitalização da guerra na política internacional do século XXI:** uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá. Dissertação (Mestrado em Ciência Política) – Universidade Federal de Pernambuco Centro de Filosofia e Ciências Humanas Departamento de Ciência Política. Re. 2013.

MARVÃO, Susana. **Brasil foi um dos afetados pelo golpe cibernético do século**. Cancun. 2015. Disponível em <http://www.bitmag.com.br/2015/02/brasil-foi-um-dos-afetados-pelo-golpe-cibernetico-seculo/>. Acesso em 13 out. 2016.

OLIVEIRA, Daniela. **O Poder da Informação na Política Internacional: A Wikileaks e a Revolução da Tunísia.** 2012. P. 115. Dissertação (Mestrado em Ciência Política e Relações Internacionais) – Faculdade de Ciências Sociais e Humanas Universidade Nova de Lisboa. 2012.

OLIVEIRA, Marcos; GAMA NETO, Ricardo; LOPES, Gills (Org.). **Relações Internacionais Cibernéticas (CiberRI): oportunidades e desafios para os estudos estratégicos e de segurança internacional.** Recife: Editora UFPE, 2016.

OTAN. **The History of Cyber Attacks – a time line.** Disponível em < http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm>. Acesso em 18 set. 2016.

PADILHA, Luiz. **Guerra dos Drones: Como a Tecnologia dos UAVs Está Transformando o Futuro da Guerra.** Defesa Aérea e Naval, 2015. Disponível em < http://www.defesaaereanaval.com.br/guerra-dos-drones-como-a-tecnologia-dos-uavs-esta-transformando-o-futuro-da-guerra/>. Acesso em 14 set. 2016.

PEDROSA, Leyberson; MATSUKI, Edgard. **Entenda o caso Snowden; Petrobras também é alvo de espionagem.** Disponível em: <http://www.ebc.com.br/tecnologia/2013/08/web-vigiada-entenda-as-denuncias-de-edward-snowden>. Acesso em 04 set. 2016.

PERLROTH, Nicole. **In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back**. The New York Times. 2012. Disponível em < http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=1&_r=1>. Acesso em 04 set. 2016.

PIRES, Hindenburgo. **Estados Nacionais, Soberania e Regulação da Internet**. Revista Eletrónica de Geografía y Ciencias Sociales, 2012. Disponível em < http://www.ub.edu/geocrit/sn/sn-418/sn-418-63.htm>. Acesso em 14 set. 2016.

POLIDO, Fabrício; ANJOS, Lucas. **Marco Civil e Governança da Internet: Diálogos entre o Doméstico e o Global.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2016. Disponível em < http://irisbh.com.br/Downloads/MCGI.pdf>. Acesso em 14 nov. 2016.

RATTRAY, Greg; EVANS, Chris; HEALEY Jason. **American Security in Cyber Commons.** 2010.
RESENDE, Marcio; ZANINI, Fábio. **Itamaraty sofre ondas de ataques de hackers.** Folha da UOL.2014. Disponível em < http://www1.folha.uol.com.br/mundo/2014/05/1460646-itamaraty-sofre-onda-de-ataques-de-hackers.shtml>. Acesso em 13 out. 2016.

SANDRONI, Gabriela A. **Prevenção da Guerra no Espaço Cibernético.** Anais do IV Simpósio de Pós-Graduação em Relações Internacionais do Programa "San Tiago Dantas" (UNESP, UNICAMP e PUC/SP), Apresentado de 05 a 08 de Novembro de 2013. Disponível em: <http://www.santiagodantassp.locaweb.com.br>. Acessado em: 15 mar.2016.

SCHNEIER, Bruce, Institute of International and European Affairs – IIEA (2010): **On Cyber War and Cyber Crime** (https://www.youtube.com/watch?v=Tkcxi-D5_C0), consultado em 20 set. 2016.

SCHNEIER, Bruce, TEDEducation (2013): **The security mirage**. Disponível em http://www.youtube.com/watch?v=NB6rMkiNKtM. Acesso em 20 set. 2016

SCHNEIER, Bruce, TEDxPSU (2010): **Reconceptualizing Security.** Disponível em <http://www.youtube.com/watch?v=CGd_M_CpeDI>. Acesso em 20 set. 2016.

SHEETER, Laura. **Estônia acusa Rússia de 'ataque cibernético' ao país**. BBC Brasil. 2007. Disponível em <http://www.bbc.com/portuguese/reporterbbc/story/2007/05/070517_estoniaataquesinternetrw.shtml>. Acesso em 04 set. 2016.

SINGER, Peter W.; FRIEDMAN, Allan. **Cybersecurity: What Everyone Needs to Know.** Oxford University Press, 2014.

SPUTNIK BRASIL. **Depois de Anonymous, hackers turcos atacam sites do governo da Armênia.** 2016. Disponível em https://br.sputniknews.com/ciencia_tecnologia/201604064040191-ataques-cibernticos-armenia/. Acesso em 10 nov. 2016.

SYMANTEC. **Internet Security Threat Report.** Volume 21, Abril 2016. Disponível em < https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>. Acesso em 13 out. 2016.

THE GUARDIAN. **History of 5-Eyes – explainer**. Disponível em: <https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer>. Acesso em: 23 nov. 2016.

TI SAFE **Segurança da Informação. Ataques atribuídos ao Anonymous colocam em risco as infraestruturas críticas do Brasil.** 2015. Disponível em <http://tisafe.com.br/site/index.php/pt-br/blog/item/102-ataques-atribuidos-ao-anonymous-colocam-em-risco-as-infraestruturas-criticas-do-brasil>. Acesso em 20 nov. 2016.

TSUKAYAMA, Hayley. **Flame cyberweapon written using gamer code, report says.** The Washington Post. 2012. Disponível em < https://www.washingtonpost.com/business/technology/flame-cyberweapon-written-using-gamer-code-report-says/2012/05/31/gJQAkIB83U_story.html>. Acesso em 04 set. 2016.

UNDER-LINUX.ORG. **Crimes Cibernéticos: Ataques mais Direcionados para Infraestruturas Críticas.** 2015. Disponível em < https://under-linux.org/content.php?r=9455>. Acesso em 13 out. 2016.

VIANNA, Nilson. **A defesa cibernética na visão da MB**. Marinha do Brasil. 2012.

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