UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

EDUARDO KREIBICH

CIBERESPAÇO BRASILEIRO: CARACTERIZAÇÃO, ORGANIZAÇÃO E POLÍTICAS

Porto Alegre
2016

EDUARDO KREIBICH

CIBERESPAÇO BRASILEIRO: CARACTERIZAÇÃO, ORGANIZAÇÃO E POLÍTICAS

Trabalho de conclusão submetido ao Curso de Graduação em Relações Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título de Bacharel em Relações Internacionais.

Orientador: Prof. Dr. Marco Aurélio Chaves Cepik

Porto Alegre

2016

CIP - Catalogação na Publicação

Kreibich, Eduardo
Ciberespaço Brasileiro: caracterização, organizações e políticas / Eduardo Kreibich. -- 2016.
83 f.

Orientador: Prof. Dr. Marco Aurélio Chaves Cepik.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Ciências Econômicas, Curso de Relações Internacionais, Porto Alegre, BR-RS, 2016.

1. Ciberespaço. 2. Brasil. 3. Segurança. 4. Crimes cibernéticos. 5. Defesa. I. Cepik, Prof. Dr. Marco Aurélio Chaves, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

EDUARDO KREIBICH

CIBERESPAÇO BRASILEIRO: CARACTERIZAÇÃO, ORGANIZAÇÃO E POLÍTICAS

Trabalho de conclusão submetido ao Curso de Graduação em Relações Internacionais da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para obtenção do título de Bacharel em Relações Internacionais.

Aprovada em: Porto Alegre, _____de _____de 2016.

BANCA EXAMINADORA:

Prof. Dr. Marco Aurélio Chaves Cepik – Orientador
UFRGS

Prof. Dr. Érico Esteves Duarte – Examinador
UFRGS

Prof. Dr. José Miguel Quedi Martins – Examinador
UFRGS

AGRADECIMENTOS

Gostaria de agradecer primeiramente a meus pais, Marli e Sergio, cujo apoio e carinho foram essenciais para que pudesse realizar esta tarefa. Muitos foram os momentos de dúvida, mas sempre poder contar com as palavras motivadoras transformou essa tarefa em algo um pouco menos difícil e complicado. Agradecer a meu irmão, Gustavo, que com seu jeito engraçado e falador conseguia diminuir minhas preocupações.

Ao professor Marco Cepik, que em todo esse trajeto me auxiliou com grande atenção, sempre demonstrando estar disponível e ser paciente para acompanhar o trabalho e indicar a direção a ser seguida. Ao Osvaldo, por sacrificar seu próprio tempo para me auxiliar na revisão deste trabalho.

A todos os meus amigos que sempre me apoiaram e com os quais dividi momentos de risos e descontração, que foram essências para tornar esse trabalho muito mais prazeroso. À Mina e a Luna, cuja companhia e alegria me acalmava e me auxiliava a focar na realização deste trabalho.

Por último, agradecer também ao desenvolvimento industrial que tornou o café e as bebidas energéticas facilmente acessíveis à população brasileira, podendo ser encontrados em qualquer supermercado, e que desempenharam um papel crucial na realização deste trabalho.

RESUMO

Dado o desenvolvimento tecnológico e a dependência cada vez maior em relação às tecnologias, surgem atualmente ameaças cibernética, para cujas quais os Estados já estão se preparando estrategicamente e institucionalmente. Este trabalho tem o objetivo de apresentar e analisar a situação atual da estratégia brasileira para o ciberespaço bem como a maneira como as instituições e organizações foram moldadas com suas respectivas atribuições e responsabilidades. Com isso, faz-se uma avaliação crítica em relação à adequação brasileira diante das novas ameaças para a segurança nacional. O trabalho demonstra que o ciberespaço brasileiro está crescendo, e diante disso surge a necessidade de respaldo de estruturas físicas, além de sinalizar que os incidentes cibernéticos tem tendência de aumentar futuramente. Além disso, o trabalho descreve e analisa a arquitetura institucional brasileira, identificando os atores e as suas responsabilidades em relação ao ciberespaço. Por último, analisam-se os documentos nacionais para identificar as políticas que são desenvolvidas para a Segurança e Defesa cibernética, além de se fazer uma conclusão sobre a adequabilidade ou não das políticas tomadas em relação às principais ameaças cibernéticas, quais sejam, os crimes cibernéticos e a espionagem cibernética.

Palavras-chave: Ciberespaço. Brasil. Segurança. Crimes cibernéticos. Defesa.

ABSTRACT

Given the technological development and the increasingly bigger dependence in relation to the technologies, cyber threats arise at present, for which States are already preparing strategically and institutionally. This study's objective is to present and analyze the current situation of the Brazilian strategy for cyberspace as well as the manner in which the institutions and organizations have been shaped with their respective attributions and responsibilities. With that, a critical evaluation is made in relation to the adequacy of the Brazilian policies before the new threats to national security. This study demonstrates that cyberspace in Brazil is growing, and in relation to that that, arise the need to have a response in terms of physical infrastructure, beyond signalizing that the cybernetic incidents have a tendency to increase in the future. Furthermore, this study describes and analyzes Brazil's institutional architecture, identifying the actors and their responsibilities in relation to cyberspace. For last, the national documents are analyzed to identify the policies that are developed with Cybersecurity and Cyberdenfese in mind, beyond that a conclusion is made about the adequacy or not of the policies made in relation to the primary cyber threats to Brazil, which are cybernetic crimes and cyber espionage.

Keywords: Cyberspace. Brazil. Security. Cybernetic crimes. Defense

LISTA DE FIGURAS

Figura 1 - Usuários de Internet (% população) 27
Figura 2 – Assinantes de Banda Larga (% população) 28
Figura 3 – Usuários de telefonia móvel (% da população) 29
Figura 4 – Mapa dos cabos submarinos que conectam o Brasil 31
Figura 5 – Modelo de ameaças no ciberespaço: atores, alvos e capacidades 35
Figura 6 – Total de incidentes reportados ao CERT.br por ano 39
Figura 7 – Distribuição de incidentes por categoria 40
Figura 8 – Organograma das instituições brasileiras 42

LISTA DE ABREVIATURAS E SIGLAS

ABIN	– Agência Brasileira de Inteligência
ANATEL	– Agência Nacional de Telecomunicações
ANSSI	– *Agence Nationale de la Sécurité des Systèmes d'Information*
APF	– Administração Pública Federal
Casa Militar	– Casa Militar da Presidência da República
CEGSIC	– Curso de Especialização em Gestão de SIC
CEPESC	– Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações
CERT.br	– Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CDCiber	– Centro de Defesa Cibernética
CDN	– Conselho de Defesa Nacional
CGI.br	– Comitê Gestor da Internet no Brasil
ComDCiber	– Comando de Defesa Cibernética
CREDEN	– Câmara de Relações Exteriores e Defesa Nacional
CTIR.gov	– Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal
DDoS	– *Distributed Denial of Service*
DSIC	– Departamento de Segurança da Informação e Comunicações
EB	– Exército Brasileiro
ENaDCiber	– Escola Nacional de Defesa Cibernética
END	– Estratégia Nacional de Defesa (2008)
FA	– Forças Armadas
GSI/PR	– Gabinete de Segurança Institucional da Presidência da República
IBGE	– Instituto Brasileiro de Geografia e Estatística
ITI	– Instituto Nacional de Tecnologia da Informação
MCI	– Marco Civil da Internet
MD	– Ministério da Defesa
NIC.br	– Núcleo da Informação e Coordenação do ".br"
PAED	– Plano de Articulação e Equipamento da Defesa

PF	– Polícia Federal
PNAD	– Pesquisa Nacional por Amostra de Domicílio
PND	– Política Nacional de Defesa (2005)
RENASIC	– Rede Nacional em Segurança da Informação e Criptografia
SGDC	– Satélite Geoestacionário de Defesa e Comunicações Estratégicas
SIC	– Segurança da Informação e Comunicações
SISBIN	– Sistema Brasileiro de Inteligência
SMDC	– Sistema Militar de Defesa Cibernética
TIC	– Tecnologias de Informação e Comunicação
URCC	– Unidade de Repressão a Crimes Cibernéticos
US DoD	– *United States Department of Defense*
USCYBERCOM	– *United States Cyber Command*

SUMÁRIO

1. INTRODUÇÃO 11

2. CIBERESPAÇO BRASILEIRO: UMA CARACTERIZAÇÃO 22

2.1 Conceito de Ciberespaço e de Infraestruturas Críticas 22

2.2 O Ciberespaço brasileiro 26

2.3 Fontes de insegurança e ameaça às infraestruturas críticas 34

3. DEFENDENDO O CIBERESPAÇO: ORGANIZAÇÕES 41

4. DEFENDENDO O CIBERESPAÇO: POLÍTICAS 54

4.1 Abordagem política para a segurança cibernética 54

4.2 Abordagem militar de defesa do ciberespaço 60

5. CONCLUSÃO 71

REFERÊNCIAS 77

1. INTRODUÇÃO

A inovação acelerada e a contínua atualização das Tecnologias de Informação e Comunicação (TIC) têm permeado os diversos campos da atividade humana, gerando crescente relevância e abrangência em diferentes áreas (GASTALDI, JUSTRIBÓ, 2016, p.: 133). Toda a humanidade que tem acesso a algum nível de desenvolvimento econômico se acostumou, em decorrência desse acesso, a facilidades em seu cotidiano para realizar diversas tarefas ou atividades como, por exemplo, assistir um filme, pesquisar em bibliotecas, comprar livros, etc. Com o advento principalmente da internet, essas mesmas atividades agora podem ser realizadas muito mais rapidamente de forma eletrônica através das TIC. Além disso, diversas novas tecnologias para a comunicação e processamento de dados vão surgindo com o passar do tempo. Os telefones celulares com acesso à internet já dominam as mãos e a atenção de diversas pessoas ao redor do mundo, assim como os *tablets* e os *notebooks*. Atualmente, fluxos gigantescos de informação são transmitidos de maneira quase instantânea para qualquer lugar do globo em que exista a infraestrutura necessária para poder recebê-los. Com isso, acostuma-se cada dia mais com a independência e o conforto que as TIC proporcionam, tornando possível a realização de tarefas cotidianas em qualquer hora e de qualquer lugar (MANDARINO, 2010, p.: 31).

Ademais, essa verdadeira revolução informacional atinge não somente os cotidianos individuais das pessoas, mas também o setor industrial bem como o setor estatal. Os Estados e as indústrias passam cada vez mais a depender dessas novas tecnologias e dos fluxos informacionais para manterem o seu pleno funcionamento. Por isso, nas últimas décadas, a informação tem sido cada vez mais considerada um bem valioso.

Em virtude da crescente dependência das sociedades e dos Estados em relação a esses diversos sistemas computacionais e de comunicação, a integridade da informação se coloca cada vez mais como um aspecto essencial para a segurança nacional de um Estado. Sendo assim, segundo as palavras de Gonçalves (2016):

> O grande desafio para todos os que nascemos antes da Internet e desse Big Bang tecnológico ocorrido ao final da Guerra Fria é exatamente como entender e se portar na nova realidade em que o mundo esta ao alcance de um toque no smartphone, em que os sistemas de abastecimento de água e eletricidade, transportes, comunicações, finanças e tudo mais com que lidamos no dia a dia está conectados a um universo virtual, do qual nos tornamos completamente dependentes. Se isso se aplica no campo pessoal, mais ainda se dá no espaço coletivo, particularmente na relação entre os povos. Por

> consequência, tem-se cooperação e conflito, ou seja, a essência da vida humana e das nações. (GONÇALVES, 2016, p.: 20)

Em virtude do crescimento do mercado de produtos e serviços cada vez mais revolucionários e baseados em TIC, observa-se uma dependência tecnológica e informacional sem precedentes, que além de oferecer as vantagens citadas anteriormente, se coloca como ameaça para a segurança nacional dos Estados (FONSECA; DELGADO, 2016, p.: 179). Segundo Fonseca e Delgado (2016), é necessário perceber que a amplitude de informações que seguem o desenvolvimento das TIC é bastante atrativa para criminosos cibernéticos, já que torna possível o roubo de dados confidenciais, além de existir a possibilidade de dano a alguma estrutura ou serviço crítico de um Estado (FONSECA; DELGADO, 2016, p.: 179).

Nesse novo ambiente virtual chamado de "Ciberespaço", *hackers* podem explorar, principalmente através da Internet, falhas de segurança computacionais de diversas maneiras. Em particular, a informação armazenada digitalmente pode ser interrompida, atrasada, corrompida, roubada e modificada. Além disso, os invasores podem deixar *backdoors*[1] nos sistemas para que possam dispor da informação em outro momento, ou utilizar um computador invadido para perpetrar ataques (CAVELTY, 2012, p.: 106). Com o auxílio de Cavelty (2012) podemos fazer uma breve exposição sobre as principais formas utilizadas para se realizar ataques pela Internet. Os vírus e os *worms* são programas de computador que replicam cópias funcionais de si mesmos com diversos efeitos, de simples inconveniências até o comprometimento da integridade de informações confidenciais. Já os *spywares* são *softwares* maliciosos que coletam informações sobre os usuários sem o seu conhecimento. Os "Cavalos de Tróia" são programas que agem de maneira automática, e que podem atuar como ladrões de informação ou até mesmo como um ponto estratégico para o *hacker* ter acesso facilitado ao computador invadido. Por último, os *bots* ou *botnets* são constituídos por uma rede de computadores infectados, em que o programa malicioso fica no plano de fundo executando continuamente, permitindo acesso remoto para o invasor bem como deixar essa rede à sua disposição. Um dos principais usos dessas *botnets* é para a perpetração de ataques DDoS[2]. Nesses ataques, o objetivo é fazer com que um computador

[1] Backdoor é um recurso utilizado por diversos malwares com o intuit de garantir acesso remoto à sistemas ou à redes infectadas, explorando falhas críticas não documentadas existentes em programas instalados, softwares desatualizados e do firewall para abrir portas do roteador.

[2] Em um ataque distribuído de negação de serviço (*Distributed Denial of Service*), um computador mestre denominado Master pode ter sob seu comando até milhares de computadores Zombies, literalmente zumbis. Nesse caso, as tarefas de ataque de negação de serviço são distribuídas a um "exército" de máquinas escravizadas.

ou uma rede fique indisponível para seus usuários principalmente através da saturação do alvo com um grande fluxo informacional, fazendo com que seja impossível que o alvo consiga responder às informações de tráfico legítimo (CAVELTY, 2012, p.: 120).

É através dessas diversas ferramentas e métodos que os chamados "ciberataques" ocorrem. Atualmente, existem diversos exemplos que podem ser citados e que correspondem a esses ataques cibernéticos. Os grupos *hacktivistas*[3] Anonymous e Lulzsec já são bem famosos mundialmente por invadirem sites de governos e de grandes empresas e interromperem o serviço virtual oferecido por eles, geralmente com um objetivo ideológico por trás dessa ação. Por outro lado, existem organizações criminosas especializadas em atuar no meio cibernético Esse é o caso da América Latina, em que a fraude bancária através do ciberespaço perpetrada por essas organizações especializadas gera grande preocupação para as sociedades.

Outro exemplo importante de ser citado no que diz respeito aos ataques cibernéticos seria o chamado "Caso Snowden", que revelou uma arquitetura de espionagem e vigilância internacional estruturada pelos EUA, fazendo alvos tanto na América quanto na Europa (EMPRESA BRASIL DE COMUNICAÇÃO, 2013). Esse caso escapa um pouco do que poderia ser uma conceituação de ataque cibernético, já que não há um dano real propriamente dito, mas sim a identificação e a interceptação da informação, sem modifica-la. Entretanto, a utilização do meio virtual para a espionagem nesse caso é muito importante para demonstrar até onde podem chegar esses ataques cibernéticos.

Os ataques cibernéticos aos sites do governo estoniano em 2007 estão entre os casos internacionais que mais recebem destaque. O governo russo foi acusado pelos líderes estonianos de terem sido os atores dos ataques. Supostamente, então, o governo russo teria utilizado *botnets* para realizarem ataques de DDoS em sites governamentais da Estônia, fazendo com que eles ficassem indisponíveis. Entretanto, a Estônia admitiu não ter provas que apoiassem a acusação feita (THE GUARDIAN, 2007).

Em 2008, os ciber ataques ocorridos durante a Guerra Russo-Georgiana também tiveram efeitos similares sobre os sites governamentais, com alguns deles ficando indisponíveis pelo período de um dia inteiro (NY TIMES, 2008). Novamente os russos foram acusados, e negaram

[3] Junção de *hack* e "ativismo". É entendido como a atuação através de ataques cibernéticos que tem o objetivo de expresser uma ideologia política.

as acusações. Além disso, as evidências eram insuficientes para que se demonstrasse uma ligação clara entre os ataques e o governo russo.

Possivelmente, o mais notório dos ataques cibernéticos é o caso Stuxnet, ocorrido em 2010. O Stuxnet é o nome que foi dado ao *worm* que atacou os sistemas SCADA da Siemens, sistemas esses que são utilizados para controlar e monitorar o processo industrial. Em virtude disso, os atacantes supostamente teriam conseguido causar danos nas centrífugas do programa nuclear iraniano. Esse caso recebeu, e ainda recebe grande atenção pela comunidade internacional em virtude do alto nível de sofisticação envolvido nesse ataque. É nesse sentido que a descoberta do Stuxnet em 2010 modificou bastante o tom e a intensidade do debate internacional acerca do ciberespaço (CAVELTY, 2012, p.: 111). Dada a grande complexidade envolvida nesse *worm*, requerendo habilidades muito avançadas de programação e conhecimento interno sobre o processo industrial, o argumento de que houve envolvimento estatal direto com o Stuxnet ganhou bastante espaço no debate.

Seguindo esse pensamento, e sabendo que a informação e a comunicação adquirem cada vez mais um papel importante para as sociedades e para os Estados, pode-se afirmar que o ciberespaço começou a ser percebido como um espaço que pudesse ser utilizado como instrumentos de poder para as ações estatais, sobretudo no que diz respeito às relações internacionais. Com efeito, cada vez mais os Estados compreendem a importância das TIC e do ciberespaço para as relações interestatais, e com as consequentes imersões das esferas pública e privada no ciberespaço, surge a possibilidade, por parte da primeira esfera, de projetar poder em tal ambiente (NETO, LOPES, 2016, p.: 61). Tendo esse objetivo, alguns teóricos se esforçam para criar um conceito de poder cibernético, como é o caso de Joseph Nye. Ele argumenta que o poder cibernético é aquele mesmo que sempre foi perseguido pelos grandes estadistas e analisados pelos teóricos políticos ao longo da história humana, mas que foi moldado pela Revolução da Informação. Com isso, surge o poder cibernético, entendido por ele como a capacidade de se obter resultados preferidos por meio do uso de recursos de informação eletronicamente interligados ao ciberespaço (NYE, 2010). Apesar de existirem diversas críticas contundentes em relação à conceituação sobre o ciberespaço, são notáveis os esforços de diversos autores no sentido de tentar criar conceitos para esse campo.

Decorrente da ideia de utilização do ciberespaço como instrumento de poder, alimentada principalmente pelo que ocorreu nos três ataques cibernéticos citados anteriormente – caso

estoniano, caso Guerra Russo-Georgiana, e o caso Stuxnet – (IISS, 2011, p.: 27), surge atualmente a chamada "guerra cibernética". A literatura especializada nesse assunto é dividida, apresentando grandes divergências em relação ao que se caracteriza efetivamente como guerra cibernética. De um lado temos o grupo dos estudiosos que afirmam que a guerra cibernética é uma ameaça real e inevitável (ARQUILLA, 2012; BRENNER; CLARKE, 2010). De outro lado temos um grupo mais cético em relação ao assunto, que debate se a iminência de uma guerra cibernética é real (RID, 2012; CAVELTY, 2012).

Para esse primeiro grupo, os três casos citados anteriormente (caso da Estônia, caso da Guerra Russo-Georgiana, e o caso Stuxnet) são exemplos claros de guerra cibernética. Segundo as palavras de Arquilla (2012):

> A guerra cibernética de 2007 contra a Estônia, surgida aparentemente de raiva étnica russa em relação à remoção de um monumento da II Guerra Mundial, ofereceu um exemplo claro. O ataque, inicialmente, foi altamente disruptivo, forçando o governo a tomar medidas rápidas e abrangentes para instalar *patches* de segurança, aperfeiçoar *firewalls*, e tornar disponível às pessoas fortes ferramentas de encriptação. A Estônia é pequena, mas um dos países mais conectados no mundo; 97% de sua população fazem as operações bancárias pela internet. Custos infligidos pelos ataques – de interrupção e disrupção de negócios até a necessidade de erigir novas defesas – são estimados na casa de muitos milhões de euros. (ARQUILLA, 2012, p.: 1-2, tradução livre)[4]

Para Arquilla (2012), no que diz respeito ao caso de 2008, a ciberguerra contra a Geórgia se provou devastadora. Isso porque o avanço dos tanques russos teria sido facilitado por ciberataques aos sistemas de comando, controle, e comunicações de Tbilisi, que foram rapidamente e quase completamente interrompidos. (ARQUILLA, 2012, p.: 1). Ademais, para os autores dessa corrente:

> Enquanto a guerra cibernética provavelmente não irá substituir a tradicional guerra cinética, ela se tornará uma arma cada vez mais importante nos arsenais dos Estados-Nação por muitas razões. Uma delas é custo: desenvolver a capacidade de fazer guerra cibernética é uma proposta barata se comparado ao que está envolvido no desenvolvimento e manutenção da capacidade de fazer guerra cinética no século XXI. Já que a guerra cibernética será na maior parte travada sobre redes que podem ser acessadas publicamente, o gasto envolvido primariamente é composto do treinamento e pagamento

[4] The 2007 cyberwar against Estonia, apparently arising out of ethnic Russian anger over removal of a World War II monument, offered a clear example. The attack was initially highly disruptive, forcing the government to take swift, widespread measures to install security patches, improve firewalls, and make strong encryption tools available to the people. Estonia is small, but one of the world's most wired countries; 97 percent of its people do all their banking online. Costs inflicted by the attacks - from business interruption and disruption to the need to erect new defenses - are estimated in the many millions of euros. (ARQUILLA, 2012, p.: 1-2)

> de "guerreiros cibernéticos" e a compra e manutenção de *hardware* e *software* que será necessário para eles lançaram e também mitigarem ataques cibernéticos. (BRENNER & CLARKE, 2010, p.: 3, tradução livre)[5]

Para o grupo dos mais céticos em relação ao assunto, os casos citados anteriormente não se classificam como ciberguerra. Utilizando-se da teoria clausewitziana da guerra, Rid (2012) faz uma argumentação sobre a interpretação desses ataques como sendo atos de guerra cibernética. Sendo assim, qualquer ação agressiva que aspire ser considerada um ato de guerra, ou que possa ser interpretada desse jeito, precisa alcançar três critérios: caráter violento, caráter instrumental, e natureza política. Sobre o primeiro ponto, Rid (2012) afirma que se um ato não é potencialmente violento, ele não pode ser considerado um ato de guerra. Em um ato de guerra, existe sempre a potencialidade ou a realidade de que ele seja letal para pelos menos alguns dos participantes. Emprestando-se das ideias de Clausewitz, Rid afirma que a violência é o ponto crucial de toda a guerra. Em relação ao segundo ponto, Rid afirma que um ato de guerra é sempre instrumental, que deve ter um meio e um fim. A violência ou a ameaça da força seriam os meios. O fim, então, seria forçar o inimigo a aceitar a vontade do atacante (RID, 2012, p.: 7). Por último, no que diz respeito ao terceiro ponto, um ato de guerra seria sempre política em sua natureza. A guerra, em si, nunca é um fenômeno isolado, sempre tendo um propósito político que transcende o uso da força (RID, 2012, p.: 8).

Para Rid, então, a própria utilização do conceito de "guerra" para explicar esses casos de ataques cibernéticos é errônea, já que eles não poderiam ser classificados como atos de guerra por não cumprirem com os critérios anteriores. Tomando o primeiro ponto como exemplo, os ataques cibernéticos não são qualificados como violentos por que nunca causaram a perda de uma vida, nunca machucaram uma pessoa, e nunca danificaram uma construção (RID, 2012, p.: 11). Rid afirma que quando a guerra é propriamente definida conceitualmente, não se conhece atualmente nenhum ato de guerra cibernética. Entretanto, ele afirma que existem ações cibernéticas de caráter ofensivo com objetivos político. Mas, segundo ele, todos esses incidentes conhecidos e que parecem carregar teor político não são consideradas nem crime comum, e nem guerra

[5] While cyberwarfare will probably not displace traditional, kinetic warfare, it will become an increasingly important weapon in the arsenals of nation-states for several reasons. One is cost: Developing the capacity to wage cyberwar is an inexpensive proposition compared to what is involved in developing and maintaining the capacity to wage twenty-first century kinetic war. Since cyberwarfare will for the most part be waged over publicly-accessible networks, the expense involved primarily encompasses training and paying cyberwarriors and purchasing and maintaining the hardware and software they will need to launch and counter cyberattacks. (BRENNER & CLARKE, 2010, p.: 3)

comum. Os objetivos seriam os de subversão, espionagem e sabotagem (RID, 2012, p.: 15). Nessa mesma linha de pensamento, Cavelty (2012) também afirma que não existem exemplos de ataques cibernéticos que resultaram em violência física contra pessoas, assim como muitos poucos ataques realmente resultaram em algum tipo de dano substancial, como foi o caso Stuxnet (CAVELTY, 2012, p.: 115). Além disso, o possível dano causado por um ato de guerra cibernética estaria fortemente associado a uma complexa sequência de causas e consequências, que em última instância resultariam em violência e em vítimas (RID, 2012, p.: 9). McGraw (2013) também levanta um questionamento sobre a classificação de um incidente sem nenhum impacto cinético no mundo real como ato de guerra cibernética. Para ele:

> Por exemplo, derrubar um site ou infectar um computador com um vírus malicioso é um ato de guerra cibernética? Mesmo que essas atividades sejam enquadradas às vezes como guerra, essa é uma abordagem muito geral para se tomar. (MCGRAW, 2013, p.: 111-112, tradução livre)[6]

Entretanto, o que os dois grupos parecem concordar é sobre o fato de que o ciberespaço, e principalmente a internet, gera algum tipo de ameaça para os Estados, mesma que não seja exatamente na forma de guerra cibernética. Para eles, o crime cibernético e a espionagem cibernética se caracterizam por serem ameaças reais e sérias para a segurança nacional dos Estados (CAVELTY, 2012, p: 119). Cavelty (2012) afirma que:

> Indubitavelmente, ataques à tecnologia da informação, manipulação de informação, ou espionagem podem ter sérios efeitos presentes e/ou futuros sobre a efetividade defensiva e ofensiva das forças armadas de um país. (CAVELTY, 2012, p.: 121-122, tradução livre)[7]

Em relação à espionagem cibernética, McGraw (2013) afirma que ela é muito mais comum que a guerra cibernética. Devido à natureza massivamente interconectada e altamente distribuída dos sistemas informacionais, as informações são cada vez mais difíceis de se manterem secretas (MCGRAW 2013, p.: 111). Com isso, ele argumenta que ao mesmo tempo em que é tão fácil armazenar e transferir informações, também é muito mais fácil de que a

[6] For example, is taking down a website or infecting a computer with a malicious virus an act of cyber war? Although these activities are sometimes framed as war, this is far too sweeping an approach to take. (McGRAW, 2013, p.: 111-112)

[7] Undoubtedly, attacks on information technology, manipulation of information, or espionage can have serious effects on the present and/or future of defensive or offensive effectiveness of one's own armed forces. (CAVELTY, 2012, p.: 121-122)

informação seja manipulada. Já sobre crime cibernético, McGraw afirma que ele é muito mais pervasivo do que a guerra cibernética ou a espionagem, mas que mesmo assim o debate desse assunto entre os tomadores de decisões é pouco amplo. (MCGRAW, 2013, p.: 110)

A autoria dos ataques cibernéticos e a responsabilização desses autores pelos danos causados é um ponto sensível nos debates sobre o ciberespaço e as relações interestatais. Com efeito, o que caracteriza os espaços territoriais soberanos dos Estados é o uso de demarcações fronteiriças. Entretanto, no ciberespaço é muito difícil precisar exatamente o *situs* de origem do ataque, assim como o *situs* onde se consuma o ataque (NETO; LOPES, 2016, p.: 60). Exemplo dessa situação pode ser dado com o uso das *botnets*, já que dessa forma, por haver muitos computadores envolvidos e em lugares diferentes, fica difícil de se conseguir provas putativas sobre os atores por trás do ataque, já que não existe origem única relacionada ao incidente. Além disso, o envolvimento de atores civis nos atos de agressão faz com que seja difícil responsabilizar Estados pelos incidentes cibernéticos. Essa dificuldade de atribuição surge porque os computadores situados no suposto ponto de origem de um ataque podem ter sido sequestrados ou manipulados por terceiros, como é o caso mencionado anteriormente sobre as *botnets*. Dessa forma, é difícil para um Estado achar a fonte de um ataque cibernético e decidir sobre a resposta apropriada a ser tomada (IISS, 2011, p.: 7).

Vale ressaltar também que a própria dificuldade em se atribuir responsabilidade sobre os ataques pode ser algo conveniente para os atores estatais. Os ataques cibernéticos que aparentemente beneficiam os Estados podem ser o trabalho de terceiros operando sobre uma variedade diferente de motivações. Ao mesmo tempo, os Estados também podem se aproveitar dessa dificuldade para poder se distanciar oficialmente dos ataques cibernéticos, tornando possível que ataques sejam realizados sem que uma conexão direta possa ser estabelecida (CAVELTY, 2012, p.: 110). Sobre o caso Stuxnet, Cavelty (2012) afirma que:

> As evidências para o Stuxnet ser considerado uma arma cibernética patrocinada por governo e direcionada ao Irã, apesar de convincente e plausível, é inteiramente circunstancial. Devido ao problema de atribuição, é impossível saber quem deu a ordem, quem realmente programou o Stuxnet, e as reais intenções por trás dele. (CAVELTY, 2012, p.: 112, tradução livre)[8]

[8] The evidence for Stuxnet being a government-sponsored cyber weapon directed at Iran, though convincing and plausible, is entirely circumstantial. Due to the attribution problem, it is impossible to know who gave the order, who actually programmed Stuxnet, and the real intent behind it. (CAVELTY, 2012, p.: 112)

Relacionado ao debate sobre guerra cibernética e a dificuldade de atribuição de responsabilidades, Cavelty (2012) argumenta que o uso indiscriminado do termo "guerra cibernética" não é útil. Para ela, o necessário é que exista uma categorização conceitual sobre as várias formas de conflito no ciberespaço. Essa seria uma condição indispensável para que os Estados possam lidar com as ameaças cibernéticas, alocando responsabilidades, implementando medidas preventivas e conduzindo investigações criminais (CAVELTY, 2010, p.: 1).

Mesmo que a possibilidade real de guerra cibernética ainda seja alvo de intensos debates da literatura especializada, e que exista ainda grande dificuldade para atribuir responsabilidade para os atores dos ataques, os Estados já reconhecem as ameaças provenientes do ciberespaço. Em virtude disso, diversos países já desenvolvem suas estratégias de segurança nacional cibernética bem como suas doutrinas de defesa no ciberespaço (NETO, LOPES, 2016, p.: 70).

Em 2011, o Departamento de Defesa dos Estados Unidos (US DOD) lançou a sua estratégia para o ciberespaço, em um documento intitulado "*Department of Defense Strategy for Operating in Cyberspace"*. Nesse documento, foram definidos cinco iniciativas estratégicas para a atuação do DoD no ciberespaço. A primeira e mais importante dessas iniciativas afirma que o DoD tratará o ciberespaço como um domínio operacional para organizar, treinar e equipar de maneira que o DoD possa aproveitar todo o potencial que o ciberespaço proporciona (US DOD, 2011, p.: 5). Juntamente com a criação do "*United States Cyber Command"* (USCYBERCOM) em 2009, a estratégia de segurança de 2011 demonstra que os EUA percebem o ciberespaço como um meio possível de se travar a guerra, implicando que é necessária a criação de capacidades para ataque, defesa e dissuasão no ciberespaço.

Em 2015, essa estratégia é atualizada e desenvolvida em um documento mais extenso que, segundo especialistas, demonstra uma mudança na maneira como os EUA veem as ameaças do ciberespaço. Nesse sentido, os EUA não estariam mais preocupados com um possível Pearl Harbor cibernético, mas sim com as ameaças persistentes de ataques de baixo perfil que podem causar danos aos indivíduos e às firmas, bem como aos sistemas industriais (FARRELL, 2015). Entretanto, deve-se ressaltar que o ciberespaço ainda é visto como um domínio operacional para os EUA, e juntamente com isso existe o desenvolvimento de capacidades de ataque cibernético. A mudança basicamente se dá pela diminuição do tom alarmista que se tinha no primeiro documento. Além disso, ao tratar sobre os adversários estatais no ciberespaço, o documento aponta que Rússia e China têm desenvolvido capacidades cibernéticas avançadas. Segundo o

documento, a "China rouba propriedade intelectual de negócios globais para beneficiar as empresas chinesas e diminuir a competitividade dos EUA" (US DOD, 2015, p.: 9). No que diz respeito aos atores não estatais, o Estado Islâmico é citado como ameaça por usar o ciberespaço para recrutar seguidores e disseminar sua propaganda, além de já terem demonstrado interesse em adquirir capacidades cibernéticas com objetivo militar (US DOD, 2015, p.: 9).

Além dos Estados Unidos, diversos outros países já lançaram suas estratégias de segurança cibernética e atuação no ciberespaço, algumas delas já estando em sua segunda versão. A França, por exemplo, lançou em 2011 sua estratégia de segurança cibernética, e em 2015 essa estratégia foi atualizada. Além disso, para auxiliar em seus objetivos de segurança cibernética, em 2009 foi criada a "*Agence nationale de la sécurité des systèmes d'information*" (ANSSI). Essa agência é responsável por propor regras para a proteção dos sistemas de informação do Estado e verificar a implementação das medidas adotadas, além de monitorar, detectar, alertar e reagir a ataques cibernéticos, especialmente nas redes do Estado (ANSSI, 2016).

A fim de ilustrar essa preparação dos Estados que reflete na elaboração de estratégias para o ciberespaço, podemos citar mais alguns exemplos. Em 2011, a Alemanha publicou a "*Cyber Security Strategy for Germany*". O Reino Unido, também em 2011, lançou o documento intitulado "*The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*", cuja estratégia foi atualizada em 2016 no documento "*National Cyber Security Strategy 2016-2021*". A Turquia publicou em 2013 o "*National Cyber Security Strategy and 2013-2014 Action Plan"*, cuja estratégia para o ciberespaço foi atualizada em 2016. A Índia, em 2013 publicou a "*National Cyber Security Policy (2013)"*. A Rússia publicou há 16 anos o "*Information Security Doctrine of the Russian Federation"*, e atualmente essa doutrina está em processo de atualização. Além disso, publicou em 2011 o documento intitulado "*Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space"*.

É evidente que nos últimos anos existe uma maior disposição e organização de esforços por parte dos Estados para se preparar para a guerra cibernética e para enfrentar as diversas ameaças advindas do ciberespaço. Deve ser notado, ainda, que os países citados anteriormente diferem bastante em relação aos seus modelos de segurança e defesa, econômico, social e gestão governamental. Isso só enfatiza que os problemas cibernéticos enfrentados hoje são de escala mundial e independem de princípios políticos (MANDARINO, 2010: p 27).

Tendo em vista esse movimento internacional de preparação institucional e estratégica perante o ciberespaço, o presente trabalho tem como foco analisar o caso brasileiro. O objetivo é apresentar e analisar a situação atual da estratégia brasileira para o ciberespaço bem como a maneira como as instituições e organizações foram moldadas com suas respectivas atribuições e responsabilidades. Com isso, espera-se poder entender e avaliar criticamente a adequação da resposta brasileira diante das novas ameaças para a segurança nacional. Em termos metodológicos, o trabalho se utilizou de análise da literatura especializada no assunto, documentos nacionais sobre o ciberespaço, leis nacionais, e análise de dados quantitativos.

Para cumprir esses objetivos, o trabalho foi dividido em cinco capítulos, sendo o primeiro esta introdução. No segundo capítulo, trata-se de definir o próprio conceito de ciberespaço e de infraestruturas críticas, para depois ser caracterizado o ciberespaço brasileiro e tentar definir as principais ameaças que se colocam para a segurança nacional. No terceiro capítulo, apresentam-se as organizações institucionais brasileiras e suas respectivas atribuições, além de discorrer sobre dispositivos legais que legislam sobre o ciberespaço. No quarto capítulo, abordamos a estratégia brasileira no seu sentido mais macro. Em primeiro lugar, faz-se uma análise sobre a abordagem política para a segurança cibernética. Em segundo lugar, analisa-se a abordagem militar de defesa do ciberespaço. Por último, têm-se as conclusões sobre o trabalho.

2. CIBERESPAÇO BRASILEIRO: UMA CARACTERIZAÇÃO

A definição dos conceitos relacionados ao ciberespaço e a cibersegurança ainda carece de desenvolvimento e pesquisa, e demonstram grande variação em suas diferentes conceituações. Em virtude disso, a primeira seção desse capítulo se dedica a abordar os conceitos de *ciberespaço* e de *infraestruturas críticas,* que serão importantes para o desenvolvimento das análises desse trabalho.

2.1 Conceito de Ciberespaço e de Infraestruturas Críticas

Desde a década de 1980 diversos autores deram suas contribuições e tentaram definir o que seria esse novo espaço digital que cada vez mais permeia a vida das sociedades e as relações entre os Estados. O ciberespaço, termo que hoje aparece nas diversas pautas dos debates sobre segurança nacional e estudos estratégicos, já passou por uma grande evolução desde os seus primórdios, mas mesmo assim não encontra uma definição que seja preponderante na literatura especializada sobre o assunto. Para ilustrar essa situação, basta notar que um estudo recente achou mais de 28 definições de ciberespaço (KRAMER, 2009, p.: 10), demonstrando que as áreas de estudo que intentam compreender as dinâmicas do ciberespaço e o seu efeito no Sistema Internacional ainda carecem de trabalhos de conceituação.

Um dos aspectos importantes a ser destacado é que o ciberespaço, por suas características intrínsecas de ser um meio construído e fortemente moldado pela mão humana, está sob constante mudança, o que nos leva a crer que uma própria definição de ciberespaço pode ser modificado com o tempo em virtude dos mais diversos fatores. No que diz respeito à utilização desse conceito para a construção de uma estratégia nacional de segurança cibernética e diretrizes de políticas públicas, deve ser destacado que o emprego desse conceito por parte dos Estados não deve ser feita de maneira a restringir as análises e as políticas públicas (KRAMER, 2009, p.: 10), mas sim como uma ferramenta que auxilie nesse trabalho de criação de diretrizes para as estratégias nacionais. Tendo isso em mente, e relacionando a definição de ciberespaço com os estudos estratégicos, John B. Sheldon (2012) faz um paralelo com a definição de poder aéreo sobre como as diferenças entre os países em termos de capacidade tanto quanto de cultura moldam e afetam esses conceitos:

> Como muitas outras disciplinas, o campo dos estudos estratégicos coloca primazia nas definições mesmo que, na realidade, elas sejam sempre contextualmente e culturalmente situadas. Por exemplo, uma definição norte americana de poder aéreo pode não ressoar com, digamos, uma definição ugandense, dadas as vastas diferenças de experiências históricas e operacionais, bem como as diferenças em capacidades e como o instrumento de poder aéreo é utilizado com vistas a atingir objetivos políticos traçados pelas respectivas políticas. (SHELDON, 2012, p.: 2, tradução livre)[9]

Extrai-se dessa argumentação a importância e a delicadeza com que a conceituação de ciberespaço deve ser tratada pelos Estados, em particular o Brasil, que é o foco do estudo realizado nesse trabalho. No Brasil, a própria menção relevante sobre ciberespaço é recente, recebendo primeiras atenções na Política Nacional de Defesa de 2005 (PND) e na Estratégia Nacional de Defesa de 2008 (END), tendo esse conceito sido mais bem desenvolvido somente a partir da publicação do Livro Verde de Segurança Cibernética em 2010 (Livro Verde). Mesmo já tendo evoluído no sentido de aprofundar essa definição (e outras que são pertinentes), o caso brasileiro ainda precisa receber atenção por parte dos dirigentes estatais, desenvolvendo o seu entendimento sobre ciberespaço para que com isso possa trabalhar as diretrizes de sua estratégia nacional de segurança cibernética. Importa entender que essa definição em si não é algo simples e que:

> A questão de definir ciberespaço não é trivial. O que decidimos incluir ou excluir do ciberespaço tem implicações significativas para as operações de poder, já que isso determina o alcance das estratégias para o ciberespaço e as operações de *cyber-power*. (BETZ; STEVENS, 2011, p.: 36, tradução livre)[10]

Após essa breve exposição sobre a dificuldade e a importância da definição desse conceito, passamos para a ilustração de algumas características do ciberespaço, bem como a própria definição em que o trabalho se baseia. Das diversas definições que competem por espaço nas análises dos especialistas nos assuntos, a de Kuehl (2009) parece ser a que consegue definir mais concisamente esse fenômeno:

---

[9] Like many other disciplines, the field of strategic studies places a premium on definitions even though, in reality, they are always contextually and culturally situated. For example, an American definition of air power may not necessarily resonate with, say, a Ugandan definition, given the vast differences in historical and operational experiences, as well as differences in capability and how the instrument of air power is wielded in order to achieve political objectives set out by the respective polities. (SHELDON, 2012, p.: 2)

[10] The issue of defining cyberspace is not trivial. What we decide to include or exclude from cyberspace has significant implications for the operations of power, as it determines the purview of cyberspace strategies and the operations of cyber-power. (BETZ; STEVENS, 2011, p.: 36)

> Ciberespaço é um domínio global dentro do ambiente da informação cujo caráter distinto e único é moldado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar, e explorar a informação através de redes interdependentes e interconectadas usando tecnologias, informação e comunicação. (KUEHL, 2009, p. 29, tradução livre)[11]

A partir da definição de Kuehl, o primeiro aspecto importante a ser destacado é a diferença grande que existe entre Ciberespaço e Internet. Esse primeiro precede o segundo em diversas décadas. Como o ciberespaço tem a características de uso da eletrônica e do espectro eletromagnético, as redes de telégrafo, rádio amador, telefonia fixa e/ou móvel e televisão via satélite o configuravam muito antes do advento da internet (CEPIK; CANABARRO; BORNE, 2014, p.: 3). Além disso, vale destacar que o uso incorreto de termos como "ciberespaço", "internet" e "web" compromete a pesquisa no campo de relações internacionais voltadas às questões cibernéticas, ademais de gerar dificuldades na adoção de políticas públicas ou até mesmo leis que visem legislar sobre o ciberespaço (CANABARRO; BORNE, 2013).

Em relação às características do ciberespaço, Sheldon (2012) nos auxilia com essa questão, argumentando e elencando alguns aspectos principais sobre o assunto. Em suas análises, ele leva em consideração a ideia de ciberpoder. Devido ao escopo desse trabalho, um debate sobre a definição e validade do conceito de ciberpoder não se apresenta de maneira factível. Entretanto, os argumentos e ideias desse autor ainda parecem ser válidos para entendermos algumas características do ciberespaço.

Um de seus argumentos é o de que o ciberespaço pode ser constantemente replicado, diferentemente do que ocorre com o ar, a terra e o mar. Em uma disputa de poder, a parte importante do ar, do mar e da terra é aquela que está sendo contestada. Essa visão não se aplica dessa maneira ao ciberespaço, já que podem existir ciberespaços contestados e outros não. Para exemplificar, tomamos uma situação de combate aéreo em que as aeronaves inimigas podem ser destruídas. No ciberespaço, um website de organizações criminosas ou terroristas pode ser derrubado para, dentro de horas, o mesmo grupo criar um novo website usando um domínio diferente (SHELDON, 2012, p.: 13). Com efeito, soma-se a isso outra característica importante do ciberespaço: o custo de entrada é relativamente baixo. Claro que para ataques de grande escala ou que visem causar grandes danos, um ataque cibernético requer recursos gigantescos para obter

[11] "Cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies". (KUEHL, 2009, p. 29)

esse efeito, sendo factível dizer que tais efeitos nem mesmo pudessem ser obtidos. Entretanto, para grupos e organizações menores, os recursos monetários e técnicos para tornar possível a exploração do ciberespaço são considerados muito pequenos (SHELDON, 2012, p.: 13). Todas essas características devem ser levadas em consideração quando se tem o objetivo de criar políticas públicas e doutrinas militares que interagem com esse espaço tão difuso e poroso.

Dada essa breve descrição de algumas das principais características do ciberespaço, e tendo em mente a distinção entre Ciberespaço e Internet, é inegável que esse segundo se tornou o carro-chefe de representatividade do primeiro, merecendo atenção especial. Para isso, parece ser interessante abordar sua estruturação, que é formada por, no mínimo, três camadas distintas (CEPIK; CANABARRO; BORNE, 2014, p.: 4) A camada inferior está relacionada com os elementos físicos que suportam as conexões e os fluxos de dados que circulam neles, podendo ser citado como exemplos desses elementos os satélites, as linhas telefônicas, os cabos submarinos, etc. Já a camada superior é composta pelas informações que são partilhadas e acessíveis pelos usuários, e que sofrem codificação e descodificação na camada intermediária, em que os padrões técnicos e lógicos atuam para tornar a informação acessível pelos usuários (CEPIK; CANABARRO; BORNE, 2014, p.: 4). Ao descrevermos a estrutura da internet, percebemos um dos principais problemas relacionados à ela, qual seja, a territorialidade, que se coloca como um grande desafio para os Estados e para os legisladores, já que é quase impossível precisar um limite territorial-nacional para a internet. Isso certamente dificulta e impacta nas políticas públicas dos Estados para a internet.

Passamos agora a definir conceitos e características sobre as infraestruturas que estão de alguma forma ligadas ao ciberespaço e, consequentemente à internet. Primeiramente, faz-se se necessária a definição de infraestrutura crítica. A definição mais usual que podemos ter é a de que infraestrutura crítica é aquela que, uma vez prejudicada por ações intencionais ou por desastres naturais, traz reflexos negativos para toda a nação. Como exemplo podem ser citadas as redes de distribuição de água e de energia elétrica (MANDARINO, 2010, p.: 38). Já a infraestrutura crítica da informação, segundo Mandarino (2010), busca identificar e proteger *hardware*, *software*, dados e serviços que suportam uma ou mais infraestruturas criticas (MANDARINO, 2010, p.: 39). As Infraestruturas Críticas da Informação, então são a parte da infraestrutura informacional nacional que é extremamente necessária para a continuidade dos serviços de infraestrutura crítica em um país. Podem ser citados como exemplos: o setor de informações e telecomunicações,

computadores, satélites, fibra ótica. Ademais, até mesmo os próprios fluxos de dados que correm entre essas infraestruturas podes ser considerados como infraestruturas críticas da informação, já que sua interrupção pode ter impacto negativo sobre o Estado. Em seguida, faz-se uma breve descrição sobre o ciberespaço brasileiro e algumas de suas infraestruturas críticas.

2.2 O Ciberespaço brasileiro

O Brasil é um país que apresentou desenvolvimento constante no século XXI, e apesar de enfrentar diversas crises e sobressaltos a economia brasileira e, consequentemente, o setor de tecnologias da informação e comunicação conseguiu manter-se no geral em ritmo positivo. Em relação a isso, Diniz, Muggah e Glenny fazem uma pequena síntese:

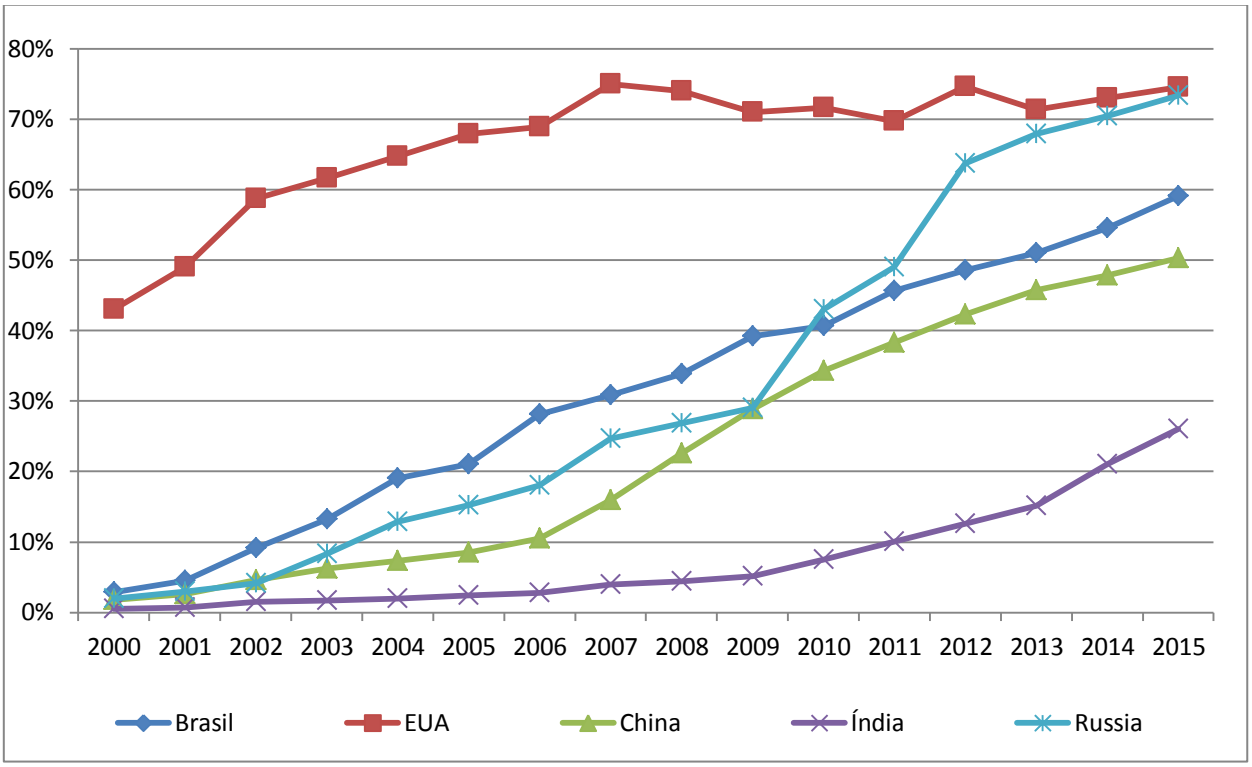
> O Brasil está passando por uma revolução digital com poucos paralelos no mundo em desenvolvimento. A taxa de penetração digital e adoção de mídias sociais subiram exponencialmente na última década. [...] Um número de fatores relacionados à melhora brasileira em desenvolvimento social e econômico estão conduzindo essas tendências. Um clima macroeconômico relativamente estável e políticas sociais fortemente redistributivas resultaram na expansão da classe média no país. Um influxo de novos consumidores simultaneamente aumentou a demanda por tecnologias da informação e comunicação (TIC) e transformou a escala de oferta em níveis proporcionais ao gigante mercado doméstico brasileiro. (DINIZ; MUGGAH; GLENNY, 2014, p.: 5, tradução livre)[12]

Tendo em mente esse panorama de forte crescimento do ciberespaço brasileiro, o objetivo deste capítulo é tentar dimensionar para o leitor esse espaço bem como sua evolução, para que se entenda a necessidade de estudo e pesquisa sobre o assunto. Com isso, deve-se ressaltar que os dados e as análises contidas nessa pretendem ser suficientemente ilustrativos para darem base à argumentação sobre a institucionalização brasileira e permitirem ao leitor dimensionar esse ciberespaço bem como suas infraestruturas críticas. Vale também relembrar que, apesar de o ciberespaço ser muito mais complexo e abrangente do que somente a internet, o foco da argumentação e análise do trabalho recai sobre esse último.

[12] Brazil is undergoing a digital revolution with few parallels in the developing world. The rate of digital penetration and social media adoption has risen exponentially over the past decade. [..] A number of factors relating to Brazil's improvements in social and economic development are driving these trends. A relatively stable macroeconomic climate and strongly redistributive social policies resulted in the expansion of the country's middle class. An influx of new costumers simultaneously ratcheted-up the demand for information and communication technologies (ICTs) and transformed the scale of supply at levels commensurate with Brazil's gigantic domestic market. (DINIZ; MUGGAH; GLENNY, 2014, p.: 5)

No Brasil, o acesso da população à internet tem tido um forte aumento nos últimos 15 anos. A **figura 1** abaixo demonstra dados sobre o caso brasileiro bem como alguns outros países selecionados:

Figura 1 - Usuários de Internet (% população)

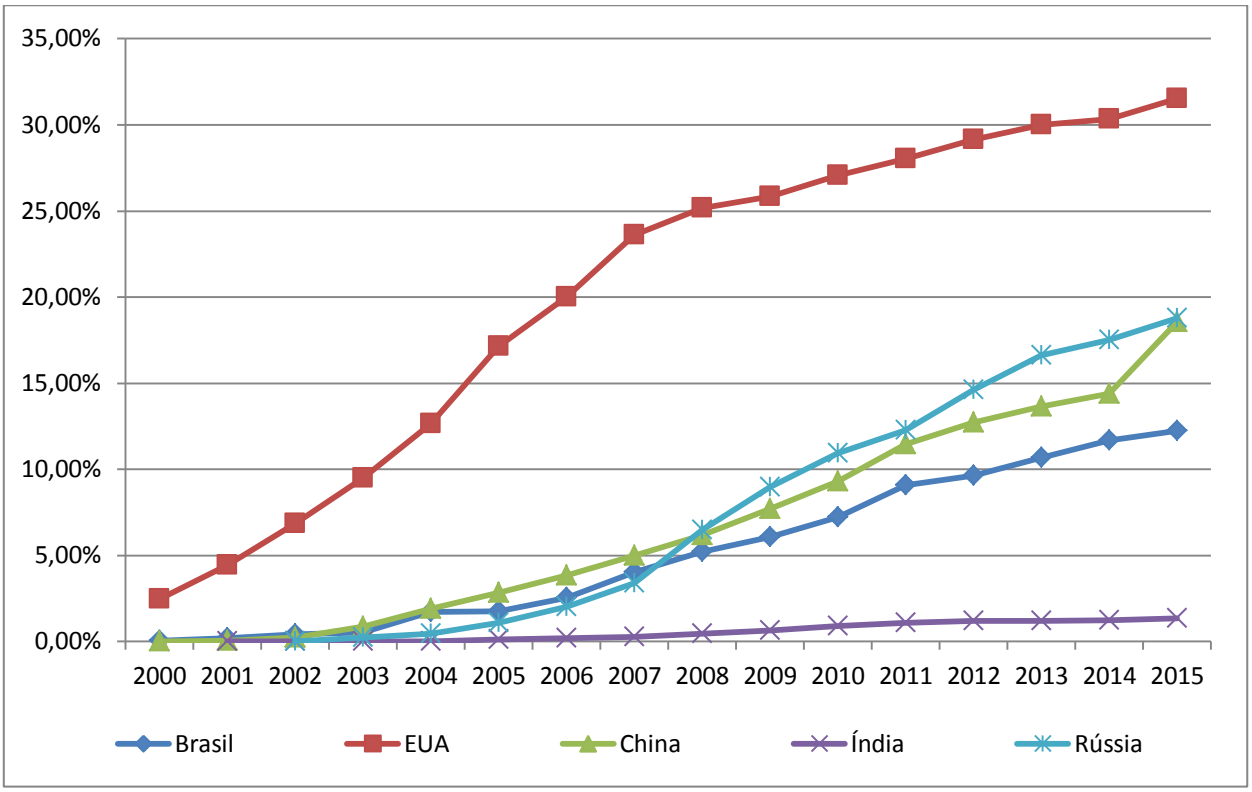


Fonte: WORLD BANK (2016). Elaboração própria.

Segundo os dados do World Bank (2016), no ano 2000 somente 2,87% da população brasileira tinha acesso à internet. Já em 2015, esse quadro demonstra significativa melhora, com mais da metade da população tendo acesso à internet (59%), o que indica vasta expansão da inserção digital da população brasileira e da necessidade de infraestrutura para gerenciar e dar suporte a essas transmissões de dados. Em termos dessa expansão, pode-se comparar o caso brasileiro com o caso chinês, que apresenta uma linha de evolução muito parecida. Além disso, mantendo-se o ritmo dessa expansão, pode-se afirmar que a situação brasileira de acesso da população à internet em alguns anos se apresentará muito parecida com a dos EUA, que exibe um indicador de 74,5% em 2015.

Em relação ao número de assinantes de banda larga no país, a **figura 2** a seguir ilustra a evolução brasileira:

Figura 2 – Assinantes de Banda Larga (% população)



Fonte: WORLD BANK, 2016. Elaboração própria.

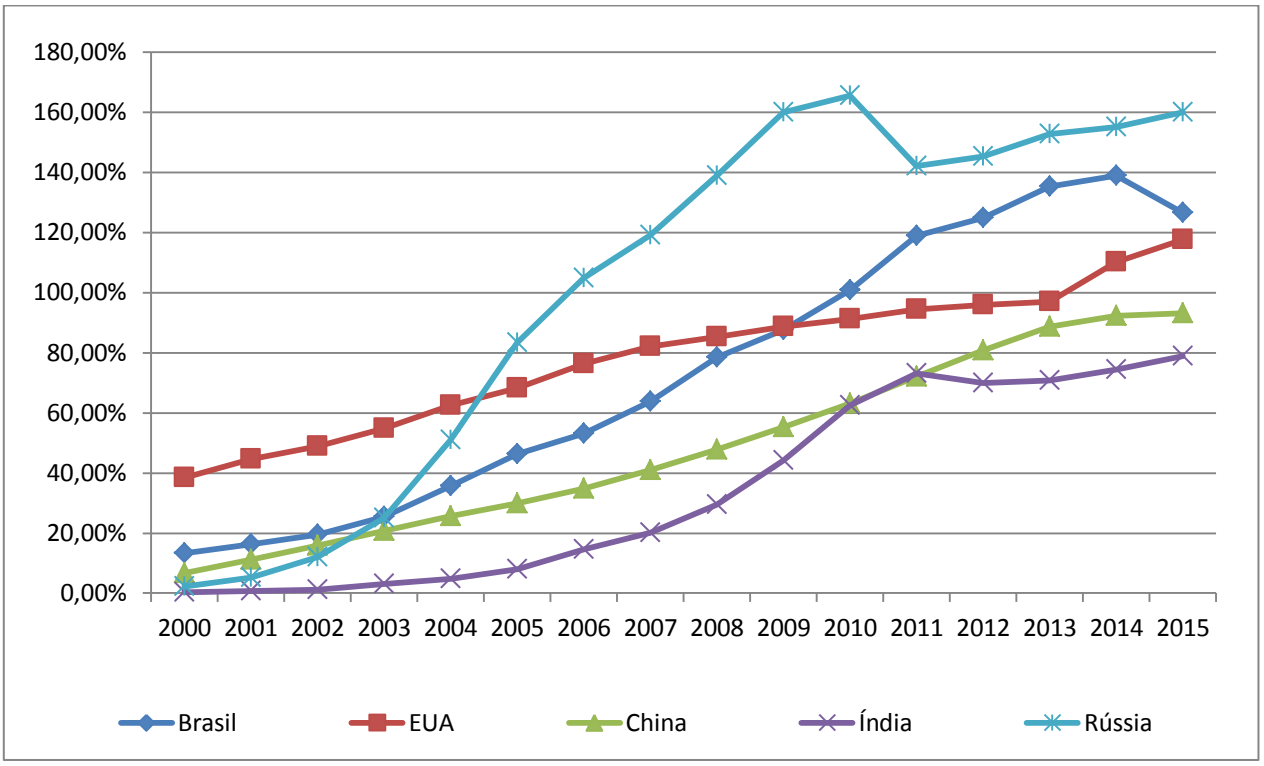
É notável o desenvolvimento brasileiro no que diz respeito a esse indicador. Há 15 anos, a população no Brasil que possuía assinatura de banda larga era muito pequena, e acessava a internet através de conexões bem mais lentas com capacidade de fluxos de dados muitas vezes menor. Em 2015, pouco mais de 12% da população já é assinante de banda larga no Brasil. O fato de cada vez mais a população estar conectada e demandar serviços de internet de banda larga estimula o crescimento do setor de tecnologia no Brasil e amplia a dimensão do ciberespaço.

Com efeito, o próprio Estado brasileiro entra nesse indicador, pois muitas vezes serviços de banda larga também são contratados para uso pelos órgãos públicos e servidores. Dada a penetração e crescente dependência que existe em relação às tecnologias, isso não é algo surpreendente. Ademais, basta notar que diversos serviços que antigamente eram fornecidos baseados na presença do indivíduo e na necessidade de documentos físicos hoje já podem ser feitos via internet.

A telefonia móvel representa uma parte significativa do setor de comunicação no país. O desenvolvimento econômico permite que a população possa cada vez mais adquirir telefones

celulares cuja capacidade de processamento é maior e que permitem o acesso à internet. O **figura 3** nos ajuda a elucidar essa questão:

Figura 3 – Usuários de telefonia móvel (% da população)



Fonte: WORLD BANK, 2016. Elaboração própria.

A trajetória ascendente da linha demonstra um crescimento elevado do setor de telefonia móvel. Analisando as informações, percebemos que no Brasil o número de usuários de telefonia móvel em 2015 foi de 126% da população. Ou seja, o número de linhas ativas ultrapassa a população em termos absolutos. Já, relacionando com outros países, esse número é maior do que o de EUA (117%) e China (93%). Ademais, é importante destacar que o principal meio de acesso à internet no território brasileiro tem mudado nos últimos anos. Segundo a Pesquisa Nacional por Amostra de Domicílio (PNAD) de 2014, o uso do telefone celular para acessar a internet ultrapassou o do computador recentemente no Brasil (IBGE, 2016). O dado de 2014, publicado em 2016, mostra que o celular é usado para navegar em 80,4% dos domicílios com acesso à internet, sendo que o uso do computador para esse fim ficou no patamar de 76,6%, demonstrando queda em relação ao ano de 2013 em que apresentava 88,4%. Em decorrência desse grande aumento da telefonia móvel com acesso à internet está o fato de que os brasileiros são fortes

consumidores de redes sociais. Uma pesquisa demonstrou que as populações latino americanas são os maiores consumidores mundiais de redes sociais, e que o Brasil demonstra posição de destaque dentre elas (WALL STREET JOURNAL, 2013).

A revolução das tecnologias da informação e o crescente acesso da população à internet fez com que o comércio eletrônico se tornasse muito presente no Brasil. As compras feitas através da internet estão cada vez mais comuns e se tornaram uma prática rotineira. Vale destacar que as compras são transações tanto internas como também, compras internacionais. Para elucidar, tomamos o relatório da Mintel[13] (2013) sobre o comércio eletrônico brasileiro demonstrando dados comparativos entre 2008 e 2013. A informação de maior importância se relaciona com o salto dado pelo segmento do *e-commerce*[14] no Brasil, que passou de R$ 14,8 bilhões em 2008 para R$ 51 bilhões em 2013, demonstrando aumento de mais de 200% (MINTEL, 2014). Dados mais atuais trazidos pela Ebit[15] em seu relatório Webshoppers (2016) mostram que em 2015 o e-commerce brasileiro demonstrou aumento nominal de 15,3% se comparado ao registrado em 2014 (EBIT, 2016). Em resumo, o que se deve extrair sobre o comércio eletrônico no Brasil é que ele apresenta basicamente tendências de crescimento contínuo, e isso vai cada vez mais impor ao governo que mantenha atenção às políticas públicas para esse setor econômico.

A partir do panorama exposto até agora nesse capítulo, podemos ter alguma ideia de como se caracteriza o ciberespaço no Brasil. Essas tendências de crescimento no acesso à internet, na disseminação da telefonia móvel, e no comércio eletrônico necessariamente precisam de um respaldo estrutural para existir. Ou seja, para que se mantenham os diversos fluxos informacionais no país e para fora dele, deve-se ter uma infraestrutura física que torne isso possível. Sendo assim, passamos agora a tratar sobre as infraestruturas críticas para a informação no país. Com isso em mente, o trabalho abordará dois elementos: cabos submarinos e satélites.

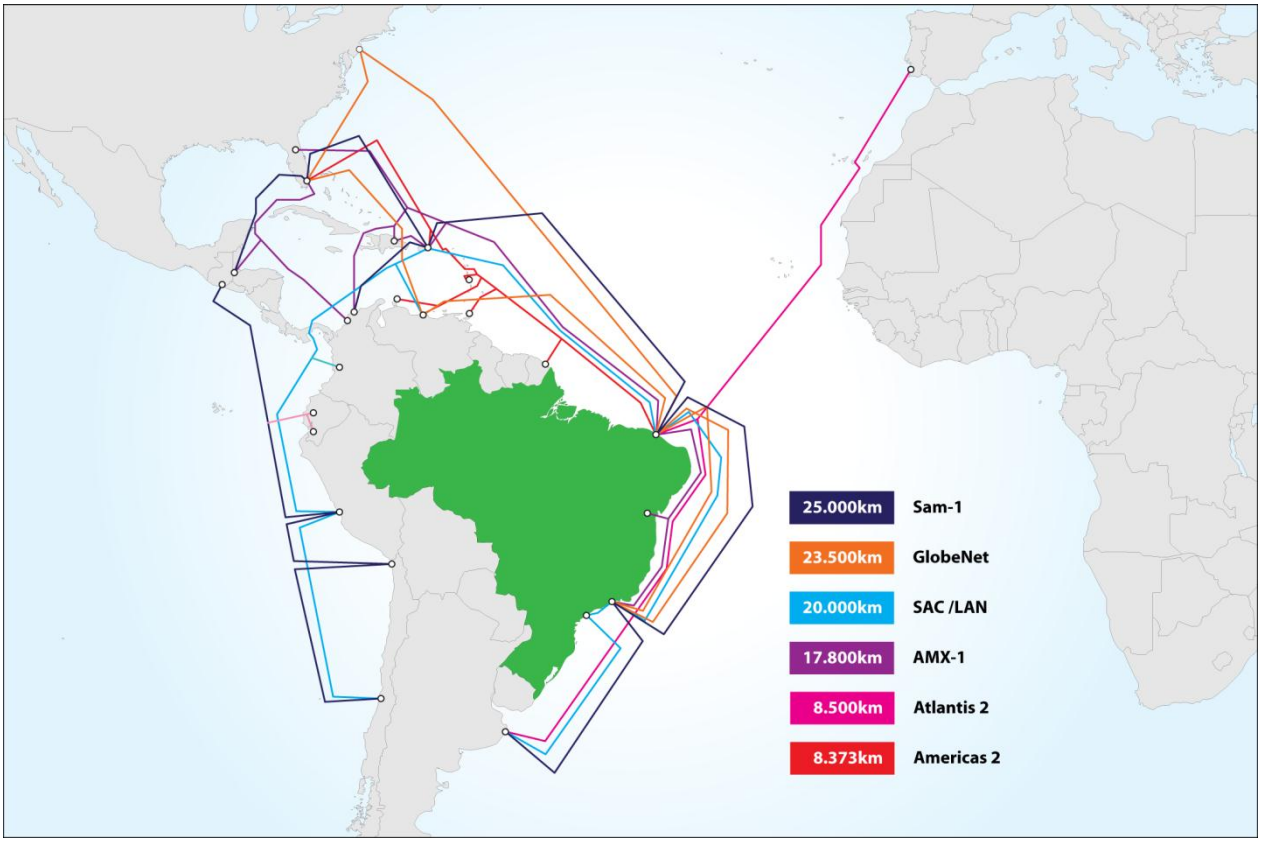
Os cabos submarinos são de grande importância para os fluxos informacionais ao redor do mundo todo, não somente no Brasil. Eles formam o que é chamado de *backbone* da comunicação, ou seja a "espinha dorsal" que estrutura as comunicações e os fluxos informacionais ao redor do

[13] A Mintel Group Ltd é uma firma privada de pesquisa de mercado, baseada em Londres.
[14] Também conhecido como comércio eletrônico, o *e-commerce* é um tipo de transação comercial (com ou sem fins lucrativos) feita especialmente através de um equipamento eletrônico, como, por exemplo, computares, *tablets* e *smartphones*.
[15] A Ebit é uma empresa que certifica lojas online com o objetivo de ajudar os consumidores na escolha de lojas com as melhores reputações e que são mais confiáveis para se fazerem compras.

mundo. Esses cabos são colocados no relevo oceânico entre continentes, ou em diferentes posições terrestres em um mesmo território nacional, e são utilizados para a telefonia, para a transmissão de dados da Internet, para o tráfego de dados privados, entre outros. Dados de 2015 levantados pela TeleGeography afirmam que existem 278 cabos submarinos em operação no mundo (TELEGEOGRAPHY, 2015). Atualizado recentemente, os dados da TeleGeography afirmam que existem 321 sistemas de cabos submarinos que estão ativos, em construção, ou que se espera estarem completamente financiados até o final de 2016 (TELEGEOGRAPHY, 2016).

No Brasil, o primeiro cabo submarino fez parte da primeira linha telegráfica brasileira. Foi inaugurado em 1857 e interligava a Praia da Saúde no Rio de Janeiro com a cidade de Petrópolis, tendo aproximadamente 15 km de cabos submersos. Atualmente, segundo o Ministério das Comunicações, existem seis cabos submarinos em operação que conectam o Brasil com diversos países, assim como demonstra a **figura 4** abaixo.

Figura 4 – Mapa dos cabos submarinos que conectam o Brasil



Fonte: MINISTÉRIO DAS COMUNICAÇÕES, 2015.

De todos os cabos submarinos em operação no Brasil[16], o SAM-1 é o que tem a maior extensão, com 25.000km. Ele foi construído pela empresa espanhola Telefónica S.A em 2001 e posteriormente em 2007 recebeu uma extensão. Esse cabo parte da Argentina, passa pelo Rio de Janeiro, Salvador, Fortaleza, e de lá continua seu trajeto para Porto Rico, Colômbia, Flórida, Guatemala. Depois disso, a expansão em 2007 fez com que o trajeto do cabo retornasse para a parte oeste da América do Sul, interligando Equador, Peru e Chile (MINISTÉRIO DAS COMUNICAÇÕES, 2015). A capacidade inicial desse cabo que entrou em operação em fevereiro de 2001 é de 40 Gb/s, expansível até 1,92 Tb/s. Essa capacidade, apesar de ser bem significativa, está aquém das altas capacidades que alguns cabos conseguem chegar. Em cada cabo submarino é possível armazenar vários pares de fibra, números expressivamente maiores do que os 4 pares que correspondem ao cabo SAM-1 e, em cada fibra, é possível transportar até 10 Tb/s (MINISTÉRIO DAS COMUNICAÇÕES, 2015).

Além dos cabos submarinos apresentados na figura anterior, existem diversos outros projetos de cabos submarinos a serem implantados, que valem ser brevemente apontados aqui. A empresa Google tem planos de instalar um cabo submarino que ligará o Rio de Janeiro a São Paulo, sendo batizado de Júnior. A previsão é de que o cabo terá 390 km, e o início das operações ocorrerá no segundo semestre de 2017 (TELETIME, 2016a). A operadora de cabos submarinos Seaborn Networks tem planos de instalar o cabo Seabras-1, que ligara Nova York à Santos (SP), até o segundo trimestre de 2017. Com seis pares de fibras óticas com capacidade inicial de 72 Tb/s, esse cabo demonstra grande capacidade de fluxo, contrastando com os cabos citados até agora (TELETIME, 2016b). Outro cabo submarino, cuja entrada em operação está estimada para o começo de 2018, é o BRUSA, do grupo espanhol Telefónica. O cabo terá 11.000 km e ligará o Brasil aos Estados Unidos, saindo do Rio de Janeiro e Fortaleza, passando por San Juan, em Porto Rico, até Virginia Beach, nos EUA (TELETIME, 2016c). A joint-venture Ellalink, empresa formada pela Telebras e pela espanhola Islalink, tem projeto de instalar um cabo submarino de 5.700 km ligando o Brasil à Europa, mais precisamente, uma conexão de Fortaleza a Lisboa. Esse cabo está previsto para começar a operar no segundo semestre de 2017, e terá capacidade de 30Tb/s (TELETIME, 2016d). O cabo submarino South Atlantic Cable System (SACS), com

[16] Podemos destacar também o cabo submarino Atlantis 2. Com 8.500 km de extensão, ele conecta Argentina, Brasil, Senegal, Cabo Verde, Ilhas Canárias e Portugal, sendo o primeiro a ligar a América Latina ao continente africano. A capacidade desse cabo é bem mais limitada, tendo apenas 40Gb/s, de forma que as transmissões de sinais de voz são priorizadas (MINISTÉRIO DAS COMUNICAÇÕES, 2015).

aproximadamente 6.000 km de extensão está previsto para iniciar suas operações em 2018, e conectará a capital angolana de Luanda ao Brasil, em Fortaleza. A capacidade estimada para esse cabo é de 40 Tb/s, e se torna uma rota alternativa de interconexão com a Europa e a Ásia (TELETIME, 2016e).

Todos esses investimentos demonstram a importância desses cabos para a transferência de dados entre continentes, ou até mesmo entre um mesmo país. Como dito anteriormente, eles formam o *backbone*[17] das comunicações, principalmente no que diz respeito à internet, e atraem vultosos investimentos das grandes empresas desse setor. Ademais, os cabos submarinos são mais baratos e mais eficientes para comunicações em massa e de longas distâncias, levando vantagem em relação a alternativas, como os satélites, que são utilizados mais frequentemente para comunicações de dispositivos móveis em *roaming* internacional (BESSA, 2014, p.: 93). Por outro lado, os satélites são importantes justamente porque complementam essa rede de comunicações, preenchendo certos vazios que são deixados pelos cabos submarinos, como por exemplo, a capacidade de os satélites entregarem banda larga mais facilmente a regiões com difícil acesso.

Segundo a ANATEL (2016), existem 66 satélites autorizados a operar no Brasil. Entretanto, a maioria deles são estrangeiros, o que gera uma vulnerabilidade e também dependência em relação às tecnologias de outros países. O primeiro satélite geoestacionário brasileiro está previsto para entrar em operação em 2017, tendo vida útil de 15 anos. O Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC) objetiva cobrir todo o território nacional com uma banda larga de qualidade, com foco principal em garantir banda larga em áreas de difícil acesso por estruturas físicas terrestre. Além disso, deve ser destacada outra função importante que o satélite irá desempenhar, qual seja, a de dar autonomia e segurança às comunicações das Forças Armadas. Isso ocorre porque atualmente as comunicações de operações militares são feitas em equipamentos controlados por empresas estrangeiras, o que se caracteriza como uma grande vulnerabilidade em caso de conflito estatal (PORTAL BRASIL, 2016).

Em resumo, o ciberespaço brasileiro está cada vez mais se expandindo. O acesso à internet, seja pelo computador, seja pelo telefone celular, está aumentando e cada vez mais inserindo a população no ciberespaço. Sendo assim, na próxima seção serão abordadas as

[17] No contexto de redes de computadores, o *backbone* designa o esquema de ligações centrais de um sistema ais amplo, tipicamente de elevado desempenho.

diversas ameaças cibernéticas que se colocam, de modo geral, frente aos Estados e as sociedades, além de enquadrar em específico as ameaças ao Estado brasileiro.

2.3 Fontes de insegurança e ameaça às infraestruturas críticas

A partir do que foi demonstrado até aqui, resta elucidar ao leitor sobre as ameaças que se originam a partir do ciberespaço. Com esse objetivo, a primeira parte dessa seção tem o objetivo de apontar aspectos gerais relacionados à essas ameaças, como tipo de atores que perpetram esses ataques e os principais alvos. Na segunda parte, analisa-se brevemente o caso brasileiro, trazendo dados que possam demonstrar o panorama brasileiro no quesito de ameaças cibernéticas.

Sem dúvida, como foi apontado anteriormente no trabalho, o carro-chefe do ciberespaço é a internet, e pode ser dito que esse é um dos grandes motivos pelos quais o ciberespaço é uma fonte de ameaças e de preocupações para os Estados. Isso ocorre porque a internet, no primórdio de seu desenvolvimento, não foi pensada com o quesito segurança em mente. Segundo Blumenthal e Clark (2009):

> A internet foi projetada para não apoiar uma aplicação específica, mas com o objetivo de generalidade. Em contraste com a rede de telefonia, por exemplo, que foi inicialmente projetada especificamente para realizar chamadas telefônicas, a Internet foi projetada para suportar uma ampla gama de aplicações, mesmo aquelas ainda não pensadas (BLUMENTHAL; CLARK, 2009, p.: 02).

Em virtude da maneira como foi desenvolvida e estruturada, a internet, então, apresenta algumas vulnerabilidades que impulsionam os ataques cibernéticos. Tavares (2013) elenca 3 principais fatores que permitem ou incentivam esses ataques. Em primeiro lugar, assim como explicado anteriormente, as "falhas" no desenho da Internet são o principal fator:

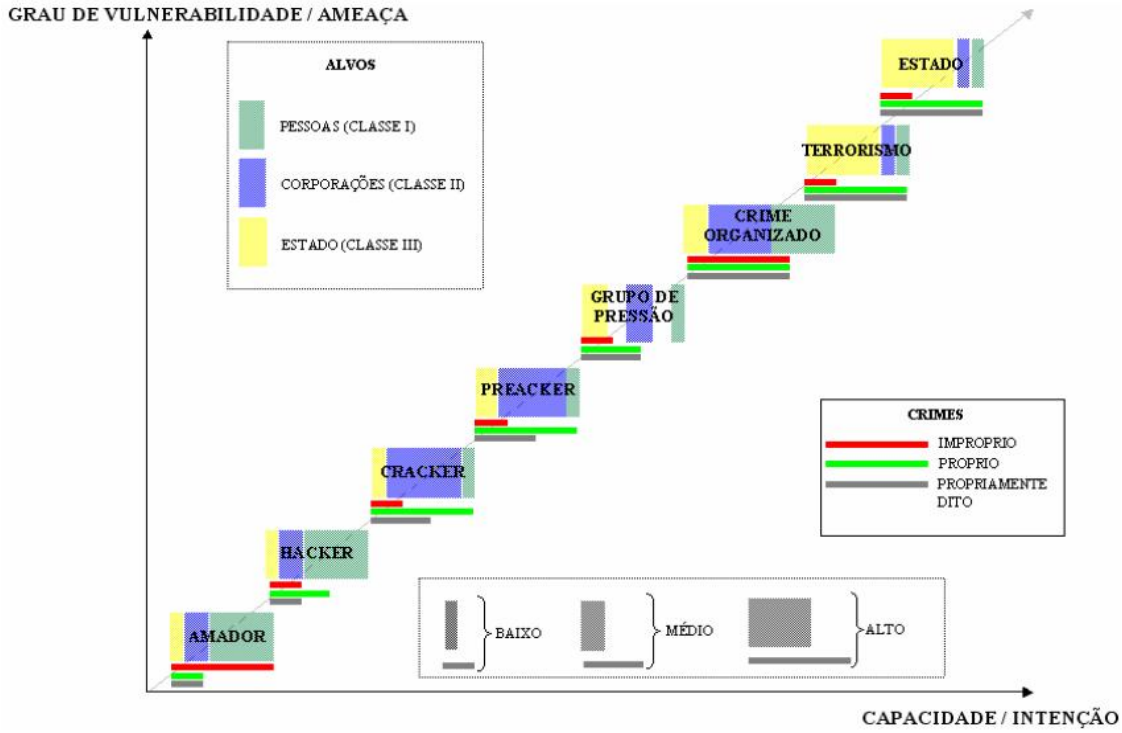
> A Internet é uma rede anárquica por natureza, assim como o sistema internacional; trata-se de uma arquitetura planejada para ser descentralizada. Esta natureza aberta determina que praticamente tudo que faz a Internet funcionar seja aberto, não protegido por encriptação. Essa natureza aberta é imutável – sem ela, a internet seria inviável (TAVARES, 2013, p.: 6).

Além do que foi explicado por Tavares, a Internet garante alto grau de anonimato para os usuários. Localizar os autores de certos ataques não é uma tarefa fácil, já que muitas vezes usam programas que mascaram sua localização. Já em segundo lugar, as falhas de desenvolvimento de

hardware e software acabam deixando brechas à penetração de malware. Em virtude das características descritas anteriormente, a Internet possui grande capacidade de propagar softwares malignos programados para se infiltrar em computadores e causar danos (TAVARES, 2013, p.: 6). Por último, tem-se a tendência global de digitalização de sistemas críticos. Cada vez mais os equipamentos e sistemas eletrônicos que antes funcionavam isoladamente agora estão integrados ou estão em processo de integração à Internet (TAVARES, 2013, p.: 7). O problema central para os Estados é que cada vez mais suas infraestruturas críticas estão de alguma maneira e em diferentes graus conectadas a essa rede ou dependendo dela para seu funcionamento.

Tendo feita essa breve explicação sobre as vulnerabilidades, faz-se necessário, nesse momento do trabalho, caracterizar os principais atores que podem se aproveitar delas. Apesar de não possuir um rigor metodológico, Mandarino (2009), com a intenção de contribuir para o desenvolvimento de uma estratégia de segurança cibernética brasileira, propôs um pequeno modelo que ilustra a capacidade de diferentes atores em perpetrar crimes nos diferentes alvos possíveis, assim como mostra a **figura 5**.

Figura 5 – Modelo de ameaças no ciberespaço: atores, alvos e capacidades



Fonte: MANDARINO, Raphael, 2009: p.: 121

O eixo vertical representa o grau de vulnerabilidade que um ator pode conhecer e explorar para ameaçar um alvo. Já o eixo horizontal representa a capacidade de pesquisa e de disponibilidade de recursos, financeiros e cibernéticos que podem ser aplicados por um ator em sua intenção de atacar um alvo. Os atores estão dispostos a partir da origem da confluência dos dois eixos. Na representação, o ator *amador* ocupa a posição mais baixa, o que representa que esse ator tem pouca capacidade de pesquisa e de disponibilidade de recursos financeiros e cibernéticos para causar dano a um alvo, além de possuir baixo grau de conhecimento sobre vulnerabilidades que podem ser exploradas para ameaçar um alvo. No outro extremo temos o *Estado*, que dispõe de enorme capacidade de recursos e conhece bem as vulnerabilidades que podem ser exploradas para efetuar ataques (MANDARINO, 2009, p.: 119). Em relação aos alvos dos ataques, eles são discriminados em 3 grupos: pessoas (verde), corporações (azul) e Estado (amarelo). Já a capacidade ou intenção de um ator em causar danos aos alvos está representada por níveis. A legenda na parte de baixo da figura auxilia na visualização. O nível 1, que corresponde à faixa mais estreita, caracteriza que o ator tem baixa capacidade de causar danos ao alvo. O nível 2 (faixa de largura média) indica capacidade média. Por último, o nível 3, que corresponde à faixa mais larga, representa alta capacidade de causar danos aos alvos.

Em relação a tipologia dos crimes, tem-se que "crimes cibernéticos impróprios" (vermelho) são aqueles em que o meio eletrônico é apenas uma via para o seu cometimento que pode ser também praticado no mundo real. Os "crimes cibernéticos próprios" (verde) são aqueles que só podem ser cometidos por meio eletrônico e que não existem em outros meios. Exemplo desse tipo pode ser o acesso não autorizado a bases de dados ou sistemas, ou também disseminação de códigos maliciosos. Por último, os "crimes cibernéticos propriamente ditos" (cinzas) que são aqueles onde o próprio computador ou seu processamento é o alvo, como, por exemplo, sabotagem e terrorismo cibernético (MANDARINO, 2009, p.: 96-97).

Os Estados, naturalmente, são os atores mais capazes de perpetrar um ataque cibernético que gere efeitos sérios, devido ao montante de recursos que tem ao seu dispor. Entretanto, no que diz respeito a ataques cibernéticos com impactos sérios à infraestrutura, é importante notar o seguinte:

> Enquanto o dano potencial causado por um possível ataque cibernético contra infraestrutura crítica nacional e outros serviços fundamentais é merecedor de preocupação, nenhum ataque desse tipo ocorreu, até hoje, resultando nesses danos. Isso não significa dispensar a noção de que tais ataques não poderiam ocorrer no futuro, mas

> dados os vários tipos, e crescente número de *threat actors*, os meios cibernéticos cada vez mais sofisticados à sua disposição, e o ambiente rico em alvos que eles podem vir a atacar, é notável que esses ataques devastadores não ocorreram ainda. (SHELDON, 2012, p.: 17, tradução livre)[18]

Apesar da espionagem não ser caracterizada exatamente como um ataque cibernético, ela é uma das principais atividades realizadas pelos Estados no que diz respeito à sua atuação no meio cibernético. Segundo o modelo, poderíamos enquadrar essa ação na categoria de *"crimes cibernéticos próprios*[19]*"*. Como exemplo, podemos tomar o caso Snowden, em que o Brasil foi alvo do esquema de vigilância internacional dos EUA, que interceptou comunicações presidenciais bem como informações da Petrobrás (EMPRESA BRASIL DE COMUNICAÇÃO, 2013). Assim como demonstra o modelo, os Estados têm como principais alvos outros Estados, mas também podem realizar ações de espionagem contra empresas de outros países, como no caso em questão, a Petrobrás.

Em relação aos grupos de pressão como fonte de ameaça no ciberespaço, podemos referenciar o caso do grupo hacktivista Lulzsec. Em 2011, o grupo assumiu a autoria de ataques de negação de serviço contra sites da presidência da República, que ficaram fora de funcionamento por alguns minutos. Além disso, o grupo também teve como alvo a empresa brasileira Petrobrás, que também teve seu site inutilizado por algumas horas (TECMUNDO, 2011). Baseando-se no modelo de Mandarino (2009), percebe-se que essa classe de atores não possui a mesma capacidade e os recursos que um Estado tem para perpetrar ataques cibernéticos. Mesmo assim, essa ameaça deve ser considerada, já que esses grupos podem, como já foi reportado em alguns casos, expor informações sigilosas de Estado e de empresas estratégicas brasileiras.

No modelo de Mandarino (2009) para a estratégia brasileira de segurança cibernética, o crime organizado ocupa a terceira posição no que concerne a disponibilidade de recursos e ao conhecimento das vulnerabilidades a serem exploradas. Definitivamente, no Brasil, o crime organizado é um problema sério, e que tem como principais alvos as pessoas e as empresas. Os

---

[18] While the potential damage caused by a possible cyber-attack against critical national infrastructure and other core services is rightly of concern, no such attack has occurred resulting in such damage to date. This is not to dismiss the notion that such attacks could not occur in the future, but given the various types, and growing number of threat actors, the increasingly sophisticated cyber means at their disposal, and the target-rich environment which they might attack, it is noteworthy that such devastating attacks have not occurred as yet. (SHELDON, 2012, p.: 17)

[19] Os "crimes cibernéticos próprios" são aqueles que só podem ser cometidos por meio eletrônico e que não existem em outros meios.

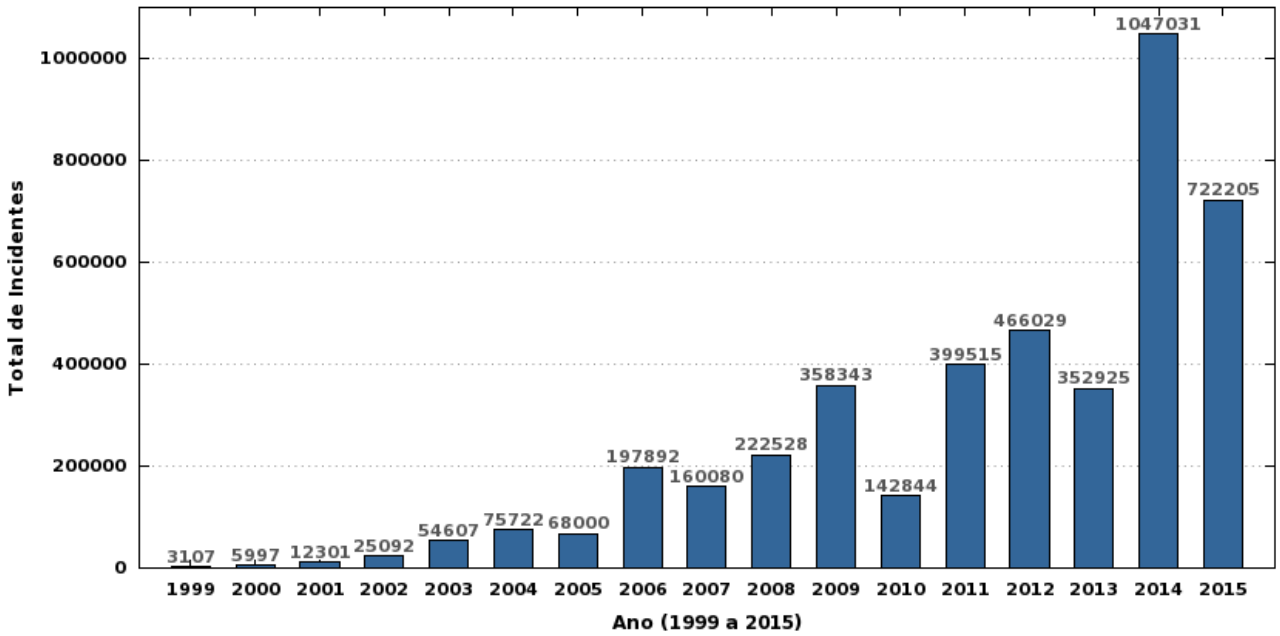
métodos utilizados por esses grupos sãos os mais variados, assim como o tipo de atividades à que se dedicam. A seguir, faz-se uma breve exposição com dados recentes para elucidarmos essa questão.

No Brasil, as operações bancárias online responderam por 41% do número total de transações, e as operações bancárias em dispositivos móveis registraram taxa de crescimento médio exponencial de 270% ao ano, entre 2009 e 2013 (FEBRABAN, 2013, p.: 34). Mesmo com a queda na utilização do e-mail para propagação de ameaças (TREND MICRO, 2015, p.: 38), esse serviço ainda é bastante utilizado quando a motivação é o roubo de informações confidenciais de usuários. De acordo com provedores de serviço e conteúdo no Brasil, cerca de dois milhões de e-mails de spam são gerenciados por dia, com uma porcentagem significativa desses e-mails imitando avisos de cartões de crédito (TREND MICRO, 2015, p.: 20). Alguns dados demonstram que Brasil, México e Colômbia foram os primeiros na lista de países remetentes de spam em 2014, representando mais de 75% do número total nas Américas (TREND MICRO, 2015, p.: 38).

Cada vez mais novas ferramentas são desenvolvidas com a finalidade de roubar informações bancárias. Um exemplo bom, por sua complexidade e sofisticação, é o cavalo de troia BANLOAD, que visa especificamente às instituições bancárias do Brasil. Em 2014 foi descoberto que uma variante do BANLOAD conseguia evitar muito bem sua detecção, e limitava sua propagação para outras regiões (TREND MICRO, 2015, p.: 41). Com efeito, não é de espantar que o Brasil tenha ficado em segundo lugar no mundo em termos de contagem de infecção por malware bancário *online* no terceiro trimestre de 2014, sendo que o país foi responsável por quase 9% do número total de sistemas infectados por malware bancário online em todo o mundo (TREND MICRO, 2014, p.: 7).

Recorrendo à dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), podemos ter uma visão geral sobre os incidentes cibernéticos no Brasil (**figura 6**):

Figura 6 – Total de incidentes reportados ao CERT.br por ano

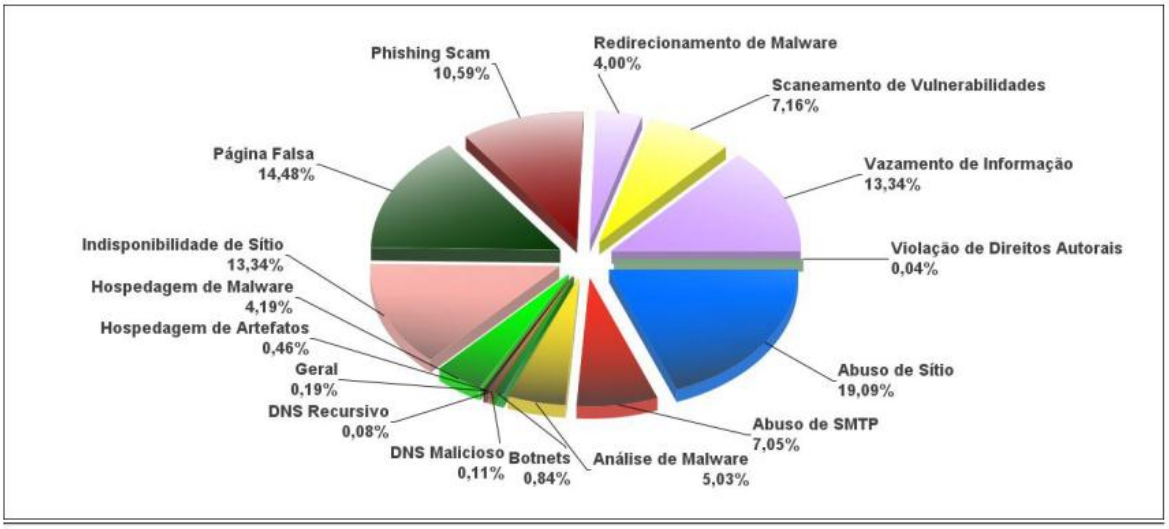


Fonte: CERT.br, 2016a.

Claramente, percebe-se que existe uma trajetória ascendente no que diz respeito aos incidentes reportados ao CERT.br. Entretanto, é difícil afirmar que isso necessariamente reflete um aumento dos ataques cibernéticos ao Estado, empresas e população, já que estas notificações são voluntárias e refletem os incidentes ocorridos em redes que espontaneamente os notificaram ao CERT.br. Sendo assim, seria possível argumentar que simplesmente esse gráfico não reflete um aumento real na quantidade de incidentes que realmente ocorrem. Mesmo que esse fosse o caso, esse seria um bom sinal de que cada vez mais a preocupação com a segurança cibernética está presente no cotidiano das sociedades. Para o entendimento desse trabalho, assume-se que o aumento dos incidentes cibernéticos ocorre de maneira real, em virtude de toda a argumentação já desenvolvida até aqui, em especial na seção sobre o ciberespaço brasileiro.

Já o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR.gov) nos traz algumas informações específicas relacionadas a ameaças cibernéticas contra o Estado (**figura 7**):

Figura 7 – Distribuição de incidentes por categoria



Fonte: CTIR.gov, 2016a.

O gráfico acima nos demonstra a distribuição de incidentes cibernéticos, por categorias, no primeiro trimestre de 2016. Nesse caso, optou-se por um gráfico que conseguisse demonstrar a grande miríade de diferentes ameaças às quais devem ser enfrentadas. Percebe-se que o *vazamento de informações* ocupa espaço importante do gráfico, representando 13,34% dos incidentes na APF. Outro dado interessante de ser mencionado é o de *scaneamento de vulnerabilidades*, que correspondeu a 7,16% dos incidentes. Esse "scaneamento" diz respeito às atividades de varreduras em redes de computadores com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Esse tipo de atividade é amplamente utilizada por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador (CERT.br, 2016a).

Em suma, esse capítulo buscou, além de debater o conceito de ciberespaço, dimensionar o espaço cibernético brasileiro ao leitor, bem como as ameaças que surgem a partir dele. Com isso, pode-se partir para a descrição e análise da institucionalização brasileira que diz respeito ao ciberespaço.

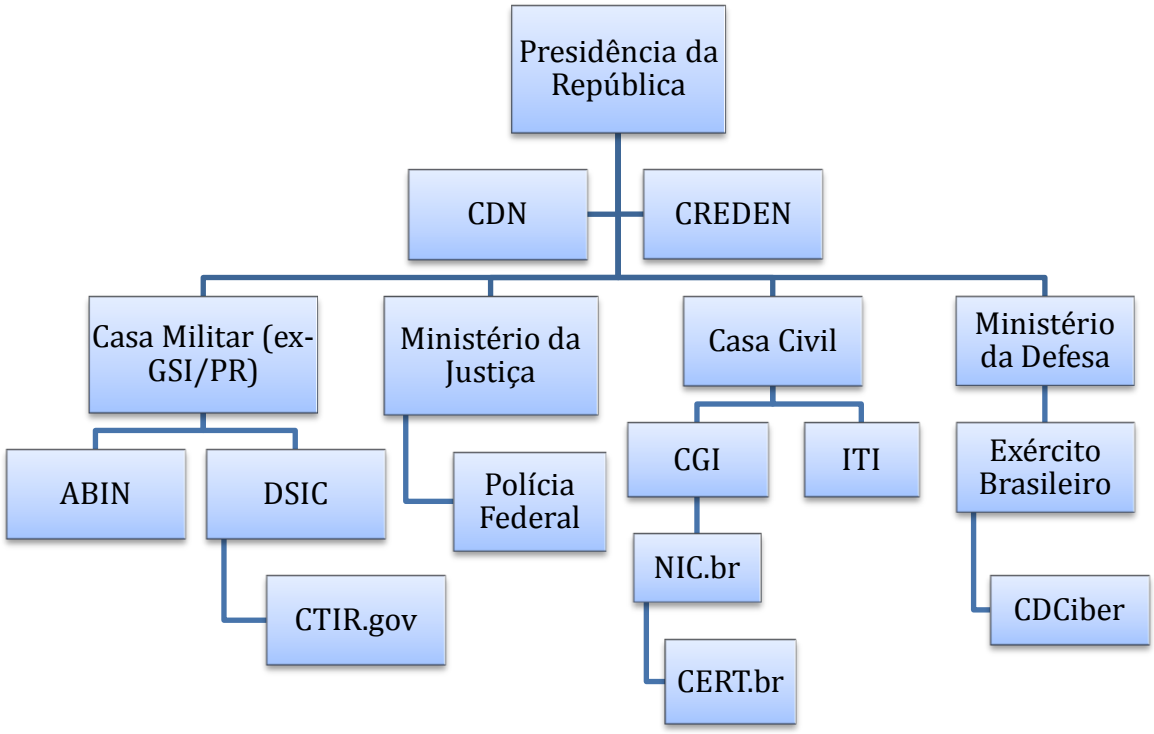
3. DEFENDENDO O CIBERESPAÇO: ORGANIZAÇÕES

Para lidar com todas essas novas ameaças advindas do ciberespaço, os Estados necessitam desenvolver uma arquitetura institucional que distribua competências para as diferentes entidades atuantes. Segundo MANDARINO (2010):

> A necessidade de marco legal no Estado virtual é essencial para o Estado real exercer a soberania interna e externa de seu espaço cibernético – apesar de não haver ainda o reconhecimento consensual de que sua existência é fato, caracterizando-o como parte do Estado / Nação. (MANDARINO, 2010, p.: 43)

Sendo assim, nesse capítulo objetiva-se descrever, explicar, e analisar a estrutura institucional brasileira que se refere ao ciberespaço. O objetivo é tentar perceber se o Brasil avança na questão da institucionalização e quais são os problemas que ainda enfrenta. Dado que existem diversos órgãos, comitês, grupos, entre outros, que lidam com a segurança e defesa do espaço cibernético – seja diretamente focado ou por abrangência de suas funções –, o capítulo aborda somente as instituições que foram consideradas de maior importância para esse objetivo, e que conseguem elucidar melhor os desafios que o Estado deve enfrentar. Abaixo está um organograma (**figura 8**) das instituições que serão abordadas nesse capítulo, e que pretende auxiliar na compreensão do capítulo:

Figura 8 – Organograma das instituições brasileiras



Fonte: DISC, 2016; CERT.br, 2016; BRASIL, 2015b. Elaboração própria.

O Conselho de Defesa Nacional (CDN) é um órgão de consulta do Presidente da República nos assuntos relacionados com a soberania nacional e a defesa do Estado democrático (BRASIL, 1988). Segundo a constituição de 1988, as suas competências são: i) opinar nas hipóteses de declaração de guerra e de celebração da paz ii) opinar sobre a decretação do estado de defesa, do estado de sítio e da intervenção federal. iii) propor os critérios e condições de utilização de áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo. iv) estudar, propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do Estado democrático. Na esfera do ciberespaço, a adaptação dessas competências constitucionais certamente se coloca como um desafio (MANDARINO, 2010, p.: 110), já que muitos dos conceitos imbricados nas competências desse órgão, como por exemplo, as questões da territorialidade e soberania não se adaptam muito bem, em sua maneira clássica, com o ciberespaço. Mesmo que se trate de um órgão de consulta, percebe-se que existe a necessidade de desenvolver esses conceitos para que

eles possam ser aplicados pelo governo através de seus diversos órgãos, com o objetivo de solidificar a estrutura institucional visando maior clareza para a construção das políticas para o ciberespaço. Segundo MANDARINO (2010), "dada sua importância estratégica, o CDN deve manter-se como o palco para as decisões estratégicas relativas às ações de segurança e defesa cibernética". Com efeito, essa função só poderá ser executada de maneira eficiente quando se intensificar o debate de como se dá a territorialidade e a soberania nacional no ciberespaço.

No âmbito do Conselho de Governo, o Decreto nº 4.801, de 6 de agosto de 2003 criou a Câmara de Relações Exteriores e Defesa Nacional (CREDEN), um órgão de assessoramento do Presidente da República nos assuntos pertinentes às relações exteriores e de defesa nacional (BRASIL, 2003a). A finalidade da câmara, segundo o decreto, seria a de formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do Governo Federal, aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidos, no âmbito de ações cujo escopo ultrapasse a competência de um único Ministério. O texto do decreto ainda destaca alguns temas que englobam suas atribuições, qual seja a segurança da informação, a segurança das infraestruturas críticas e a segurança cibernética (BRASIL, 2003b). É possível notar certa falta de rigor nessas atribuições quando percebemos que a "segurança da informação" e a "segurança das infraestruturas críticas" são tratadas como questões separadas da "segurança cibernética". Poderia ser dito que a própria maneira como esses termos são utilizados é sintomática de uma dificuldade em compreender e se adaptar às questões pertinentes ao ciberespaço.

De grande importância para a Segurança cibernética brasileira é a Casa Militar da Presidência da República (Casa Militar), antigo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que foi renomeado pela Medida Provisória nº 696, de 2 de outubro de 2015. Das atribuições dadas a Casa Militar bem como das atribuições dos órgãos que são geridos por ela, percebe-se o papel de destaque que ela tem como engrenagem principal para a coordenação da estratégia de segurança cibernética do país. Do Decreto Nº 8.577, de Novembro de 2015, extraem-se as competências da Casa Militar que estão mais diretamente relacionadas com a segurança cibernética: I- assistir direta e imediatamente o Presidente da República no desempenho de suas atribuições; II- realizar o assessoramento pessoal em assuntos militares e de segurança; III- coordenar atividades de segurança da informação no âmbito da administração pública federal; VII- apoiar técnica e administrativamente o funcionamento do Conselho de

Defesa Nacional[20]. Vale destacar também que os assuntos relacionados à Segurança da Informação e das Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas vêm sendo tratados no âmbito do CDN e do CREDEN, por intermédio da Casa Militar (BRASIL, 2015b, p.: 93).

Sob a égide da Casa Militar, outros órgãos são gerenciados e possuem funções importantes para a segurança cibernética. O Departamento de Segurança da Informação e Comunicações (DSIC) tem suas competências estabelecidas pelo Decreto Nº 8.577, das quais a ele compete: I- orientar a implementação de ações de segurança da informação e comunicações, inclusive as de segurança cibernética, no âmbito da administração pública federal; II- definir normativos e requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da administração pública federal, no âmbito da Secretaria-Executiva do Conselho de Defesa nacional; III- operacionalizar e manter o centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal (CTIR.gov); IV- avaliar tratados, acordos ou atos internacionais relacionados ao tratamento e à troca de informação classificada; V- exercer, por meio do Núcleo de Segurança e Credenciamento, na qualidade de órgão de Registro Central, atividades relacionadas ao credenciamento de segurança e ao tratamento de informação classificada. A partir das atribuições do DSIC descritas acima, percebe-se o caráter central desse departamento, já que ele é responsável por operacionalizar as atividades de segurança da informação e comunicações na Administração Pública Federal (APF). Sendo assim, o pleno cumprimento de suas funções é de vital importância para tornar a segurança informacional da APF mais robusta, bem como para disseminar uma cultura de cibersegurança ao definir normativas que devem ser seguidas dentro dos órgãos de governo.

O CTIR.gov, que funciona sob a gestão do DSIC, cumpre a função de notificação, bem como análise dos incidentes cibernéticos nos computadores da APF (CTIR.gov, 2016b). Além disso, entre seus serviços está o suporte e coordenação na resposta a esses incidentes.

[20] IV- realizar a segurança pessoal do Presidente da República, do Vice-Presidente da República e de seus familiares e, quando determinado pelo Presidente da República, dos titulares dos órgãos essenciais da Presidência da República e de outras autoridades ou personalidades, assegurado o exercício do poder de polícia; V- realizar a segurança dos palácios presidenciais e das residências oficiais do Presidente da República e do Vice-Presidente da República, assegurado o exercício do poder de polícia; VI- planejar e coordenar as ações para a execução de eventos, o uso dos meios de transporte aéreos nas viagens presidenciais e a realização do cerimonial militar nos palácios presidenciais ou em locais determinados pelo Presidente da República; VIII- exercer as atividades de Órgão Central do Sistema de Proteção ao Programa Nuclear Brasileiro.

Efetivamente, o CTIR.gov é de importância para que se avance na identificação de vulnerabilidades na APF, já que ele administra em primeira mão as informações sobre os ataques cibernéticos direcionados às redes federais. As informações que o CTIR.gov consegue agregar podem ser utilizadas para determinar tendências e padrões de atividades de ataques, tornando viável a recomendação de estratégias de prevenção adequadas para toda a APF.

A Agência Brasileira de Inteligência (ABIN) é o órgão central do Sistema Brasileiro de Inteligência (SISBIN), sendo subordinada à Casa militar. Em termos de objetivo, a ABIN tem como foco o desenvolvimento de atividades de Inteligência voltadas para a defesa do Estado Democrático de Direito, da sociedade, da eficácia do poder público e da soberania nacional. Sendo assim, ela atua nas vertentes de inteligência e contra-inteligência em prol do Estado e tem como competência principal, no que diz respeito ao assunto abordado nesse trabalho, a avaliação de ameaças, internas e exterasm à ordem constitucional. Com efeito, a percepção de ameaças em tempo útil permite que se construam mecanismos de defesa nas redes brasileiras de forma muito mais eficiente (MANDARINO, 2009, p.: 105). Como foi abordada em seção anterior, a espionagem perpetrada pelos Estados através do meio cibernético é de fato uma das principais ameaças cibernéticas atuais. Sendo assim, a ABIN cumpre um papel importante de inteligência que deve ser utilizada para fortalecer a arquitetura de segurança cibernética brasileira.

Sendo criada pelo decreto-lei nº 920 de dezembro de 1938, e tendo suas diretrizes e competências modificadas em 2003 com a lei nº 10.683, a Casa Civil é um órgão essencial da Presidência da República, que tem como função geral o assessoramento direto do Chefe do Poder Executivo na coordenação de ações de governo. De suas atribuições que interagem com a segurança do ciberespaço, a principal delas é a de "execução das políticas de certificados e normas técnicas e operacionais, aprovadas pelo Comitê Gestor da Infraestrutura de Chaves Públicas Brasileiras" (ICP-Brasil). Para cumprir com essa função existe o Instituto Nacional de Tecnologia da Informação (ITI), uma autarquia federal vinculada à casa Civil. O ICP-Brasil é "uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para a identificação virtual do cidadão" (ITI, 2016). O avanço brasileiro no sentido de conseguir criar e consolidar uma rede que viabilize essa emissão de certificados digitais é de grande importância para todos os setores da sociedade. Isso por que os certificados digitais permitem que se enviem documentos de maneira virtual e que se possa garantir a autenticidade dos documentos, bem como a identificação do autor do documento. Dessa forma, garante-se que informações

importantes e documentos legais possam ser enviados de maneira digital de um canto do país para outro, terminando com a necessidade de envio físico de documentos que torna o processo informacional muito lento.

Segundo a Portaria Interministerial nº147 de 31 de maio de 1995, "no sentido de tornar efetiva a participação da Sociedade nas decisões envolvendo a implantação, administração e uso da Internet, será constituído um Comitê Gestor da Internet" (CGI.br), que conta com representantes de diversos setores da sociedade relacionados com a internet, como por exemplo, representantes de provedores de internet, usuários finais e comunidade acadêmica. Já em 2003, o decreto nº 4.829 dispõe sobre a criação efetiva do CGI.br que tem como objetivos principais a coordenação e integração de todas as iniciativas de serviços de Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Dentre suas atribuições está "o estabelecimento de diretrizes estratégicas, de recomendações de normas e padrões técnicos e operacionais, a proposição de programas de P&D e de difusão, entre outras" (GADELHA, 2009, p.: 3). É notável que, para se conseguir gestar políticas e diretrizes para esse espaço, a governança da internet, tanto em seus aspectos técnicos de infraestrutura e operação, como nas questões legais e regulatórias, é essencial. Com efeito, a proposta desse Comitê é de estruturar essa governança sobre a internet no Brasil, mas de maneira inclusiva, o que reflete bastante na composição diversificada de seus membros (CGI, 2009, p.: 3).

Indo além, na busca de estruturar essa governança, o CGI.br aprovou em sua 3ª reunião ordinária de 2009 uma cartilha de dez princípios básicos para a governança e o usa da Internet no Brasil. Dos princípios, temos: 1) Liberdade, privacidade e direitos humanos. O uso da internet deve guiar-se pelos princípios de liberdade de expressão, privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática. 2) Governança democrática e colaborativa. A governança da internet deve ser exercia de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva. 3) Universalidade. O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos. 4) Diversidade. A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores. 5) Inovação. A governança da internet deve promover a contínua evolução e

ampla difusão de novas tecnologias e modelos de uso e acesso. 6) Neutralidade da rede. Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento. 7) Inimputabilidade da rede. O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos. 8) Funcionalidade, segurança e estabilidade. A estabilidade, a segurança e a funcionalidade globais de rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas. 9) Padronização e interoperabilidade. A internet deve basear-se em padrões abertos que permitam a interoperabilidde e participação de todos em seu desenvolvimento. 10) Ambiente legal e regulatório. O ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração (CGI.br, 2009).

Esses princípios demonstram uma iniciativa inovadora por trazer a relação do ambiente virtual com a sociedade, destacando a necessidade de se manter princípios garantidos na Constituição, como a liberdade de expressão, e de se manter também a diversidade cultural na rede, em um país fortemente marcado pelo preconceito e por desigualdades. Além disso, essa cartilha não deixa de contemplar a necessidade de combate aos crimes cibernéticos, mantendo-se os princípios de privacidade. É claro que essa não é uma tarefa fácil, já que muitas vezes a análise de tráfegos informacionais é necessária nas investigações. Adicionalmente, o que ainda é muito difícil é a questão sobre até onde fica o limite para esse tipo interceptação ser considerada como necessária ou como um desrespeito à privacidade.

Outra das atribuições do CGI.br é a de organização dos números e nomes de domínios "*.br*", que é operacionalizada pelo Núcleo da Informação e Coordenação do Ponto BR. O NIC.br é uma entidade civil, de direito privado e sem fins lucrativos, que implementa as decisões e projetos do CGI.br (NIC.br, 2014). No que diz respeito ao domínio .br, pode-se dizer que a sua implementação atinge níveis muito bons, considerando-se patamares internacionais. Em 2009, de todas as empresas e pessoas com nomes na rede, 83% utilizavam a terminação ".br", contrastando com a média internacional que era de 20% (GADELHA, 2009, p.: 3). Todos os aspectos até aqui demonstram uma estrutura de governança forte e bem pensada sobre a internet, com a devida atenção à parte técnico-administrativa, necessária para que se mantenha nessa direção.

Um dos órgãos que definitivamente desempenha um papel muito importante para a estratégia brasileira de segurança cibernética é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira (CERT.br), que está vinculado ao CGI.br. De seus objetivos gerais está a atuação como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta e incidentes e também colocando em contato as partes envolvidas, caso seja necessário (CERT.br, 2016b). Aprofundando em suas atividades, percebemos melhor o motivo de sua importância. Por ser responsável por tratar sobre incidentes cibernéticos e pela análise de tendências de ataques, o CERT.br contribui vitalmente para mapear melhor as vulnerabilidades no ciberespaço brasileiro, o que é essencial para se criar políticas públicas efetivas. Em sua atribuição de tratar incidentes, quando o CERT.br dá suporte ao processo de recuperação e ao estabelecimento de um trabalho colaborativo com outras entidades, ele ajuda a desenvolver a cultura de segurança cibernética entre os setores da sociedade brasileira, do empresarial ao pessoal-individual. A última de suas atribuições, que também diz respeito ao desenvolvimento de uma cultura de segurança cibernética, é a de treinamento e conscientização, oferecendo cursos na área de tratamento de incidentes de segurança e desenvolvimento de documentos de apoio pra administradores de redes de internet e usuários (CERT.br, 2016).

Uma das grandes medidas regulatórias relacionadas ao ciberespaço brasileiro é o Marco Civil da Internet (MCI), que foi instituído pela Lei nº 12.965, de 23 de abril de 2014, e que "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2014a). Essa lei tem como um de seus objetivos conseguir regular a relação conturbada entre provedores e usuários dos serviços de internet. Apesar de ter uma natureza não penal, mas administrativa, seus princípios se aplicam ao esforço de repressão dos crimes cibernéticos (BRASIL, 2015b, p.: 79). A criação do MCI passou por intenso debate parlamentar, com a participação direta da sociedade por meio de canais que a própria internet propicia, buscando um equilíbrio justo entro os interesses em disputa, que variavam desde os extremos que propunham estrito controle ou liberdade total. O MCI, então, tem o fundamento da responsabilidade civil na internet, trazendo:

> [...] garantia da liberdade de expressão, privacidade, intimidade dos usuários e inviolabilidade das comunicações; vedação de divulgação de dados pessoais; obrigatoriedade de guarda dos registros de conexão por um ano e proibição de guarda dos registros de navegação; obrigação de retirada dos conteúdos infringentes; e garantia de neutralidade. (BRASIL, 2015b, p.: 79-80)

O MCI e a cartilha de princípios para a Internet, do CGI.br, demonstram a iniciativa brasileira de estabelecer governança sobre o ciberespaço nacional. Essas iniciativas indicam que o Brasil entende a necessidade de se estabelecer regras na relação da sociedade com o ciberespaço, principalmente a Internet. O combate aos crimes cibernéticos das mais variadas ordens necessita de marcos legais para que torne possível e claro o enquadramento de certos incidentes como crimes, sendo aplicada a medida repressiva cabível. Sendo assim, a iniciativa de criação do MCI é colocada como um elemento que indica a preocupação brasileira em se preparar internamente para lidar com as ameaças cibernéticas.

Já existem diversas outras leis que discorrem sobre a segurança da informação e sobre crimes cibernéticos na legislação brasileira (BRASIL, 2015b, p.: 79-82). Entretanto, muitas dessas leis sofrem dificuldades de serem aplicadas e cumprirem os objetivos originais para os quais foram desenvolvidas. Isso porque, de um lado, o ciberespaço tem características únicas, como o forte anonimato dos autores. De outro lado, entretanto, a própria adaptação das leis ao meio cibernético não é feita corretamente, deixando vazios que corroem a credibilidade da legislação. Para exemplificar, podemos tomar o próprio MCI citado anteriormente. Segundo o MCI, apenas os administradores que possuem endereços IP diretamente alocados pela autoridade de registro da internet no Brasil, o CGI.br, possuem a necessidade de guardar registro de conexão de seus usuários. Com isso, provedores de conexão que não se encaixam nesses requisitos estão isentos da obrigação de guarda de registros de usuários. Como consequência, indivíduos podem cometer toda sorte de crimes cibernéticos quando conectados a esses provedores com a certeza da impunidade, uma vez que seus registros de conexão não serão guardados (BRASIL, 2015b, p. 154-155).

No Brasil, a Polícia Federal (PF) é a organização que trata de reprimir os crimes cibernéticos. Em 2011, foi aprovado o Regimento Interno do Departamento Federal que criou, dentre outros, a Unidade de Repressão a Crimes Cibernéticos (URCC). Mesmo que a PF tenha a competência de reprimir vários crimes cibernéticos, o URCC é o único serviço na estrutura orgânica da PF, e não consegue lidar efetivamente com todos os crimes cibernéticos (BRASIL, 2015b, p.: 81). Além disso, mesmo que a polícia federal utilize equipamentos sofisticados, o efetivo ainda é escasso em relação a esse tipo de demanda (BRASIL, 2015b, p.: 81). Quando se percebe que compete a Polícia Federal apurar alguns dos crimes mais rentáveis do mundo, como o narcotráfico, o tráfico de armas, e o tráfico de pessoas, os quais utilizam profusamente o

ambiente cibernético, nota-se que a PF ainda não tem os recursos humanos e materiais suficientemente adequados para fazer face à criminalidade virtual (BRASIL, 2015b, p.: 81-82).

No que diz respeito à defesa do ciberespaço, é o Exército Brasileiro (EB), vinculado ao Ministério da Defesa (MD), que comanda o Centro de Defesa Cibernética (CDCiber). O CDCiber foi criado em 2010 e se tornou operacional ao final de 2011, tendo como objetivo a coordenação das ações de defesa cibernética. Além disso, um de seus objetivos mais específicos é o de garantir proteção às redes militares e governamentais, de ataques tanto internos quanto externos (DINNIZ; MUGGAH; GLENNY, 2014, p.: 24-25).

A delegação da liderança das ações de defesa cibernética ao EB pode ter algumas consequências sobre a efetividade das atividades institucionais. Alguns autores afirmam que isso pode criar uma multiplicidade de lideranças dentro do Ministério da Defesa, já que o foco recai sobre o EB, quando na verdade a defesa cibernética deveria ter representações nas três Forças (CRUZ JR, 2013, p.: 27-28). Essa representação existe, com cada unidade das Forças Armadas tendo o seu próprio núcleo de defesa cibernética cuidando daquilo que lhe cabe, mas essa configuração não parece ser adequada. Isso porque a defesa cibernética se difunde em todos os sistemas das Forças Armadas, o que exige ações coordenadas e um nível decisório mais elevado dentro da estrutura institucional brasileira (CRUZ JR, 2013, p.: 28).

Em relação ao papel dos militares no ciberespaço, alguns autores afirmam que o governo brasileiro está preparando as forças armadas para assumirem posição crucial na proteção do ciberespaço brasileiro, mesmo que o seu uso primário seja civil. Por outro lado, os investimentos feitos para se aumentarem as capacidades militares cibernéticas são maiores do que o dispendido com a aplicação interna da legislação contra crimes cibernéticos (DINNIZ; MUGGAH; GLENNY, 2014, p.: 23), que como já foi apontado anteriormente é a principal ameaça cibernética ao Brasil. O fato seria o de que o Brasil, que comparativamente tem menos ameaças externas originadas de governos estrangeiros ou de grupos terroristas do que de ameaças internas (como crimes cibernéticos e protestos digitais), estaria militarizando de maneira demasiada o problema do ciberespaço, e que a resposta às ameaças não estaria adequada (DINNIZ; MUGGAH; GLENNY, 2014, p.: 29). Existe então uma necessidade para que as ameaças sejam percebidas com base em informações e evidências, a fim de melhor adequar a arquitetura institucional e o direcionamento dos investimentos que são feitos.

Existe ainda outro debate a ser mencionado e que diz respeito a atribuição de responsabilidades pela segurança cibernética e pela defesa cibernética. No Brasil, decidiu-se separar a direção das ações de segurança da informação e da defesa cibernética em dois órgãos distintos e independentes entre si, quais sejam, a Casa Militar (Ex-GSI/PR) e o CDCiber. O caso é que no ciberespaço a defesa não pode ser realizada da mesma maneira que no meio terrestre ou marítimo, por exemplo. Os ataques cibernéticos não são repelidos com a presença de tropas ou tanques, mas sim com o desenvolvimento de sistemas computacionais cada vez mais seguros, e que possam contar com equipes de resposta à resolução dos incidentes. A defesa do ciberespaço não pode ser tratada, então, como reativa, mas sim como medidas constantes e preventivas que almejem aumentar cada vez mais a segurança da informação e das infraestruturas críticas nacionais. Parece, então, que a divisão clássica entre órgãos para defesa e órgãos para segurança não se adequa muito bem ao ciberespaço.

O que pode ocorrer é que em um espaço tão difuso quanto o ciberespaço, essa configuração tenda a fragilizar o programa de proteção cibernética nacional. Isso porque essa separação favorece tanto a sobreposição de tarefas quanto lacunas por indefinição de responsabilidades. Caso ambas as organizações (Casa Militar e CDCiber) estivessem em uma mesma estrutura hierárquica, seria favoreceria uma melhor distribuição de tarefas (CRUZ JR, 2013, p.: 27). Além disso, com essa configuração os dois órgãos estariam mais isolados, e passariam a depender da afinidade, integração e colaboração dos dirigentes maiores das instituições, o que dificultaria ações conjuntas de longo prazo (CRUZ JR, 2013, p.: 34).

Portanto, em relação à institucionalização brasileira para o ciberespaço, é notável o grande número de órgãos que estão envolvidos de alguma maneira com a Segurança e a Defesa do ciberespaço. Para que haja resultados a partir dessa arquitetura complexa, os órgãos devem encontrar uma maneira de se manterem em contato próximo. Segundo Mandarino (2010):

> Uma diretriz fundamental em uma doutrina de segurança e de defesa cibernética a ser desenhada deve ser a de aglutinar os mais diferentes atores que hoje se dedicam à segurança das informações e comunicações nos mais diversos órgãos e entidades da Administração Pública Federal, de modo que atuem como uma só instituição ou, no mínimo como um só sistema. (MANDARINO, 2010, p.: 29).

Mesmo que exista essa busca pela coordenação entre os órgãos, é necessário ainda que existam dispositivos legais para que as políticas possam ser postas em prática. No que diz

respeito ao combate e à prevenção de crimes cibernéticos, a legislação ainda carece de desenvolvimento para que esteja adequada ao ciberespaço, como foi visto na análise sobre o MCI, em que foram detectadas falhas no texto legislativo, deixando brechas que fragilizam a segurança cibernética. Além disso, a PF, como força incumbida de apurar e reprimir os crimes cibernéticos, ainda não parece estar aparelhada de maneira suficiente para lidar com a situação (BRASIL, 2015b, p.: 85) Esse cenário demonstra que o direcionamento dos investimentos feitos para lidar com as ameaças do ciberespaço não estaria ocorrendo da melhor forma possível. Isso porque, como foi demonstrado anteriormente, os crimes cibernéticos são as principais ameaças no espaço cibernético brasileiro. Sendo assim, a definição de legislação apropriada para esse escopo, bem como o aparelhamento da PF, deveriam ser uma prioridade.

Se por um lado a legislação específica para lidar com os crimes cibernéticos ainda não é muito efetiva no Brasil, por outro a institucionalização com o objetivo de estabelecer governança sobre a Internet já se encontra em nível de destaque internacional. Tanto a cartilha de princípios para a Internet, do CGI.br, como o MCI, demonstra o esforço brasileiro de se estabelecer regras para a convivência da sociedade no ciberespaço. É importante notar, então, que existem esforços governamentais para que se garantam os direitos dos indivíduos no ciberespaço, o que denota certa maturidade brasileira a respeito da legislação e dispositivos legais sobre o ciberespaço.

Ademais, deve-se notar que a institucionalização brasileira demonstra atenção aos aspectos técnicos necessários para a governança na Internet. Isso se reflete quando analisamos o domínio "*.br*", coordenado pelo NIC.br, e o ICP-Brasil, administrado pelo ITI. Ambas as iniciativas apresentam funções importantes para que se mantenha a segurança da informação, a primeira pela nacionalização do registro de domínio e a segunda por assegurar a autenticidade de documentos digitais.

Além disso, é necessário ainda destacar o papel que o CERT.br e o CTIR.gov desempenham para a segurança cibernética brasileira. Visto que o crescimento da população brasileira conectada à Internet é notável, deve haver a ciência de que o crescimento do ciberespaço irá requerer maiores investimentos para se monitorar e resolver os incidentes que ocorrem nele. Com efeito, os investimentos feitos nesses órgãos também servem para que sejam identificadas as vulnerabilidades nas redes informacionais brasileiras, sejam elas governamentais ou não, o que contribui bastante para a construção de uma estratégia eficiente.

Em resumo, então, a arquitetura de segurança cibernética no Brasil apresenta evolução. Existe ainda certa superposição de responsabilidades entre os órgãos, além de prioridades de investimento não muito adequadas e legislação contra crimes cibernéticos com algumas falhas, e até mesmo a importação de soluções estrangeiras para desafios locais (DINNIZ; MUGGAH; GLENNY, 2014, p.: 29). Mas mesmo que seja possível fazer essas críticas, o caso brasileiro, pelo que foi demonstrado até aqui, parece ter desenvolvido e adequado suas instituições de maneira suficiente para que seja possível a criação e execução de políticas públicas que contribuam para a estratégia de segurança do ciberespaço. Sendo assim, o próximo capítulo trata de abordar as políticas que compõem a estratégia para a segurança do ciberespaço a partir da abordagem política da segurança bem como do aspecto militar da defesa do ciberespaço.

4. DEFENDENDO O CIBERESPAÇO: POLÍTICAS

Tendo apresentado e analisado a arquitetura institucional brasileira de atuação sobre o ciberespaço, passamos agora para a análise das políticas que são adotadas para a Segurança e Defesa Cibernética Nacional. O objetivo desse capítulo é o de entender e avaliar as principais diretrizes da estratégia brasileira de Segurança e Defesa Cibernética, com o intuito de que possamos fazer uma avaliação sobre o nível de adequação da resposta brasileira frente às ameaças que surgem a partir ciberespaço. Além disso, na seção 4.2 busca-se dar destaque a atuação militar de defesa do ciberespaço, abordando a doutrina e os conceitos sobre o emprego de ações no meio cibernético.

4.1 Abordagem política para a segurança cibernética

O Brasil, apesar de não ter um documento específico que defina sua Estratégia Nacional de Segurança Cibernética, publicou diversos documentos que versam sobre a segurança, bem como a defesa do ciberespaço. Com isso, podemos analisar as diretrizes e propostas desses documentos e extrair os principais objetivos brasileiros em sua estratégia para a segurança cibernética, além de avaliarmos a face mais empírica das políticas desenvolvidas para o setor.

Inicialmente, o setor cibernético ganhou sua primeira menção de destaque na Política Nacional de Defesa (PND) de 2005. Essa PND definiu o setor cibernético[21] como estratégico para a Defesa do país (BRASIL, 2012a, p.: 32), e afirmou que o domínio crescentemente autônomo de tecnologias sensíveis é essencial para que se garantam a autonomia e o desenvolvimento nacional (BRASIL, 2012a, p.: 19). Além disso, a PND também aborda que, para o Brasil se opor aos possíveis ataques cibernéticos, é preciso aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a "vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação ou permitam o seu pronto restabelecimento" (BRASIL, 2012a, p.: 34). Resumidamente, o ponto tônico da visão abordada na PND é o de necessidade desenvolvimento de capacidades nos setores estratégicos para garantir a soberania e o desenvolvimento nacional. A PND é importante enquanto impulsionadora da atenção brasileira

[21] Juntamente com o setor Cibernético, o setor Nuclear e o setor Espacial também foram definidos como estratégicos para a Defesa do país (BRASIL, 2005, p.: 32).

em relação ao seu espaço cibernético, já que é a primeira manifestação oficial brasileira relevante que reconhece a grande importância desse setor. Entretanto, a maioria de suas diretrizes, pelo menos no que diz respeito ao ciberespaço, é bem limitada e genérica, deixando de abordar a necessidade de organização institucional necessária para atuar nesse setor.

Dando um passo à frente, a Estratégia Nacional de Defesa (END) de 2008 aprofunda as diretrizes brasileiras em relação ao espaço cibernético. Ela estabelece que a Segurança Cibernética do Brasil deve ficar a cargo da Presidência da República, juntamente com a Casa Militar (ex-GSI/PR); e que a Defesa do Setor Cibernético deve ficar sob os cuidados do Exército Brasileiro, coordenado pelo Ministério da Defesa. No setor cibernético, como argumenta a END, o desenvolvimento de capacidades seria destinado a um amplo espectro de usos, como o industrial, o educativo, e o militar (BRASIL, 2012a, p.: 94). Em resumo, no que diz respeito ao setor cibernético, a END elenca algumas prioridades que devem ser seguidas para garantir a Segurança no ciberespaço, e dessas prioridades grande parte está relacionada com o desenvolvimento de tecnologias e de pesquisa sobre o setor cibernético.

Já com a publicação do Livro Verde de Segurança Cibernética (Livro Verde) em 2010, o debate sobre a Segurança Cibernética e as possíveis políticas para esse setor ganharam mais profundidade em sua elaboração. Com vistas a ser uma espécie de guia para a elaboração definitiva da Estratégia de Segurança Cibernética, o Livro Verde inova ao abordar mais extensamente os desafios e as oportunidades do Brasil no setor cibernético. Além disso, nota-se o esforço dedicado na tentativa de elaboração de arcabouço conceitual para ser aplicado nessa temática. Com isso em mente, a Segurança Cibernética é definida como:

> "[...] a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas. É um conceito abrangente, portanto, e maior que segurança em Tecnologia da Informação, pois envolve pessoas e processos". (BRASIL, 2010, p.: 18-19)

Ademais, o Livro Verde afirma que:

> Urge formalizar, portanto, a estrutura da Segurança Cibernética no País, bem como apoiar e fortalecer suas atividades, de forma a viabilizar e agilizar tanto a formulação de políticas, normas e regulação, a pesquisa e o desenvolvimento de metodologias e tecnologias, quanto à cooperação internacional e a implantação e promoção de uma macrocoordenação que propicie a integração de processos, visando assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações de

> interesse do Estado brasileiro e da sociedade, bem como a resiliência de suas infraestruturas críticas. (BRASIL, 2010, p.: 25)

Uma das contribuições importantes do Livro Verde para o desenvolvimento da Segurança Cibernética brasileira parece ser a constatação da carência de arcabouço conceitual nas instituições designadas como responsáveis pelo setor cibernético (BRASIL, 2010, p.: 34). Efetivamente, o Livro Verde propõe que uma das principais diretrizes que deve compor a Estratégia de Segurança Cibernética seja o desenvolvimento de arcabouço conceitual para o setor (BRASIL, 2010, p.: 43). Nesse sentido, pode-se dizer que um dos principais objetivos da Estratégia Brasileira de Segurança Cibernética é o de criar uma arquitetura institucional que disponha dos marcos legais necessários e das atribuições claras de responsabilidade para tornar efetiva a atuação nesse setor. Desse modo, o Brasil tem dedicado grandes esforços, assim como foi visto no 3º capítulo deste trabalho, para que os atores envolvidos em Segurança Cibernética possam atuar de maneira cooperativa, e que seja diminuída a superposição de responsabilidades.

Mais uma das contribuições do Livro Verde para a Segurança Cibernética Brasileira é a sua abordagem, mesmo que marginal, sobre o problema dos crimes cibernéticos (BRASIL, 2010, p.: 23). Isso porque no Brasil, como já foi demonstrado anteriormente no capítulo 2, os crimes cibernéticos se constituem como uma das principais ameaças cibernéticas ao Estado. Entretanto, a resposta brasileira contempla também a preparação das forças militares para o emprego no caso de Guerra Cibernética, além de se focar na construção atual de capacidades defensivas que se refletem no aparelhamento do CDCiber. Mesmo que essa preparação seja necessária, deveria ser feito um balanço melhor sobre a resposta perante as ameaças do Ciberespaço, para evidenciar que a prevenção e repressão dos crimes cibernéticos merece receber parte adequada do orçamento para o setor cibernético, assim como a defesa já bem recebendo.

Nesse sentido, a Polícia Federal cumpre o importante papel de ator principal na repressão de crimes cibernéticos. Tendo essa missão, a PF necessita dos recursos tanto humanos quanto de infraestrutura para tornar efetivo o seu papel. É nesse ponto em que cabe a crítica principal que se faz nesse trabalho. Em termos de custo-benefício, a aquisição por parte das Forças Armadas de capacidades cibernéticas ofensivas para a possibilidade de Guerra Cibernética não deve ser desmedida, a ponto de não contemplar a análise baseada em evidências, que demonstra que os crimes cibernéticos, como por exemplo as fraudes bancárias, são extremamente comuns no Brasil e já causam prejuízos significativos (BRASIL, 2015b, p.: 10). Segundo Diniz, Muggah e Glenny:

> A polícia exibe fracas capacidades forenses e de investigação. Os problemas vão desde a falta de infraestrutura técnica e de recursos financeiros até pessoal mal preparado, cooperação limitada entre as agências de *law enforcement* e o silêncio das firmas privadas em divulgar a extensão do crime cibernético. Desafios se mantém, notavelmente a carência de padronização nos processos forenses e de coleta de evidências, bem como uma capacidade limitada para reunir ciber inteligência. Finalmente, existem questões abertas sobre como lidar com o crime cibernético em uma estrutura federal complexa em que permanece confusa a definição de responsabilidades em liderar investigações ou gerenciar os julgamentos. (DINIZ; MUGGAH; GLENNY, 2014, p.: 23, tradução livre)[22]

Conforme esses argumentos, não é somente a falta de investimentos em estrutura e recursos humanos que prejudica o trabalho da PF. A carência de padrões que possam ser utilizados para agregar evidências necessárias para o enquadramento dos perpetradores dos crimes nos dispositivos legais disponíveis também é um dos fatores que atrapalha a PF no desempenho de suas funções. O que importa entender é que parece difícil conceber uma estratégia de Segurança e Defesa Cibernética brasileira sem que se tenha uma força policial adequadamente preparada para lidar com as principais ameaças cibernéticas no Brasil.

Por outro lado, o Livro Verde destaca a inexistência de satélite geoestacionário nacional como um desafio e vulnerabilidade para a Segurança e a Defesa Cibernética do Brasil (BRASIL, 2010, p.: 38). O destaque a esse ponto é válido, pois atualmente, como demonstrado no 2º capitulo, o Satélite Geoestacionário de Defesa e Comunicações Estratégicas passa por testes para simular as condições encontradas no espaço, além de estar sendo preparado lançamento para o segundo semestre de 2016 (AEB, 2016). Esse projeto é uma parceria entre os Ministérios da Defesa, das Comunicações e da Ciência, Tecnologia e Inovação, com um investimento da ordem de R$ 1,7 bilhão (AEB, 2016). Esse projeto é um bom exemplo de investimento em infraestrutura que auxilia na garantia da Segurança e Defesa do espaço cibernético, isso porque o satélite, além de proporcionar acesso à internet para pessoas que residem em lugares mais isolados, serve como centralizador das comunicações das Forças Armadas em suas operações.

---

[22] The police exhibit weak investigative and forensic capability. Problems range from the lack of technical infrastructure and financial resources to poorly trained personnel, limited cooperation between law enforcement agencies and continued reticence of private firms to disclose the extent of cyber-crime. Challenges remain, notably the lack of standardization in evidence gathering and forensic procedures, as well as a limited capability to gather cyber-intelligence. Finally, there are open questions about how to manage cyber-crime in a complex federal structure in which it is remains unclear who is responsible for leading investigations or managing trials. (DINIZ; MUGGAH; GLENNY, 2014, p.: 23)

A oficialização do texto do Livro Branco de Defesa Nacional ocorreu em 2013, e o texto traz alguns apontamentos sobre o ciberespaço e a sua relação com a soberania nacional. Nesse sentido, o Livro Branco afirma que "a ameaça cibernética tornou-se uma preocupação por colocar em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional" (BRASIL, 2013, p.: 69). O que se percebe a partir da maneira como é abordado o setor cibernético no Livro Branco, é que o entendimento das principais ameaças cibernéticas ao Estado não evoluiu no período de três anos entre a publicação do Livro Verde e a oficialização do Livro Branco de Defesa Nacional. A atenção continua recaindo mais sobre a pequena possibilidade de Guerra Cibernética, que é corretamente devida, mas sem atentar para a necessidade de prevenção e repressão dos crimes cibernéticos.

O documento mais atual, e que entrega mais densidade em relação à elaboração das diretrizes e das políticas a serem adotadas é a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018", publicada em 2015. Do seu texto, extraímos sua finalidade:

> [...] apresentar as diretrizes estratégicas para o planejamento de segurança da informação e comunicações e de segurança cibernética no âmbito da APF, objetivando a articulação e a coordenação de esforços dos diversos atores envolvidos, de forma a atingir o aprimoramento da área no Governo e a mitigação dos riscos aos quais se encontram expostas as organizações e a sociedade. (BRASIL, 2015a, p.: 34)

Dos problemas abordados por esse documento, a questão sobre o orçamento específico para a Segurança Cibernética é um deles. Tanto que o primeiro objetivo estratégico descrito nesse documento diz respeito à institucionalização do tema de Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética no planejamento e orçamento federal (BRASIL, 2015a, p.: 43). Segundo essa Estratégia:

> A institucionalização desses temas nos instrumentos de planejamento e orçamento do Governo é fundamental para que tais áreas avancem e sejam vistas no nível estratégico requerido, conquistando destaque no planejamento, bem como aportes contínuos e adequados de recursos do orçamento federal. (BRASIL, 2015a, p.: 43)

O principal destino desses recursos é tratado no segundo objetivo estratégico, que diz respeito a capacitação de recursos humanos para atuação nesse setor. O método proposto é o de estímulo de parcerias com Escolas de Governo, bem como com outras instituições, como

universidades e empresas, no sentido de desenvolver programas de ensino, em todos os níveis, voltados para a formação de recursos humanos capazes de atuarem nas áreas de SIC e de Segurança Cibernética (BRASIL, 2015a, p.: 44). Segundo a Estratégia:

> Tais ações visam atender as demandas de sensibilização, conscientização, capacitação e especialização, de modo a fomentar o aperfeiçoamento contínuo e a permanência de tais profissionais, e contribuir com a robustez da Governança Sistêmica de SIC e de SegCiber da APF. (BRASIL, 2015a, p.: 44)

Em relação a essa capacitação de recursos humanos, o Curso de Especialização em Gestão de SIC (CEGSIC) se coloca como uma das muitas ferramentas que podem ser utilizadas tanto para o treinamento e ensino como também para fortalecer a cultura de segurança cibernética na APF. O objetivo geral do CEGSIC é o de fomentar a pesquisa, o desenvolvimento, e a inovação para a construção de uma estratégia e metodologia brasileira de gestão de segurança da informação e comunicações na APF. Especificamente, o CEGSIC busca i) dotar os agentes públicos de conhecimentos teóricos e práticos acerca da gestão da segurança da informação e comunicações, ii) fomentar a realização de pesquisas aplicadas e iii) fomentar a disseminação de conhecimento sobre Segurança da Informação e Comunicações (SIC) (DSIC, 2015). Em 2015, foi realizada a cerimônia de formatura da 4ª turma do CEGSIC, em que os 114 concluintes receberam a declaração de Especialista em Gestão da Segurança da Informação e Comunicações (DSIC, 2015). Vale ressaltar, ainda, que os concluintes eram oriundos de 38 órgãos e entidades diferentes da APF, e que ao total, as quatro edições do CEGSIC formaram mais de 300 pessoas. Esse tipo de iniciativa de parcerias entre os órgãos responsáveis pela Segurança Cibernética e as instituições de ensino deve ser continuamente fomentado, já que o Brasil necessita de pessoal qualificado para poder gerenciar os seus projetos para o setor. O número pequeno de servidores formados por essa iniciativa, que surgiu em meados de 2007, elucida a necessidade de se debater melhor sobre a alocação dos recursos para a Segurança e Defesa do ciberespaço, já que evidentemente a capacitação de recursos humanos não tem recebido a atenção orçamentária necessária.

Já o terceiro objetivo estratégico discorre sobre a necessidade contínua de pesquisa, desenvolvimento, e Segurança Cibernética na APF. Nesse sentido, a pesquisa e o desenvolvimento de soluções para a APF baseadas em *hardware* e algoritmos criptográficos próprios de Estado buscam garantir a confidencialidade, integridade e a autenticidade das

comunicações estratégicas entre órgãos que integrem a APF (BRASIL, 2015a, p.: 45). A ABIN possui em sua estrutura o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC), que foi criado em 1982 com o objetivo de sanar a deficiência do Brasil em garantir o sigilo dos canais de comunicação na APF (BRASIL, 2015a, p.: 19). O CEPESC é quem desenvolve a criptografia que é utilizada atualmente nas comunicações governamentais. Como exemplo, temos aplicativo de mensagens instantâneas para smartphones utilizado pela inteligência brasileira, chamado "Athena", que foi desenvolvido para agilizar as comunicações da ABIN de maneira confiável e segura. Além disso, o CEPESC também é responsável pela criptografia implementada nas urnas eletrônicas utilizadas nas eleições brasileiras (ABIN, 2016).

Em suma, o que se percebe das políticas brasileiras para a Segurança Cibernética é que parece ainda faltar coordenação entre os diversos órgãos e entidades que estão envolvidos com esse assunto. Essa dificuldade de coordenação pode ser um dos motivos pelos quais as iniciativas de políticas públicas para o Ciberespaço parecem ainda serem muito pontuais, além de sofrerem bastante com a falta de recursos para a execução das políticas. Ainda assim, é evidente que existe um esforço governamental para organizar e definir as responsabilidades de cada ator, bem como diretrizes a serem seguidas, identificando os passos a serem dados para que se fortaleça a Segurança Cibernética brasileira.

4.2 Abordagem militar de defesa do ciberespaço.

No Brasil, foi garantido ao setor militar papel de destaque na proteção do ciberespaço, adquirindo consequentemente diversas responsabilidades diferentes em relação à operacionalização da Defesa. Nessa seção serão analisados os conteúdos e as políticas propostas pelos documentos nacionais mais importantes sobre o assunto, e que dizem respeito sobre a organização e atuação militar para a Defesa do Ciberespaço. Apesar de o Livro Branco abordar o tema da defesa do espaço cibernético nacional, considera-se que os principais documentos que estão relacionados com a abordagem militar de defesa do ciberespaço são: a Política Cibernética de Defesa (2012) e a Doutrina Militar de Defesa Cibernética (2014).

A Política Cibernética de Defesa, publicada em 2012, tem como finalidade última "orientar, no âmbito do Ministério da Defesa, as atividades de Defesa Cibernética, no nível

estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando a consecução dos seus objetivos" (BRASIL, 2012b, p.: 11). As diretrizes propostas nesse documento possuem um caráter de generalidade, e abordam de maneira um tanto superficial os problemas da Defesa Cibernética, quando comparado com a Doutrina Militar de Defesa Cibernética (2014). Mesmo assim, existem elementos nesse documento que devem ser analisados e que dizem respeito a construção brasileira de Defesa do ciberespaço.

A elaboração dessa política se baseou na definição de alguns objetivos para a Defesa Cibernética, dos quais parece importante de se destacar a capacitação e o gerenciamento de talentos humanos necessários à condução das atividades do Setor Cibernético no âmbito do MD (BRASIL, 2012b, p.: 13). Em relação a essa questão, a Política afirma a necessidade de criação de cargos e funções específicas, juntamente com o preenchimento das posições com pessoal especializado para atender às necessidades do Setor Cibernético (BRASIL, 2012b, p.: 15). É para o cumprimento desse objetivo que existe no Brasil atualmente o Instituto de Defesa Cibernética (IDCiber), e que se planeja a criação da Escola Nacional de Defesa Cibernética (ENaDCiber).

Antes do IDCiber, a capacitação operacional era realizada pelo Centro de Comunicações e Guerra Eletrônica do Exército, que adequava os cursos já existentes nas forças armadas às necessidades do Setor Cibernético no âmbito da Defesa (IDCiber, 2015). Com sua evolução, o IDCiber se tornou um Portal de Ensino, nos níveis técnico e de pós-graduação que também coordena cursos na área de Defesa Cibernética, contando com parcerias de instituições de ensino do setor acadêmico nacional e do exterior (IDCiber, 2015).

Em relação à ENaDCiber, o Programa Estratégico de Defesa Cibernética na Defesa Nacional[23], conduzido no âmbito do Ministério da Defesa (MD), prevê a criação dessa instituição, que será considerada como centro polarizador de ensino e pesquisa da Defesa Cibernética Nacional. Segundo as palavras de Carneiro (2016), essa estrutura de ensino apresentará um caráter dual, por envolver tanto o setor militar quanto o civil, e possibilitará avanços significativos na sensibilização, conscientização, formação e especialização de pessoas capazes de atuar no setor cibernético (CARNEIRO, 2016, p.: 27).

[23] Segundo Carneiro (2016), "O Programa Estratégico Defesa Cibernética na Defesa Nacional, conduzido no âmbito do Ministério da Defesa (MD), tem a finalidade de incrementar as atividades relativas ao Setor Cibernético para assegurar, de forma conjunta, o uso efetivo do espaço cibernético (preparo e emprego operacional) pelo MD e pelas Forças Armadas (FA) e a impedir ou dificultar sua utilização contra interesses da Defesa Nacional. Esses procedimentos incluem ações nas áreas de capacitação, doutrina, ciência, tecnologia e inovação, inteligência e operações, no domínio da Defesa Nacional". (CARNEIRO, 2016, p.: 24-25)

Além da criação do ENaDCiber, o Programa também prevê alguns outros projetos que ainda estão em via de serem implementados. Um deles é o projeto de Implantação e Consolidação de Sistemas de Informações Seguras, que visa à busca por inovações na área de Segurança da Informação e Comunicações, em especial a Criptografia, por intermédio de uma rede de laboratórios virtuais em instituições de pesquisas públicas e privadas nacionais (BRASIL, 2014b). O objetivo que se tem é elevar a competência brasileira nesta área, reduzindo-se o gap em relação aos países mais desenvolvidos (CARNEIRO, 2016, p.: 29). O principal exemplo relacionado a esse projeto é a Rede Nacional em Segurança da Informação e Criptografia (RENASIC), que funciona sob a égide do CDCiber. Dos objetivos específicos do RENASIC, está o fortalecimento e a integração das pesquisa em Segurança da Informação e Criptografia na Brasil, buscando a diminuição da fragmentação das competências através da criação de uma infraestrutura de pesquisa e de organização em laboratórios virtuais, estabelecendo uma agenda de pesquisa e de projetos conjuntos nessas áreas[24] (RENASIC, 2016).

Em relação à necessidade apontada pela Política Cibernética de Defesa de organização, estruturação e cooperação entre os atores envolvidos na Defesa Cibernética, o Estado-Maior do Exército emitiu a Portaria nº61, em 3 de março de 2016, cujo texto aprova a Implantação do Comando de Defesa Cibernética (ComDCiber) (CARNEIRO, 2016, p.: 22). No nível estratégico, o ComDCiber é a organização que tem como responsabilidade coordenar e integrar as ações de Defesa Cibernética no âmbito do Ministério da Defesa (CARNEIRO, 2016, p.: 36). Segundo o Plano de Articulação e Equipamento da Defesa (PAED):

> O Comando conta com servidores militares e civis altamente especializados, com seu valor estratégico amparado no aumento da capacidade nacional de combate às ameaças cibernéticas contra os interesses nacionais. Ao dotar o MD e as Forças Armadas dos meios necessários para exercer a defesa e o controle contínuo do espaço cibernético de interesse para a Defesa Nacional, garantirá fluxo ágil e seguro de informações confiáveis e oportunas, impactando positivamente nas áreas científico-tecnológica e operacional da Defesa Nacional, da indústria nacional e do País. Entre os benefícios sociais mais diretos, destacam-se o incremento da segurança e da proteção das infraestruturas estratégicas dependentes do ambiente cibernético e a integração entre as ações do MD, das Forças Armadas e de todas as outras agências envolvidas nessas atividades. (BRASIL, 2014b apud CARNEIRO, 2016, p.: 25)

[24] Atualmente o RENASIC conta com 8 projetos diferentes, e que englobam instituições de ensino como a Universidade de Brasília e o Instituto Tecnológico de Aeronáutica, por exemplo. Além da atuação na pesquisa e desenvolvimento de tecnologias, o RENASIC também promove diversos seminários que abordam temáticas variadas da Segurança Cibernética, o que contribui para o desenvolvimento de uma cultura de segurança cibernética no Brasil, o que foi destacado como essencial por Mandarino (2010) para o desenvolvimento do setor cibernético no Brasil.

Passamos agora a enfocar a Doutrina Militar de Defesa Cibernética, publicada em 2014, e que define as diretrizes principais para a preparação e atuação das Forças Armadas no meio cibernético, principalmente no que diz respeito à guerra cibernética[25]. Segundo a Doutrina, sua finalidade é a de proporcionar unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), e contribuir para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético (BRASIL, 2014c, p.: 13). De início, já se percebe que o Brasil considera veemente a possibilidade de agressões a partir do espaço cibernético, sejam elas estatais ou não estatais, através da guerra cibernética[26]. É importante destacar essa questão inicialmente, pois ela constitui a tônica da crítica que se faz aqui em relação a doutrina militar brasileira de atuação em guerra cibernética. A abordagem militar para a defesa e operação no ciberespaço, se focada para a construção de capacidades ofensivas, juntamente com a consideração de que são possíveis ataques através do ciberespaço que causem danos estruturais e que possam ser letais, não parece ser adequada para o Brasil. Já que as principais ameaças ao ciberespaço brasileiro parecem se dar na forma de espionagem e de crimes cibernéticos, é possível contestar a adequação da doutrina brasileira. Ademais, deve-se levar em conta que existe diferença em se pensar a Defesa no espaço cibernético em relação aos domínios clássicos.

O conceito de Defesa Cibernética é abordado pela Doutrina como sendo:

> Conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (BRASIL, 2014c, p.: 18)

[25] Segundo a Doutrina, Guerra Cibernética corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC (BRASIL, 2014c, p.: 19).

[26] Segundo a Doutrina Militar de Defesa Cibernética, a Guerra Cibernética ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2014c, p.: 19)

Efetivamente, a Doutrina brasileira define que a Defesa do espaço cibernético deve ser constituída e operacionalizada por um planejamento integrado entre as Forças Armadas e os demais órgãos que desempenham funções importantes para o esforço de Defesa. Além disso, um dos objetivos principais da Política Cibernética de Defesa (2012) é o de "assegurar, de forma conjunta, o uso do espaço cibernético (preparo e emprego operacional) pelas Forças Armadas e impedir ou dificultar sua utilização contra interesses da Defesa Nacional" (BRASIL, 2012, p.: 15). Com vistas a cumprir com essa diretriz, está sendo instituído o Sistema Militar de Defesa Cibernética (SMDC), que diz respeito ao conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviço e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, com o objetivo de assegurar o seu uso efetivo pelas Forças Armadas, além de impedir ou dificultar essa utilização contra os interesses da Defesa Nacional (BRASIL, 2014c, p.: 25). O SMDC é composto por atores governamentais em diversos níveis, abrangendo desde o nível político em que atua a Presidência da República e a Casa Militar até o nível tático em que atuariam os componentes das Forças Armadas. Sendo assim, a sua concepção geral conta com a participação do setor civil dentro do projeto de Defesa do ciberespaço (BRASIL, 2014c, p.: 26).

Naturalmente, as Forças Armadas são responsáveis pela Defesa Nacional de um país. No meio cibernético isso ainda se mantém, já que, existindo a possibilidade de amaças advindas do ciberespaço à soberania nacional, as FA devem intervir através das ações defensivas para restabelecer a Segurança. A questão é que para o Ciberespaço a Defesa não pode ser pensada da mesma maneira do que para os domínios clássicos (terrestre, marítimo, aéreo). No ciberespaço, diferentemente do domínio terrestre, por exemplo, não se pode existir uma área de contestação entre dois atores adversários (LIBICKI, 2012). As características do Ciberespaço tornam a sua defesa uma tarefa que envolve esforços por parte de todos os setores da sociedade, isso porque todos estão diretamente envolvidos, já que os alvos são as infraestruturas críticas e as mais variadas redes e TIC. Com isso, defender esse espaço requer uma abordagem que entenda que mais do que criar capacidades para se atuar no Ciberespaço, a Defesa dele passa por uma estreita coordenação com os esforços de segurança da informação e dos sistemas a nível nacional, tanto na esfera pública quanto à privada. Essa relação mais estreita da Defesa com o setor público é certamente um dos grandes desafios para a implementação e pleno funcionamento do SMDC. Para finalizar esse argumento sobre o caráter distinto da Defesa no Ciberespaço, podemos tomar as palavras de Libicki (2012), que nos apresenta mais um elemento que elucida essa diferença:

> Uma característica chave de operações ofensivas no ciberespaço é que a maioria delas é difícil de ser repetida; uma vez que o alvo entenda o que aconteceu com os seus sistemas no despertar de um ataque, o alvo pode frequentemente entender como o sistema foi penetrado e fechar os buracos que permitiram o ataque. Mesmo que não possa achar o buraco, o alvo aprende em que parte seu sistema é vulnerável e pode repensar a acessibilidade ou confiabilidade de seu sistema. A forte probabilidade de que alvos de guerra cibernética farão tais ajustes sugere que operações cibernéticas ofensivas podem se tornar previamente planejadas durante o curso de uma campanha. O uso de operações ofensivas contra um alvo ingênuo é provável de ser consideravelmente mais efetivo do que contra o alvo mais difícil que foi definido diversas semanas antes. Isso não é tão característico de outros domínios de guerra que retêm sua importância durante a campanha. (LIBICKI, 2012, p.: 331, tradução livre)[27]

No que diz respeito ao emprego da Defesa Cibernética, a Doutrina destaca quatro princípios relevantes. O Princípio do Efeito, em que ações no Espaço Cibernético devem produzir efeitos que se traduzam em vantagem estratégica, operacional ou tática que afetem o mundo real, mesmo que esses efeitos não sejam cinéticos. O Princípio da Dissimulação, em que medidas ativas devem ser adotadas para se dissimular no Espaço Cibernético, dificultando a rastreabilidade das ações cibernéticas ofensivas e exploratórias levadas a efeito contra os sistemas de tecnologia da informação e de comunicação do oponente. O objetivo que se tem é mascarar a autoria e o ponto de origem das ações. Princípio da Rastreabilidade, em que medidas efetivas devem ser adotadas para se detectar ações cibernéticas ofensivas e exploratórias contra os sistemas de tecnologia da informação e de comunicações amigos. Por último, o Princípio da Adaptabilidade, que consiste na capacidade da Defesa Cibernética de adaptar-se à característica de mutabilidade do Espaço Cibernética, mantendo a proatividade mesmo diante de mudanças súbitas e imprevisíveis (BRASIL, 2014c, p.: 20). No geral, esses princípios somente refletem as características do ciberespaço, ainda mais no que está relacionado à dissimulação e à rastreabilidade, que se relacionam com o alto de grau de anonimato das atividades cibernéticas e que dificultam o enquadramento do autor do ataque. Entretanto, o Princípio do Efeito pode ser destacado, já que a partir dele é possível fazer uma crítica à maneira como os ataques cibernéticos são entendidos pela maioria das autoridades militares no Brasil.

[27] A key characteristic of offensive cyberspace operations is that most of them are hard to repeat; once the target understands what has happened to its system in the wake of an attack, the target can often understand how its system was penetrated and close the hole that let the attack happen. Even if it cannot find the hole, the target learns where its system is vulnerable and may rethink the accessibility or trustworthiness of its system. The strong likelihood that targets of cyberwar will make such adjustments suggests that offensive cyber operations may be front-loaded over the course of a campaign. The use of offensive operations against a naïve target set is likely to be considerably more effective than against the harder target set several weeks later. This is not so characteristic of other warfighting domains which retain their importance throughout a campaign. (LIBICKI, 2012, p.: 331)

A Doutrina para o Ciberespaço está alinhada com a ideia de que a guerra cibernética é real e possível, e que danos sérios às infraestruturas críticas podem ser perpetrados por esse meio, por um custo relativamente menor do que operações militares clássicas (BRASIL, 2014c, p.: 22). Sendo assim, o que se pode argumentar, e que está relacionado com o Princípio do Efeito - em que devem ser produzidos efeitos que se traduzam em vantagens -, é que as ações ofensivas no meio cibernético sofrem de certo elemento, que é a incerteza. Esse próprio aspecto está abordado na Doutrina, quando ela diz que as ações no Espaço Cibernético podem não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados (BRASIL, 2014c, p.: 21). Nessa mesma linha de pensamento, Cavelty (2012) argumenta que:

> [...] Ataques computacionais poderiam ter efeitos colaterais através das interdependências que são uma característica essencial desse ambiente. Mesmo vírus e *worms* relativamente inofensivos causariam disrupção aleatória considerável para negócios, governos, e consumidores. Esse risco provavelmente pesaria muito mais do que os benefícios incertos a serem ganhos de atividades de guerra cibernética. (CAVELTY, 2012, p.: 118, tradução livre)[28]

A visão da Doutrina de que as Forças Armadas necessitam imprescindivelmente de capacidades cibernéticas ofensivas para poder responder às diversas agressões (BRASIL, 2014c) parece, então, ser um pouco desmedida. Isso porque mesmo com os casos da Estônia, da Geórgia, e do *worm Stuxnet*, a efetividade real e a viabilidade, do ponto de vista orçamentário, de um ataque cibernético ainda se situam como alvo de intensos debates, e não pode ser afirmada com certeza. Sobre o ponto de vista dos recursos necessários para um ataque, é importante mencionar algumas nuances que vão de encontro com essa ideia. Existem diversos sistemas diferentes que controlam as mais variadas tarefas, e esses sistemas são projetados para cumprirem funções específicas. Sendo assim, o desenvolvimento de uma ferramenta cibernética que vise causar danos s sistemas industriais, por exemplo, necessita de grande conhecimento interno sobre o sistema, além de recursos humanos de alto nível técnico. Sintetizando esses argumentos, Cavelty (2012) afirma que:

[28] [..] Computer attacks could 'blow back' through the interdependencies that are such an essential feature of the environment. Even relatively harmless viruses and worms would cause considerable random disruption to businesses, governments, and consumers. This risk would most likely weigh much heavier than the uncertain benefits to be gained from cyber war activities. (CAVELTY, 2012, p.: 118)

> De fato, é difícil entender como ataques cibernéticos poderiam algum dia se tornar realmente efetivos para propósitos militares: é excepcionalmente difícil derrubar diversos alvos específicos e mantê-los inoperantes por determinado tempo. A dificuldade chave é o reconhecimento e o enquadramento adequado dos alvos, bem como a necessidade de lidar com uma variedade de sistemas diversos e estar preparado para medidas de contra-ataque de seu adversário. (CAVELTY, 2012, p.: 117, tradução livre)[29]

Existe ainda outra questão importante que deve ser levantada quando abordamos os ataques cibernéticos e a sua utilização efetiva. Dado a permeabilidade do ciberespaço entre todos os setores da sociedade, e a multiplicidade de atores envolvidos, é difícil de decidir quando um incidente cibernético se caracteriza como assunto civil ou militar, o que consequentemente se torna uma tarefa complicada no momento de se atribuir a responsabilidade e enquadrar a resposta necessária por parte dos setores de *law-enforcemnt* (PF), inteligência (ABIN) e organizações militares (CDCiber). Além disso, um contra-ataque cibernético, assim como é abordado na Doutrina, não parece ser algo factível atualmente, pelo menos quando se percebe que as características do ciberespaço, de alto grau de anonimato, fazem com que uma resposta militar a incidentes cibernéticos sofra de alguns obstáculos, que corroem a legitimidade da resposta:

> Incidentes em que as forças armadas são o alvo parecem ser intuitivamente uma responsabilidade militar, mas seria um contra-ataque militar adequado, a quem isso seria direcionado, e que nível ou tipo de resposta seria proporcional? Se existem respostas militares no ciberespaço, direcionadas contra alvos no ciberespaço percebidos como "militar", seria possível (dada a natureza interconectada do ciberespaço) para qualquer resposta evitar danos colaterais, e seria essa resposta considerada legítima no direito nacional e internacional, já que ela não pode definir seus alvos com precisão? Há outra complicação e risco em que os Estados podem perceber um ataque cibernético com consequências sérias intencionais ou não intencionais como sendo merecedor de uma resposta cinética, particularmente enquanto os Estados diferem em suas interpretações sobre o que é vital para a segurança nacional. (IISS, 2011, p.: 28, tradução livre)[30]

---

[29] Indeed, it is hard to see how cyber attacks could ever become truly effective for military purposes: It is exceptionally difficult to take down multiple, specific targets and keep them down over time. The key difficulty is proper reconnaissance and targeting, as well as the need to deal with a variety of diverse systems and be ready for countermoves from your adversary. (CAVELTY, 2012, p.: 117)

[30] Incidents where armed forces are targeted seem intuitively to be a military responsibility, but would a military counter-attack be merited, at whom would this be directed, and what level or type of response would be proportionate? If there are military responses in cyberspace, directed against targets in cyberspace assessed as 'military', would it be possible (given the interconnected nature of cyberspace) for any response to avoid collateral damage, and would a response that cannot be precisely targeted be legitimate in national and international law? There is a further complication and risk in that states may perceive an attack directed through cyberspace with very serious intended or unintended consequences as meriting a kinetic response, particularly as states maintain differring interpretations of what is vital to national security". (IISS, 2011, p.: 28)

Mesmo que se possa debater e contestar a efetividade militar de um ataque cibernético, isso não significa que o setor cibernético não seja importante para as Forças Armadas. Nesse sentido, a Doutrina assinala que existe uma característica de função assessora por parte das ações de Defesa Cibernética, em que elas não seriam, então, um fim em si mesmas, mas empregadas, geralmente, para apoiar a condução de outros tipos de operação (BRASIL, 2014c, p.: 21). Consequentemente, as ações no ciberespaço que poderiam ser consideradas como ataques a um adversário seriam acompanhadas, então, de ações militares clássicas nos outros domínios. Entretanto, como afirmado anteriormente, o Brasil não se envolve em conflitos há bastante tempo; então, ter uma doutrina que a afirma a necessidade de capacidades cibernéticas ofensivas para operar juntamente com ações militares clássicas não parece ser, novamente, o enquadramento mais adequado a ser feito na Doutrina.

Já tendo debatido sobre a concepção dos ataques cibernéticos[31], é importante destacar que a Doutrina também nos traz a caracterização de outros dois tipos de ações cibernéticas, quais sejam, a Proteção Cibernética e a Exploração Cibernética. A primeira diz respeito a uma atividade de caráter permanente, em que se prezam as ações para neutralizar ataques e exploração cibernética contra os dispositivos computacionais e redes de computadores e de comunicações nacionais, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito (BRASIL, 2014c, p.: 23). A segunda se refere à ação de busca ou coleta nos Sistemas de tecnologia da Informação de interesse, objetivando obter a consciência situacional do ambiente cibernético. Ao mesmo tempo, essas ações devem servir para a produção de conhecimento ou identificar as vulnerabilidades desses sistemas (BRASIL, 2014c, p.: 24).

Dado o papel importante desempenhado pelo CDCiber na Defesa Cibernética brasileira, é interessante dedicar algumas palavras em relação aos efeitos da implementação e operacionalização desse centro para a Defesa Cibernética como um todo. O CDCiber teve o "mérito de conferir objetividade para a questão de riscos cibernéticos em nível de segurança nacional e, mais que isto, efetivou uma articulação de esforços envolvendo a esfera militar com a sociedade" (FRAGOLA, 2016). Possivelmente o principal efeito que o CDCiber teve foi o de ter conseguido introduzir uma rubrica orçamentária específica para a Defesa Cibernética no país, a exemplo do que já é feito em diversos outros países, como os EUA (FRAGOLA, 2016). Quando

[31] Segundo a Doutrina, um ataque cibernético "compreende ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente". (BRASIL, 2014c, p.: 23).

foi lançado, o CDCiber conquistou a liberação de R$ 400 milhões para o período de quatro anos, que se iniciou em 2012 quando o centro foi efetivamente inaugurado. Até o fim de 2015, o CDCiber executou gastos de R$ 190 milhões, abrangendo desde a sua própria organização até as atividades operacionais realizadas durante os grandes eventos (FRAGOLA, 2016). Além disso, é válido também apontar a atuação do CDCiber nos grandes eventos que tiveram lugar no Brasil nos últimos anos, com o intuito de defender o espaço cibernético nesse momento em que aumentam o fluxo de informações e a frequência dos ataques. O CDCiber operacionalizou a Defesa Cibernética na Conferência Rio +20, na Copa do Mundo de 2014, e mais recentemente nas Olimpíadas de 2016, em que atuou em conjunto com a URRC da Polícia Federal.

Portanto, a partir do que foi exposto nesse capítulo, é possível perceber elementos que demonstram o empenho brasileiro de se organizar e se preparar em relação ao ciberespaço. Em termos de Segurança Cibernética, percebe-se que o Brasil busca adequar sua arquitetura institucional para que disponha de órgãos com responsabilidades bem definidas no setor cibernético, sem esquecer que a cooperação e a atuação coordenadas são essenciais para o êxito no setor cibernético. Além disso, o entendimento sobre a importância da capacitação de recursos humanos especializados no assunto é evidente na Estratégia brasileira, materializando-se nas iniciativas do CEGSIC, no que diz respeito à Segurança Cibernética, e no IDCiber e a ENaDCiber, relacionadas com a Defesa Cibernética. Ademais, é difícil encontrar evidências que apontem no sentido de que o estímulo de parcerias entre o setor público e o privado está sendo feito de forma correta. O que parece dificultar realmente o avanço nesse tema é a questão do orçamento específico para a segurança cibernética. Sem os recursos necessários, dificilmente será possível formar profissionais especializados em Segurança Cibernética para atuarem junto ao governo na operacionalização das políticas para esse setor.

Outra questão muito importante que também está relacionada com a falta de recursos e orçamento específico é o caso da Polícia Federal. Sendo os crimes cibernéticos uma das maiores ameaças cibernéticas ao Brasil, e sendo da competência da PF o dever de reprimi-los, parece natural que boa parte dos recursos destinados ao setor cibernético dentro do orçamento federal deveriam ser aplicados com o objetivo de aparelhar a URRC da PF não somente com equipamentos, mas também com os agentes devidamente treinados e especializados no assunto. Ocorre, entretanto, que a maioria dos investimentos realizados está direcionado para as Forças Armadas e a sua atuação na Defesa Cibernética.

Com relação a isso, a Doutrina Militar de Guerra Cibernética e a Política Cibernética de Defesa afirmam que existe a necessidade de desenvolvimento de capacidades cibernéticas que tornem possível às Forças Armadas realizarem ataques cibernéticos, na medida em que esse recurso pareça ser necessário. Entretanto, a plausibilidade real de utilização de ataques cibernéticos como resposta à uma agressão esbarra no alto grau de volatilidade que esse tipo de ação tem, e que consequentemente corrói a legitimação do uso dessa ferramenta (CAVELTY, 2012). Nesse sentido, conforme as palavras de Cavelty (2012):

> […] guerra cibernética não deveria receber muita atenção em detrimento de problemas cibernéticos mais plausíveis e possíveis. Usar muitos recursos para eventos de alto impacto e baixa probabilidade – e consequentemente ter menos recursos para os eventos de baixo a médio impacto e alta probabilidade – não faz sentido nem politicamente, nem estrategicamente e certamente também não quando aplicamos uma lógica de custo-benefício. (CAVELTY, 2012, p.: 118, tradução livre)[32]

A atuação militar no espaço cibernético é importante e necessária, na medida em que deve garantir a Defesa Cibernética. O que deve ser ressaltado é que a Defesa e a Segurança Cibernética se entrelaçam de maneira bem complexa, fazendo com que muitas vezes se desenvolva uma resposta militar a um problema que é de cunho civil em sua essência. Pretende-se deixar claro que a atuação das Forças Armadas é necessária no ciberespaço, mas que ela deveria ser direcionada para lidar com problemas mais reais e plausíveis, como a espionagem através do meio cibernético. Além disso, vale notar também que alguns autores criticam esse papel preponderante garantido às Forças Armadas com a ideia de que isso pode vir a ameaçar a garantia das liberdades individuais (DINIZ; MUGGAH; GLENNY, 2014).

Por último, o CDCiber se demonstra como uma grande ferramenta disponível para o Brasil atuar no ciberespaço. Desde a sua institucionalização até atualmente, o CDCiber já conseguiu adquirir experiência e conhecimento técnico avançado através das diversas operações de monitoramento e defesa que realizou nos grandes eventos no Brasil. Sendo assim, parece interessante que esse conhecimento seja explorado, e que ele possa ser disseminado também na APF através de parcerias com os órgãos encarregados da Segurança Cibernética.

---

[32] […] cyber war should not receive too much attention at the expense of more plausible and possible cyber problems. Using too many resources for high-impact, low-probability events – and therefore having less resources for the low to middle impact and high probability events – does not make sense, neither politically, nor strategically and certainly not when applying a cost-benefit logic. (CAVELTY, 2012, p.: 118)

5. CONCLUSÃO

Portanto, tendo em vista esse movimento internacional dos Estados de se prepararem institucionalmente e estrategicamente perante o ciberespaço, este trabalho teve como foco analisar o caso brasileiro. Com isso, o objetivo foi o de tentar apresentar e analisar a situação atual da estratégia brasileira para o ciberespaço bem como a maneira como as instituições e organizações são moldadas com suas atribuições e responsabilidades. Tendo esse objetivo, esperou-se entender e avaliar criticamente se a resposta brasileira diante das novas ameaças para a segurança nacional é adequada.

A partir da conceitualização de "ciberespaço" e de "infraestruturas críticas" foi possível apresentar a diferença existente entre "ciberespaço" e "Internet" [33] (CEPIK; CANABARRO; BORNE, 2014, p.: 3), e como existe ainda bastante confusão em relação aos diversos termos utilizados.. Sendo assim, percebeu-se que isso pode atrapalhar no desenvolvimento de políticas nacionais e também na pesquisa sobre esse tema (CANABARRO; BORNE, 2013).

Conforme o que foi abordado no capítulo 2.2 e 2.3, percebe-se que existe no Brasil uma tendência de "crescimento" do ciberespaço. Isso se reflete pelo aumento constante dos usuários de internet que se tem visto nos últimos 10 anos, chegando atualmente perto de níveis internacionais. Também está respaldado no aumento gigantesco das linhas de telefonia móvel no Brasil, que ultrapassa a população em termos absolutos (WORLD BANK, 2016). Além disso, a maioria desses dispositivos conta com acesso à Internet, o que está se tornando em uma das principais maneiras de acesso da população brasileira, que passa a fazer grande parte das suas operações bancárias através da Internet (IBGE, 2016). Nesse mesmo sentido, houve também grande aumento do comércio eletrônico no Brasil (MINTEL, 2014; EBIT, 2016).

Entende-se, portanto, que esse crecimento necessita de amparo de infraestrutura para funcionar adequadamente. Ou seja, para que se mantenham os diversos fluxos informacionais no país e para fora dele, deve-se existir uma infraestrutura crítica informacional que torne isso possível. Então, em relação aos cabos submarinos, existem atualmente diversos projetos privados que já estão em andamento (TELETIME, 2016a,b,c,d) e que visam aumentar esse *backbone* da Internet, conectando o Brasil com novos pontos no globo. Em termos de satélites, o Brasil com o projeto do SGDC demonstra preocupação em garantir o acesso à Internet pelo país inteiro, além

[33] Entende-se que Internet se configura como o "carro-chefe" do ciberespaço.

de buscar a garantia de que as FA possam se comunicar em rede com o uso de um satélite nacional, que não depende de tecnologia e de relação com o estrangeiro, o que diminui as vulnerabilidades do país. Esse aumento do fluxo informacional e da estrutura adequada para sua existência parece garantir que haverá futuramente mais ameaças cibernéticas, e que elas passarão a demandar cada vez mais recursos e esforços do governo nacional para lidar com elas.

Em relação à análise das principais ameaças cibernéticas no Brasil, podemos tirar algumas conclusões. Conforme a análise de dados do CERT.br, percebe-se que os incidentes cibernéticos estão aumentando no Brasil nos últimos. Consequentemente, existem também grande aumento nos casos de crimes cibernéticos. Desde o hacktivismo até o caso de guerra cibernética, o que marca o ciberespaço brasileiro é a atuação de grupos de criminosos organizados que atuam especificamente nesse meio. Isso é corroborado pela constatação da existência de um mercado negro no Brasil destinado a venda de ferramentas utilizadas para se cometerem os crimes (TREND MICRO, 2014). O Brasil têm sofrido alguns ataques por parte de grupos hacktivistas como Anonymous e Lulzsec (TECMUNDO, 2011), mas a principal expressão são os crimes cibernéticos, principalmente aqueles relacionados às fraudes bancárias (FEBRABAN, 2013).

Claro que não se pretende dizer que essa é somente a única preocupação que merece receber atenção por parte do governo. O que se entende é que, em termos de ameaças provenientes de governo externos, a principal a se preocupar é a espionagem, seja ela direcionada às informações do governo ou às informações privadas de empresas, e não a pequena possibilidade de guerra cibernética, em que haja a ocorrência de danos materiais e humanos em virtude de um ataque cibernético.

Conforme o capítulo 3, percebe-se que o Brasil dispende esforços para tentar criar uma estrutura institucional em que o atores sejam dotados de funções e responsabilidades claras. Nesse sentido, a Segurança e a Defesa do ciberespaço estão divididas e são centralizadas basicamente em dois órgãos distintos e independentes, quais sejam, respectivamente, a Casa Militar e o CDCiber. Da análise feita, é possível extrair elementos que demonstram que a divisão clássica entre órgãos para defesa e órgãos para segurança não se adequa muito bem ao ciberespaço. A separação feita dessa forma e sem contemplar a colaboração entre os dois lados parece favorecer a sobreposição de tarefas e as lacunas por indefinição de responsabilidades. Além disso, a delegação da defesa do ciberespaço como atribuição de quase exclusividade do EB não parece ser muito produtiva, já que ela deveria contemplar igualmente todas as forças (CRUZ

JR, 2013, p.: 27-28). O esforço brasileiro de criação do SMDC juntamente com o ComDCiber parece ser a solução encontrada para esse problema, com vistas a estabelecer tanto a representação adequada de todas as forças como a colaboração com os setores governamentais mais direcionados para a Segurança.

Adicionalmente, também se percebem esforços dedicados à criação de governança para a Internet, tanto em aspectos sociais como em aspectos técnicos. Eles são refletidos na Cartilha de Princípios para a Internet, do CGI.br, e o Marco Civil da Internet, que estabelecem normas e princípios para a relação da sociedade com a Internet. Em termos técnicos, o desenvolvimento do ICP-Brasil visa a garantir a autenticidade dos documentos para poderem ser emitidos através da Internet, tentando adequar a administração pública às atividades dentro do ciberespaço

Vale destacar, também a atuação do CERT.br e do CTIR.gov. Em virtude do papel que lhes foram atribuídos, de diagnosticar incidentes cibernéticos, bem como tratar da resolução desses incidente, esses órgãos parecem essenciais para se identificarem as principais vulnerabilidades dos sistemas e redes, o que contribui diretamente para a construção da Estratégia Nacional de Segurança Cibernética.

Em termos de legislação sobre crimes cibernéticos, percebe-se que o Brasil avança nesse tema, já desenvolvendo um arcabouço notável para atuar na repressão deles. Entretanto, como exemplificado pelo MCI, a legislação ainda sofre por não estar completamente adequada às peculiaridades do ciberespaço (BRASIL, 2015b, p. 154-155). Além disso, a PF, apesar de contar com uma unidade especializada, a URCC, ainda não dispões dos recursos humanos e materiais para combater esse problema que cresce cada vez mais no Brasil.

Com o capítulo 4.1 teve-se o objetivo de entender e avaliar as principais políticas e diretrizes da Estratégia Brasileira de Segurança e Defesa Cibernética, com o intuito de que fosse possível fazer uma avaliação sobre o nível de adequação da resposta brasileira frente às ameaças que surgem a partir do ciberespaço. Dessa forma, entende-se que a partir da constatação por parte das autoridades da importância do setor cibernético (BRASIL, 2012a), e da constatação da importância e seriedade dos crimes cibernéticos (BRASIL, 2010), as políticas brasileiras parecem estar cientes da necessidade de especificação e alocação orçamentária (BRASIL 2015a; BRASIL, 2010; BRASIL, 2015b) que é essencial para se abordar o desenvolvimento de recursos humanos e tecnológicos para se garantir a segurança e defesa do ciberespaço.

Em termos de desenvolvimento de recursos humanos, podemos destacar o CEGSIC, o IDCiber, e o ENaDCbier como as principais representações políticas brasileiras que visam contemplar essa necessidade. Por outro lado, em termos de desenvolvimento tecnológico, o CEPESC e o RENASIC se configuram como as principais iniciativas para o desenvolvimento tecnológico visando à segurança cibernética. Segundo o documento de 2015 que versa sobre a segurança cibernética na APF, uma das maneiras que o Brasil tem para lidar com esses obstáculos são as parcerias com Escolas de governo bem como instituições privadas, como universidades e empresas (BRASIL, 2015a, p.: 44). O que se percebe a partir da análise das iniciativas feitas anteriormente no trabalho, é que o Brasil sinaliza no sentido de realizar parcerias que são benéficas para o desenvolvimento de uma Estratégia Cibernética de Segurança, como exemplificado pelo IDCiber e pelo RENASIC. Entretanto, a relação com as instituições privadas e as empresas parece ainda necessitar de fomento e atenção por parte das autoridades. Além disso, é possível contestar a efetividade de algumas dessas iniciativas, como o CEGSIC cuja formação de pessoal capacitado não parece atingir números muito expressivos[34].

Por outro lado, a falta de investimentos para o desenvolvimento de recursos humanos e de recursos estruturais é sinalizada como motivo pelo qual a PF não está devidamente aparelhada para agir no ciberespaço (BRASIL, 2015b). Segundo a CPI de crimes cibernéticos de 2015, a polícia não tem numero suficiente de pessoal qualificado para lidar com esse problema (BRASIL, 2015b, p.: 81). O que importa entender é que parece difícil conceber uma estratégia de Segurança e Defesa Cibernética brasileira sem que se tenha uma força policial adequadamente preparada para lidar com as principais ameaças cibernéticas no Brasil.

Com o capítulo 4.2, buscou-se dar destaque para a atuação militar de defesa do ciberespaço, abordando a doutrina e os conceitos sobre o emprego de ações no meio cibernético. Com isso, foi feita uma contestação sobre a necessidade de se ter capacidades para atuações ofensivas no ciberespaço, em virtude dos problemas envolvendo a empregabilidade e legitimidade de um ataque cibernético[35]. Além disso, o CDCiber já demonstra prática e experiência para lidar com a Defesa do Ciberespaço, adquirida através de sua atuação nos

[34] Assim como se demonstrou anteriormente, em suas quatro edições o CEGSIC formou somente 300 pessoas.

[35] Os problemas que são referidos no texto dizem respeito: i) ao Princípio do Efeito, que diz que as ações no ciberespaço podem não gerar os efeitos desejados em decorrência das diversas variáveis que afetam o comportamento dos sistemas informatizados (BRASIL, 2014c, p.: 21); à ii) dificuldade de se determinar o autor dos ataques (CAVELTY, 2012, p.: 118) ; e a dificuldade de se precisar exatamente os alvos de um ataque, o que fere a legitimação de um contra-ataque cibernético.

grandes eventos que ocorreram no Brasil nos últimos anos. Sem dúvida isso reflete a posição central que lhe foi garantida no planejamento brasileiro sobre a Defesa do ciberespaço

A Doutrina Militar e a Política Nacional de Defesa apontam bastante para a necessidade de o Brasil estar pronto para atuar em guerra cibernética. O que se percebe da análise é que o Brasil necessita realmente de recursos destinados a Defesa do ciberespaço, mas que, além disso, a abordagem sobre as ameaças não está sendo feita de maneira adequada. Certamente, como foi demonstrado anteriormente no trabalho, a principal ameaça cibernética estatal se configura como a espionagem realizada por governos estrangeiros direcionada às informações sigilosas de outro governo, bem como às informações sigilosas de uma empresa ou indústria. Nesse sentido, a visão abordada nos documentos sobre guerra cibernética não parece estar muito bem adequada, pelo menos do ponto de vista conceitual, às ameaças mais prováveis de serem enfrentadas pelo Brasil no ciberespaço. Por exemplo, se tomarmos a visão de Thomas Rid (2012) sobre o que é – ou não é – guerra cibernética, definitivamente é necessário uma melhor adequação conceitual do que é entendido como guerra cibernética pelas FA brasileiras, já que a espionagem cibernética, a principal ameaça estatal nesse meio, não seria considerada como guerra cibernética.

Resumidamente, a atuação militar no espaço cibernético brasileiro é importante para a Defesa cibernética na medida em que não foque no desenvolvimento de capacidades ofensivas e possa se adequar ao fato de que a espionagem se configura como a principal ameaça estatal e os crimes cibernéticos se configuram como a principal ameaça em geral. Sendo assim, deve-se existir definição clara sobre a atuação pelo lado militar através do CDCiber e atuação de repressão dos crimes cibernéticos a cargo da PF, já que com a o entrelaçamento que ocorre com a defesa e a segurança do ciberespaço, é favorável que se evite respostas militares a problemas que tem cunho essencialmente civil.

A partir deste trabalho, se percebe então, a necessidade de se ter em mente que o ciberespaço brasileiro está em expansão e que isso demandará cada vez mais atenção das autoridades. Nesse sentido, percebe-se também que ainda existe inadequação das respostas brasileiras perante as principais ameaças cibernéticas. Faz-se necessário estimular mais os debates sobre os crimes cibernéticos para que seja possível a alocação de investimentos com o objetivo de adequar a PF à função de repressão dos crimes cibernéticos no Brasil.

Por último, pode-se apontar algumas ideias que podem nortear a pesquisa que visa a contribuir nesse tema. Dada a grande dificuldade conceitual que o autor deste trabalho percebeu

em relação ao conceito de guerra cibernética, parece extremamente válido que os estudos sobre a conceituação de guerra cibernética sejam estimulados.

REFERÊNCIAS

ABIN. **Principais tecnologias disponibilizadas ao Governo Federal.** 2016. Disponível em: <http://www.abin.gov.br/atuacao/produtos/tecnologia/>.

ANATEL. **Relação de satélites autorizados a operar no Brasil.** 2016. Disponível em: <http://www.anatel.gov.br/Portal/verificaDocumentos/documentoVersionado.asp?numeroPublicacao=231007&documentoPath=231007.pdf&Pub=&URL=/Portal/verificaDocumentos/documento.asp>. Acesso em: 20 set. 2016.

ANSII. A word from the director general. **Agence nationale de la sécurité des systèmes d'information**, 2016. Disponível em: <https://www.ssi.gouv.fr/en/mission/word-from-director-general/>. Acesso em: 3 nov. 2016.

ARQUILLA, John. Cyberwar is already upon us. **Foreign Policy**, 2012. Disponível em: <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us?page=full>. Acesso em: 12 out. 2016.

BESSA, Jorge. **O escândalo da espionagem no Brasil.** Brasília: Thesaurus, 2014.

BETZ, David J; STEVENS, Tim. **Cyberspace and the State**: Toward a Strategy for Cyber-Power. Routledge for the International Institute for Strategic Studies, 2011. p. 36-37.

BLUMENTHAL, Marjory.; CLARK, David D.. The Future of the Internet and Cyberpower. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security.** Washington D.C.: National Defense University, 2009. Cap. 8, p.31.

BRASIL. **Constituição da República Federativa do Brasil**. 1998.

BRASIL. Lei nº 10.683, de 28 de Maio de 2003. **Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências.** 2003a. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/2003/L10.683.htm>.

BRASIL. Decreto nº 4.801, de 6 de Agosto de 2003. **Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho Governo**. 2003b. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2003/d4801.htm>.

BRASIL. Decreto nº 4.829, de 3 de Setembro de 2003. **Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGI.br, sobre o modelo de governança da Internet no Brasil, e dá outras providências.** 2003c. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm>.

BRASIL. **Livro Verde de Segurança Cibernética no Brasil**. 2010

BRASIL. **Política Nacional de Defesa** e **Estratégia Nacional de Defesa.** Brasília, 2012a.

BRASIL. **Política Cibernética de Defesa**. 2012b

BRASIL. **Livro Branco de Defesa Nacional.** 2013.

BRASIL. Lei nº 12.965, de 23 de Abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** 2014a. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

BRASIL. **Plano de Articulação e Equipamento de Defesa (PAED).** Ministério da Defesa. Brasília, 2014b.

BRASIL. **Doutrina Militar de Defesa Cibernética.** Ministério da Defesa. Brasília, 2014c.

BRASIL. Decreto nº 8577, de 26 Novembro de 2015. **Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Casa Militar da Presidência da República e remaneja cargos em comissão e funções de confiança**. 2015a Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Decreto/D8577.htm>.

BRASIL. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018.** Brasíli, 2015a.

BRASIL. **Relatório final da CPI – Crimes Cibernéticos.** Câmara dos Deputados. 2015b. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015>

BRENNER, Susan W.; CLARKE, Leo L. Civilians in Cyberwarfare: Casualties. **SMU Science & Technology Law Review**, 2010. v. 13, ed. 3, Disponível em: <https://works.bepress.com/susan_brenner/3/>. Acesso em: 17 out. 2016.

CANABARRO, Diego Rafael; BORNE, Thiago. **Ciberespaço e Internet:** Implicações Conceituais para os Estudos de Segurança. MUNDORAMA, 2013. Disponível em: <http://www.mundorama.net/2013/05/19/ciberespaco-e-internet-implicacoes-conceituais-para-os-estudos-de-seguranca-por-diego-rafael-canabarro-e-thiago-borne/>. Acesso em: 10 out. 2016.

CAVELTY, Myriam Dunn. The militarisation of cyber security as a source of global tension. In: MÖCKLI, Daniel (ed.). **Strategic Trends 2012:** key developments in global affairs. Center for Security Studies (CSS). Disponível em: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Strategic-Trends-2012-Cyber.pdf. Acesso em: 12 out. 2016.

CARNEIRO, Aristides Sebastião Lopes. A Defesa Cibernética como Extensão do papel constitucional da Forças Armadas na Defesa Nacional. In: PINTO, José Cimar Rodrigues. **Ciberdefesa e cibersegurança:** novas ameaças à segurança nacional. Rio de Janeiro: ESG, 2016.

CEPIK, Marco; CANABARRO, Diego Rafael; BORNE, Thiago. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: SOUZA, Andre; NASSER, Reginaldo M.; MORAES, Rodrigo F. **Do 11 de setembro de 2001 à guerra ao terror:** reflexões sobre o terrorismo no século XXI. Brasília: IPEA, 2014.

CERT.br. **Estatísticas dos Incidentes Reportados ao CERT.br**. 2016. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 14 out. 2016a.

CERT.br. **Sobre o CERT.br**. Principais Atividades. 2016b. Disponível em: < http://www.cert.br/sobre/>.

CGI.br. Resolução CGI.br/RES/2009/003/P – **Princípios para a Governança e Uso da Internet no Brasil**. 2009. Disponível em: <http://www.cgi.br/resolucoes/documento/2009/003>.

CRUZ JR. **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). 2013.

CTIR.gov. **Estatísticas de incidentes de rede na APF – 1º Trimestre de 2016**. 2016a. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2016/Estatisticas_CTIR_Gov_1o_Trimestre_2016.pdf>. Acesso em: 16 out. 2016.

CTIR.gov. **Sobre o CTIR.gov**. Missão. 2016b. Disponível em: <http://www.ctir.gov.br/sobre-CTIR-gov.html>.

DINIZ, Gustavo; MUGGAH, Robert; GLENNY, Misha. **Deconstructing cyber security in Brazil:** Threats and Responses. Instituto Igarapé. Strategic Paper 11. Dezembro, 2014. Disponível em: <https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf>. Acesso em: 10 out. 2016.

DSIC. **Conclusão do 4º Curso de Especialização em Gestão da Segurança da Informação e Comunicações (2012-2014).** Departamento de Segurança da Informação e Comunicações. 2015. Disponível em: < http://dsic.planalto.gov.br/noticias/471-conclusao-do-4-curso>.

EBIT. **Relatório Webshoppers**, ed. 33. 2016. Disponível em: <http://img.ebit.com.br/webshoppers/pdf/33_webshoppers.pdf>. Acesso em: 28 set. 2016.

EMPRESA BRASIL DE COMUNICAÇÃO. **Entenda o caso Snowden; Petrobras também é alvo de espionagem.** 2013. Disponível em: <http://www.ebc.com.br/tecnologia/2013/08/web-vigiada-entenda-as-denuncias-de-edward-snowden>. Acesso em: 20 out. 2016.

FARRELL, Henry. What's new in the U.S. cyber strategy. **Washington Post**, 2015. Disponível em: <https://www.washingtonpost.com/news/monkey-cage/wp/2015/04/24/whats-new-in-the-u-s-cyber-strategy/>.

FEBRABAN. **Pesquisa Febraban de Tecnologia Bancária 2013**. 2013. Disponível em: <www.ciab.org.br/Downloads/pesq_2013.pdf>. Acesso em: 20 out. 2016.

FONSECA, Lucas Ribeiro de Belmont; DELGADO, Tiago Medeiros. A Estratégia Interamericana para combater Ameaças Cibernéticas. In: OLIVEIRA, Marcos Aurélio Guedes de; NETO, Ricardo Borges Gama; LOPES, Gills Vilar (orgs). **Relações Internacionais Cibernéticas (CiberRI):** oportunidades e desafios para os estudos estratégicos e de segurança internacional. Coleção Defesa e Fronteiras Virtuais, v.3. Recife: Editora UFPE, 2016. P. 177-200.

FRAGOLA, Rodrigo Jonas. **Os Próximos Passos da Estratégia Cibernética de Defesa do Brasil.** DefesaNet. 2016. Disponível em: < http://www.defesanet.com.br/cyberwar/noticia/21837/Os-Proximos-Passos-da-Estrategia-Cibernetica-de-Defesa-do-Brasil/>.

GADELHA, Augusto Cesar. Pensar e compreender a Internet. Comitê Gestor da Internet. **Revista.br,** ed. 1, ano 1. 2009.

GASTALDI, Sol; JUSTRIBÓ, Candela. As Estratégias de Segurança e Defesa Cibernéticas na Argentina. In: OLIVEIRA, Marcos Aurélio Guedes de; NETO, Ricardo Borges Gama; LOPES, Gills Vilar (orgs). **Relações Internacionais Cibernéticas (CiberRI):** oportunidades e desafios para os estudos estratégicos e de segurança internacional. Coleção Defesa e Fronteiras Virtuais, v.3. Recife: Editora UFPE, 2016. P. 133-154.

GONÇALVES, Joanisval Brito. Segurança e Defesa Cibernética neste Admirável Mundo Novo. In: OLIVEIRA, Marcos Aurélio Guedes de; NETO, Ricardo Borges Gama; LOPES, Gills Vilar (orgs). **Relações Internacionais Cibernéticas (CiberRI):** oportunidades e desafios para os estudos estratégicos e de segurança internacional. Coleção Defesa e Fronteiras Virtuais, v.3. Recife: Editora UFPE, 2016. P. 19-26.

IBGE. **Pesquisa Nacional por Amostra de Domicílio**: acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal (2014). Rio de Janeiro, 2016.

IDCIBER. **Histórico.** Instituto de Defesa Cibernética. 2015. Disponível em: < http://www.idciber-eb.unb.br/index.php?option=com_content&view=article&id=87&Itemid=260>

IISS. **The Military Balance:** the annual assessment of global military capabilities and defence economics**.** London: Routledge, 2011.

ITI. **ICP-Brasil: o que é?**. Instituto de Tecnologia da Informação. 2016. Disponível em: <http://www.iti.gov.br/icp-brasil>.

KRAMER, Franklin D. Policy Recommendations for a Strategic Framework. . In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security.** Washington D.C.: National Defense University, 2009. Cap. 1, p.18.

KUEHL, Daniel T. From Cyberspace to Cyberpower: Defining the Problem. In: KRAMER, Franklin D.; STARR, Stuart H.; WENTZ, Larry. **Cyberpower and National Security.** Washington D.C.: National Defense University, 2009. Cap. 2, p.19.

LIBICKI, Martin C.. Cyberspace Is Not a Warfighting Domain. **I/S: A Journal of Law and Policy for the Information Society.** 2012.

MANDARINO, Raphael Jr. **Um estudo sobre a segurança e a defesa do espaço cibernético brasileiro**. Universidade de Brasília. Instituto de Ciências Exatas. Departamento de Ciência da Computação – CIC. Monografia apresentada ao Departamento de Ciência da Computação como requisito parcial para a obtenção do título de Especialista em Ciência da Computação: Gestão da Segurança da Informação e Comunicações. Brasília, junho de 2009.

MANDARINO, Raphael Jr. **Segurança e defesa do espaço cibernético brasileiro**. Recife: Cubzac, 2010.

MCGRAW, Gary. Cyber War is Inevitable (Unless we build Security in). **Journal of Strateigc Studies**, 2013. v. 36, n.1, p. 109-119. Disponível em: <http://www.tandfonline.com/doi/abs/10.1080/01402390.2012.742013>. Acesso em: 12 out. 2016.

MINISTÉRIO DAS COMUNICAÇÕES. **Conheça os cabos submarinos do Brasil**. 2015. Disponível em: < http://www.comunicacoes.gov.br/sala-de-imprensa/todas-as-noticias/institucionais/36231-o-fundo-do-mar-a-servico-das-telecomunicacoes>. Acesso em: 25 set. 2016.

MINTEL. **Setor de comércio eletrônico no Brasil cresceu 250% nos últimos cinco anos**. 2014. Disponível em: < http://brasil.mintel.com/imprensa/varejo-imprensa/setor-de-comercio-eletronico-no-brasil-cresceu-250-nos-ultimos-cinco-anos>. Acesso em: 27 out. 2016.

NETO, Walfredo Bento Ferreira; LOPES, Gills Vilar. Teoria da Fronteira Cibernética: inquietações interdisciplinares. In: OLIVEIRA, Marcos Aurélio Guedes de; NETO, Ricardo Borges Gama; LOPES, Gills Vilar (orgs). **Relações Internacionais Cibernéticas (CiberRI):** oportunidades e desafios para os estudos estratégicos e de segurança internacional. Coleção Defesa e Fronteiras Virtuais, v.3. Recife: Editora UFPE, 2016. P. 59-82.

NIC.br. **Estatuto NIC.br**. Núcleo de Informação e Coordenação do Ponto BR. 2014. Disponível em: < http://www.nic.br/pagina/estaturo-nic-br/160>.

NY TIMES. **Before the Gunfire, Cyberattacks.** 2008. Disponível em: <http://www.nytimes.com/2008/08/13/technology/13cyber.html>.

NYE, Joseph Samuel Jr. **Cyber Power.** Belfer Center for Science and International Affairs. Cambridge: Harvard Kennedy School, 2010. Disponível em: <http://belfercenter.hks.harvard.edu/files/cyber-power.pdf>. Acesso em: 20 out. 2016.

PORTAL BRASIL. **Satélite que ampliará banda larga no País passa por fase final de testes**. 2016. Disponível em: <http://www.brasil.gov.br/ciencia-e-tecnologia/2016/09/satelite-que-ampliara-banda-larga-no-pais-passa-por-fase-final-de-testes>. Acesso em: 20 out. 2016.

RENASIC. Conheça a RENASIC. **Objetivos específicos da RENASIC.** 2016. Disponível em: < http://www.renasic.org.br/institucional>.

RID, Thomas. Cyber War will not take place. **Journal of Strategic Studies**, v. 35, n. 1, 5-32. Fevereiro, 2012.

SHELDON, John B. State of the Art: Attackers and Targets in Cyberspace. **Journal of Military and Strategic Studies.** V. 14, ed. 2º. 2012.

TAVARES, Ricardo. **Defesa da Democracia brasileira no contexto da Guerra Cibernética**. Nota Técnica à Comissão de Relações Exteriores do Senado Federal. Brasília, 2013.

TECMUNDO. Grupo LulzSec tem braço brasileiro e já derrubou páginas governamentais. 2011. Disponível em: <https://www.tecmundo.com.br/seguranca/10947-grupo-lulzsec-tem-braco-brasileiro-e-ja-derrubou-paginas-governamentais.htm>. Acesso em: 20 out. 2016.

TELEGEOGRAPHY. **Submarine Cable Map**. 2015

TELEGEOGRAPHY. **Submarine Cable Map**. 2016. Disponível em: <https://www.telegeography.com/telecom-maps/submarine-cable-map.1.html>. Acesso em: 20 nov. 2016.

TELETIME. **Google quer sistema submarino ligando Rio a São Paulo em 2017**. 2016a. Disponível em: < http://convergecom.com.br/teletime/15/03/2016/google-quer-sistema-submarino-ligando-rio-sao-paulo-em-2017/>. Acesso em: 20 nov. 2016.

TELETIME. **Cabo Seabras-1, que ligará NY a SP, recebe financiamento de US$ 500 milhões**. 2016b. Disponível em: <http://convergecom.com.br/teletime/11/01/2016/cabo-que-ligara-ny-a-sp-recebe-financiamento-de-us-500-milhoes/>. Acesso em: 20 nov. 2016.

TELETIME. **Telefónica anuncia novo cabo ligando Brasil aos Estados Unidos**. 2016c. Disponível em: <http://convergecom.com.br/teletime/09/03/2016/telefonica-anuncia-novo-cabo-ligando-brasil-aos-estados-unidos/>. Acesso em: 20 nov. 2016.

TELETIME. **João Pedro Flecha de Lima assume comando da empresa de cabos submarinos Ellalink**. 2016d. Disponível em: < http://convergecom.com.br/teletime/12/02/2016/joao-pedro-flecha-de-lima-assume-comando-da-empresa-de-cabos-submarinos-ellalink/>. Acesso em: 20 nov. 2016.

TELETIME. **Angola Cables garante US$ 100 mi para cabo Fortaleza-Luanda; lançamento fica para 2018**. 2016e. Disponível em: <http://convergecom.com.br/teletime/04/04/2016/angola-cables-garante-us-100-mi-para-cabo-fortaleza-luanda-lancamento-fica-para-2018/>. Acesso em: 20 nov. 2016

THE GUARDIAN. **Russia accused of unleashing cyberwar to disable Estonia.** 2007. Disponível em: <https://www.theguardian.com/world/2007/may/17/topstories3.russia>.

TREND MICRO. **O submundo do Crime Digital Brasileiro**: Um Mercado de Aspirantes a Cibercriminosos?. Série sobre a Economia do Submundo do Cibercrime. 2014.

TREND MICRO. **Relatório sobre Segurança Cibernética e Infraestruturas Críticas nas Américas**. 2015

US DOD. **Department of Defense Strategy for Operating in Cyberspace.** Julho, 2011. Disponível em: <http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>. Acesso em: 10 out. 2016.

US DOD. **The DoD Cyber Strategy.** Abril, 2015. Disponível em: <http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>.

WALL STREET JOURNAL. **Brazil: The Social Media Capital of the Universe**. 2013. Disponível em: <http://www.wsj.com/articles/SB10001424127887323301104578257950857891898>. Acesso em: 23 out. 2016.

WORLD BANK. **Base de dados sobre os usuários de Internet no mundo.** 2016. Disponível em: <http://data.worldbank.org/indicator/IT.NET.USER.P2>. Acesso em: 22 set. 2016.