ESCOLA DE GUERRA NAVAL

CC EDUARDO RODRIGUES DE PAULA

GUERRA CIBERNÉTICA

Perspectivas para a consolidação de uma Estratégia cibernética para o Estado brasileiro

Rio de Janeiro

2016

CC EDUARDO RODRIGUES DE PAULA

GUERRA CIBERNÉTICA

Perspectivas para a consolidação de uma Estratégia cibernética para o Estado brasileiro

Monografia apresentada à Escola de Guerra Naval como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF Paulo Roberto Blanco Ozório

Rio de Janeiro

Escola de Guerra Naval

2016

Dedico este trabalho à minha filha Rafaella
pelos muitos momentos de ausência paterna.

AGRADECIMENTO

A Deus, pelo sopro da vida.

Aos instrutores, pelo despertar do estímulo científico.

Aos Oficiais-Alunos da Turma Ary Rongel, pelos 22 anos de companheirismo.

A todos que puderam me ajudar neste trabalho.

"No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids. We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism."

Presidente Barack Obama, Janeiro de 2015.

RESUMO

O propósito deste trabalho é analisar as perspectivas para a consolidação da Estratégia Cibernética brasileira baseado no avanço tecnológico, na arquitetura ultrapassada da Internet, na fragilidade de governos, empresas e instituições perante as vulnerabilidades digitais, no surgimento de novos atores internacionais e na indefinição jurídica do espaço cibernético. A relevância do tema reside na oportunidade de contribuir para a compreensão da capilaridade das ameaças cibernéticas para o Estado Brasileiro, identificando medidas a serem adotadas com a finalidade de melhorar a consciência nacional quanto a segurança cibernética. Para alcançar este objetivo, realizou-se uma pesquisa bibliográfica e documental, adotando-se uma metodologia descritiva e estudo de casos. O trabalho apoiou-se alicerçado na leitura de fontes bibliográficas, consultas a artigos científicos, documentos internacionais como a Carta das Nações Unidas, o Manual de Tallinn e as Estratégias Cibernética publicada por diversos países e, internamente, pela Política e Estratégia Nacional de Defesa, Constituição Federal dentre outros documentos. Após expor a situação atual brasileira e em alguns países, concluiu-se com propostas de melhorias para a estratégia cibernética nacional.

Palavras-chave: Direito Internacional. Direito Internacional dos Conflitos Armados. Carta das Nações Unidas. Manual de Tallinn. Guerra Cibernética. Ciberespaço. Ataque cibernético. Forças Armadas.

RESUMEN

El propósito de este trabajo es analizar las perspectivas de la consolidación de la estrategia cibernética de Brasil en base a los avances tecnológicos en la arquitectura antigua de Internet, la debilidad de los gobiernos, empresas e instituciones a las vulnerabilidades digitales, la aparición de nuevos actores internacionales y la inseguridad jurídica de lo ciberespacio. La importancia radica en la posibilidad de contribuir a la comprensión de la capilaridad de las amenazas informáticas al Estado brasileño, la identificación de las medidas que deben adoptarse con el fin de mejorar la conciencia nacional de la ciberseguridad. Para lograr este objetivo, hubo una investigación bibliográfica y documental, la adopción de una metodología y estudios descriptivos de casos. El trabajo fue apoyado arraigada en la lectura de fuentes bibliográficas, consultas con los artículos científicos, documentos internacionales como la Carta de las Naciones Unidas, el Manual Tallinn y la estrategias cibernética publicadas por diversos países e internamente por la Política y Estrategia de Defensa Nacional, Constitución Federal, entre otros documentos. Después de exponer la situación actual de Brasil y en algunos países, se concluyó con propuestas para mejorar la estrategia nacional cibernética.

Palabras clave: Derecho internacional. Derecho internacional de los conflictos armados. Carta de las Naciones Unidas. Manual de Tallinn. Guerra cibernética. Ciberespacio. Ciberataque. Fuerzas Armadas.

ABSTRACT

The purpose of this paper is to analyze the prospects for the consolidation of Brazilian Cybernetics strategy based on technological advancement in the outdated architecture of the Internet, the weakness of governments, companies and institutions to digital vulnerabilities, the emergence of new international actors and legal uncertainty of cyberspace. The relevance lies in the opportunity to contribute to the understanding of the capillarity of cyber threats to the Brazilian State, identifying measures to be taken in order to improve national awareness of cybersecurity. To achieve this goal, there was a bibliographical and documentary research, adopting a descriptive methodology and case studies. The work was supported rooted in reading literature sources, consultations with scientific papers, international documents like the United Nations Charter, the Tallinn Manual and Cybernetics Strategies published by various countries and internally by the Policy and National Defense Strategy, Federal Constitution among other documents. After exposing the Brazilian current situation and in some countries, it was concluded with proposals for improvements to national cybersecurity strategy.

Keywords: International Law. International Law of Armed Conflict. United Nations Charter. Tallinn Manual. Cybernetics war. Cyberspace. Cyberattack. Armed Forces.

SUMÁRIO

1 INTRODUÇÃO

Vivemos em um mundo conectado. As empresas e os países contam com o ciberespaço para tudo, desde transações comerciais até a movimentação das forças militares. Códigos de computador embaraçam a linha divisória entre o mundo cibernético e o físico e conectam milhões de dispositivos na Internet. Companhias elétricas contam com sistemas de controle industrial para fornecer energia à rede. Empresas logísticas utilizam satélites e a Internet para rastrear navios mercantes em rotas marítimas internacionais. Governos e Forças Armadas dependem de redes e dados seguros para o cumprimento de suas tarefas.

Segundo a Organização das Nações Unidas (ONU), em quinze anos o acesso à Internet aumentou de 400 milhões para 3,2 bilhões de pessoas[1]. No entanto, essas mesmas qualidades de abertura e dinamismo, que levaram à rápida expansão da Internet, produziram atores estatais e não-estatais perigosos com o objetivo de minar interesses adversos.

As pessoas, as instituições, o governo, enfim todos passaram a ser vulneráveis neste mundo conectado. A Internet não foi originalmente concebida com a segurança em foco, mas como um sistema aberto para permitir que cientistas e pesquisadores pudessem compartilhar dados rapidamente. Sem fortes investimentos em segurança e defesa cibernética, sistemas de dados permanecem abertos e suscetíveis de exploração e de ataque. Atores mal-intencionados usam o ciberespaço para roubar dados e propriedade intelectual para seus próprios objetivos econômicos ou políticos.

A utilização crescente de ataques cibernéticos como um instrumento político reflete uma tendência perigosa nas relações internacionais. Durante um conflito, um adversário poderá atacar a infraestrutura crítica e redes militares para ganhar uma vantagem estratégica.

---

1 https://nacoesunidas.org/em-15-anos-numero-de-usuarios-de-internet-passou-de-400-milhoes-para-32-bilhoes-revela-onu/

Governos, empresas e organizações devem priorizar cuidadosamente os sistemas e dados que eles precisam para proteger, avaliar riscos e fazer investimentos prudentes nas capacidades de segurança cibernética e de defesa cibernética para alcançar suas metas e objetivos de segurança.

Neste início de século em que o domínio cibernético tomou forma leva-nos a uma importante questão: "O que precisa ser feito para o desenvolvimento da Estratégia Cibernética brasileira?"

O propósito deste trabalho é, portanto, analisar as perspectivas para a consolidação da Estratégia Cibernética brasileira, tendo como premissas: o avanço tecnológico; a arquitetura ultrapassada da Internet; a fragilidade do governo e de instituições frente as vulnerabilidades digitais; o surgimento de novos atores contra Estados; a falta de um entendimento estabelecido pelo Direito Internacional; e a utilização da cibernética para objetivos políticos, econômicos e militares.

Complementarmente, evidenciaremos a Guerra Cibernética como nova forma de conflito; analisaremos como os conflitos cibernéticos ocorrem entre diversos atores; e mostraremos o silêncio jurídico do tema cibernético no Direito Internacional.

A relevância do tema fundamenta-se na compreensão da capilaridade das ameaças cibernéticas para o Estado Brasileiro identificando medidas a serem adotadas com a finalidade de melhorar a consciência nacional quanto a segurança cibernética.

Para alcançar o objetivo, a metodologia empregada neste trabalho é descritiva[2] e estudo de casos[3], fundamentada em pesquisa bibliográfica e documental. Para a consecução do propósito, foi realizado uma pesquisa documental e bibliográfica, baseados na leitura de documentos da Administração Pública nacional e internacional e na leitura de fontes bibliográficas diversas.

---

2 MARCONI, M. de A.; LAKATOS, E. M. Técnicas de Pesquisa. 7ª Edição. São Paulo: Editora Atlas, 2008.
3 YIN, Robert K. Estudo de Caso: Planejamento e Métodos. 5ª Edição. Porto Alegre: Editora Bookman, 2015.

Este trabalho está organizado em cinco capítulos. Após esta introdução, o capítulo dois abordará a Guerra Cibernética como o conflito do século atual, evidenciando os danos de alguns ataques recentes, as vulnerabilidades da Internet e os entendimentos internacionais a respeito.

O capítulo três contextualizará a situação da Estratégia Cibernética dando ênfase no período de 1999 (criação do Ministério da Defesa) até os dias atuais realçando os acontecimentos e o que foi produzido pelos níveis político e estratégico no Brasil e em outros países. Com base em apontamentos de especialistas após o vazamento de informações de governo, ocorrido em 2013, o capítulo quatro abordará propostas do que precisa ser feito para melhorar a Estratégia cibernética brasileira. Por último, o capítulo cinco apresentará as conclusões da pesquisa.

Assim, inicia-se o estudo com a apresentação da Guerra Cibernética e suas características.

2 O CONFLITO DO SÉCULO XXI: A GUERRA CIBERNÉTICA

Este capítulo abordará o surgimento de um novo domínio de se fazer a guerra mostrando alguns fatos recentes marcantes, os pontos fracos da arquitetura da Internet e interpretações na ordem mundial à luz de documentos internacionais. Mostrará também como o avanço tecnológico provocará mudanças nos indivíduos, instituições e governos.

2.1 Características do domínio cibernético[4]

Até o final do século XX existiam quatro domínios da guerra: Terrestre, Marítimo, Aéreo e Espacial. A partir do início do atual século, o espaço cibernético foi reconhecido, conforme veremos adiante, entre os atores Estatais, como um novo domínio onde operações militares podem ser conduzidas.

Este novo domínio possui as seguintes características particulares: alcance global; inexistência de fronteiras físicas; incerteza da segurança; simplicidade de acesso; e velocidades instantâneas. Além dessas características, pode-se dizer que os "*bits*" não vestem uniforme.

Com o aumento da inclusão digital em escala global, o ciberespaço vem se tornando o mediador das relações sociais e um motor de desenvolvimento para todos os países. O espaço físico, então, perde importância e as interações humanas passam a ser dirigidas num espaço virtual onde a informação está disponível *online*, independentemente do local e da hora do dia.

Apesar de não ter sido projetado para isto, o ciberespaço é hoje palco de diversos tipos de ataques e crimes contra pessoas físicas e jurídicas, infraestruturas críticas e sistemas de governança e de Defesa dos Estados.

---

4 O termo "cibernético" é usado genericamente para descrever computadores, redes e informações digitais.

2.2 Internet: arquitetura e vulnerabilidades

A Internet como conhecemos hoje foi concebida na década de 1960 influenciada pelas sensibilidades e ideologias da época. Os hippies dos campus do MIT, Stanford e Berkeley, financiados pela ARPA[5], construíram a ARPANET para as comunicações militares. Em seguida, criaram um protocolo de transmissão básico, que é utilizado até hoje, para conectá-la a outras redes em desenvolvimento. Robert Kahn[6] definiu quatro princípios para essas conexões:

> a) Cada rede distinta deve ser mantida independente e nenhuma mudança interna deve ser exigida a qualquer tipo de rede para conectá-la à Internet;
> b) As comunicações devem funcionar na base do melhor esforço. Se um pacote não chegou até o seu destino final, ele deve ser retransmitido rapidamente pela fonte;
> c) Caixas pretas seriam utilizadas para conectar as redes; posteriormente, estas seriam chamadas de gateways e roteadores. Não deve existir a retenção de informações pelos gateways sobre os pacotes individuais trafegados, mantendo-os, portanto, simples e evitando complicadas adaptações e recuperações de vários modos de falha; e
> d) Não deve existir nenhum controle global no nível de operações. (CLARKE, 2015, p.70).

Até meados da década de 1990, a Internet foi quase que universalmente vista como uma ferramenta para o bem ao facilitar as trocas de comunicação entre indivíduos, acadêmicos, cientistas, governos e instituições. Entretanto, com a entrada de mais usuários e a criação do comércio eletrônico, a Internet passou a ser também um local de atuação de criminosos.

Desde a sua criação, a arquitetura descentralizada da Internet permanece a mesma e os transgressores da lei sabem muito bem disto. Conforme indicado por Clarke (2015), a Internet apresenta pelo menos seis grandes vulnerabilidades.

---

5 ARPA acrônimo em inglês para a Agência de Projetos e Pesquisas Avançadas do Departamento de Defesa dos EUA.

6 Considerado um dos criadores da Internet.

A primeira delas é o DNS[7], sistema que traduz nomes para os endereços IP e endereços IP para os nomes respectivos. Existem no mundo treze servidores DNS principais e sem eles a Internet não funcionaria. Destes, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa. Na arquitetura que foram originalmente concebidos, quando um servidor principal falha, os demais conseguem manter o funcionamento da rede sem maiores complicações.[8] [9] [10] [11] Para os guerreiros cibernéticos, o DNS é um alvo. Eles podem redirecionar os pacotes de dados para o lugar errado ou ainda atacar o próprio sistema.[12]

A segunda fragilidade da Internet é o roteamento entre os ISPs[13], um sistema conhecido como BGP[14] que é um protocolo de roteamento interdominios, criado para uso nos roteadores principais da Internet. Por design, roteadores que executam BGP aceitam rotas anunciadas de outros roteadores BGP por padrão. Isto permite o roteamento automático e descentralizado de tráfego através da Internet, mas também deixa a Internet potencialmente vulnerável a interrupções acidentais ou maliciosas. Devido à extensão em que BGP é incorporado nos sistemas de núcleo da Internet, e o número de diferentes redes operadas por diferentes organizações que coletivamente constituem a Internet, corrigir esta vulnerabilidade (tal como ao introduzir a utilização de chaves criptográficas para verificar a identidade de roteadores BGP) é um problema tecnicamente complexo e dispendioso economicamente.[15]

A terceira vulnerabilidade da Internet é a falta de governança. Não existem pessoas, nem sistemas, nem instituições no comando. No passado, a ARPA, assumiu a função de administradora da rede, mas hoje ninguém mais tem este papel.

7 Domain Name System. É um banco de dados que liga nomes significativos (conhecidos como nomes de host), tais como http://www.microsoft.com, para um endereço IP específico, como 192.168.124.1.
8 http://www.iana.org/domains/root/servers
9 http://ietf.org
10 https://tools.ietf.org/html/rfc1034
11 https://tools.ietf.org/html/rfc4033
12 http://www.tecmundo.com.br/ataque-hacker/100994-hackers-usar-falha-dns-controlar-pcs-mundo.htm
13 Internet service provider (provedor de serviço de Internet)
14 Border Gateway Protocol. (protocolo de roteamento. Em uso desde 1994)
15 http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2

O fato de quase tudo trafegar sem criptografia, ou seja, em aberto, faz desta a quarta vulnerabilidade da Internet. A quinta é a aptidão dela propagar intencionalmente todo tipo de malware[16]. E a sexta grande vulnerabilidade segundo Clarke e Knake (2015, p. 69) é que a Internet é uma grande rede com arquitetura descentralizada. Como os criadores não queriam que ela fosse controlada, eles desenvolveram um sistema que priorizou na descentralização ao invés da segurança.

2.3 Primeiros ataques e incidentes em grande escala

Em 26 de abril de 2007, o governo da Estônia transferiu um memorial soviético da Segunda Guerra Mundial do centro da capital para um cemitério militar. A transferência inflamou a opinião pública tanto da Estônia quanto da Rússia. No dia seguinte, o governo Estoniano, os serviços de Polícia e as infraestruturas bancárias, de mídia e de Internet, sofreram três semanas de ataques cibernéticos, cujo impacto ainda gera imenso interesse dos governos em todo o mundo.

Estonianos realizam mais de 98% das suas operações bancárias através de meios eletrônicos. Portanto, ficou evidente para o mundo, o impacto de múltiplos *Distributed Denial-of-Service* (DDoS), que cortaram todas as comunicações com a Internet nos dois maiores bancos do país.

Foram grandes os interesses diplomáticos na crise da Estônia, em parte devido à possível reinterpretação do artigo 5º da OTAN, que afirma que "um ataque armado contra um membro da Aliança será considerado um ataque contra todos eles."[17] Este artigo só foi invocado uma única vez, logo após os atentados terroristas de 11 de setembro de 2001 mas, segundo Clarke e Knake (2015) e Geers (2011), um dia poderá ser interpretado para incluir ataques cibernéticos.

16 Código malicioso. Alguns tipos: vírus, worms e phishing scams
17 "The North Atlantic Treaty" 1949.

Para muitos especialistas, os ataques na Estônia representam o marco zero de um modelo de ataque cibernético contra um país dependente de TI. Segundo Geers (2011), o mundo testemunhou a transformação da segurança cibernética de uma disciplina técnica a um conceito estratégico. O crescente poder da Internet, o rápido desenvolvimento de ferramentas *hacker* associado a novas táticas e exemplos claros dos eventos atuais sugerem que ataques cibernéticos crescerão em termos de ameaças importantes e em futuros conflitos internacionais.

Sobre os eventos atuais pós-Estônia podemos citar alguns de ampla repercussão:

a) em 2007, Israel relatou ter realizado um ataque cibernético contra a defesa aérea Síria antes da destruição de um suposto reator nuclear (CLARKE; KNAKE, 2015);

b) em 2008, muitos analistas argumentaram que a guerra russo-georgiana demonstrou que haverá uma estreita relação entre as operações cibernéticas e convencionais em todas as futuras campanhas militares (BORG; BUMGARNER, 2009);

c) em 2010, o *worm*[18] *Stuxnet* destruiu fisicamente centenas de centrífugas numa usina de enriquecimento nuclear no Irã. É o *malware* mais sofisticado desenvolvido até então e amplamente considerado como criação de um ator Estatal (KUSHNER, 2013);

d) em 2011, invasores cibernéticos comprometeram a *Sony PlayStation Network*, com a divulgação de dados pessoais de mais de 100 milhões de contas de clientes custando à empresa, oficialmente, US$ 171 milhões e talvez até US$ 250 milhões, de acordo com algumas estimativas (GAUDIOSI, 2014);

e) em 2012, a companhia de petróleo *Saudi Aramco* levou mais de duas semanas para se recuperar do apagamento de mais de 30.000 unidades de disco rígido conectadas à sua rede interna por intrusos digitais (OECD, 2015);

18 Worm (“verme”, na língua inglesa) é um programa de computador autorreplicante, diferente do vírus. Enquanto um vírus infecta um programa e necessita deste programa hospedeiro para se alastrar, o worm é um programa completo e não precisa de outro para se propagar na rede. Além de se autorreplicar, pode deletar arquivos em um sistema ou enviar documentos por email. Para saber mais: http://www.psafe.com/blog/worm/

f) em 2013, um ataque DoS[19] foi realizado contra a organização internacional *Spamhaus*, que monitora o spam e ameaças virtuais relacionados em tempo real em todo o mundo, chegando a um número sem precedentes de 300 Gigabits por segundo (Gbs), seis vezes a média de ataque DoS e três vezes o maior ataque de negação de serviço já detectado (Leyden, 2013). No mesmo ano, a empresa de varejo estadunidense "*Target*" foi atingida durante a temporada de vendas de Natal por um ataque sofisticado envolvendo dispositivos de ponto-de-venda que roubaram o número de 40 milhões de cartões de crédito, custando à empresa quase US$ 1 bilhão. Algumas semanas mais tarde, o presidente e chefe executivo da empresa renunciou (WRIGHT, 2014);

g) em 2014, os dados de milhões de famílias norte-americanas e de pequenas empresas foram comprometidos pelo vazamento no banco *JPMorgan Chase* (Kitten, 2014). No mesmo ano, uma invasão em na rede interna da *Sony Pictures Entertainment* levou a divulgação pública de e-mails internos, dados pessoais de funcionários da empresa e parceiros bem como filmes que ainda não estavam no mercado. Em dezembro, o governo da Alemanha reconheceu que um *malware* causou danos materiais no sistema de produção de uma usina de aço no país. A invasão dos sistemas de controle resultou em um incidente no qual uma fornalha não conseguiu ser desligada da forma correta, resultando em danos físicos em todo o sistema (GARCIA, 2014).

2.4 O que diz o Direito Internacional

Nada envolve tanto os seres humanos, de maneira tão íntima e completa, quanto a guerra. Segundo Julien Freund (1995):

19 Os ataques DoS (sigla para Denial of Service), que podem ser interpretados como "Ataques de Negação de Serviços", consistem em tentativas de fazer com que computadores - servidores Web, por exemplo - tenham dificuldade ou mesmo sejam impedidos de executar suas tarefas. Para isso, em vez de "invadir" o computador ou mesmo infectá-lo com malwares, o autor do ataque faz com que a máquina receba tantas requisições que esta chega ao ponto de não conseguir dar conta delas. Em outras palavras, o computador fica tão sobrecarregado que nega serviço. Para saber mais: http://www.infowester.com/ddos.php

> Conflito é um enfrentamento por choque intencional entre dois seres ou grupos da mesma espécie que manifestam, uns em relação a outros, uma intenção hostil, em geral a um propósito de direito, para manter, afirmar ou restabelecer o direito. Trata-se de romper a resistência do outro, eventualmente pelo recurso da violência, e que pode tender ao aniquilamento físico do outro. (FREUND, 1995, p.58).

De acordo com Clausewitz (2010, p.7), "A guerra é um ato de violência com o qual se pretende obrigar o nosso oponente a obedecer à nossa vontade".

No século XX foram desenvolvidas as armas de destruição em massa (nucleares, químicas e biológicas). O século XXI observa agora o surgimento de um novo domínio de conflitos – com novos tipos de "armas" – que merece atenção do Direito Internacional: a guerra cibernética. Este é um fenômeno tão novo que, independentemente do poderio econômico ou militar, todos os Estados apresentam grande vulnerabilidade.

O Direito Internacional analisa lentamente as alterações por que passou a guerra neste último século com a multiplicação dos atores dos conflitos armados para além dos Estados soberanos e as modificações na geografia dos conflitos.

2.4.1 Carta da ONU e Convenções de Genebra

As referências legais que regulam os conflitos entre Estados desde a II Grande Guerra Mundial são a Carta das Nações Unidas (ONU, 1945) e as Convenções de Genebra (CICV, 1949). A Carta das Nações Unidas, legitima o recurso ao uso da força por parte dos Estados (o *jus ad bellum*) ao passo que a Convenção de Genebra, a principal fonte de direito humanitário internacional, regula a condução dos conflitos armados e é vista como a Lei da Guerra (o *jus in bello*). Ainda não foi aprovada emenda alguma textualizando explicitamente ataques cibernéticos nestes documentos.

Na medida em que o tempo passa e continua o silêncio conceitual no Direito Internacional, vários Estados e organizações supranacionais estão, isoladamente, tentando

definir conflitos cibernéticos enquanto atos de força. Graham (2009, p. 101) afirma que "é possível concluir que certos ataques cibernéticos podem ser considerados como ataques armados". Sklerov (2009, p. 65), justifica que "Estados reconhecem que usos não convencionais de força podem justificar o tratamento como um ataque armado quando seu escopo, duração e intensidade forem de gravidade suficiente".

Os Estados questionam-se: "um ataque cinético, por meio das forças armadas, em resposta a um ataque cibernético, estaria respaldado no Direito Internacional?".

2.4.2 Manual de Tallinn

O "Manual de Tallinn sobre o Direito internacional aplicável a guerra cibernética", é um documento acadêmico, não vinculativo, publicado em 2013 e escrito por um grupo internacional e independente de especialistas, sendo o resultado de um esforço do CCDCOE[20] da OTAN (Organização do Tratado do Atlântico Norte) para examinar como normas internacionais se aplicam a esta "nova" forma de guerra.

O Manual de Tallinn presta atenção especial para o *jus ad bellum*, o direito internacional que rege o recurso à força por parte dos Estados como um instrumento de sua política nacional, e o *jus in bello*, o direito internacional que regula a conduta dos conflitos armados (também conhecido como a lei da guerra, a lei de conflito armado, ou o direito humanitário internacional). As Convenções de Genebra e de Haia e as regras de Nova York são tratadas no contexto da guerra cibernética. O Manual de quase trezentas páginas deixa claro que não é um documento oficial mas sim uma expressão das opiniões de um grupo de peritos independentes que atuam exclusivamente a título pessoal e que não possui a intenção de representar as opiniões do CCDCOE, das organizações e dos Estados envolvidos ou da

20 CCDCOE (Cooperative Cyber Defence Centre of Excellence). Centro de Excelência de Ciberdefesa Cooperativa

própria OTAN, porém, segundo vários autores, é considerado o primeiro manual de guerra cibernética[21] devido a sua relevância e influência jurídica internacional.

Consiste de um conjunto de regras, acompanhada da respectiva base legal e suas implicações práticas. Ele alerta que a guerra cibernética pode levar a crimes de guerra cibernética. Lançar um ataque de rede de computadores de uma nação neutra, por exemplo, é proibido, da mesma forma que o exército inimigo não está autorizado a marchar através do território de um país neutro.

Tallinn, capital da Estônia, local onde foi escrito o manual, não é mera coincidência. Em 2007, a Estônia foi vítima de uma série de ciberataques que duraram três semanas conforme descrito anteriormente.

Segundo o Manual (CCDCOE, 2013), um ciberataque pode refletir um uso efetivo da força desde que observados oito critérios de elegibilidade: severidade, imediatez, direcionamento, capacidade invasiva, mensurabilidade dos efeitos produzidos, caráter militar, envolvimento de Estados e presumível legalidade.

O ciberataque à Estônia em 2007 não pode, à luz destes critérios, ser enquadrado legalmente como uso efetivo da força devido tanto às suas consequências (não letais) como à atribuição da origem dos ataques do seu originador (só foram identificados, oficialmente, atores não-Estatais). No caso do Stuxnet, que em 2010 afetou o programa nuclear iraniano, a aplicação destes critérios aponta para o uso efetivo da força, caso seja provado a identidade de um determinado Estado. Porém, a menos que em autodefesa, a ação conduzida por esse Estado (não identificado) será considerada ilegal pois inexiste aprovação do Conselho de Segurança da ONU.

Quando um ciberataque constituir um “perigo grave e iminente” e ameaçar a sua soberania, um determinado Estado pode invocar a necessidade de autodefesa para alegar a

21 http://www.theage.com.au/it-pro/security-it/first-cyber-war-manual-released-20130319-2gegk.html

adoção de contramedidas. Neste caso, o Estado vítima poderá, para proteger-se, infringir os direitos de outros Estados. A necessidade desta ação não requer a atribuição do ataque a outro Estado, podendo apenas ser invocada em ocorrências excepcionais e desde que não prejudique os interesses essenciais de outros Estados, conforme os artigos 2º (4) e 51º[22] da Carta das Nações Unidas (ONU, 1945) que enquadra e legitima o direito à autodefesa individual e coletiva.

Projetada para ampliar o escopo do manual original, "Tallinn 2.0" está previsto para ser publicado ainda neste ano. O foco da primeira edição está em operações cibernéticas mais destrutivas, isto é, aquelas que permitem aos Estados uma resposta em autodefesa e aquelas que se realizam durante o conflito armado. Uma vez que a ameaça de operações cibernéticas com tais consequências é especialmente alarmante para os Estados, a maioria das pesquisas acadêmicas tem-se centrado sobre estas questões.

No entanto, os Estados são desafiados diariamente por ciberoperações malignas inferiores. O projeto Tallinn 2.0 examina o quadro jurídico internacional que se aplica a essas operações cibernéticas.

22 Art. 51: Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um ataque armado contra um membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacional. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacional.

3 ESTRATÉGIA CIBÉRNÉTICA

Este capítulo abordará como se encontra a Estratégia Cibernética brasileira bem como a estratégia de outros países como EUA, China, Rússia dentre outros.

3.1 A situação do Brasil

Veremos nesta seção a repercussão recente envolvendo denúncias de espionagem de cidadãos e instituições brasileiras e como se encontra a estratégia cibernética brasileira.

3.1.1 Vazamento de Informações de Governo

Nas últimas duas décadas a internet invadiu o dia a dia das pessoas em todo o mundo. Ela trouxe uma possibilidade de liberdade de expressão nunca antes vista mas ela trouxe também a capacidade de controle de dados e informações que por ela trafegam.

Em maio de 2013, o ex-agente da *National Security Agency* (NSA)[23], Edward Snowden, trouxe a público revelações de que os EUA bisbilhotaram há tempos informações que circulam por redes telefônicas e pela internet tanto de empresas quanto de governos ao redor do mundo. O mundo acompanhou perplexo tais revelações e o Brasil foi um dos alvos preferenciais de espionagem. Embaixadas brasileiras, Ministério das Minas e Energia, Petrobras e até as ligações telefônicas da presidente Dilma Rousseff foram interceptadas.

Reagindo, o Palácio do Planalto foi até a ONU e, acompanhado da Alemanha, redigiu uma resolução que mais tarde foi aprovada. Internamente, o Senado Federal instaurou uma Comissão Parlamentar de Inquérito (CPI) para investigar não apenas o alcance das denúncias, mas também as fragilidades do sistema de telecomunicações brasileiro e do sistema de inteligência e defesa cibernética.

23 Agência de Segurança Nacional dos Estados Unidos, criada em 4 de novembro de 1952 com funções relacionadas a Inteligência de sinais (SIGINT), incluindo interceptação e criptoanálise. Também é um dos órgãos estadunidense dedicados a proteger as comunicações americanas. A NSA é parte do Departamento de Defesa dos Estados Unidos.

O relatório da CPI da Espionagem, como ficou conhecido, apontou que o poderio dos EUA sobre a governança da internet é muito grande e qualquer iniciativa tomada em um fórum global sobre este assunto não vem prosperando até então. Não foram apontadas a autoria de crimes mas evidenciou-se diversos problemas, destacando-se:

a) Política Nacional de Inteligência não publicada;

b) ausência de regulamentação das atividades de inteligência e de contrainteligência de maneira transparente e com mecanismos de controle externo;

c) ausência de uma Estratégia Nacional de Segurança Cibernética englobando ações coordenadas entre os setores público e privado;

d) inexistência de órgão central e distribuição descoordenada dos assuntos relacionados à segurança cibernética e segurança de infraestruturas críticas;

e) baixo investimento em educação, pesquisa e desenvolvimento no setor cibernético; e

f) ausência de softwares, hardwares de comunicação e algoritmos de criptografia nacionais associada a elevada dependência de sistemas de telecomunicações estrangeiros.

3.1.2 Desenvolvimento nos níveis político e estratégico

Somente em 1999, o Ministério da Defesa foi criado[24], substituindo os antigos Ministérios da Marinha, do Exército e da Aeronáutica, que foram transformados em Comandos do Ministério da Defesa. Somente em 2010, foi criado o Estado-Maior Conjunto das Forças Armadas[25] e foram inseridas as atribuições do Ministro de Estado da Defesa. Uma delas é a que o Ministro fica responsável pela elaboração do Livro Branco de Defesa Nacional, a ser elaborado a cada quatro anos, a partir de 2012, com base na Estratégia Nacional de Defesa e nas discussões e debates entre os integrantes das Forças armadas e

24 http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp97.htm
25 http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp136.htm

diferentes setores da sociedade brasileira, o meio acadêmico, cientistas e políticos. Em 2012, houve então a primeira edição do Livro Branco de Defesa Nacional.

Atualmente, no Brasil, são os seguintes os documentos norteadores da Administração Pública Federal para o setor cibernético: Constituição Federal e Leis Complementares, Política Nacional de Defesa, Estratégia Nacional de Defesa, Livro Branco de Defesa Nacional. Além destes, integram outros aprovados pelo Ministério da Defesa: Política Militar de Defesa e Estratégia Militar de Defesa (publicações sigilosas), Política Setorial de Defesa, Estratégia Setorial de Defesa e Doutrina Militar de Defesa Cibernética. Encontra-se em fase final de elaboração a Concepção Operacional do Sistema Militar de Defesa Cibernética.

O primeiro documento do nível político versando sobre as ações destinadas à defesa nacional foi a Política de Defesa Nacional[26], aprovado em 2005. Este documento foi atualizado em 2012 passando a se chamar Política Nacional de Defesa (PND).

"A PND é o documento condicionante de mais alto nível do planejamento de ações destinadas à defesa nacional coordenadas pelo Ministério da Defesa." (PND, 2012, p.1) Ela orienta que o setor cibernético é um setor estratégico para a Defesa da Pátria e que deve ser fortalecido. A PND orienta também que é essencial aperfeiçoar os dispositivos de segurança para se opor a possíveis ataques cibernéticos e adotar procedimentos que reduzam a vulnerabilidade dos sistemas ou que permitam seu pronto restabelecimento. (PND, 2012)

Acompanhado da PND, foi publicada em 2012 a Estratégia Nacional de Defesa (END). Juntos, estes documentos norteiam o planejamento setorial de alto nível. A END estabelece como fazer o que foi enunciado pela Política. Ambos os documentos frisam que a Defesa não deve ser assunto restrito aos militares ou ao governo mas sim uma preocupação de toda a sociedade.

---

26 http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm

Analisando os parágrafos anteriores, percebemos que a documentação sobre Defesa e Segurança Nacional, nos mais altos níveis do País, foi recém-concebida e que muito ainda precisa ser feito para melhorar o arcabouço doutrinário deste setor.

A existência de ameaças à paz mundial requer a atualização permanente devendo-se buscar à redução da dependência tecnológica. Com o progressivo desenvolvimento do País, maior cuidado requer a segurança das infraestruturas críticas[27]. Faz-se necessário, portanto, identificar os principais pontos estratégicos e implementar suas defesas.

Dentre os objetivos estratégicos, a END enumera itens que deverão ser obtidos domínio nacional, ainda que parcialmente, dentre eles: a fabricação de satélites e seus veículos lançadores, alternativas nacionais ao GPS[28] e as capacitações e os instrumentos cibernéticos necessários para assegurar comunicações. No setor cibernético, as capacitações se destinarão aos usos industriais, educativos e militares.

Na abordagem do contexto geral em que o País se situa, foram mencionados na END, os problemas atuais que as Forças Armadas enfrentam listando as vulnerabilidades da atual estrutura de defesa do País. Citamos algumas delas:

a) o baixo envolvimento da sociedade com os assuntos de defesa;

b) a descontinuidade de recursos financeiros para a defesa;

c) a defasagem tecnológica das Forças Armadas e a dependência de produtos de defesa estrangeiros;

d) a ausência de carreira civil na área de defesa;

---

27 Infraestrutura Crítica (IC): "instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional", extraída do Guia de Referência para a Segurança das Infraestruturas Críticas da Informação do Gabinete de Segurança Institucional da Presidência da República do Brasil.

28 GPS: (global positioning system) é um sistema de posicionamento global por satélite que fornece a um aparelho receptor móvel a sua posição. Encontram-se em funcionamento dois sistemas: o GPS norte-americano e o GLONASS russo. Outros dois sistemas estão em fase de implementação: o *Galileo* da União Europeia e o *Compass* chinês. O sistema norte-americano é operado pelo Departamento de Defesa dos Estados Unidos. Inicialmente o seu uso era exclusivamente militar, estando atualmente disponível para uso civil gratuito. No entanto, poucas garantias apontam para que em tempo de guerra o uso civil seja mantido.

e) a pesquisa científica e tecnológica atrasada em relação ao desenvolvimento de material de emprego militar e produtos de defesa;

f) a ausência de programas para aquisição de produtos de defesa, calcados em planos plurianuais;

g) o isolamento tecnológico forçado pelos países desenvolvidos; e

h) a logística e a mobilização deficiente.

A atual END não aponta nenhuma ameaça militar concreta e definida, quer por forças adversas inimigas quer por agentes não estatais. Ela cita que as Forças Armadas devem estar preparadas para cumprir diversos tipos de missões. Nenhum aspecto cibernético foi considerado para a elaboração das hipóteses de emprego[29] na Estratégia Militar de Defesa. (BRASIL, 2013)

Na listagem de ações estratégicas, está previsto que, no setor cibernético, o Ministério da Defesa e o Ministério da Ciência Tecnologia e Inovação, por intermédio do Departamento de Ciência e Tecnologia do Exército, promoverão ações que contemplem a multidisciplinaridade e a dualidade das aplicações; o fomento da Base Industrial de Defesa com duplo viés: aquisição de conhecimento e geração de empregos; e a proteção das infraestruturas estratégicas, com ênfase para o desenvolvimento de soluções nacionais inovadoras. (END, 2012, p. 20)

Outros aspectos importantes observados nas ações estratégicas são os seguintes: a ênfase na integração de todos os órgãos do Sistema Brasileiro de Inteligência (SISBIN); o desenvolvimento que amplie a capacidade de comunicações, meteorologia e sensoriamento remoto com satélites nacionais; a busca de parcerias nas áreas cibernética, nuclear e espacial

29 HIPÓTESE DE EMPREGO – Antevisão de possível emprego das Forças Armadas em determinada situação ou área de interesse estratégico para a Defesa Nacional. É formulada considerando-se o alto grau de indeterminação e imprevisibilidade de ameaças ao País, sendo perfeitamente caracterizada e mensurável. Com base nas hipóteses de emprego, serão elaborados e mantidos atualizados os planos estratégicos e operacionais pertinentes, visando a possibilitar o contínuo aprestamento do Poder Nacional como um todo, e em particular do Poder Militar, para emprego na defesa dos interesses nacionais. (MD, 2007, p. 129)

com as Forças Armadas das nações amigas; a busca de maior integração e participação dos setores civis governamentais nos assuntos afetos à defesa bem como a participação efetiva da sociedade brasileira através de uma Política de Ensino de Defesa e de convênios com entidades correlacionadas aos assuntos estratégicos de defesa.

Em 2010, o Gabinete de Segurança Institucional da Presidência da República publicou o "Livro Verde – Segurança Cibernética no Brasil". Elaborado por um grupo técnico com opiniões de especialistas de diferentes órgãos da Administração Pública Federal, o documento reúne propostas de diretrizes básicas relacionadas a Segurança Cibernética visando seu aprimoramento e também servir como subsídio para a Política Nacional de Segurança Cibernética – ainda não publicada.

O Livro Verde, apesar de não ter sido atualizado com a END 2012, traz os primeiros passos, as condições iniciais necessárias para as exigências de uma segurança cibernética para a proteção do Estado no cenário atual. É o documento que mais se aproxima dos documentos internacionais chamados de "Cyber Security Strategy"[30].

De acordo com o Livro Verde, devemos focar em algumas áreas visando a segurança cibernética: combate ao crime cibernético, criação a nível nacional de CERTs/CSIRTs[31], promoção da educação e de uma cultura de segurança, pesquisa, avaliação de risco e monitoramento, e atendimento às necessidades de pequenas e médias empresas.

O Livro Verde listou diversos desafios do país em vetores: Político-estratégico, Econômico, Social e Ambiental, CT&I, Educação, Legal, Cooperação Internacional, e Segurança das Infraestruturas Críticas.

Do ponto de vista legal, não existe regulação e mecanismos de certificação de segurança cibernética além de não existir legislação nacional e internacional específica de segurança cibernética, em especial contra crimes cibernéticos. Houve um avanço em 2012,

30 Estratégia de Segurança Cibernética
31 Computer Emergency Response Teams/Computer Security Incident Response Teams

ainda tímido, com a publicação da Lei Carolina Dieckman (como ficou conhecida a Lei 12.737/2012) que alterou o Código Penal tipificando os crimes informáticos. Segundo Macedo (2013), muitos juristas e criminalistas, entretanto, apontam falhas nesta Lei[32].

A Política Nacional de Segurança Cibernética, ainda não publicada, deverá prover quantidade significativa de recursos financeiros específicos, fortalecer os setores de pesquisa básica e avançada e regular o mercado de Segurança Cibernética. O país deverá se manter como um dos principais protagonistas para a construção de marco legal no cenário internacional como a criação de uma Convenção na ONU. Acordos bilaterais e entre blocos (Mercosul, Unasul, BRICS etc) deverão ser incentivados.

3.2 Outros casos

Diferentemente do Brasil que ainda não publicou uma Política ou Estratégia Cibernética, países de economias desenvolvidas estão, desde 2010, revisando ou divulgando suas "Estratégias nacionais de segurança cibernética", indicando que ainda há muito o que fazer, particularmente em termos de cooperação internacional, legislação nacional e internacional, normalização e preparo de recursos humanos especializados. Analisaremos a seguir alguns países protagonistas no espaço virtual.

3.2.1 Estados Unidos da América

Os EUA desenvolveram armas cibernéticas baseados em suas tecnologias disponíveis no início do século porém sem uma estratégia bem definida. Em 2010 foi criado o USCYBERCOM[33] para a condução de um novo tipo de guerra de elevada tecnologia porém

32 http://politica.estadao.com.br/noticias/geral,juristas-e-criminalistas-apontam-falhas-na-lei-carolina-dieckmann,1016111

33 Comando militar cibernético dos EUA

sem que antes houvesse debate público, análise acadêmica ou discursos internacionais[34] (CLARKE; KNAKE, 2015).

Força Aérea, Exército e Marinha se reorganizaram, nessa ordem, com a ativação da 24ª Força Aérea, a criação dos batalhões *NetWar* do Exército e a reativação da 10ª Esquadra (sem Navios), todos inteiramente voltados para operações no espectro cibernético.

O USCYBERCOM fica localizado junto à *National Security Agency* (NSA) e o seu comandante também é o diretor da agência. O comando único permite ao governo norte-americano operar com eficiência, maximizando as capacidades operacionais.

A NSA opera o sistema de vigilância global de comunicações e de espionagem ECHELON que foi amplamente usado para rastrear as atividades terroristas no pós 11 de setembro de 2001 e hoje é acusada de supostamente monitorar bilhões de comunicações privadas em todo o mundo. A agência compartilha informação secreta com a aliança de inteligência dos cinco países anglófonos conhecida como *Five Eyes*[35]

Em 2011, foi publicada a primeira estratégia cibernética do Departamento de Defesa (DoD). No documento, o próprio sub-secretário de Defesa, William J. Lynn III, exaltou a complexidade da missão: “We do not know the exact way in which cyber will figure in the execution of DOD’s mission, or the precise scenarios that will arise.” (EUA, 2011)

Ele também deixou claro a elevada dependência do país em tecnologia da informação tanto para as operações quanto para a sociedade norte-americana e que os adversários tentarão atingir esta dependência para ganhar uma vantagem estratégica.

Em novembro de 2014, provavelmente em retaliação ao lançamento do filme "A Entrevista", da *Sony Pictures*, uma comédia sobre um assassinato fictício do líder norte-

34 Em 2007 foi criado, provisoriamente, um cibercomando dentro da Força Aérea.
35 EUA, Reino Unido, Austrália, Canadá e Nova Zelândia

coreano Kim Jong Un, a Coreia do Norte realizou um ataque cibernético[36] contra a *Sony*, tornando inoperantes milhares de computadores além de roubar uma série de filmes inéditos.

O ataque à *Sony Pictures* foi considerado um dos mais destrutivos contra uma empresa em solo norte-americano (EUA, 2015a, p. 10) e estimulou o debate nacional sobre a natureza da ameaça cibernética e da necessidade de melhoria da segurança cibernética.

Na nova estratégia, publicada em 2015, o Diretor de Inteligência Nacional atribuiu a ameaça cibernética como a ameaça estratégica número um na frente inclusive do terrorismo que ocupou a primeira posição desde os atentados de 11 de setembro de 2001. Os potenciais adversários têm investido em cibernética pois proporciona uma alternativa exequível para atingir o território dos EUA e seus interesses. O texto publicado menciona que Rússia e China desenvolveram capacidades e estratégias cibernéticas avançadas exemplificando com o roubo de propriedade intelectual executado pela China e as intenções hostis executadas pela Rússia. Além destes, o documento aponta o Irã e a Coreia do Norte com intenções hostis menos desenvolvidas e o Estado Islâmico como ator não estatal. (EUA, 2015a, p. 17)

Por fim, a estratégia aponta que ameaças estatais e não estatais se misturam e que estas últimas podem fornecer cobertura para as primeiras dificultando a atribuição dos ataques conforme visto também em Clarke, Knake (2015).

O orçamento do USCYBERCOM foi de 120 milhões de dólares na sua criação, em 2010, subindo para 509 milhões em 2015[37].

A missão do Comando Cibernético é defender o Departamento de Defesa (DoD) e órgãos do governo. Quando se trata de defender alvos civis nos Estados Unidos, a estratégia se dirige para o Departamento de Segurança Interna (DHS). Clarke (2015) afirma que ainda não há planos ou recursos para defender a infraestrutura civil. Analistas da NSA acreditam

36 http://g1.globo.com/tecnologia/noticia/2014/12/eua-suspeitam-que-coreia-do-norte-teve-ajuda-no-ataque-sony-pictures.html

37 http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/27/us-cyber-command-budget-expand-fort-meade-offensive/28829321/

que essa missão deve ser atribuída ao Departamento de Segurança Interna (DHS), mas nem o DoD nem o DHS possuem, atualmente, capacidade de defender o ciberespaço corporativo que faz a maior parte do país funcionar.

A importância do ciberespaço e da guerra cibernética para os norte-americanos mostra sua força quando menciona que "O Departamento de Defesa (DoD) realizará missões cinéticas para preservar a liberdade de ação e a vantagem estratégica no ciberespaço".

O documento reconhece que os adversários poderão tirar proveito da dependência dos Estados Unidos pelo ciberespaço e que sem um esforço relevante serão guiados a perder a vantagem cibernética. Embora possa parecer que os Estados Unidos tenham certa vantagem, o fato é que a guerra cibernética oferece a este país um risco maior do que para qualquer outra nação. (CLARKE; KNAKE, 2015, p. 40 a 42)

No campo diplomático, os EUA já estabeleceram diversos acordos bilaterais com outros países amigos[38] a fim de unir forças eficazes no combate as ameaças comuns no domínio cibernético. Desenvolveram uma Estratégia Internacional para o ciberespaço na forma de convite a outros Estados em prol da prosperidade do mundo em rede. Possui apontamentos nos níveis políticos, econômicos, militares, e de governança para os setores privados, sociedades civis e usuários finais. (EUA, 2011)

Por fim, desde junho de 2016[39], os líderes do Pentágono, trabalham para definir quando, exatamente, um ciberataque contra os EUA representa um ato de guerra, e quando, exatamente, o Departamento de Defesa responderia a um ciberataque contra a infraestrutura civil. O seguinte texto ainda precisa ser aprovado no Congresso:

> "Quando se justifique, os Estados Unidos vão responder a atos hostis no ciberespaço como faríamos com qualquer outra ameaça ao nosso país. Reservamo-nos o direito de usar todos os meios necessários – diplomática, informativa, militares e econômicos – como apropriadas e consistentes com o direito internacional aplicável, a fim de defender a nossa nação, nossos

38 Como é o caso de Israel. Ver http://www.defensenews.com/story/defense/2016/06/21/us-israel-sign-cyber-defense-declaration/86195530/

39 http://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html

> aliados, nossos parceiros e nossos interesses". (EUA, 2011, p. 14) (Tradução nossa)[40]

O Senado, através da publicação em maio do *Cyber Act of War*[41], exigiu que o presidente, em 180 dias, desenvolvesse uma política de ação no ciberespaço considerando as formas pelas quais os efeitos de um ataque cibernético pode ser equivalente aos efeitos de um ataque com armas convencionais, inclusive com relação à destruição física ou vítimas; e os efeitos intangíveis de significativo alcance, intensidade ou duração.

A perda de vidas resultante de um ataque contra a rede elétrica que derruba a energia nos hospitais constituiria um ato de conseqüências significativas? Não há consenso na resposta até agora.

Segundo a metodologia de Clarke e Knake (2015, p. 122), os EUA possuem elevada capacidade de ataque cibernético, elevada dependência cibernética e baixa capacidade de defesa cibernética.

3.2.2 Rússia

Clarke e Knake (2015, p. 22) aponta que nos episódios contra a Estônia e a Geórgia, na verdade, os russos demonstraram bastante moderação no uso de suas armas cibernéticas e, provavelmente, salvaguardaram suas melhores armas cibernéticas para quando realmente precisarem delas, em um conflito em que a OTAN e os Estados Unidos estiverem envolvidos.

A Rússia e a China assinaram um termo de cooperação digital em maio de 2015 no qual os dois países se comprometem a não realizar ataques cibernéticos um contra o outro[42].

40 When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means - diplomatic, informational, military, and economic - as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.

41 https://www.congress.gov/bill/114th-congress/senate-bill/2905/text

42 http://g1.globo.com/tecnologia/noticia/2015/05/china-e-russia-firmam-acordo-de-paz-digital-para-nao-se-hackearem.html

No termo, os países devem se opor a tecnologias que possam “desestabilizar o ambiente político e socioeconômico interno”, “perturbar a ordem pública” ou “interferir com assuntos internos do estado”.

O presidente russo, Vladimir Putin, promulgou em julho de 2016 um conjunto de leis antiterroristas[43], enormemente rejeitadas, para intensificar a vigilância das comunicações, obrigando as empresas da internet a armazenar mensagens, chamadas e dados de usuários por seis meses e entregar para as agências governamentais. A oposição e o ex-consultor da agência norte-americana de segurança *NSA*, Edward Snowden, refugiado na Rússia, criticaram o ato como esforço de monitoramento generalizado pelas autoridades.

Grossmann (2015) nos lembra que a desvinculação entre o governo americano e a ICANN[44] está prevista para o final de 2016[45] e que a transição da governança da Internet para uma organização independente é apoiada pelo presidente norte-americano Barack Obama enquanto a oposição sustenta que ele “está entregando a internet para a Rússia e China”. Estes dois países são a favor de alterações na condução e governança da internet.

Como visto no capítulo anterior, foram os russos os protagonistas da guerra cibernética na Estônia. Conforme Chiaretti (2015), o país é conhecido internacionalmente por possuir crackers extremamente competentes mas, atualmente, cedeu seu lugar a China[46], segunda economia do mundo[47] e atual superpotência rival dos EUA.

Segundo a metodologia de Clarke e Knake (2015, p. 122), a Rússia possui elevada capacidade de ataque cibernético, mediana dependência cibernética e mediana capacidade de defesa cibernética.

---

43 http://www.defesanet.com.br/cyberwar/noticia/22859/Putin-promulga-serie-polemica-de-leis-antiterroristas/

44 ICANN (acrônimo em inglês para Corporação da Internet para Atribuição de Nomes e Números). Subordinada ao governo dos EUA.

45 http://www.abranet.org.br/Noticias/Governanca-da-Internet%3A-Fim-do-contrato-da-ICANN-e-adiado-para-o-final-de-2016-689.html?from_info_index=281#.V5LlIrgrK01

46 http://www1.folha.uol.com.br/ilustrissima/2015/01/1572753-eua-e-china-sao-protagonistas-da-era-da-guerra-cibernetica.shtml

47 Banco de dados macroeconômicos do Fundo Monetário Internacional http://www.imf.org/external/pubs/ft/weo/2016/01/weodata/index.aspx

3.2.3 China

A Estratégia Militar da China[48], publicada em 2015, não trouxe novidades para os analistas do mundo oriental mas divulgou, pela primeira vez, o compromisso chinês de construção de uma Força cibernética capaz de se envolver em ações ofensivas.

Segundo relatórios da *Freedom House*, organização independente dedicada à expansão da liberdade e da democracia em todo o mundo, a China figura no topo da lista de países que mais censuram na Internet[49]. O Projeto Escudo Dourado, também chamado de Grande *Firewall* da China[50], é um projeto de vigilância e de censura operado pelo governo chinês desde 2003[51]. Ele bloqueia serviços ocidentais famosos como o *Google*, o *Facebook*, e o *Youtube*. Nos últimos anos, o programa foi aperfeiçoado e hoje bloqueia seletivamente páginas com termos "sensíveis" pelo governo, em vez de uma censura completa de sites. A ideia é fazer com que os quase 700 milhões de internautas chineses se comuniquem com o resto do mundo, mas, ao mesmo tempo, bloquear as opiniões ocidentais usadas como ferramenta ideológica. A censura poderia deixar de existir no futuro caso a influência chinesa avance no mundo e a internet se desprenda da herança ideológica ocidental[52].

Em pronunciamento recente, o Presidente chinês disse que cada país deve controlar a sua internet[53]:

> Tal como no mundo real, a liberdade e a ordem são ambas necessárias no ciberespaço. A liberdade tem na base a ordem e a ordem é a garantia da liberdade. Devemos usar os ensinamentos morais para a Internet (SONG, 2015).

48 http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm
49 https://freedomhouse.org/report/freedom-net/freedom-net-2015
50 http://agenciabrasil.ebc.com.br/geral/noticia/2016-02/china-reforca-censura-conteudos-publicados-na-internet
51 http://www.rfa.org/english/commentaries/china_internet-11242008134108.html
52 http://economia.uol.com.br/noticias/efe/2016/04/11/imprensa-oficial-chinesa-defende-censura-as-revistas-time-e-the-economist.htm
53 http://www.dn.pt/mundo/interior/presidente-chines-diz-que-cada-pais-deve-controlar-a-sua-internet-4932656.html

Segundo a metodologia de Clarke e Knake (2015, p. 122), a China possui mediana capacidade de ataque cibernético, mediana dependência cibernética e alta capacidade de defesa cibernética.

3.2.4 Coreia do Norte

O governo autoritário da Coreia do Norte pode cortar sua limitada conexão ao ciberespaço de maneira simples e eficaz além de possuir pouca infraestrutura crítica dependente do ciberespaço. Um grande ataque cibernético contra o país não causaria dano (CLARKE; KNAKE,2015).

Segundo a metodologia de Clarke e Knake (2015, p. 122), a Coreia do Norte possui fraca capacidade de ataque cibernético, baixíssima dependência cibernética e elevada capacidade de defesa cibernética.

3.2.5 Países euro-asiáticos da OTAN[54]

A Estônia, curiosamente, é um dos países mais conectados do mundo, competindo com a Coreia do Sul, e bem à frente dos Estados Unidos, na utilização de aplicações de Internet e na penetração de banda larga na vida cotidiana. (CLARKE; KNAKE,2015)

Na reunião de cúpula em junho de 2016[55], ministros da Defesa dos países membros da OTAN nomearam o ciberespaço como um domínio operacional, unindo terra, mar, ar e espaço. Isto criou a possibilidade de invocar o artigo 5º do Tratado em resposta a um ciberataque. Interpretando e atualizando o artigo significa que um ataque – agora incluindo um ataque cibernético – contra um aliado da OTAN é considerado um ataque contra todos os membros da aliança militar. No entanto, apesar da declaração, ainda não está claro perante o

54 Organização do Tratado do Atlântico Norte. É uma aliança militar intergovernamental.
55 http://www.c4isrnet.com/story/military-tech/blog/net-defense/2016/06/23/nato-extends-article-5-powers-cyber/86298254/

Direito Internacional, conforme visto no capítulo anterior, quando um ciberataque se torna um ato de guerra assim como a participação de atores não Estatais.

Os especialistas militares e civis em segurança computacional de 26 países participaram em maio do *Locked Shields* 2016[56], um exercício internacional indispensável de defesa cibernética em tempo real promovido pelo CCDCOE[57] da OTAN. O exercício simulava a defesa das infraestruturas críticas de um país invadidas por cibercriminosos. Os eslovacos ganharam o prêmio pela melhor defesa.

O CCDCOE promove desde 2008 vários eventos para aumentar a capacidade, a cooperação e o intercâmbio de informações entre os países-membros da OTAN, países e parceiros em defesa cibernética, dentre os quais destacam-se: exercícios de defesa cibernética, *workshops*, conferências de segurança cibernética, cursos técnicos, cursos em direito internacional etc.

Finalizando este capítulo, podemos perceber que vários países estão hoje criando ou atualizando suas estratégicas cibernéticas. E graças a Snowden e outros atores, várias agências de governo – de países democráticos e autoritários – estão ativamente envolvidas em espionagem, sabotagem e ataques cibernéticos. Os ataques de 11/9 popularizaram o conceito de guerra assimétrica[58]. Os ataques cibernéticos, cada vez mais fortes, provenientes de não-democracias contra governos democráticos e suas empresas privadas, centros científicos, fundações e organizações da sociedade civil é uma nova forma de assimetria para os quais os países democráticos, incluindo o Brasil, carecem de respostas eficazes.

---

56 https://ccdcoe.org/locked-shields-2016.html

57 Cooperative Cyber Defense Centre of Excellence. Localizado em Tallin (Estônia).

58 GUERRA ASSIMÉTRICA – 1. Conflito caracterizado pelo emprego de meios não convencionais contra o oponente, normalmente pela parte que se encontra muito inferiorizada em meios de combate. 2. Conflito armado que contrapõe dois poderes militares que guardam entre si marcantes diferenças de capacidades e possibilidades. Trata-se de enfrentamento entre um determinado partido e outro com esmagadora superioridade de poder militar sobre o primeiro. Neste caso, normalmente o partido mais fraco adota majoritariamente técnicas, táticas e procedimentos típicos da guerra irregular. (MD, 2007, p. 123)

4 OS PRÓXIMOS PASSOS PARA A ESTRATÉGIA CIBERNÉTICA BRASILEIRA

A CPI da Espionagem apontou a fragilidade do sistema de telecomunicações brasileiro e de nosso sistema de inteligência e defesa cibernética frente a espionagem eletrônica internacional e sugere medidas e propostas para a melhoria da segurança cibernética nacional.

O relatório considera que o Brasil deve desenvolver mecanismos de proteção do conhecimento e de segurança cibernética e propõe investimentos em inteligência e em contrainteligência, com um esforço especial no desenvolvimento de tecnologias próprias e nacionais e de quadros capacitados. Sugere ainda uma série de medidas a serem tomadas pelo governo federal para investimentos. Entre elas, mais dinheiro para os serviços secretos, a compra e o desenvolvimento de equipamentos, integração entre os órgãos que compõem o Sistema Brasileiro de Inteligência (SISBIN) e a capacitação de profissionais. Propõe também uma legislação que ampare o setor de inteligência e permita que o pessoal da área atue em defesa do Estado e da sociedade.

Muitas das considerações do relatório podem e devem ser levados em consideração também por Estados e Municípios.

Neste capítulo será apresentado o que está sendo realizado e que caminhos faltam ainda percorrer para a consolidação da Estratégia Cibernética Brasileira.

4.1 Legislação de defesa nacional

Apesar da Lei 9.883/99 ter instituído o SISBIN e criado a Agência Brasileira de Inteligência (ABIN), a fixação da Política Nacional de Inteligência (PNI), prevista em seu artigo 5º, só veio a ocorrer em junho de 2016 por decreto[59] do vice-presidente da República, então presidente em exercício após afastamento da presidente eleita por processo de

59 http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8793.htm

impeachment. Marco legal, a PNI deverá, finalmente, orientar a atuação de todos os órgãos de inteligência em toda a esfera pública.

Foi apontado em Brasil (2014) que o país precisa estabelecer uma Política Nacional de Inteligência de Sinais para a implementação de medidas de proteção e defesa, para garantir maior segurança no campo cibernético. A criação de uma Agência Brasileira de Inteligência de Sinais foi recomendada por especialistas entrevistados com a tarefa de "operar no ambiente virtual tanto na busca de dados de interesse do Brasil, quanto na proteção dos ativos nacionais nessa área". (BRASIL, 2014, p. 138)

Foi proposta a criação de uma comissão temporária no Senado para avaliar e aperfeiçoar a legislação que trata da defesa e inteligência nacionais. Além disso, o relatório defendeu a aprovação de proposta de emenda à Constituição (PEC) que dá status constitucional à atividade de inteligência. A PEC 398/2009, proposta pela Câmara dos Deputados foi arquivada devido ao fim da legislatura do autor. A PEC 331/2013 também foi arquivada pelo mesmo motivo. A PEC 67/2012, proposta no final de 2012 por 34 senadores encontra-se ainda na pauta para ser discutida. Ela prevê garantias aos cidadãos e aos setores de inteligência em suas atividades de produção e proteção ao conhecimento e dispõe sobre mecanismos de controle dos serviços secretos. (BRASIL, 2014)

A lei de mobilização nacional deverá ser atualizada visando adequar as necessidades de mobilização do pessoal a ser empregado na Segurança Cibernética. Um levantamento de equipamentos, pessoal e instalações, passíveis de serem mobilizados, deverá ser realizado com um esforço interagências.

A presidente Dilma Rousseff sancionou a Lei 12.965/2014[60] na cerimônia de abertura do NETmundial - Encontro multissetorial global sobre o futuro da Governança da Internet[61]. O encontro, organizado pelo Comitê Gestor da Internet no Brasil (CGI.br) contou

60 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
61 http://netmundial.br/

com as participações do subsecretário-geral da Organização das Nações Unidas (ONU), de representantes de governos de 80 países, de representantes da sociedade civil, universidades, empresas e organizações internacionais[62].

O encontro ocorreu fruto do discurso da presidente Dilma Rousseff defendendo um marco civil multilateral para a governança e proteção de dados da internet na abertura da Assembleia Geral da ONU em 2013.

O Marco Civil da Internet, como ficou conhecida a Lei 12.965/2014, foi muito elogiado por diversas organizações e personalidades, dentre elas, Tim Berners-Lee, considerado o pai da Internet, que afirmou: "O Brasil está partindo na direção certa, porque parte da perspectiva de direitos humanos da questão" (SANTANA, 2013). Conforme visto em McCarthy (2014), em seu discurso, Tim mencionou a iniciativa da lei como "fantástico exemplo de como os governos podem desempenhar um papel positivo na promoção dos direitos da Internet e mantê-la aberta"[63] e apelou para outros países a seguirem o mesmo caminho.

O Marco Civil da Internet foi regulamentado pelo decreto presidencial nº 8.771[64] em maio de 2016. Segundo observa Gomes (2016), o texto estabeleceu que dados trafegando na rede não podem ser discriminados de acordo com seu conteúdo (princípio da neutralidade) exceto em situações de emergência e de urgência técnica, como a disseminação de spam e durante ataques hackers[65]. Outro tema polêmico regulamentado foi o que versa sobre a guarda e a inviolabilidade de dados de brasileiros frente as empresas estrangeiras prestadoras de serviço que deverão respeitar a legislação do país e entregar informações quando requisitadas pela Justiça. Caso contrário, enfrentarão sanções entre advertência, multa de até 10% de seu faturamento, suspensão das atividades ou proibição de atuação. A Justiça brasileira já

62 http://exame.abril.com.br/tecnologia/noticias/80-paises-se-reunem-para-debater-governanca-da-internet
63 http://www.theregister.co.uk/2014/04/23/new_bill_signed_in_brazil_guaranteeing_civil_rights_on_internet/
64 http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm
65 http://g1.globo.com/tecnologia/noticia/2016/05/ataque-hacker-whatsapp-gratis-marco-civil-da-internet-ganha-regras.html

bloqueou bens e serviços de redes sociais como o *Facebook* e o *Whatsapp* por não contribuírem nas investigações criminosas com a quebra do sigilo de mensagens trocadas em seus serviços (DEMARTINI, 2016).

4.2 Defesa cibernética nacional

O Exército Brasileiro (EB) está desenvolvendo dez projetos estratégicos[66] de Defesa Cibernética dentre os quais podemos destacar: arcabouço documental; estrutura de capacitação e de preparo e emprego da Força Cibernética; a Rede Nacional da Segurança da Informação e Criptografia (RENASIC); e Rádio Definido por Software (RDS).

Além disso, o EB está construindo a Escola Nacional de Defesa Cibernética (ENaDCiber). O projeto foi encomendado à Universidade de Brasília (UnB) mas ainda não foi entregue e não existe data para o início das atividades. A Escola servirá para a capacitação de recursos humanos para atuação no setor cibernético em prol da defesa do país. Hoje, essa capacitação cabe ao Centro de Defesa Cibernética (CDCiber). Com a implementação da Escola, o CDCiber poderá se concentrar nas operações de guerra cibernética.

A ENaDCiber terá uma sede física mas os cursos serão espalhados por todo o país, em parcerias com universidades e centros técnicos. A metodologia de ensino da futura escola precisa ser muito bem concebida pois as pessoas que se interessam nessa área normalmente aprendem de forma autônoma diferentemente do sistema tradicional de ensino.

O Instituto Militar de Engenharia (IME) criou o Laboratório de Defesa Cibernética (LabDCiber-IME) que tem como principal objetivo a formação especializada de recursos humanos voltados para o setor cibernético. O Laboratório conta com as parcerias do Laboratório Nacional de Computação Científica (LNCC), vinculado ao Ministério da Ciência,

66 http://www.epex.eb.mil.br/index.php/defesa-cibernetica/escopodciber

Tecnologia e Inovação (MCTI); e da Rede Nacional de Segurança da Informação e Criptografia, vinculada ao CDCiber.

O Comando de Defesa Cibernética (ComDCiber) foi ativado junto a criação da ENaDCiber e passou a contar, desde julho de 2015, com militares das três Forças Armadas mas, apesar dos significativos avanços, ainda conta com efetivo reduzido.

4.3 Cultura de segurança e educação

Segundo o senador Ricardo Ferraço, relator da CPI da espionagem, é necessário que os governantes brasileiros promovam, entre a população, "uma cultura de segurança e inteligência". Campanhas educativas, cursos de capacitação e inclusão do tema nas diversas modalidades de ensino (do básico ao superior) para mostrar que cada cidadão também é responsável pela própria segurança eletrônica. Até mesmo uma criança já deve saber, por exemplo, dos riscos do compartilhamento de senhas, do uso incorreto de celulares etc.

O país deverá elaborar e manter atualizado um banco de talentos e, ao mesmo tempo, aumentar a massa crítica de especialistas incentivando o ensino superior, público e privado, para formar profissionais em segurança cibernética. (BRASIL, 2014, p. 160)

Deverá estabelecer, pela via diplomática, convênios internacionais com centros universitários e centros especializados como o United States Naval War College e o Cooperative Cyber Defence Centre of Excellence (CCD CoE), em Tallinn, Estônia. O Brasil poderá incentivar a criação de exercícios de segurança cibernética bem como participar dos exercícios internacionais como forma de incrementar a discussão e as experiências com outros atores globais.

4.4 Estrutura Nacional de Segurança Cibernética

Desde a sua inauguração em 2012, o CDCiber desenvolve e executa vários projetos para a Defesa Cibernética contribuindo para o incremento da segurança e da proteção das infraestruturas estratégicas nacionais.

O Centro posicionou a questão cibernética em seu patamar de relevância capacitando e aperfeiçoando recursos humanos, civis e militares, para realizar ações cibernéticas bem como coordenando projetos com as universidades e empresas do governo (ex.: UnB e SERPRO).

Destacam-se as recentes participações efetivas do CDCiber: Conferência da ONU sobre desenvolvimento sustentável "Rio+20" em 2012; Jornada Mundial da Juventude e Copa das Confederações FIFA em 2013; Copa do Mundo FIFA 2014; Operações conjuntas Laçador, Ágata, Dínamo, Atlântico e Panamax; estágios, fóruns e competições internacionais. (LOUREIRO, 2016)

Apesar do louvor merecido, muitos especialistas ouvidos nas audiências do Senado Federal (Brasil, 2014) acreditam que é necessário ir além do CDCiber. Como previsto, sua missão é coordenar e integrar as atividades de Defesa Cibernética no âmbito do Ministério da Defesa (MD). Para aqueles, o caráter eminentemente militar, foca na defesa nacional na perspectiva da guerra cibernética e falta um órgão análogo ao CDCiber para a segurança cibernética das infraestruturas e operações civis. O novo órgão, conforme Fragola (2016), especialista em defesa cibernética, poderia abranger os projetos para desenvolvimento da indústria e aumentar a massa crítica, no âmbito do MEC, de intelectuais no setor. A iniciativa do CDCiber deve servir de estímulo para um avanço além da tutela das forças armadas. Poderíamos adotar um modelo análogo ao dos EUA que possuem o *Department of Defense* (DoD), para proteção das infraestruturas críticas do governo, e o *Department of Homeland*

Security (DHS), para regular a atuação das empresas do setor privado na operação de sistemas de telecomunicações, de transporte e de distribuição de água etc.

4.5 Segurança das infraestruturas críticas nacionais

Infraestruturas críticas são todas as estruturas físicas e serviços que, se forem interrompidos ou destruídos total ou parcialmente, poderão provocar impactos social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade de maneira isolada ou concomitante.

Vários incidentes internacionais de segurança em sistemas de controle e automação industrial já foram reportados como a sabotagem das centrífugas de enriquecimento de urânio no Irã; a interrupção do tráfego ferroviário; a perda de controle na usina de tratamento de água e do controle das turbinas na usina de aço da Alemanha; linha de produção automobilística inoperante; sistemas bancários fora do ar etc.

Segundo o relatório final da CPI da espionagem, o setor privado e, principalmente, o Estado, investem ainda de maneira tímida na proteção das infraestruturas críticas e na maioria das vezes de forma isolada. Faz-se necessário identificar, conhecer e integrar todas essas infraestruturas para aumentar a segurança nacional conforme estabelecido na END. Tarefa esta atribuída a vários órgãos dos Ministérios da Defesa, Comunicações, Minas e Energia, Transportes e Integração Nacional.

O governo federal deverá obter informações sobre a vulnerabilidades críticas dos principais setores da sociedade e fomentar os órgãos públicos com recursos humanos, tecnológicos e financeiros para a utilização de sistemas que permitam, nos setores público e privado, identificar, analisar, avaliar e tratar os riscos conjuntos das infraestruturas críticas de maneira coordenada e integrada.

4.6 Desenvolvimento tecnológico nacional

Conforme dito por especialistas nas audiências da CPI, a arquitetura da Internet foi concebida para concentrar o tráfego de dados nos Estados Unidos e, atualmente, 90% do tráfego de informações que sai do Brasil passa pelo território norte-americano, ainda que se destine a outras localidades.

Para minimizar a dependência externa, é preciso investir em produtos e serviços nacionais destacando-se:

a) o investimento em satélites e cabos submarinos de comunicação próprios, conforme aponta a Estratégia Nacional de Defesa;

b) a multiplicação de *datacenters* e o arquivamento na "nuvem" no país;

c) o desenvolvimento de *software* livre e de um correio eletrônico nacional para uso do governo e, futuramente, da população; e

d) a criação de criptografia de dados genuinamente brasileira.

Os *softwares* pagos passam a impressão de que são mais seguros que os livres, mas, na verdade, por terem código aberto, os livres podem ser modificados, aperfeiçoados e auditados diferentemente de *softwares* proprietário estrangeiros que podem possuir *backdoors*[67] sem possibilidade de auditoria. Segundo relatos do representante da SERPRO (BRASIL, 2014), o programa para declaração do imposto de renda desde 2012 é desenvolvido integralmente em software livre, o que atende também à necessidade de portabilidade. Dessa forma, o programa pode ser utilizado em qualquer sistema operacional além da Microsoft.

Em termos de *hardware*, as universidades brasileiras já possuem capacidade de desenvolver roteadores com elevada transferência de dados, compatíveis com os internacionais.

---

67 Backdoor é um utilitário de administração remota que, uma vez instalado em um computador, permite um acesso de usuário e controlá-lo através de uma rede ou da Internet. Para saber mais: http://www.crimespelainternet.com.br/entenda-o-que-um-backdoor/

Paralelamente ao desenvolvimento de *hardware* e *software* nacionais, deverá ser criado e adotado um sistema de criptografia brasileiro. O uso de criptografia normalmente ocorre com algoritmos de criptografia estrangeiros e apenas no chaveamento do caminho de mensagens. Com o desenvolvimento de sistemas criptográficos nacionais, seu uso deverá também se estender para o conteúdo integral das mensagens.

A existência de *backdoors* nos programas de correio eletrônico *Outlook* e *BlackBerry* já foram detectadas [68] [69] Ainda falta uma mentalidade de inteligência em todos os indivíduos até mesmo em chefes de Estado. Muitos ainda misturam correspondências particulares com as de trabalho.

O SERPRO vem desenvolvendo o programa de correio eletrônico "Expresso" que será adotado pela Administração Pública Federal[70]. Ele já se encontra operacional e possui as características de hospedar todas as mensagens nos servidores próprios da SERPRO e todo o conteúdo das mensagens ser criptografado. Apesar do programa já possuir reconhecimento internacional e ter um custo menor, ele possui baixa aderência nas instituições do próprio governo. Na Marinha do Brasil, por exemplo, a dificuldade é migrar os milhões de *bytes* da plataforma *IBM Lotus Notes* para o Expresso.

O SERPRO vem desenvolvendo, também, a nuvem de Governo com uso de *software* livre desde 2012 e redes sociais semelhantes ao *Facebook* e *Twitter.*

No setor espacial, a Visiona – *joint-venture* da Embraer e a Telebras – foi contratada para desenvolver o projeto do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC) com o objetivo de assegurar a soberania nas comunicações estratégicas brasileiras. O satélite será operado pelo Ministério da Defesa na banda X (militar) e pela Telebras na banda Ka (civil). As comunicações satelitais, o controle da órbita e da altitude do

68 http://www.scmagazine.com/backdoor-in-ms-outlook-webmail-raises-security-doubts/article/443415/
69 https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how
70 http://www.ebc.com.br/noticias/brasil/2013/10/correio-eletronico-do-governo-sera-ativado-em-novembro

satélite será feito dentro do País por instituições nacionais. O tráfego de voz e dados ocorrerão por rede própria permitindo a troca segura de informações governamentais[71] colocando um fim na vigilância estrangeira. (MC, 2015)

O satélite permitirá, além da cobertura plena do território nacional, uma cobertura regional (América Central e do Sul, Atlântico Norte e Sul, e costa oriental da África) satisfazendo os interesses do Poder Naval especialmente na Amazônia Azul[72].

4.7 Cooperação internacional

Finalmente, a segurança da informação e das comunicações não pode ser obtida com os esforços de um país isolado, pois as redes são integradas e as ameaças tendem a ter caráter global. Para que seja efetiva, a coordenação internacional deve ser institucionalizada, tanto no governo quanto no setor privado. Nesse particular, as organizações internacionais do setor têm papel essencial.

Da mesma forma que hackers compartilham, entre si, novas técnicas de invasão, os Estados também terão que compartilhar, entre si, dados e sistemas de informações para coordenarem a defesa das diversas infraestruturas críticas cada vez mais interligadas.

Segundo relatório da CPI da espionagem, além de redes de relacionamento internacionais para a troca de informações e experiências, o Brasil precisa estar apto a fornecer, a qualquer momento quando requisitado, equipes de resposta a incidentes fortalecendo os laços diplomáticos com os países envolvidos.

O Brasil, até o fechamento deste trabalho, já realizou acordos bilaterais com os seguintes países: África do Sul, Alemanha, Argentina, Bolívia, Canadá, Chile, China, Colômbia, Coréia do Sul, Equador, Espanha, EUA, França, Holanda, Índia, Israel, Itália,

71 http://www.mc.gov.br/sala-de-imprensa/todas-as-noticias/institucionais/36448-soberania-via-satelite
72 https://www.marinha.mil.br/content/amazonia-azul-0

Japão, México, Paraguai, Peru, Portugal, Reino Unido, Rússia, Sri Lanka, Suécia, Suriname, Turquia e Polônia. (LOUREIRO, 2016)

5 CONCLUSÃO

Este trabalho apresentou a relevância do assunto cibernético nos dias de hoje, o que está sendo feito no Brasil e em alguns países e que caminhos faltam ainda percorrer para a consolidação da Estratégia Cibernética Brasileira.

Procuramos demonstrar a compreensão da extensão das ameaças cibernéticas para indivíduos, empresas e governo, identificando medidas a serem adotadas com a finalidade de melhorar a consciência nacional brasileira quanto a segurança cibernética.

Inicialmente, a Guerra Cibernética foi apresentada como um novo tipo de conflito, não mais no campo da ficção e dos filmes futurísticos mas real e com perdas materiais e às vezes humanas.

Foi mencionado que o domínio cibernético possui características peculiares e distintas dos demais domínios convencionais (terrestre, marítimo, aéreo e espacial).

A Internet que foi concebida para ser uma ferramenta do bem, do desenvolvimento acadêmico, de pesquisas, passou a ser usada para comércio eletrônico e prática de crimes virtuais. A sua arquitetura é basicamente a mesma desde a sua criação e pessoas mal intencionadas passaram a explorar suas vulnerabilidades e desenvolveram técnicas de invasão e ataque sofisticadas.

Os ataques, que antes eram atribuídos a adolescentes aventureiros, aumentaram os danos e começaram a serem atribuídos também a atores Estatais sem contudo haver provas. Países com objetivos políticos e/ou econômicos os mais diversos passaram a observar a relação custo/benefício que tais ataques proporcionam. Os ataques maciços, vindos de computadores de várias partes do mundo contra a Estônia marcaram 2007 como o ano que a guerra cibernética deixou de ser mera ficção e se tornou realidade afetando governo, sistema financeiro e empresas de comunicações estonianas.

Os ataques e incidentes se expandiram em larga escala atingindo o que veio a se chamar de infraestruturas críticas que são os setores mais sensíveis, ou seja, instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sérios impactos sociais, econômicos, políticos e/ou internacionais. Prejuízos na ordem de milhões de dólares afetaram vários setores da economia como bancos, empresas de telecomunicações e centrífugas nucleares.

Diante dos prejuízos, os países se debruçaram no Direito Internacional que até então ainda não se manifestou claramente sobre os conflitos cibernéticos. A Carta da ONU, que data de 1945, ainda não foi atualizada para incluir este novo conflito entre Estados soberanos. Como visto neste trabalho, o problema se torna mais complexo com a realização de ataques por atores não estatais que não são contemplados pela Carta.

Apesar do silêncio da ONU, diversos especialistas se reuniram sob o esforço da OTAN e lançaram em 2013 o Manual de Tallin, livro acadêmico não vinculante mas que passou a ser adotado como referência na interpretação do Direito internacional aplicável a guerra cibernética.

Após evidenciar o conflito cibernético, o trabalho abordou como o Brasil e alguns países estão reagindo, analisando suas respectivas Estratégias Cibernéticas.

O Brasil foi alvo de intensa espionagem de dados conforme divulgação de Snowden, ex-agente da NSA, em maio de 2013. Até mesmo ligações telefônicas da presidente foram interceptadas fazendo com que o país apresentasse uma proposta de resolução na ONU. Internamente foi instalada uma CPI pelo Senado Federal que ao final de 180 dias não conseguiu apresentar a autoria de crimes mas apresentou as fragilidades da inteligência e da defesa cibernética nacional.

A Inteligência brasileira precisa ter status constitucional como atividade essencial de Estado e se desenvolver plenamente na esfera civil. Conforme vimos, a Política Nacional

de Inteligência só foi publicada neste ano, dezessete anos após a criação do SISBIN. O próprio Ministério da Defesa foi criado recentemente. A Estratégia Nacional de Defesa de 2012 aponta vários desafios a serem enfrentados e o país ainda não aprovou a Política Nacional de Segurança Cibernética. Urge identificar todas as infraestruturas críticas, públicas e privadas, e protegê-las de forma eficaz e coordenada.

Na estratégia cibernética dos EUA vimos que o país atribuiu a ameaça cibernética como a principal ameaça na frente inclusive do terrorismo. O país tem investido cada vez mais em defesa cibernética pois possui muita dependência tecnológica e tem conhecimento que seus adversários tem investido em ataques digitais. Possui agência de inteligência com capacidade de vigilância global nas telecomunicações e dados digitais, fato que a torna alvo de severas críticas internacionais. O país estabeleceu diversos acordos de cooperação com países amigos para operarem em conjunto no domínio cibernético e encontra-se no momento debatendo no Congresso quando um ciberataque contra os EUA representa um ato hostil e que meios apropriados poderiam ser empregados num contra-ataque.

A Rússia, considerada a precursora da guerra cibernética, assinou recentemente um termo de cooperação digital com a China e decretou um conjunto de leis aumentando a vigilância dos dados e obrigando o seu fornecimento por parte das empresas.

A China divulgou em 2015 a preocupação de criar um Força cibernética para realizar ações ofensivas. O governo opera um enorme sistema de vigilância e também de censura com a finalidade de preservar a identidade e valores chineses e não se contaminar pela influência ocidental.

A Coreia do Norte é considerado um ator cibernético relevante mas, por ser um país pequeno, possui a vantagem de poder se desligar da Internet sem maiores problemas para suas infraestruturas críticas.

Os países da OTAN atualizaram este ano a interpretação do artigo 5º do Tratado ao mencionar que um ataque cibernético contra um membro é considerado um ataque contra todos da aliança militar. Estes países seguem as orientações do Manual de Tallin, possuem um centro de excelência para assuntos de segurança cibernética e realizam exercícios entre seus membros de forma regular.

Por fim, apresentamos uma proposta de ações a serem feitas para o desenvolvimento da estratégia cibernética brasileira. O país precisa seguir as prioridades estabelecidas pela END; fomentar a mentalidade de inteligência e segurança com a Política Nacional de Inteligência recém-estabelecida propondo emendas a Constituição e atualização de leis federais; capacitar pessoal civil e militar; estudar a criação de um centro coordenador para o setor privado; conhecer em profundidade a infraestrutura crítica nacional e integrar a resposta a incidentes; participar de treinamentos, intercâmbios e exercícios internacionais; protagonizar no cenário externo e promover acordos bilaterais e multilaterais de cooperação; desenvolver satélites, cabos submarinos, datacenters, software de correio eletrônico e criptografia genuinamente nacionais.

A análise deste trabalho nos permitiu observar que ainda há muito a ser feito para o desenvolvimento da Estratégia Cibernética brasileira. Neste sentido, apresenta-se como valiosa oportunidade de trabalhos futuros o acompanhamento de tal desenvolvimento no seio da Marinha do Brasil, do Ministério da Defesa e da sociedade civil organizada como um todo.

REFERÊNCIAS

ARENDS, R. *et al*. *DNS Security Introduction and Requirements*. Reston: The Internet Society, 2005. Disponível em: <https://tools.ietf.org/html/rfc4033>. Acesso em: 02 jul. 2016.

BORG, Scott; BUMGARNER, John. *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008*. U.S. Cyber Consequences Unit, 2009. Disponível em: <http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf >. Acesso em: 02 jul. 2016.

BRASIL. Constituição Federal (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 2 jul. 2016.

_____. Decreto Legislativo n. 373, de 25 de setembro de 2013. Aprova a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro Branco de Defesa Nacional, encaminhados ao Congresso Nacional pela Mensagem nº 83, de 2012 (Mensagem nº 323, de 17 de julho de 2012, na origem). Diário Oficial da União, Brasília, DF, v. 150, n. 187, Seção n. 1, p. 1-2, 26 set. 2013. Disponível em: < http://portal.in.gov.br/>. Acesso em: 2 jul. 2016.

_____. Decreto nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. Brasília, 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm >. Acesso em: 2 jul. 2016.

_____. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, 2008a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm >. Acesso em: 2 jul. 2016.

_____. Lei Complementar nº 97, de 09 de junho de 1999. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. Brasília, 1999. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp97.htm> Acesso em: 2 jul. 2016.

_____. Lei Complementar nº 136, de 25 de agosto de 2010. Altera a Lei Complementar nº 97, de 9 de junho de 1999. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas, para criar o Estado-Maior Conjunto das Forças Armadas e disciplinar as atribuições do Ministro de Estado da Defesa. Brasília, 2010. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp136.htm> Acesso em: 2 jul. 2016.

_____. Estratégia Nacional de Defesa (2012a). Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/end.pdf>. Acesso em: 2 jul. 2016.

_____. Livro Branco de Defesa Nacional (2012c). Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf >. Acesso em: 2 jul. 2016.

_____. Livro Verde de Segurança Cibernética (2010). Disponível em: <http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf>. Acesso em: 2 jul. 2016.

_____. Lei nº 12.965, de 23 abr. 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 2 jul. 2016.

_____. Lei nº 12.737, de 30 nov. 2012. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 2 jul. 2016.

_____. Ministério da Defesa, 2007. Aprova Doutrina Militar de Defesa (Portaria nº 113/SPEAI/MD, de 1º de Fevereiro). Brasília: Ministério da Defesa

_____. Ministério da Defesa. Portaria normativa nº 196/EMD/MD, de 22 de fev. 2007. Aprova o Glossário das Forças Armadas. Disponível em: <http://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md35_g_01_glossario_fa_4aed2007.pdf >. Acesso em: 2 jul. 2016.

_____. Política Nacional de Defesa (2012d). Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/pnd.pdf >. Acesso em: 2 jul. 2016.

_____. Presidência da República. Discurso da Presidenta da República, Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas - Nova Iorque/EUA. Publicado em: 24 set. 2013. Disponível em: <http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua >. Acesso em: 2 jul. 2016.

_____. Ministério da Defesa. Glossário das Forças Armadas, 4ª edição: MD35-G-01. Brasília, DF, 2007. Disponível em: <http://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md35_g_01_glossario_fa_4aed2007.pdf>. Acesso em: 02 jul. 2016.

_____. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9883.htm>. Acesso em: 2 jul. 2016.

_____. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, 18 de novembro de 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 2 jul. 2016.

_____. Proposta de Emenda à Constituição n.º 331, de 26 agosto de 2013. Acrescenta o inciso VIII ao § 3º do art. 12, o inciso XXVI ao art. 21, o inciso XXX ao art. 22, o inciso XVIII ao art. 49, o inciso XXXVIII ao art. 84 e os arts. 144-A e 144-B, altera o inciso IV do art. 52, todos da Constituição Federal, para dispor sobre as atividades de inteligência no País, e dá outras providências. Câmara dos Deputados, Brasília-DF. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=597716>. Acesso em: 2 jul. 2016.

_____. Proposta de Emenda à Constituição n.º 398, de 26 de agosto de 2009. Insere o Capítulo IV ao Título V da Constituição Federal referente à atividade de inteligência e seus mecanismos de controle. Câmara dos Deputados, Brasília-DF. Disponível em:<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=447024>. Acesso em: 2 jul. 2016.

_____. Proposta de Emenda à Constituição n.º67, de 18 de dezembro de 2012. Insere o Capítulo IV ao Título V da Constituição Federal referente à atividade de inteligência e seus mecanismos de controle. Senado Federal, Brasília-DF. Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=109900>. Acesso em: 2 jul. 2016.

_____. Resolução do Congresso Nacional n.º2, de 22 de novembro de 2013. Dispõe sobre a Comissão Mista de Controle das Atividades de Inteligência (CCAI), comissão permanente do congresso nacional, órgão de controle e fiscalização externos da atividade de inteligência, previsto no art. 6º da lei nº 9.883, de 7 de dezembro de 1999. Congresso Nacional, BrasíliaDF. Disponível em: <http://legislacao.planalto.gov.br/legisla/legislacao.nsf/fraNotesDocumento?OpenFrameSet&Frame=frmDocumento&Src=%2Flegisla%2Flegislacao.nsf%2F0%2F70cd2eecfe5e138d83257c2e00397b81%3FOpenDocument%26AutoFramed>. Acesso em: 2 jul. 2016.

_____. CPI da Espionagem: relatório final. Brasília: Senado Federal. Disponível em: <https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco >. Acesso em: 2 jul. 2016.

_____. Lei nº 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 8 dez. 1999. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9883.htm>. Acesso em: 2 jul. 2016.

_____. Decreto nº 8.135, de 4 nov. 2013. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. Brasília: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm>. Acesso em: 2 jul. 2016.

_____. Decreto nº 8.793, de 29 jun. 2016. Fixa a Política Nacional de Inteligência. Brasília: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8793.htm >. Acesso em: 2 jul. 2016.

_____. Lei nº 12.965, de 23 abr. 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 2 jul. 2016.

_____. Decreto nº 8.771, de 11 maio 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.. Brasília: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm >. Acesso em: 2 jul. 2016.

_____. Projeto Estratégico do Exército Defesa Cibernética. Escritório de projetos do Exército Brasileiro. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica/escopodciber >. Acesso em: 30 jul. 2016.

BUCKLEY, Neil; KUCHLER, Hannah. *Ataque de hackers derruba rede de energia da Ucrânia*. São Paulo: Folha de São Paulo. Publicado em: 7 jan. 2016. Disponível em: <http://www1.folha.uol.com.br/mercado/2016/01/1726880-ataque-de-hackers-derruba-rede-de-energia-da-ucrania.shtml >. Acesso em: 02 jul. 2016.

CHIARETTI, Marco. *EUA e China são protagonistas da era da guerra cibernética*. Folha de São Paulo. Publicado em: 11 jan. 2015. Disponível em: <http://www1.folha.uol.com.br/ilustrissima/2015/01/1572753-eua-e-china-sao-protagonistas-da-era-da-guerra-cibernetica.shtml >. Acesso em: 15 jul. 2016.

CHINA. *China's Military Strategy. Chinadaily*. Publicado em: 26 maio 2015. Disponível em: <http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm>. Acesso em: 02 jul. 2016.

CLARKE, R.A.; KNAKE, R.K. *Guerra cibernética*: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015. 241 p. Título original: *Cyber War*: the next threat to national security and what to do about it.

CLAUSEWITZ, Carl von. *Da Guerra*. Tradução de Maria Teresa Ramos. 3 ed. São Paulo: Martins Fontes, 2010. 933p. Título original: Vom Kriege.

COLEMAN, Kevin G. *NATO extends Article 5 powers to cyber*. C4ISR. Publicado em: 23 jun. 2016. Disponível em: <http://www.c4isrnet.com/story/military-tech/blog/net-defense/2016/06/23/nato-extends-article-5-powers-cyber/86298254/>. Acesso em: 02 jul. 2016.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA (CICV). *Convenções de Genebra*. Genebra: CICV, 1949. Disponível em: <https://www.icrc.org/por/resources/ihl-databases/index.jsp >. Acesso em: 28 mar. 2016.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Adotada e proclamada pela resolução 217 A (III) da Assembléia Geral das Nações Unidas em 10 de dezembro de 1948. Disponível em: <http://portal.mj.gov.br/sedh/ct/legis_intern/ddh_bib_inter_universal.htm >. Acesso em: 27 jul. 2016.

DEMARTINI, Marina. *Facebook descumpre decisão judicial e pode ser bloqueado*. G1. Publicado em: 28 jul 2016. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/facebook-descumpre-decisao-judicial-e-tem-contas-bloqueadas >. Acesso em: 30 jul. 2016.

Em 15 anos, número de usuários de internet passou de 400 milhões para 3,2 bilhões, revela ONU. Nações Unidas no Brasil. Publicado em: 28 maio 2015. Disponível em: <https://nacoesunidas.org/em-15-anos-numero-de-usuarios-de-internet-passou-de-400-milhoes-para-32-bilhoes-revela-onu/>. Acesso em: 2 jul. 2016.

EUA. Department of Defense. *National Security Strategy*. Washington, 2011.

EUA. Department of Defense. *National Security Strategy*. Washington, 2015.

EUA. Department of Defense. *The Department of Defense Cyber Strategy*. Washington, 2015a.

EUA. Congress. Senate bill nº 2905 – *Cyber Act of War*. Washington, 2016. Disponível em: <https://www.congress.gov/bill/114th-congress/senate-bill/2905/text >. Acesso em: 02 jul. 2016.

EUA. White House. *International Strategy for Cyberspace*. Washington, 2011. Disponível em: <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf >. Acesso em: 02 jul. 2016.

EUA suspeitam que Coreia do Norte teve ajuda no ataque à Sony Pictures. Ataque atingiu sistema e revelou informações de filmes e funcionários. A Coreia do Norte negou sua participação. G1. Publicado em: 30 dez. 2014. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/12/eua-suspeitam-que-coreia-do-norte-teve-ajuda-no-ataque-sony-pictures.html >. Acesso em: 02 jul. 2016.

Força Aérea dos EUA cria comando cibernético. Folha de São Paulo. Publicado em: 19 set. 2007. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u329582.shtml>. Acesso em: 02 jul. 2016.

FOURTH Amendment: an overview. Legal Information Institute. Cornell University Law School. Disponível em: <http://www.law.cornell.edu/wex/fourth_amendment >. Acesso em: 2 jul. 2016.

FRAGOLA, Rodrigo Jonas. *Os Próximos Passos da Estratégia Cibernética de Defesa do Brasil*. O Brasil precisa de um novo órgão com as virtudes do CDCiber, mas com foco na segurança empresarial e na capacitação da indústria. Defesanet. Publicado em: 15 mar. 2016. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/21837/Os-Proximos-Passos-da-Estrategia-Cibernetica-de-Defesa-do-Brasil/ >. Acesso em: 2 jul. 2016.

FREUND, Julien. *Sociología del conflicto*. Madrid: Ediciones Ejército, 1995. p. 19 – 151.

FREEDOM HOUSE. *Freedom on the Net 2015*. Freedom House, 2015. Disponível em: <https://freedomhouse.org/report/freedom-net/freedom-net-2015 >. Acesso em: 02 jul. 2016.

FUNDO MONETÁRIO INTERNACIONAL. Análise econômica e financeira mundial. FMI, 2016. Disponível em: <http://www.imf.org/external/pubs/ft/weo/2016/01/weodata/index.aspx >. Acesso em: 15 jul. 2016.

GARCIA, Gabriel. *Alemanha diz que usina de aço do país foi comprometida por ataque hacker*. Revista Exame. Publicado em: 19 dez. 2014. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/usina-de-aco-na-alemanha-foi-comprometida-por-ataque-hacker>. Acesso em: 02 jul. 2016.

GAUDIOSI, J. *Why Sony didn't learn from its 2011 hack*. Fortune. Publicado em: 24 dez. 2014. Disponível em: <http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack >. Acesso em: 02 jul. 2016.

GEERS, Kenneth. *Strategic Cyber Security*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2011. Disponível em: <https://ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF >. Acesso em: 02 jul. 2016.

GOMES, Helton Simões. *Ataque hacker, 'WhatsApp grátis'... Marco Civil da Internet ganha regras*. Decreto presidencial regulamentou 2 das questões mais polêmicas da lei. Fixadas brechas a neutralidade de rede e segurança sobre dado pessoal. São Paulo: G1. Publicado em: 13 maio 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/05/ataque-hacker-whatsapp-gratis-marco-civil-da-internet-ganha-regras.html >. Acesso em: 2 jul. 2016.

GOULD, Joe. *Constructing a Cyber Superpower*. At 5 Years Old, US Cyber Command Faces Growth, Challenges. Defensenews. Publicado em: 29 jun. 2015. Disponível em: <http://www.defensenews.com/story/defense/policy-budget/cyber/2015/06/27/us-cyber-command-budget-expand-fort-meade-offensive/28829321/>. Acesso em: 02 jul. 2016.

GRAHAM, David E. Cyber Threats and the Law of War. *Journal of National Security Law & Policy*, 2010. v. 4, n. 1, p. 87-102.

GREENWALD, Glenn; KAZ, Roberto; CASADO, José. *EUA espionaram milhões de e-mails e ligações de brasileiros*. País aparece como alvo na vigilância de dados e é o mais monitorado na América Latina. O Globo. Publicado em: 6 jul. 2013. Disponível em: <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>. Acesso em: 02 jul. 2016.

GRIESINGER, Denise. *China reforça censura a conteúdos publicados na internet*. Agência Brasil. Publicado em: 16 fev. 2016. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2016-02/china-reforca-censura-conteudos-publicados-na-internet >. Acesso em: 02 jul. 2016.

GROSSMANN, Luis Osvaldo. *Governança da Internet: Fim do contrato da ICANN e adiado para o final de 2016*. Associação Brasileira de Internet. Publicado em: 22 jun. 2015. Disponível em: <http://www.abranet.org.br/Noticias/Governanca-da-Internet%3A-Fim-do-contrato-da-ICANN-e-adiado-para-o-final-de-2016-689.html?from_info_index=281#.V64a9pgrK02 >. Acesso em: 15 jul. 2016.

INTERNET ASSIGNED NUMBERS AUTHORITY. *List of Root Servers*. Los Angeles. Disponível em: <http://www.iana.org/domains/root/servers>. Acesso em: 17 jul. 2016.

Imprensa oficial chinesa defende censura às revistas "Time" e "The Economist". UOL Economia. Publicado em: 11 abr. 2016. Disponível em: <http://economia.uol.com.br/noticias/efe/2016/04/11/imprensa-oficial-chinesa-defende-censura-as-revistas-time-e-the-economist.htm >. Acesso em: 02 jul. 2016.

JORDAN, Bryant. *US Still Has No Definition for Cyber Act of War*. Military.com. Publicado em: 22 jun. 2016. Disponível em: <http://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html>. Acesso em: 02 jul. 2016.

KANIA, Elsa. *China: Active Defense in the Cyber Domain*. What implications does China's new defense white paper have for its cyber strategy? The Diplomat. Publicado em: 12 jun. 2015. Disponível em: <http://thediplomat.com/2015/06/china-active-defense-in-the-cyber-domain/ >. Acesso em: 02 jul. 2016.

KITTEN, Tracy. *Chase's Cybersecurity Budget to Double*. Princeton: BankInfoSecurity. Publicado em: 10 out. 2014. Disponível em: <www.bankinfosecurity.com/chases-cybersecurity-budget-to-double-a-7427>. Acesso em: 02 jul. 2016.

KOCHETKOVA, Kate. *Casos curiosos de violação de dados em 2014*. Kaspersky Lab. Publicado em: 28 jan. 2015. Disponível em: <https://blog.kaspersky.com.br/casos-curiosos-de-violacao-de-dados-em-2014/4709/>. Acesso em: 02 jul. 2016.

KUSHNER, David. *The Real Story of Stuxnet*. IEEE. Publicado em: 26 fev. 2013. Disponível em: <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/>. Acesso em: 02 jul. 2016.

LEYDEN, J. *Biggest DDoS attack in history hammers Spamhaus*. The Register. Publicado em: 27 mar. 2013. Disponível em: <www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood >. Acesso em: 02 jul. 2016.

LING, Justin; PEARSON, Jordan. *Exclusive: Canadian Police Obtained BlackBerry's Global Decryption Key*. Vice News. Publicado em: 14 abr. 2016. Disponível em: <https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how >. Acesso em: 2 jul. 2016.

LOUREIRO, Castro. *Defesa Cibernética*. In: Palestra de Defesa Cibernética. Rio de Janeiro. Centro de Jogos da Escola de Guerra Naval. 6 jul. 2016

MACASKILL, Ewen; DANCE, Gabriel. *NSA files: Decoded*. What the revelations mean to you. The Guardian. Publicado em: 1º nov. 2013. Disponível em: <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>. Acesso em: 02 jul. 2016.

MACEDO, Fausto. *Juristas e criminalistas apontam falhas na lei Carolina Dieckmann*. Legislação que leva o nome da atriz prevê punições contra crimes eletrônicos. O Estado de São Paulo. Publicado em: 2 abr. 2013. Disponível em: <http://politica.estadao.com.br/noticias/geral,juristas-e-criminalistas-apontam-falhas-na-lei-carolina-dieckmann,1016111 >. Acesso em: 02 jul. 2016.

MANJIKIAN, Mary McEvoy. From Global Village to Virtual Battlespace: the colonizing of internet and the extension of realpolitik. *International Studies Quarterly*, 2010. Ed. 54. p.381-401. Disponível em: <https://www.e-education.psu.edu/drupal6/files/sgam/virtual_space/globalvillagevirtualbattlespace.pdf>. Acesso em: 28 mar. 2016.

MARCONI, M. de A.; LAKATOS, E. M. Técnicas de Pesquisa. 7ª Edição. São Paulo: Editora Atlas, 2008.

Marinha do Brasil (MB). *Amazônia Azul*. Disponível em: <https://www.marinha.mil.br/content/amazonia-azul-0 >. Acesso em: 2 jul. 2016.

McCARTHY, Kieren. *Brazilian president signs internet civil rights law*. Marco Civil bill enshines 'net neutrality', 'privacy' as law. The Register. Publicado em: 23 abr. 2014. Disponível em: <http://www.theregister.co.uk/2014/04/23/new_bill_signed_in_brazil_guaranteeing_civil_rights_on_internet/ >. Acesso em: 2 jul. 2016.

MEHTA, Aaron. *Industry Fears Massive Losses Through Espionage*. Defensenews. Publicado em: 21 dez. 2014. Disponível em: <http://www.defensenews.com/story/defense/policy-budget/cyber/2014/12/10/industry-fears-massive-losses-through-espionage-/20211863/>. Acesso em: 02 jul. 2016.

Ministério das Comunicações (MC). *Saiba os benefícios do satélite geoestacionário*. Publicado em: 3 ago. 2015. Disponível em: <http://www.mc.gov.br/sala-de-imprensa/todas-as-noticias/institucionais/36448-soberania-via-satelite >. Acesso em: 2 jul. 2016.

Ministério da Defesa (MD). Portaria normativa nº 2.624/MD, de 7 de dezembro de 2015. Aprova a Política Setorial de Defesa. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=09/12/2015&jornal=1&pagina=36&totalArquivos=136 >. Acesso em: 2 jul. 2016.

Ministério da Defesa (MD). Portaria normativa nº 2.621/MD, de 7 de dezembro de 2015. Aprova a Estratégia Setorial de Defesa. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=09/12/2015&jornal=1&pagina=32&totalArquivos=136 >. Acesso em: 2 jul. 2016.

Ministério da Defesa (MD). Portaria normativa nº 3.010/MD, de 18 de novembro de 2014. Aprova a Doutrina Militar de Defesa Cibernética. Disponível em: <http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf >. Acesso em: 2 jul. 2016.

MOCKAPETRIS, Paul V. *Domain names*: concepts and facilities. Fremont: The Internet Engineering Task Force, 1987. Disponível em: <https://tools.ietf.org/html/rfc1034>. Acesso em: 02 jul. 2016.

NAÇÕES UNIDAS NO BRASIL. Em 15 anos, número de usuários de internet passou de 400 milhões para 3,2 bilhões. Publicado em 28 maio 2015. Disponível em: <https://nacoesunidas.org/em-15-anos-numero-de-usuarios-de-internet-passou-de-400-milhoes-para-32-bilhoes-revela-onu/>. Acesso em: 02 jul. 2016.

NATO. Cyber Defence Exercises. *Locked Shields 2016*. NATO CCDCOE. 2016. Disponível em: <https://ccdcoe.org/locked-shields-2016.html >. Acesso em: 02 jul. 2016.

NATO. *Cyber Security Strategy Documents*. NATO CCDCOE. 2016. Disponível em: <https://ccdcoe.org/cyber-security-strategy-documents.html>. Acesso em: 02 jul. 2016.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). North Atlantic Treaty. Washington: NATO, 1949. Disponível em: <http://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=pt>. Acesso em: 02 jul. 2016.

NETMUNDIAL. *Global multistakeholder meeting on the future of Internet Governance*. São Paulo. 2014. Disponível em: <http://netmundial.br >. Acesso em: 2 jul. 2016.

OPALL, Barbara. *US-Israel Sign Cyber Defense Declaration*. Defensenews. Publicado em: 21 jun. 2016. Disponível em: <http://www.defensenews.com/story/defense/2016/06/21/us-israel-sign-cyber-defense-declaration/86195530/>. Acesso em: 02 jul. 2016.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). *Adoção de uma Estratégia Interamericana Integral para Combater as Ameaças à Segurança Cibernética*. Ottawa: OEA, 2004. Disponível em: <http://www.oas.org/xxxivga/portug/docs/doc_aprovados/adocao_estrategia_combater_seguranca_cibernetica.htm>. Acesso em: 02 jul. 2016.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Digital Security Risk Management for Economic and Social Prosperity*. Paris: OECD, 2015. Disponível em: <http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf>. Acesso em: 02 jul. 2016.

ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Guidelines for the Security of Information Systems and Networks: Towards a culture of security*. Paris: OECD, 2002. Disponível em: <https://www.oecd.org/sti/ieconomy/15582260.pdf>. Acesso em: 02 jul. 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). *Charter of the United Nations.* São Francisco. Publicada em: 26 jun. 1945. Disponível em: <http://www.un.org/en/charter-united-nations/index.html>. Acesso em: 28 mar. 2016.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Comissão Interamericana de Direitos Humanos. Declaração Americana dos Direitos e Deveres do Homem (Aprovada na Nona Conferência Internacional Americana, Bogotá, 1948). Disponível em: <http://www.cidh.org/Publicacoes.htm >. Acesso em: 2 jul. 2016.

OECD. *Digital Security Risk Management for Economic and Social Prosperity*: OECD Recommendation and Companion Document. Paris: OECD Publishing, 2015. Disponível em: <http://dx.doi.org/10.1787/9789264245471-en>. Acesso em: 02 jul. 2016.

ORWELL, George. Ninety eighty four. London: Eric Blair, 1949

PEDUZZI, Pedro. *Correio eletrônico do governo será ativado em novembro*. Agência Brasil. Publicado em: 14 out. 2013. Disponível em: <http://www.ebc.com.br/noticias/brasil/2013/10/correio-eletronico-do-governo-sera-ativado-em-novembro >. Acesso em: 2 jul. 2016.

Pentágono Revela Estratégia para Ciber Operações. Defesanet. Publicado em: 15 jul. 2011. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/1922/Pentagono-Revela-Estrategia-para-Ciber-Operacoes-/>. Acesso em: 02 jul. 2016.

PHILIPP, Joshua. *Sob véu da segurança cibernética, China planeja governar internet global*. O PCC quer o controle de todos os âmbitos da internet e de todas as empresas envolvidas. Epoch Times. Publicado em: 12 abr. 2016. Disponível em: <https://www.epochtimes.com.br/sob-veu-seguranca-cibernetica-china-planeja-governar-internet-global/#.V5GNWLgrK00 >. Acesso em: 02 jul. 2016.

Privacy Scandal: NSA Can Spy on Smart Phone Data. SPIEGEL has learned from internal NSA documents that the US intelligence agency has the capability of tapping user data from the iPhone, devices using Android as well as BlackBerry, a system previously believed to be highly secure. Spiegel. Publicado em: 7 set. 2013. Disponível em: <http://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html >. Acesso em: 2 jul. 2016.

Putin promulga série polêmica de leis antiterroristas. Defesanet. Publicado em: 8 jul. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/05/china-e-russia-firmam-acordo-de-paz-digital-para-nao-se-hackearem.html >. Acesso em: 15 jul. 2016.

QIANG, Xiao. *How China's Internet Police Control Speech on the Internet*. Radio Free Asia. Publicado em: 24 nov. 2008. Disponível em: <http://www.rfa.org/english/commentaries/china_internet-11242008134108.html >. Acesso em: 02 jul. 2016.

RING, Tim. *Backdoor in MS Outlook webmail raises security doubts*. SC Magazine. Publicado em: 6 out. 2015. Disponível em: <http://www.scmagazine.com/backdoor-in-ms-outlook-webmail-raises-security-doubts/article/443415/ >. Acesso em: 2 jul. 2016.

ROHR, Altieres. *China e Rússia firmam "acordo de paz digital" para não se "hackearem"*. Texto também prevê cooperação policial. Nova lei de segurança nacional chinesa fala em "soberania". G1. Publicado em: 11 maio 2015. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/05/china-e-russia-firmam-acordo-de-paz-digital-para-nao-se-hackearem.html >. Acesso em: 02 jul. 2016.

SANG-HUN, Choe. *Theft of Data Fuels Worries in South Korea*. Nova York: The New York Times. Publicado em: 20 jan. 2014. Disponível em: <http://www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html >. Acesso em: 02 jul. 2016.

SANTANA, Ana Elisa. *Tim Berners-Lee: "Vamos fazer da internet um lugar livre"*. Empresa Brasil de Comunicação. Publicado em: 16 maio 2013. Disponível em: <http://www.ebc.com.br/tecnologia/2013/05/tim-berners-lee-vamos-fazer-da-internet-um-lugar-livre >. Acesso em: 2 jul. 2016.

SATTER, Raphael. *First cyber war manual released*: NATO's manual possibly the first step towards a cyber 'Geneva Convention'. Disponível em: <http://www.theage.com.au/it-pro/security-it/first-cyber-war-manual-released-20130319-2gegk.html>. Acesso em: 02 jul. 2016.

SCHMITT, Michael (Ed.). Tallinn Manual on the International Law applicable to Cyber Warfare. Nova York: Cambridge University Press, 2013. Disponível em: <https://ccdcoe.org/tallinn-manual.html>. Acesso em: 02 jul. 2016.

SKLEROV, Matthew J. *To cyberattacks: A justification for the use of active defenses against.* United States Navy. 2009.

SONG, Aly. *Presidente chinês diz que cada país deve controlar a sua internet*. Diário de Notícias. Publicado em: 16 dez. 2015. Disponível em: <http://www.dn.pt/mundo/interior/presidente-chines-diz-que-cada-pais-deve-controlar-a-sua-internet-4932656.html >. Acesso em: 02 jul. 2016.

STILLER, Akos. *Ataque hacker afeta mil empresas energéticas de 84 países*. O Globo. Publicado em: 30 jun. 2014. Disponível em: <http://oglobo.globo.com/sociedade/tecnologia/ataque-hacker-afeta-mil-empresas-energeticas-de-84-paises-13085928>. Acesso em: 02 jul. 2016.

THE INTERNET ENGINEERING TASK FORCE. *The IETF working groups*. Fremont. Disponível em: <http://ietf.org/>. Acesso em: 02 jul. 2016.

TIMBERG, Craig. *The making of a vulnerable Internet*. Washington: The Washington Post, 2015. Disponível em: <http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/>. Acesso em: 02 jul. 2016.

UNIVERSIDADE AUTÓNOMA DE LISBOA. *Janus 2014 anuário de relações exteriores*. Lisboa: Observare, 2014. Disponível em: <https://irelunb.files.wordpress.com/2014/10/janus-2014-pp1_170.pdf >. Acesso em: 02 jul. 2016.

VOLTOLINI, Ramon. *Hackers podem usar falha de DNS para controlar PCs de quase todo o mundo*. Publicado em: 22 fev. 2016. Disponível em: <http://www.tecmundo.com.br/ataque-hacker/100994-hackers-usar-falha-dns-controlar-pcs-mundo.htm>. Acesso em: 02 jul. 2016.

WHATSAPP. *Privacidade e Termos*. 2016. Disponível em: <https://www.whatsapp.com/legal/ >. Acesso em: 2 jul. 2016.

WRIGHT, L. *Target CEO resigns after security breach*. The Star. Publicado em: 05 maio 2014. Disponível em: <https://www.thestar.com/business/2014/05/05/target_ceo_resigns_after_security_breach_canadian_fiasco.html >. Acesso em: 02 jul. 2016.

YIN, Robert K. Estudo de Caso: Planejamento e Métodos. 5ª Edição. Porto Alegre: Editora Bookman, 2015.

YON-SE, Kim. *Top executives resign over massive data leak*. Seoul: The Korea Herald. Publicado em: 20 jan. 2014. Disponível em: <www.koreaherald.com/view.php?ud=20140120001002>. Acesso em: 02 jul. 2016.

ANEXO A – ESTRUTURA NACIONAL DE SEGURANÇA CIBERNÉTICA

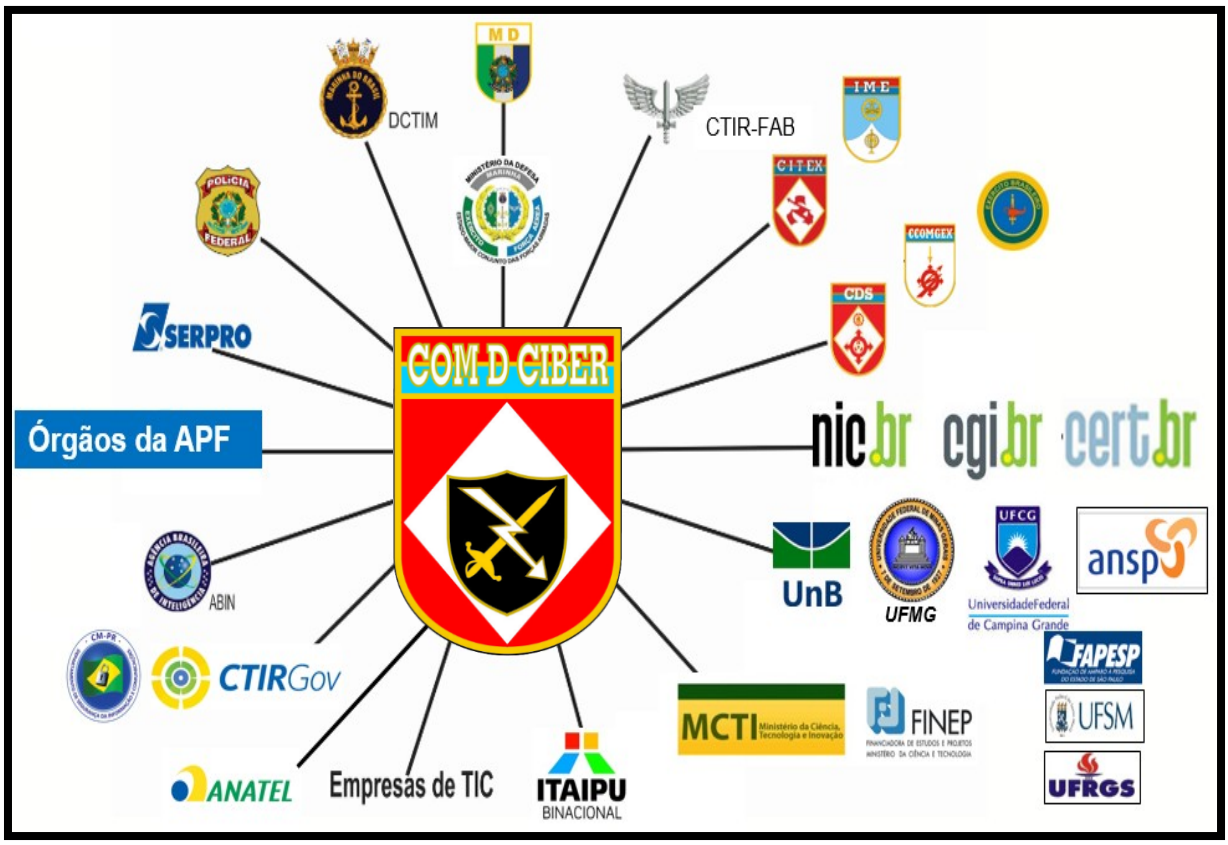

FIGURA 1 – Comando de Defesa Cibernética e instituições interligadas

Fonte: LOUREIRO (2016)

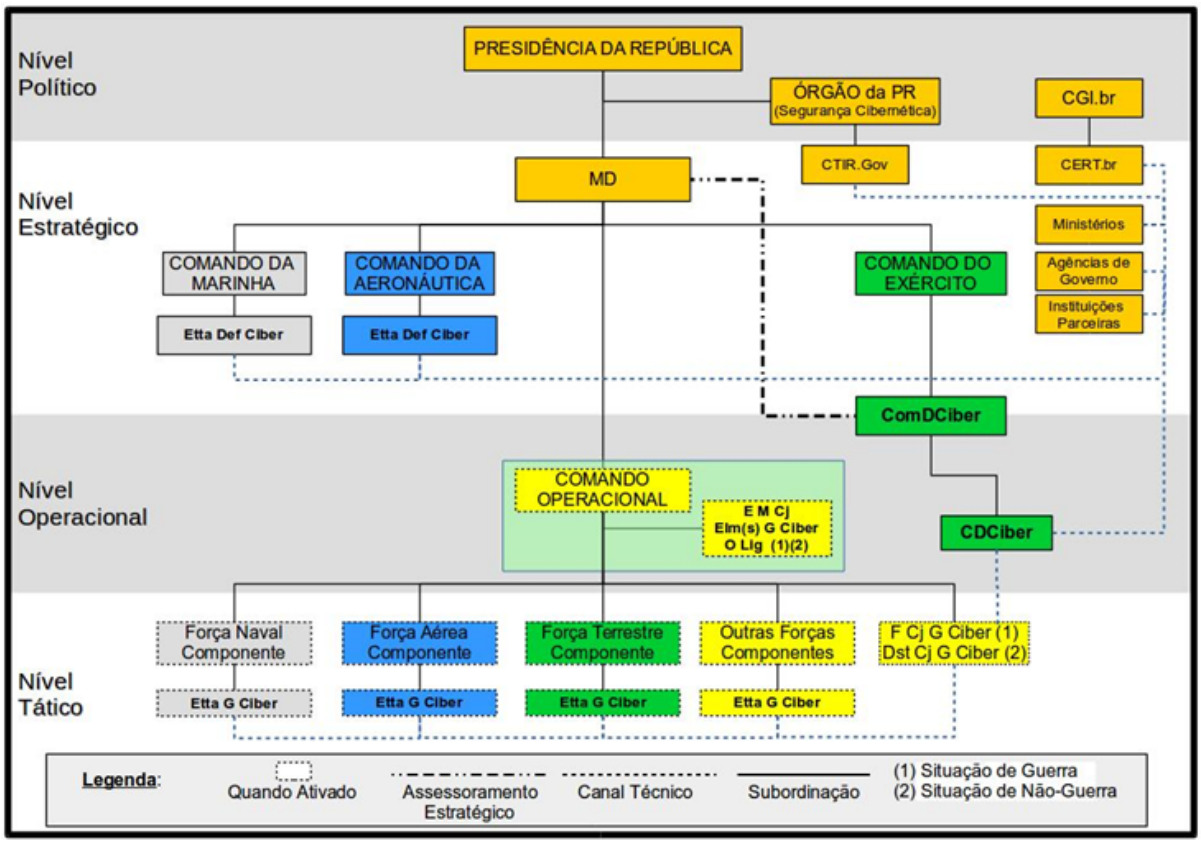

FIGURA 2 – Organograma brasileiro de defesa cibernética

Fonte: LOUREIRO (2016)

APÊNDICE A – PRIVACIDADE E TERMOS DO APLICATIVO GRATUITO DE TROCA DE MENSAGENS WHATSAPP

Política de Privacidade que as pessoas aceitam sem ler[73]:

> "[…] WhatsApp também **se reserva o direito de divulgar informações** pessoalmente identificáveis e /ou informações não pessoalmente identificáveis que WhatsApp acredita, de boa fé, é adequado ou necessário para fazer valer os nossos Termos de Serviço, tomar precauções contra responsabilidade, para investigar e defender-se contra qualquer reclamações de terceiros ou alegações, para ajudar as agências de aplicação do governo, para proteger a segurança ou a integridade do site WhatsApp ou nossos servidores e para proteger os direitos, propriedade, ou segurança pessoal do WhatsApp, nossos usuários ou outros.
>
> […] **Não podemos**, no entanto, **assegurar ou garantir a segurança de qualquer informação que você transmita** pelo WhatsApp e você o faz por sua própria conta e risco.
>
> […] Se você é um usuário que acessa o Site WhatsApp e Serviço por parte da União Europeia, na Ásia ou em qualquer outra região com as leis e regulamentos que regem a recolha de dados pessoais, uso e divulgação, que diferem das leis dos Estados Unidos, por favor, esteja ciente de que através de seu continuado uso do site WhatsApp e Serviço, que são regidos pelas leis da Califórnia, esta política de privacidade e os Termos de Serviço, **você está transferindo suas informações pessoais para os Estados Unidos e você expressamente concorda com essa transferência e consentimento para ser governado pela lei da Califórnia para estes fins**." (WHATSAPP, 2016) (tradução nossa) (grifo nosso)

---

73 "[…] WhatsApp also reserves the right to disclose Personally Identifiable Information and/or non-personally-identifiable information that WhatsApp believes, in good faith, is appropriate or necessary to enforce our Terms of Service, take precautions against liability, to investigate and defend itself against any third-party claims or allegations, to assist government enforcement agencies, to protect the security or integrity of the WhatsApp Site or our servers, and to protect the rights, property, or personal safety of WhatsApp, our users or others.

[…] We cannot, however, ensure or warrant the security of any information you transmit to WhatsApp and you do so at your own risk.

[…] If you are a user accessing the WhatsApp Site and Service from the European Union, Asia, or any other region with laws or regulations governing personal data collection, use, and disclosure, that differ from United States laws, please be advised that through your continued use of the WhatsApp Site and Service, which are governed by California law, this Privacy Policy, and our Terms of Service, you are transferring your personal information to the United States and you expressly consent to that transfer and consent to be governed by California law for these purposes.