ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

TC QEM JOSÉ RICARDO CABRAL **AVELAR**

A GUERRA CIBERNÉTICA E SEUS DESAFIOS PARA O BRASIL

Rio de Janeiro

2018

TC QEM JOSÉ RICARDO CABRAL **AVELAR**

A GUERRA CIBERNÉTICA E SEUS DESAFIOS PARA O BRASIL

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como pré-requisito para matrícula no Programa de Pós-graduação *lato sensu* em Ciências Militares.

Orientador: Maj Com **Glauber** Juarez Sasaki Acácio

Rio de Janeiro

2018

A948g

Avelar, José Ricardo Cabral

A Guerra Cibernética e seus desafios para o Brasil / José Ricardo Cabral Avelar . —2018.

74 f.: il.; 30cm

Orientação:Glauber Juarez Sasaki Acácio.

Trabalho de Conclusão de Curso (Especialização em Ciências Militares). —Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018.

Bibliografia: f. 71-74.

1. GESTÃO DE DEFESA. 2. LOGÍSTICA E MOBILIZAÇÃO. 3. INFRAESTRUTURA. I. Título.

CDD 355.02

.

TC QEM JOSÉ RICARDO CABRAL **AVELAR**

A GUERRA CIBERNÉTICA E SEUS DESAFIOS PARA O BRASIL

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como pré-requisito para matrícula no Programa de Pós-graduação *lato sensu* em Ciências Militares.

Aprovado em de novembro de 2018.

COMISSÃO AVALIADORA

_____
Glauber Juarez Sasaki Acácio – Maj Com QEMA – Me. – Presidente
Escola de Comando e Estado-Maior do Exército

_____
Sidney Marinho Lima – TC QMB QEMA – Membro
Escola de Comando e Estado-Maior do Exército

_____
Anderson Luiz Alves Figueiredo – Maj Eng QEMA – Membro
Escola de Comando e Estado-Maior do Exército

AGRADECIMENTOS

Ao major Com **Glauber** Juarez Sasaki Acácio, pela correta e oportuna orientação acerca do tema escolhido, pelo auxílio em todos os momentos que se fizeram necessários e pela confiança depositada no meu trabalho.

Aos companheiros do Curso de Direção para Engenheiros Militares, pelo apoio nos momentos difíceis, pela amizade sempre demonstrada e pelos conhecimentos compartilhados.

À minha família, por ser a minha fortaleza de todas as horas, pelo apoio e suporte sempre demonstrados e pela compreensão com as necessidades de ausência na realização deste e de outros trabalhos.

RESUMO

Este trabalho teve como objetivo estudar o tema Guerra Cibernética a fim de obter conhecimentos para o fomento da capacidade de Defesa Cibernética do Brasil, a partir de uma concepção de necessidade de integração entre as Forças Armadas brasileiras, mais especificamente o Exército e toda a sociedade brasileira. Inicialmente, foram apresentadas as principais inovações que permitiram o surgimento do ambiente cibernético e em consequência a sua utilização como espaço de batalha. Foram apresentados em seguida os principais conceitos que devem ser entendidos para um boa compreensão do assunto em questão. Foram apresentados ainda relatos de casos de ataques cibernéticos, tais como o da Estônia em 2007, o da Geórgia em 2008 e o da Ucrânia em 2013. Estes casos foram utilizados como base para a identificação dos principais modos de operação e ataques utilizados na prática, para em seguida servirem de ensinamento para o setor cibernético no Brasil. Em seguida fez-se uma abordagem das principais características da política cibernética dos Estados Unidos da América, Rússia e China. Após isso, realizou-se uma abordagem da estruturação da política cibernética do Brasil, com especial atenção aos seus aspectos políticos e estratégicos, buscando abordar também a sua relação com a vertente civil da sociedade e a necessidade de envolvimento consciente daquela parcela da sociedade brasileira. Buscou-se extrair ensinamentos e lições que possam ser aproveitados pelo Brasil e sua sociedade, integrando suas vertentes civil e militar.

Palavras-chave: Estados Unidos,Rússia, China, Internet, Guerra Cibernética, Estratégia

ABSTRACT

This work aimed to study the theme of cybersecurity to acquire knowledge to improve Brazilian Cyberdefense capacity, based on a conception of nedd of integration between Brazilian Military Forces, Brazilian Army specificaly, and the whole Brazilian society. Initially, we presented the main inovations that allowed the cyber environment creation and consequently its use as a battlefield. We presented later the main concepts that should be understood for a good comprehension of the subject matter. We presented some case reports of cyber attacks, such as Estonia in 2007, Georgia in 2008 and Ukraine in 2013. Those case reports were used later on as a foundation to identify the main operation modes and attacks used for real, and after that they were used as a precept to the brazilian cyber branch. After that we mentioned the main aspects of cyber policy of USA, Russia and China. Then we mentioned the brazilian cyber policy organization, with special attention to its politics and strategics aspects, searching to highlight its relationship with civilian branch of society and the need of a conscient involvement of that part of brazilian society. We seeked for knowledge and lessons that can be used by Brazil and its society, integrating their civilian and miitary branches

keywords: USA,Russia, China, Internet, Cyberwarfare, Strategy

SUMÁRIO

1. INTRODUÇÃO

A capacidade do ser humano para adaptar-se e vencer as dificuldades impostas pelo ambiente onde vive sempre foi, sem sombra de dúvidas, o grande diferencial que permitiu o seu domínio sobre todas as outras criaturas que habitam o planeta.

A humanidade vem demonstrando, desde os seus primórdios, uma capacidade extraordinária de criação e evolução tecnológica que permitiram avanços extraordinários ao longo do tempo. Desde o seu domínio sobre o fogo, sobre as técnicas de plantio e agricultura, a caça e criação de animais, técnicas de construção que permitiram empreendimentos de grande complexidade, como as pirâmides do Egito, passando pelas grandes navegações, o homem tem levado a sua sociedade a patamares de evolução tecnológica surpreendentes.

Porém, se uma análise das inovações citadas, ocorridas ao longo dos séculos, demonstra que a taxas maiores ou menores de avanços tecnológicos o homem vem desenvolvendo a sua sociedade desde o seu princípio, é correto afirmar que o século XX representou um salto tecnológico fantástico que mudaria as relações humanas de forma considerável.

Com o surgimento da eletrônica como disciplina, na forma como é conhecida nos dias de hoje, a partir de diversas pesquisas e invenções, entre elas a concepção por J.A. Fleming do primeiro dispositivo eletrônico, o diodo de tubo de vácuo, em 1904, e da invenção do transistor em 1947, por William Shockley, John Bardeen e Walter Brattain, houve uma verdadeira reação em cadeia de novas descobertas e inovações.

Utilizando como ponto de partida as tecnologias recém desenvolvidas, além de conhecimentos básicos de eletrônica, eletricidade, física, química, matemática, entre outras, foram construídos máquinas e dispositivos com grande valor tecnológico agregado, que incrementaram ainda mais as possibilidades de novas pesquisas e desenvolvimentos. Entre essas descobertas, devem ser destacadas a invenção do computador e a criação da Internet, por possuírem estreita ligação com o espaço cibernético, o ambiente onde ocorrem as ações de Guerra Cibernética.

Os computadores considerados modernos surgiram na década de 1940, sendo o ENIAC (1946) o mais famoso projeto de sua época, por ser muito mais rápido do que as máquinas até então desenvolvidas. A geração do ENIAC é considerada a primeira geração de computadores modernos, com máquinas de grandes dimensões e que alcançavam

temperaturas muito elevadas. Após diversas inovações, como a substituição das válvulas eletrônicas por transistores, houve uma diminuição considerável do Hardware utilizado nos projetos, chegando-se aos computadores de quarta geração, marcada pela comercialização dos computadores pessoais.

Com o advento da miniaturização e a popularização dos circuitos integrados, redução de tamanho e preço, os computadores que inicialmente eram utilizados basicamente em cálculos e pesquisas científicas, tornaram-se objetos de uso pessoal e atingiram um nível de popularização surpreendente, principalmente a partir da última década do século XX.

Em consequência do surgimento dos computadores e sua modernização, foram sendo criados diversos serviços e aplicações que os utilizavam como ferramenta para diversos fins, entre eles o compartilhamento de informações no contexto da Guerra Fria. O resultado mais importante das inovações ligadas aos computadores foi o surgimento da rede que hoje é conhecida mundialmente como Internet.

Tanenbaum (2002, p.50), define a Internet como uma vasta coleção de redes que utilizam certos protocolos comuns e fornecem serviços padronizados. Porém nem sempre foi assim, especialmente em seu início.

Ainda, segundo Tanenbaum (2002, p.50), as origens da Internet podem ser encontradas em uma tentativa do Departamento de Defesa (DoD) dos Estados Unidos da América (EUA) de criar uma rede de comando e controle que pudesse sobreviver a uma guerra nuclear, no final dos anos de 1950, já que naquela época todas as comunicações militares utilizavam a rede de telefonia pública, considerada vulnerável. Essa vulnerabilidade se dava principalmente porque a rede de telefonia pública apresentava pouca redundância, e a destruição de poucos pontos chave poderia tornar o sistema inoperante como um todo, deixando apenas áreas isoladas umas das outras.

Como parte do mesmo contexto da Guerra Fria e competição com os soviéticos na corrida espacial, foi criada a ARPA (Advanced Research Projects Agency), que deveria buscar entre as universidades e empresas privadas americanas ideias que fossem promissoras para a solução dos problemas tecnológicos do país e que impactassem em sua segurança nacional.

A solução visualizada para o problema americano de comando e controle do início dos anos de 1960 era de uma rede altamente distribuída e resistente a falhas, que oferecesse uma grande possibilidade de redundâncias. A Figura 1 mostra a diferença entre

as duas concepções, a rede de telefonia existente à época (a) e a rede distribuída então idealizada (b). Uma simples comparação entre as duas estruturas permite identificar a robustez oferecida pela rede distribuída (b) em termos de interrupções físicas de um ou mais ramais.

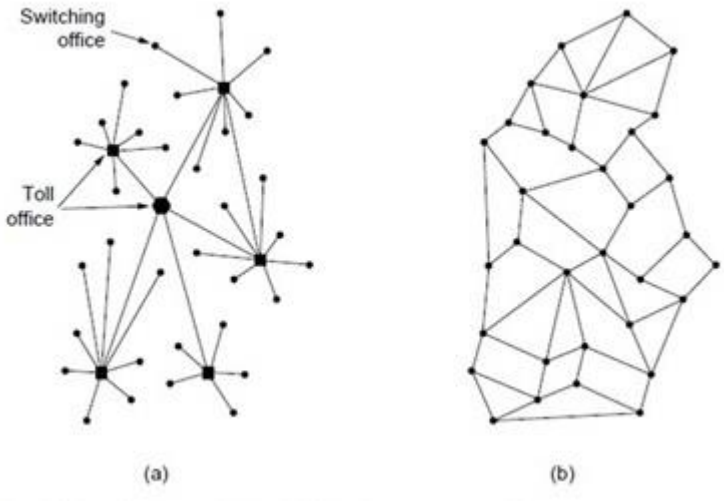


Figura 1 - Rede de Telefonia/rede distribuída
Fonte: Tanenbaum (2003)

De acordo com Kurose (2003, p.58), três grupos trabalharam ao redor do mundo na solução distribuída que atendia aos requisitos do DoD americano, cada um deles sem o conhecimento do trabalho dos outros. Porém, os três grupos percorreram caminhos semelhantes, desenvolvendo conceitos de comunicação por comutação de pacotes, uma alternativa eficiente e robusta à comutação de circuitos utilizada até então. Esse conceito de comutação de pacotes seria um conceito chave e uma das bases para o desenvolvimento da Internet.

Diversos anos se passaram até que em 1967 surgiu o projeto efetivo para a implantação de uma rede de computadores utilizando o conceito de comutação de pacotes, trabalhado nos laboratórios e universidades desde o início da década. Essa rede era formada de minicomputadores chamados IMPs (Interface Message Processors), conectados por linhas de transmissão de 56 Kbps, e ficou conhecida como ARPANET.

A primeira versão da ARPANET foi ao ar em dezembro de 1969, em caráter experimental, após muito trabalho e diversas dificuldades superadas. Possuía apenas quatro nós e conectava as universidades americanas de Utah, Universidade da Califórnia em Los Angeles (UCLA), Universidade da Califórnia em Santa Bárbara (UCSB) e

Universidade de Stanford (SRI). Esse pode ser considerado o embrião da rede física que daria origem à Internet. (Tanenbaum ,2002, p.53)

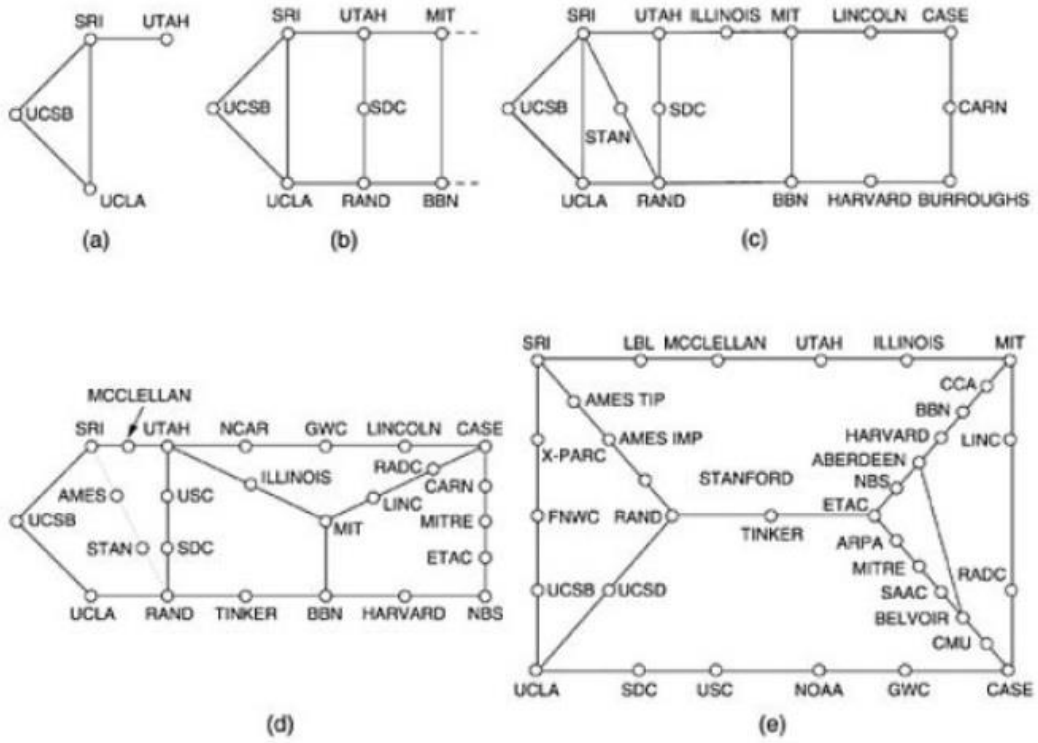


Figura 2 - ARPANET: dezembro de 1969 a setembro de 1972
Fonte: Tanenbaum (2003)

Observando-se a Figura 2 é possível verificar o espantoso crescimento da ARPANET nos seus primeiros anos, passando dos 4 nós iniciais (a) para uma rede de aproximadamente 34 nós em 1972 (e), apenas três anos após o seu início. Da observação da mesma figura fica evidente o incremento da robustez da rede, oferecida pelas redundâncias de caminhos alternativos, requisito inicialmente solicitado pelo DoD e alcançado no decorrer dos anos.

Inicialmente, a ARPANET era uma rede única e fechada. Entre os anos de 1972 a 1980, o número de redes começou a crescer, baseado principalmente em algumas inovações presentes na Internet até os dias de hoje, como o desenvolvimento do Protocolo Ethernet por Robert Metcalfe, que permitiu uma enorme proliferação das redes locais, e os protocolos TCP (Transmission Control Protocol), UDP (User Datagram Protocol) e IP(Internet Protocol), que podem ser considerados os três protocolos chave da Internet até os dias de hoje.

Entre os anos de 1980 a 1990 houve uma imensa proliferação de redes que foram sendo conectadas à rede original, além do desenvolvimento de protocolos como o X.25,

que iam agregando novos valores e serviços à ARPANET. A adoção do protocolo TCP/IP como padrão oficial da rede em 1983 e o desenvolvimento do conceito de DNS (Domain Name Server), que mapeava um endereço IP de 32 bits em um nome que qualquer ser humano fosse capaz de memorizar foram pontos chave para o aumento de sua popularidade. (Kurose, 2003, p.60)

Ainda na década de 1980, o governo americano, por intermédio da NSF (U. S. National Science Foundation), após verificar o imenso sucesso da ARPANET, e os ganhos que ela proporcionava para a pesquisa científica nos EUA, começou a preparar a sua sucessora. A ideia era criar uma rede que fosse aberta a qualquer grupo de pesquisa universitária, mesmo que a universidade em questão não estivesse ligada diretamente à ARPANET. Para iniciar esse projeto, a NSF decidiu construir a estrutura física central de uma rede (backbone) que interligava 6 supercomputadores espalhados por todo o país, como mostra a Figura 3. A NSFNET foi interconectada à ARPANET e foi de cara um grande sucesso, permitindo um grande aumento no número de usuários. (Tanenbaum ,2002, p.55)

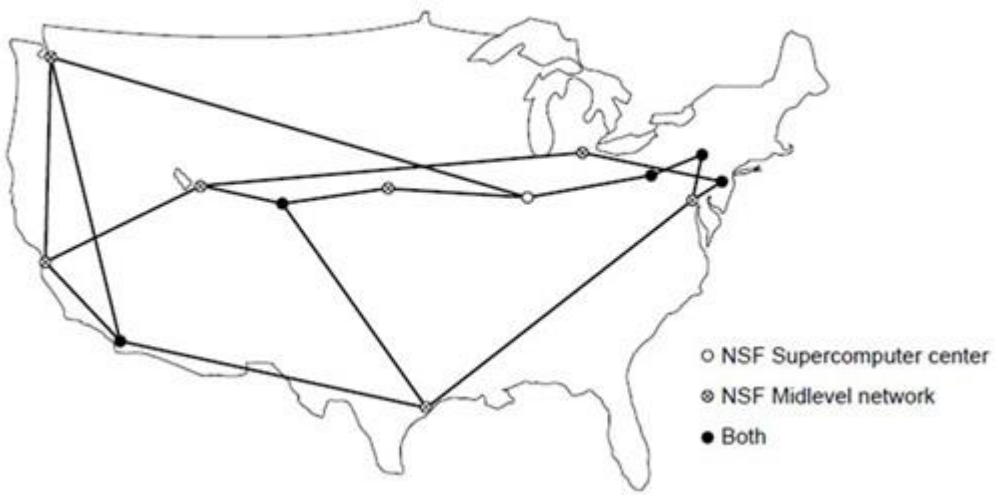


Figura 3 - Backbone NSFNET – 1988
Fonte: Tanenbaum (2003)

É possível observar que até aquele momento, início dos anos de 1990, o acesso à esta rede que seria a Internet era privilégio basicamente de pesquisadores ligados ao mundo acadêmico e alunos das universidades americanas, órgãos do governo dos EUA e pesquisadores da iniciativa privada. Porém, com a criação do “World Wide Web”, pelo físico e professor Tim Berners Lee, surge finalmente a rede mundial de computadores, a

INTERNET, de forma muito semelhante ao que conhecemos hoje em dia, e que teria uma expansão formidável em pouquíssimo tempo. (Kurose, 2003, p.63)

A partir deste ponto, milhares de aplicações passaram a ser desenvolvidas, que simplificaram a utilização daquele ambiente, antes restrito à especialistas e pesquisadores, trazendo milhões de usuários para a Internet, que viria a conectar praticamente todo o planeta.

Para que se tenha uma ideia da dimensão do crescimento da utilização da Internet ao longo do tempo, estima-se que em 1995 havia 16 milhões de usuários, representando 0,4 % da população mundial. Em dezembro de 2017 estima-se que o número de usuários fosse de 4,157 bilhões de usuários, representando 54,4% da população mundial (Internet World Stats, 2018).

A imensa popularização de algumas tecnologias, especialmente o computador pessoal e a Internet, contribuíram sobremaneira para o processo de globalização, que se acentuou a partir do final do século XX. Com a interdependência econômica, política e até mesmo psicossocial resultante, a maior parte dos sistemas essenciais para o funcionamento da sociedade moderna, bancos, sistema financeiro, hospitais, etc..., podem ser acessados atualmente através de um computador pessoal e de uma ligação à Internet, não importando onde se encontrem fisicamente.

Novas ameaças surgiram a partir desta nova dimensão de mundo, a dimensão virtual. Atreladas a ela, surgiram novas possibilidades de conflitos entre países ou mesmo ataques partindo de grupos não estatais, tão poderosos pelas suas consequências como um ataque de uma guerra convencional. É nesse contexto que surge a Guerra Cibernética.

A título de demonstração dos imensos riscos e perigos ligados à esta nova modalidade de combate, serão relatados adiante alguns casos históricos encontrados na literatura especializada, que podem servir de alerta e motivação para os que se interessam pelo assunto.

Por ser um assunto ainda novo, é interessante identificar as suas origens, como forma de facilitar o seu entendimento. Obviamente, pela complexidade do tema, principalmente pelo sigilo que muitas vezes o envolve por parte de governos e atores envolvidos, não se tem a pretensão de esgotar o assunto, apenas remontar e trazer à tona fatos devidamente registrados em fontes confiáveis e que ajudem a elucidar as origens da utilização do espaço cibernético como ferramenta de guerra.

Segundo Lawson (2011, p.3), as primeiras preocupações com a cibersegurança

surgiram ainda na década de 1980, nos EUA, quando se achava que a maior ameaça seria quanto à espionagem de segredos militares ou industriais americanos por outros países, devido à crescente dependência de computadores e suas redes de dados.

Já na década de 1990, segundo Lawson (2011, p.4), os especialistas americanos começaram a se preocupar com as possibilidades de ameaças às infraestruturas críticas da sociedade civil americana, através de possíveis atos de ciberterrorismo que poderiam ser conduzidos por atores não estatais. Essa preocupação foi reforçada pelas ações de invasão realizadas contra a Intranet da empresa General Electric (GE) e a intranet da rede de TV americana NBC, no ano de 1994, que causaram milhões de dólares em prejuízo (Almeida, 2011, p.88).

Ao final da década de 1990, no ano de 1999, o satélite inglês "Skynet" foi posto fora de ação, segundo a agência "Reuters", por obra de "Hackers" que teriam tomado o controle do satélite britânico (Almeida, 2011, p.88).

No início da administração de George W. Bush, no ano de 2001, as autoridades americanas acreditavam que a maior ameaça que poderiam sofrer em relação ao ciberespaço seria a partir de atores estatais. Certamente a partir dos ataques terroristas sofridos no 11 de setembro de 2001, a percepção de maior risco de ameaça cibernética aos EUA, por parte de seu governo, voltou a se concentrar em atores não estatais atuando contra infraestruturas civis (Lawson, 2011, p.4).

Embora a preocupação americana com a defesa cibernética tenha seguido a linha acima descrita, de acordo com Clarke (2010, p.9), em termos ofensivos, os EUA elaboraram planos para invadirem uma rede de computadores da defesa aérea do Iraque e inutilizar seus sistemas de radar e de mísseis, em 1990, durante a primeira guerra contra aquele país.

Essa ação seria realizada por meio de comandos infiltrados em bases no Iraque, que, juntamente com hackers da Força Aérea Americana, deveriam inserir programas que fizessem com que computadores da rede de todo o país travassem e fossem impossíveis de reiniciar. Embora essa ação não tenha sido realmente posta em prática, evidencia que já naquela época os americanos estavam começando a se preparar para aproveitarem as vulnerabilidades de seus inimigos no espaço cibernético.

Um pouco mais tarde, durante a Guerra do Kosovo, as Forças Americanas realmente utilizaram ataques cibernéticos para comprometer os sistemas de defesa aérea sérvios (Almeida, 2011, p.88).

Na segunda Guerra do Iraque, os iraquianos perceberam, antes da fase inicial de bombardeios, que a sua rede militar privada, que eles acreditavam segura e fechada, havia sido comprometida pelos americanos. E-mails enviados de dentro do próprio Ministério da Defesa iraquiano, foram enviados para milhares de oficiais do Iraque, com mensagens americanas, incentivando a deserção e a rendição das forças iraquianas. (Clarke, 2010, p.28)

Todas essas ações, conforme aconteciam e eram expostas deixavam claro para o mundo que a Era da Informação trazia consigo um novo conjunto de capacidades, que em consequência exigiria novas concepções de doutrina, organização, adestramento, materiais, educação, pessoal e infraestrutura. Mas era apenas o início.

Segundo Clarke (2010, p.26), no ano de 2007, a Força Aérea Israelense executou um ataque a uma instalação em construção no território Sírio, cuja finalidade seria a de abrigar uma instalação nuclear, com tecnologia norte coreana. O mais impressionante nessa ação não foi a completa destruição da instalação, ação relativamente comum para as Forças Armadas Israelenses em sua disputa com os países árabes da região, mas sim o fato de que os F-15 Eagle e F-16 Falcon israelenses, que não possuem tecnologia "stealth", não foram sequer notados pelos modernos sistemas de radares e defesa antiaérea sírios, adquiridos ao custo de bilhões de dólares da Rússia.

Apesar do silêncio inicial dos atores envolvidos, característica comum às ações cibernéticas desde o seu início e que muito dificulta o seu estudo e identificação, foi possível apurar à época, por fontes de imprensa e especialistas, que os israelenses conseguiram penetrar nos sistemas de radar sírios e fazer com que as telas de radar não mostrassem os aviões atacantes, mas se comportassem como se nenhum intruso estivesse se movimentando no espaço aéreo sírio, até que estes executassem o seu bombardeio.

Não foi possível identificar se a atuação cibernética se deu através de pulsos enviados por Veículos Aéreos Não Tripulados (VANTs), ou por agentes infiltrados no território sírio, porém ficou evidente que as Forças Armadas Israelenses executaram com uma precisão sem precedentes um ataque cibernético que lhes permitiu dominar as defesas aéreas sírias e fazer com que se comportassem da forma como Israel desejava. Foi uma demonstração prática e irrefutável dos novos riscos trazidos pela combinação de ações cibernéticas com ações de guerra convencional.

Desde então, houve inúmeras outras ações de Guerra Cibernética ao redor do mundo, e algumas delas serão abordadas em outros pontos deste trabalho de pesquisa, após a abordagem dos conceitos básicos relativos ao tema, que ocorrerá no Capítulo 3 e

facilitará o seu entendimento. Contudo, com base nos casos expostos até aqui, percebe-se claramente a importância do assunto e a sua relevância para a Defesa Nacional de qualquer país.

No caso do Brasil, embora com relativo atraso em relação à outras potências, principalmente EUA, Rússia e China, o assunto vem ganhando importância cada vez maior dentro da Doutrina de Defesa Nacional. Essa importância fica evidenciada pela inclusão do tema e a forma como é abordado na Política Nacional de Defesa (PND).

Conforme descrito na própria introdução do documento, a PND é o documento condicionante de mais alto nível do planejamento de ações destinadas à defesa nacional coordenadas pelo Ministério da Defesa. Voltada essencialmente para ameaças externas, estabelece objetivos e orientações para o preparo e o emprego dos setores militar e civil em todas as esferas do Poder Nacional, em prol da Defesa Nacional.

Sobre o setor cibernético, a PND enviada para a provação do Congresso Nacional no ano de 2016, no seu item 2.2.17, estabelece que:

> 2.2.17. Adicionalmente, o amplo espectro de possibilidades no ambiente cibernético requer especial atenção à segurança e à defesa desse espaço virtual, composto por dispositivos computacionais conectados em redes ou não, no qual transitam, processam-se e armazenam-se informações digitais, essenciais para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações, dos quais depende parcela significativa das atividades humanas.

Nesse item, fica claro que o país elenca o setor cibernético como essencial para o seu desenvolvimento e autonomia. A partir da identificação, pelo nível político, da área como estratégica para o país, diversas ações foram e estão sendo tomadas ao longo do tempo para que o Brasil consiga superar os desafios tecnológicos existentes e possa desenvolver as capacidades necessárias para proteger as suas infraestruturas críticas e sua sociedade de ameaças provenientes do espaço cibernético. No capítulo 5 serão abordadas essas políticas e estratégias desenvolvidas nos últimos anos na área de Defesa Cibernética.

1.1 PROBLEMA DE PESQUISA

O mundo se vê diante de uma proliferação cada vez maior das redes de computadores e da Internet, com o número de usuários alcançando a marca dos bilhões. O número

de serviços, essenciais ou não, que exigem cada vez mais conectividade aumenta a cada dia, tornando a sociedade cada vez mais dependente do ambiente virtual. Bancos, sistema financeiro, hospitais, redes de telecomunicações, redes de energia, redes de telefonia celular, entretenimento a partir de redes sociais, são exemplos de serviços e aplicações que se tornaram corriqueiros e que são acessados remotamente via algum tipo de rede de dados e muitos deles pela própria Internet.

Nesse ambiente complexo, surgem também novas ameaças, sendo a mais terrível a Guerra Cibernética, que tem o potencial de levar o caos ao mundo real, a partir desse mundo virtual, ainda pouco explorado e conhecido pela maioria dos seus usuários.

A fim de verificar as atuais ameaças da Guerra Cibernética para o mundo e de maneira mais específica para o Brasil, diante dos desafios impostos por essa vertente de poder ainda pouco desenvolvida em grande número de países, foi formulado o seguinte problema:

- Em face das ações de Guerra Cibernética identificadas ao redor do mundo até o presente momento, e das estruturas montadas pelos países mais desenvolvidos para enfrentarem este desafio, qual é a capacidade atual do Brasil para fazer frente a ataques a partir do espaço cibernético que suporta os serviços essenciais à sua sociedade, sejam eles perpetrados por nações agressoras ou grupos terroristas?

1.2 OBJETIVOS

1.2.1 OBJETIVO GERAL

Apresentar um estudo prospectivo sobre o atual estágio de desenvolvimento do tema Guerra Cibernética ao redor do mundo, e sobre o nível de preparo e a capacidade de defesa do Brasil, para o enfrentamento de ações de Guerra Cibernética que venham a ameaçar os diversos campos de poder da nação, tanto o campo militar, quanto o político, econômico, psicossocial e o tecnológico.

1.2.2 OBJETIVOS ESPECÍFICOS

Para tanto foram criados os seguintes objetivos específicos:

- Apresentar os aspectos mais relevantes de ações de Guerra Cibernética pelo mundo;

- Apresentar a estrutura existente atualmente no Brasil para fazer face a ações de Guerra Cibernética contra o país;

1.3 HIPÓTESE

Tendo em vista a dinâmica do mundo atual, altamente conectado às redes de dados, cada vez mais automatizado, especialmente em virtude da globalização, e os riscos advindos desse contexto, o domínio do tema Guerra Cibernética se faz necessário e indispensável para qualquer país que busque de forma séria e responsável manter a sua autonomia e sua soberania.

Sendo assim, analisando os diversos casos presentes na literatura, em que foram desencadeadas ações ofensivas no ambiente cibernético e suas características, que serviram de subsídio e base bibliográfica para este trabalho, foi formulada a seguinte hipótese:

- A conscientização e engajamento da sociedade civil, em conjunto com as Forças Armadas no Âmbito do Ministério da Defesa, são condições necessárias e imprescindíveis para que o Brasil atinja os seus objetivos estratégicos ligados à Segurança Cibernética.

1.4 VARIÁVEIS

Considerando-se que o objetivo principal deste trabalho é uma análise dos recursos cibernéticos do Brasil, e que a almejada capacidade de atuação do país no espaço cibernético está diretamente relacionada a estes recursos, procurou-se identificar fatores de relevância que possam afetar essa capacidade. Assim, foram elencadas como variáveis:

1.4.1 Variável Independente – atuação da sociedade civil

A definição da sociedade civil como a variável independente se dá porque de acordo com a hipótese levantada, o seu comportamento é determinante para o sucesso de uma nação, em especial o Brasil, na proteção do seu espaço cibernético. Este trabalho de pesquisa buscará mostrar que a conscientização dessa sociedade e sua atuação em conjunto com as Forças Armadas e o Ministério da defesa irão influenciar decisivamente os objetivos estratégicos de Segurança e Defesa Cibernética.

1.4.2 Variável Dependente – capacidade de atuação no espaço cibernético

A capacidade de atuação no ambiente cibernético foi definida como a variável dependente deste estudo porque ela vai determinar o estado final desejado para as pretensões brasileiras em relação ao espaço cibernético, e de acordo com a hipótese levantada, ela é relacionada e dependente do nível de conscientização da sociedade civil em relação ao tema.

1.5 CONTRIBUIÇÃO DA PESQUISA

A Guerra Cibernética é ainda um tema bastante novo no contexto mundial, com possibilidades e alcances ainda não totalmente mapeados, cujas ações registradas pelo mundo tem causado temor e assombro mesmo em países altamente desenvolvidos tecnologicamente, como é o caso dos EUA.

Por diversas questões relativas ao seu desenvolvimento histórico e suas dificuldades econômicas e sociais, o Brasil tem demonstrado grande dificuldade de acompanhar os desenvolvimentos tecnológicos de vanguarda que surgem no mundo, principalmente os mais recentes e com maior valor tecnológico agregado.

Sendo assim, este trabalho contribuirá para chamar a atenção para um tema extremamente atual e que pode ser considerado uma nova modalidade de combate, conferindo uma vantagem significativa para países que o dominem.

Outra contribuição importante será fazer um levantamento da atual estrutura montada para o enfrentamento das ameaças, apresentando resultados alcançados até o momento e as vulnerabilidades e sugestões de melhoria porventura encontradas.

2. METODOLOGIA

Este capítulo tem como finalidade apresentar a metodologia utilizada neste trabalho para a solução do problema de pesquisa enunciado. Assim, serão apresentados os procedimentos a serem realizados para alcançar os objetivos propostos, evidenciando a concepção metodológica, a delimitação da pesquisa e as limitações do método.

2.1 DELIMITAÇÃO DA PESQUISA

A pesquisa estará focada nas ameaças já registradas por ações de Guerra Cibernética no mundo, nos danos e consequências já registrados aos diversos campos de poder dos países que sofreram tais ataques e nas capacidades de defesa da sociedade brasileira e de suas Forças Armadas, em especial do Exército Brasileiro, frente às ameaças conhecidas e já documentadas e nas estruturas existentes no país para fazer frente aos desafios relativos ao tema Guerra Cibernética.

O tema Guerra Cibernética é muito amplo e seu alcance ainda pouco delimitado. Diversos tipos de ataques criminosos ocorridos no ambiente cibernético podem ser confundidos com ações de Guerra Cibernética. Sendo assim, este estudo irá buscar fazer uma clara distinção entre ataques criminosos e açõesde Guerra Cibernética propriamente dita, embora muitas vezes ataques aleatórios e isolados perpetrados por simples hackers e criminosos possam ser citados devido à utilização de métodos e tecnologias semelhantes e que podem vir a ser utilizadas, principalmente contra estruturas brasileiras conectadas ao espaço cibernético.

2.2 CONCEPÇÃO METODOLÓGICA

Segundo Prodanov (2013, p.14), a Metodologia é a aplicação de procedimentos e técnicas que devem ser observados para construção do conhecimento, com o propósito de comprovar sua validade e utilidade nos diversos âmbitos da sociedade.

Em busca de construção de conhecimento válido e útil, este trabalho de pesquisa foi desenvolvido a partir das seguintes etapas: levantamento e seleção bibliográfica, leitura da bibliografia selecionada e análise de dados.

Este trabalho realiza um estudo que pode ser classificado quanto aos seus objetivos

como exploratório e descritivo. Segundo Mattar (apud Oliveira, 2011, p.21), os métodos utilizados pelas pesquisas exploratórias são amplos e versáteis, e compreendem: levantamentos em fontes secundárias, levantamentos de experiências, estudos de casos selecionados e observação informal. Já de acordo com Gil (apud Oliveira, 2011, p.21), as pesquisas descritivas têm por finalidade principal a descrição de características de determinada população ou fenômeno. Esta pesquisa fará uso de fontes primárias e secundárias e estudos de caso selecionados. Além disso será feita uma descrição do fenômeno da Guerra Cibernética com estudos exploratórios sobre o tema, ainda relativamente novo e pouco explorado tanto no contexto brasileiro quanto no contexto mundial.

Este trabalho usa uma abordagem qualitativa, que segundo Triviños (apud Oliveira, 2011, p.24), trabalha os dados buscando o seu significado, tendo como base a percepção do fenômeno dentro do seu contexto. Prosseguindo, estabelece que o uso da descrição qualitativa procura captar não só a aparência do fenômeno como as suas essências, procurando explicar a sua origem, relações e mudanças e tentando intuir as suas consequências. Estes são os objetivos deste trabalho no que se refere à Guerra Cibernética, que por ser um assunto ainda novo carece de maiores estudos sobre suas origens e consequências, principalmente no cenário brasileiro.

Este trabalho faz uso de estudos de caso baseados nas experiências encontradas na literatura especializada sobre o assunto Guerra Cibernética, como o caso das eleições americanas de 2016, onde foram amplamente divulgadas pela imprensa mundial supostas manobras de “hackers” russos tentando influenciar o resultado supostamente em favor do agora Presidente Donald Trump. Este é sem dúvida um estudo de caso valioso pelas implicações e que serve de base para ilustrar os riscos potenciais de supostos ataques de Guerra Cibernética para a soberania de um país. Outros casos são também abordados, como as ações russas contra algumas de suas ex-repúblicas,

Esta pesquisa é também bibliográfica, com fontes baseadas em livros, artigos científicos, manuais militares, revistas e coleta de dados em fontes confiáveis na Internet, de forma a enriquecer o seu conteúdo.

2.3 LIMITAÇÕES DO MÉTODO

Esta seção tem por finalidade realizar uma descrição das limitações do método empregado para esta pesquisa.

Considerando-se o fato do assunto Guerra Cibernética ser ainda relativamente novo na história mundial, e principalmente pelas ações relativas ao tema serem na maioria das vezes cercadas de sigilo e tratadas como questões de segurança dos Estados envolvidos, em diversas ocasiões este trabalho de pesquisa irá se deparar com fatos ainda não totalmente esclarecidos e elucidados pelas fontes históricas tradicionais.

Nestes momentos, uma análise crítica das fontes e dos fatos em si será realizada para mostrar as questões envolvidas e as possibilidades existentes, evitando assim conclusões precipitadas e correntes ideológicas de pensamento que possam influenciar nas conclusões porventura explicitadas.

Além disso, nos pontos em que sejam tratados casos sem uma conclusão histórica, tais fatos serão tratados à luz dos ensinamentos que podem ser colhidos para efeitos de preparação contra atos daquela natureza, independente se houve uma confirmação formal ou não de sua existência, à luz da verdade histórica.

Novamente convém fazer esta ressalva pela característica sigilosa e dos interesses em jogo em um ambiente tipicamente de informação, contra informação e até mesmo desinformação como vem sendo cada vez mais comum, nos ambientes de Guerra Cibernética e algumas de suas possíveis vertentes, como a utilização de “Fake News” como será abordado posteriormente.

3. CONCEITOS DE GUERRA CIBERNÉTICA

3.1 GENERALIDADES

Este capítulo tem por objetivo apresentar os principais conceitos ligados à Guerra Cibernética, tendo em vista a necessidade de expor os fundamentos que irão embasar os aspectos mais técnicos porventura abordados durante este trabalho de pesquisa.

Diferente de outros temas, já consolidados por pesquisas científicas, não existe um consenso sobre uma definição de Guerra Cibernética. O manual MD31-M-08, Doutrina Militar de Defesa Cibernética, de 2014, apresenta a seguinte definição:

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

Já Camper (apud Carneiro, p.27), cita que uma das primeiras definições encontradas na literatura, estabelece que

> "a Guerra Cibernética corresponde ao uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil."

Observando-se as duas definições, é possível verificar que ambas situam a Guerra Cibernética em um contexto mais amplo, evidenciado pela citação dos Sistemas de Informação. Tal relação é imediata pois segundo Libicki (apud Costa, p.12) a Guerra Cibernética é uma das categorias de Guerra da Informação, que possui ainda seis outros tipos de operações, a saber: Guerra de Comando e Controle, Guerra baseada em Inteligência, Guerra Eletrônica, Guerra Psicológica, Guerra de Hacker e Guerra da Informação Econômica.

A tabela a seguir, apresentada por Castello Branco (apud Alencar, p. 19), traz um resumo dos tipos de operações encontrados na Guerra de Informação.

Tipo 1 – Command and Control Warfare (Guerra de Comando e Controle)	• Ataque a sistemas de comando e controle para separar o comando das forças.
Tipo 2 – Intelligence-Based Warfare (Guerra Baseada em Inteligência)	• Coleta, exploração e proteção de informações por sistemas que dão suporte a ataques em outras formas de guerra.
Tipo 3 – Electronic Warfare (Guerra Eletrônica)	• Combate de comunicações nas esferas da transferência física da informação (rádio-eletrônica) e dos formatos abstratos de informação (criptográfico).
Tipo 4 – Psychological Warfare (Guerra Psicológica)	• Combate contra a mente humana.
Tipo 5 – Hacker Warfare (Guerra de Hacker)	• Combate em todos os níveis sobre a Infraestrutura Global de Informação (GII).
Tipo 6 – Economic Information Warfare (Guerra da Informação Econômica)	• Controle da economia por meio do controle de informações por bloqueios ou controles imperialistas.
Tipo 7 – Cyber Warfare (Guerra Cibernética)	• Formas abstratas futurísticas de terrorismo, combates completamente simulados e controle da realidade são combinados nesta categoria de guerra e são considerados relevantes apenas a longo prazo.

Tabela 1: Operações de Guerra de Informação
Fonte: Alencar (2010)

Retornando às definições de Guerra Cibernética apresentadas, percebe-se que as duas são importantes no âmbito do que se pretende nesta pesquisa, porque não apenas se complementam, mas permitem que se inicie uma abordagem mais completa, que não se preocupa apenas com o aspecto militar que a palavra “Guerra” poderia sugerir, mas também com as suas consequências que podem ser eminentemente civis, mesmo em um contexto mais abrangente que envolva também ações militares convencionais.

É exatamente essa característica da Guerra Cibernética, a atuação sobre estruturas civis, que a torna tão impactante e perigosa para a sociedade moderna. Observando-se as ações registradas pela literatura específica, que serão abordadas de forma aprofundada em capítulos posteriores, os principais alvos são as infraestruturas críticas de um Estado, que resultarão maiores impactos nos campos de poder econômico, político, militar, psicossocial ou científico. Alguns exemplos são:

- Infraestruturas do setor energético;
- Infraestruturas do setor financeiro;
- Infraestruturas de transportes;
- Infraestruturas de telecomunicações;
- Infraestruturas da rede de saúde.

Essas infraestruturas são, em praticamente todo o mundo, conectadas a redes de dados que permitem uma série de funcionalidades e facilidades em sua operação e gerenciamento, mas que também aumentam os riscos à sua segurança. Para que se compreenda na plenitude esses riscos, é necessário o entendimento do conceito de Espaço Cibernético.

3.2 O ESPAÇO CIBERNÉTICO E A INTERNET

Libicki (2009, p.6), caracteriza o espaço cibernético como um aglomerado de dispositivos computacionais individuais que são conectados entre si e ao mundo exterior via algum tipo de rede de comunicações.

Já o manual EB70-MC-10.232, Guerra Cibernética, define o Espaço Cibernético como o espaço virtual composto por dispositivos computacionais conectados em redes ou não, onde as informações digitais transitam e são processadas e/ou armazenadas.

Embora a definição apresentada por Libicki seja um pouco mais intuitiva, a abordagem do manual de Guerra Cibernética do Exército Brasileiro é mais abrangente e pode ser melhor explorada. Inicialmente porque faz menção ao fato do espaço cibernético ser um espaço virtual, trazendo consigo uma nova realidade e até mesmo uma nova forma de percepção de mundo. O espaço virtual pode ser considerado até mesmo como uma nova dimensão, que não se restringe aos conceitos já consagrados de espaço físico, embora necessite de alguma estrutura física para existir.

Exatamente para facilitar o entendimento, o espaço virtual e em consequência o espaço cibernético costuma ser dividido em camadas, de acordo com abordagens diversas. Uma divisão interessante é apresentada por Carneiro (2012, p.80), contendo três camadas:

- Camada Física: é o componente físico da rede e inclui o componente geográfico. Inclui todo o hardware e a infraestrutura que suporta a rede e os conectores (fios, cabos, rádio frequência, roteadores, servidores, computadores, etc...)
- Camada lógica: consiste nas conexões lógicas existentes entre os nós da rede. Esses nós são os dispositivos físicos conectados a uma rede (computadores, roteadores, telefones celulares, etc...)

- Camada Social: representa os aspectos humanos e cognitivos que interagem com as camadas anteriores.

Verifica-se claramente, das camadas acima, que o espaço cibernético é construído utilizando as facilidades oferecidas pelas camadas física e lógica, sendo utilizado pelas pessoas que com ele interagem e que formam a camada social.

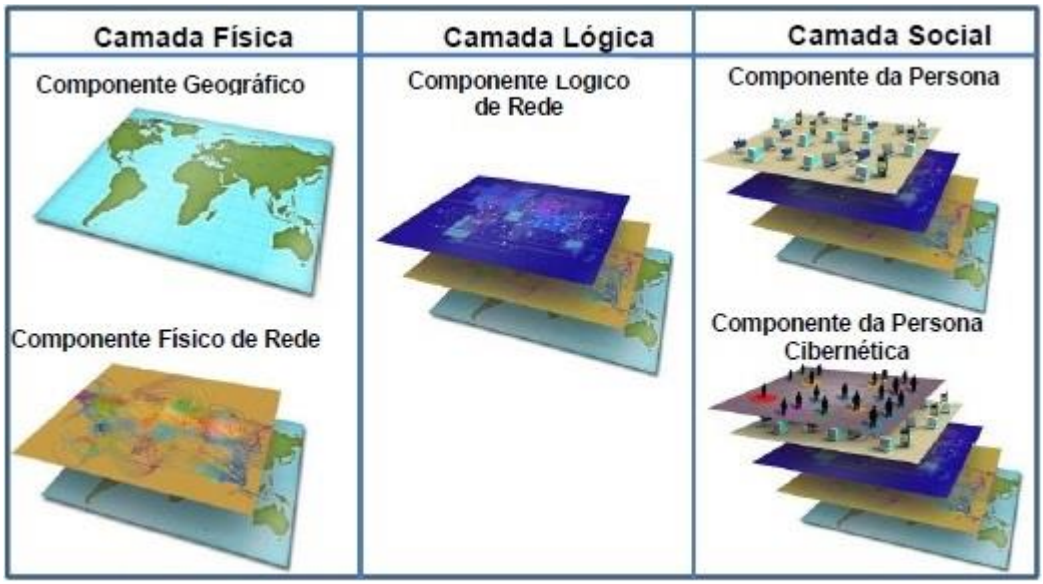


Figura 4 - Camadas do Espaço Cibernético
Fonte: Carneiro (2012)

Uma outra característica importante que deve ser observada da divisão em camadas apresentada é que embora a camada física inclua o componente geográfico, e assim respeite as fronteiras geopolíticas existentes entre os países, as informações que por ele transitam podem ser acessadas a partir de diversos pontos do espaço virtual em questão de segundos. Essa é uma característica importantíssima do espaço cibernético, que permite que ele não respeite os marcos fronteiriços normalmente já consagrados, abrindo assim novas perspectivas geopolíticas no cenário internacional, que podem ser exploradas por ações de guerra cibernética.

Retornando à definição apresentada pelo manual de Guerra Cibernética, ela diz que o espaço cibernético é composto por dispositivos computacionais conectados em redes ou não. Essa é uma distinção importante, porque permite a discussão da participação da Internet no espaço cibernético.

O Capítulo 1 apresentou a origem e a evolução da Internet até os dias atuais, tendo em vista a sua dimensão e alcance mundial e, em consequência, a sua importância para as ações cibernéticas. Porém, é preciso ter em mente que o espaço cibernético inclui a

Internet, mas não se limita a ela. Existem máquinas e redes que não se conectam à Internet, até por questões de segurança, mas que estão contidas no espaço cibernético e que podem ser acessadas por ações de guerra cibernética, embora sem dúvida, a Internet, pelas facilidades que apresenta à vida moderna, e pelas vulnerabilidades inerentes que possui, representa a maior ameaça em termos de Guerra Cibernética, como ficará claro mais adiante.

Em dezembro de 2017, estimou-se que 54,4 % da população mundial, cerca de 4,2 bilhões de pessoas, fosse usuária da Internet (Internet World Stats, 2018). Essas pessoas são atraídas para a grande rede por um número infindável de aplicações e serviços que estão cada vez mais presentes na vida moderna. Na atualidade, é difícil fazer distinção entre um telefone celular conectado simplesmente à sua rede de telefonia móvel ou à Internet.

O que se iniciou como consequência das facilidades oferecidas pela Internet, acabou criando uma nova cultura indissociável da vida moderna, o que faz com que diversas daquelas infraestruturas críticas citadas na seção 3.1, tenham o seu funcionamento atrelado à serviços acessados via grande rede. O setor financeiro, por exemplo, incluindo os bancos, tem grande parte de seus serviços disponíveis para seus usuários via Internet, inclusive a movimentação de recursos financeiros.

E como foi possível observar na evolução da Internet, embora ela tenha se iniciado como uma aplicação militar, e certamente com diversos requisitos importantes de segurança, com o tempo essa finalidade acabou sendo desvirtuada e as preocupações ligadas à segurança da rede e de seus usuários deixou de ser um aspecto essencial. Portanto, a Internet, por si só, é considerada um ambiente virtual inseguro, ficando por conta de seus usuários o desenvolvimento de aplicações que tornem os seus serviços seguros.

E mesmo aquelas infraestruturas críticas que não estão conectadas à Internet diretamente, estão conectadas, em sua maioria, ao espaço cibernético, permitindo assim que sejam desenvolvidas formas de acessá-las, mesmo sem a autorização de seus administradores.

Por tudo o que foi exposto até aqui, o espaço cibernético (incluindo a Internet) é classificado pela literatura especializada como um novo domínio que se abre para disputa no combate moderno, em conjunto com os domínios terrestre, marítimo, aéreo e espacial, onde as ações ofensivas e defensivas de Guerra Cibernética se desenvolvem.

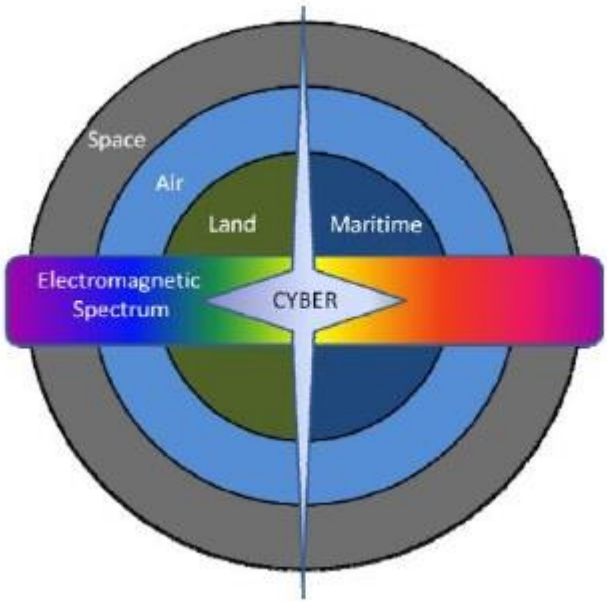


Figura 5 - Domínios de Combate
Fonte: Carneiro (2012)

3.3 ATAQUES E VULNERABILIDADES UTILIZADOS NA GUERRA CIBERNÉTICA

O objetivo deste trabalho não é abordar de maneira aprofundada os tipos de ferramentas utilizadas para executar ações de Guerra Cibernética e os tipos de ataques a elas associados. Porém, como se pretende demonstrar a importância da participação da sociedade civil em conjunto com as Forças Armadas dos respectivos países na prevenção dessas ações, torna-se necessário apresentar alguns conceitos relacionados e que serão necessários mais adiante.

Uma das principais motivações para esta seção é o fato de que grande parte das ações de Guerra Cibernética já registradas, fizeram uso das vulnerabilidades encontradas nas redes conectadas ao espaço cibernético (através da Internet ou não). Essas vulnerabilidades normalmente ocorrem por conta de má configuração das aplicações por parte de seus desenvolvedores, mal uso por parte de usuários, que muitas vezes não utilizam corretamente essas aplicações, ou ambos.

Essas vulnerabilidades são utilizadas por softwares maliciosos que muitas vezes infectam os computadores ou dispositivos móveis dos usuários, normalmente sem o seu conhecimento, e são utilizados no momento oportuno pelos agentes empenhados em realizarem ações de Guerra Cibernética, com resultados extremamente danosos para as sociedades impactadas por essas ações.

As ações realizadas normalmente utilizam os seguintes vetores (Nakamura, 2007, p.79)(CERT.BR, 2018a) :

- Vírus: foram introduzidos na década de 1980 e são pedaços de códigos maliciosos escritos com o objetivo de corromper o funcionamento de um computador, copiar e/ou roubar informações privadas. Um vírus infecta uma máquina a partir de uma aplicação hospedeira, fazendo cópias de si mesmo e tentando infectar outros computadores.
- Worm: diferente do vírus, não precisam de portadores para se replicarem. Eles se auto replicam e se espalham de um computador para outro, podendo ainda conter vírus para infectar outro sistemas.
- Spywares: são programas maliciosos que infectam uma máquina sem o consentimento de um usuário e normalmente sem o seu consentimento com a finalidade de roubar informações e obter informações sensíveis de pessoas físicas ou de empresas.
- Trojan: também conhecidos como “trojan horses” ou cavalos de tróia, infectam um determinado sistema operacional de um computador como se fossem outros programas inofensivos, mas sua real intenção é a de abrir “portas” (“backdoors”) nos sistemas operacionais, sem o conhecimento do usuário, permitindo assim outros tipos de ataques. A partir desse “backdoor”, a máquina pode ser invadida ou até mesmo controlada por outras pessoas, em diversos níveis, dependendo da sofisticação do ataque executado.
- Bombas lógicas: são tipos específicos de vírus ou worms que infectam as máquinas sem o conhecimento de seus usuários e permanecem inertes por determinado tempo, sendo executados quando uma determinada condição ocorre. São muito utilizados em ataques de negação de serviço.
- Ataques de negação de serviço: são ações que visam sobrecarregar determinado serviço acessado normalmente via Internet, de maneira que os computadores que executam esses serviços sejam inundados por requisições (solicitações) para que prestem os serviços ou informações que foram projetados para prestarem, num tempo muito curto. O objetivo deste tipo de ataque é sobrecarregar a máquina que presta o serviço com uma quantidade maior de solicitações de serviço do que ela pode atender num determinado período de tempo.

- Ataques de Pishing: são tentativas de enganar os usuários da Internet fazendo com que eles forneçam informações sigilosas, como senhas e números de contas bancárias. Normalmente são utilizados e-mails falsos, tentando se fazer passar por aplicações legítimas, como os verdadeiros bancos dos usuários.
- Botnets: são redes de computadores que são controladas remotamente sem o conhecimento de seus usuários, executando tarefas automatizadas que podem ter como objetivo disseminar vírus, disseminar spams, atacar servidores ou cometer fraudes pela Internet. São também chamados de redes zumbis.

Como a Internet ocupa grande parte do espaço cibernético, com uma quantidade imensa de usuários, as aplicações e serviços que são oferecidos por ela acabam sendo o alvo da maior parte das ações de Guerra Cibernética. A Internet apresenta diversas falhas de segurança que facilitam a proliferação dos vetores e aplicações maliciosas citadas anteriormente.

Algumas dessas falhas são citadas por Clarke (apud Bernat Júnior, 2012, p. 31) e condensadas na forma das seguintes vulnerabilidades:

- Sistema de endereçamento e dependência do DNS: pela forma que o endereçamento da Internet foi realizado, utilizando o protocolo IP, com endereços de 16 números, e o imenso número de usuários e aplicações, principalmente após a inserção do sistema de hipermídia “www”, foi necessário o desenvolvimento do DNS, que representa uma vulnerabilidade por ter sido idealizado com pouca preocupação com a segurança e ser um alvo constante de ataques e indisponibilidade de serviços e sistemas para a maior parte das aplicações quando os ataques que os seus servidores sofrem são bem sucedidos.
- Sistema de roteamento dinâmico ou Protocolo BGP (“Border Gateway Protocol”): é o protocolo responsável por rotear (ou seja, direcionar) o tráfego entre as redes de provedores diferentes. Não há mecanismo de verificação interna no protocolo BGP, de forma que determinado tipos de ataques são capazes de modificar as suas tabelas de rotas, utilizadas para a tomada de decisão para onde os pacotes IP serão roteados em cada caso.
- Navegação em claro: a maior parte do tráfego que utiliza a Internet está em claro e apenas uma pequena parcela utiliza criptografia. Assim, a maior parte das informações é suscetível a interceptação e as informações podem ser

utilizadas por terceiros.

- Capacidade de propagar softwares maliciosos: a Internet não possui, por si só, nenhum tipo de verificação em relação ao que está trafegando entre os seus nós ou equipamentos de rede. Sendo assim, os softwares e códigos maliciosos se propagam com relativa facilidade.
- Projeto descentralizado: a Internet como foi visto, se iniciou como um projeto do Departamento de Defesa dos EUA, mas foi logo "abandonado" por aquele órgão em relação à finalidade inicial que se idealizava e deixado a cargo da iniciativa privada. A partir daí, foi se expandindo, buscando agregar as novas funcionalidades que surgiam, que por sua vez atraíam cada vez mais usuários, em um círculo vicioso que se se realimenta mesmo nos dias atuais, dificultando o controle e o seu gerenciamento, principalmente nos aspectos relativos à segurança do espaço cibernético.

Observando-se a descrição dos diversos vetores e programas maliciosos que podem ser utilizados em ações cibernéticas, percebe-se que as mesmas ferramentas podem ser utilizadas em crimes cibernéticos. É importante assim identificar a diferença entre os dois tipos de ações.

Para os fins a que se destina este trabalho de pesquisa, serão consideradas ações de Guerra Cibernética as ações de um Estado-nação ou grupo organizado que tenha objetivos políticos, contra outro Estado-nação, nos níveis político, estratégico, operacional ou tático, com a intenção de atingir alguma de suas expressões de poder, a partir do espaço cibernético.

Ações de grupos organizados, contra empresas ou pessoas físicas, utilizando os mesmos métodos, mas visando apenas a subtração de recursos financeiros a partir do espaço cibernético, serão considerados apenas crimes cibernéticos e não serão objeto de discussão.

Um exemplo extremamente interessante que reflete esta diferença é a ação de supostos hackers coreanos contra a empresa americana Sony Pictures Entertainment.

No ano de 2014, quando o filme "The interview" (A entrevista), que satirizava o líder máximo da Coreia do Norte, Kim Jon Um, estava previsto para estrear, diversas ameaças começaram a ser feitas à empesa americana que era a distribuidora do filme, no caso a Sony, aos cinemas que apresentassem o filme e aos próprios Estados Unidos, caso o filme viesse a ser exibido. As ameaças foram feitas por um grupo que se auto intitulava "Os

Guardiões da Paz" e foram amplamente divulgadas através das principais redes de informação mundiais, como CNN, Deutsche Welle, BBC, entre outros.

Embora a estreia do filme tenha sido adiada, de outubro para 25 dezembro, no final do mês de novembro ou início de dezembro um ataque cibernético classificado como sem precedentes pela própria empresa foi efetuado contra a Sony (BBC, 2014). Na ação foi roubada uma quantidade imensa de dados e informações sigilosas da empresa e de seus funcionários. Algum tempo após a ação, diversos desses dados, como filmes ainda não lançados pela empresa e salários de seus executivos foram divulgados em diversos sites, causando prejuízo financeiro e embaraço para a companhia.

Novas ameaças foram feitas caso o filme fosse exibido, o que levou a Sony a cancelar a sua exibição em um primeiro momento, e em um segundo momento, após pressões do próprio governo americano, o filme acabou sendo exibido em um número reduzido de salas, já que diversos cinemas se negaram a exibi-lo, temendo represálias dos hackers.

Devido à repercussão do caso, o FBI foi chamado e após avaliar o software, técnicas e fontes de redes utilizadas na ação, divulgou que o ataque era de origem norte coreana (Oliveira, 2015, p.45).

Para os efeitos desta pesquisa, a ação ocorrida contra a empresa Sony é considerada um ataque de Guerra Cibernética, por algumas razões. A razão principal é que as investigações apontam para uma ação de um Estado-nação, no caso a Coréia do Norte, contra um alvo situado no coração de outro Estado-nação, os EUA.

O ataque foi realizado contra uma empresa privada americana, mas em um contexto de uma disputa estratégica que ocorre entre os americanos e norte coreanos nos últimos anos, que gira em torno das tentativas do regime de Kim Jon Um de produzir armas nucleares. O ataque foi dirigido de forma direta contra a expressão psicossocial dos EUA, atingindo um ponto nevrálgico de propagação de sua cultura e que o povo americano preza e valoriza, a sua indústria cinematográfica.

O ataque, porém, atingiu também a expressão política dos EUA, causando embaraço político, já que uma disputa estratégica com um país consideravelmente menor e menos poderoso gerou efeitos adversos dentro do próprio território americano, sendo necessário que o governo se posicionasse defendendo que a empresa não cedesse à pressão e mantivesse a exibição do filme. O próprio Presidente Barack Obama criticou a o recuo da empresa na exibição do filme (www.elpais.com/brasil).

E finalmente a ação atinge também a expressão de poder militar americano, tendo

em vista a incumbência das Forças Armadas Americanas em relação à Defesa Cibernética do país e de suas estruturas críticas. Cabe aqui a observação de que o povo americano valoriza muito a sua cultura e seus valores, principalmente a liberdade de expressão, que foram muito afetados neste caso.

Esse episódio deixou claro não apenas para a Coreia quanto para todo o mundo, que apesar do seu pioneirismo na Internet e de todo o seu desenvolvimento tecnológico, mesmo um país como os EUA possui vulnerabilidades que podem ser exploradas no espaço cibernético. Mesmo por países (ou quem sabe grupos terroristas) muito menos desenvolvidos em outras áreas, mas que estão investindo em conhecimentos relativos ao espaço cibernético.

4. AÇÕES E ESTRATÉGIAS DE GUERRA CIBERNÉTICA AO REDOR DO MUNDO

4.1 GENERALIDADES

A importância do tema Guerra Cibernética está sendo demonstrada na prática neste início de século, tanto pelos diversos ataques que puderam ser identificados em conflitos localizados ao redor do mundo, como pelas ações que tem sido realizadas pela maioria dos países para se prepararem para fazer face a esta nova modalidade de ameaça.

Sendo assim, neste capítulo serão descritas algumas das principais ações ofensivas de Guerra Cibernética e seus efeitos no contexto dos conflitos em que estavam enquadradas, assim como as principais ações estratégicas adotadas por alguns países para o desenvolvimento da área cibernética em suas sociedades.

A escolha dos países a serem abordados se deu pelo seu ativismo na área ou pela importância estratégica dos mesmos para a geopolítica mundial. Desta forma, foram identificados como sendo de maior relevância os Estados Unidos da América, a Rússia e a China, tanto pelo seu peso geoestratégico quanto pelo seu ativismo na área cibernétcia. O Brasil será tratado em um capítulo a parte.

4.2 Estados Unidos da América

Devido ao seu pioneirismo em relação à Internet e seu alto nível de desenvolvimento tecnológico, os Estados Unidos da América têm buscado protagonismo em relação à atuação no ambiente cibernético.

Principalmente a partir da década de 1990, com a popularização da Internet, as preocupações do Departamento de Defesa Americano com as vulnerabilidades que poderiam ameaçar os EUA a partir da conexão de suas redes com a Internet aumentaram sensivelmente. No ano de 1995, o General da Força Aérea Albert J. Edmonds, então diretor da Agência de Defesa de Sistemas de Informação (Defense Information Systems Agengy – DISA) ao proferir uma palestra na Universidade de Harvard alertou que as redes de computadores dos EUA eram vulneráveis a ataques remotos (USA, 2018a).

No final da década de 1990, a preocupação com a defesa dessas redes era da própria DISA, por intermédio da Força Tarefa Conjunta de Defesa de Redes de Computadores (Joint Task Computer Network Defense – JTF-CND), primeira organização do DoD com autoridade para supervisionar e dirigir operações nas redes de dados daquele

departamento. Essa Força Tarefa se transformou no final de 1999 na Força Tarefa de Operações em Redes de Computadores (Joint Task Computer Operations – JTF-CNO) (USA, 2018a).

No ano de 2000, o Comando Espacial dos Estados Unidos (USSPACECOM) assumiu as funções cibernéticas do DoD que pertencial ao JTF-CNO. Um pouco mais tarde, o USSSPACECOM foi dissolvido e algumas de suas funções relativas a defesa das redes de computadores americanas foram absorvidas pelo Comando Estratégico dos Estados Unidos (USSTRATCOM) no ano de 2002 (USA, 2018a).

Em 2004, a JTF-NCO se transformou na Força Tarefa Conjunta de Operações de Gedes Globais (JTF-GNO) e neste mesmo ano a Estratégia Militar Nacional Americana passou a incorporar o conceito de que o Ciberespaço era um domínio, assim como os domínios aéreo, terrestre, marítimo e espacial, e como tal os EUA deveriam possuir condições de operar através dele com ampla liberdade de ação (USA, 2018a).

No ano de 2005, o USSTRATCOM foi reorganizado, sendo criados diversos componentes conjuntos com finalidades específicas, entre eles o Comando Componente Funcional Conjunto para Guerra em redes (JFCC-NW). Em 2008, o JFCC-NW assumiu o controle do JTF-GNO para facilitar as operações integradas no Ciberespaço (USA, 2018a).

Ao final do ano de 2008, o secretário de Estado Gates dirigiu a criação de um novo comando unificado, o Cibercomando americano (USCYBERCOM), que deveria operar sob a autoridade do USSTRATCOM. Essa criação envolveu também um acordo com a NSA (National Security Agency), que àquela altura também estava bastante envolvida em operações no ciberespaço, ocasionando inclusive disputas com os meios militares em relação a este tema. Para solucionar a questão, o Diretor da NSA se tornaria um General de quatro estrelas que também seria Diretor do USCYBERCOM. Este comando se tornou operacional em maio de 2010 (USA, 2018a).

O Presidente Donald Trump decidiu, no ano de 2017, aceitar a recomendação do Secretário de Defesa James Mattis e elevar o USCYBERCOM, localizado em Fort Mead, a um comando combatente unificado responsável pelas operações cibernéticas, não mais estando subordinado ao USSTRATCOM. A mudança se concretizou em maio de 2018. (USA, 2018b)

O USCYBERCOM executa as suas atividades por intermédio das unidades cibernéticas componentes existentes nas diversas Forças Armadas dos EUA, a saber (apud Bernat Júnior, 2012, p. 16):

- 2nd Army – U.S. Army Cyber Command (ARCYBER);
- 24th Air Force – Air Forces Cyber (AFCYBER);
- U.S. Tenth Fleet – Fleet Cyber Command (FLTCYBER);
- U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER).

É possível observar a estrutura do DoD na Fig 8, destacando-se a elevação do US-CYBERCOM à condição de grande Comando, já aparecendo como o décimo Comando combatente na estrutura do Departamento. A figura possui uma observação informando que a elevação ainda ocorreria, mas a mesma já está em vigor conforme mencionado neste capítulo.

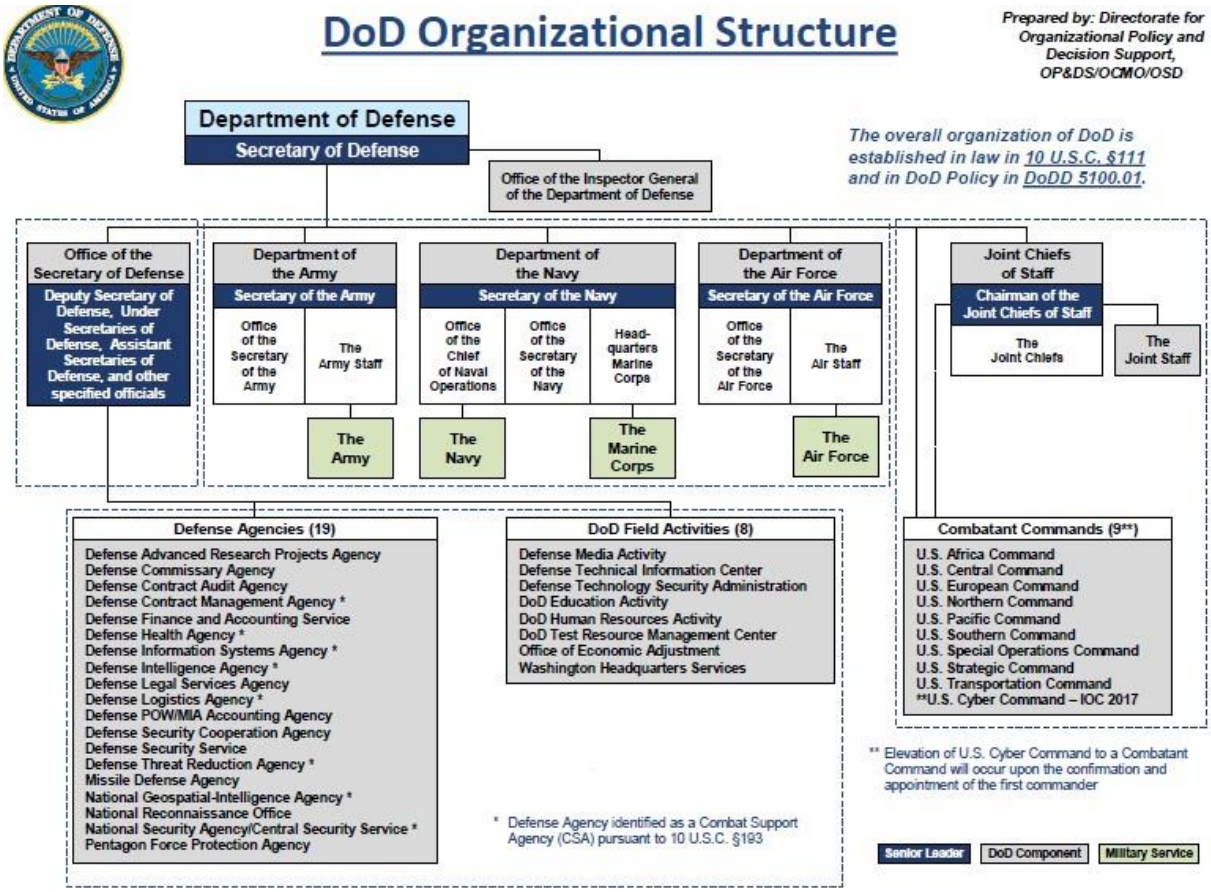


Figura 6: Departamento de Defesa dos EUA
Fonte: USA (2018)

Especificamente em relação ao Espaço Cibernético, o DoD estabeleceu no ano de 2011 cinco iniciativas estratégicas USA-2011 (apud Bernat Júnior, 2012, p. 44) que ainda estão sendo praticadas dentro dessa nova conformação do USSCYBERCOM:

- Primeira iniciativa estratégica: O DoD irá tratar o ciberespaço como um domínio operacional para organizar, treinar, e equipar, de forma que seja possível ao

DoD se aproveitar de todas as suas vantagens potenciais.

- Segunda iniciativa estratégica: o DoD irá empregar novos comceitos operacionais de defesa para defener as suas redes e sistemas.
- Terceira iniciativa estratégica: o DoD irá realizar parcerias com outras agências do governo americano e com a iniciativa privada, que permitam estabelecer uma estratégia completa de segurança cibernética.
- Quarta iniciativa estratégica: o DoD irá estreitar os laços com os aliados americanos e parceiros internacionais de forma a aumentar a cibersegurança coletiva.
- Quinta iniciativa estratégica: o DoD irá trabalhar para diminuir a ingenuidade da nação em termos de atuação nos ambientes cibernéticos, na tentativa de gerar uma força de trabalho cibernético excepcional, capaz de produzir com rapidez inovações tecnológicas na área em questão.

Das estratégias citadas, é preciso destacar as grandes vantagens americanas devido às possibilidades de parcerias com a iniciativa privada. Destaca-se em relação a este tema que os EUA tem uma história de sucesso envolvendo parcerias entre o seu governo, a sua base industrial e suas universidades. A chamada triplice hélice foi capaz de alavancar o desenvolvimento americano em várias áreas do conhecimento, sendo o desenvolvimento inicial da Internet, entre muitos outros que poderiam ser citados, um exemplo clássico desse sucesso.

Também é preciso destacar a identificação, na quinta iniciativa, da necessidade de desenvolver no povo americano como um todo os conhecimentos necessários à utilização correta e segura dos serviços disponíveis e cada vez mais comuns no espaço cibernético, principalmente a Internet. A partir dessa declaração, é possível concluir que o governo americano identifica que sem essa conscientização, todos os esforços do DoD e seus órgãos ligados à defesa cibernética ficarão seriamente comprometidos, principalmente devido às vulnerabilidades que podem surgir do uso da Internet sem os cuidados mínimos com a segurança pelos usuários americanos em suas atividades, sejam elas profissionais ou sociais.

4.3 Rússia

A Rússia surgiu nos últimos anos como um dos países que mais tem sido associado

a ações de Guerra Cibernética no mundo. Uma série de ações à ela atribuídas em diversos conflitos demonstram que o gigante russo tem conseguido se adaptar à nova era e entender as potencialidades deste novo tipo de guerra.

Com o fim da União das Repúblicas Socialistas Soviéticas em 1991, a Rússia, sua herdeira natural precisou se readaptar à nova geopolítica mundial. Uma transição difícil para uma economia de mercado no início da década de 1990, com programas radicais de desestatização e liberalização econômica, provocou grande inflação, recessão, desemprego e crescimento do crime organizado, na forma das máfias que arpoveitaram a transição para se expandir por vários setores da nova economia.

Sob a liderança do então Presidente Bóris léltsin, foi um período turbulento para o país, que viu seu prestígio e sua tradicional influência internacional serem questionados e diminuírem consideravelmente, principalmente em diversas das ex-repúblicas soviéticas localizadas em sua tradicional área de interesse geopolítico, o Leste Europeu. Ao mesmo tempo, a Rússia observava o seu tradicional rival da Guerra Fria, os EUA, se consolidarem no papel de única superpotência mundial, assim como foi obrigada a permitir um alargamento da aliança militar da OTAN.

Esse cenário começou a mudar com a ascenção do Presidente Vladimir Putin no ano 2000. Após um período voltado para a recuperação de sua economia, através de ofensivas voltadas principalmente para as empresas que exploram os principais recursos energéticos do país, buscando recuperar o seu controle acionário, a Rússia voltou a se sentir forte o bastante para tentar restaurar, ao menos em parte, o seu poder regional perdido na década de 1990.

A consequência imediata foi uma série de conflitos com ex-repúblicas soviéticas, nos quais a Rússia empregou não apenas as suas forças armadas convencionais, mas principalmente utilizou diversas ações de Guerra Cibernética que mostraram ao mundo toda a sua eficiência e potencial.

O primeiro país a sofrer tais ataques foi a Estônia, que havia se tornado independente da URSS em 1989. O conflito com a Rússia se iniciou em 2007, quando por pressões populares, o legislativo da Estônia aprovou a Lei das Estruturas Proibidas, que determinava que qualquer símbolo que fizesse menção às cinco décadas de ocupação soviética fosse derrubado (Clarke, 2010, p.33). Isso incluía a estátua de um soldado de bronze do Exército Vermelho, situada na capital da Estônia, e erguida para lembrar o sacrifício feito pelo Exército Soviético para libertar a Europa dos nazistas na II Guerra mundial.

Além do simbolismo existente na estátua, havia soldados soviéticos enterrados ao redor da mesma, o que provocou um forte posicionamento de Moscou declarando que derrubar o Soldado de Bronze seria difamar os soldados soviéticos mortos. Na tentativa de contornar a crise o Presidente estoniano vetou a lei, provocando um aumento das pressões internas, fosse de cidadãos estonianos favoráveis à retirada da estátua, fosse de cidadãos russos moradores da região, que defendiam a sua permanência (Clarke, 2010, p.33).

Após a eclosão de um conflito entre manifestantes russos e estonianos em torno da derrubada da estátua, naquela que ficou conhecida como Noite de Bronze, as autoridades estonianas moveram a estátua numa tentativa de acalmar o conflito.

Logo após, a Estônia foi vítima de um ataque cibernético até então sem precedentes (Clarke, 2010, p.34). O país sofreu um ataque distribuído de negação de serviço (DDoS) que levaram ao colapso os principais servidores do país. Este é um tipo de ataque em que milhares, de computadores são mobilizados para enviar *pings* a vários alvos na Internet. Um "ping" é um comando para que um computador envie um pacote padronizado a outro computador específico, por meio do seu endereço IP. Neste tipo de ataque, os milhares de computadores infectados enviam simultaneamente os pacotes "ping" a um alvo específico, inundando-os e fazendo com que não consigam responder à demanda provocada e parem de funcionar corretamente.

Os computadores atacantes são chamados de *botnet*, uma rede robótica de computadores "zumbis" controlados remotamente. Os zumbis atacam seguindo instruções que são acionadas sem o conhecimento de seus proprietários (Clarke, 2010, p.34). Esses computadores muitas vezes estão infectados há semanas ou mesmo meses, apenas esperando um comando do seu computador "mestre" para que iniciem o ataque.

O ataque de DDoS à Estônia foi sem precedentes até aquele momento porque normalmente, servidores que sofriam este tipo de ataque eram atingidos por pouco tempo, dias no máximo. No caso da Estônia porém, o ataque durou semanas e atingia centenas de sites importantes do país, de forma ininterrupta, impedindo-os de voltar a funcionar corretamente.

Durante o ataque, foram atingidos servidores que apoiavam parte da rede telefônica da Estônia, do sistema de cartões de crédito e do serviço de diretório da Internet, do Hansapank, que era o maior banco do país, afetando o comércio e os serviços de comunicação, provocando caos e prejuízo ao país.

A Estônia solicitou apoio à OTAN, que mobilizou um equipe para apoiar o país, mas os ataques continuaram, já que os computadores zumbis aparentemente se adaptaram,

talvez reprogramados pelo seu “mestre” (Clarke, 2010, p.34).

Especialistas rastrearam os “*pings”* e alegaram que as máquinas de controle finais estavam na Rússia, e que o código do programa havia sido escrito em alfabeto cirílico (Clarke, 2010, p.34). O país negou com veemência qualquer participação nos ataques, mas se recusou a identificar os autores que alegava-se estarem em seu território.

Pressionado, o governo russo admitiu que os ataques poderiam ter partido de nacionalistas russos em seu território, inconformados com os acontecimentos na Estônia e sua “hostilidade contra o povo russo”. Mas negou que tais nacionalistas fossem patrocinados ou mesmo incentivados pelo governo russo.

O ataque cibernético levou a OTAN a criar, em 2008, um centro de defesa cibernética a poucos quilômetros do local onde o soldado de bronze gigante originalmente ficava, onde há agora um pequeno e agradável bosque (Clarke, 2010, p.39).

A criação desse centro não foi capaz porém de impedir que novas ações cibernéticas vitimassem outra nação independente da Europa Oriental, também ex-república soviética. A Geórgia tornou-se um Estado independente com a dissolução da URSS em 1991. Porém, no ano de 1993 as populações russas dos territórios da Ossétia do Sul e da Abkhásia, apoiadas por Moscou, expulsaram o Exército Georgiano de suas regiões e se declararam independentes.

Embora a Geórgia e a maior parte da comunidade internacional não reconhecessem a independência dos dois territórios, a sua situação de “independência” se manteve inalterada com apoio russo até o ano de 2008, quando ataques de mísseis contra aldeias georgianas provenientes da Ossétia do Sul levaram o Exército da Geórgia a novamente investir contra a região na tentativa de retomar o controle dos territórios separatistas.

Ao mesmo tempo em que o Exército russo avançava para a Ossétia do Sul para expulsar os georgianos, os sites do governo da Geórgia e dos seus meios de comunicação sofreram um ataque de DDoS, que bloquearam diversos serviços, incluindo os seus acessos aos sites de eissoras internacionais como BBC e CNN (Clarke, 2010, p.41).

O conflito terminou com cerca de 850 mortes e o deslocamento de mais de 100 mil pessoas. Além disso, os dois territórios tiveram a sua independência reconhecida pela Rússia, que após concordar em abandonar a região como resultado do acordo de paz firmado por mediação da França, foi convidada pelos governos independentes a retornar como sua benfeitora.

Porém, a característica mais interessante desse conflito, tendo em vista a imensa

disparidade entre as duas forças armadas, foi a maneira como o combate cibernético se desenvolveu. Os ataques cibernéticos foram crescendo de intensidade ao longo do desenrolar do conflito físico, até chegar ao ponto da Geórgia perder completamente o controle sobre o domínio ".ge" do país, e ficar completamente sem acesso a qualquer fonte de notícia ou informação externa, sendo forçada a mudar sites do governo para outros países (Clarke, 2010, p.43).

O Governo Georgiano até que tentou fazer face aos ataques cibernéticos utilizando diversas soluções, sendo uma delas o bloqueio do tráfego que era proveniente da Rússia. Porém os ataques foram redirecionados e começaram a vir de outros locais, como a China. Os ataques também fizeram uso de botnets espalhadas por diversos países e obrigaram os bancos georgianos a desligarem seus servidores, ao mesmo tempo em que bancos internacionais encerraram suas conexões com a Geórgia, já que durante o conflito, os russos fizeram suas botnets atacarem a comunidade bancária internacional simulando ataques provenientes da Geórgia (Clarke, 2010, p.45).

Novamente o governo russo negou qualquer envolvimento com os ataques cibernéticos que atingiram a Geórgia, alegando que poderiam ser iniciativa do povo da Rússia, sem o seu controle, mas especialistas na área cibernética rastrearam o tráfego dos ataques a sites ligados ao aparato de inteligência russa (Clarke, 2010, p.46).

Certamente um aspecto muito importante a ser salientado sobre os ataques cibenéticos à Geórgia é que o seu alto nível de coordenação e sofisticação, a sua complementaridade com as ações cinéticas russas, além do alto nível de controle que o país historicamente sempre teve sobre os seus aparatos de inteligência, além do controle que estes sempre exerceram sobre a sua sociedade, deixam poucas margens de dúvidas sobre a sua autoria.

A crise da Rússia com a Ucrânia, pela posse da Crimeia, também desencadeou ataques cibernéticos entre os países, com acusações mútuas que duram até os dias de hoje. Com início em novembro de 2013, devido à recusa da Ucrânia em assinar um acordo comercial que vinha sendo encaminhado com a União Europeia (UE), por pressões russas, a crise levou à manifestações populares ucranianas contra o seu Presidente Yanukovich, que resultaram em sua fuga em fevereiro de 2014 após mais de 80 mortos em conflitos e manifestações e sua posterior destituição (BBC, 2014b).

Após a queda do Presidente, a península da Crimeia, de grande importância geopolítica para a Rússia, por permitir acesso ao Mar negro, foi tomada por manifestantes pró-

Rússia e seu Parlamento aprovou a sua libertação da Ucrânia e sua anexação pelo Estado Russo. Essa decisão foi ratificada por um referendo popular, apesar de fortes pressões internacionais contrárias (BBC, 2014c).

Com as tensões o governo russo decidiu enviar tropas à região da Crimeia para proteger os cidadãos russos (58,3% dos aproximadamente 2 milhões de habitantes da região). Após o referendo na Crimeia o governo russo anunciou que anexaria formalmente a região ao seu território em março de 2014.

Durante a crise da Crimeia, ainda segudo a BBC, as Forças de Segurança da Ucrânia acusaram a Rússia de ter bloqueado as comunicações celulares do país, assim como diversos sites de serviços na região da Crimeia sofreram ataques de DDoS segundo o INFOSEC Institute.

Posteriormente, devido ao clima de permanente tensão que se instalou entre os dois países, diversos ataques cibernéticos foram realizados no decorrer dos anos, provocando prejuízos de milhões de dólares ao governo ucraniano, mas cuja autoria é constantemente negada pelo governo russo (BBC, 2018d).

Uma análise dos conflitos citados permite concluir que a Rússia vem desenvolvendo ao longo dos anos capacidades importantes no campo cibernético que tem permitido que ela se movimente com grande liberdade de ação pelo espaço cibernético, principalmente em ações que envolvam o seu entorno estratégico.

Devido ao sigilo que envolve o tema e as constantes negativas do governo russo em relação à sua participação em ações cibernéticas contra outros países, existem poucas fontes de pesquisa disponíveis envolvendo órgãos ou estruturas específicas voltadas para a Guerra Cibernética. Porém, segundo Branco Júnior (apud Alencar, 2010, p. 29), a Rússia possui uma grande organização de inteligência que trata de Guerra da Informação e, por consequência, dos assuntos relativos à G Ciber: a Agência Federal do Governo para Comunicações e Informações (*Federal'naya Agenstvo Pravitel'stvennoy Svayazi i Informatsii – FAPSI).*

Segundo Carneiro (2012, p.98), só recentemente a Rússia divulgou a sua estratégia de Guerra da Informação, no documento intitulado "Visões conceituais sobre as ações das Forças Armadas da Federação da Rússia no espaço de informação" elaborado em 2011 e divulgado no site do Ministério da Defesa no início de 2012. O documento porém foi considerado vago pelos especialistas e pouco esclarecedor em relação à estruturas e organizações do país que podem ser relacionadas ao tema.

4.4 Rússia e EUA: o caso da eleição americana de 2016

O caso da eleição americana de 2016, em que o Presidente Donald Trump foi eleito, suscitou uma série de desconfianças e até mesmo denúncias sobre possíveis interferências russas que teriam sido capazes de mudar o resultado da eleição a favor do novo Presidente eleito.

Caso essa interferência tenha realmente ocorrido com sucesso, principalmente pela possível utilização do ambiente virtual de forma decisiva como muitos alegam, teria sido certamente uma ação sem precedentes. Pelos métodos utilizados e pelo resultado alcançado.

Até o presente momento ainda não se tem uma conclusão sobre o assunto, tanto pela dificuldade inerente de apuração em relação à atividades virtuais, quanto pelo sigilo envolvido nas investigações, já que a segurança nacional da nação mais poderosa do planeta, assim como seu orgulho, estão em jogo. Além disso, sempre que questões políticas envolvem uma discussão, sempre existirão grupos ou facções propensos a apoiarem um lado em detrimento do outro, em muitas situações ignorando inclusive indícios e provas técnicas, mesmo que sejam abundantes.

Sendo assim, mesmo sem a possibilidade de esgotar o assunto, optou-se por abordar a questão neste trabalho de pesquisa, buscando mostrar os métodos utilizados na suposta ação, os atores envolvidos e analisando de forma isenta e imparcial os fatos que se apresentaram em torno do tema, com o objetivo de colher ensinamentos que possam auxiliar a prevenir ou identificar este tipo de ação no futuro.

A suposta interferência russa durante a campanha presidencial americana para as eleições de 2016 teria acontecido principalmente de duas formas. Uma delas por meio da utilização de “hackers” que teriam invadido os computadores dos comitês de campanha de ambos os partidos políticos americanos (Partido Democrata e Partido Republicano) e tido acesso a emails trocados pelos seus integrantes, acessando diversas informações que poderiam embaraçar os candidatos a Presidência, no caso a candidata do Partido Democrata Hillary Clinton e o candidato do Partido Republicano Donald Trump. A segunda forma de interferência teria sido por meio da utilização de páginas e perfis criados em redes sociais que seriam fontes de “fake news”, numa tentativa de influenciar a eleição americana.

No que diz respeito à invasão das redes dos comitês dos partidos, o jornal americano

New York Times, em sua edição online do dia 23 de abril de 2017, publicou um artigo com o título "CIA had evidence of Russian effort to help Trump earlier than believed", em tradução livre "A CIA teve acesso a evidências de esforços russos para ajudar Trump mais cedo do que se acreditava" (New York Times, 2017).

O artigo traz uma série de depoimentos de fontes de inteligência e evidências que mostram que realmente houve acesso de hackers russos aos computadores dos comitês americanos, corroborando as informações veículadas em diversas outras fontes da mídia e até mesmo fontes oficiais do governo americano.

Algumas das informações obtidas pelo acesso às redes em questão foram tornadas públicas através do "Wikileaks" (site especializado em vazamentos de informações sigilosas) e outras fontes, trazendo embaraços à campanha da candidata Hillary Clinton. Segundo o New York Times, embora as fontes de inteligência apontem para acesso russo aos comitês eleitorais dos dois partidos, o material relativo ao Partido Republicano não foi divulgado, aumentando as desconfianças de um suposto favorecimento russo à campanha do atual Presidente Donald Trump.

O jornal afirma ainda que tanto a CIA quanto o FBI possuíam, ainda antes da eleição americana de 2016, um alto grau de certeza de que havia uma tentativa em curso por parte dos russos de favorecerem Donald Trump naquela eleição presidencial. Outra agência da comunidade de segurança americana, a NSA, apresentava nesta mesma época um grau de certeza moderado em relação à esta questão.

Outras fontes da comunidade de inteligência eram mais cautelosas na afirmação de que os russos estavam tomando partido de algum dos candidatos, mas reconheciam ainda assim a tentativa de interferência, no que classificavam como uma tentativa de desacreditar a democracia americana.

Com relação à utilização de notícias falsas, as "fake news", elas foram bastante utilizadas no processo eleitoral americano de 2016. Com a imensa popularização das mídias sociais, tanto o problema das "fake news" quanto o seu impacto, principalmente nos processos políticos e sociais dos Estados, tem sido cada vez mais debatidos.

Embora seja tratado em diversos momentos como algo novo, a utilização de notícias falsas com diferentes objetivos não é novidade. Histórias de monstros marinhos que eram capazes de engolir navios inteiros, atuação de bruxas, entre outros estão registradas na literatura mundial e mostram que este fenômeno é bastante antigo.

A grande diferença que existe nos dias de hoje é a utilização coordenada e

estratégica das “fake news”, utilizando recursos cibernéticos, com o propósito de interferir em processos importantes, especialmente políticos, como foi o caso da eleição presidencial americana de 2016. A extrema conectividade e disponibilidade de informações em diferentes plataformas surgidas como consequência da Revolução Informacional, somadas à correria do mundo moderno, criam ambiente propício para a propagação desse tipo de notícia.

E no caso específico da eleição americana de 2016, tanto fontes da Inteligência dos EUA, como pesquisadores independentes, chegaram à conclusão que a Rússia lançou uma sofisticada campanha de propaganda para interferir no resultado da eleição. Essa campanha incluiu a criação de de uma rede de “websites” e perfis em mídias sociais para espalhar notícias falsas, atacando a candidata Hillary Clinton (Timberg, apud Nelson, p.4, 2016).

É certamente tarefa extremamente complexa avaliar o real impacto da utilização de “fake news” para o resultado final da eleição americana de 2016. Porém, é possível afirmar que grande parte da mídia americana, baseada em investigações jornalísticas que utilizam fontes, normalmente não reveladas, da Inteligência americana, acredita que houve realmente interferência russa com o objetivo de favorecer o atual Presidente Donald Trump.

Certamente, por outro lado, muitos acreditam que as afirmações sobre essa interferência russa não passam de teoria da conspiração, alimentadas pelos partidários da candidata derrotada. Consideram que uma democracia sólida como a americana estaria imune a tais interferências e duvidam até mesmo que os russos tivessem os meios ou mesmo intenção de realizá-las.

Embora não seja possível afirmar que especificamente os russos tiveram a intenção de interferir no processo eleitoral americano, é possível afirmar que os governos das grandes nações desenvolvem atividades, dentro do contexto das operações de Informação, para influenciar o comportamento de um determinado público alvo e seu processo decisório.

E um dos maiores indícios da existência desse tipo de atividade vem do próprio governo americano, que no ano de 2010 lançou um edital de licitação no dia 22 de junho, no site “www.FedBizOpps.gov”, que realiza pregões do governo americano. No edital é licitada a prestação de um serviço de gerenciamento de pessoas cibernéticas online, cujo software permitiria que cada operador gerenciasse dez pessoas diferentes, completas, com contexto, histórico e presença cibernética que pudessem interagir através de plataformas de diversas mídias sociais (Carneiro, 2012, p.82).

Esse edital é extremamente importante porque ele descreve, na forma de uma solicitação de serviço, ainda no ano de 2010, um método extremamente utilizado na

propagação de “fake news” nos dias de hoje, que é a utilização de perfis falsos em redes sociais, que espalham os mais diversos tipos de notícias. Esses perfis são realmente capazes de enganar as pessoas que interagem com eles, pois possuem todas as características de qualquer outro perfil real, e apenas investigações mais detalhadas são capazes de mostrar que são falsos e não correspondem à pessoas reais.

Utilizando-se esse método, nações como os EUA ou a própria Rússia seriam capazes de montar verdadeiros exércitos virtuais contendo grandes quantidades (com números difíceis de determinar) de perfis falsos nas mais diversas redes sociais, que podem apoiar quaisquer causas e ideias, com o objetivo de influenciar a maneira como as pessoas, especialmente eleitores, enxergam determinado asssunto ou candidato a cargo eletivo. Quando se verifica que foram identificados diversos desses perfis falsos atuando durante a campanha eleitoral americana de 2016, independente de conclusões sobre o seu impacto no resultado final, percebe-se que esta é uma ameaça real e de potencial ainda desconhecido.

Por fim, com base nas informações conhecidas sobre a ação dos “hackers” vazando notícias dos comitês eleitorais e também sobre o que se sabe em relação às “fake news”, é possível afirmar que os indícios de uma tentativa de interferência russa, utilizando recursos cibernéticos, na eleição de Donald Trump são realmente muito fortes e não podem ser desconsiderados.

4.5 China

A China tem ocupado cada vez mais espaço como uma potência geopolítica nos últimos anos. Combinando aspectos de liberalização econômica com a hegemonia do Estado na produção, além de um regime fechado de partido único no campo político, o país apresentou taxas de crescimento econômico surpreendentes no final do século XX que o projetam como uma potência capaz de rivalizar em um futuro próximo com os EUA em todos os campos, inclusive o militar.

Buscando se desenvolver em todas as suas expressões de poder, a China tem feito grandes esforços nos últimos anos para desenvolver seus setores estratégicos, entre eles o setor cibernético, com resultados importantes nessa área.

Os Estados Unidos e a China, atualmente, são os principais atores mundiais no ambiente cibernético. Eles estão entre os mais apontados pela imprensa especializada como

responsáveis por ataques a diversos países, especialmente entre eles mesmos (Cruz Júnior, 2013, p.13).

Um caso importante de atuação cibernética ocorreu durante o desenvolvimento dos caças F-35 e F-22 pela Força Aérea Americana. Segundo Mccaul (apud Cruz Júnior, 2013, p. 7), o governo norte-americano reconheceu que houve acessos não autorizados aos arquivos de desenvolvimento dos caças F-35 e F-22 da Força Aérea norte- americana. Cerca de dois anos depois, a China apresentou seus próprios jatos, em muitos aspectos semelhantes aos caças americanos que tiveram os dados invadidos.

Este caso acaba por corroborar uma característica peculiar apontada por especialistas da comunidade internacional na área cibernética em relação à China, que é o envolvimento entre suas agências militares e de inteligência com o setor corporativo do país, especialmente em ações cibernéticas.

Outro caso importante ocorreu em abril de 2009, quando *hackers*, que se acredita serem apoiados pelo regime comunista chinês, penetraram nos computadores críticos para o funcionamento de redes de energia elétrica dos Estados Unidos e instalaram um *software* que permitia interromper o serviço quando comandado (Oliveira, 2015, p.80).

Os casos se repetiam com uma frequência tão grande que, em 2010, um consultor independente do governo americano registrou que nos´anos anteriores era comum funcionários americanos terem suas redes de computadores parcialmente interrompidas por dias deois de invasões normalmente atribuídas aos chineses (Presidência da República-Secretaria de Assuntos Estratégicos, 2011, p.81).

Segundo Feakin (apud Oliveira, 2015, p. 71) o Exército de Libertação Chinês possui três Departamentos, nomeados como Segundo, Terceiro e Quarto, ficando a critério deste último as operações cibernéticas de ataques a redes de computadores. Essa estrutura pode ser vista na Figura 9.

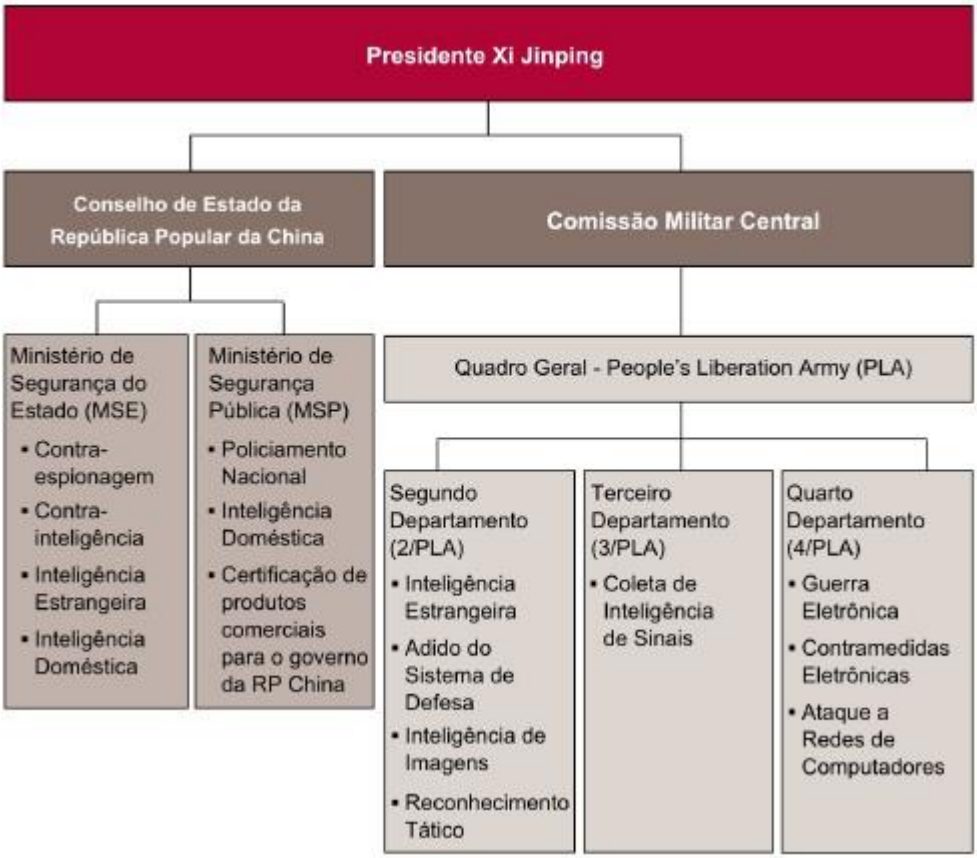
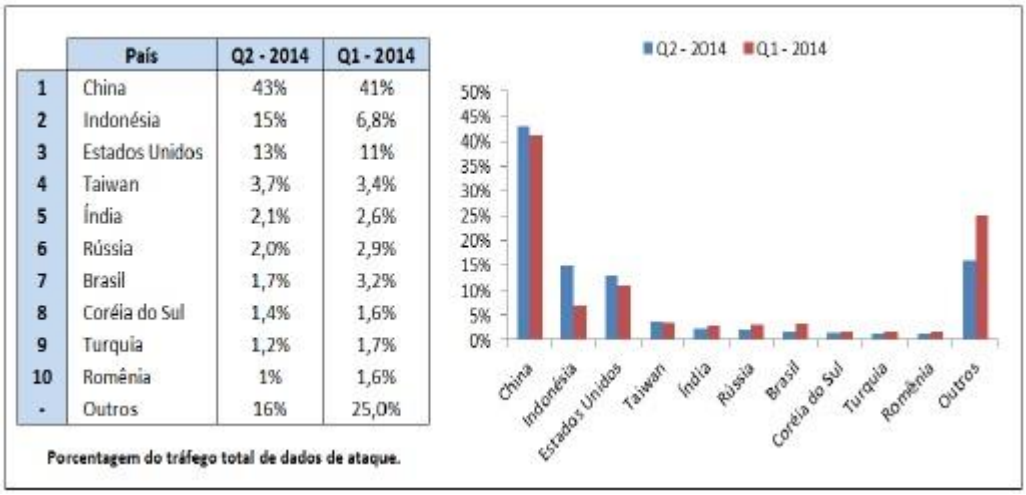


Figura 7: Estrutura de poder da China
Fonte: Oliveira (2015)

A China possui a capacidade de guerra cibernética mais extensa e mais praticada da Ásia atualmente, atrás apenas de Rússia e EUA. Tem sido registrado um grande número de treinamentos de ataques cibernéticos por parte das Forças Armadas da China. Essa grande quantidade de exercícios denota a crescente importância que o país dá ao assunto e o pesado investimento que vem sendo feito na área (Oliveira, 2015, p.69).

O Exército de Libertação do Povo já desenvolveu centenas de *trojans* e ferramentas similares. Além disso, a Academia Chinesa de Ciências, que fornece sugestões sobre a Política Nacional de Segurança da Informação e do Direito, criou o Laboratório de Estado da Segurança da Informação (Carneiro, 2012, p.106).

Existe na atualidade uma grande desconfiança em relação à atuação da China no espaço cibernético, principalmente pelos dados obtidos em relação ao tráfego de dados relativos a ataques cibernéticos. A figura abaixo mostra os citados ataques, ocorridos no ano de 2014, primeiro e segundo quadrimestre (Q1 e Q2).



	País	Q2 - 2014	Q1 - 2014
1	China	43%	41%
2	Indonésia	15%	6,8%
3	Estados Unidos	13%	11%
4	Taiwan	3,7%	3,4%
5	Índia	2,1%	2,6%
6	Rússia	2,0%	2,9%
7	Brasil	1,7%	3,2%
8	Coréia do Sul	1,4%	1,6%
9	Turquia	1,2%	1,7%
10	Romênia	1%	1,6%
-	Outros	16%	25,0%

Porcentagem do tráfego total de dados de ataque.

Figura 8: Fonte Oliveira (2015)

A capacitação na área cibernética é realizada na Academia do Comando de Comunicações (em Wuhan), na Universidade de Engenharia de Informação (em Zhengzhou) e na Universidade Nacional de Ciência e Tecnologia para a Defesa (em Changsha) (Costa, 2010, p. 32).

5. A DEFESA CIBERNÉTICA NO BRASIL

A partir da inclusão do tema Defesa Cibernética na PND, o setor ganhou maior relevância e respaldo para a priorização e implementação das ações práticas necessárias ao seu desenvolvimento. Como consequência direta, a Estratégia Nacional de Defesa (END), documento que orienta os segmentos do Estado brasileiro quanto às medidas que devem ser implementadas para que os objetivos nacionais sejam alcançados, estabelece o setor cibernético como estratégico e essencial para a Defesa Nacional, em conjunto com o setor espacial e o setor nuclear.

A END prossegue definindo as responsabilidades sobre cada um dos setores considerados estratégicos. Sendo assim, ela atribui à Marinha do Brasil a responsabilidade pelo desenvolvimento do Setor Nuclear, à Força Aérea a responsabilidade pelo Setor Espacial e ao Exército Brasileiro a responsabilidade pelo Setor Cibernético.

Além disso, a END reconhece a importância da atuação conjunta da sociedade nas suas vertentes civil e militar para o domínio do ambiente cibernético e sua defesa efetiva. Esta importância pode ser destacada no seguinte trecho daquele documento:

> No **Setor Cibernético**, as capacitações destinar-se-ão ao mais amplo espectro de emprego civil e militar. Incluirão, como parte prioritária, as tecnologias de comunicações entre as unidades das Forças Armadas, de modo a assegurar sua interoperabilidade e a capacidade de atuar de forma integrada, com segurança.

Prosseguindo em suas definições, o documento em questão ressalta ainda mais a necessidade imperativa de cooperação entre civis e militares, da seguinte forma:

> Para tanto, deverá ser fortalecida a atuação colaborativa entre o Setor de Defesa e a comunidade acadêmica nacional, os setores público e privado e a Base Industrial de Defesa. Adicionalmente, é importante que sejam intensificadas as parcerias estratégicas e o intercâmbio com as Forças Armadas de outros países, sobretudo daqueles que compõem o entorno estratégico do Brasil.

Por fim, buscando acelerar ainda mais o desenvolvimento do setor cibernético, e alinhada com os Objetivos Nacionais de Defesa (OND), a END inseriu o Setor Cibernético em uma série de Ações Estratégicas de Defesa (AED), priorizando ainda mais as atividades relativas ao tema. As AED que se relacionam com o setor Cibernético são as seguintes:

- AED-1 Desenvolver os setores estratégicos de defesa (nuclear, cibernético e espacial).
- AED-2 Contribuir para o incremento do nível de segurança das Estruturas Estratégicas (sistema de captação, tratamento e distribuição de água, geração e distribuição de energia elétrica, sistemas de transporte, produção e distribuição de combustíveis, finanças, comunicações e cibernética).
- AED-69 Promover o desenvolvimento da tecnologia cibernética.

Com essa visão estratégica sobre a questão cibernética, diversas ações efetivas para o desenvolvimento do setor tem sido realizadas, especialmente dentro das Forças Armadas. A seguir serão abordadas algumas dessas ações, tanto no âmbito da sociedade civil quanto na esfera militar.

As considerações expostas nessa seção sobre a END, assim como as considerações sobre a PND, são baseadas na versão mais atual, que está em apreciação pelo Congresso Nacional, enviada no ano de 2016 e ainda não aprovada.

5.1 A Defesa Cibernética no EB

Considerando-se a responsabilidade confiada ao Exército Brasileiro na END, em relação ao desenvolvimento da Defesa Cibernética, era de se esperar que as maiores ações relativas ao tema fossem tomadas no âmbito da Força Terrestre. E realmente, percebe-se nos últimos anos uma série de ações efetivas que demonstram a preocupação com o tema.

A estruturação da Defesa Cibernética no âmbito do Exército teve início no ano de 2009, com a assinatura da Portaria Nr 03 RES, de 31 de junho, que insituiu a criação do Setor Cibernético no EB, dividindo-o em três níveis: o político, que trata da Segurança da Informação, o Estratégico que trata de Defesa Cibernética e o Operacional que se refere à Guerra Cibernética. (Costa, 2010, p. 17).

Prosseguindo com a estruturação do setor cibernético no âmbito do EB, foi ativado no ano de 2010 o Núcleo do Centro de Defesa Cibernética (NuCDCiber), pela Portaria nº 667 do Comandante do Exército (Carneiro, 2012, p.72). Esse núcleo tinha como responsabilidade inicialmente estruturar os diversos temas de interesse na área Cibernética, como gestão de pessoal, capacitação, estruturação do setor e seu emprego.

No ano de 2012, o Ministro da Defesa, através do Decreto nº 7.809, decidiu transformar o NuCDCiber em uma estrutura conjunta, criando assim o Centro de Defesa Cibernética (CDCiber). Posteriormente, através da Portaria nº 3.028, do Ministério da Defesa, ainda no ano de 2012, foi atribuída ao CDCiber a responsabilidade pela coordenação e

integração das atividades de defesa cibernética no âmbito do Ministério da Defesa (Carneiro, 2012, p.63).

Com o crescimento de importância do tema no cenário mundial, e com a necessidade de colocar o país em condições de obter liberdade de ação no espaço cibernético em um prazo razoável, maiores investimentos continuaram sendo feitos no setor dentro da Força Terrestre, sendo finalmente criado em 2014, através da Portaria Normatida do MD nº 2.777 o Comando de Defesa Cibernética (ComDCiber), dentro da estrutura regimental do Exército.

O novo Comando criado foi posicionado em Brasília, na mesma área do Centro de Comunicações e Guerra Eletrônica do Exército (CCOMGEx), por uma questão de racionalização de meios. O CDCiber passou a integrar a estrutura do ComDCiber, conforme pode ser visualizado na Figura 11.

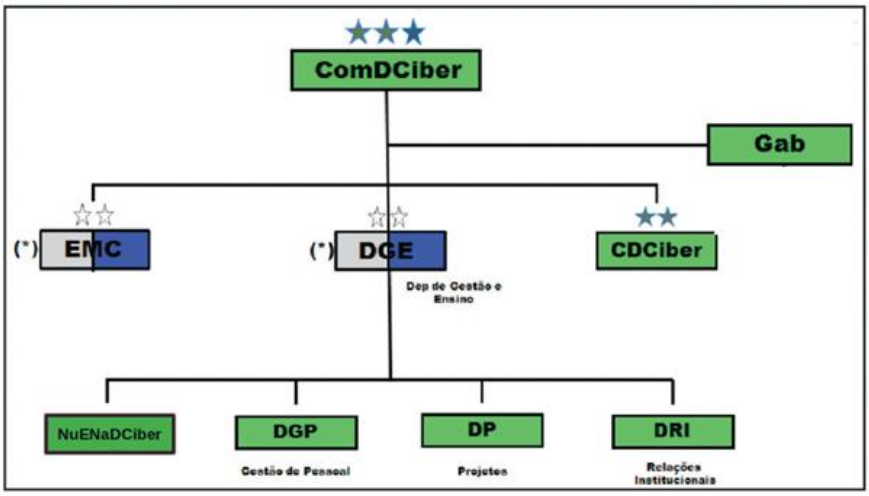


Figura 9: Estrutura do ComDCiber
Fonte: Carneiro (2017)

A criação do ComDCiber ocorreu no âmbito do Programa da Defesa Cibernética na Defesa Nacional, do MD, que tem o objetivo de potencializar o setor cibernético no país e do Programa Estratégico Defesa Cibernética do Exército Brasileiro.

É importante ressaltar que mesmo antes da criação de qualquer estrutura específica voltada para a Defesa Cibernética, o Exército já possuía a sua Rede Corporativa, a EBNet, de grande importância estratégica e cuja principal finalidade era, e ainda é, proporcionar as bases físicas e lógicas para o funcionamento seguro dos sistemas estratégicos do Exército Brasileiro.

A EBNet é um dos principais ativos do Exército Brasileiro a ser protegido no espaço cibernético, tendo em vista a sua importância estratégica como integradora das Regiões

Militares, Comandos Militares de Área e demais unidades militares espalhadas pelo imenso território brasileiro, permitindo que tenham acesso aos diversos sistemas de que a Força necessita para as suas atividades de apoio e execução do seu preparo e emprego.

A EBNet é operada e mantida pela estrutura integrante do Sistema de Telemática do Exército (SisTEx). Fazem parte do SisTEx o Centro Integrado de Telemática do Exército (CITEx), os Centros de Telemática de Área (CTA) e os Centros de Telemática (CT). O CITEx integra o Departamento de Ciência e Tecnologia (DCT) e possui ao todo 12 (doze) CTAs e CTs como Organizações Militares diretamente subordinadas.

O CITEx tem por finalidade estabelecer, manter e operar os sistemas de informática e comunicações de interesse do Sistema de Comando e Controle do Exército (SC²Ex) no seu nível mais elevado. Para atingir essa finalidade, o CITEx precisa proporcionar as bases físicas e lógicas para o funcionamento dos sistemas de interesse do Sistema Estratégico de Comando e Controle do Exército (SEC²Ex), sua integração ao Sistema de Comando e Controle da Força Terrestre (SC²FTer), e ao Sistema Militar de Comando e Controle.

Figura 10: CITEx e OMs subordinadas
Fonte: CITEx (2018)

Além da própria operação, manutenção e gerenciamento da EBNet, destacam-se ainda como serviços prestados pelo SISTEx as Redes Rádios Fixas e a Rede Integrada de Telefonia do Exército (RITEx). A RITEx é uma rede VoIP em seu backbone, que permite as ligações de longa distância entre as diversas Organizações Militares através da EBNet, sem custo adicional e utilizando um plano de numeração específico. Já a Rede Rádio Fixa é uma rede de segurança que permite a sua utilização em casos de necessidade, como um

comprometimento das demais redes (EBNet e RITEx), sendo capaz de operar com grande capilaridade no território nacional.

Destaca-se nesta Seção a pré-existência, em relação à qualquer órgão de Defesa Cibernética, de uma estrutura robusta de TI, com serviços estratégicos para o Exército Brasileiro, para salientar a extrema necessidade de proteção dessa estrutura em relação ao Espaço Cibernético e o quão oportuna foi a criação do ComDCiber, voltado não apenas à proteção dos ativos militares ligados ao Espaço Cibernético, mas também à proteção das infraestruturas críticas da sociedade civil brasileira ligada àquele Espaço.

Além disso, a pré-existência dessa estrutura já consolidada de Tecnologia da Informação, demonstra que o Exército já possuía um trabalho importante voltado para a proteção de suas redes e sistemas corporativos. Muito desse trabalho certamente tem servido e ainda servirá de suporte e apoio para o ComDCiber, especialmente nos seus primeiros anos. Isso fica evidente na Tabela 2, que elenca os principais projetos ligados ao setor cibernético a partir do ano de 2012, com a criação do CDCiber.

Certamente, até pelo hiato tecnológico e em termos de desenvolvimento existente entre o Brasil e os principais países que tem agido com maior liberdade de ação no Espaço Cibernético, a destacar-se EUA, Rússia e China, as dificuldades a serem enfrentadas pelo projeto cibernético brasileiro são consideráveis. Para mitigar os óbices e aumentar as chances de sucesso, as Forças Armadas, sob a liderança do Exército, tem buscado um planejamento estratégico eficiente que leve a uma racionalização dos custos e efetividade nas ações, principalmente nas ações estratégicas.

Projeto	Responsabilidade
Estrutura de capacitação e de preparo e emprego operacional	CCOMGEx
Estrutura de Apoio Tecnológico e desenvolvimento de sistemas	CDS
Planejamento e execução da Segurança Cibernética	CITEx
Rádio Definido por Software	CTEx
Estrutura de pesquisa científica na área cibernética	DCT, por intermédio de seu Grupo Finalístico da Segurança da Informação, com apoio do IME
Gestão de Pessoal	Centro de Defesa Cibernética
Arcabouço Documental	
Estrutura para produção do conhecimento oriundo da fonte cibernética	
Implantação do Centro de Defesa Cibernética	
Rede Nacional de Segurança da Informação e Criptografia	

Tabela 2 – Principais Projetos do Setor Cibernético a partir de 2012
Fonte: Carneiro (2012)

Este Planejamento tem como eixos principais:

- Segurança Cibernética
- Capacitação, preparo e emprego operacional
- Gestão de Pessoal
- Inteligência Cibernética
- Arcabouço Documental
- Pesquisa Cibernética
- Integração com outros desenvolvimentos estratégicos (RDS, SISFRON, etc...)

5.2 A Guerra Cibernética no Brasil: o componente civil

Um dos objetivos desta pesquisa é mostrar a importância do trabalho conjunto, da sociedade civil com as estruturas militares no que se refere ao tema Guerra Cibernética. Sendo assim, é de suma importância que se conheça inicialmente as estruturas ligadas ao assunto na sociedade civil, de forma semelhante ao que foi feito com as estruturas militares na seção anterior.

Entre os principais órgãos da sociedade civil que possuem ligações de forma direta ou indireta com as questões cibernéticas, em maior ou menor grau, é possível destacar: Conselho de Defesa Nacional, Casa Civil, Câmara de Relações exteriores e Defesa Nacional (CREDEN), GSI, Departamento de Segurança da Informação e Comunicação (DSIC), Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Centro de Tratamento de Incidentes de Segurança em Redes de Computadores (CTIR Gov), ABIN, Polícia Federal e a Agência Nacional de Telecomunicações (ANATEL) (Carneiro, 2012, p. 56).

- Conselho de Defesa Nacional: órgão de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado Democrático. Sua relação com a questão cibernética se dá pela sua importância e psocionamento nos níveis político/estratégico.
- CREDEN: tem por finalidade formular políticas, estabelecer diretrizes, aprovar e acompanhar programas e ações relacionadas à: cooperação internacional

em assuntos de segurança e defesa. Possui um Grupo Técnico de Segurança Cibernética.

- Casa Civil: a estrutura da Casa Civil conta com três órgãos importantes na elaboração das normas e regulamentos da segurança da informação e comunicações e segurança cibernética: o Instituto Nacional da Tecnologia da Informação (ITI), a Diretoria de Tecnologia da Informação (DIRTI) e a Diretoria de Telecomunicações (DITEL).
- GSI: coordena com os órgãos da Administração Pública Federal atividades relativas à Segurança das Infraestruturas Críticas nacionais, o que o torna de importância central para a Defesa Cibernética no Brasil.
- DSIC: entre outras responsabilidades, possui a incumbência de planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal.
- CTIR Gov: é responsável pela notificação de incidentes, análise, suporte e coordenação à resposta a incidentes, a distribuição de alertas, recomendações e estatísticas, assim como a cooperação com outras equipes de tratamento de incidentes.
- CERT.br: é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet, sendo responsável por receber, analisar e responder a incidentes de segurança envolvendo redes conectadas à Internet no Brasil.
- ABIN: como o seu objetivo estratégico é desenvolver atividades de inteligência voltadas para a defesa do Estado Democrático de Direito, da sociedade, da eficácia do poder público e da soberania nacional, é também órgão de suma importância nas questões cibernéticas.
- Polícia Federal: possui entre as suas atribuições a responsabilidade de apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei; e exercer, com exclusividade, as funções de Polícia Judiciária da União. Possui um Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos.

- Agência Nacional de Telecomunicações (ANATEL): além de suas funções relativas à regulação dos serviços de telecomunicações no país, a ANATEL estabeleceu políticas relacionadas a defesa cibernética para a proteção das infraestruturas críticas do país.

Assim como nas Forças Armadas, o país vem desenvolvendo uma infraestrutura de Tecnologia da Informação ao longo dos anos, mesmo antes da existência de qualquer órgão ou mesmo ação efetiva voltada à Defesa Cibernética. Sendo assim, as preocupações iniciais relativas ao tema foram tratadas no ambiente da Segurança da Informação. E com a finalidade de tratar dos assuntos relativos à Segurança da Informação foi criado no ano de 2006, pelo Decreto nº 5772 o DSIC (Carneiro, 2012, p.52).

Percebe-se, da observação da Figura 12, que o DSIC foi criado dentro da estrutura do GSI, até pela importância estratégica na proteção de infraestruturas críticas atribuída a este órgão.

Outra questão importante a ser salientada é que, pela estrutura pré-existente já tratar as questões de segurança e incidentes de redes de computadores como Segurança da Informação, com o surgimento do tema Segurança Cibernética/Defesa Cibernética, convencionou-se manter a separação existente. Sendo assim, cabe ao GSI e outras estruturas da sociedade civil a gestão e execução das atividades de Segurança da Informação, e ao Ministério da Defesa a gestão e execução das atividades de Defesa Cibernética (Alves, p. 6, 2014).

Observa-se ainda da Figura 13 o posicionamento do CDN, do CREDEN e da ABIN como partícipes da estrutura pertencente ao GSI, o que facilita os contatos e discussões desses órgãos em torno do tema Cibernético.

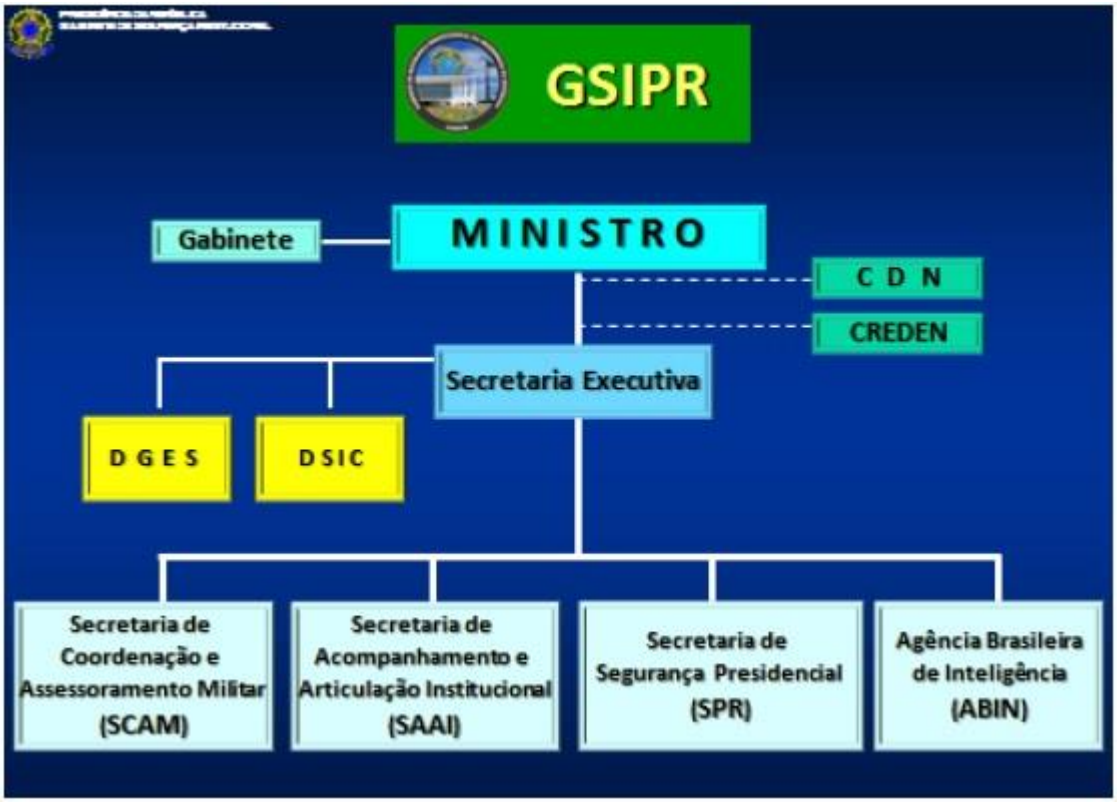


Figura 11: Organograma do GSI
Fonte: Alves (2014)

Além dos órgãos e estruturas voltadas à Segurança da Informação, existem no Brasil um conjunto de leis e normas federais que tratam do tema. A Constituição Federal, no seu artigo 5º, inciso XII, estabelece que

> XII - é inviolável o sigilo da correspondência e das **comunicações** telegráficas, **de dados** e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Além da própria constituição, o Código Civil, o Código Penal e o Código de Defesa do Consumidor possuem artigos que são utilizados, de forma mais direta ou indireta, na prevenção e tratamento das questões que envolvem a Segurança da Informação no âmbito legal.

A necessidade de criação dessa estrutura de Segurança da Informação se justificou ao longo dos anos pela própria evolução da utilização da Internet e do consequente aumento do número de incidentes de segurança reportados no âmbito da sociedade civil, que poderá ser observada de forma mais detalhada na próxima seção.

5.3 Segurança da Informação e Defesa Cibernética: a necessidade de atuação conjunta

As Forças Armadas Brasileiras tem passado por grandes transformações nos últimos anos, em um processo evolutivo que tem aumentado as suas capacidades de atuação e sua efetividade. A necessidade de atuação conjunta, inicialmente entre as Forças singulares, já era prevista doutrinariamente e os exemplos práticos legados pela História justificavam a sua busca incessante.

Com a realização dos grandes eventos no Brasil, principalmente a Copa do Mundo de 2014 e a Olimpíada de 2016 e os eventos menores a elas atrelados, ficou comprovada na prática a necessidade de integração também com as outras instituições ligadas à Segurança Pública, como a Polícia Federal, ABIN, Polícias Militares Estaduais, entre outros órgãos.

Surgem a partir daí novas doutrinas de operações Interagências, englobando as Forças Armadas e demais órgãos de segurança Federais, Estaduais e até mesmo Municipais, que certamente vão facilitar as atuações em diversos setores ligados à Segurança Nacional nos próximos anos.

Um dos setores que certamente necessita dessa atuação conjunta e que pode se beneficiar do conhecimento legado pelas Operações Interagências já realizadas é o Setor de Defesa Cibernética.

Na seção anterior, foi estabelecida uma distinção entre a Defesa Cibernética e a Segurança da Informação, do ponto de vista da atuação formal das Forças Armadas mais voltada à Defesa Cibernética, enquanto a responsabilidade relativa à Segurança da Informação é atribuída aos órgãos e autoridades civis.

A distinção mais clara entre os conceitos de Segurança da Informação e Defesa Cibernética, pode ser vista na Figura 14. Nela, é possível observar que o conceito de Segurança da Informação é mais amplo, e até por isso já praticado antes do surgimento da Defesa Cibernética. Da mesma forma é conclusão óbvia que as próprias Forças Armadas praticavam e ainda praticam os conceitos atinentes à Segurança da Informação em suas redes, buscando proteger os seus ativos e informações de qualquer tipo de violação externa, independente de suas operações cibernéticas.

A observação da figura permite também observar o caráter majoritariamente militar atribuído ao ramo da Defesa Cibernética.

Na prática porém, essa distinção é muito tênue, porque como foi possível observar nas ações classificadas como emprego de ataques de Guerra Cibernética, citadas no Capítulo 4 deste trabalho, muitas dessas ações se originam a partir de técnicas ou ferramentas que também podem atentar apenas contra a Segurança da Informação, resumindo-se a questões policiais e não a questões de ameaça à soberania de um país.

A utilização de Botnets, para a realização de ataques maciços de Guerra Cibernética, conforme ocorrido na Geórgia, por exemplo, é uma excelente demonstração disso. As Botnets, compostas de milhares de computadores, são formadas pela infecção de cada um deles de forma individual. Essa infecção se inicia na maioria das vezes por processos simples utilizados também em ações que poderiam ser utilizadas apenas para crimes comuns, como acontece na maioria das vezes por todo o mundo. Porém, essas infecções individuais, somadas e controladas por determinados grupos, tem potencial para ações maiores, estratégicas, que ameaçam a soberania dos países atacados.

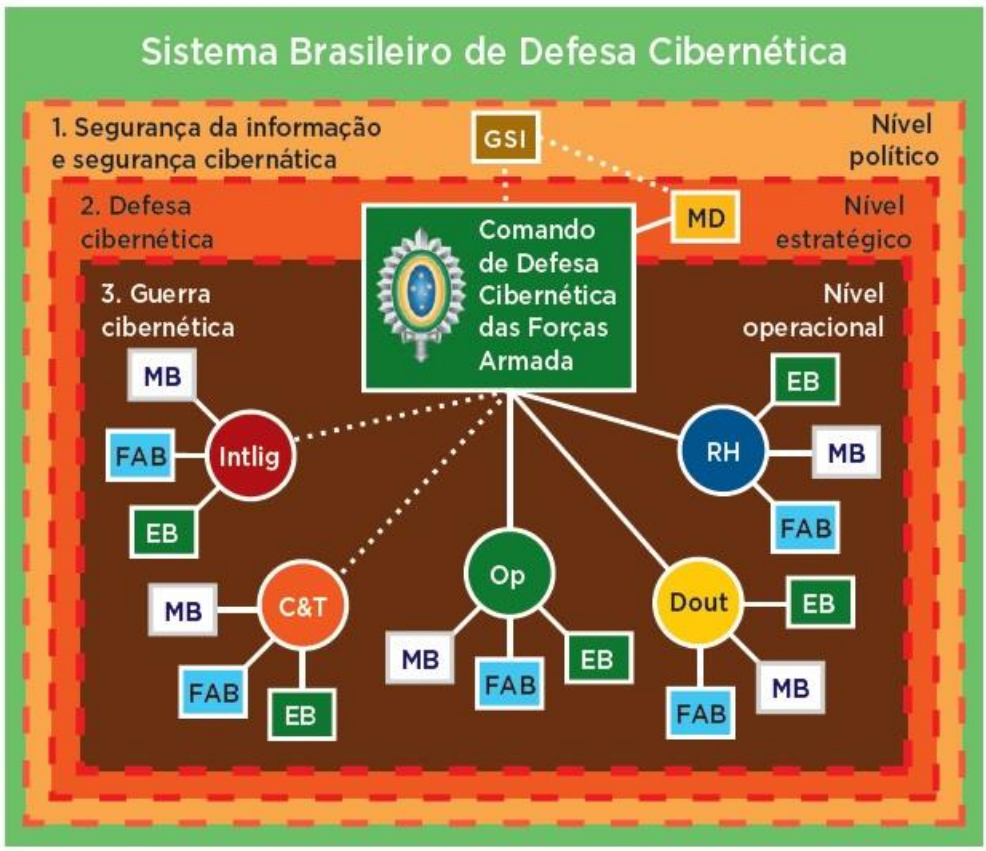


Figura 12: Sistema Brasileiro de Defesa Cibernética
Fonte: Brasil, Presidência da República (2011)

Essa gradação, partindo de ataques isolados mas que podem chegar ao nível de

ameçar a soberania de um país pode ser traduzida pelos níveis de ameaça cirbenética estabelecidos por Paul Cornish (Cornish, 2010). Em seu trabalho para o Comitê de Assuntos Exteriores do Parlamento Europeu, estabeleceu a existência de 4 níveis de ameaças cibernéticas:

- Nível 1 - Crime de baixo nível/individual (hacking)
- Nível 2 - Criminalidade cibernética organizada
- Nível 3 - Extremismo cibernético ideológico e político
- Nível 4 - Agressão Cibernética patrocinada por Estados

A seguir, serão apresentadas algumas estatísticas de incidentes relacionados à Segurança da Informação no Brasil, com o intuito de embasar a necessidade de atuação conjunta dos meios civis e militares para a atuação do Brasil no Espaço Cibernético com a liberdade de ação, protagonismo e segurança desejados.

A Figura 15 mostra a evolução dos incidentes de Segurança da Informação reportados ao CERT.br ao longo dos anos, a partir de 1999.

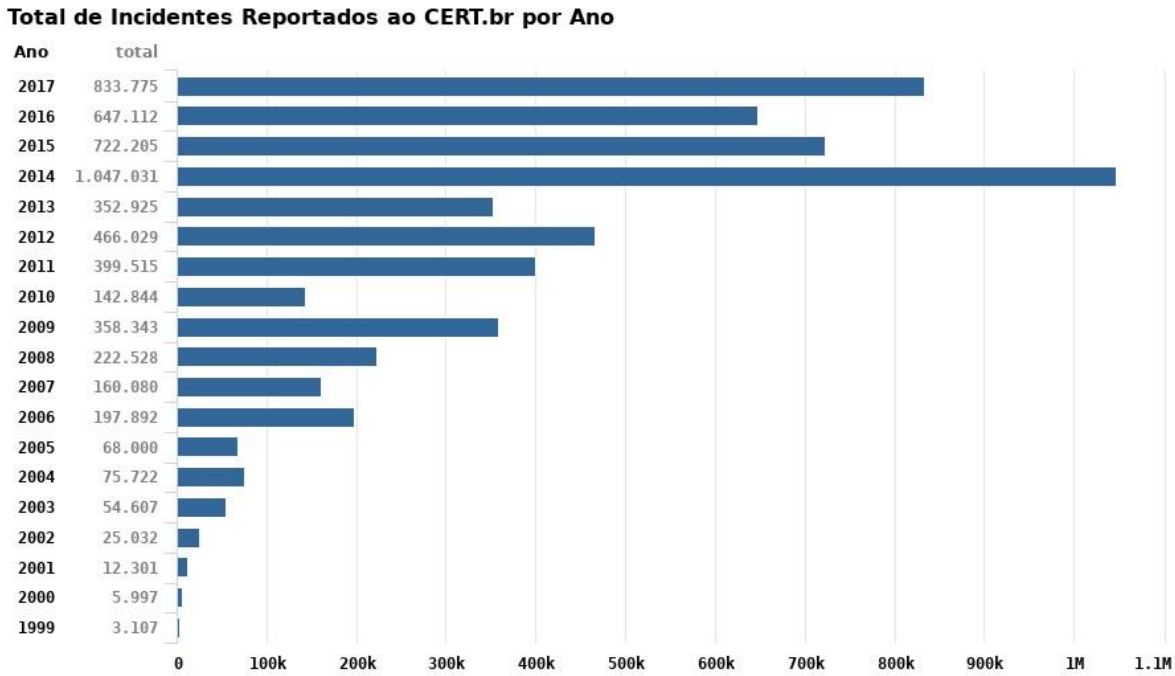


Figura 13: Evolução dos Incidentes de Segurança reportados ao CERT.br
Fonte: CERT.br (2018)

Observando-se os dados da figura, percebe-se claramente a tendência de aumento dos incidentes ao longo dos anos, com picos em momentos importantes como no ano de 2014, em que foi realizada no Brasil a Copa do Mundo de futebol profissional organizada

pela FIFA.

A Figura 16 mostra os incidentes reportados ao CERT.br por tipos de ataques, permitindo uma análise das principais táticas utilizadas contra os usuários e a população brasileira, apenas para o ano de 2017.

Observando-se os dados, percebe-se que o principal tipo de ação é o “scan”, varredura que permite verificar quais são os computadores de uma determinada rede e quais os serviços nela disponíveis, com uma incidência de 53,16%. Em segundo lugar aparecem os ataques de negação de serviço (DoS), já explicados em capítulos anteriores, com 26,41%. Esses dados são significativos e bastante lógicos, porque é realmente natural que os atacantes primeiro verifiquem a rede através de ferramentas de “scan” para apenas em seguida realizarem ataques específicos, como o DoS ou os ataques “Web”, que aparecem em terceiro lugar nas estatísticas apresentadas, com 7,29%, sendo ações específicas contra servidores de páginas “web”, ou seja, páginas de internet.

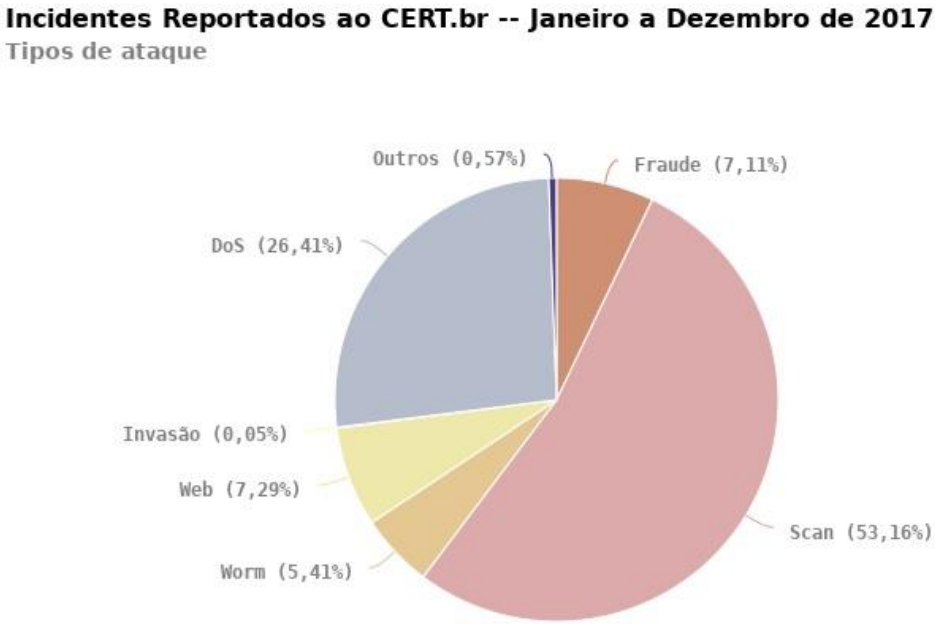


Figura 14: Tipos de incidentes
Fonte: CERT.br (2018)

Ainda analisando as estatísticas mostradas na Figura 16, percebe-se que as fraudes aparecem apenas em quarto lugar nas ocorrências, com 7,11%, seguidas pela proliferação de Worms com 5,41%.

A Figura 17, também focada no ano de 2017, permite uma análise dos ataques de acordo com os países de origem. Percebe-se que pouco menos de 50% dos ataques totais realizados são provenientes de outros países, sendo que destes, destacam-se o Vietnã

(10,63%), EUA (7,83%) e China (5,93%).

Continuando com a análise dos resultados referentes aos ataques ocorridos no ano de 2017, um relatório da “Norton Cyber Security” apresenta a cifra de US$ 22 bilhões em prejuízos causados ao Brasil com ataques cibernéticos apenas naquele ano (Defesanet, 2018a).

Para que se prossiga na análise dos ataques às redes brasileiras, mas utilizando uma quantidade maior de amostras, a tabela 3 sintetiza os dados de tipos de ataques por ano, em termos percentuais, obtida entre os anos de 2008 a 2016.

Observando-se a evolução dos tipos de ataques perpetrados no Brasil, nos últimos anos, percebe-se um aumento significativo e preocupante no número de “scans” realizados nas redes brasileiras. O grande problema nesse aumento é que o “scan” pode sugerir ações mais elaboradas, a medida em que se está “investigando” mais as redes, em busca de descobrir os serviços oferecidos e as potenciais vulnerabilidades. Associado ao aumento no número de “Scans”, verifica-se também um aumento considerável no número de ataques DoS e aos servidores Web que podem ser indicativos de vulnerabilidades do país que podem ser exploradas no futuro, em caso de conflitos com outros países.

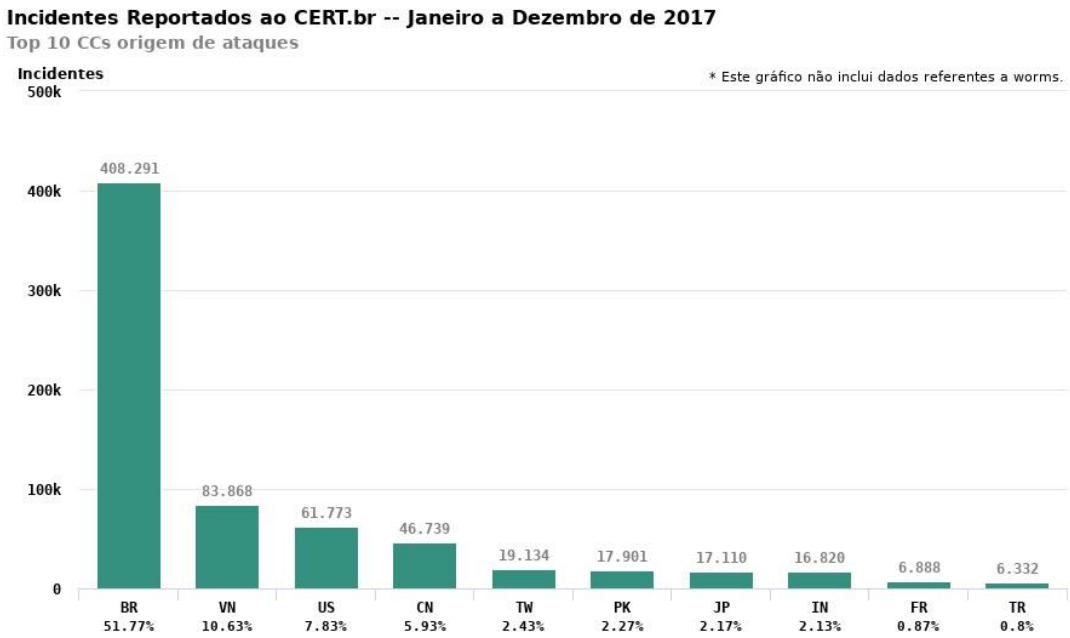


Figura 15: Origem dos ataques reportados no Brasil
Fonte: CERT.br (2018)

Essa preocupação aumenta quando se verifica que grande parte dos ataques realizados nas ações identificadas como ações de Guerra Cibernética na História, compreenderam ataques de DoS e ataques à servidores de páginas Web, que causaram grandes

estragos aos países atacados, como nos casos da Estônia, Geórgia e outros.

	2008	2009	2010	2011	2012	2013	2014	2015	2016
Scan	19,69	14,54	56,54	29,98	49,89	46,86	25,18	54,17	59,33
DoS	0,04	0,25	0,14	0,07	0,07	0,29	21,39	3,51	9,34
Web	1,89	1,56	6,10	3,88	5,48	5,30	2,75	9,09	8,57
Fraude	62,94	69,87	21,71	10,11	14,93	24,28	44,66	23,37	15,87
Inva-são	0,15	0,03	0,06	0,03	1,68	3,18	0,62	0,34	0,26
Worm	14,81	12,59	12,34	6,73	8,25	7,93	4,03	6,61	4,37
Outros	0,47	1,16	3,11	49,21	19,70	12,16	1,37	2,91	2,27

Tabela 3: Tipos de crimes cibernéticos de 2008 a 2016 (percentual)
Fonte: CERT.br (2018)

Ainda da análise dos dados apresentados, é possível concluir que os níveis de ameaça existentes no Brasil situam o país entre os níveis 1 e 2 da classificação de Cornish. Não há indicações da existência das ações previstas nos níveis 3 e 4 da classificação, exceto no caso da possibilidade de utilização de “Fake News” nas eleições, especialmente nas eleições presidenciais de 2018, que serão tratadas na próxima seção.

5.4 As Fake News no Brasil

Após os acontecimentos da eleição americana de 2016, que levaram à eleição do Presidente Trump, a preocupação com a utilização de “Fake News” como ferramenta estratégica para interferir em eleições presidenciais tornou-se uma realidade.

No caso do Brasil, a utilização de “Fake News” na eleição Presidencial é uma preocupação para os principais setores da sociedade. Uma prova disso é que o Tribunal Superior Eleitoral (TSE) demonstrou em diversos momentos do ano de 2018 essa preocupação, realizando parcerias, seminários sobre o assunto e assinando termos de combate com órgãos de imprensa e empresas controladoras de mídias sociais para que se comprometam com o seu combate.

No mês de abril de 2018, o TSE prometeu lançar um portal para combater as notícias falsas, contando com a colaboração das maiores empresas que atuam na área de checagem de fatos, permitindo assim ao eleitor conferir a veracidade das notícias compartilhadas através de mídias sociais (O Globo, 2018a).

No dia 28 de junho de 2018, o Presidente do TSE, Ministro Luís Fux, asssinou dois

termos de parceria com associações de jornalismo e plataforma digítais para o combate de notícias falsas. Os signatários se comprometeram a prevenir e combater a desinformação gerada por terceiros (O Globo, 2018b).

Foi realizado ainda no mês de junho de 2018, o seminário Internacional Brasil-União Europeia sobre “Fake News”. Participaram do seminário entre outras autoridades o Ministro e Presidente do TSE Luis Fux, a Procuradora Geral da República Raquel Dodge, o Ministro Aloysio Nunes Ferreira, das Relações Exteriores além de catedráticos estrangeiros como o Sr Martim Emmer, da “Freie Universität”, de Berlim (TSE, 2018a).

Todas essas providências mostram a seriedade com que está sendo encarado o tema por parte do TSE, tendo em vista toda a controvérsia envolvendo a eleição americana de 2016.

Foi instituído ainda pelo TSE, por meio da portaria TSE nº 949/2017, o Conselho Consultivo sobre Internet e Eleições, com a participação de diversos órgãos, entre eles a ABIN e o MD. O objetivo do Conselho é a realização de pesquisas e estudos sobre as regras eleitorais e a influência da internet nas eleições, em especial o risco de “Fake News” e o uso de robôs na proliferação deste tipo de conteúdo (TSE, 2018b).

6. CONCLUSÃO

Com os surpreendentes avanços tecnológicos que a humanidade experimentou especialmente na segunda metade do século XX e início do século XXI, houve uma profunda modificação nos hábitos e costumes das sociedades em todo o mundo. Os efeitos mais marcantes dessa modificação estão relacionados principalmente a uma aceleração sem precedentes nos fluxos de informações, capitais, mercadorias e pessoas, que caracterizam o fenômeno da globalização.

Outra característica marcante desse fenômeno é a alta conectividade de pessoas, empresas e instituições, governamentais ou não, em uma organização em redes em torno do que se convencionou chamar de Espaço Cibernético (que inclui a Internet) e que acaba tornando as fronteiras nacionais porosas e reduz a capacidade dos Estados de controlarem seus próprios territórios.

Embora tragam em seu bojo enormes benefícios e facilidades, essas mudanças trazem também novas ameaças, novas formas de crimes e delitos e, em última instância, novas formas de conflitos e guerras. Nessa nova realidade, o Brasil precisa se adaptar e estar em condições de proteger não apenas o seu povo, suas riquezas materiais e recursos naturais, garantidos pelas suas Forças Armadas desde o nascimento do país, mas também as suas redes, informações e o seu Espaço Cibernético.

Este novo modelo de mundo, em que o conhecimento é uma das principais ferramentas, se não a principal, exige novas formas de organização e engajamento, principalmente em termos de participação da vertente civil da sociedade na defesa do país.

Conforme foi tratado em diversas passagens deste trabalho de pesquisa, a forma com que as sociedades se organizaram em torno das facilidades oferecidas pela parcela do Espaço Cibernético mundialmente conhecida como a Internet, fazem com que cada indivíduo que se conecta a ela diariamente esteja se expondo também em um possível e até provável campo de batalha. E o problema se torna mais crítico porque aquele indivíduo hoje em dia se conecta à Internet para executar suas atividades, triviais ou de grande importância, muitas vezes sem ter o conhecimento que a ela está conectado, e sem saber em grande parte dos riscos que corre. Especialmente em um país com as desigualdades sociais e dificuldades na área de educação como o Brasil.

Essa nova configuração social torna o trabalho das Forças Armadas mais dependente da vertente civil da sociedade não apenas nos campos político e estratégico, mas também

no tático.

Chega-se a essa conclusão com base nas ações de Guerra Cibernética já identificadas ao longo deste século, e também com base na análise dos dados referentes aos ataques identificados nas redes brasileiras e extraídos das estatísticas do CERT.br.

Conforme foi possível verificar, grande parte dos ataques registrados de Guerra Cibernética foram realizados a partir de Botnets formadas por computadores infectados de pessoas comuns, que provavelmente tiveram sua máquina comprometida realizando as suas tarefas rotineiras no Espaço virtual, mas que acabaram se transformando em meios de ataque quando os grupos que controlavam os seus computadores desencadearam as suas ações cibernéticas.

É preciso destacar inclusive que, pelo fato do Espaço Cibernético não reconhecer as fronteiras físicas, da forma tradicional que os combates sempre foram travados ao longo da história, computadores de cidadãos de países que não eram os atacantes, foram utilizados, mesmo contra a sua vontade, dificultando as medidas que poderiam mitigar os ataques realizados.

Prosseguindo nessa mesma linha, os computadores dos próprios cidadãos do país que está sendo atacado podem ser utilizados pelo país atacante, o que pode dificultar ainda mais as medidas de defesa. Este é um ponto ainda mais preocupante quando se observa a realidade brasileira, em que apenas no ano de 2017, foram registrados US$ 22 bilhões em prejuízos por ataques cibernéticos. Este é certamente um indicativo de vulnerabilidades importantes no Espaço Cibernético brasileiro.

Quando se observa os dados apresentados no Capítulo 5, extraídos das estatísticas do CERT.br, mesmo não havendo subsídios para afirmar que os ataques citados foram realizados sob a supervisão ou controle de governos estrangeiros, essa conclusão torna-se ainda mais preocupante, já que o número de ataques e prejuízos é elevado quando se considera que são produzidos sem qualquer objetivo estratégico orientado a deliberadamente prejudicar o desenvolvimento do país.

O Brasil possui atualmente uma população superior a 200 milhões de habitantes, dos quais, segundo um relatório sobre economia divulgado no final de 2017 pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento, 120 milhões de pessoas estão conectadas à Internet, uma taxa de mais de 50%. Segundo o mesmo relatório, o país é o quarto colocado em termos de pessoas conectadas, perdendo apenas para EUA (242 milhões), Índia (333 milhões) e China (705 milhões) (Revista Exame, 2017).

E esse número tende a aumentar pelas iniciativas governamentais na área de inclusão social e digital, que acabam gerando mais usuários conectados a cada dia, muitas vezes sem maiores conhecimentos na área de informática, e muito menos nas áreas de Segurança da Informação.

Quando se analisa esse número de pessoas conectadas em conjunto com os índices de educação brasileiros, percebe-se uma situação extremamente preocupante. Observando-se os resultados do país no "Programme For International Student Assessment" (PISA) de 2015, da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), mundialmente aceito, verifica-se que o Brasil obteve resultados muito ruins, estando inclusive abaixo da média mundial. O país ficou na 63ª posição em ciências e na 66ª em matemática (INEP, 2015).

Soma-se ainda ao baixo desempenho citado o alto índice de evasão de estudantes brasileiros no ensino médio, conforme registrado em relatório da própria OCDE no ano de 2017, com uma taxa de abandono de 41% dos estudantes, o que torna o quadro ainda mais sombrio (INEP, 2015).

Estes índices de desempenho educacional são relevantes para o setor cibernético porque este além de ser ainda relativamente pouco explorado na sociedade brasileira, trata de assuntos bastante técnicos e que requerem ao menos determinados conhecimentos básicos voltados à área de informática e raciocínio lógico.

O problema é o mesmo quando se analisa as infraestruturas críticas que devem ser protegidas no Espaço Cibernético. Embora essas estruturas certamente possuam equipes especializadas em questões de Segurança da Informação e se projete para um futuro próximo que possuam meios especializados de Defesa Cibernética, a atuação isolada de indivíduos sem o devido conhecimento pode afetar os níveis de proteção a serem alcançados.

Quando se analisa a questão do setor cibernético no Brasil sob o enfoque das "Fake News", a questão dos níveis educacionais permanece no centro da discussão. As falhas existentes no processo educacional brasileiro dificultam em muito a formação do pensamento crítico, essencial para a interpretação de notícias em um ambiente extremamente favorável a todos os tipos de manipulação como é o ambiente virtual.

As polêmicas em torno da eleição presidencial americana que elegeu o atual Presidente Donald Trump, assim como os fatos envolvendo a possível contratação de indivíduos com o objetivo de "gerenciamento de perfis" em redes sociais citada no Capítulo 4 deste trabalho, demonstram que o risco de utilização do ambiente virtual para ações de alcance

estratégico é real e pode ter consequências funestas tanto para o processo democrático quanto para a soberania do país.

É imperativo assim a conscientização de toda a sua sociedade, não apenas a sua vertente militar, mais acostumada à se preocupar com as questões de soberania e segurança nacional, mas também da sociedade civil. A crescente informatização da sociedade, com os consequentes níveis de elevada conectividade, tornam os cidadãos protagonistas no processo de Defesa Cibernética, já que suas ações podem ter impactos significativos em todo o processo.

Apesar das vulnerabilidades encontradas no campo psicossocial, e do atraso relativo em relação às principais potências mundiais, é possível concluir que o Brasil vem realizando ações importantes para se estabelecer como uma potência com capacidade de atuar de maneira efetiva no setor cibernético.

A inserção do tema na PND o colocou de vez na agenda nacional, permitindo o aumento dos investimentos e organização de estruturas oficiais voltadas para o seu desenvolvimento. A partir daí diversas ações importantes já foram realizadas, levando a um avanço considerável no setor cibernético.

Entre essas iniciativas, é preciso ressaltar a criação dos Programas Estratégico de Defesa Cibernética do MD e do EB, do Comando de Defesa Cibernética, além da criação na sua estrutura da Escola Nacional de Defesa Cibernética, cujo núcleo já está em funcionamento. Busca-se com esta iniciativa agir em um dos principais pontos da questão Cibernética, que é a formação de mão de obra qualificada, não apenas para as Forças Armadas, mas para o país.

Pode-se afirmar porém que as dificuldades econômicas e os problemas que o país tem enfrentado nos últimos anos constituem-se em óbices importantes para a busca do desenvolvimento do Setor Cibernético no país, especialmente em termos de políticas públicas voltadas para o seu fomento na sociedade civil.

No setor militar, embora também seja diretamente afetado pelas crises econômicas a que o país está sujeito, a existência de um Planejamento Estratégico Organizacional em diversos níveis, alinhados com os Programas Estratégicos das Forças Singulares, torna mais fácil manter a busca pelos objetivos estratégicos, mesmo nos momentos de dificuldades financeiras.

Naturalmente a sociedade civil não possui a mesma coesão na maior parte do tempo, até pelas diferenças estruturais e de formação, sendo portanto necessário que haja políticas

públicas que estimulem os setores estratégicos, priorizando-os e fazendo com que avancem mesmo nos momentos de crise.

Essa priorização é muitas vezes complexa no que se refere aos assuntos ligados à Defesa, pelas próprias características do povo brasileiro, que enfrenta muitas vezes dificuldades diárias em questões básicas de saúde, infraestrutura, serviços e segurança (interna) que dificultam o seu entendimento sobre as necessidades voltadas à Segurança Nacional.

Sendo assim, por tudo o que foi apresentado, principalmente levando-se em conta as vulnerabilidades de segurança serem inerentes à própria criação e desenvolvimento da Internet, além dos principais ataques cibernéticos já resgistrados terem sido realizados a partir de algum tipo de falha de configuração ou utilização de equipamentos ou sistemas, conclui-se que para que o país avance de maneira uniforme no setor cibernético e consiga alcançar a liberdade de ação almejada, são imprescindíveis a conscientização e engajamento da sociedade civil, em conjunto com as Forças Armadas no âmbito do Ministério da Defesa.

Apenas através da associação e trabalho conjunto das vertentes civil e militar da sociedade brasileira, será possível progredir no campo cibernético e atingir os importantes objetivos estratégicos do país neste setor, que se desenha de importância vital nas relações futuras no concerto das nações.

REFERÊNCIAS

_____. AGÊNCIA BRASIL. **Fake news e controle na internet são desafios para as eleições de 2018.** Disponível em < http://agenciabrasil.ebc.com.br/geral/noticia/2017-12/fake-news-censura-e-controle-na-internet-desafios-para-eleicoes-de-2018>. Acesso em 05 de julho de 2018.

ALENCAR, Márcio Faccin de. **Guerra Cibernética: cenário atual e perspectivas./ Márcio Faccin de Alencar.** TCC (Especialização) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, Brasil, 2010.

ALVAREZ, T. **Guerra e defesa cibernética**. Rio de Janeiro. Blog SegInfo, 2010. Disponível em: <http://www.seginfo.com.br/guerra-e-defesa-cibernetica>. Acesso em 25 de março de 2018.

ALVES, André Gustavo de Miranda Pineli. **O Renascimento de uma potência. A Rússia no século XXI. IPEA. Secretaria de Estudos Estratégicos.** Brasília 2012.

ALVES, Valéria Farias; Souza, Cristina Gomes; Chrispino, Álvaro; Ogasawara, Eduardo. **Segurança Cibernética e Políticas públicas no Brasil.** XI Simpósio de Excelência em Gestão e Tecnologia. Rio de Janeiro, 2015.

_____. BBC. **Como o termo 'fake news' virou arma nos dois lados da batalha política mundial.** Disponível em: <http://www.bbc.com/portuguese/internacional-42779796> Acesso em 30 de janeiro de 2018.

_____. BBC. **A Coreia e o enredo do filme a entrevista.** <https://www.bbc.com/portuguese/noticias/2014/12/141222enredotheinterviewcoreiars> Acesso em 28 de agosto de 2018.

_____. BBC. **As razões da crise na Ucrânia**. Disponível em <https://www.bbc.com/portuguese/noticias/2014/03/140304_crise_ucrania_razoes_russia_fn- b>. Acesso em 15 de julho de 2018.

_____. BBC. **Entenda o referendo da Crimeia.** Disponível em <https://www.bbc.com/portuguese/noticias/2014/03/140316crimeiaentendareferendoatualizacaolgb-c>. Acesso em 29 de agosto de 2018.

BERNAT JÚNIOR, Stefan Cavalcante. **O Setor Cibernético nos Estados Unidos da América: ensinamentos para o Exército Brasileiro.** Trabalho de Conclusão de Curso (Especialização) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, Brasil, 2012

CARNEIRO, João Marinonio Enke. **A Guerra Cibernética: uma proposta de elementos para a formulação doutrinária no Exército Brasileiro.** Tese de Doutorado - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, Brasil, 2012.

CARNEIRO, João Marinonio Enke. **Perspectivas para o setor cibernético no âmbito do Ministério da Defesa, com ênfase no Exército Brasileiro 22018-2030.** Artigo Científico - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, Brasil, 2017.

_____. CERT.br. **Cartilha de malware**. 2018. Disponível em <https://cartilha.cert.br/malware>. Acesso em 15 de agosto de 2018.

_____. CERT.br. **Incidentes.** Dipsonível em <www.cert.br/stats/incidentes>. Acesso em 20 de agosto de 2018.

_____. CERT.br. **Tipos de incidentes.** Disponível em <www.cert.br/stats/incidentes/2017-jan-dec/tipos-ataque.html>. Acesso em 23 de agosto de 2018.

_____. CERT.br. **Tipos de Incidentes até Jan de 2017**. Disponível em <https://www.cert.br/stats/incidentes/2017-jan-dec/>. Acesso em 26 de agosto de 2018.

_____. CERT.br. **Tipos de crimes cibernéticos de 2008 a 2016**. Disponível em <https://www.cert.br/stats/incidentes/2017-jan-dec/total.html>. Acesso em 28 de agosto de 2018.

CLARKE, Richard A., Robert K**.** Knake. **Guerra Cibernética - A Próxima Ameaça À Segurança e o Que Fazer A Respeito. Harper Collins Publishers,** Estados Unidos da América, 2010.

CORNISH, Paul. **Cyber Security and Politically, Socially And Religiously Motivated Cyber Attacks.** Directorate-General for External Policies of the Union, Feb. 2009. Disponível em:<http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf>. Acesso em 18 de setembro de 2018.

COSTA, Angelo Giusepp Amaral da**. O Exército Brasileiro e a Guerra cibernética: situação atual e Perspectivas.** Trabalho de Conclusão de Curso (Curso de Política Estratégia e Alta Administração do Exército) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, Brasil, 2010.

CRUZ JÚNIOR, Samuel César da. **A Segurança e Defesa Cibernética no Brasil e uma revisão das Estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual.** Instituto de Pesquisa Aplicada-IPEA. 2013.

DARNELL, Tony. **The Election Crimes of Donald J. Trump: Evidence of his collusion with Russia.** 1 Ed. Estados Unidos da América.

_____. El PAIS, Brasil. **Obama autoriza sanções contra a Coréia do Norte após ciberataque contra a Sony**. Disponível em <https://brasil.elpais.com/brasil/2015/01/02/internacional/1420227417_470414.html>.Acesso em 18 de setembro de 2018.

_____. EUA. Cyber Command. **Histórico da Defesa Cibernética dos EUA.** Disponível em <https://www.cybercom.mil/About/History/> Acesso em 14 de julho de 2018.

_____. EUA. Department of Defense. **Departamento de Defesa inicia processo para elevar o Cyber Comando dos EUA a um Comando Unificado.** Disponível em

<https://dod.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/. Acesso em 23 de Agosto de 2018.

_____. EUA. Department of Defense. **Organograma**. Disponível em <https://virginiaptap.org/wp-content/uploads/2018/03/DoD-Face-Chart-20180222.pdf>.Acesso em 28 de agosto de 2018.

_____. EXAME. **Brasil é o quarto país Disponível em número de usuários de Intenet**. Disponível em < https://exame.abril.com.br/tecnologia/brasil-e-o-4o-pais-em-numero-de-usuarios-de-internet/> Acesso em 22 de Agosto de 2018.

_____. EXÉRCITO. Comando de Operações Terrestres**. Manual de Campanha EB70-MC-10.232 – Guerra Cibernética.** Brasília, 2017.

Harding, Luke**. Collusion: Secret Meetings, Dirty Money, and How Russia Helped Donald Trump Win.** 1 Ed. 2017. Estados Unidos da América.

ISIKOFF, Michael, David Corn. **Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump.** 1 Ed. 2018. Estados Unidos da América.

LIBICKI, Martin C. **Cyberdeterrence and cyberwar.** RAND Corporation, 1 Ed. 2009. Estados Unidos da América.

_____. MINISTÉRIO DA DEFESA. **Manual MD31-M08 – Doutrina Militar de Defesa Cibernética.** Brasília, 2014.

_____. MINISTÉRIO DA EDUCAÇÃO. **Brasil no PISA 2015: Análises e reflexões sobre o desempenho dos estudantes**. Fundação Santillana, INEP. Brasília, 2016.

NAKAMURA, Emílio Tissato; Paulo Lício de Geus. **Segurança de Redes em Ambientes Corporativos.** São Paulo, Novatec Editora, 2007.

NELSON, Jacob L. **Fake News? Fake problem? An analysis of the fake news audience in the lead up to the 2016 Presidential Election**. Disponível em < https://www.researchgate.net/publication/318470831_Fake_News_Fake_Problem_An_Analysis_of_the_Fake_News_Audience_in_the_Lead_Up_to_the_2016_Presidential_Election>. Acesso em 18 de setembro de 2018.

_____. NEW YORK TIMES. **CIA had evidence of Russian effort to help Trump earlier than believed.** Disponível em < https://www.nytimes.com/2017/04/06/us/trump-russia-cia-john-brennan.html>. Acessado em 18 de setembro de 2018.

_____. O GLOBO. **TSE assina termo de parceria para combater fake news.** Disponível em <https://oglobo.globo.com/brasil/tse-assina-termo-de-parceria-para-combater-fake-news-22830883> Acesso em 23 de agosto de 2018.

_____. O GLOBO. **TSE decide lançar portal para combater fake news.** Disponível em <https://oglobo.globo.com/brasil/tse-decide-lancar-portal-para-combater-fake-news-22620328> Acesso em 23 de agosto de 2018.

OLIVEIRA, Ahmina Raiara Solsona. **O comprometimento Asiático com o desenvolvimento cibernético da região e a utilização Sínica do Ciberespaço como extensão de sua estratégia tradicional.** Dissertação de pós Graduação – Universidade Estadual da Paraíba. João Pessoa, 2015.

OLIVEIRA, Maxwell Ferreira de. **Metodologia científica: um manual para a realização de pesquisas em Administração**. Catalão: UFG, Brasil, 2011.

PORTELA, José Eduardo. **A Tendência Mundial para a Defesa Cibernética**. Disponível em Desafios Estratégicos para a Segurança Cibernética. Presidência da República, Secretaria de Assuntos Estratégicos. Brasília, 2011.

_____. REDE BRASIL ATUAL. **O desafio das Fake News nas eleições de 2018.** Disponível em <http://www.redebrasilatual.com.br/politica/2018/01/o-desafio-das-fake-news-nas-eleicoes-de-2018> Acesso em 04 de fevereiro de 2018.

_____. TSE. **TSE assina acordo para combate a fake news.** Disponível em < http://www.tse.jus.br/imprensa/noticias-tse/2018/Julho/eleicoes-2018-acordo-para-nao-proliferacao-de-noticias-falsas-conta-com-assinatura-de-28-partidos>. Acesso em 01 de setembro de 2018.

_____.TSE. **Seminário sobre combate a fake news.** Disponível em <http://www.tse.jus.br/hotsites/fakenews/>. Acesso em 01 de setembro de 2018.