FACULDADE ASCES

CURSO DE BACHARELADO EM RELAÇÕES INTERNACIONAIS

A SECURITIZAÇÃO DO CYBER SPACE E SEUS DESDOBRAMENTOS PARA AS RELAÇÕES INTERNACIONAIS

SALVATTORE BERTINI CAVALCANTI SIQUEIRA CAMPOS DE OLIVEIRA

CARUARU
2014

FACULDADE ASCES
CURSO DE BACHARELADO EM RELAÇÕES INTERNACIONAIS

A SECURITIZAÇÃO DO CYBER SPACE E SEUS DESDOBRAMENTOS PARA AS RELAÇÕES INTERNACIONAIS

Monografia apresentada por Salvattore Bertini Cavalcanti Siqueira Campos De Oliveira, ao curso de Relações Internacionais da Faculdade ASCES, como exigência para obtenção do grau de bacharel em Relações Internacionais, sob a orientação do Professor Mestre Fábio Nobre.

CARUARU
2014

BANCA EXAMINADORA

Aprovada em ___/___/___.

_____

Presidente: Prof.

_____

Primeiro Avaliador: Prof.

_____

Segundo Avaliador: Prof.

CARUARU
2014

AGRADECIMENTOS

Gostaria de agradecer ao meu professor, amigo, e orientador Fábio Nobre pelo apoio, à Gills Lopes (UFPE) por compartilhar comigo estudos importantes quanto ao tema, e me incentivar sobre o mesmo, e à professora e amiga Anahí Barbosa pelas conversas sobre filosofias orientais.

RESUMO

O *cyber space*, aportuguesado por ciberespaço, é o espaço cibernético, o mundo virtual, a Internet, onde bilhões de pessoas se conectam diariamente com infinitos motivos diferentes. Essa nova dimensão, é um novo palco para os diversos atores das Relações Internacionais, impactando fortemente nessa disciplina, desencadeando várias reações de seus atores. Essa pesquisa busca entender essa nova realidade, e se ela foi securitizada, à luz da Escola de Copenhague e do construtivismo, a qual o mundo cibernético entraria nos temas da agenda internacional, em que o mesmo mostra-se cada vez mais importante. Será analisada as agências criadas pelos países, e a importância dada por seus governos quanto ao tema, a qual já se presenciou vários incidentes envolvendo o espaço cibernético.

Palavras Chaves: Securitização; Ciberespaço; Cibernética.

ABSTRACT

The cyber space, is the cibernetic space, is the virtual world, the Internet, where billions of people connect daily with endless different reasons. This new dimension is a new stage for the various actors of International Relations, impacting strongly on this subject, triggering various reactions from their actors. This research seeks to understand this new reality, and if it was securitized in the light of the Copenhagen School and constructivism, which enter the cyber world on issues of international agenda, in which it shows itself increasingly important. Agencies established by countries will be analyzed, and the importance given by their governments on the subject, which has already witnessed several incidents involving cyberspace.

Key words: Securitization; Cyberspace; Cybernetics.

SUMÁRIO

CONSIDERAÇÕES INICIAIS

O budismo não faz diferença entre a "realidade" enquanto acordado e a "realidade" uma vez em que se está dormindo. A "realidade" é o conjunto de estímulos que se tem e em função dos quais os indivíduos reagem. As ações e reações são essencialmente fundamentadas segundo nossas percepções do que é "real". Portanto, na medida em que há implicações práticas e consequências reais nas percepções dos indivíduos não há diferenciação entre "realidade material" e "realidade virtual". De modo que os indivíduos vão reagir, tomar decisões com base nos estímulos/informações recebidas qualquer que seja essa "realidade" (RINPOCHE, 1995).

O budismo assemelha a própria vida como um longo sonho. De modo que toda a existência, os sofrimentos, as experiências sublimes são tão insubstanciais quantos os nossos sonhos (RINPOCHE, 1995).

Depreende-se a partir do ensinamento budista a cima, que outras formas de realidade como o espaço cibernético, em termos pragmáticos, não obedece à visão clássica de dicotomia entre o mundo real tal qual a entendemos e o mundo virtual, na medida em que tal mundo virtual traz impactos no mundo real.

Este trabalho tem como objetivo compreender quais são os desdobramentos e impactos causados nas Relações Internacionais advindos do espaço cibernético, ou seja, esse mundo irreal/virtual que erroneamente distinguimos do real.

A hipótese dessa pesquisa é a de que os países securitizaram o ciberespaço. Que seus governos tratam o ciberespaço como mais uma nova área de batalha, de influência, política, conquista e tudo que envolva as Relações Internacionais.

O problema de pesquisa desse trabalho é: Qual o papel do ciberespaço para as Relações Internacionais? Buscar-se-á responder, afinal, em que medida os Estados estão ou não securitizando o ciberespaço, e quais serão os desdobramentos causados dessa securitização para as Relações Internacionais.

O presente trabalho está estruturalmente dividido em três capítulos, além da considerações iniciais e considerações finais. No primeiro capítulo, será explicado o embasamento teórico, se destacando para a compreensão da securitização do ambiente cibernético a Escola de Copenhague e a inserção desse tema na agenda internacional através do construtivismo. Ademais será apresentado nesse mesmo capítulo o histórico da Internet e do ciberespaço, e alguns conceitos necessários para uma boa compreensão do tema. No segundo capítulo, será desenvolvida uma análise sobre as várias agências criadas pelos países

escolhidos nesse estudo, a saber: Brasil, Estados Unidos, Rússia, e Índia. E por fim, no terceiro capítulo, tratar-se-á sobre o nível de força dos principais países em capacidades cibernéticas e contendas já ocorridas envolvendo alguns países.

1 A EVOLUÇÃO DO CONTEXTO CIBERNÉTICO NAS RELAÇÕES INTERNACIONAIS

Todo o recente desenvolvimento tecnológico humano resultou em uma grande dependência direta ou indireta dos serviços baseados em sistemas informatizados. Na ocasião de qualquer um desses serviços serem interrompidos, tem como consequência enorme impacto sobre as populações afetadas. Basta imaginar a interrupção de serviços elétricos, telefônicos, bancários, como exemplos dos danos que poderiam ser sofridos por uma população, serviços todos esses informatizados, em outras palavras, conectados de alguma forma à rede mundial de computadores (MORESI, 2013).

Tudo isso mostra o quão estamos vivenciando uma nova circunstância, apresentada em um novo contexto, a realidade virtual, ou seja, o espaço cibernético. Nele existe um fluxo de informações podendo significar operações lícitas ou ilícitas. No espaço cibernético o papel de ator pode ser exercido por qualquer um, seja recebendo, interpretando, ou propagando informações, até a ameaçar o mundo virtual, por meio de sabotagens, crimes, espionagem, terrorismo, e guerra (MORESI, 2013).

No atual cenário da informatização, se apresenta como uma mais nova forma de política e disputas entre atores (principalmente os Estados), no espaço cibernético – a chamada guerra cibernética. Na história, tanques militares, força aérea, e bombas nucleares, foram vistas como inovadoras, e hoje as armas cibernéticas são almejadas pelos países, tido como prioritárias em suas políticas. Por meio de invasões, ataques, ou espionagem, o ciberespaço conecta o mundo como uma extensão das Relações Internacionais (PHILIPS, 2010).

1.1 A Segurança Internacional

Os Estudos de Segurança Internacional (ESI), cresceram a partir de debates sobre como proteger o Estado contra ameaças externas, e internas, logo depois da Segunda Guerra Mundial. Segurança era o lema, como apontado por diversos autores que distinguem ESI das disciplinas de Estudos de Guerra e da História Militar. (Wolfers, 1952; Yergin, 1978 apud BUZAN, 2011). A definição de ESI infelizmente não é tão simples como se desejaria. O rótulo de *segurança internacional* não foi adotado desde o início, gradualmente tornou-se aceito, porém não há consenso sobre a sua definição.

Os ESI tem sido estruturado a partir de 4 questões: a primeira baseia como seu referencial para estudos o Estado; a segunda, deseja incluir ameaças internas, bem como as

externas; já a terceira, trata de ampliar o escopo de segurança para além do setor militar e uso da força; e por fim, a quarta, vê a segurança como intrinsicamente ligada a uma dinâmica de ameaças, perigos e urgências (BUZAN, 2011).

Já para os pensadores da Escola de Copenhague, se tratando de securitização[1], os mesmos criticam a maioria das tentativas de encaixar determinadas questões como sendo de segurança. Pois, uma vez consideradas como urgentes ou de defesa, um ator automaticamente acaba por cercear o fluxo natural dos procedimentos políticos habituais (BUZAN et al., 1998 apud LOPES, 2013), mesmo com o aval de uma audiência relevante.

> Em Segurança Internacional, duas difundidas escolas de pensamento vêm à tona: a tradicionalista, que restringe segurança a questões meramente político-militares; e a abrangente – ou widener –, que a estende a outros setores (BUZAN et al., 1998, p. 1, 239). Assim, a fim de comparar essas duas abordagens e de explicar como as questões (*issues*) são securitizadas, Buzan et al. (1998, p.1) buscam prover uma classificação do que é e do que não é uma questão de segurança. (LOPES, 2013, p.26)

Torna-se visível que o conceito de Segurança, do ponto de vista internacional, sempre foi objeto de debate. Mesmo entre os tradicionalistas, pouco consenso foi encontrado. Tal circunstância abre espaço para a expansão do debate, no momento da ascensão de novos temas à agenda.

1.2 Novas Ameaças

Para os tradicionalistas, ao fim da Guerra-Fria, a agenda estado-cêntrica e militar das relações internacionais, não foi prejudicada de forma alguma. No entanto, alguns discordaram disso, como os *'wideners'* e *'deepeners'*[2]. Eles procuraram expandir o conceito de segurança em contra posição a agenda centrada no militar, acrescentando temas como: o crescimento dos conflitos intraestatais, o medo das sociedades ocidentais ante as migrações, a degradação do meio-ambiente, a aceleração de epidemias, como o HIV/AIDS. Demonstrando que os

1 "Segundo Buzan e Wæver (2003), a securitização funciona como um processo discursivo no qual é formado um entendimento intersubjetivo dentro de uma comunidade de que algo é uma ameaça existencial a um valor (território, soberania, princípios, vida) de um objeto de referência (Estados, grupos, indivíduos)." (NOBRE, 2013)

2 Segundo Buzan, o processo de *widening* e *deepening* diz respeito à modificações na agenda de segurança tradicional. Enquanto o chamado processo de alargamento (*widening*) concerne à ampliação na percepção das naturezas das ameaças – para além da lógica militar – o aprofundamento (*deepening*) sinalizava modificações quanto ao objeto de referência – para além do Estado. (BUZAN, 2011)

tradicionalistas encontraram profundas dificuldades para lidar com os desafios do pós Guerra-Fria (BUZAN, 2013).

Os *'wideners'* e *'deepeners'* foram importantes para mostrar definitivamente, que as Relações Internacionais, quando se trata de segurança internacional, não se resumem apenas a assuntos referentes à Defesa do Estado. Abriu-se um horizonte para novos temas. O terrorismo, o narcotráfico, o aquecimento global, o tráfico de pessoas entre países ou continentes, são temas mais conhecidos pela agenda global, e pela sociedade civil (BUZAN, 2013).

Porém, um tema presente na agenda internacional, a ganhar cada vez mais destaque, e securitização por parte de países, é a *cyber warfare*[3], traduzido como guerra cibernética. A guerra cibernética é um novíssimo palco de disputas e políticas entre os Estados e outros atores, presentes numa nova dimensão, o ciberespaço.

Ela trata de um mundo completamente novo, englobando várias maneiras de conflitos cibernéticos, defesas e ataques cibernéticos entre países presentes no ciberespaço, lugar onde qualquer um pode ser ator, ativo ou passivo, atacante ou vítima, desde países por meios de agências, ou empresas, grupos de hackers[4], indivíduos, e qualquer outro ator que simplesmente tenha um computador com acesso à internet, uma dimensão que possui esse principal diferencial, o baixíssimo custo.

1.3 A Escola de Copenhague

1.3.1 O Construtivismo das Relações Internacionais

Segundo Emanuel Adler, o construtivismo seria uma alternativa, um meio-termo no debate teórico entre racionalistas (principalmente realistas, neo-realistas e institucionalistas liberais) e partidários de epistemologias interpretativistas (pós-modernos e pós estruturalistas, teóricos críticos e teóricas feministas (NOBRE, 2013).

---

3 *Cyber warfare* é uma definição mais ampla do inglês para englobar todos os assuntos relativos à conflitos cibernéticos, como espionagem, segurança, a guerra cibernética etc. Ao passo que para a guerra cibernética propriamente dita, como entre partes adversárias, usa-se o termo *cyber war*. Em português usamos ambas definições como guerra cibernética (LOPES, 2013).

4 Originalmente, o termo hacker era usado para designar usuários habilidosos em *hardware* e *software*, com capacidades para adaptar, ou modificar, seus sistemas para fazerem coisas além do pretendido por seus criadores, algo visto como positivo, ou avanço. Porém, na linguagem comum, esse termo vem ganhando conotação negativa, para designar pessoas com essas habilidades, que invadem computadores, ou redes de forma não autorizada (CLARKE; NACKE, 2010).

O Construtivismo das Relações Internacionais interpreta os acontecimentos do sistema internacional como sendo formados pela ação e interação humana a depender de intepretações. Diferente de enxergar o mundo de forma natural, determinados por forças ou constrangimentos físicos (NOBRE, 2013).

Quanto a relação agente-estrutura, essa corrente teórica analisa que tanto os agentes quanto a estrutura se auto-influenciam, de forma que nenhum precede o outro, nem no tempo e nem na capacidade de influenciar, de maneira que podemos identificar o fator da intersubjetividade da Escola de Copenhague. É um processo contínuo e permanente (NOBRE, 2013).

De forma resumida, os construtivistas argumentam que o mundo é constituído socialmente por meio da interação intersubjetiva; que os agentes e as estruturas estão mutuamente constituída; e que os fatores ideacionais tal como normas, identidade e ideias em geral são fundamentais para a constituição e dinâmica da política mundial (MCDONALD, 2008).

Podemos ver que o construtivismo traz à tona uma nova abordagem, uma nova maneira de enxergarmos as Relações Internacionais, o qual não só existe temas na agenda internacional como a segurança e ameaças, ou Estados como atores únicos. O ciberespaço traz para as RIs, uma nova realidade, novos atores, e novas maneiras de se ver relações internacionais.

1.3.2 Securitização (O ambiente virtual foi securitizado)

Para os teóricos da Escola de Copenhague, a segurança é uma prática autorreferencial, sendo assim, algo pode se tornar questão de segurança, não sendo de fato uma ameaça existencial, mas sim por ter sido dramatizada. Quem cria essa situação é o agente securitizador, reivindicando tratar esse tema por meios extraordinários, através do *speech act*, o ato de fala, esse artifício pode ser descrito através de quando se fala constantemente sobre um assunto, se gera uma reação, se causa uma resposta, algo é feito, gerado (LOPES, 2013).

Por meio dessa definição, se cria um processo de securitização, o qual uma questão de segurança passa por um processo até se tornar-se securitizada. A primeira fase é quando a questão se encontra não politizada, não estando a mesma na pauta do Estado, nem nas esferas públicas de discussão e decisão. A segunda parte desse processo seria quando a questão vira politizada, ou seja, quando ela vira parte de política pública, pedindo decisão e alocação de recursos do governo. E por fim, ela se torna securitizada, quando a mesma é apresentada

como uma ameaça existencial, passa a exigir medidas emergenciais e podendo justificar ações fora do processo político normal do Estado (LOPES, 2013).

O processo de securitização do ciberespaço, na política de segurança americana, seguido pelos outros países, pode ser bem entendida através da linha de tempo criada por Gagnon. Ele compara o ciberespaço com as fases da vida humana, sendo então: a infância, como desenvolvimento da ARPANET; a adolescência, pela comercialização dos provedores de Internet; e ao fim a maioridade, tendo o ciberespaço se tornado um ambiente estratégico (LOPES, 2013).

A securitização é principalmente forte nos Estados Unidos, onde suas Forças Armadas veem o espaço cibernético como mais um ambiente de projeção de poder, além da terra, ar, mar, e espaço sideral (LOPES, 2013). Esse país é o único que onde suas autoridades de segurança admitem publicamente o uso de armas cibernéticas em conflitos (LOPES, 2013). Securitizar a questão da defesa cibernética, para a política americana, pode ser vista como uma desculpa para legitimar o uso da força militar tradicional. O pentágono vê qualquer constrangimento ciberespacial vindo de outro país como um ato de guerra tradicional, trocando por poucas palavras, um ataque virtual tem consequências bastante reais, algo considerado "virtual" transbordaria, facilmente, para o mundo real" (LOPES, 2013).

> Outro exemplo da tentativa de securitização do ciberespaço por parte dos EUA é visto na National Strategy to Secure Cyberspace (EUA-NSSC) (ESTADOS UNIDOS, 2003, passim), quando esta imprime mais de 40 vezes o termo "national cyberspace" e faz a explícita diferença entre os ciberespaços estadunidense e não estadunidense – "our" e "their", respectivamente (GAGNON, 2008, p. 51) –, dando poderes especiais ao U.S. Department of Homeland Security (EUA-DHS). (LOPES, 2013, p.39)

Podemos ver a securitização da cibernética em diversos países, através de criações de agências, ou encaixamento dessa área em agências já existentes. Vários países estão a se preocupar em investir recursos na sua defesa cibernética, ainda mais que várias contendas se mostram cada vez mais presentes.

1.4 A Internet

Para se ter um bom entendimento sobre o ciberespaço, e toda as coisas nela inseridas, faz-se necessário, antes de tudo uma compreensão sobre o histórico da Internet. Tendo ela seu início durante a Guerra Fria, onde procuraram-se meios mais seguros de comunicação, a espionagem naquela época era bastante comum, sendo assim, os americanos, no sentido de superar os soviéticos em ciência e tecnologia, criam, então, uma agência com o intuito de fazer pesquisas avançadas quanto a comunicação segura, a *Advanced Research Projects Agency*[5] (ARPA).

Assim, cria-se o projeto que origina a Internet sob o codinome ARPANET (GAGNON, 2008; LOPES, 2011a) "a qual obtém forte aporte da seara militar". (DUARTE, 2012a). Mesmo a ARPANET tendo sido criada nesse contexto, segundo um dos primeiros desenvolvedores desse projeto, ela não foi criada para ser um projeto militar. Kleinrock diz que tinha como objetivo, ter um projeto entre os vários computadores de pesquisas existentes (LOPES, 2013).

É da tese de doutoramento dele, no *Massachusetts Institute of Technology* (MIT), onde ele cria uma das maiores contribuições para a Internet, a conhecida troca de pacotes de dados o *packet switching*. Esse processo dividi um arquivo virtual em pequenos pedaços sistemáticos e eficientes, o então chamado pacote, endereçados a algum computador. Apenas por meio desse processo é que arquivos trafegam pela *web* (LOPES, 2013).

Na época em que a União das Repúblicas Socialistas Soviéticas começam a se dividirem, ocorrem, então, dois importantes acontecimentos para o desenvolvimento da internet: quando a ARPANET cria a *Militar Network* ou MILNET e quando e o Protocolo de Controle de Transmissão (TCP, de *Transmission Control Protocol*) é implementado. Eles são de suma importância pois os mesmos mostram que o interesse militar na área das comunicações seguras continuou. Quando foi implantado o protocolo universal para comunicação em redes de computadores, foi sucedido pela concretização do hipertexto, concebido graças ao Protocolo de Controle de Transmissão/Protocolo de Internet (TCP/IP, de *Transmission Control Protocol/Internet Protocol*). Isso finalmente fez criar um verdadeiro nascimento do espaço cibernético, o ciberespaço (LOPES, 2013).

5 Atualmente a Defense Advanced Research Projects Agency (DARPA) – Agência criada em 1958 para prevenir surpresas estratégicas que impactasse negativamente na segurança nacional dos Estados Unidos da América, e com função de desenvolver tecnologia armamentista contra os adversários americanos para manter a superioridade dos Estados Unidos (DARPA, 2014).

Entre o final da década de 1980 e início dos anos 1990, o pesquisador britânico Tim Bernes-Lee escreve sobre como poderia interconectar redes de computadores numa única rede mundial de computadores, essa ideia seria a base da Internet. Os trabalhos desse pesquisador são importantes para o desenvolvimento da Internet como a conhecemos hoje, onde juntamente com o trabalho da ARPANET dão vida à rede mundial de computadores, ou simplesmente a WWW[6] (LOPES, 2013).

> Nesse sentido cronológico, Gagnon (2008, 49-50) sugere uma linha do tempo para demarcar a influência do ciberespaço na política de segurança estadunidense – e, consequentemente, mundial –, a saber: (i) infância, com o desenvolvimento militar-acadêmico da Advanced Research Projects Agency Network (ARPANET); (ii) adolescência, marcada pela chegada comercial dos provedores de serviços de Internet ou (ISP, do inglês, Internet Service Providers), fazendo com que "o centro original de poder se dividisse em dois oceanos de novos atores, cada um com novos níveis de poder dentro da Internet" (GAGNON, 2008, p. 50, tradução nossa 45); e (iii) maioridade, quando o ciberespaço vira um ambiente estratégico. (LOPES, 2013, p.33)

1.5 Ciberespaço

As palavras iniciadas com *cyber*, aportuguesadas por ciber, derivam da palavra cibernética, do grego *kybernetiké*, que significava a arte de o timoneiro, o *kybernetes*, controlar ou governar seu navio, dando-lhe direção, a *kubernesis*. (DE MOURA, 2014)

Norbert Wiener[7] usou esse termo para designar uma nova área de conhecimento criada por ele, a cibernética, em 1948, ao estudar os fatores de controle e comunicação dos seres vivos, das máquinas e das organizações sociais. Uma de suas ideias consistia em que os seres vivos e as máquinas possuem algumas funções semelhantes, e por isso podem se enquadrar nos mesmos modelos e leis matemáticas. Desde então, o termo cibernético ganhou o sentido atual de informática, deferente do antigo sentido grego. (O GLOBO, 2011)

---

6 Significando Grande Rede Mundial, a *World Wide Web*, recebeu esse nome pelo motivo de seus desenvolvedores assimilaram a ideia da Internet como uma grande teia de aranha, uma rede gigante, que conecta vários computadores pelo mundo, abrangendo todo o globo.

7 Norbert Wiener (1894 - 1964) foi um físico-matemático americano, considerado o fundador da ciência da cibernética, por estabelecedor as bases dessa ciência, que estuda a relação entre os fatores de controle e comunicação dos seres vivos, das máquinas e das organizações sociais. Especialista em matemática e física-matemática, durante a Segunda Guerra Mundial, trabalhou em pesquisas sobre sistemas eletrônicos de defesa nas áreas de comunicação e informação, tornando-se, então, interessado em computação automática, a partir do qual criou a ciência da cibernética (UFCG, s/a, s/p).

Em 1984, aparece pela primeira vez o termo ciberespaço, publicado por William Gibson[8] (ZANINI, 2013) em sua novela Neuromancer, utilizando-o para definir uma realidade virtual que ocorre dentro dos microcomputadores e redes do mundo (DISCOVERY BRASIL, 2014). Sua ideia de ciberespaço, muitíssimo antes da popularização da Internet, condiz com a atualidade, onde bilhões de usuários o acessam num grande servidor, a Matrix, ou seja, a rede *www* que conhecemos hoje. Na novela Neuromancer, já há a presença de hackers sendo o próprio protagonista, Case, um. O autor também profetizou, ou inspirou, produtos atuais e possivelmente vindouros relativos à cibernética e ao mundo *high tech*.

Depois do livro Neuromancer, com a popularização do termo ciberespaço, o prefixo ciber, *cyber* em inglês, passou a exprimir atividades relacionadas ao espectro eletromagnético, e computacional, assim como a total interconexão de seres humanos através de computadores, e de telecomunicação, sem considerações de geografia física. Observa-se, assim, o ciberespaço nas diversas relações homem-máquina, bem como da telemática. (LOPES, 2013) William Gibson descreve assim o ciberespaço:

> Ciberespaço. Uma alucinação consensual vivenciada diariamente por bilhões de operadores autorizados, em todas as nações, por crianças que estão aprendendo conceitos matemáticos... uma representação gráfica de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz alinhadas no ar não-espaço da mente, aglomerados e constelações de dados. Como luzes da cidade se afastando. (DE ASSIS, 2010, p.6)

A definição de ciberespaço é um conceito amplo e difícil de definir. Cada autor dependendo de sua área de atuação, ou escritor, dará uma definição diferente, com suas próprias palavras. Os conceitos mais recentes podem agora desfrutar da experiência de ver um mundo bastante interligado, conectado, e dar uma definição mais exata.

> Para Farmer (2010) define o ciberespaço como um domínio global dentro do ambiente de informação que consiste na rede interdependente de tecnologia da informação, infraestrutura física e do espectro eletromagnético para armazenar, modificar e trocar de dados através de sistemas de rede. (MORESI, 2013)

8 Famoso escritor americano de ficção-científica, participante do movimento de contracultura, ficou conhecido como profeta *noir* do *cyberpunk*, dando início a este último gênero. Criou o termo *cyberespace* na sua obra mais famosa, Neuromancer, ganhando os principais prêmios de ficção-científica da época, inspirando vários filmes, animes, e mangás (UNISINOS, 2014).

A definição de Cebrowski destaca pontos importantes que hoje presenciamos, como o baixo custo de acessar o ciberespaço, e o seu anonimato. Dois fatos presentes na guerra cibernética, onde um país pode apoiar seus *hackers* de maneira informal, e caso descoberto de onde veio a invasão ou ataque a um sistema, como exemplo, o Estado não irá se responsabilizar, negando seu envolvimento. O baixo custo desse tipo de guerra também incentiva países de economias e/ou exércitos pequenos a se aventurarem nela.

> O Ciberespaço, como um ambiente global comum, compreende a sinergia de elementos e eventos que criam uma nova estratégia compartilhada por países, organizações e pessoas. Considerando esses bens comuns globais, para Cebrowski (2004) o ciberespaço tem pelo menos cinco características únicas de preocupação pelos responsáveis pela segurança estratégica: custo de acesso é extremamente baixo, basicamente, despesas com um microcomputador e com a taxa de um cibercafé; alto grau de anonimato, que impõe esforços para detectar, rastrear e identificar um usuário específico que deseja se esconder; capacidade de iniciar uma grande variedade de efeitos físicos independentes de distâncias e à velocidades quase instantâneas; um ambiente em expansão, onde cada novo computador ou telefone celular com acesso Internet pode expandir suas fronteiras; o ciberespaço não tem dimensões tradicionais de altura, profundidade e comprimento, mas ele tem métricas únicas que podem ser usadas para mapear seus limites e operações (MORESI, 2013).

O ciberespaço acaba incluindo, então, todo um mundo conectado e informatizado. Tudo pode ser tocado e afetado pelo seu poder, qualquer coisa imaginável conectado à rede, como telefones, bancos, satélites, usinas elétricas, isso dá ideia do poderio imenso das proporções que a guerra cibernética pode tomar. Pode-se através do ciberespaço espionar, fazer roubos de informações, transferências bancárias, acessar dados sigilosos, ou até se "desligar" um país. Uma nova dimensão em que qualquer um pode ser ator, utilizando o anonimato, e além disso, é somado o fato da difícil localização originária de algum ato cibernético.

1.6 Temas pertinentes à segurança

Como hoje quase tudo que envolve tecnologia está conectado ao ciberespaço, como os serviços de um país, informações de suas agências de segurança, dados de suas multinacionais, como alguns exemplos, fazem com que de forma bastante natural tornem o

ciberespaço uma nova dimensão de influência e conflitos estre os Estados. Suas habilidades agora são medidas também em capacidades ofensivas e defensivas no espaço cibernético.

A guerra cibernética é a mais nova forma de guerra na Era da Informação, um período caracterizado pela comunicação proporcionada pela internet a todos. A Internet foi reconhecida pelo governo americano como um mais novo espaço de sua infraestrutura, acrescentado o ciberespaço às outras dimensões de segurança, onde se inclui o ar, o mar, a terra, e o espaço sideral (SANDRONI, 2013).

A soberania, a segurança de um Estado, e da sua população, atualmente, depende de quão poderoso um país é em termos cibernéticos, onde se há várias maneiras de invasões, capacidades, e termos diferentes, para designar cada tipo específico de uso do ciberespaço.

1.6.1 Segurança Cibernética e Defesa Cibernética

A segurança cibernética refere-se à proteção de informações estratégicas, principalmente os ligados às infraestruturas críticas da informação, ou seja, as redes informatizadas que controlam as infraestruturas críticas nacionais. Ela abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas[9] nacionais, especialmente os órgãos da administração pública federal (DA CRUZ JÚNIOR, 2013).

Enquanto que a defesa cibernética se refere ao conjunto de ações defensivas, exploratórias, e ofensivas no contexto de um planejamento militar, realizadas no espaço cibernético. Em outras palavras, a defesa cibernética seria a salvaguarda da segurança nacional contra ameaças ciberexistenciais, condizendo ela com aspectos militares, operacional, tático, onde as Forças Aramadas aplicam de forma estratégica com a finalidade de prevenir ou contra-atacar ameaças cibernéticas (LOPES, 2013).

Tanto a segurança quanto a defesa cibernética, pertencem ao gênero segurança da informação[10], levada à cabo tanto por agentes públicos quanto por privados (LOPES, 2013).

9 Infraestruturas críticas são o conjunto de processos, sistemas, instalações, tecnologias, redes, bens e serviços necessários para garantir a saúde, a segurança ou o bem-estar da sua população, bem como a eficácia do seu governo. O rompimento dessas infraestruturas pode resultar em perda de vidas e efeitos econômicos adversos, além de prejudicar significativamente a confiança do cidadão. (LOPES, 2013, p.29)

10 A segurança da informação, se dar pela proteção dos dados presentes nos sistemas de informação e comunicação de um Estado. Neles estão presentes dados que representam a base do desenvolvimento econômico e social de um país. A segurança e a defesa cibernética são usadas para manter o sigilo dessas informações, como as de um parque industrial nacional, responsável pelas vantagens comparativas ou especializações de um país. A segurança da informação também diz respeito à proteção, contra ataques ou sabotagens, essa proteção se dar tanto em âmbito governamental, com empresarial. Os sistemas de segurança e defesa cibernética, nele presentes, de um Estado, visam a garantir, sobretudo, a soberania nacional. (DA CRUZ JÚNIOR, 2013, p.7)

Esses dois termos são complementares, ambos buscam viabilizar a integridade, a confidencialidade, a autenticidade, e a disponibilidade das informações (DA CRUZ JÚNIOR, 2013).

Todo país contém dados sigilosos que necessitam uma defesa e segurança cibernética para protege-los de ameaças, sejam dados de empresas, políticos, agências de inteligência, secretas ou não, e dados altamente sigilosos como militares ou estratégicos.

1.6.2 Ataque Cibernético

Numa guerra cibernética, o objetivo é causar danos ou impedir a capacidade de combate do inimigo, sendo o ataque cibernético a ferramenta usada para esse fim. As principais formas de ataque podem ser através de vírus, *worms*[11], entre outros tipos de programas semelhantes que têm a capacidade de derrubar sistemas, roubar informações, ou dar informações falsas (LOPES, 2013).

Os ataques e as armas cibernéticas exigem um profissional militar qualificado e diferenciado, chamado de guerreiro cibernético, ou *cyber warrior*. Ele será o profissional militar que atingirá o inimigo de uma maneira diferente que costumamos a conhecer pela História. Para o estudo das Relações Internacionais, é válido perceber a ascensão do indivíduo como ator e agente do processo político. Seguindo esta ideia Woodward fez o seguinte questionamento: "por que bombardear um país quando você pode neutralizá-lo a ponto de ele ter de capitular"? (LOPES, 2013)

As possibilidades que um ataque cibernético pode causar a um país são infinitas, podendo desligar todos os seus serviços informatizados, ficar a não utilizar bancos, metrôs, telefonia, permanecendo em um *blackout*, além do atacante permanecer no anonimato. Há também a possibilidade de danificar sua estrutura, sua rede, seus computadores, e em algumas vezes até sem o seu conhecimento. Esse tipo de ofensiva, em termos militares, seria muito mais eficiente que a guerra comum, pois abre oportunidades de se afetar um Estado por completo da noite para o dia.

11 Vírus, *worms*, cavalos de tróia, dentre outros programas de computador, são eles capazes de derrubar sistemas, roubar informações, dar informações falsas, espionar, entre outras diversas finalidades malignas. (LOPES, 2013)

1.6.3 Ciberespionagem

A espionagem se define como atividade de inteligência projetado para coletar informações acessando dados que o outro Estado, ou que qualquer outro ator, nega o seu acesso, em outras palavras, se trata de invadir e recolher esses dados sem a permissão do outro. A ciberespionagem é apenas uma versão cibernética da espionagem comum, nesse caso, o invasor entra de forma não autorizada em redes, computadores, organizações, empresas, como exemplos, com finalidade de obter dados e informações confidenciais (CLARKE; NACKE, 2010).

A espionagem cibernética é amplamente usada principalmente por agências de espionagem dos principais países, nelas trabalham os *cyber warriors.* Como atores de motivações individuais ou difusas, podemos encontrar a ação dos *hackers*. Essas agências são geralmente capazes de invadir os mais altos níveis de dificuldades, como governos, chefes-de-estado, grandes multinacionais, a criação de vírus ou programas semelhantes, com a utilidade de possível guerra cibernética.

1.6.4 Guerra Cibernética

A guerra cibernética pode ser vista como mais uma forma de conflitos entre os Estados, ou seja, uma alternativa à guerra convencional, bem mais eficiente, uma vez que faz uso da Internet como ferramenta de ação política ou militar que pode, de fato, aumentar a ocorrência de combates tradicionais. Sua eficácia se apresenta devido aos baixos riscos territoriais e de vidas humanas que são arriscadas – diretamente – nesse tipo de evento (LOPES, 2013).

As infraestruturas críticas de um Estado são os principais alvos de uma guerra cibernética, sua interrupção, sabotagem ou danos potencializam o curso de uma guerra, ou mesmo de um ataque não declarado. Tais efeitos, sobretudo em uma era contextualizada pela informação compartilhada em redes de computadores, são ampliadas em escala e velocidades peculiares (LOPES, 2013).

Algumas estratégias dessa nova modalidade de guerra se caracterizam por objetivos como o de obter informações privilegiadas e/ou desestabilizar o sistema gerenciador de informações da rede de computadores do inimigo, para degradar o poder de combate. Isso

poderia causar sua destruição física, ou quebra da sua vontade de lutar[12]. Seu uso é essencial na redução do poder de combate do inimigo. Pode-se resumir como objetivo principal de uma guerra cibernética causar danos ou impedir a capacidade de combate de um alvo. (LOPES, 2013)

Faz-se necessário observar uma característica essencial da guerra no ciberespaço, ela só poderá ser usada contra um inimigo que seja informatizado, em outras palavras, cuja estrutura esteja conectada à rede, por exemplo, um país pobre, de caráter agrário, não seria muito atingido pelos efeitos de um conflito de tal natureza. (LOPES, 20131)

Ainda não houve propriamente uma guerra[13] cibernética no sentido de confronto entre Estados, apesar de casos pontuais já terem ocorridos de ciberespionagem, de ataques cibernéticos, entre diversas outras contendas terem acontecido no ciberespaço. Porém, uma guerra cibernética de fato, ainda não ocorreu, que se indicaria por fatores como: destruição física definitiva do inimigo, ou como impossibilitar a volta ativa do inimigo numa guerra (CLARKE, s/a).

12 Tais objetivos, apesar de buscado por meios considerados inovadores, são os mesmos daqueles buscados em um conflito convencional. Segundo Carl Von Clausewitz, maior estrategista da era moderna, os propósitos da guerra são os seguintes: "As forças combatentes devem ser destruídas: isto é, devem ser colocadas numa situação tal que não possam continuar lutando. Sempre que empregamos a expressão 'destruição das forças inimigas' é somente isto que queremos dizer. (...) quebrada a *determinação* do inimigo: em outras palavras, enquanto o governo inimigo e os seus aliados não forem levados a pedir a paz, ou enquanto a população não for levada a se render" (CLAUSEWITZ, 1976, p.94).

13 A guerra se define por ser um tipo de conflito violento caracterizado por: ao menos dois oponentes com forças militares organizadas; não ser uma luta esporádica, mas determinada num certo período de tempo; e pelo fato da luta ser intensa, deixando vítimas e destruição (BAROMETER, 2002).

2 O DESENHO INSTITUCIONAL FRENTE ÀS TRANSFORMAÇÕES VIRTUAIS

Ao se observar o atual nível de informatização da sociedade, do Estado, de empresas, e indivíduos, faz-se necessário se proteger dos riscos do ciberespaço. Além dessa proteção, e dessa defesa, o alto nível de informatização do globo também é usado para ataques, ou espionagem principalmente, entre outros fins. Os dados, serviços, infraestruturas críticas de um Estado – uma vez que tudo está conectado à Internet – abre-se uma lacuna para um mundo de oportunidades de invasões através da rede.

Com a securitização do ciberespaço, vários países criaram agências para defenderem seus dados das ameaças cibernéticas, e consequentemente, a própria soberania nacional. A utilização do ciberespaço como ferramenta de guerra, e o desenvolvimento de armas cibernéticas, se mostram cada vez mais presentes, sendo assim, a necessidade de proteção, e a possível utilização de ataques cibernéticos, andam juntas.

As agências de inteligência são as encarregadas de defender o país das ameaças cibernéticas, proteger dados governamentais ou empresarias, e atacar ciberneticamente quando necessário, além de serem encarregadas para quaisquer outros interesses do Estado, como exemplo a ciberespionagem. Elas estão relacionadas diretamente com as forças armadas e governos de seus países, podendo uma ameaça cibernética facilmente transbordar para respostas militares tradicionais. São utilizadas, praticamente, como mais uma força armada de um país, ademais da aérea, marinha, e exército, sendo elas instrumento de política de governo estatal.

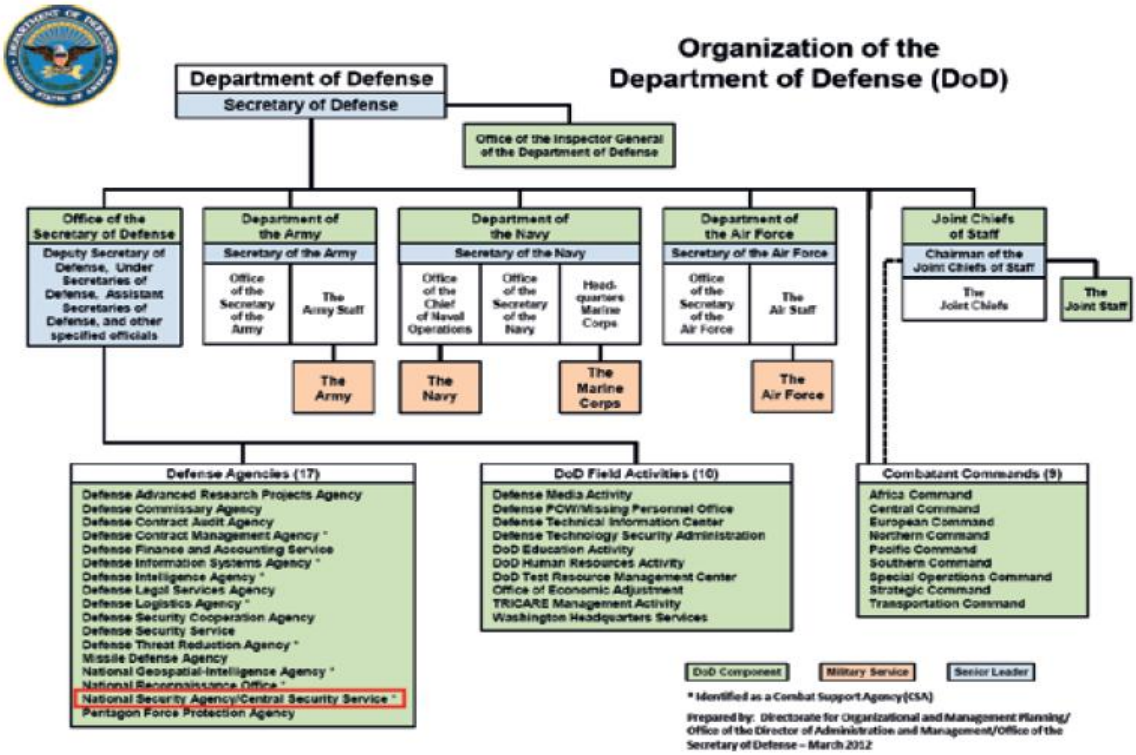
Para se fazer um caso comparativo com o Brasil, quanto à organização interna dos assuntos cibernéticos, referentes a cada país, foi escolhido os Estados Unidos, a Rússia, e a Índia. A China, como segunda maior economia do mundo, e por ser um dos principais atores no ambiente cibernético, também seria um ótimo caso a ser estudado, porém a falta de documentos oficiais chineses inviabilizou sua participação. A escolha da Rússia, então, é utilizada para ser uma contra parte aos EUA entre os países desenvolvidos, e a Índia, por se igualar com o Brasil como economias emergentes (DA CRUZ JÚNIOR, 2013).

2.1 Estados Unidos da América

2.1.1 A NSA

Os Estados Unidos da América (EUA) tem como seu principal órgão encarregado pela condução da política nacional de segurança da informação a Agência Nacional de Segurança, do inglês *National Security Agency* (NSA). Essa agência é responsável por tudo que afeta a segurança cibernética americana, pela segurança das comunicações e tecnologia da informação dos órgãos federais – ela se encontra integrada a estrutura do Departamento de Defesa americano (DA CRUZ JÚNIOR, 2013).

FIGURA 1 - ESTRUTURA ORGANIZACIONAL DO DEPARTAMENTO DE DEFESA NORTE-AMERICANO



Fonte: Da Cruz Júnior (2013)

A NSA, além de servir de apoio ao Departamento de Defesa, e a Comunidade de Inteligência Norte-Americana, apoia também às agências de governo e parceiros das indústrias relativas a produtos e serviços que dizem respeito ao ciberespaço. A NSA até financiou a própria criação da Internet em 1960 (DA CRUZ JÚNIOR, 2013).

2.1.2 A Comunidade de Inteligência Norte-Americana

O governo americano, além de possuir a Agência Nacional de Segurança, possui mais outras 15 agências e escritórios, que contribuem umas com as outras na condução das atividades de inteligência estadunidense, com intuito de preservar a segurança nacional. Atuam tanto independentemente quanto em conjunto, formando um corpo único chamado de Comunidade de Inteligência Norte-Americana. No total, há 16 agências e escritórios (vide tabela 1).

TABELA 1 – AGÊNCIAS E ESCRITÓRIOS ESTADUNIDENSES

ÓRGÃO	NATUREZA	SIGLA
Central Intelligence Agency	Agência	CIA
Air Force Intelligence, Surveillance & Reconnaissance Agency	Agência	AFISRA
Army Military Intelligence	Forças Armadas	MI
Defense Intelligence Agency	Agência	DIA
Marine Corps Intelligence Activity	Forças Armadas	MCIA
National Geospatial-Intelligence Agency	Agência	NGA
National Reconnaissance Office	Escritório	NRO
National Security Agency	Agência	NSA
Office of Naval Intelligence	Forças Armadas	ONI
DOE Office of Intelligence and Counter Intelligence	Escritório	OICI
DHS Office of Intelligence and Analysis	Escritório	I&A
Coast Guard Investigative Service	Forças Armadas (Guarda Costeira)	CGIS

Federal Bureau of Investigation	Agência	FBI
Drug Enforcement Administration	Agência	DEA
State Department Bureau of Intelligence and Research	Agência	INR
Treasury Office of Terrorism and Financial Intelligence	Escritório	TFI

Fonte: Elaboração própria, com base em Da Cruz Júnior (2013)

É notável nessa tabela, a presença das Forças Armadas, refletindo, como explicado antes, a grande importância, e principalmente a securitização, que os estadunidenses dão ao ciberespaço. Dentre os 16 integrantes que formam a Comunidade de Inteligência Norte-Americana, 4 são pertencentes às forças armadas.

2.1.3 O *U.S. Cyber Command*

Os órgãos da Comunidade de Inteligência Norte-Americana são antigos, alguns possuem décadas, isso comparadas ao recente órgão criado em junho de 2009, o *U.S. Cyber Command*, abreviado por *USCyberComm*. O mesmo é responsável pela coordenação de ações de defesa e prevenção cibernética dos Estados Unidos (DA CRUZ JÚNIOR, 2013).

Esse órgão é uma subunidade das Forças Armadas, subordinada ao Comando Estratégico americano. Foi criada para ter acesso e cooperação como as forças militares e com a Comunidade de Inteligência Norte-Americana. O próprio comandante do *USCyberComm*, é o mesmo indivíduo que exerce a função de diretor da NSA, que por sua vez, também é o chefe do Serviço Central de Segurança. Dessa maneira, um único indivíduo se torna responsável pela segurança e pela defesa nos Estados Unidos. Algo perspicaz, pois as ações de segurança e defesa se confundem, sendo necessário que as políticas de ação de ambas estejam juntas (DA CRUZ JÚNIOR, 2013).

Em 2011, os EUA lançaram seu ponto de vista quanto ao espaço cibernético, intitulado de Estratégia Internacional para o Espaço Cibernético. Entre seus vários pontos, destaca a importância do tema para o desenvolvimento da humanidade, e convida interessados, sejam países, sociedade civil, setor privado, a fim de colocar em prática a proposta governamental exibida nesse documento (DA CRUZ JÚNIOR, 2013).

2.1.4 A estratégia cibernética estadunidense

O governo norte-americano convida a todos os interessados, sendo ele qualquer ator, a se juntar e a colaborar com a visão governamental americana. Tal convite se dá em âmbito formal, em sua *Estratégia Norte-Americana para o espaço cibernético*. O documento estadunidense referente a estratégia dos EUA com a cibernética, é dividido em quatro partes: Construção de uma política para o ciberespaço; O futuro do ciberespaço; Prioridades políticas; e Seguindo em frente (DA CRUZ JÚNIOR, 2013).

A Construção de uma política para o ciberespaço, trata, da necessidade das nações se unirem para a proteção do espaço cibernético, tornando-o seguro. Os Estados Unidos buscará uma política internacional ciber espacial, para o bem da Internet (DA CRUZ JÚNIOR, 2013).

O Futuro do ciberespaço, se refere ao plano futurístico americano, junto em cooperação com a comunidade internacional. Esse plano beneficiará tanto interesses nacionais, quanto internacionais, reconhecendo que esse objetivo não pode ser conseguido sozinho (DA CRUZ JÚNIOR, 2013).

Prioridades políticas, fala que para realizar esse plano, o governo americano se organizará em torno de sete atividades, sendo eles: (i) Economia, promovendo o comércio internacional, protegendo a propriedade intelectual, livre de invasões cibernéticas; (ii) Proteção de redes dos Estados Unidos, promovendo a segurança, e a confiabilidade da rede estadunidense; (iii) Aplicação da lei, em que se trata do desenvolvimento de políticas internacionais contra o cibercrime[14]; (iv) Militar, no sentido de reforçar alianças, para enfrentar as potenciais ameaças ciber espaciais, com intuito de existir segurança coletiva internacional; (v) Governança da Internet, priorizando a transparência e a inovação da Internet, preservando a segurança e a estabilidade das redes globais; (vi) Desenvolvimento internacional, com intuito de compartilhar o conhecimento, treinamento e outros recursos necessários para os países adquirirem capacitação técnica em cibersegurança; e por fim, (vii) Liberdade na Internet, defendendo os fundamentos de liberdade e privacidade na rede (DA CRUZ JÚNIOR, 2013).

E por último, Seguindo em frente, defende que a rede mundial não deve ser privilégio de algumas nações. Sendo o espaço cibernético um lugar aberto à inovação, seguro, e confiável, em que as pessoas se sintam confortáveis para trabalhar nela (DA CRUZ JÚNIOR, 2013).

---

14 Ciber crime, são os crimes que ocorrem no ciberespaço, em que usuários roubam dados, senhas, informações, com intuito de roubar dinheiro (CLARKE, s/a).

2.2 Rússia

2.2.1 A estratégia russa para o espaço cibernético

A responsabilidade pelos assuntos cibernéticos no território russo, cabe ao Ministério de Defesa da Rússia. Em 2011, o site do Ministério de Defesa desse país, publicou um documento sobre o ponto de vista russo para com o espaço cibernético, com o título de "Visões conceituais sobre as atividades das Forças Armadas da Federação da Rússia no espaço da informação" (DA CRUZ JÚNIOR, 2013). Pode-se facilmente notar a total securitização do ciberespaço no caso russo, já que esse tema é completamente abraçado pelas Forças Armadas da Federação da Rússia.

A visão russa para com o ciberespaço, valoriza o respeito ao Estado de direito e aos princípios de legalidade. Reconhece que o espaço cibernético é um tema complexo, juntamente com esse novo paradigma e suas dimensões envolvidas. O Federação russa acredita que, apenas por meio da interação e cooperação com outro países é possível efetivar o campo dos sistemas de proteção. O documento russo supracitado não menciona a estrutura organizacional quanto a segurança e a defesa cibernética (DA CRUZ JÚNIOR, 2013).

2.2.2 Destrinchando o documento russo

O documento russo *Visões conceituais sobre as atividades das Forças Armadas da Federação da Rússia no espaço da informação*, traz seis princípios: (i) Respeito ao Estado de Direito, exigindo que as Forças Armadas da Federação Russa no ciberespaço sejam guiadas por normas e princípios da legislação russa vigente, bem como pelas normas e princípios universalmente reconhecidos, e pelo direito internacional; (ii) Prioridade e respeito pelo princípio das necessidades prioritárias das Forças Armadas da Federação Russa durante; (iii) Cumprimento do princípio de integralidade exige que as Forças Armadas da Federação da Rússia usem todas as forças eficazes disponíveis para enfrentar os desafios que se apresentem; (iv) Respeito pelo princípio da interação requer que o Ministério da Defesa russo coordene as suas ações no espaço de informações com outros órgãos federais do Poder Executivo; (v) Respeito pelo princípio da cooperação exige a coordenação de esforços com países amigos e organizações internacionais; (vi) Inovação, respeito pelo princípio da inovação requer das Forças Armadas da Federação Russa que, para a preparação e execução de tarefas, sejam

utilizadas tecnologias avançadas, ferramentas e técnicas, bem como seja agregada uma equipe de segurança da informação altamente qualificada (DA CRUZ JÚNIOR, 2013).

Em seguida, são apresentadas três regras de conduta das Forças Armadas da Federação Russa: dissuadir, prevenir e resolver conflitos armados no espaço de informações. Com relação à resolução de conflitos, a Rússia considera legítimo o uso das Forças Armadas, e outras tropas para repelir a agressão contra ela e (ou) de seus aliados (DA CRUZ JÚNIOR, 2013).

2.3 Índia

2.3.1 As agências indianas

A Índia não tem um órgão exclusivamente responsável pelos assuntos cibernéticos, o tema é tratado através de diferentes órgãos, 13 no total, onde cada um trabalha independentemente do outro, sendo o tema específico colocado ao órgão que se encaixar melhor. Através de cooperação geral, a segurança e a defesa cibernética indiana são conduzidas de forma conjunta por essas 13, a saber:

TABELA 2 – AGÊNCIAS E ESCRITÓRIOS INDIANOS

ÓRGÃO	NATUREZA	SIGLA
National Information Board	Governamental	NIB
National Crisis Management Committee	Governamental	NCMC
National Security Council Secretariat	Agência	NSCS
Ministry of Home Affairs	Governamental	MHA
Ministry of Defence	Governamental	MoD
Department of Information Technology	Governamental (sob o Ministério das Comunicações e Tecnologia da Informação)	DIT
Department of Telecommunications	Governamental (sob o Ministério das Comunicações e Tecnologia da Informação)	DoT

National Cyber Response Centre - Indian Computer Emergency Response Team	Governamental	CERT-In
National Information Infrastructure Protection Centre	Governamental	NIIPC
National Disaster Management of Authority	Governamental	NDMA
Standardisation, Testing and Quality Certifcation Directorate	Braço do Departamento de Tecnologia da Informação	STQC
Sectoral CERTs	Governamental	-

Fonte: Elaboração própria, com base em Da Cruz Júnior (2013) e India (2011)

O país enfatiza a necessidade de integração entre os setores público e privado, bem como a integração com outros Estados, assim como a visão russa, para alcançar uma segurança cibernética global.

2.3.1 A estratégia cibernética indiana

A Índia apresenta considerações fundamentais para o tema cibernética: (i) Segurança no ciberespaço, a qual a mesma não é uma questão opcional, e sim imperativa; (ii) Soluções em cibersegurança sempre devem estar à frente de tecnologias tradicionais; (iii) Inteligência em segurança cibernética, considerada uma parte da segurança do espaço cibernético, com intuito defesa, contra-ataque, adotando medidas de defesa contra invasões; (iv) Correlação de informações efetivas para monitorar ativos que necessitam ser protegidos; (v) Necessidade de uma postura adequada de segurança; (vi) Política de segurança; (vii) Utilização de recursos humanos adequadamente treinados e qualificados (DA CRUZ JÚNIOR, 2013).

2.4 Brasil

2.4.1 Segurança e a defesa cibernética brasileira

A segurança cibernética brasileira é composta pelo Departamento de Segurança da Informação e Comunicações, vinculado ao Gabinete de Segurança Institucional, da Presidência da República, e pelo Centro de Defesa Cibernética, do Exército Brasileiro, vinculado ao Ministério da Defesa (DA CRUZ JÚNIOR, 2013)

A segurança e a defesa cibernética são tratadas, quando necessário, pelo Conselho de Defesa Nacional. O mesmo é um órgão de consulta do presidente da República, para assuntos relacionados à soberania e à defesa do Estado democrático (DA CRUZ JÚNIOR, 2013).

2.4.2 Gabinete de Segurança Institucional

O Gabinete de Segurança Institucional (GSI), trata dos assuntos estratégicos que afetam à segurança da sociedade e do Estado, relativos a segurança das infraestruturas críticas nacionais, a segurança da informação e comunicação, e a segurança cibernética (DA CRUZ JÚNIOR, 2013).

O GSI é dividido estrategicamente em cinco órgãos, sendo eles: Comitê Gestor de Segurança da Informação, Secretaria de Acompanhamento e Estudos Institucionais, Agência Brasileira de Inteligência, Departamento de Segurança da Informação e Comunicações, Rede Nacional de Segurança da Informação e Criptografa (DA CRUZ JÚNIOR, 2013).

NÍVEL	**DENOMINAÇÃO**	**ÓRGÃO DE COORDENAÇÃO**
Político	Segurança da Informação e Comunicações (SIC) Segurança Cibernética	Gabinete de Segurança Institucional de Presidência da República (GSI-PR)
Estratégico	Defesa cibernética	Ministério da Defesa
Operacional & Tático	Guerra Cibernética	Forças Armadas

Enquanto que o GSI fica com assuntos mais políticos estratégicos, as operacionais e táticas ficam a cabo de outros órgão. Como pode-se ver, o Brasil tem uma clara divisão de tarefas quanto a tema cibernética em seu quadro estrutural.

2.4.3 A Estratégia Nacional de Defesa

O Ministério da Defesa, em 2008, apresentou a Estratégia Nacional de Defesa (END), tendo como objetivo elaborar um plano de defesa focado em ações estratégicas de médio e longo prazo, para modernizar a estrutura nacional de defesa. A END definiu três setores estratégicos para defesa nacional, delegando cada um a uma das Forças Armadas (DA CRUZ JÚNIOR, 2013).

FIGURA 2 – ORGANIZAÇÃO DA END

Fonte: Lopes (2013)

A Estratégia Nacional de Defesa estabelece que as capacitações cibernéticas devem incluir, prioritariamente, as tecnologias de comunicações entre todos os contingentes das Forças Armadas, para que seja assegurada sua capacidade de atuar em rede. A END indica que todas as instâncias do Estado, devem contribuir para aumentar o nível de segurança nacional, com particular preocupação para as infraestruturas críticas. Deve-se criar mecanismos que reduzam as vulnerabilidades dos sistemas relacionados à defesa nacional contra ataques cibernéticos (DA CRUZ JÚNIOR, 2013).

A END traz algumas diretrizes referentes à defesa nacional, entre elas estão: desenvolver, lastreado na capacidade de monitorar/controlar, a capacidade de responder prontamente a qualquer ameaça ou agressão, ou seja, a mobilidade estratégica; fortalecer três setores de importância estratégica, sendo o espacial, o cibernético e o nuclear; unificar as operações das três Forças Armadas nacionais, muito além dos limites impostos pelos protocolos de exercícios conjuntos; desenvolver, para atender aos requisitos de monitoramento/controle, mobilidade e presença, o repertório de práticas e de capacitações operacionais dos combatentes; otimizar o emprego dos recursos humanos das Forças Armada para melhor se adequarem a END (DA CRUZ JÚNIOR, 2013). Quanto a defesa cibernética, a Estratégia Nacional de Defesa diz:

> As capacitações cibernéticas se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas de modo a assegurar sua capacidade para atuar em rede. Contemplarão o poder de comunicação entre os contingentes das Forças Armadas e os veículos espaciais. No setor cibernético, será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. (...) O aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, que permitam seu pronto restabelecimento, a cargo da Casa Civil da Presidência da República, dos Ministérios da Defesa, das Comunicações e da Ciência e Tecnologia, e do GSI-PR (Brasil, 2008, p. 33 e p. 66). (DA CRUZ JÚNIOR, 2013, p.29)

2.4.4 A responsabilidade do Exército brasileiro

Como a responsabilidade da defesa cibernética brasileira, coube ao exército nacional, delegada a ele através da Estratégia Nacional de Defesa, o mesmo criou em 2010, o Centro de Defesa Cibernética (CDCiber). Além disso, conta também com o apoio tecnológico do Centro

de Desenvolvimento de Sistemas (CDS), nesse centro, como exemplo, os engenheiros militares podem desenvolver linhas códigos com os padrões, requisitos técnicos, e operacionais do sistema, exigidos de um determinado projeto de âmbito interno (DA CRUZ JÚNIOR, 2013).

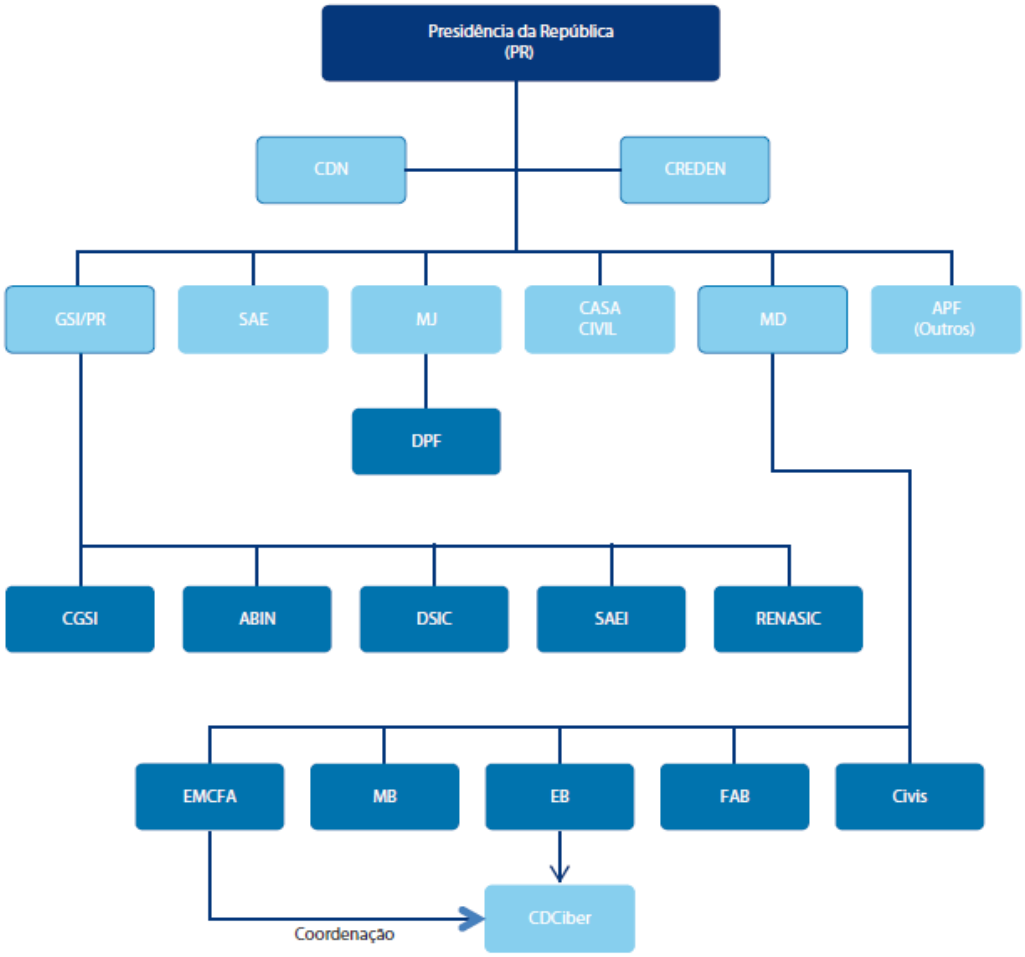
Entre alguns dos objetivos do CDCiber, se encontra a criação de um simulador de guerra cibernética, a elaboração de um antivírus nacional, o desenvolvimento de um sistema de criptografa e a capacitação de militares para situações críticas (DA CRUZ JÚNIOR, 2013).

2.4.5 Outros órgãos de apoio cibernético do Brasil

Além dos organismos governamentais supracitados, há outros atores que também contribuem para a finalidade da defesa cibernética nacional, entre eles estão: a Polícia Federal (PF), o Ministério da Justiça (MJ), o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT), o Serviço Federal de Processamento de Dados (Serpro), centros de pesquisa e universitários, além dos profissionais de tecnologia da informação e comunicação nos órgãos públicos (DA CRUZ JÚNIOR, 2013). O desenho da estrutura brasileira para o âmbito cibernético pode ser melhor observado na figura 3.

Não só o setor público atua na defesa nacional, como também o setor privado, através de organizações privadas relacionadas à segurança de rede, proteção de dados, sistemas de criptografa, antivírus como exemplos. O setor privado é considerado mais eficiente em termos operacionais e produtivos em comparação ao setor público, tendo o Exército percebido isso, se utiliza da indústria nacional para desenvolver estratégias para a segurança brasileira (DA CRUZ JÚNIOR, 2013).

FIGURA 3 - SISTEMA INSTITUCIONAL DE SEGURANÇA E DEFESA CIBERNÉTICA BRASILEIRAS



Fonte: Da Cruz Júnior (2013)

3 O CIBERESPAÇO E A SEGURANÇA EM CONTEXTO HISTÓRICO

3.1 Mensurando a força dos principais países em capacidades cibernéticas

Apesar de ainda não ter havido uma guerra cibernética de fato, o ciberespaço já está se mostrando como um ambiente estendido das Relações Internacionais, uma nova dimensão palco de espionagem, conflitos políticos, inclusão de outros atores além dos Estados, de ataques, bem como tudo que existe nas relações entre os países. O qual já se foi presenciada várias contendas pequenas, envolvendo o espaço cibernético, além de outras de maior relevância.

Por ser uma prática de custo baixo, a cibernética altera a forma das Relações Internacionais, pela inclusão de vários outros atores[15] - pois basta adquirirem computadores e serem qualificados - e por colocar países economicamente e militarmente pequenos em pé de igualdade com países mais desenvolvidos. Vários conflitos entre Estados, que militarmente, ou seja, com base nas forças tradicionais, seriam altamente desiguais, são atualmente plausíveis no ciberespaço. Ainda assim, até no ciberespaço, a desproporcionalidade se mostra visível, e ainda continua possível, em relativa igualdade, um conflito cibernético.

Em 2000, uma contenda entre *hackers* palestinos e israelenses, derrubou 40 *websites* israelenses, e 15 *websites* palestinos. Os *hackers* israelenses atacaram *websites* palestinos fazendo uso do ataque cibernético da distribuição de negação de serviço[16], em resposta os palestinos contra-atacaram os *sites* israelenses colocando neles mensagens como "Palestina Livre" e "Caxemira Livre[17]". Essa contenda foi causada pelas negociações de paz desses dois países não darem resultados satisfatórios. Os *hackers* paquistaneses, por sua vez, também invadiram *sites* americanos em sinal de repúdio (ISMAIL; YUNOS, 2005).

Além de outros conflitos como exemplos de desproporcionalidade drásticas, como a do Irã e EUA, e o entre Índia e Paquistão, o qual o mesmo em um dos seus últimos conflitos cibernéticos, envolveu 150 *hackers* paquistaneses e 10 indianos (HEICKERÖ, 2009). Há,

15 Pelo ciberespaço ser um novo ambiente comum e estratégico a todos, não só a Estados, faz com que indivíduos, empresas, *hackers*, entre outros usuários, sejam capazes de invadirem redes não autorizadas, acessando sistemas computacionais, dados sigilosos, e funcionalidades críticas de um Estado (DUTRA MORESI, s/a).

16 O ataque distribuído de negação de serviço, em inglês usado também apenas pelas siglas DDOS (distributed *denial-of-service attack*), não é considerado uma arma importante no arsenal cibernético, e sim apenas um incômodo menor. Ele é basicamente um dilúvio de acessos pré-programado, com o intuito de sobrecarregar o servidor, tornando-o inativo, atolando-o com a enorme sobrecarga (CLARKE; NACKE, 2010).

17 As mensagens de Caxemira livre são justificadas pelo apoio do grupo *hacker* paquistanês G-Force aos palestinos (ISMAIL; YUNOS, 2005).

entre outros como exemplos, os casos envolvendo China e Taiwan, Coréia do Sul e Japão, e Malásia e Indonésia (ISMAIL; YUNOS, 2005). Alguns conflitos tiveram maior impacto para o campo em questão, e serão melhor abordados adiante.

3.1.1 As capacidades cibernéticas

Os Estados Unidos, de forma geral, tem as mais sofisticadas e complexas capacidades cibernéticas, seguido logo depois pela Rússia. Em um segundo nível, estão países como a China e França, porém, mais de vinte países possuem uma relevante capacidade cibernética, tais quais o Brasil, o Irã, e a Coréia do Norte (CLARKE; NACKE, 2010; CLARKE, s/a).

Isso é possível graças aos investimentos em cibernética, como os computadores, capacitação de recursos humanos, e o desenvolvimento de programas de computador[18], serem baixos. Seu custo é relativamente baixo, barato, em comparação ao custo das forças militares tradicionais, como mísseis intercontinentais, caças, tanques, ainda mais comparadas com outras armas desenvolvidas bem mais modernas, como exoesqueletos, carros ou tanques anfíbios, equipamentos *high tech*, e derivados da robótica[19] (CLARKE, s/a).

Para se medir a força das capacidades cibernéticas de um país, se leva em conta três fatores: sua capacidade ofensiva, defensiva, e dependência. A ofensiva se refere ao fator mais conhecido, a capacidade de atacar, de invadir sistemas, bem como espionagem e outros ataques. A capacidade defensiva trata da mensuração da habilidade de um país agir sob ataque, ações que reduzam ou bloqueiem uma ofensiva. E por fim, a dependência, mostra o quão o país está conectado, dependente de redes e sistemas, refletindo suas vulnerabilidades frente a uma guerra cibernética (CLARKE; NACKE, 2010).

A tabela a seguir mostra os países mais fortes em capacidades cibernéticas, e seus devidos motivos explicados após a mesma:

---

18 Numa linguagem mais técnica, o investimento se daria no famoso tripé da informática, em que um precisa necessariamente do outro para sua existência: o *hardware*, o *peopleware*, e o *software*. O primeiro é a parte física do computador e suas peças; o segundo é o usuário, nesse caso, um bastante capacitado, *hacker*, ou *cyber warrior*; o terceiro são os diversos programas de computador, sistemas operacionais, armas cibernéticas, entre outros.

19 Em termos comparativos, os desenvolvimentos da DARPA, ou da Boston Dynamics, entre outros, como instituições militares, universidades, e empresas, produzem robôs, equipamentos de alta tecnologia, dentre vários inventos científicos que necessitam um grande aporte financeiro, investimento, e capacitação de recursos humanos (DARPA; BOSTON. s/a, s/p). Por isso, a utilização do espaço cibernético, como ferramenta de guerra, é bem mais acessível pelo seu baixo custo financeiro, tanto para países, ou qualquer outro ator das Relações Internacionais.

TABELA 3 – CAPACIDADES CIBERNÉTICAS

PAÍS	CIBER OFENSA	CIBER DEPENDÊNCIA	CIBER DEFESA	TOTAL
	8	2	1	11
	7	5	4	16
	5	4	6	15
	4	5	3	12
	2	9	7	18

Elaboração própria com base em Clarke & Nacke (2010)

As três mensurações receberam peso igual, e depois são somadas para se receber um total. O *ranking* está na ordem dos países mais ciber ofensivos. Quanto à mensuração de ciber dependência, receberam mais pontos os países que mais estão desconectados à Internet. Ser um país informatizado e conectado, geralmente significa algo positivo, porém, numa guerra cibernética, isso seria algo perigoso, já que suas estruturas críticas e serviços, estariam vulneráveis à invasões cibernéticas (CLARKE; NACKE, 2010).

A Rússia é vista como o maior competidor frente aos EUA por tecnologias cibernéticas (DA CRUZ JÚNIOR, 2013), sua capacidade ciber ofensiva já foi colocado a prova nos ataques cibernéticos a Estônia e a Geórgia.

A China, recebeu uma grande pontuação na capacidade defensiva, em parte, pela habilidade que ela possui de, simplesmente, poder “desligar” a nação inteira dos resto do ciberespaço. A Internet na China, se assemelha mais a uma intranet de uma empresa. O governo chinês é o provedor e o encarregado da defesa de rede chinesa. Em comparação, os americanos estão totalmente conectados à rede, por isso recebeu uma pontuação baixa nesse quesito (CLARKE; NACKE, 2010).

A China, também se utiliza de ciber espionagem, para conseguir acessar dados de multinacionais americanas e europeias, dando de graça esses dados para empresas chinesas.

(CLARKE, s/a) Um dos casos mais famosos dessa espionagem cibernética chinesa[20] para com os EUA, foi em que o próprio governo americano reconheceu que houve acessos não autorizados à arquivos de desenvolvimento de caças da Força Aérea dos Estados Unidos, no caso o F-35[21] e o F-22. Pouco tempo depois, os chineses lançaram caças bastante parecidos com esses dois caças estadunidenses. (DA CRUZ JÚNIOR, 2013) Como de costume no espaço cibernético, o anonimato é amplamente presente, e bastante difícil a localização geográfica originária da invasão. Fazendo-se uso desse anonimato, os Estados sempre negam sua autoria.

O Irã mostra sua capacidade ciber ofensiva em ataques a uma petrolífera da Arábia Saudita, e a diversos bancos americanos. A capacidade cibernética iraniana, é alta ao ponto de retaliar ataques cibernéticos americanos, utilizando principalmente a vulnerabilidade americana das suas infraestruturas críticas e serviços, privados ou públicos, estarem altamente conectados à rede. (CLARKE, s/a)

A Coréia do Norte, recebeu uma alta pontuação tanto para a defensiva, quanto para a ciber dependência. Os norte-coreanos podem cortar sua conexão ao ciberespaço, ainda mais fácil e eficazmente do que a própria China, além de possuírem pouquíssimas infraestruturas críticas conectadas ao espaço cibernético, sendo assim, caso houvesse até o maior ataque cibernético possível a Coréia do Norte, poderia fazer danos mínimos, ou até quase nenhum (CLARKE; NACKE, 2010).

20 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 (DA CRUZ JÚNIOR, 2013).

21 Há alguns modelos do F-35, destacando-se entre eles o F-35A. É definitivamente um caça singular, completamente incomum, com design moderno e futurístico, também chamado de Raio 2. Sua velocidade máxima de cruzeiro pode atingir *mach* 1.6, o suficiente para ir de Los Angeles até Nova York em incríveis duas horas. É um jato supersônico, ou seja que atinge a velocidade do som ou o supera, com motor diferenciado, possuindo a turbina mais potente já colocada em um caça. Seu computador de bordo é igualmente veloz, capaz de processar mais de um trilhão de operações por segundo, e é mais rápido que todos do seu tipo. Tem um sensor integrado de velocidade, que por sua vez ativa um radar eletrônico capaz de rastrear simultaneamente ameaças no ar e em terra. Nele existe um sensor eletro-ótico capaz de rastrear e atingir alvos no chão e assim como no ar, usando meios óticos ao invés de radar, ótimo para voos secretos. Possui um avançadíssimo visor nos capacetes, onde o piloto pode enxergar o céu através de duas lentes eletro-óticas, o qual projetam imagens diretamente no visor, além de também disponibilizar nessa imagem dados do voo e informações sobre o alvo inimigo, o piloto, então, será capaz de enxergar o céu até em tempo ruim, nublado, ou à noite (CAMBOU, 2009).

3.2 Casos de Conflitos

3.2.1 Canadá (5-eyes) x Brasil

Durante a Segunda Guerra Mundial, oficiais dos Estados Unidos e Reino Unido, juntaram esforços para decodificar transmissões de rádio do inimigo. Esse esforço fez criar um acordo de compartilhamento de inteligência, que até os dias atuais continua em voga, mesmo com as mudanças drásticas das comunicações, informações e dados da atualidade. Esse acordo incluiu, além dos EUA e Reino Unido, o Canadá, a Austrália, e a Nova Zelândia, conhecidos como os 5-eyes (THE GUARDIAN, 2014).

O Canadá, apoiado pela NSA e pelo 5-eyes, espionou o Brasil através do espaço cibernético, com fins de ajudar suas empresas com informações privilegiadas brasileiras, de utilidade em leilões de reservas naturais.

3.2.1.1 Os recursos naturais brasileiros como alvos da ciberespionagem

O Brasil, se destaca no cenário internacional, como grande detentor de riquezas naturais, e matrizes energéticas expressivas, se tornando um alvo preferencial para a espionagem cibernética.

Dentre essas riquezas estão: (i) Petróleo: em que a área total do pré-sal atinge 150 quilômetros quadrados, cerca de três vezes o tamanho do estado do Rio de Janeiro, e possui largura aproximada de 200 quilômetros; (ii) Gás: estimativas da Agência Internacional de Energia colocam o Brasil entre os países como as maiores reservas de gás de xisto. Esse gás desperta o interesse estadunidense por ser ele importante na sua autossuficiência energética. Além deste gás, a Agência Nacional do Petróleo afirma a existência de reservas gigantescas de gás natural; (iii) Patrimônio Genético[22] e Atividades de Bioprospeção: Importantes para o desenvolvimento de pesquisa e tecnologia estratégica de vanguarda relacionados à biodiversidade, já sendo utilizada por empresas e órgão. (iv) Nióbio: Sendo empregado na indústria nuclear, aeroespacial, bélica e nuclear, possui o Brasil a quase totalidade de seu controle, tendo as maiores reservas mundiais de nióbio, 98,43% desse mineral se encontra em

22 O Brasil possui a maior biodiversidade do mundo, estimada em cerca de 20% do número total de espécies do planeta. Esse patrimônio genético, já escasso nos países desenvolvidos, tem na atualidade valor econômico estratégico inestimável em várias atividades, mas é no campo do desenvolvimento de novos medicamentos onde reside sua maior potencialidade (...) O mercado mundial desse grupo de drogas atinge vários bilhões de dólares (DE MOURA, 2014).

território nacional; (v) Urânio: O Brasil possui uma das maiores reservas mundiais de urânio; (vi) Aquífero Guarani: um dos maiores reservatórios de água subterrânea do mundo, e que abrange 1.190.000 km², com um volume total de cerca de 37.000 km³, e uma recarga natural de 166 km³ por ano (DE MOURA, 2014)

Além dessas riquezas naturais, possui o Brasil tantas outras que o colocam como um país singular no planeta. Tais riquezas e pesquisas brasileiras, atraem interesses estrangeiros por informações armazenadas em sistemas computacionais de instituições públicas e privadas. As informações estratégicas brasileiras obtidas por meio da ciberespionagem estrangeira, colocam em risco a soberania nacional, primeiro pela intrusão com uso de arsenal cibernético superior e, segundo, pela capacidade de causar desequilíbrios econômicos com as informações coletadas (DE MOURA, 2014).

A importância dos recursos naturais brasileiros, e da preocupação estrangeira nessas reservas, é refletida, como exemplo, em um documento secreto do Departamento de Estado americano, divulgado em 2010 pelo *site* hacktivista[23] Wikileaks. No referido documento, é tratado as minas brasileiras de nióbio e manganês, as quais estariam incluídas na lista de infra-estrutura considerada estratégica aos Estados Unidos:

> "(…)Due to its relevance in aerospace and defense, Niobium is considered a "strategic metal" by the U.S. government, meaning there are few or no substitutes for the metal's essential use. Furthermore, of all strategic metals, Niobium is regarded as one of the most highly critical. (…) Almost 90% of the world supply comes from Brazil (…)"[24] (DE MOURA, 2014, p.36)

3.2.1.2 O Brasil como vítima da NSA

Os programas de espionagem cibernética da National Security Agency foram recentemente em parte divulgados por um de seus colaboradores terceirizados: Edward Snowden. O Brasil, entre outras nações, foi alvo da espionagem cibernética estrangeira (DE MOURA, 2014)

---

23 *Hacktivism* é a junção em inglês das palavras *hacker* e *ativism*, em português ativismo. Palavra usada para designar *websites* com fins políticos de disponibilizar arquivos e documentos secretos ao público de agências de inteligência, governos, entre outros. Seus colaboradores geralmente são funcionários do governo e de agências de inteligência, fazendo o *upload* de arquivos secretos com fins de esclarecer ao público sobre temas relevantes a sociedade civil, ou casos abusivos de espionagem, entre outros temas. Os mais famosos são os *sites* Wikileaks, e o Anonymous. (CLARKE, s/a)

24 Devido à sua relevância na indústria aeroespacial e de defesa, o Nióbio é considerado um "metal estratégico" pelo governo dos EUA porque existem poucos ou nenhum substituto para o uso essencial desse metal. Além disso, de todos os metais estratégicos, Nióbio é considerado altamente crítico (...) Quase 90% da oferta mundial vem do Brasil (...) (DE MOURA, 2014, p.36)

Em outubro de 2013, a mídia divulgou documentos vazados por Snowden demonstrando que as comunicações telefônicas e computacionais do Ministério de Minas e Energia do Brasil foram detalhadamente monitoradas por agência de espionagem do Canadá – parceira da NSA juntamente com Inglaterra, Austrália e Nova Zelândia (DE MOURA, 2014)

O programa Fantástico, do canal de televisão Globo, foi quem revelou que esses dois ministérios brasileiros tinham sido alvo de espionagem canadense, o invasor tinha sido a agência de inteligência canadense de cibernética, a CSEC - Comunications Security Establishment Canada - (CANALTECH, 2014).

A CESC, parceira da NSA, espionou as rede de comunicações do ministério, incluindo telefonemas, e-mails, e a Internet tendo sido totalmente mapeada (CANALTECH, 2014). A operação de espionagem foi nomeada *Man on the side*:

> (...) Não há, nos documentos, nenhuma indicação de que o conteúdo das comunicações tenha sido acessado, só quem falou com quem, quando, onde e como. Mas quem assina a apresentação secreta termina dizendo o que deve ser feito daqui pra frente: entre as ações sugeridas, uma operação conjunta com um setor da NSA americana, o Tao, que é a Tropa de Elite dos espiões cibernéticos. Objetivo: realizar uma invasão conhecida como 'Man on the side' - o homem ao lado. Com ela, toda a comunicação que entra e sai da rede pode ser copiada. É como trabalhar no computador com alguém ao lado, bisbilhotando. Daí o nome da invasão. (...) (DE MOURA, 2014, p.37)

O programa de computador utilizado foi o Olympia, fazendo ele mapeamento das comunicações telefônicas do ministério, além do uso de e-mails. Há registros de ligações para outros países, como Peru, Equador e África do Sul. O objetivo da espionagem era descobrir informações de empresas como a Petrobrás e Eletrobrás, diretamente relacionadas com o Ministério de Minas e Energia. A espionagem canadense foi capaz de identificar informações como número de celulares, registro de chips e até as marcas e modelos dos celulares. Essas informações seriam utilizadas por empresas que quisessem concorrer a leilões de operação e produção do pré-sal, por exemplo. Poderiam saber o que vai ocorrer antecipadamente, em um jogo econômico de bilhões de dólares. Também foi revelado que a NSA, que a própria presidente, e seus assessores, foram alvos dessa espionagem (CANALTECH, 2014).

Os documentos foram disponibilizados por Edward Snowden, um ex-analista da *National Security Agency*, que disponibilizou ao jornalista americano Glenn Greenwald, ações de inteligência da NSA, tendo o ultimo ajudado no levantamento de informações do caso.

Snowdem se exilou na Rússia por segurança, uma vez que quebrou protocolos de sigilo. A apresentação vazada por Snowden foi exibida em junho de 2012 em uma conferência que reunia analistas de agências de espionagem dos cinco países aliados no compartilhamento de inteligência, o 5-Eyes (CANALTECH, 2014).

3.2.1.3 A defesa canadense

A presidente Dilma Roussef[25] exigiu explicações do Canadá sobre as acusações apresentadas pela mídia. O primeiro-ministro canadense, Stephen Harper, expressou preocupação quanto ao incidente, e disse que as autoridades canadenses estão disponíveis para tratar o tema. Porém, o mesmo não poderia comentar sobre operações de segurança nacional, Stephen Harper falou:

> As autoridades canadenses estão em contato muito pró-ativo com seus homólogos ... Estou obviamente muito preocupado com essa história e algumas reportagens sobre isso, muito preocupado. Dito isto, vocês sabem que eu não posso comentar operações de segurança nacional (TERRA, 2014).

O embaixador do Canadá em Brasília, Jamal Khokhar, foi convocado pelo ministro das Relações Exteriores, Luiz Alberto Figueiredo, para prestar esclarecimentos sobre as denúncias. O porta-voz do ministro das Relações Exteriores canadense, John Baird, disse que o embaixador do Canadá no Brasil fala com o Ministério das Relações Exteriores de modo regular e constante, mas se recusou a fazer mais comentários sobre o assunto. O ministro da Defesa do Canadá, Rob Nicholson, responsável pelo CSEC, não quis tratar das acusações de espionagem (TERRA, 2014).

3.2.1.4 Desdobramentos no Brasil

Além da presidenta Dilma ter feito nota de repúdio a ciberespionagem internacional, e sobre ao caso envolvendo os ministérios brasileiros, (CANALTECH, 2014) promulgou o Decreto Nº 8.135, de 4 de novembro de 2013, que falava da segurança da informação, como a preocupação com as comunicações, e auditorias nos *hardwares* e *softwares* em equipamentos da administração pública federal (DA CRUZ JÚNIOR, 2013).

25 Presidenta da República Federativa do Brasil do período de 2010 até os dias atuais.

3.2.2 Rússia x Estônia

Mesmo com o fim da Guerra Fria, e da União das Repúblicas Socialistas Soviéticas (URSS), a Rússia continua querendo influenciar suas antigas repúblicas uma vez que eram integradas aos soviéticos. Esse país pode não ser uma potência econômica, mas político e militarmente ainda é, e a Rússia faz uso de seu aparato bélico para barganhar no cenário internacional. Entre vários exemplos que poderiam ser dados, houve um contenda política que transbordou para o espaço cibernético.

3.2.2.1 Contextualizando o caso

Em 1989, a cidade de Tallinn tornou-se, novamente, capital da Estônia, país que obteve independência quando da desintegração da União das Repúblicas Socialistas Soviéticas, em que a mesma gerou vários Estados independentes. A Estônia tinha sido obrigada a fazer parte da União Soviética quando o Exército vermelho "libertou" os Balcãs dos nazistas (CLARKE; NACKE, 2010).

A URSS não queria que os países do Leste europeu esquecessem os "sacrifícios que ela sofreu para libertar" esses países, sendo assim, ergueu na maioria dessas capitais gigantes estátuas heroicas de soldados do Exército vermelho, em Tallinn foi erguida uma dessas estátuas, no caso um gigante soldado feito a bronze (CLARKE; NACKE, 2010).

Desde a independência estoniana, há tensões entre a população étnica russa e os nativos estonianos. A maioria estoniana queriam remover qualquer lembrança das cinco décadas de opressão soviética. Em fevereiro de 2007, o legislativo desse país balcânico aprovou uma lei que removeria tudo que denotasse a ocupação da URSS, incluindo naturalmente, a tal estátua de bronze (CLARKE; NACKE, 2010).

Moscou reagiu dizendo que a remoção da estátua seria uma difamação para os soldados soviéticos mortos. Com intuito de evitar um incidente diplomático, o presidente estoniano vetou a lei, porém a pressão pública estoniana reagiu reclamando a remoção da estátua, assim como a reação do grupo étnico russo, querendo a proteção desse monumento (CLARKE; NACKE, 2010).

Em 27 de abril de 2007, que depois ficou conhecido como Noite do Bronze, ocorreu um incidente no dia da remoção dessa estátua, envolvendo manifestações nas ruas, e violência entre radicais de ambas as partes étnicas e a polícia. As autoridades, então, moveram a estátua

para um cemitério militar. Longe de acalmar os ânimos, os nacionalistas russos na Estônia contataram a mídia e o legislativo da Rússia (CLARKE; NACKE, 2010).

3.2.2.2 A contenda chega ao ciberespaço

A Estônia é um dos países mais conectados ao espaço cibernético do mundo, junto com a Coréia do Sul, bem mais informatizado do que o próprio Estados Unidos, com seu alto grau de penetração da banda larga e conexão com a Internet, onde seus cidadão o acessam bastante na vida cotidiana (CLARKE; NACKE, 2010).

Como já explicado, isso normalmente seria algo bom para um país, como em sua economia, serviços, inclusão social, porém, quando falamos de guerra cibernética isso é algo negativo. Depois da conhecida Noite do Bronze, de repente, os servidores que sustentam os sites mais utilizados no país foram inundados de pedidos de acesso, um dilúvio de pedidos, que por sua vez faz com que o servidor não suporte essa enorme quantidade de pedidos de aceso, fazendo-o com que se desligue. Os Estonianos, então, não puderam seguir com sua vida cotidiana, como acessar bancos, jornais virtuais, ou serviços eletrônicos do governo (CLARKE; NACKE, 2010).

A Estônia foi alvo de um ataque de distribuição de negação de serviço, nele, os computadores atacantes, chamados de *botnets*[26], que controlam computadores zumbis[27], lançaram essa propagação de acessos na Estônia, sofrendo o maior ataque DDOS já visto. Vários *botnets* diferentes, cada um controlando dezenas de computadores infectados, causaram o desligamento de sites públicos, telefonia, serviços de cartão de crédito, o comércio, as comunicações em todo o país, a própria Internet, como também afetando, naturalmente, o maior banco estoniano, o Hansapank. No começo dos ataques a algumas páginas estonianas da Internet, os estonianos acharam que isso era só algum ataque cibernético pequeno russo de hackers aborrecidos. Até que tomou as proporções conhecidas (CLARKE; NACKE, 2010).

26 *Botnets*, é a junção dos diminutivos de *robot* e *network*. São os computadores que controlam os zumbis, ordenando-os a obedecerem seus comandos (CLARKE; NACKE, 2010).

27 Computadores zumbis são computadores que estão sob controle remoto de outro. Seguem instruções sem o conhecimento, ou consentimento de seus proprietários. Seus donos nunca percebem quando seu computador está ou não zumbi, o único indicador dessa atividade maligna é quando o computador se mostra um pouco devagar, ou demora mais do que o de costume a abrir um *site* (CLARKE; NACKE, 2010).

3.2.2.3 Pós ataque

A Estônia trouxe o assunto para o Conselho do Atlântico Norte, o mais alto órgão da aliança militar da Organização do Tratado do Atlântico Norte (OTAN). Prontamente uma equipe ciber defensiva começou a tentar contra medidas que já tinham sido bem sucedidas contra DDOS menores. As informações enviadas dos *botnets* para os computadores zumbis foram rastreadas, chegando até aos computadores finais. A conclusão encontrada, como era de se esperar, foi a de que o ataque tinha vido da Rússia, e o código dos *botnets* estavam escrito no alfabeto cirílico, o alfabeto utilizado nesse país (CLARKE; NACKE, 2010).

A Rússia, obviamente, negou indignada qualquer envolvimento no ataque cibernético a Estônia. Ela recusou o pedido formal diplomático estoniano para auxilia-la na detecção dos atacantes. Alguns funcionários do governo russo admitiram que era possível que russos patrióticos, irritados com a Estônia, tenham realizado o ataque DDOS (CLARKE; NACKE, 2010).

Em 2008, a OTAN criou um centro de defesa cibernética em Tallinn, o *Cooperative Cyber Defence Centre of Excellence*, a poucos quilômetros de onde a estátua gigante do soldado de bronze se encontrava. Hoje, no lugar desse monumento, existe um bosque (CLARKE; NACKE, 2010).

3.2.3 EUA, Israel x Irã

Em 2010, os sistemas computacionais de infraestrutura crítica nuclear iraniana de enriquecimento de urânio sofrem sérios danos. A causa: a atuação sistemática e imperceptível do *worm* (verme) denominado Stuxnet. Especialistas em segurança da informação do mundo todo ficam surpresos com tamanha sofisticação da engenharia dessa praga virtual a qual atacou o sistema SCADA – ou sistema de controle de supervisão e aquisição de dados – desenvolvido pela Siemens, atrasando o programa nuclear iraniano em muitos meses (LOPES, 2013).

Os especialistas cogitam sobre a autoria do *worm* Stuxnet, já que analisando o código-fonte do verme, afirmam que é praticamente impossível que o Stuxnet tenha sido desenvolvido por uma empresa ou uma universidade, pois seu alvo é bastante incomum: o sistema SCADA da Siemens de centrífugas enriquecedoras de urânio iraniana. O que era apenas cogitação, começou a ser visto com maior certeza, de que o Irã tenha sofrido em suas usinas um ataque cibernético mais avançado existente na época, motivado por questão de

política externa, com intuito de sabotar programa nuclear iraniano, sem o uso de forças armadas tradicionais (LOPES, 2013).

O verme Stuxnet foi resultado de uma parceria entre os Estados Unidos e Israel, maquinada como um programa ultrassecreto, intitulado de Olympic Games, o qual é política, jurídica e tecnicamente arquitetado, tendo a construção dele demandado meses, sobretudo para que a equipe jurídica se certificasse de que seu código-fonte não violasse nenhuma lei de conflito armado, tendo início no final do segundo governo W. Bush. Tal programa teve tanto um objetivo estratégico quanto político, sendo eles o de sabotar o programa nuclear iraniano, e o de convencer Israel de que é possível lidar com a questão iraniana sem ser por meio de ataques aéreos (LOPES, 2013).

3.2.4 Índia x Paquistão

Um dos conflitos mais sérios que ocorrem no espaço cibernético, está a intensa rivalidade entre a Índia e o Paquistão. Desde 1998 já ocorre essa rivalidade no ciberespaço entre grupos de hackers de ambos os países (HEICKERÖ, 2009).

Após o anunciamento oficial de teste do míssel Pokhran II pelo governo indiano, o grupo *hacker* Milworm atacou o site do Centro de Pesquisa Atômica de Bhabha, desconfigurando suas informações, colocando nele mensagens anti-indianas. A identidade do grupo não ficou bem clara, porém especialistas afirmam que possa ser paquistanesa (HEICKERÖ, 2009).

Algum tempo depois, outro grupo hacker paquistanês fez um ataque ciberespacial à Índia, dessa vez, ao site do Exército indiano. Às pessoas responsáveis pelo web site do Exército foram pedidos que mudassem o número do IP dos computadores para outro número. Depois dessa mudança, o grupo novamente colocou mensagens anti-indianas. A razão do ataque ter sido altamente bem sucedido foi causado pelo servidor que controlava este site não estar sob controle físico de autoridades indianas, estava no exterior. Isso mostra o perigo de não ter controle cibernético sobre informações críticas (HEICKERÖ, 2009).

Entre os anos de 1998 e 2001 o número de ataques cibernéticos paquistaneses contra web sites indianos aumentou de apenas 4 em 1999 para mais de 150 em 2001, de acordo com a agência indiana CERT, já o número de ataques indianos contra seus inimigos era de 7 em 2000 crescendo depois para 18. Entre os anos de 2002 e 2004 a situação se estabeleceu e o conflito caducou (HEICKERÖ, 2009).

Depois desses sucessivos ataques, houve um cessar fogo entre ambas as partes. Os grupos de hackers paquistaneses Pakistan Hackers Club e G-Force, juntamente com o grupo indiano NEO, concordaram em não continuarem essa luta. O conflito causou centenas de ataques aos sites dos dois países, envolvendo mais de 150 grupos de hackers paquistaneses e no mínimo 10 grupos indianos (HEICKERÖ, 2009).

Entretanto, em novembro de 2008 um novo conflito cibernético começou novamente. O motivo foi causado por um ataque terrorista em Bombaim iniciado em solo paquistanês. Juntamente a isso, o grupo indiano HMG atacou o site do Paquistão referente ao Ministério de Petróleo e Gás, em que ele saiu do ar por alguns minutos. Em resposta, o Pakistan Cyber Army (PCA) lançou um ataque a cerca de 5 sites indianos, como exemplo ao site indiano de gás natural e petróleo. O PCA também enviou alertas a comunidade hacker de seu país inimigo a não continuarem suas atividades (HEICKERÖ, 2009).

Os ataques continuaram prosseguindo, afetando o ciberespaço dos dois Estados, até afetando bancos, como os indianos Barroda e State Bank of India. Os governos desse dois países concordaram em tentar prevenir esses ataques cibernéticos (HEICKERÖ, 2009).

CONSIDERAÇÕES FINAIS

O presente trabalho mostrou os desdobramentos e impactos causados nas Relações Internacionais advindos do espaço cibernético como uma nova realidade que os Estados e atores das relações internacionais vivem.

A partir das discussões é possível depreender que, de fato, foram consolidados processos de securitização do cibernético. Dentre as ações identificadas e integrantes da securitização, podem ser ressaltadas a criação de várias agências de inteligência cibernética, que foram concebidas tanto para estratégias de defesa quanto estratégias de ataque.

No capítulo 2, percebeu-se a emergência de uma governança interna voltada para o ciberespaço, para tanto, os países estudados promoveram a criação de uma série de instituições e dessas agências. É perceptível que tais instituições, normalmente, compõem o quadro de órgãos militares. Outro fator a ser ressaltado diz respeito ao papel das Forças Armadas e sua a responsabilidade e defesa da soberania do país, tendo documentos governamentais regulando a criação desses órgãos e sua organicidade interna.

No capítulo 3, através dos conflitos cibernéticos entre países, foi mostrado o quão é importante para defesa da soberania do próprio país ter capacidades cibernéticas para se prevenir e se defender de ataques.

Portanto, observa-se através da pesquisa apresentada, as repercussões desse mundo virtual no mundo real, e que não há diferença entre esses. Vários países já alegaram que qualquer ataque cibernético poderá ser respondido militarmente. O espaço cibernético está comprovado como um tema securitizado, assim como sua alta importância para as Relações Internacionais.

REFERÊNCIAS

ASSIS, Emanuel César Pires. *Ciberespaço e Pós-Modernidade em Neuromancer De Wiliam Gibson*. Anais do VI Encontro de Estudos Multidisciplinares em Cultura. 2010. Disponível em: http://www.cult.ufba.br/wordpress/24841.pdf. Acesso em 10 de novembro de 2014.

BOSTON DYNAMICS. *Changing Your Idea of What Robots Can Do*. Digital, S/P. Disponível em: http://www.bostondynamics.com//. Acesso em 10 de novembro de 2014. s/a

BUZAN, Barry, HANSEN, Lene. *A Evolução dos Estudos de Segurança Internacional.* Trad. Flávio Lira. São Paulo: Editora Unesp, 2012.

CANALTECH. *Ministério de Minas e Energia foi Alvo de Espionagem de Agência Canadense*. Digital, S/P. Disponível em: http://canaltech.com.br/noticia/espionagem/Ministerio-de-Minas-e-Energia-foi-alvo-de-espionagem-de-agencia-canadense/. Acesso em 4 de novembro de 2014. s/a

CLARKE, Richard A; KNAKE, Robert K. *Cyber War: The Next Threat to National Security and What To Do About It*. Nova Iorque: HarperCollins, 290 p. 2010.

CLAUSEWITZ, Carl von**. Da Guerra: A Arte da Estratégia**, ed. and trans. Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press. 1976.

COLLINS, Allan. *Contemporary Security Studies - second edition.* Oxford: Oxford Universiyy Press. p. 109 – 123. 2010.

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

DARPA. *Our Work***.** Digital, S/P. Disponível em: http://www.darpa.mil/our_work/. Acesso em 10 de novembro de 2014. s/a

DISCOVERY BRASIL. *A Era do Ciberespaço*. Digital, S/P. Disponível em: http://discoverybrasil.uol.com.br/internet/a-era-do-ciberespaco.shtml. Acesso em 10 de novembro de 2014. s/a

EMMERS, Ralf. *Securitization***.** In: COLLINS, Allan. **Contemporary Security Studies - second edition.** Oxford: Oxford Universiyy Press. p. 109 – 123. 2010.

GLOBO CIÊNCIA. Norbert Wiener – Cibernética. Vídeo (6min56ss). Disponível em: http://globotv.globo.com/rede-globo/globo-ciencia/v/norbert-wiener-cibernetica-parte-1/1552323/. Acesso em 10 de novembro de 2014.

CAMBOU, Don. *Maravilhas Modernas*: Velocidade. History Channel. s/p, 2009

HEIDELBERG INSTITUTE ON INTERNATIONAL CONFLICT RESEARCH. *Conflict Barometer - 11th Annual Conflict Analysis.* Department of Political Science, University of Heidelberg, Marstallstrasse 6, D- 69117 Heidelberg. 2002.

INDIA. *Discussion draft On National Cyber Security Policy*. Department of Information Technology. Ministry of Communications and Information Technology. Electronics Niketan, Lodhi Road. Government of India New Delhi – 110003. 2011.

ISMAIL, Shaharudin; YUNOS, Zahri. *Cyberspace the new war frontier.* National ICT Security and Emergency Response Centre (NISER). 2005.

LOPES, Gills. *Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá* / Gills Lopes Macêdo Souza. – Recife: O autor, 2013. 133 f.,: il. ; 30 cm. Orientador: Prof. Dr. Marcelo de Almeida Medeiros. Dissertação (mestrado) – Universidade Federal de Pernambuco, CFCH. Programa de Pós-Graduação em Ciência Política, 2013.

MORESI, Eduardo Amadeu Dutra. *Informação: uma arma cibernética?* Décima Segunda Conferencia Iberoamericana en Sistemas, Cibernética e Informática. Orl. USA. 2013.

NOBRE, Fábio. *O processo de securitização no subcomplexo amazônico de segurança – explicando as reações do Brasil frente à militarização da Colômbia* / Fábio Nobre – Recife: O autor, 2013. 116 f.,: il. ; 30 cm. Orientador: Prof. Dr. Marcos Aurélio Guedes de Oliveira. Dissertação (mestrado) – Universidade Federal de Pernambuco

RIBAS DE MOURA, João Batista. *NSA e a soberania brasileira: análise das contramedidas*. Revista Inteligência Em Foco Edição Especial Nº 01. Brasília – DF. Janeiro/2014.

RINPOCHE, Chagdud Tulku. **Gates to Buddhist Practice**. Tradução: Manoel Vilas. Taquara: Paramita, 1995

SANDRONI, Gabriela A. *Prevenção Da Guerra No Espaço Cibernético*. Anais do IV Simpósio de Pós-Graduação em Relações Internacionais do Programa "San Tiago Dantas" (UNESP, UNICAMP e PUC/SP) de 05 a 08 de Novembro de 2013. Disponível em: http://www.jurisway.org.br/v2/dhall.asp?id_dh=12381. Acesso em 10 de novembro de 2014.

TED. *How cyberattacks threaten real-world peace*. Vídeo (9min24ss). Disponível em: http://www.ted.com/talks/guy_philippe_goldstein_how_cyberattacks_threaten_real_world_peace. Acesso em 10 de novembro de 2014. 2010.

TERRA. *Premiê Canadense se diz Muito Preocupado com Acusações de Espionagem no Brasil*. Digital, S/P. Disponível em: http://noticias.terra.com.br/mundo/premie-canadense-se-diz-muito-preocupado-com-acusacoes-de-espionagem-no-brasil,c547c05a38591410VgnCLD2000000dc6eb0aRCRD.html. Acesso em 4 de novembro de 2014. s/a

THE GUARDIAN. *History of 5-eyes*. Digital, S/P. Disponível em: http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer. Acesso em 4 de novembro de 2014. s/a

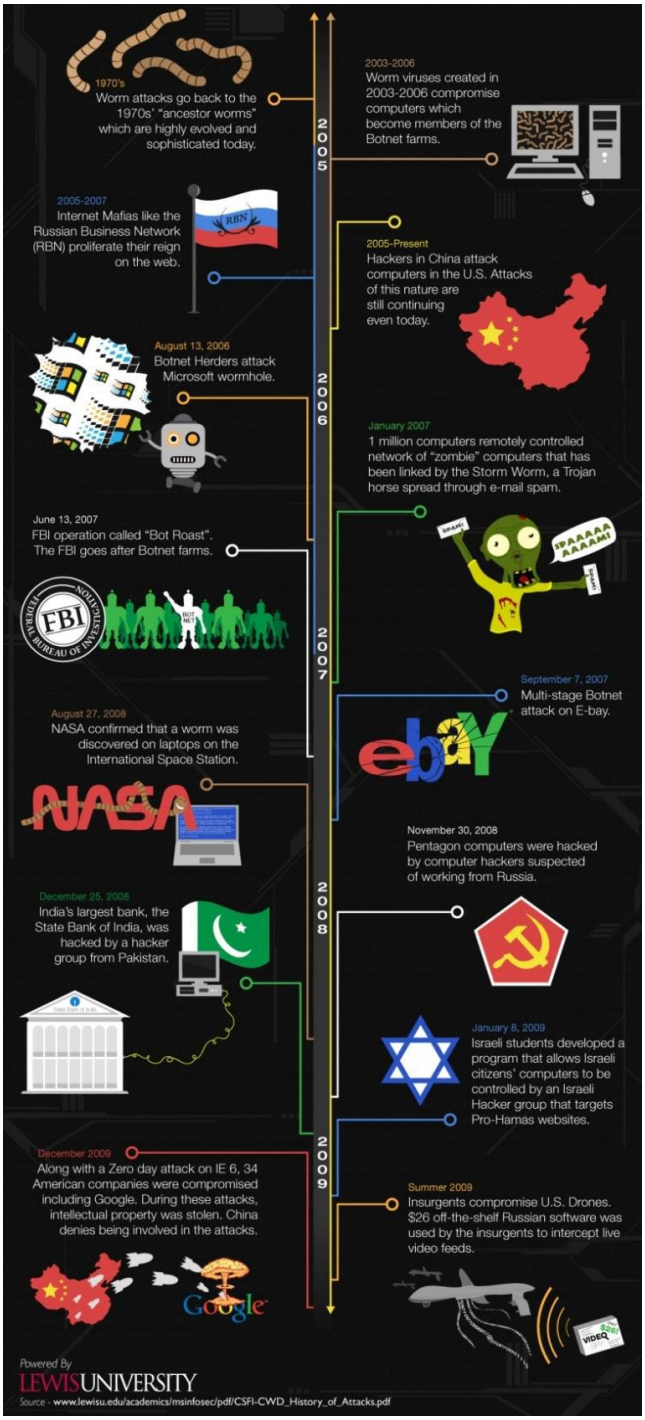
YOUTUBE. *Clube do Livro - Neuromancer, de William Gibson - B1*. Vídeo (14min14ss). Disponível em: https://www.youtube.com/watch?v=ESNovDPqTgY. Acesso em 10 de novembro de 2014. s/a

YOUTUBE. *Richard A. Clarke: Cyberwar in 2013*. Vídeo (21min27ss). Disponível em: https://www.youtube.com/watch?v=6_ek8mugOUc. Acesso em 10 de novembro de 2014. s/a.

ANEXOS

ANEXO I

Histórico da *cyber warfare* na política internacional (1970-2009)



FONTE: Lopes (2013)

ANEXO II

Comparativo das principais diferenças encontradas entre Brasil, Estados Unidos, Rússia e Índia

	Estados Unidos	Rússia	Índia	Brasil
Arranjo institucional	US Cyber Command cuida da defesa e NSA cuida da segurança, ambos dentro da estrutura do DoD e com o mesmo dirigente.	-	Não há um órgão que assuma as responsabilidades da segurança e defesa. Algumas ações são tomadas no Ministério das Comunicações e Tecnologias da Informação.	Segurança: GSI/PR Defesa: CDCiber/EB/MD São estruturas distintas e com lideranças distintas.
Orçamento de gestão em 2012 para segurança e defesa cibernética	DoD: US$ 2,3 bilhões CyberComm: U$ 119 milhões (United States, 2012b)	-	-	GSI/PR: US$ 7 milhões CDCiber: US$ 45 milhões (Hulse, 2012)

Diretrizes	• Espaço cibernético:
	  • Aberto
	  • Interoperável
	  • Seguro
	  • Confiável
	• Liberdades fundamentais
	• Respeito à propriedade
	• Privacidade
	• Proteção contra o crime
	• Autodefesa
	• Estabilidade de rede
	• Governança multilateral
	• Dever de diligência
		• Respeito ao Estado de direito
		• Prioridade (Rússia)
		• Atenção à complexidade do ambiente virtual
		• Interação internacional
		• Cooperação
		• Inovação
			• Prioridade governamental
			• Vanguarda tecnológica
			• Inteligência cibernética
			• Hierarquia
			• Foco da política em pessoas
			• O tema deve ter força a partir dos níveis estratégicos
				Defesa nacional:
				• Dissuadir hostilidades
				• Agilidade de resposta a ameaças
				• Fortalecer o setor cibernético
				• Flexibilidade operacional
				• Unificar a operação das três Forças
				• Estruturar o potencial estratégico em torno de capacidades
				• Preparar combatentes
				• Integração da América do Sul
				• Capacitar a indústria nacional

Resumo	Propõem-se a liderar o processo regulatório e influenciar o desenvolvimento da internet para o mundo a partir do que julgam ser melhor para todos.	Já reconheceram a importância do setor e, em resposta às iniciativas dos Estados Unidos, estão se estruturando para eventuais conflitos cibernéticos.	Ainda com pouca expressão no espaço cibernético. Está atenta ao que vem acontecendo no mundo e não pretende se distanciar das discussões.	Apesar de algumas ações estarem em andamento, a infraestrutura nacional de TI é ruim. A organização institucional tende a não favorecer ações integradas.

Fonte: Da Cruz Júnior (2013)