UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO SÓCIO-ECONÔMICO
DEPARTAMENTO DE CIÊNCIAS ECONÔMICAS E RELAÇÕES INTERNACIONAIS

Marcos Tocchetto Agostini

A CIBERNÉTICA SOB A ÓTICA DO FENÔMENO DA GUERRA E DA AGENDA DE SEGURANÇA

FLORIANÓPOLIS 2014

MARCOS TOCCHETTO AGOSTINI

A CIBERNÉTICA SOB A ÓTICA DO FENÔMENO DA GUERRA E DA AGENDA DE SEGURANÇA

Monografia submetida ao curso de Relações Internacionais da Universidade Federal de Santa Catarina, como requisito obrigatório para obtenção do grau de Bacharelado.

Orientador: Prof.Dr(a). Graciela De Conti Pagliari

FLORIANÓPOLIS 2014

MARCOS TOCCHETTO AGOSTINI

A CIBERNÉTICA SOB A ÓTICA DO FENÔMENO DA GUERRA E DA AGENDA DE SEGURANÇA

A Banca Examinadora resolveu atribuir a nota 10,0 (dez) ao aluno Marcos Tocchetto Agostini na disciplina CNM 7280 – Monografia, pela apresentação deste trabalho.

Banca Examinadora:

_____

Prof.Dr.(a). Graciela De Conti Pagliari

_____

Ten.Cel. Inf. Wagner Alves de Oliveira

_____

Prof. Ms. Luiz Felipe Rebello

AGRADECIMENTOS

À minha mãe Vera e ao meu pai Moacir por todo o incentivo, esforço, carinho e estrutura que me proporcionaram ao longo da vida. Pela impecável educação que puderam me oferecer e por sempre terem acreditado no meu esforço. Aos meus irmãos Leandro e Liane, aos quais tenho em suas vidas uma grande inspiração, por me mostrarem que o amor e a amizade fraternal prevalecem apesar de toda a distância. Aos meus inúmeros familiares, tios e tias, primos, com seus conselhos importantes, e, principalmente, à minha avó, Cecília. Com certeza a família é tudo, é o principal meio para conquistarmos nossos objetivos, para nos fornecer alegria, apoio e força. Não poderia comemorar tal etapa importante da minha vida sem a presença de vocês.

À minha namorada Cassiê, pelo apoio emocional, pelo tempo dedicado a mim, pelo amor e carinho destinados com tanta tenacidade. Pela compreensão nos momentos difíceis e por ter acreditado no nosso relacionamento mesmo permanecendo longos anos distantes. Agradeço pelos conselhos, por me ajudar a seguir os meus objetivos profissionais, por toda a preocupação diária e, também, por me auxiliar em várias revisões e opiniões deste trabalho.

À minha admirada professora e orientadora, Graciela De Conti Pagliari, pelos ensinamentos e conselhos sempre construtivos. Pela fidúcia no meu potencial e no presente trabalho e pela liberdade na produção do mesmo. Agradeço pela sua constante presença durante toda minha graduação e ter feito aflorar meu entusiasmo pelos estudos na área de Segurança Internacional. Sem dúvidas, levarei sua postura pessoal e profissional pelo resto da minha vida.

Agradecer também aos demais professores do curso de Relações Internacionais da Universidade Federal de Santa Catarina, sem os quais não seria possível a criação e desenvolvimento de um novo e tão desafiador curso de graduação. Meu muito obrigado pelo empenho e dedicação que me proporcionaram uma formação de ótima qualidade.

Por fim, mas não menos importantes, aos meus colegas de Relações Internacionais, em especial aos meus queridos e eternos amigos que estiveram constantemente ao meu lado ao longo desses quatro anos: Raphael, João, Xuxa e Thiago. Agradeço pela diversão, pelas viagens, pela parceria, pela ajuda nos estudos, pela confiança que pude depositar e que pude ter a honra de receber. Ao meu amigo de longa data Ednaldo, pelos carinhosos, verdadeiros e insuperáveis conselhos, pelos seus admiráveis valores e princípios aos quais eu tenho como exemplo a ser seguido e pela completa dedicação a nossa amizade. Sem amigos, não somos nada.

RESUMO

O fenômeno da guerra e a questão da segurança são discutidos e estudados desde os primórdios da criação dos Estados nacionais. Os adventos da informação, da comunicação e do conhecimento incidiram diretamente em tais questões, conferindo àqueles que os detém e deles se aproveitam uma enorme vantagem na competição e nos conflitos internacionais. Nesse sentido, a chegada de novas tecnologias gera uma necessidade de avaliar seus efeitos nas relações estratégicas. Então, para fins do presente trabalho, as tecnologias de comunicação e informação (TICs) adquirem importância para a formação de um novo tema e novo campo de batalha entre os Estados: a cibernética. O objetivo deste trabalho consiste em analisar como o setor cibernético tem se tornado relevante para a agenda de segurança e para as relações estratégicas no âmbito das relações internacionais contemporâneas, e especificamente, para o Brasil. Parte-se da concepção de que há um processo de securitização do espaço cibernético em uma perspectiva construtivista e uma utilização dos elementos do setor de forma ofensiva contra outros Estados e organizações, servindo também como auxiliar numa guerra convencional, colocando em risco a integridade e a sobrevivência dos Estados numa perspectiva realista. Nas já tão complexas relações internacionais, a cibernética surge como mais um complicador, capaz de modificar as relações de poder interestatais, inserindo-se na agenda de segurança dos Estados e na arte de fazer a guerra.

Palavras-chave: agenda de segurança, guerra, setor cibernético, securitização, construtivismo.

ABSTRACT

The phenomenon of war and security issues are discussed and studied since the beginning of creation of national states. The advent of information, communication and knowledge were directly levied on such issues, giving those who hold and take advantage of them a huge advantage in the competition and in international conflicts. In this sense, the arrival of new technologies generates a need to evaluate their effects on strategic relationships. So, for purposes of this study, the information and communication technologies (ICTs) acquired importance for the formation of a new theme and new battleground between states: the cybernetics. The objective of this study is to examine how the cyber sector has become relevant to the security agenda and the strategic relationship in contemporary international relations, and specifically, to Brazil. It starts from the idea that there is a process of securitization of cyberspace in a constructivist perspective and an utilization of the elements of the sector offensively against other states and organizations, also serving as an assistant in a conventional war, putting at risk the integrity and the survival of the States in a realistic view. In the ever so complex international relations, cybernetic emerges as another complicating factor able to modify relations of interstate power, being part of the security agenda of States and the art of warfare.

Key words: security agenda, war, cybernetic, securitization, constructivism.

.

SUMÁRIO

1 INTRODUÇÃO

O fenômeno da guerra e a segurança dos Estados são discutidos e estudados desde os primórdios da criação dos Estados nacionais. Os assuntos de segurança nacional e internacional sempre estiveram presentes na lista de prioridades dos governos, assim como a arte de fazer a guerra sempre apreendeu a atenção de várias gerações de estudiosos das relações internacionais e dos setores estratégicos.

O advento da informação, da comunicação e do conhecimento, tornou tais elementos fundamentais para as questões estratégicas dos Estados, aferindo àqueles que os detém e deles se aproveitam um indubitável proveito na competição e nos conflitos internacionais. A internet proporciona conexão em tempo real e alcance mundial. Por outro lado, sua grande vulnerabilidade, aliada à existência de novos atores de caráter transnacional, fez crescer a preocupação com a proteção da informação, dando origem à segurança da informação, expandindo-se mais tarde para o conceito de segurança cibernética ao preocupar-se também com a proteção das infraestruturas críticas nacionais.

Tanto a guerra como a agenda de segurança se modificaram ao longo da história. Os instrumentos, as finalidades, as táticas de combate, a tecnologia utilizada, a relação civis/militares, entre outros, fizeram parte da evolução das gerações e da natureza dos conflitos. Resultados do imenso avanço tecnológico do século XXI, novos elementos ganharam relevância nas disputas e preocupações interestatais. Dessa forma, as tecnologias de comunicação e informação (TICs) adquiriram importância para a formação de um novo campo de batalha entre os Estados: a cibernética. O setor cibernético vem sendo usado como meio para espionagem, enfraquecimento das forças militares adversárias, sabotagem e ataques contra sistemas e infraestrutura de outros países. Assim, para muitos especialistas, a cibernética pode tornar-se a área de defesa mais importante do novo século.

Nas já tão complexas relações internacionais, em que a guerra convencional é cada vez mais depreciada moralmente, a busca pela continuação da política por outros meios é cada vez mais inovadora. Enquanto a guerra tradicional caracteriza-se pela bem definida responsabilidade dos Estados, a guerra cibernética possui elementos particulares, como o anonimato, que torna difícil a responsabilização direta de eventuais ataques. Ao mesmo tempo, a guerra cibernética não perde

algumas características da guerra tradicional, nem mesmo das chamadas novas guerras, ora aproximando-se do modelo clausewitziano, ora da perspectiva kaldoriana.

Ainda, a ciberguerra pode servir como instrumento direto para causar enormes prejuízos ao inimigo, afetando sistemas e infraestruturas críticas, furtando dados ou projetos confidenciais do governo e de sistemas bélicos, entre outros. O atacante nesse campo possui a vantagem do anonimato e da distância física, podendo interagir igualmente com outras dimensões, servindo também, portanto, como auxiliar em uma guerra convencional. A cada regra imposta ao uso da força, novas formas de luta são criadas. E é nesse sentido que a internet pode vir a ser a arma do futuro, e, juntamente a ela, surge uma preocupação quanto à segurança cibernética.

Igualmente nesse processo evolutivo, a agenda de segurança nacional perdeu a partir de 1950 seu caráter exclusivamente militar e restrito quando novos temas surgiram e entraram nas discussões de segurança. Inicialmente de caráter nuclear e energético, seguindo para temas econômicos e ambientais, podendo incorporar agora o setor cibernético. Nesse sentido, os estudos abrangentes de segurança da Escola de Copenhagen colocam-se como fundamentais para o trabalho, sobretudo pela contribuição construtivista na teoria de securitização. O surgimento de novos atores no sistema internacional ocasionou também a ampliação dos atores ameaçadores, cada vez mais de característica transnacional, trazendo consigo novos temas de segurança. Por esse motivo, essa vertente abrangente com seu aspecto construtivista torna-se importante para o trabalho na medida em que permite maior abertura para análise do tema.

Ademais, a teoria realista[1], por se preocupar primordialmente com questões de defesa e segurança, coloca-se como corrente conveniente para uma análise incipiente, em virtude de determinar a sobrevivência como o objetivo mais importante do Estado, tendo este como principal unidade de análise. Ao mesmo tempo, a visão realista, no que tange a segurança internacional, não se diferencia da perspectiva abrangente da Escola de Copenhagen, podendo, assim, serem correlacionadas[2].

---

[1] Sempre que aqui se referir a uma teoria/concepção/abordagem/escola/paradigma/perspectiva/visão realista, deve-se inferir o que pode ser considerado como sua essência, quais sejam, a caracterização do sistema internacional como anárquico, a permanente competição-conflito, o estadocentrismo e, a segurança e o militarismo priorizados.

[2] A relação entre a teoria realista e os aspectos construtivistas de securitização da Escola de Copenhagen será mais bem desenvolvida posteriormente.

De uma maneira geral, os ataques cibernéticos podem ocorrer de forma autônoma, podem estar diretamente ligados a Estados ou, ainda, podem ser originados por atores não estatais. Esse trabalho, então, preocupa-se majoritariamente com o envolvimento estatal em alguma medida, haja vista que é a presença do Estado que caracteriza fundamentalmente uma guerra cibernética. Diante disso, casos como o ataque às instalações nucleares do Irã em 2010, aos serviços públicos da Estônia em 2007, aos sites governamentais e privados da Geórgia em 2008, entre outros exemplos, serão mais especificamente abordados. Além do mais, valerá ressaltar o crescimento dos chamados exércitos eletrônicos ou organizações por procuração, como acontece na Rússia, na China, nos Estados Unidos (EUA) e na Síria.

Não obstante, o Brasil ganha cada vez mais destaque no cenário internacional, especialmente ao organizar grandiosos eventos internacionais, como a Conferência Rio+20, a Copa do Mundo de 2014, as Olimpíadas de 2016, entre outros. Nesse sentido, é tido como fundamental para o contínuo desenvolvimento do país o investimento em segurança nacional, incluindo, então, a segurança cibernética. Tais eventos citados serviram como impulsionadores dos primeiros esforços do país no setor cibernético. Cresce cada vez mais a importância de proteção de dados confidenciais militares e da sociedade, assim como das infraestruturas críticas do país. Os primeiros esforços concretos e significativos para esse novo ramo da segurança e defesa no Brasil foram iniciados com a Estratégia Nacional de Defesa (END) de 2008. Ademais, os debates, competências e atribuições estão envoltas, sobretudo, sob o Ministério da Defesa (MD) e sob o Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Há um entendimento de vários países de que a segurança cibernética é um tema novo. É uma nova agenda que se abre para as relações internacionais contemporâneas. Diante disso, o presente trabalho possui como objetivo geral analisar e explicar como o meio cibernético pode ser utilizado como nova forma de conflito entre os atores estatais. Dessa maneira, o problema de partida da pesquisa proposta é o seguinte: Porque o setor cibernético tornou-se relevante para a agenda de segurança e para as relações estratégicas do Brasil e das relações internacionais a partir do século XXI?

A hipótese levantada inicialmente é de que há um processo de securitização do espaço cibernético por parte dos Estados – mais especificamente, no caso

brasileiro que será apresentado – em uma perspectiva construtivista. Além do mais, nota-se a utilização dos elementos do setor cibernético de forma ofensiva contra outros Estados e organizações, servindo também como auxiliar numa guerra convencional, colocando em risco a integridade e a sobrevivência dos Estados numa perspectiva realista.

O primeiro capítulo consiste na construção de um arcabouço teórico pautado na evolução da natureza e das gerações da guerra, e na evolução dos temas presentes na agenda de segurança dos Estados. Dessa forma, pretende-se retomar os principais aspectos do conceito de guerra e segurança, bem como seus progressos, sob a base da Escola de Copenhagen e seus preceitos construtivistas. Serão utilizados como base produções acadêmicas de autores como Barry Buzan, Ole Waever, Grace Tanno, Lene Hansen, Helen Nissenbaum, Carl von Clausewitz, Mary Kaldor e Willian Lind.

No capítulo sucessivo, será abordado o espaço cibernético mais detalhadamente. Serão apresentados os conceitos basilares, os componentes, as características relacionadas a esse meio, fazendo uma análise de como a guerra cibernética pode se manifestar ou já se manifesta no cenário internacional. Ainda, será exibida uma análise de casos no Irã, Estônia e Geórgia em que a cibernética é propriamente utilizada como um novo domínio de guerra. As fontes primárias tomadas para auxiliar na construção deste capítulo serão produções acadêmicas dos autores Walfredo Bento Ferreira Neto, Richard Clarke, Robert Knake, Jeffrey Carr, Thomas Rid e Joseph Nye Jr. As principais fontes secundárias e auxiliares serão o Manual Tallin de Direito Internacional aplicado à guerra cibernética, preparado pela Cambridge University Press a pedido do Centro de Defesa Cibernético da Organização do Tratado do Atlântico Norte (OTAN); e o relatório sobre infraestrutura crítica em defesa cibernética elaborado pela empresa McAfee.

Por fim, propõem-se explanar a importância do meio cibernético para o Estado Brasileiro, delimitando as políticas e órgãos responsáveis em sua formação, atuação e segurança. Este último capítulo será finalizado com a apresentação de desafios e obstáculos cibernéticos para o país. Os materiais empregados no trabalho para a consecução deste objetivo final serão, sobretudo, a Estratégia Nacional de Defesa de 2008 e 2012, o Livro Verde de Segurança Cibernética no Brasil, o Livro Branco de Defesa Nacional, a Política Cibernética de Defesa brasileira e o

documento Desafios Estratégicos para a Segurança e Defesa Cibernética – elaborados por secretarias e ministérios do governo.

A pesquisa será complementada com uma série de artigos acadêmicos que viabilizarão um parâmetro mais generalizado sobre o tema na esfera internacional e também em âmbito nacional, e ajudarão na construção dos objetivos escolhidos.

Vale ressalvar que o tema proposto ainda é consideravelmente recente, carecendo de trabalhos acadêmicos sólidos e substanciais em grande número. Ainda que muitas vezes o tema possa parecer exagerado, digno de filmes hollywoodianos, acredita-se na concretude e realidade do setor cibernético como um novo campo de batalha e como um alvo de preocupação cada vez maior dos Estados. Não faz parte da abrangência deste trabalho considerar questões tecnicamente complexas sobre o funcionamento dos componentes do setor, os quais ultrapassariam o conhecimento exigido por um analista de relações internacionais. A característica incipiente do setor tornou a elaboração do trabalho desafiador, mas, considerando-se o desígnio de exigência de uma monografia, tentar-se-á alcançar de forma concisa e realística os objetivos supracitados.

2 AGENDA DE SEGURANÇA, GERAÇÕES E NATUREZA DA GUERRA

Analisar o surgimento dos diferentes temas presentes nas discussões sobre a agenda de segurança[3], bem como suas evoluções e consequências, juntamente com um estudo do fenômeno da guerra, abordando suas diversas gerações e naturezas, fazem-se parte auxiliar na elaboração deste trabalho que tem como objetivo pesquisar o setor cibernético como uma nova agenda de segurança nas relações internacionais (RI) e como uma nova forma de conflito. O presente capítulo, assim sendo, pretende traçar um panorama sobre a evolução desta agenda e do modo de fazer a guerra, relacionando-os ao tema central. Em relação à evolução da agenda de segurança, o trabalho basear-se-á, sobretudo, na Escola de Copenhagen e seus preceitos construtivistas; e em relação a evolução do fenômeno da guerra, nas análises das gerações de guerra e da natureza destas de Clausewitz (1832) e de Kaldor (1998, 2005). Finalizaremos esta seção com uma exposição sobre a teoria de securitização proposta por Waever (1995) e também abordada por Buzan (1998, 2012), que servirá para diagnósticos mais específicos em relação à cibersegurança.

2.1 A EVOLUÇÃO DA AGENDA DE SEGURANÇA INTERNACIONAL

O fenômeno da guerra e da preocupação com a segurança sempre apreenderam a atenção de várias gerações de estudiosos das relações internacionais e dos setores estratégicos. Essas duas questões estiveram continuamente presentes nas concepções basilares dos Estados nacionais, os quais estão constantemente em busca de sobrevivência. Nesse sentido, as primeiras discussões no campo das relações internacionais surgiram ao findar da Primeira Guerra Mundial como uma tentativa de entendimento dos conflitos, apoiada, sobretudo, pela teoria realista. Mas as necessidades e preocupações com a defesa dos elementos constitutivos do Estado, quais sejam, território, povo e governo[4]

[3]Ao que se entende por segurança, para os fins do presente trabalho, deve-se pensá-la como sendo o controle ou a ausência de ameaças ao Estado. Para Waever (1995), ainda, o conceito de segurança refere-se ao Estado, mas a segurança nacional não pode ser compreendida apenas no nível do Estado, ela é dependente das dinâmicas internacionais e regionais. Para Buzan e Hansen (2012), o conceito de segurança internacional acompanha (e não substituiu) o de segurança nacional, resultado da globalização que pormenorizou a distinção entre “dentro” e “fora”.

[4]Darcy Azambuja (1957) destaca que o povo é a população do Estado sujeita aos mesmos aspectos jurídicos; o território é a delimitação territorial que dará limite à soberania do Estado; o governo estaria ligado à ideia de soberania, vista como a força ou ideia de força que decide o destino do povo. Assim, os dois primeiros elementos são tidos como elementos materiais, enquanto, o terceiro elemento está

(AZAMBUJA, 1957, p.17-18), datam desde a solidificação do sistema de Estados soberanos a partir da Paz de Vestefália. No mesmo sentido:

> "o ponto de partida das relações internacionais é a existência de estados, comunidades políticas independentes, cada uma das quais possuí um governo e afirma a sua soberania com relação a uma parte da superfície terrestre **(território)** e a um segmento da população humana **(povo)**" (BULL, 1977, p.13, grifo nosso).

Portanto, segurança passou a ser a palavra de ordem dos Estados e, aos poucos, as discussões sobre como proteger o Estado contra ameaças externas e internas surgiram, em especial, diante dos Estudos de Segurança Internacional (ESI) após a Segunda Guerra Mundial (BUZAN; HANSEN, 2012, p.33).

Nesse sentido, é mister ter em conta que o sistema internacional está sempre em constante mudança, agregando novas questões e excluindo outras, entre elas o surgimento de novos temas para além dos militares e de novos atores para além do Estado, afora o avanço da tecnologia e da crescente incidência de novas técnicas de informação e comunicação. Na medida em que novas ameaças advindas de diversas esferas de atuação – não mais somente do ator estatal – foram sendo reconhecidas, iniciou-se um debate a respeito da ampliação ou conservação da agenda de segurança, a qual inicialmente era predominantemente dominada pelo paradigma realista:

> "A análise da mudança do significado atribuído ao conceito de segurança parte, em primeiro lugar, do entendimento do texto maior em que se encontra tal conceito. Por sua vez, este texto maior é dado pela conotação conferida ao conceito pelo paradigma realista. A hegemonia desta perspectiva consolidou um entendimento do conceito de segurança relacionado e subordinado à lógica estatal. Remetia-se ao Estado, dizendo respeito apenas aos aspectos militares da segurança dessa entidade" (TANNO, 2003, p.8).

Iniciaram-se, então, questionamentos visando redefinir os limites teóricos da área de segurança por parte de críticos ao realismo, em especial da Escola de Copenhagen. Ou seja, o conceito de segurança utilizado em relações internacionais que se encontrava imbuído pelos preceitos realistas, ganhou outras questões a serem discutidas para além do militarismo.

A questão nuclear/energética obtém grande relevância internacional após a Segunda Guerra Mundial e durante a Guerra Fria, muito em conta pelo ineditismo das armas de destruição em massa. Na década de 1970, é a vez de o cenário

---

relacionado ao "poder ou alguma de suas expressões, como autoridade, governo ou soberania" (DALLARI, 1998, p.29).

econômico demandar sua inclusão no conceito de segurança, sobretudo devido aos dois choques do petróleo em vista de garantir as condições de desenvolvimento econômico dos países, especialmente do hemisfério sul.

A partir da década de 1980 tem-se a inclusão de variados temas transnacionais. Assim, assuntos ambientais e alimentícios ganharam espaço diante das preocupações com o processo de degradação ambiental e a fome, que atingiam diretamente a população de determinados Estados. Da mesma forma, o fim da Guerra Fria em 1991 e a Guerra Global contra o Terror (GGcT) iniciada em 2001 são marcos importantes para a redistribuição de forças no sistema internacional e, por conseguinte, para mudanças na agenda. Isso por que o pós-Guerra Fria apresenta uma mudança significativa no cenário estratégico no sentido de ampliar a acessibilidade a novas tecnologias militares. Ainda, preocupações com o tráfico de armas, drogas e pessoas, além da imigração e de doenças relacionadas à saúde, também ganharam relevância e passaram a ser tratados como ameaçadoras à segurança. Nesse sentido, variadas dimensões são abarcadas na agenda de segurança com diferentes graus de primazia.

O posicionamento da corrente realista, então, tornava insuficiente para o estudo dos novos fenômenos, abrindo possibilidades para discussões que visavam redefinir os estudos na área de segurança. A vertente teórica abrangente desses estudos, representada pela Escola de Copenhagen, em especial por Bary Buzan, propôs que nas análises, além dos aspectos militares, deveriam ser levados em conta aspectos econômicos, societais, políticos e ambientais (BUZAN, 1991, p. 19-20) e, mais tarde, de saúde, desenvolvimento e gênero (BUZAN; HANSEN, 2012, p.39), apoiadas também pelos Estudos Críticos de Segurança.

Assim, a abordagem construtivista iniciou seu questionamento às teorias mais tradicionais, através de uma crítica à centralização da segurança no nível militar e estatal, propondo-se uma análise multidimensional, expandindo seus setores. Dessa forma, a Escola possibilitou o alargamento do campo da segurança, fazendo surgir outras perspectivas teóricas e, ao mesmo tempo, instituiu um definido procedimento para a categorização e análise das questões relacionadas ao tema. A ampliação da agenda e a multiplicação de categorias/dimensões acarretaram também no maior envolvimento de atores não estatais de caráter transnacional, que podem ser tanto ameaçadores da segurança (como grupos armados ou associações

criminosas) como promotores (vide organizações internacionais e não governamentais).

A redefinição e o alargamento da agenda de segurança foram bastante polêmicos. No momento em que se consideram outros atores e surgem novas formas de ameaças não relacionadas ao militarismo, alguns autores, como Peter Hough (2004), consideram que a área da segurança incorporou temas excessivos. Assim sendo, questões que deveriam ser tratadas em âmbito político, são levadas para a esfera da segurança. No entanto, pode-se criticar a visão do autor, pois preocupar-se tão somente com questões militares na agenda de segurança torna-se demasiadamente simplista, na medida em que outras áreas e questões também podem ameaçar a sobrevivência e segurança do Estado – e, portanto, da sua sociedade. O que muda, então, é o grau de primazia de determinado tema, fazendo com que altere igualmente o tipo de resposta dada pelo Estado. Assim, a agenda de segurança torna-se geograficamente específica para cada realidade.

O fenômeno da segurança, portanto, ganhou complexidade adotando um tom multidimensional, misturando elementos de variada natureza – como ameaça e inimigos diversos – e de diferentes origens – como societais, econômicas, ambientais, energéticas e políticas. Nesse sentido, o advento e progresso da tecnologia – para fins do presente trabalho, a de comunicação e informação – deram um caráter ainda mais complexo a esse fenômeno. As novas Tecnologias da Informação e Comunicação (TICs) possibilitaram o encurtamento das distâncias territoriais e o surgimento de novas técnicas e, por conseguinte, novas ameaças. A Revolução da Informação[5] provocou um grande salto cientifico-tecnológico. As TICs, então, inserem-se como fator importante nesse efetivo processo evolucionário, haja vista que o contínuo desenvolvimento de novas tecnologias gera uma necessidade de estimar seus impactos nas relações estratégicas. Deste modo, “depois de chegar ao mundo, a tecnologia cria pressões por si só, as quais, mais uma vez, tem impacto sobre o processo político” (BUZAN; HANSEN, 2012, p.99).

Dessa forma, o Estado está cada vez mais dependente das novas TICs que impactam profundamente na organização política, econômica e militar de suas

[5]Nas palavras de NYE JR (2010, p.1, tradução nossa) “a atual revolução da informação, às vezes chamada de terceira revolução industrial, é baseada em rápidos avanços tecnológicos em computadores, comunicações e softwares, que por sua vez levaram a reduções dramáticas no custo de criação, processamento e transmissão de informações”. Ainda, segundo Cavalcanti (1995, p.1), a Revolução da Informação é a terceira grande mudança na história da humanidade, tendo como resultado o rápido avanço das tecnologias da informática e das telecomunicações.

instituições e sua sociedade, ocasionando não uma alteração fundamental na preponderância do Estado, mas sim na forma de se exercer poder (NYE JR. 2010). Nas palavras de Nye Jr:

> "Mudanças nas informações sempre tiveram um impacto importante sobre o poder, mas o domínio cibernético é tanto um novo como um volátil ambiente virtual. As características do ciberespaço reduzem alguns dos diferenciais de poder entre os atores e, portanto, são um bom exemplo da difusão do poder que caracteriza a política global neste século. [...] Mas o ciberespaço também ilustra o ponto de que a difusão do poder não significa igualdade de poder ou a substituição de governos como os atores mais poderosos da política mundial. Enquanto o ciberespaço pode criar algumas mudanças de poder entre os estados, abrindo oportunidades limitadas para pequenos estados através da guerra assimétrica, é pouco provável que seja uma virada de jogo nas transições de poder. Por outro lado, o domínio cibernético é susceptível de aumentar a difusão do poder de atores não-estatais e ilustra a importância das redes como uma dimensão chave de poder no século 21" (NYE JR. 2010, p.19, tradução nossa).

Dessa forma, percebem-se algumas mudanças analisadas pela literatura ocasionadas por essa Revolução da Informação, quais sejam: (i) a transformação da natureza do poder, passando a abarcar, por exemplo, o poder econômico e não somente militar e, ainda, nesse caso, o poder cibernético, tido como a "habilidade em usar o espaço cibernético para criar vantagens e influenciar eventos em outros ambientes operacionais e através dos instrumentos de poder" (KUEHL apud NYE JR, 2010, p.4, tradução nossa). Ainda, "pode ser usado para produzir resultados preferidos dentro do ciberespaço ou pode usar instrumentos virtuais para produzir resultados preferenciais em outros domínios fora do ciberespaço" (NYE JR, 2010, p.4, tradução nossa); (ii) a perda do posicionamento do Estado como único ente organizador da política internacional, surgindo mais espaço para atores não estatais e; (iii) a ampliação do número de ameaças, em sua grande maioria de caráter assimétrico.

A informatização da sociedade, portanto, esta cada vez mais complexa e globalizada, fazendo surgir novos conceitos, como são os casos da segurança cibernética e informacional, as quais se encontram cada vez mais presentes nas agendas dos Estados como novas formas de ameaça, na medida em que essa informatização da sociedade não veio acompanhada necessariamente por medidas de segurança adequadas (CLARKE; KNAKE, 2010). Ou seja, dependendo do grau de informatização das estruturas do Estado, a possibilidade de um ataque cibernético pode se tornar uma séria ameaça tanto em termos de defesa nacional quanto em termos de segurança da sociedade.

Apesar de recente, a internet já é considerada fundamental para o funcionamento das sociedades. Por ela, a troca de informações tornou-se mais rápida e eficiente. Encurtaram-se as distâncias entre os países, produzindo efeitos praticamente em todas as partes da sociedade e repercutindo nas esferas social, econômica, política e, inclusive, de segurança. Apesar de todas as benfeitorias, vantagens e oportunidades que a rede de internet oferece, ela também se sujeita a vulnerabilidades que podem ser usadas para ações ilegítimas e ataques cibernéticos (CANONGIA, MANDARINO JUNIOR, 2009, p.22).

Há um consenso entre autores de que a segurança cibernética é um conceito proveniente da agenda pós-Guerra Fria em função da combinação entre inovações tecnológicas e transformações nas condições geopolíticas (HANSEN; NISSEMBAUM, 2009, p.1155), e que a GGcT, após o 11 de setembro, potencializou o interesse nesse setor e elevou a preocupação a um nível novo e mais complexo (BUZAN; HANSEN, 2012, p. 345,373). Nesse sentido, esse espaço tem-se tornado um grande objeto de discussão política, às vezes visto como apenas um espaço de comunicação em si, outras vezes com um verdadeiro recurso de poder (FERREIRA NETO, 2013, p.74).

Por isso, existe uma real preocupação de que os conflitos nesse domínio estejam cada vez maiores na medida em que tanto os Estados quanto outros atores o desvendem, surgindo, então, como “uma área crítica para a segurança dos Estados e para o funcionamento das economias. [...] com grande probabilidade, será também um espaço de projeção de poder” (RODRIGUES, 2012, p.5). A segurança cibernética vem, dessa forma, tornando-se cada vez mais presente nas análises estratégicas de governo, sendo essencial para a manutenção, preservação e defesa das infraestruturas críticas de um país (CANONGIA; MANDARINO JUNIOR, 2009, p.25).

O campo de Estudos de Segurança Internacional está sempre em uma dinâmica de continuidade e permanências, readaptando-se a realidade de cada contexto histórico. O ciberespaço, então, que inclui informações sensíveis aos Estados e que pode ser ligado a infraestruturas críticas, apresenta-se como a realidade do momento em termos de segurança, mostrando-se como um ambiente fornecedor de vulnerabilidades e de possíveis vantagens ofensivas, seja por ataques

cibernéticos patrocinados por Estados, seja por criminosos comuns ou defensores de princípios políticos[6].

No campo militar, a preocupação decorre pelo fato de que os sistemas de comando/controle e os dados são informatizados, enquanto no campo civil, serviços de suma necessidade podem ser dependentes e vulneráveis a novas TICs. Portanto, o espaço cibernético, para além de facilitar as operações cotidianas do viver social, pode servir para efetuação de operações militares explorando seus recursos oferecidos, abrindo possibilidades para ações que visam coagir adversários e/ou ser alvo da prática de crimes. Conforme o Estado vai percebendo a importância da segurança cibernética, eleva-se sua institucionalização, alocação de capacidades e definição de conceitos de acordo com a sua percepção de ameaça. Nas palavras do então Ministro das Relações Exteriores do Brasil e atual Ministro da Defesa, Celso Amorim, percebe-se a adoção da segurança cibernética como uma ameaça da segurança internacional:

> "O monitoramento de dados e a guerra cibernética têm em comum o emprego de instrumentos de altíssima tecnologia para atividades que importam em graves violações de soberania. [...] O monitoramento e a guerra cibernética podem alvejar tanto países tidos como hostis ou como ameaças imediatas quanto países amigos e aliados. Não se pode excluir que o mesmo ocorra com ataques cibernéticos, provenientes de qualquer quadrante. Essas atividades ilustram em tons muito fortes alguns dos novos desafios da segurança internacional" (AMORIM, 2013, p.289).

O fato da sociedade, de mecanismos geradores de riqueza (bancos e empresas) e das infraestruturas críticas do Estado apresentar forte dependência às TICs, faz com que o espaço cibernético possa afetar decididamente o bem-estar, a segurança e os interesses nacionais. As sucessivas e recentes ocorrências intrusivas e ofensivas através da internet ou de instrumentos informáticos – os quais serão analisados em capítulo posterior – revela a importância do debate e reflexão sobre o desenvolvimento e a segurança nesse espaço, fornecendo assim novas potencialidades/vulnerabilidades estratégicas às nações.

O que se pretendeu abordar nesta seção introdutória foi que a percepção da segurança como especifica para cada realidade histórica e geográfica, acompanhada por um processo evolutivo dos temas da agenda de segurança, juntamente com o desenvolvimento das novas TICs – para fins do presente trabalho, a cibernética – permite inserir o setor cibernético não só como uma dimensão militar

[6] No último caso, a literatura tem denominado a prática de defender princípios políticos na internet como "hackativismo" (DUNN, 2010, p.1).

da política de defesa dos Estados, mas também como um setor peculiar de análise com seus objetos de referência, atores funcionais, atores de securitização e dinâmica de funcionamento próprios que serão melhor descritos posteriormente. Após esta explanação da evolução da agenda de segurança, o espaço, a segurança e a guerra cibernéticos – e seus conceitos – serão mais bem aprofundados no capítulo seguinte. Antes disso, é necessário tratar fundamentalmente da evolução do modo de fazer a Guerra, subtema que abordaremos nesta próxima seção.

2.2 A EVOLUÇÃO DO MODO DE FAZER A GUERRA

O campo das relações internacionais surge diante da necessidade de estudar o fenômeno da guerra. Na medida em que os diferentes conflitos interestatais ocorreram, os dispositivos utilizados e o modo de atuação também se desenvolveram. Assim, Clausewitz (1832) afirma que:

> "A guerra é essencialmente uma luta [...]. A luta, por sua vez, é um teste de forças morais e físicas [...]. A necessidade de lutar levou o homem rapidamente a inventar os dispositivos adequados para obter vantagens em combate, e esses dispositivos provocaram grandes mudanças na forma de lutar" (CLAUSEWITZ, 1832, p.137).

O que este subcapítulo propõe abordar é que as formas de guerra entre as nações acompanham um processo evolutivo, tanto em termos tático-estratégicos-instrumentais – separados por gerações – quanto em sua essencial natureza. As guerras tradicionais de Clausewitz (1832) e as novas guerras de Kaldor (1998, 2005) possuem natureza essencialmente distintas, mas notar-se-á que a guerra cibernética possui traços das duas naturezas. Constata-se, então, o surgimento de uma geração multidimensional que pode interligar o ciberespaço, em seu aspecto eletromagnético, com as ações militares habituais, servindo, igualmente, como um recurso alternativo ao uso da força propriamente dito. Nessa linha evolutiva de pensamento, as formas de guerrear são divididas em quatro distintas gerações, que serão abordados a seguir.

Primeiramente, é imprescindível entender que a "guerra é um ato de força para obrigar o nosso inimigo a fazer a nossa vontade" (CLAUSEWITZ, 1832, p.75). Para que esta vontade ocorra, é preciso desarmar/derrotar o inimigo, sendo este, para Clausewitz (1832), o objetivo primário da guerra. Ou seja, é preciso desarmar o adversário ao ponto de impedi-lo ou dificulta-lo em sua defesa e da possibilidade de um ataque imediato. O modelo clausewitziano da guerra (convencional/tradicional),

elaborado no livro Da Guerra (CLAUSEWITZ, 1832) é um modelo regular, em que os principais atores são os Estados, suas forças armadas e sua população. Caracteriza-se por uma sequência lógica bem determinada de início, meio e fim. Ou seja, normalmente é desencadeada por uma crise, seguida pela incapacidade de encontrar uma solução nas negociações diplomáticas, culminando em uma declaração formal de guerra. A guerra, nesse caso, surgirá sempre que existir uma situação política, derivando, então, de um motivo político. Para o autor, "a guerra é a continuação da política por outros meios" (CLAUSEWITZ, 1832, p.70). Portanto, ela não é somente um ato político, mas um instrumento político, uma realização das relações políticas por outros meios dentre as diversas possiblidades de resolver um conflito internacional – tais como diplomacia, negociação, barganha, bloqueio econômico e, finalmente, guerra[7].

Assim, a primeira geração caracteriza-se por batalhas formais em formação de campo ordenado, com táticas de linha e coluna, compreendida entre os anos de 1648 e 1860. Essa geração tem como maior exemplo o período napoleônico. Utilizavam-se estratégias bem determinadas e armas arcaicas. A cultura militar de ordem (uniformes, contingências, hierarquia) é produto dessa geração. Nesse caso, existia uma clara separação entre combatentes e civis, sendo o objetivo a rendição do inimigo e não sua aniquilação (LIND, 1989, p.23).

A partir de meados do século XIX, inicia-se o desordenamento dos conflitos com o surgimento de equipamentos de maior poder, como metralhadoras. Ainda que as guerras continuassem sendo travadas nos campos de batalha, o surgimento da Revolução Industrial e do desenvolvimento de armas de fogo atribuíram novas características aos conflitos, tendo-se, então, a segunda geração. Essa foi desenvolvida pelo exército francês, culminando na Primeira Guerra Mundial. Já não existe mais uma clara separação entre combatente e civil, aumentando o número de vítimas civis drasticamente. Há, ainda, uma bem determinada estratégia militar, com infantaria, carros de combate e artilharia agindo de maneira sincronizada (LIND, 1989, p.23).

[7]Ainda, para Clausewitz (1832), a guerra é um instrumento racional de política nacional. Racional, pois a tomada de decisão pela realização da guerra deve ser avaliada em termos de custo-benefício; Instrumental visto que deveria ser empreendida para fins de alcançar um objetivo e nunca pelo simples fato de guerrear e; Nacional porque a finalidade deve ser a satisfação dos interesses de um Estado nacional.

Em seguida, a guerra de terceira geração foi articulada pelo exército alemão, fruto do pós-primeira Guerra Mundial, também conhecida como guerra de manobra ou “blitzkrieg”, tendo-se como tradução do alemão “ataque-relâmpago”. Assim, baseia-se na surpresa e rapidez do ataque, transferindo-se a utilização tão somente do poder de fogo para uma combinação entre esse e a movimentação. Ocorrem mudanças nas táticas (agora, não linear) e no desenvolvimento dos transportes e armas (carro de combate, submarino, aviação, etc). É exemplificada pela Segunda Guerra Mundial, mostrando-se muito mais severa com os civis do que as anteriores, surgindo um temor psicológico para com a guerra (LIND, 1989, p.23).

Essas três gerações da guerra, que eram marcadas pela presença nítida do Estado-nação, das armas convencionais e cinéticas, sofrem algumas mudanças importantes a partir do fim da Segunda Guerra Mundial. Após 1945, não ocorreu nenhuma guerra direta entre as grandes potências. As etapas lógicas do modelo clausewitziano estavam deixando de ser bem definidas. Inicia-se, então, uma mudança na natureza e objetivos da guerra. Para Kaldor (1998), a globalização foi a grande responsável por essa transformação. Segundo a autora, o fenômeno complexo da globalização atinge as ações que se desenvolvem também no ambiente estratégico. Não só o campo de batalha se modificou como os atores envolvidos, os quais eram exclusivamente estatais e apoiados por seus exércitos, foram substituídos por grupos transnacionais, infraestaduais e também organizações internacionais.

No período que compreende a Guerra Fria os conflitos aconteceram nas zonas de influência dos interesses das grandes potências da época, quais sejam Estados Unidos e União Soviética, como a Guerra da Coréia (1950), as guerras entre árabes e israelitas no Oriente Médio, a Guerra do Vietnã (1964), a do Afeganistão (1979), entre outros. Assim, as grandes potências não conflitavam abertamente entre si, mas enfrentavam inimigos de menor capacidade militar ou influenciavam algum dos lados nos conflitos de menor escala. As guerras do Golfo também fazem parte dessa mudança, especialmente por terem introduzido a tecnologia da informação e comunicação no meio do combate (KIEVIT; MELTZ, 1995). Assim sendo, esse período tem uma característica peculiar conhecida como guerra por procuração, em que os Estados confrontam-se de forma indireta, apenas financiando e/ou influenciando doutrinariamente os lados do conflito.

Dessa forma, Kaldor (1998, 2005) afirma que as guerras tradicionais do século XVII a meados do século XX foram substituídas pelas chamadas novas guerras. Estas se encaixam no conceito de guerra irregular, sem frentes, sem campanhas, sem uniformes, sem limite territorial, de combatentes misturados com a população e de objetivos diversos. Não se pode mais determinar claramente onde começa e termina o conflito. Dessa maneira, surge um atributo assimétrico dos conflitos, em que os envolvidos apresentam significativas diferenças no tocante ao nível de organização, finalidades e recursos. Ainda, a sociedade passa a fazer parte da violência. Nas palavras da autora:

> "Estas são guerras travadas por redes estatais e não estatais, muitas vezes sem uniformes ou às vezes com sinais distintos. São guerras em que as batalhas são raras e a maior parte da violência é dirigida contra os civis. [...] São guerras em que as distinções entre combatentes e não-combatentes e a violência legítima estão desaparecendo" (KALDOR, 2005, p.3, tradução nossa).

Kaldor (1998), também, acredita que existem duas formas dominantes das novas guerras: a primeira é aquela a qual a autora foca sua análise, denominada guerras predatórias; a segunda é o que ela chama de alta tecnologia de guerras, mas não aborda profundamente. A primeira aproximação refere-se, sobretudo, acerca da identidade política, em que a luta pelo poder ocorre com base em valores exclusivos de grupos não estatais (como movimentos identitários étnicos, raciais ou religiosos, o crime organizado e grupos paramilitares), não havendo clara disputa geopolítica ou ideológica como nas guerras anteriores. Já a segunda aproximação tem como elemento central a tecnologia, especialmente a da informação, que possibilitou uma Revolução dos Assuntos Militares (RAM). A RAM, do inglês Revolution in Military Affairs (RMA), é um conceito relacionado ao futuro da guerra e leva em consideração o desenvolvimento de novas tecnologias que impactam no setor militar. Esse termo materializou-se na primeira Guerra do Golfo Pérsico (KIEVIT; MELTZ, 1995). Mais tarde, recebeu uma nova denominação: Guerra Rede-Cêntrica – do inglês Network Centric Warfare (NCW)[8]. Este último, além de incorporar novas tecnologias, provoca uma mudança no cumprimento das missões, na forma de organização e apoio efetivo aos combatentes, encorpando, então, novos conceitos, como os de Guerra Cibernética e Segurança da Informação.

[8]WILSON, Clay. Network Centric Warfare: Background and Oversight Issues for Congress. Congressional Research Service. 2004. Disponível em: http://www.fas.org/man/crs/RL32411.pdf; Acesso em 19 abr. 2014.

É importante ressaltar, também, que a mudança direta na natureza da guerra não fez com que as gerações mais tradicionais deixassem de existir integralmente. Seus elementos fundamentais são transmitidos de geração para geração, não entrando em desuso. Por exemplo, os exércitos e estratégias de combate continuaram sendo importantes e constantemente presentes para o sucesso no conflito, bem como a presença do Estado. O ponto principal a ser compreendido é que o avanço tecnológico e o surgimento de atores não estatais configuraram uma nova violência internacional, isto é, uma violência organizada global possibilitada pela globalização que transnacionalizou os conflitos, apresentando novos objetivos, atores, instrumentos e formas de fazer a guerra, inclusive, financiando-a.

Dentro desta lógica interpretativa, temos a quarta geração da guerra, a qual surge como mais complexa que as anteriores. Ela se desenvolve em congruência com o avanço nas TICs. As guerras dessa geração são acompanhadas pelo conceito de guerra assimétrica, irregular e não convencional. Estes conceitos fazem referência aos conflitos em que há prevalência da assimetria nos recursos utilizados, nas capacidades, nos atores, na estruturação, havendo, portanto, uma descaracterização do conflito convencional e exclusivamente entre Estados, utilizando-se, ainda, de armamentos não tradicionais.

Dessa forma, a quarta geração caracteriza-se por ser um conflito multidimensional[9], que envolve ação na terra, no mar, no ar, no ciberespaço (satélite e veículo não tripulado) e no espectro eletromagnético deste último (meio cibernético/eletrônico). Assim, o conflito multidimensional tem correlação com a assimetria no uso da força na medida em que os meios não convencionais, para fins do presente trabalho aqueles advindos do avanço das TICs, tornam-se importantes para alcançar uma vantagem estratégica com o intuito de contrabalancear os pontos fracos do atacante e tentar compensar a superioridade do adversário. Dessa forma, busca-se aumentar a vulnerabilidade do inimigo através de meios alternativos, até mesmo causando impacto físico e psicológico, sem necessariamente correr risco por uma represália, como é o caso dos ataques cibernéticos que serão vistos no próximo capítulo.

[9]Alguns doutrinadores consideram cinco gerações de guerra, separando esta quarta geração, considerando diferentes aquelas de manobras em terreno daquelas em campo informacional/eletromagnético. Este trabalho não acha necessária esta divisão, visto que por vezes uma pode substituir a outra, e outras vezes as duas podem ser utilizadas conjuntamente.

Nesse sentido, uma força reduzida no domínio cinético, mas bem treinada e avançada tecnologicamente no âmbito eletromagnético (cibernético) pode causar danos significativos em um adversário superior, tornando, então, este novo domínio um interessante novo recurso de poder. Além disso, ocorre uma descentralização da guerra, visto que o Estado perde o monopólio desta, não sendo a prática do conflito mais de exclusividade dele, tendo que se preocupar também com outros atores não estatais (LIND, 1989, p.24). Mas a guerra cibernética assimétrica, por exemplo, não precisa obrigatoriamente ser um recurso de um estado pouco poderoso, pequenos grupos ou indivíduos, mas também pode ser utilizado por Estados maiores, como a China, por exemplo, com a finalidade de compensar sua perda no campo militar convencional por outro Estado, como os EUA.

Conforme aponta LIND (1989, p.26), a quarta geração dos conflitos caracteriza-se como irregular, assimétrico e não convencional por apresentar particularidades como: (i) não linearidade; (ii) obscura distinção entre guerra e paz (não existe uma declaração formal de guerra, um inimigo bem determinado e caracterizado); (iii) não demarcação definida de fronts e campos de batalha (o adversário pode estar em todos os lugares e ao mesmo tempo em lugar algum); (iv) colapsar o inimigo é mais importante do que sua destruição física (torna-se mais eficaz e importante dificultar a transmissão de dados, informações e distribuição de energia elétrica por alguns dias, por exemplo) e, por último; (v) a incorporação de novas tecnologias (as quais modificam a dimensão do combate e a atuação dos combatentes).

Assim sendo, referente à última particularidade, é importante compreender que as armas empregadas e a forma de luta influenciam no modo de combater. Nas palavras de Clausewitz (1832):

> "A luta determinou a natureza das armas empregadas. Estas, por sua vez, influenciam o combate. Essencialmente, portanto, a arte da guerra é a arte de empregar em combate os meios que lhe forem atribuídos. A arte da guerra compreende todas as atividades que existem por causa da guerra, tais como a formação das forças combatentes, o seu recrutamento, armamento, equipamento e adestramento" (CLAUSEWITZ, 1832, p.137-8).

As TICs, então, tem papel fundamental no combate de quarta geração. As operações de informação e comunicação inserem-se nas atividades de guerra irregular, quais sejam, operações em rede computadorizada, guerra eletrônica (cibernética), simulação militar, operações de segurança e as operações psicológicas (KIEVIT; MELTZ, 1995, p.7). Nesse caso, a geração multidimensional

não deixa de utilizar métodos convencionais, mas ganha componentes militares não convencionais e indiretos, a fim de perturbar, fragilizar e exaurir o inimigo.

O amadurecimento científico-tecnológico-militar proporcionou uma mudança estratégica nas intervenções militares, a fim de não necessitar um deslocamento maciço de tropas e evitar o contato ou o movimento, mas também é importante salientar que a guerra assimétrica ou irregular poderá ocorrer, e, em regra, ocorre, concomitantemente, a uma guerra convencional. Ou seja, as ferramentas e instrumentos de cada tipo de guerra podem interagir e servir-se como auxiliares. É nesse contexto, então, de evolução das gerações da guerra, tendo-se como foco a tecnologia, que se acrescentam os conceitos de guerra e segurança cibernéticas. De fato, a natureza essencialmente tradicional clausewitziana do fenômeno da guerra evoluiu para uma natureza de guerra irregular, global, assimétrica e pautada, sobretudo, na tecnologia.

Ainda que Kaldor (1998) não tenha analisado detalhadamente as novas guerras baseadas no incremento tecnológico, alguns aspectos da guerra irregular podem ser notados na guerra cibernética, sobretudo no fato de não existir frentes combatentes, campanhas claras, exércitos uniformizados e bem determinados, em que muitas vezes os militares cibernéticos escondem-se no anonimato e são patrocinados/financiados pelos Estados, caracterizando uma nítida guerra por procuração. Assim sendo, há uma mistura entre atores estatais e não estatais, e a violência é dirigida para infraestruturas críticas do Estado que podem afetar diretamente a sociedade, tal qual é afetada pelas novas guerras. Da mesma forma, os ataques cibernéticos podem ocorrer a qualquer momento, não existindo mais a clara distinção entre onde começa e onde termina o conflito. A natureza kaldoriana da guerra, então, possuí traços na guerra cibernética na medida em que esta se configura também por se tratar de um conflito de caráter transnacional e globalizado com características similares.

Por outro lado, percebe-se que a guerra cibernética também não deixou de ser um instrumento racional de política nacional em determinados casos. Ainda que a participação estatal não seja clara em muitas ocasiões, é possível designar a responsabilidade direta ou indireta de governos nos ataques cibernéticos ocorridos até então. Além do mais, a guerra cibernética pode ter como um de seus propósitos, ainda, tornar o inimigo militarmente impotente, facilitando uma intervenção militar convencional no território inimigo, possuindo, portanto, traços da natureza

clausewitziana da guerra no que concerne em desarmar o adversário ao ponto de impedi-lo ou dificulta-lo em sua defesa ou da possibilidade de um ataque e até mesmo para forçar o inimigo a fazer a sua vontade. De tal modo, o uso das armas cibernéticas serviria para alcançar fins que dificilmente seriam obtidos por outros meios.

Enfim, se nas sociedades agrárias o primeiro objetivo tático era tomar a posse da terra; nas sociedades industriais era prejudicar a capacidade de produção; na era das armas convencionais era derrotar o inimigo ocupando seu território, tomando seu governo e seus recursos econômicos; na era da informação o fim primordial é destruir os sistemas de informação do adversário: os bancos e os serviços financeiros, os sistemas de controle de tráfego aéreo, de distribuição de energia elétrica, de abastecimento de gás e petróleo, de transporte, de redes de telefonia, os serviços de emergências, entre outros; mas sem perder também traços característicos dos objetivos tradicionais, como enfraquecer as forças adversárias e faze-las submeter-se a sua vontade. Assim, a intenção é imobilizar, controlar, fragilizar, alterar e moldar o adversário e o seu comportamento.

Ademais, no tocante especificamente a guerra cibernética, esta ainda possui traços característicos peculiares, como veremos no capítulo seguinte. Assim sendo, é no sentido de surgir como um setor próprio de preocupação em segurança e de um novo domínio do conflito que a cibernética implica na importância de uma política de segurança e defesa próprios. Até mesmo porque a maior preocupação quanto a reações negativas da opinião pública, haja vista que a guerra tradicional é cada vez mais depreciada moralmente, faz com que outras maneiras de guerrear sejam criadas e utilizadas, sendo a cibernética uma dessas possibilidades. Feita essa abordagem sobre a evolução das formas de fazer a guerra, cabe agora tratar sobre a teoria de securitização de Waever (1995) e a inserção da cibernética nessa conjetura.

2.3 A TEORIA DE SECURITIZAÇÃO

Conquanto o presente trabalho não tenha a intenção de revisar a teoria, dispensando, assim, os prefácios das teorias das relações internacionais, faz-se importante demarcar algumas premissas teóricas para que possamos, mais a frente, relaciona-las com o tema central de pesquisa.

Os realistas definem o sistema internacional como anárquico, condicionado pela incessante busca pela aquisição de poder pelos Estados, reafirmando a priorização da segurança militar na política internacional. Nesse sentido, os realistas enxergam a segurança como um seguimento do poder, em que um ator alcança sua segurança quando ocupa uma posição dominante. Dessa maneira, essa anarquia caracteriza-se pela inexistência de um formulador de política internacional que seja independente e soberano, acima do nível estatal. Portanto, a visão predominante do conceito de segurança realista está ligada ao poder de cada nação para assegurar a sua sobrevivência.

Apesar de o construtivismo considerar a anarquia como construída socialmente, sendo ela o que os Estados fazem dela, e, portanto, diferenciar-se da visão realista nesse ponto, no que tange a segurança internacional, ambas se aproximam na medida em que tem o Estado como privilegiada unidade na estrutura política internacional. Mas a questão central para o trabalho é o fato de o construtivismo priorizar a interpretação e, portanto, a formulação da realidade. Nesse sentido, as crenças dos atores conformam suas identidades, que, por sua vez, moldam os interesses, caracterizando uma dinâmica de transformações. Assim, cria-se a ideia de que a realidade é socialmente construída, em que suas estruturas são formadas por ideias compartilhadas (WENDT, 1992).

Portanto, o conhecimento não é limitado, ele sofre continuamente processos de construção e reconstrução, abrindo espaço para a permanente possibilidade de transformação. No que se referem ao campo da segurança, as possíveis mudanças sistêmicas acontecem sempre relacionadas ao Estado. Assim sendo, o construtivismo possui uma maior abertura empírica que possibilita maior moldagem para tratar também de questões relacionadas às percepções de ameaça à segurança. Essas percepções, então, são construídas a partir de estímulos externos.

Diante dos questionamentos sob os temas na agenda de segurança internacional por ser inicialmente relacionada apenas ao tema militar, fez-se necessário criar conceitos e categorizações específicas para acompanhar a maior demanda de diferentes temas que foram incluídos nas agendas estratégicas dos Estados e que possuem especificidades para cada um deles. Assim, Waever (1995) desenvolveu a teoria da securitização, a qual se refere ao processo de apresentar uma questão em termos de segurança. Dessa forma, a dinâmica de cada uma das categorias/setores de segurança separadas primeiramente por Barry Buzan – quais

sejam militar, ambiental, societal, econômico e político – é determinada por objetos de referência, atores funcionais, atores de securitização e dinâmica de funcionamento particulares.

Os setores para securitização seriam como espécies de lentes pelas quais questões são observadas, em que o analista deve ter consciência de que cada setor esta embutido de valores e características próprios, que a natureza das ameaças modifica-se de setor para setor e que a securitização pode ser institucional ou *ad hoc* (BUZAN et al, 1998, p.27). Nas palavras dos autores, "a definição exata e os critérios de securitização são constituídos pelo estabelecimento intersubjetivo de uma ameaça existencial com uma saliência suficiente para ter efeitos políticos substanciais" (BUZAN et al, 1998, p.25, tradução nossa).

No que se refere aos objetos, Waever (1995) afirma que qualquer grupo ou indivíduo pode virar um objeto referente caso tenha sua segurança/existência ameaçada. Mas para que uma ameaça torne-se um problema de segurança na agenda política, é preciso que "um representante estatal declare uma condição de emergência, reivindicando o direito de utilizar quaisquer meios necessários para barrar um desenvolvimento ameaçador" (BUZAN et al, 1998, p.21, tradução nossa). Ou seja, a segurança é vista como "um discurso por meio do qual as identidades e as ameaças são constituídas em vez de ser uma condição objetiva" (BUZAN; HANSEN, 2012, p.366). Por sua vez, ator de securitização é aquele que securitiza uma questão declarando que o objeto de referência encontra-se ameaçado. E, por fim, ator funcional é aquele que afeta a dinâmica do setor em que faz parte.

Dessa forma, enquadra-se a segurança como um tipo especial de política, definindo a abrangência de questões públicas em três categorias, quais sejam, não politizado, politizado e securitizado. Buzan et al (1998, p.23) afirmam que a primeira acontece quando o Estado não lida e não faz da questão um assunto de debate público e de decisão e, portanto, não requer atenção nem ao nível político nem ao nível de segurança; a segunda ocorre quando o assunto torna-se parte de políticas públicas, exigindo decisão governamental e alocação de recursos; até chegar à última, significando que a questão é vista como uma ameaça existente, necessitando medidas de emergência aceleradas, podendo violar regras legais e sociais, sendo, assim, uma versão mais extremada da politização.

Nesse sentido, é importante ressaltar que se deve entender o conceito de ameaça como "qualquer acontecimento ou ação (em curso ou previsível) que

contraria a consecução de um objetivo e que pode ser causador de danos, materiais ou morais [para algum objeto], podendo ser de variada natureza" (COUTO, 1988, p. 329). Logo, os teóricos da Escola de Copenhagen veem a segurança como uma questão de sobrevivência e, portanto, quando existir qualquer preocupação, esta será definida como sendo uma ameaça existencial, não necessariamente porque ela existe, mas sim porque é apresentada como tal para algum objeto referente, podendo ser, tradicionalmente, mas não obrigatoriamente, o Estado, incorporando o governo, o território e a sociedade.

Assim, percebe-se que a corrente abrangente dos estudos estratégicos define a ameaça com a possibilidade de vir de fora da unidade de análise mais aceita nas relações internacionais – o Estado – e, apesar de expandir os temas ameaçadores para além do militarismo, essa perspectiva não se difere da visão realista, pois mantêm a lógica segurança-sobrevivência. Mesmo que nem sempre a ameaça seja proveniente de um Estado Nacional devido à expansão de atores, conceitos e temas, é impossível deixa-lo de lado como objeto de referência e unidade de análise chaves, isso por que "todos os debates sobre o que pode ser a segurança e para quem ela deveria ser orientada giram em torno deste [do Estado]" (BUZAN; HANSEN, 2012, p.52).

É fundamental ter em conta, ainda, que sempre que se falar a respeito desse tópico estará sendo falado sobre ameaças. Por isso, vale-se ressaltar uma das quatro questões que orientam os ESI e que ajuda a compreender também a dinâmica do campo da segurança, qual seja, a visão das "ameaças, perigos e urgências como diretamente ligadas à segurança" (BUZAN e HANSEN, 2012, p. 36). Assim, como podemos definir a agenda de segurança de um Estado? Na verdade, suas diretrizes serão diversas de acordo com as condições de cada Estado e o que é visto como ameaça para seus objetos referentes. Além disso, Buzan et al (1998, p.21) afirmam que a definição de uma ameaça justifica o uso de medidas extraordinárias a fim de lidar com ela. Por esse motivo, "a invocação da segurança tem sido a chave para a legitimação do uso da força, pois ela tem servido como a forma do Estado mobilizar ou invocar poderes especiais a fim de lidar com uma ameaça existente, real ou não" (RUDZIT, 2005, p.308).

No que tange a segurança cibernética, para as análises a serem feitas no presente trabalho, pode-se afirmar que os atores de securitização são os Estados – em especial, os governos – visto que estes se utilizam do discurso e da produção

legislativa interna e externa – além da maior alocação de recursos que antes eram inexpressivos –, para colocar esse tema no nível politizado e securitizado. Em notícia publicada no jornal "*The New York Times",* o presidente dos EUA, Barack Obama, no Congresso, em 12 de fevereiro de 2013, demonstrou preocupação com os possíveis ataques cibernéticos, afirmando: "agora nossos inimigos também estão buscando a capacidade de sabotar nossa rede elétrica, as nossas instituições financeiras, e os nossos sistemas de controle de tráfego aéreo"[10]. Portanto, percebe-se que o discurso em direção à politização e securitização do setor cibernético já teve início, nesse caso, pela maior potência do sistema internacional.

Da mesma forma, o "Manual Tallin" (SCHMITT, 2013) – que leva o nome da capital da Estônia –, elaborado a pedido do Centro de Defesa Cibernética da Organização do Tratado do Atlântico Norte (OTAN), mesmo não sendo documento oficial ou político da organização, é um exemplo relevante por ser uma tentativa de enquadramento dos conflitos cibernéticos no Direito Internacional. Mas, em especial por, em seu artigo 22, abrir a possibilidade de resposta proporcional a um ataque cibernético, nesse caso, sem uso da força. No entanto, se por ventura, ocorrerem mortes ou significativos danos ao Estado tem-se o pressuposto de uma contramedida em nível militar propriamente dito[11]. Nesse contexto, percebe-se uma das premissas da teoria da securitização na qual um ataque cibernético pode vir a ser uma ameaça e, por isso, assegura-se a justificativa para utilização de medidas extraordinárias e, portanto, a legitimação do uso da força.

Então, finaliza-se este capítulo buscando relacionar a cibersegurança com a teoria de securitização apresentada. No entanto, a segurança cibernética não é tratada especificamente por Buzan e Waever, mas alguns autores como Nissenbaum (2005) e Hansen e Nissenbaum (2009) aplicam a teoria desenvolvida pela Escola de Copenhagen a esse setor, propondo, inclusive, a adesão da cibernética como um setor particular de análise, não sendo incluída em outra

[10]SCHMIDT, Michael S.; PERLROTH, Nicole. Obama order gives firms cyberthreat information. *New York Times.* p.A16. Fev. 2013. Tradução nossa. Disponível em: http://www.nytimes.com/2013/02/13/us/executive-order-on-cybersecurity-is-issued.html?_r=0. Acesso em: 14 jan. 2014.

[11]Conforme o artigo 22 do Manual: "An international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations" (SCHMITT, 2013, p.71). Um comentário anexado acrescenta: "To date, no international armed conflict has been publicly characterised as having been solely precipitated in cyberspace. Nevertheless, the international group of experts unanimously concluded that cyber operations alone might have the potential to cross the threshold of international armed conflict" (SCHMITT, 2013, p.75).

categoria já teorizada pela Escola, haja vista a importância que a cibersegurança adquiriu no cenário recente de segurança internacional.

Buscando desenvolver seu argumento, as autoras delineiam “três modalidades de segurança que são específicas para o setor cibernético” (HANSEN; NISSENBAUM, 2009, p.1163, tradução nossa) e que se pode fazer referência às três categorias da teoria de securitização dos autores da Escola de Copenhagen, quais sejam, (i) hipersecuritização (securitizado), (ii) práticas de segurança diárias (politizado), (iii) tecnificações (não politizado).

A primeira coloca o tema como uma ameaça existencial devido aos possíveis danos que um ataque cibernético pode causar em âmbito social, econômico e militar, destacando que a velocidade desses ataques podem causar efeitos em cascata trazendo os objetos de referência desses respectivos setores. A segunda faz referência aos discursos que se direcionam para a segurança cibernética do cidadão comum, como e-mail, internet Bank, sites maliciosos, etc., e que servem para conseguir a legitimação da população e a aceitação pública. Dessa forma, a hipersecuritização tornar-se-ia mais aceitável em virtude da associação entre possíveis ataques cibernéticos de grande escala com as ocorridas no cotidiano. A última faz referência a um nível técnico de análise, a qual não é politizada (ou despolitizada), colocando as ameaças cibernéticas como hipotéticas e especulativas, rechaçando as habilidades do pesquisador de Segurança Internacional para tratar dessa área e restringindo a opinião para especialistas em informática (HANSEN; NISSENBAUM, 2009, 1163-1168).

Assim, a securitização do setor cibernético tem gerado grande polêmica entre especialistas de setores estratégicos e de técnicos em informática. Enquanto os primeiros veem o ciberespaço como uma fonte de insegurança internacional e um novo possível domínio para uma guerra, os últimos afirmam que essas preocupações não passam de “uma fantasia hollywoodiana com bases na cultura conservadora estadunidense de desconfiança a inovações” e que foi “gradualmente alimentada como uma ameaça militar considerável, numa ficção [...] em total dissonância com a realidade da segurança digital” (CARREIRO, 2012. p.137). Até mesmo os ESI afirmam que a segurança em informática carece “do drama e da urgência da segurança nacional/internacional, que lidam com [...] ameaças técnicas, e não político-militares” (BUZAN; HANSEN, 2012, p.43). Mas apesar desse aspecto não politizado do setor cibernético, quer possam ser exageros quer sejam mesmo

uma realidade, as ameaças cibernéticas ganharam uma importância relevante no pensamento de segurança, sobretudo no pós-Guerra Fria e, particularmente, entre os analistas e os formuladores de políticas de segurança e defesa.

Como prova disso, para satisfazer a necessidade de proteger o espaço cibernético e também controla-lo para usos ofensivos em um contexto militar, vários Estados publicaram estratégias para operações no ciberespaço e para segurança cibernética. É o caso dos EUA[12], da França[13], da Suíça[14], Reino Unido[15], entre outros. Da mesma maneira, foram e ainda estão sendo criados centros de unidades de defesa cibernética, como foi o caso da OTAN em 2008[16], da China (KLIMBURG, 2011, p.46), da Alemanha[17], do Comando de Defesa Cibernética (CDCiber) no Brasil[18] e, entre outros, dos EUA[19]. Assim, de "um assunto abordado por órgãos de segurança institucional e pública, a cibernética atingiu o status de segurança política e militar, tendo em vista as possibilidades de seu uso" (FERREIRA NETO, 2012, p.141). Portanto, conforme a construção de Weaver (1995) e Buzan et al (1998) apresentada, o tema passou de não politizado para politizado em alguns casos e securitizado em outros, sendo vista como uma ameaça extrema pelos Estados, haja visto que a sociedade e os sistemas militares são, atualmente, extremamente dependentes da utilização desse espaço e de suas tecnologias.

Enfim, após abordar neste capítulo a evolução dos temas na agenda de segurança com base em teóricos abrangentes da Escola de Copenhagen, tentando demonstrar a percepção da segurança como particular para cada realidade,

---

[12]A estratégia estadunidense para o ciberespaço foi criado em 2011, e pode ser visualizado no endereço: http://www.defense.gov/news/d20110714cyber.pdf. Acesso em 17 abr. 2014

[13]A estratégia francesa, também publicada em 2011, pode ser verificada em: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf. Acesso em 17 mai. 2014.

[14]A estratégia de proteção contra cyber riscos da Suíça foi publicada em 2012, disponível em: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Switzerlands_Cyber_Security_strategy.pdf. Acesso em 17 mai. 2014.

[15]Disponível em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf. Acesso em 17 mai. 2014.

[16]Ver site da organização em: https://www.ccdcoe.org/.

[17]FARIVAR, Cyrus. German cyber-defense center to launch in 2011. *DW*. Dez. 2010. Disponível em: http://www.dw.de/german-cyber-defense-center-to-launch-in-2011/a-14740503. Acesso em 17 mai. 2014.

[18]Ver a Portaria de criação do Centro de Defesa Cibernético brasileiro, nº 667, de 4 de agosto de 2010. Também, pode-se acessar o website do Centro em: http://www.dct.eb.mil.br/index.php/2013-02-01-13-23-38. Acesso em 14 mai. 2014.

[19]Este, uma das figuras mais importantes das novas unidades dedicadas a dimensão cibernética dos conflitos. Ver website da organização em: http://www.arcyber.army.mil/org-uscc.html. Acesso em 15 mai. 2014.

podendo inserir o setor cibernético como um assunto particular de análise, principalmente devido ao desenvolvimento e surgimento das novas TICs; depois de tratar do processo também evolucionário das gerações da guerra e da natureza desta, procurando descrever o surgimento de uma geração multidimensional e buscando relacionar a guerra cibernética com os modelos clausewitziano e kaldoriano, descreveram-se os preceitos construtivistas dando maior importância à teoria de securitização de Waever (1995), relacionando esta com a securitização do setor cibernético. Assim sendo, no próximo capítulo, faz-se necessário apresentar os conceitos e características basilares relacionados ao meio cibernético, delineando explicações que permitem tomar a guerra cibernética como uma realidade em construção, ganhando importância no cenário internacional. Ainda, serão feitas algumas observações de casos que permitem afirmar este setor como um novo e integrado domínio de conflito.

3 A REALIDADE DA GUERRA CIBERNÉTICA

Após se verificar a evolução dos temas na agenda de segurança internacional e da forma e natureza da guerra, além da apresentação da teoria de securitização relacionando-a com a cibernética, analisando-a como um tema securitizado, os atores estatais, ainda que com níveis de prioridade diversos, vêm se preparando para atuar nesse domínio, considerando-o como um novo recurso de poder. Assim, faz-se necessário abordar neste capítulo o espaço cibernético mais detalhadamente. Dessa forma, inicialmente, serão apresentados os conceitos basilares e os componentes relacionados a esse meio. Em seguida, apresentar-se-ão as características da ciberguerra e também uma análise de como ela pode se manifestar e já se manifesta no cenário internacional, delimitando explicações do porque podemos falar em guerra cibernética. Por último, uma análise de casos em que a cibernética é tida como um novo e integrado domínio de conflito.

3.1 CONCEITOS E COMPONENTES CIBERNÉTICOS

A busca da definição da cibernética e seus elementos que atendam aos objetivos deste trabalho visa delimitar sobre a possibilidade deste meio tornar-se um novo campo de conflito e um setor securitizado. Está fora do alcance deste trabalho, portanto, examinar definições tecnicamente complexas sobre o seu funcionamento, as quais ultrapassariam o conhecimento requerido por um analista de relações internacionais. Assim sendo, no intuito de alcançar esse objetivo primordial supracitado, é necessário antes apresentar brevemente a internet.

Primeiramente, os meios de comunicação e informação são fatores potencializadores para avanços nos mais diversos campos do conhecimento. Para fins deste estudo, a internet não pode se restringir tão somente aos seus aspectos puramente técnicos, devendo ser levado em consideração a interação da tecnologia com a sociedade, com as infraestruturas dos Estados e com o aparato militar. É importante lembrar, então, que, historicamente, a tecnologia em geral possuí um caráter de "dupla utilização"[20], ou seja, há uma interação entre a utilização de um meio de forma civil e de maneira militar. É o caso da internet, que foi "desenvolvida primeiramente como uma tecnologia militar, como uma rede distribuída para transmitir informações sob um ataque nuclear" (BUZAN; HANSEN, 2012, p.98) e,

[20]Buzan; Hansen (2012), p.98.

posteriormente, ganhou força na sociedade como ferramenta indispensável de busca por informação e meio de comunicação, tornando-se um recurso revolucionário no mundo moderno.

No início da década de 1990 havia apenas um milhão de usuários na internet e, dentro de quinze anos, esse número alcançou um bilhão (STARR *apud* NYE JR., 2010, p.3). Já em 2012, esse número aumentou ainda mais, alcançando dois bilhões de usuários no mundo, um crescimento de cerca de 200% em sete anos[21]. Assim sendo, o tráfego de internet e seus usuários estão acendendo cada vez mais rapidamente. Dessa forma, a internet tornou-se, ao final do século passado, a rede das redes. Mas ainda que esse crescimento seja "louvável por razões econômicas, ele também traz riscos, sobretudo para atores maliciosos", os quais lançam "ataques virtuais, escondendo suas identidades e protegendo-se atrás de estruturas sociais e governamentais" (CORNISH et al., 2010, p.18, tradução nossa). Por isso, a quantidade de ataques a sistemas de computadores governamentais por meio da internet ou por dispositivos de computadores[22] ganharam espaço na cena internacional, entre outros exemplos:

> "Em abril de 2007, foram divulgados ataques maciços a instituições públicas e privadas da Estônia; em agosto de 2008, ocorreram ações cibernéticas em setores estratégicos da Geórgia; em 2010, foram noticiadas ações nos complexos industriais da China, da Indonésia e do Irã – incluindo neste seu setor nuclear –, e, recentemente, tornou-se público o caso WikiLeaks que divulgou cerca de 250.000 mensagens confidenciais envolvendo o governo dos Estados Unidos da América. Em 2011, empresas brasileiras, como a Petrobras, e até a Administração Pública Federal (APF), pelo website da Presidência da República, sofreram alguma forma de tentativa de intrusão, com ou sem êxito" (FERREIRA NETO, 2013, p. 80).

O sentido do termo cibernética, que servirá neste trabalho, refere-se, de maneira ampla, "sobre o controle e a comunicação por meio de uma máquina processadora de mensagem: o computador" (FERREIRA NETO, 2013, p.80). Com o surgimento das redes de computadores, incluindo, então, a internet, o termo adquiriu a conotação de sistemas de informação interligados. Dessa maneira, o espaço

[21]Dados retirados do Internet World Stats, disponível em http://www.internetworldstats.com. Acesso em 12 jan. 2014.

[22]Nesse caso, deve-se levar em consideração que o ciberespaço inclui outras redes/componentes de computadores além da internet, que, supostamente, não são acessíveis a partir desta (CLARKE; KNAKE, 2010). É o caso do worm ("verme") *Stuxnet,* que em 2010 atingiu e danificou centrífugas nucleares iranianas. No entanto, o programa viral não foi propagado por meio da internet, mas sim por *pendrives* contaminados, haja vista que as centrifugas não tinham conectividade com a rede externa. Inicialmente o ataque foi atribuído aos EUA e Israel, mas suas participações nunca foram completamente comprovadas, como veremos detalhadamente mais adiante.

cibernético é designado como “o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores” (LEVY, 1995, p.95), formando, assim, uma sociedade internacional em rede, com características específicas e diferentes das outras dimensões, “como a interação com os diversos domínios; a velocidade de ações e de mudanças; a transcendência de fronteiras físicas, organizacionais, institucionais e geopolíticas; o anonimato e a possível diminuição da assimetria” (FERREIRA NETO, 2013, p.76).

Por uma definição mais clara, "o ciberespaço é um domínio operacional enquadrado por uso da eletrônica para [...] explorar a informação através de sistemas interligados e as respectivas infraestruturas associadas" (KUEHL apud NYE JR., 2010, p.3, tradução nossa), podendo compreender também “as pessoas, as empresas e os equipamentos que por ventura estejam interconectados, participando, de alguma maneira, do tráfego de informações digitalizadas” (FERREIRA NETO, 2013, p.87).

Portanto, o mundo cibernético é uma realidade virtual compreendida num conjunto de computadores e redes. Difere-se do mundo concreto, em que “os governos têm o monopólio do uso da força, o agredido conhece o terreno de combate e as ofensivas terminam com a deserção ou exaustão” (NYE JR, 2010, p.5, tradução nossa). A guerra cinética, tal qual conhecemos, é determinada como sendo a guerra do mundo real, em que tanques, navios, aviões e soldados tradicionais são seus figurantes. No mundo virtual, pelo contrário, “os envolvidos são diversos e muitas vezes anônimos, a distância física é irrelevante e as formas de ataque são relativamente baratas” (NYE JR, 2010, p.5, tradução nossa).

Nesse sentido, as formas possíveis de crime/conflito no ciberespaço são categorizadas de diversas maneiras. Essa tipificação varia conforme o autor, mas para fins do presente trabalho, será adotada a de Dunn (2010, p.3), por ser vista como a mais completa e bem determinada entre as encontradas. A autora separa os conflitos cibernéticos conforme uma escada[23] de gravidade dos danos, quais sejam, em ordem crescente, cibervandalismo, crime de internet, ciberespionagem, ciberterrorismo e, por fim, guerra cibernética. Nesse caso, o presente capítulo não tem por intenção pesquisar a fundo os quatro primeiros degraus, podendo em alguns

[23]Dunn (2010, p.3) nomeia essa categorização de “Cyberladder”, tendo a tradução deste que escreve como cyberescada.

casos cita-los indiretamente e simplificadamente, mas tem sim por objetivo se preocupar com o último nível.

A principal diferença entre eles habita na procedência e na finalidade do agente: enquanto as primeiras podem sugerir conflitos no campo privado e de caráter particular, a última refere-se necessariamente a relações de poder entre Estados ou, ao menos, a ações advindas de um indivíduo ou grupo com existência de patrocínio estatal, caracterizando uma guerra por procuração. Por assim sendo, existem dois diferentes tipos de agentes no ciberespaço, os crackers – aqueles com intenção criminosa comum – e os hackers – considerados ativistas e soldados do Estado. Para que ocorra uma guerra cibernética, então, é necessária a existência de participação ou patrocínio estatal, ou seja, ações oriundas de um indivíduo com motivações pessoais não se adequam a esse derradeiro degrau.

Sob um ponto de vista realista, o ciberespaço pode ser visto como um domínio operacional novo em que a atuação dos Estados estaria projetada no sentido de adquirir mais poder e influência. Nesse sentido, Clarke e Knake (2010) centram suas análises nas capacidades cibernéticas dos Estados, que buscam constantemente a maximização de seus interesses também nesse domínio, e, para os autores, guerra cibernética refere-se sinteticamente a "ações de Estados-nação para penetrar computadores de outros Estados ou redes de computadores com o propósito de causar danos ou interrupções" (CLARKE; KNAKE, 2010, p.6, tradução nossa). De uma forma mais completa, os autores definem ciberguerra como:

> "Uma invasão não autorizada – por, por meio de ou por apoio de um governo – a um computador ou rede de computadores de outra nação, ou qualquer outra atividade que afete um sistema computacional, no qual o propósito é adicionar, alterar ou falsificar dados, causar interrupção ou dano a um computador, rede de serviço ou objetos controlados por um sistema de computadores" (CLARKE; KNAKE, 2010, p. 228, tradução nossa).

Nesse caso, percebe-se que os autores colocam em sua definição o Estado como a principal unidade de análise, compartilhando com a categorização apresentada de Dunn de que a guerra cibernética é caracterizada pela participação direta ou indireta destes.

Ainda, segundo Nye Jr. (2012), alguns autores utilizam uma definição limitada para o termo, qual seja, "uma guerra sem sangue entre Estados que consiste unicamente num conflito eletrônico no espaço virtual". No entanto, essa definição mostra-se equivocada na medida em que não leva em consideração a interconexão entre mundo virtual e físico. Nesse sentido, como mostrarão casos que

serão analisados na última seção deste capítulo, “os ataques cibernéticos podem ter consequências físicas muito reais” (NYE JR., 2010, p.6, tradução nossa).

Assim sendo, uma definição mais prática para guerra cibernética seria “uma ação hostil no ciberespaço cujos efeitos ampliam ou são equivalentes a uma violência física” (NYE JR. 2012). Por último e como melhor entendimento, ciberguerra pode ser definida como:

> “um conjunto de rede de computadores (ou sistemas) de ataque e defesa, em que um ataque é considerado bem sucedido quando o uso dos sistemas pelo alvo é prejudicado, seja por falha na sua operação, seja por funcionar produzindo erros” (LIBICKI, 2009, p. 2, tradução nossa).

Por sua vez, o termo ataque cibernético é definido simplesmente como “os ataques no ciberespaço” (VENTRE, 2012, p. 35, tradução nossa), constituído por uma ampla variedade de ações, que vão de simples tentativas para apagar dados até danos a websites, negação de serviço, espionagem e destruição de sistemas e/ou infraestruturas críticas (NYE JR., 2012). No entanto, não devem se confundir com o conceito de guerra cibernética. Este envolve um ato de guerra a partir de ataques cibernéticos, enquanto o ataque cibernético tão somente utilizado pode ter gravidade de danos menores e ser praticado por hackers e crackers independentes.

As armas que podem ser utilizadas numa guerra cibernética são diversas. As possíveis medidas ofensivas são detalhadas por Lionel Alford (2000, p.113-116), podendo ser programas de quebra de senha, de observação (espionagem), de obtenção de informação, de ataque direcionado para um sistema específico, de comportamento virulento (vírus/malwares/cavalos de Tróia), de sobrecarga do sistema; fornecimento de endereços de internet falsos; manipulação direta de dados; e, enfim, bombas lógicas (sequências de códigos específicos em arquivos de dados que manipulam os programas que acessam estes arquivos ou as instruções do processador do sistema).

Exemplificando melhor esse arsenal cibernético, tem-se que as bombas lógicas funcionam como dispositivos adormecidos em programas de sistemas críticos, instalados prontos para serem ativados em circunstâncias pré-determinadas. Outro recurso disponível, o chamado cavalo de Tróia, possui um comportamento virulento o qual pode ficar invisível até que deva executar um comando em resposta a uma determinada circunstância. Essas e outras ações podem levar o sistema alvo ao colapso, causando a destruição física de equipamentos como turbinas, reatores, válvulas, etc.

Ainda, pode-se ter como alvo o sistema bancário de um país, através de, por exemplo, um ataque simultâneo de negação de serviço (distributed denial of service attack – DDOS), em que se bombardeiam interfaces eletrônicas de acesso aos recursos bancários, gerando inúmeros acessos falsos simultâneos que congestionam o sistema tornando-o inutilizável. O mesmo pode ocorrer com qualquer acesso a website de um país. Vale ressaltar que na medida em que um sistema bancário colapsa, suas consequências podem estender-se para outros países como um efeito cascata.

Com relação às vulnerabilidades, Lionel Alford (2000) afirma que é preciso ter em mente que qualquer sistema computadorizado que possa aceitar entrada de dados, é um alvo vulnerável. Essa entrada pode ocorrer através de meios físicos (os quais compreendem os dispositivos que podem ser agregados ao computador, como CD's, disquetes, pendrives, etc.) ou através de meios de transmissão de dados (os quais são aqueles que permitem a entrada de dados quando estabelecida uma conexão direta ou indireta com o sistema, como por exemplo, internet, redes sem fio, cabo de fibra ótica, satélite, etc.). Assim sendo, mesmo que um sistema computadorizado esteja isolado de conexão, ele pode vir a ser alvo de um ataque através de dispositivos físicos.

Ademais, para Clarke e Knake (2010, p.73) existem três questões que tornariam uma guerra cibernética possível, quais sejam as falhas na estruturação da internet[24], os erros intencionais ou não em *hardwares* e *softwares*[25], e a crescente tendência de colocação online de sistemas de infraestrutura crítica. Relacionado a isso, para Baker et al (2013, p.14) a cibernética é um banquinho de três pernas, quais sejam, facilidade de uso, segurança e privacidade. O grande problema é que o

[24]Clarke e Knake (2010, p.73-85) enumeram cinco vulnerabilidades no próprio design da rede de computadores e da internet, explicando como os hackers podem utilizar essas falhas para controlar um computador alheio. Segundo os autores, "os criadores das suas regras básicas não imaginavam que ninguém além de bem-intencionados cientistas e governantes usariam a internet", e, por isso, não tiveram a preocupação com uma estrutura de segurança consideravelmente adequada para os fins que ela é utilizada atualmente, quais sejam trafego de informações e dados, comércio, transações financeiras, comunicação e proteção de sistemas militares, empresariais e de infraestruturas críticas, entre outros. Conforme afirmam os autores, os protocolos – conjunto de regras que controla e permite conexão, comunicação ou transferência de dados entre computadores – "foram desenvolvidos com bases em regras que permitiram o crescimento maciço da rede e da internet como a conhecemos hoje, mas também lançaram as sementes para os problemas de segurança".

[25]Esses erros referem-se a falhas nos programas e equipamentos. *Hardware* é a parte física do computador, ou seja, o conjunto de aparatos eletrônicos, peças e equipamentos. *Software* é a parte lógica, o qual permite a manipulação e execução das atividades do computador.

desenvolvimento da internet foi versado para maximizar a simplicidade/facilidade de comunicação, e não de sua segurança.

Dessa forma, existem diversas possibilidades para explorar suas vulnerabilidades. Nesse sentido, para se compreender a guerra cibernética em maior escala é preciso estar atento para a interconectividade existente entre os sistemas públicos e privados, em especial, a infraestrutura crítica[26] de um determinado país. Tais informações são essenciais para definir as vulnerabilidades, os riscos e os desafios existentes à defesa cibernética dos mesmos. Por isso, o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (BRASIL, 2010a) traz na sua definição de Segurança Cibernética a preocupação com as infraestruturas críticas, conforme:

> "Segurança cibernética: arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e **suas infraestruturas críticas**" (BRASILa, 2010, p.116, grifo nosso).

Presentemente, "a maioria dos sistemas de informação, necessários para o funcionamento da sociedade moderna, encontra-se interligado por meio de redes de computadores" (FERREIRA NETO, 2013, p.111). Inclusive, no relatório da empresa McAfee[27] feito com seiscentos executivos de tecnologia da informação e de segurança de infraestruturas críticas de sete setores de quatorze países, "mais de três quartos dos responsáveis por tais sistemas informaram que estes estavam conectados à Internet ou a alguma outra rede" (BAKER et al. 2013, p.19).

Os sistemas das infraestruturas críticas dos países são em sua maioria operados por um software industrial denominado SCADA (Supervisory Control and Data Acquisition/Controle de supervisão e aquisição de dados). Isto é, esse programa controla a rede de sistemas, como por exemplo, a rede elétrica nacional. Os ataques contra sistemas SCADA são "particularmente graves porque podem dar aos hackers controle direto dos sistemas operacionais" (BACKER et al, 2013, p.9) abrindo diversas possibilidades de manipulação desses sistemas, como por

[26]Por infraestrutura crítica pode-se entender os ativos fundamentais para o funcionamento de uma sociedade e de uma economia, como por exemplo o sistema financeiro; o abastecimento d'água; a produção, o transporte e a distribuição de petróleo e de gás; a geração, transmissão e distribuição de energia elétrica; as telecomunicações; o sistema de saúde (hospitais); o sistema de transportes – tais quais metrô, ônibus, trem, aeroportos; entre outros.

[27]A McAfee é uma empresa norte-americana de softwares de segurança de computadores com atuação em todo o mundo. Para maiores informações sobre a empresa, ver http://www.mcafee.com/. Acesso em 25 mai. 2014. Para o relatório elaborada pela empresa sobre a segurança de infraestruturas críticas de várias países do mundo, ver BAKER et al., 2013.

exemplo, desastres ambientais provocados por um vazamento tóxico ou cortes de energia em grande escala.

A contradição da ameaça cibernética é que quanto menos informatizado e conectado à internet os sistemas do país, menor será o risco de um ataque. Acontece que cada vez mais o Estado e a sociedade dependem da internet praticamente para tudo, até mesmo para o domínio e monitoramento das centrais hidrelétricas, termelétricas e nucleares e suas distribuições. Para Lionel Alford (2000, p.109-112), a principal forma de proteção de sistemas cibernéticos é a sua segurança física. Assim, as principais medidas defensivas seriam o isolamento de sistemas críticos; o controle manual de operações críticas; a redução do nível de integração e dependência dos sistemas; a manutenção do elemento humano no ciclo e a atenção quanto às potenciais lacunas de segurança; além de medidas ativas como senhas e autenticações complexas. No entanto, o homem torna-se o elo fraco da segurança, visto que mesmo que os sistemas estejam isolados de conexões externas, estes podem ser afetados por dispositivos físicos, como veremos na última seção deste capítulo tratando-se especificamente dos ataques às centrífugas do Irã em 2010.

Definidos, então, nesta seção, os conceitos e elementos básicos do ciberespaço e da ciberguerra, na próxima seção adentrar-se-á melhor nas características peculiares desta última, relacionando-a com o mundo real.

3.2 CARACTERISTICAS DA GUERRA CIBERNÉTICA E SEU GANHO DE IMPORTÂNCIA NO CENÁRIO INTERNACIONAL

A presente seção tem por finalidade apresentar as características peculiares da guerra cibernética e demonstrar, ao mesmo tempo, como alguns Estados tem lidado com essa questão – juntamente com a cibersegurança –, conferindo ganho de importância da cibernética no cenário internacional atual. Dessa forma, na medida em que serão apresentadas essas características, também serão dados exemplos de como tais particularidades se manifestam no mundo concreto.

Em tempos modernos, quando pensamos na guerra, pensamos automaticamente nos Estados. Em relação à guerra cibernética, não é diferente. Como mencionado na seção anterior, para que esta se caracterize é necessária, primordialmente, a presença direta ou indireta do ator estatal. Quando se fala, então, em participação indireta levanta-se uma característica de extrema importância, o

anonimato. No ataque virtual, as distâncias físicas são irrelevantes e o atacante pode se esconder atrás de um computador localizado em qualquer lugar do mundo, perto ou longe do alvo, com a mesma eficácia.

Portanto, há uma dificuldade em encontrar a origem da ofensiva, em que muitas vezes o atacante esconde-se atrás de estruturas sociais e governamentais, caracterizando, assim, uma espécie de guerra por procuração. Dessa maneira, atores não estatais, como hacktivistas[28] e hackers, recebem a responsabilidade pelos ataques isentando de culpabilidade os Estados dos quais fazem parte. Na maioria dos casos que serão apresentados na próxima seção, os conflitos cibernéticos são mobilizados e coordenados pelos Estados que possuem interesses diretos nos ataques, mas não são oficialmente assumidos por eles. Assim, os Estados teriam interesse na manutenção e tolerância do que Klimburg (2011, p.42) chama de "organizações por procuração". Estas, quando adequado para os Estados, poderiam ser envolvidas em atividades cibernéticas ofensivas e/ou defensivas.

No entanto, ainda de acordo com Klimburg (2011, p.42-43), algumas armas cibernéticas só tem capacidade para serem utilizadas através do apoio ou consentimento tácito de Estados. Aquelas que são menos sofisticadas, como os ataques de negação de serviço[29], podem ser utilizadas com suporte tácito estatal – como são os casos na Estônia em 2007 e na Geórgia em 2008 que serão analisados adiante – mas também podem ocorrer por vontade apenas particular de atores não estatais, devido às tecnologias, conhecimentos e recursos necessários mais simplificados. Por outro lado, os casos mais sofisticados, como ataques de exploração de rede/sistemas e bombas lógicas[30], requerem centenas de horas de programação, capacitação e tecnologia, tendo, com frequência, finalidades políticas adicionais que trariam algum benefício a um Estado – como será visto no caso do ataque virulento, o *stuxnet*, no Irã em 2007.

Além do mais, os governos têm procurado criar estímulos de participação de elementos dos meios empresariais, militares e da sociedade civil na área de

[28]Hacktivismo é a junção das palavras "hacker" e "ativismo". São os ataques cibernéticos com cunho ideológico, político, promovendo a liberdade de expressão, direitos humanos, etc.
[29]Um ataque simultâneo de negação de serviço, denominado "distributed denial of service attack" (DDOS), caracteriza-se pelo bombardeio de interfaces eletrônicas de acesso à websites ou sistemas de computador, gerando inúmeros acessos falsos simultâneos que congestionam a rede, tornando-a inutilizável.
[30]Sequências de códigos específicos em arquivos de dados que manipulam os programas que acessam estes arquivos ou as instruções do processador do sistema. Exemplificando melhor, tem-se que as bombas lógicas funcionam como dispositivos adormecidos em programas de sistemas críticos, instalados prontos para serem ativados em circunstâncias pré-determinadas.

segurança cibernética. Por exemplo, existe no Reino Unido um Centro para a Proteção da Infraestrutura Governamental que tem como função ajudar a indústria britânica a defender-se de ataques cibernéticos (KLINBURG, 2011, p.52). Da mesma maneira, nos Estados Unidos, as indústrias de fundamental importância para a segurança do país operam em proximidade com o governo federal no que tange a cibernética (KLINBURG, 2011, p.52). Ainda, pode-se citar o Exército Eletrônico Sírio[31], o qual utiliza a internet para divulgar o seu ponto de vista a respeito do conflito civil no país, apoiando o regime ditatorial e invadindo sistemas e páginas de internet de governos oposicionistas. Na China, do mesmo modo:

> "uma milícia da cidade de Guangzhou criou um batalhão de guerra cibernética em torno das instalações de uma empresa de comunicação dessa província chinesa, como uma espécie de quartel general, desde 2003. [...] É possível que os indivíduos chineses pertencentes a essa milícia nunca tenham usado um uniforme militar que os identificasse." (KLIMBURG, 2011, p.46, tradução nossa).

Ou seja, nota-se que empresas privadas, organizações por procuração e sociedades de hackers, podem estar comumente e estreitamente ligadas, no que tange a defesa e segurança cibernéticas, com o governo de um Estado. Muitas vezes, não existe nenhuma identificação desses grupos que levem diretamente a identifica-los como pertencentes a um Estado, o que possibilita que um governo não seja responsabilizado por um ataque, fazendo-se valer do anonimato como uma espécie de operação encoberta. Essa característica intrínseca da guerra cibernética pode ser notada no comentário de Clarke e Knake (2010, p.xi) ao afirmar que "o fenômeno da guerra cibernética é tratado com tamanho sigilo que faz parecer a Guerra Fria um tempo de abertura e transparência". Dessa forma, um dos diferencias mais interessantes entre a guerra cibernética e a cinética é que aquela pode oferecer um estado de guerra secreto, em que a participação de um ou mais lados do combate é camuflada, enquanto na guerra convencional as responsabilidades são bem determinadas.

Ademais, pode-se ter uma noção das capacidades e vulnerabilidades de alguns Estados de uma forma mais abrangente. Richard Clarke e Robert Knake (2010, p.147-148) orientam suas análises sobre o que chamam de "força global de guerra cibernética" através de três dimensões: i) poder ciberofensivo, o qual se

[31]BERCITO, Diogo. Grupo de hackers invade sites para mostrar versão sobre crise na Síria. *Folha de São Paulo.* Folha Mundo. Mai. 2013. http://www1.folha.uol.com.br/mundo/2013/05/1278280-grupo-de-hackers-invade-sites-para-mostrar-versao-sobre-crise-na-siria.shtml. Acesso em 07 mai. 2014.

refere à capacidade de atacar outros países; ii) poder ciberdefensivo, visto como a capacidade de adotar medidas enquanto um ataque ocorre; iii) ciberdependência, entendido como o quanto uma nação esta dependente de redes e sistemas informatizados que possam ser vulneráveis pelos três critérios apresentados pelos mesmos autores na primeira seção deste capítulo.

Analisando as três dimensões, pode-se aferir que a capacidade ofensiva cibernética, tão somente, não corresponde à garantia de proteção contra ataques externos, nem à considerável vantagem quando utilizada ofensivamente e, muito menos, à garantia de vitória sobre o inimigo durante uma guerra nesse domínio. Outra característica importante da guerra cibernética pode ser notada então: o fator preponderante encontra-se no nível de dependência das infraestruturas críticas do país aos sistemas de rede informatizados. Ou seja, países com grande capacidade de ataque nesse espaço podem ser concomitantemente vulneráveis diante do nível de tecnologia e interligação de seus sistemas críticos.

Nesse sentido, os autores conferem pontuações de zero a dez à cinco países, quais sejam EUA, Rússia, China, Irã e Coreia do Norte, podendo ser observadas na tabela abaixo:

TABELA 1 – ESTIMATIVA DE FORÇA GLOBAL DE CIBERGUERRA

ESTIMATIVA DE FORÇA GLOBAL DE CIBERGUERRA				
ESTADO	**CIBEROFENSIVO**	**CIBERDEFENSIVO**	**DEPENDÊNCIA**	**TOTAL**
EUA	8	1	2	11
RÚSSIA	7	4	5	16
CHINA	5	6	4	15
IRÃ	4	3	5	12
CORÉIA DO NORTE	2	7	9	18

Fonte: CLARKE; KNACK (2010, p.148)

No entanto, Clarke não aprofunda metodologicamente suas pontuações, baseando-se tão somente nos conhecimentos e experiências adquiridos quando fazia parte do departamento de Estado norte-americano das administrações de Ronald Reagan, George H. W. Bush, Bill Clinton e George W. Bush, em especial nas

duas últimas, em que foi nomeado Coordenador Nacional de Segurança, Proteção de Infraestrutura e Contraterrorismo; e Conselheiro Especial para a Segurança no Ciberespaço, respectivamente. Esta superficialidade faz com que seus dados possam incorrer em erros analíticos.

De qualquer forma, por tratar-se de uma análise pioneira no setor cibernético, as informações obtidas tem importância. Elas permitem afirmar que a Coreia do Norte teria a maior capacidade de enfrentar um conflito nesse novo domínio, não por sua capacidade ofensiva, mas sim por sua independência quanto a tecnologia nos sistemas de infraestrutura do país. No outro extremo, estaria os EUA, em virtude de seus sistemas críticos estarem altamente dependentes da informática e não existir a possibilidade de rápida desconexão entre eles. A China, apesar de seus sistemas críticos estarem intimamente ligados à informática, pode, em caso de ameaça ou ataque, desconectar todo o país da internet global (FERNANDES, 2012), o que lhe confere bom score defensivo, ainda que isso possa significar restrição de liberdades individuais em prol de segurança nacional.

Nesse caso, o que faz um país ser fácil de desconectar? Basicamente, alta centralização (controle) e baixa diversidade (provedores de serviço). A China obtém tal controle sobre a rede de computadores e da internet do país por meio de um sistema operacional próprio, um microprocessador seguro e um firewall nacional[32]. De uma forma geral, o governo chinês procura ter esse controle como uma forma de vigiar seus usuários e redireciona-los para os conteúdos de interesse do governo, ao mesmo tempo em que possibilitam “encontrar malwares instalados por Estados inimigos” (CLARKE; KNAKE, 2010, p.56).

Assim, juntos, tais dispositivos são um considerável investimento pelas autoridades chinesas para elevar o grau de bloqueio, de filtro e de monitoramento do seu ciberespaço. Em contraste, os EUA não possuem “nem planos nem capacidade para fazer isso, pois suas conexões são privadamente possuídas e controladas” (CLARKE; KNAKE, 2010, p.148, tradução nossa). Ademais, enquanto o governo chinês possui controle completo sob as comunicações, nos EUA quem regula é a

[32]O sistema operacional próprio da China é denominado “Kylin” e é produzido pela empresa norte-americana Microsoft, que permite que os chineses modifiquem a versão para introduzir um componente seguro usando sua própria criptografia. Ainda, a China desenvolveu seu próprio microprocessador denominado “Green Dam Youth Escort”, tentando coloca-lo em todos os computadores do país com a justificativa de controlar a pornografia infantil e outros materiais proibidos. Por fim, o país desenvolveu ainda o que se denomina “o grande firewall chinês”. Um firewall é uma espécie de filtro de informações e dados que trafegam pela rede do computador e tem como objetivo fornecer maior segurança e controle (CLARKE; KNAKE, 2010, p.56).

Comissão Federal de Comunicação (CLARKE; KNAKE, 2010, p.146). Ou seja, a China, por ter um governo considerado mais autoritário, pode limitar a utilização do ciberespaço, fornecendo poucos provedores de serviço de internet, ao mesmo tempo em que isso significa ampla censura, limitação de liberdades e privacidades. Diferentemente, os EUA possuem mais de quarenta provedores[33], o que impossibilita uma rápida e completa desconexão.

Os chineses, ainda, possuem um atributo peculiar que não é levado em conta pelos autores: o potencial de seu exército eletrônico. Sabe-se que a China tem o Estado mais populoso do planeta e, até por isso, tem também o maior número de usuários de internet. No entanto, a população do país ligada à rede ainda é baixa[34], muito em conta pelo subdesenvolvimento interno das cidades que estão distantes dos centros populacionais e industriais. Levando-se em consideração que o país está muito distante da força militar convencional de outros Estados, em especial, os EUA, o espaço cibernético pode vir a ser uma forma de reduzir essa diferença de poder em relação a outras nações. Assim sendo, essa potencialidade atribui à China a maior massa de hackers que, eventualmente, podem ser contratados para objetivos e interesses nacionais estratégicos. Conforme se percebe pelo que afirma Klinburg (2011), há muito a República Popular da China percebeu o valor estratégico e tático do ciberespaço:

> "O número de recrutas em potencial para o ciberespaço é impressionante. Em 2007, a China tinha mais de 25 milhões de alunos em universidades do Estado, não incluindo aqueles em formação educacional privada ou programas técnicos especializados. Milhões de pessoas são empregadas em empresas estatais de informação e tecnologia. Tendo em conta estes números, bem como o número provável de hackers patriotas chineses que podem fazer parte de estruturas militares, não é de estranhar que a maioria dos ataques cibernéticos contra os Estados Unidos venha da China. A empresa de segurança cibernética iDefense tem monitorado mais de 250 grupos de hackers localizados no país. Não mais do que 5.000 hackers podem fazer parte de estruturas e programas para-governamentais, mas as associações indiretas podem ter recrutas até dez vezes maior que esse número. Competições de hackers e afins organizadas não são apenas tentativas de identificar bons talentos, mas também para coloca-los ocupados com a segurança". (KLIMBURG, 2011, p.46, tradução nossa).

[33]COWIE, Jim. Could it happen in your contry**,** *Renezys.* Nov. 2012. Disponível em: http://www.renesys.com/2012/11/could-it-happen-in-your-countr/. Acesso em 26 mai. 2014.

[34]Segundo o Centro de Informação sobre Internet na China (CNNIC), em 2013, o país atingiu o número de 613 milhões de usuários de internet. Levando-se em consideração sua população total, cerca de 1,35 bilhão, nota-se que apenas 45,8% da população tem acesso ao recurso. O relatório estatístico de desenvolvimento da internet na China pode ser visto em: http://www1.cnnic.cn/IDR/ReportDownloads/201404/U020140417607531610855.pdf. Acesso em 27 mai. 2014.

Assim sendo, temos outra característica presente numa guerra cibernética, qual seja a presença da assimetria e sua respectiva redução. Isto é, uma força reduzida e bem treinada pode causar danos em outra superior. A ação ofensiva torna-se um elemento surpresa, sendo mais fácil e rápido atacar do que se defender. Nesse caso, coloca-se a ciberguerra no rol das guerras assimétricas, em que um oponente menos favorecido convencionalmente pode enfrentar um adversário superior pela sua maior inteligência e agilidade. Assim sendo, o "espaço cibernético oferece as oportunidades para isso, inclusive em grande escala" (CORNISH et al, 2010, p.28, tradução nossa). A ciberguerra, quando tão somente utilizada, torna-se substancialmente mais barata do que uma guerra convencional, podendo ser também destrutiva, mesmo que para o desenvolvimento de armas cibernéticas sofisticadas sejam necessários, ainda, consideráveis recursos, investimentos em tecnologia e pessoal, tempo e sigilo operacional.

Ao mesmo tempo, essa assimetria significa um limitador ao conflito virtual. A probabilidade de que Estados de menor poder no sistema internacional iniciem uma guerra é muito pequena, visto que não teriam condições de sustentar uma retaliação de armas convencionais de um Estado mais poderoso. Ou seja, deve-se também pensar nos custos reais consequentes de tais ações. Nesse sentido, o anonimato serve, novamente, como uma válvula de escape para que não se possa identificar a origem dos ataques. Portanto, o agressor não teme, inicialmente, uma represália imediata.

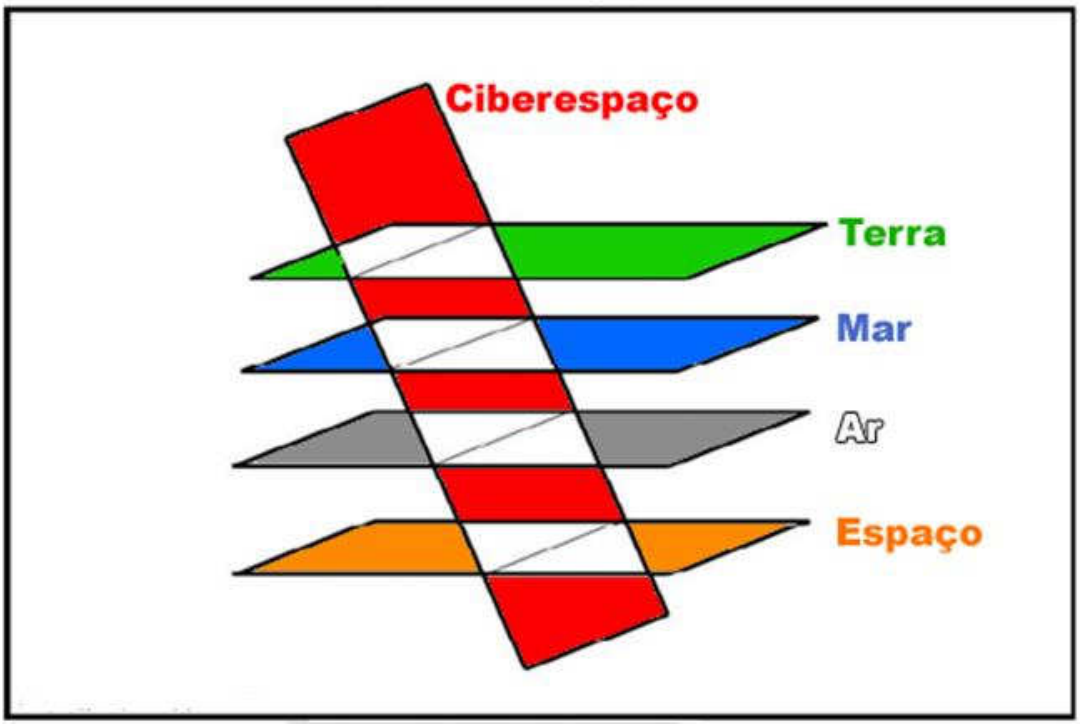
Pode-se elencar, ainda, outra característica do conflito cibernético: a incerteza de sucesso. Ainda não existe a garantia certa de que um ataque será bem sucedido. Às vezes, os programas maliciosos instalados nos alvos específicos podem não agir da forma esperada quando inseridos em um novo sistema, ou até mesmo serem interceptados por outros softwares de proteção. Em outro cenário, um ataque a uma infraestrutura bancária de outro país pode alavancar riscos de danos ao próprio atacante, uma vez que colapsado um sistema bancário, este pode estender-se para outros países.

Por último, entende-se que a guerra cibernética deve produzir efeitos no mundo real. Não teria sentido desencadear um ataque contra entidades tão somente virtuais. Ou seja, as ações devem ter resultados concretos no mundo cinético e devem fornecer alguma vantagem. Os ataques se realizam em um campo virtual, o ciberespaço, mas possuem sempre uma origem e objetivos situados em um campo

real (VENTRE, 2012, p.35). Portanto, a exploração de redes e sistemas de computadores e infraestruturas críticas de um país inimigo pode compor um competente modo de conquistar vantagem sobre este, levando até mesmo, no contexto militar, a superioridade no campo de batalha tradicional.

Em outras palavras, além do conflito virtual que o domínio cibernético pode proporcionar, ele também pode interagir com outras dimensões, servindo, portanto, como auxiliar em uma guerra convencional. Assim sendo, o espaço cibernético igualmente se caracteriza por sua transversalidade com a terra, o mar, o ar e o espaço, permitindo sua projeção de poder nesses demais domínios espaciais (VENTRE, 2012, p.34-35). Conforme aponta a figura abaixo:

FIGURA 1: TRANSVERSALIDADE/INTERAÇÃO DO CIBERESPAÇO COM AS DEMAIS DIMENSÕES.



Fonte: Adaptação de VENTRE (2012, p.35).

Por conseguinte, os ataques cibernéticos podem vir a oferecer “meios adicionais através dos quais a hostilidade pode ser prosseguida” (FERNANDES, 2012, p.60). Por exemplo, um ataque que viesse a causar a interrupção do sistema de fornecimento de energia elétrica ou de comunicação de um país, dificultaria a movimentação e transmissão de informações das tropas inimigas, tornando mais fácil uma invasão no domínio cinético. Dessa maneira, as forças cibernéticas e informatizadas tornam-se propriamente ferramentas de guerra, podendo servir para o êxito completo em um conflito. Portanto, apesar de poder ser um novo domínio, a

guerra cibernética não esta integralmente separada dos demais ambientes de conflito.

Antes de dar prosseguimento ao capítulo, é interessante discutir alguns argumentos de alguns autores que não consideram a cibernética como um novo domínio de guerra. Para isso, tomaremos como base Thomas Rid (2013). Para ele, a ciberguerra "nunca ocorreu no passado, não ocorre no presente e é altamente improvável que irá disturbar nosso futuro" (RID, 2013, p.xiv, tradução nossa). Ao contrário disso, os ataques cibernéticos seriam versões atualizadas de três atividades antigas, quais sejam subversão, sabotagem e espionagem. Ele desconsidera o caráter de guerra da cibernética baseando-se justamente em Clausewitz (1832). Rid (2013, p.1-3) elenca os três elementos principais da guerra: seu caráter violento, seu caráter instrumental e sua natureza política[35].

Nas palavras do autor, "se o uso da força na guerra é violento, instrumental e político, então não há ofensiva cibernética que atenda a esses três critérios" (RID, 2013, p.6). Analisando os mesmos casos que serão abordados na próxima seção, Rid afirma que os ataques cibernéticos não são violentos – e, portanto, não acarretam em mortes – e são constantemente anônimos – e, assim, não possuem apoio político. Por fim, escreve que nenhum ataque cibernético até hoje tenha atendido aos três critérios clausewitzianos. Na verdade, o que teria ocorrido foram atos de sabotagem, espionagem e subversão com utilização de meio cibernético.

No entanto, descreveu-se no capítulo primeiro deste trabalho que a "guerra é um ato de força para obrigar o nosso inimigo a fazer a nossa vontade" (CLAUSEWITZ, 1832, p.75) e que para que esta vontade ocorra, é preciso desarmar/derrotar o inimigo. Assim, deve-se desarmar o adversário ao ponto de impedi-lo ou dificulta-lo em sua defesa e da possibilidade de um ataque imediato. Nesse sentido, a guerra cibernética encaixa-se perfeitamente no perfil clausewitziano. Isto é, ela pode ter como intuito obrigar o atacado a fazer a vontade do atacante. Além do mais, pode servir também para dificultar ou impedir a defesa do oponente.

Vale ressaltar, ainda, que na ciberguerra não é necessário um ataque massivo ou uma destruição coletiva. O objetivo a ser atingido pode ser bem

[35]Baseando-se em Clausewitz (1832), Rid afirma que: (i) para se caracterizar um ato de guerra é necessário que o um ato seja violento; (ii) um ato de guerra é sempre instrumental e, para isso, deve existir sempre um meio para um determinado fim; (iii) a guerra é sempre política, sendo a continuação desta por outros meios.

específico, como por exemplo, causar danos às centrífugas de uma central nuclear de determinado país. Além do mais, por mais que o anonimato seja sua característica fundamental, a participação direta ou indireta do Estado está presente no ato, seja por interesses diretos ou indiretos ou seja pelo nível de sofisticação da arma cibernética. Assim, a guerra cibernética não deixa de ter um caráter instrumental, um caráter violento e uma natureza política.

De toda maneira, o livro de Thomas Rid não deixa de ser coeso e original, sendo sua obra importante para a discussão de um tema tão novo e ao mesmo tempo tão complexo e polêmico. Portanto, toda forma de contribuição nessa área para a perspectiva dos Estudos Estratégicos é válida. Contudo, contrário ao pensamento de Rid, baseando-se em eventos que serão descritos na próxima seção, através de cinco sentenças, os autores Clarke e Knake (2010) afirmam que a guerra cibernética:

[1] É real:

> "O que temos visto até agora esta longe de ser um indicativo do que pode ser feito. A maioria dos eventos conhecidos utilizou armas cibernéticas primitivas (com a notável exceção para a operação israelense [stuxnet]). É uma suposição razoável que os atacantes não quiseram, ainda, revelar suas capacidades mais sofisticadas. O que os EUA e outras nações são capazes de fazer em uma guerra cibernética poderia devastar uma nação moderna" (CLARKE; KNAKE, 2010, p.30, tradução nossa).

[2] Acontece na velocidade da luz:

> "Como os ataques ocorrem por cabos de fibra óptica, o tempo de lançamento de um ataque e seu efeito é escassamente mensurável, criando riscos para os tomadores de decisão" (CLARKE; KNAKE, 2010, p.30-31, tradução nossa).

[3] É global:

> "Em qualquer conflito, um ataque cibernético pode, rapidamente, se tornar global. Computadores e servidores podem ser invadidos e muitas nações podem ser 'desligadas'" (CLARKE; KNAKE, 2010, p.31, tradução nossa).

[4] Ignora o campo de batalha:

> "Todo tipo de sistemas que as pessoas dependem, desde bancos até radares de defesa aérea são acessíveis do ciberespaço e podem ser rapidamente derrubados, sem que seja necessário, primeiro, derrotar as defesas tradicionais de um país" (CLARKE; KNAKE, 2010, p.31, tradução nossa).

[5] Já começou:

> "Em antecipação as possíveis hostilidades, as nações já estão preparando o campo de batalha. Eles já invadem as redes e infraestruturas de cada

> Estado, preparando espécies de alçapões e bombas-relógio – agora, em tempos de paz. Esta natureza permanente de guerra cibernética, a indefinição da paz e da guerra, adiciona uma nova dimensão perigosa de instabilidade" (CLARKE; KNAKE, 2010, p.31-32, tradução nossa).

Após as análises e explanações feitas sobre a guerra cibernética, o presente trabalho irá, na próxima seção, descrever e analisar algumas observações de casos que permitem apontar para a existência da guerra cibernética, identificando-a com os princípios necessários de Clausewitz (1982).

3.3 OBSERVAÇÃO DE CASOS: A CIBERNÉTICA COMO NOVO E INTEGRADO DOMÍNIO DE CONFLITOS

Na medida em que a tecnologia cibernética se desenvolve, seus componentes "podem adquirir uma gama maior de usos, aprofundando a complexidade do ciberespaço e aumentando o poder de atritos e conflitos (CORNISH et al, 2010, p.18, tradução nossa). Assim, porque é possível falar em guerra cibernética? Esta seção tem por finalidade apresentar e analisar alguns incidentes internacionais como exemplos precursores de ataques cibernéticos como ato militar, podendo servir, então, para explicar o fenômeno da ciberguerra. Assim, ainda que alguns estudiosos rejeitem a cibernética como novo domínio de conflito, esta seção pretende demonstrar que existe uma relação entre o mundo abstrato e teórico dos seus conceitos com o mundo real do sistema internacional. Serão descritos quatro casos, fazendo-se uma análise sobre eles de acordo com o que foi tratado até então. Os incidentes a serem apresentados serão: a explosão de um oleoduto na Sibéria em 1982; os ataques à Estônia em 2007; à Geórgia em 2008 e ao Irã em 2010.

Ainda no tempo da Guerra Fria, as ações praticadas pelos EUA tinham como intenção conter o comunismo e derrubar o governo soviético. Na maioria das vezes, as ações eram políticas de contenção através de sanções econômicas e de ações encobertas, em especial, espionagem. Da mesma forma, a maioria dos planos não era detalhadamente divulgada, por se tratar de um período extremamente fechado e de atuações sigilosas. Nesse sentido, Reed (2004, p.113-132), de acordo com um documento inédito, chamado "dossiê Farewell"[36] (WEISS, 1996), afirma que os EUA forneceram à União Soviética (URSS) um software defeituoso que levou a um

[36]Mais especificadamente, o "dossiê Farewell" foi uma coleção de documentos que um coronel desertor da KGB (Comitê de Segurança do Estado Soviético), Vladimir Vetrov, formou e entregou à direção de inteligência e vigilância francesa durante a Guerra Fria.

grande desastre numa tubulação de gás do país localizada na Sibéria. A origem da cibernética como arma ofensiva está, portanto, nesse acontecimento.

A produção e o transporte de petróleo e gás estavam no topo da lista de prioridades soviéticas. Um novo gasoduto tinha como intenção transportar gás natural do campo de Urengoi na Sibéria através do Cazaquistão, da Rússia e da Europa Oriental para o mercado do Ocidente (CLARKE; KNAKE, 2010, p.92-93). Para automatizar e agilizar o processo de operação das válvulas, compressores e instalações de armazenamento eram necessários sistemas de controle mais sofisticados do que aqueles que os soviéticos possuíam na época.

No entanto, as companhias americanas rejeitaram a oferta de compra da URSS pelos softwares necessários a tais funções. Assim, os soviéticos tentaram roubar informações dos programas e códigos de fornecedores canadenses. Ciente de tais ações, a Agência governamental de Inteligência norte-americana (CIA) modificou o software com o objetivo de manipular o sistema que controla o oleoduto, fazendo-o funcionar como uma bomba lógica. Contudo, “quando os russos roubaram o programa e usaram-no para operar os oleodutos, inicialmente, tudo funcionou perfeitamente” (CLARKE; KNAKE, 2010, p.92, tradução nossa).

Após um período de tempo, como uma espécie de cavalo de Tróia, o novo software começou a apresentar mau funcionamento. O programa foi configurado para modificar a velocidade de distribuição do gás e das configurações de pressão das válvulas para níveis muito além daqueles aceitáveis. O resultado, segundo Clarke e Knake (2010, p.93) foi “a mais massiva explosão não nuclear já vista” ou, conforme Reed (2004, p.128) foi “a mais monumental explosão não nuclear vista do espaço”, sem a utilização de um míssil ou bomba sequer, mas sim através da modificação de um código em software de um sistema computadorizado. Apesar disso, vale destacar que não houve vítimas físicas com o incidente, mas os danos econômicos para a URSS à época foram significativos.

O segundo caso ocorreu em 2007, quando foram divulgados ataques maciços a instituições públicas e privadas da Estônia. O que aconteceu ao país pode demonstrar o quão vulnerável uma nação pode ser a um ataque cibernético. Nesse incidente, vários ataques foram utilizados para tirar do ar websites governamentais importantes, de empresas bancárias e de sites de notícias, causando suas sobrecargas até torna-las inutilizáveis. O método de ataque foi relativamente simples, através do chamado ataque de negação de serviço (DDoS).

No entanto, “o ataque DDoS na Estônia foi o maior já visto na história,[...] durando semanas após semanas” (CLARKE; KNAKE, 2010, p.14, tradução nossa), infectando milhares de computadores que mandavam gigantescas quantidades eletrônicas de tentativas de acesso até que os sistemas não conseguissem mais processa-las e colapsassem. Essa técnica exige a participação de inúmeros computadores dedicados aos ataques que podem ou não ter o conhecimento de seu proprietário[37].

Rapidamente, o governo da Estônia acusou a Rússia pela origem dos ataques, afirmando que o controle dos computadores de onde partiam os ataques era de território russo e os códigos utilizados estavam no alfabeto computadorizado cirílico (utilizado na Rússia). Contudo, o governo russo negou diplomaticamente tais acusações e se recusou, inclusive, a ajudar na busca para rastrear os atacantes. Mesmo assim, a Estônia evocou apoio da OTAN, que enviaram especialistas em Tecnologia da Informação para observar o ocorrido e auxiliar na retomada dos serviços eletrônicos. Vale notar que, pela primeira vez, a OTAN admitiu abertamente uma semelhança entre ataques cibernéticos e uma guerra real ao afirmar que “se o centro de comunicação de um Estado da organização é atacado por um míssil, você chama isso de um ato de guerra. Então, do que você chamaria se a mesma instalação é desabilitada por um ataque cibernético?”[38].

Ainda que se trate de um ataque pouco sofisticado, a quantidade de computadores utilizados e acessos tentados foram tão complexos que se pode acreditar que a ofensiva teve apoio do governo russo e de empresas de telecomunicações russas, visto que os ataques foram provenientes do país que se negou a auxiliar na resolução do caso. De qualquer forma, os ataques não foram em si violentos e permaneceram até hoje anônimos, sem uma responsabilidade oficial. De qualquer forma, acredita-se que a ofensiva na Estônia serviu como uma espécie de treinamento e teste para aquela que ocorreria em 2008 na Geórgia.

Logo após os ataques, em 2008, a OTAN decidiu criar um Centro de Defesa Cibernético (CCD/COE) que já vinha sendo discutido desde 2004, mas o incidente na Estônia acelerou o processo, definindo-a como uma organização internacional militar. Com sede em Bruxelas, o CCD/COE tem como objetivo aumentar a

[37]THE Cyber Raiders Hitting Estonia. *BBC News.* Londres. Mai. 2007. Disponível em: http://news.bbc.co.uk/2/hi/europe/6665195.stm. Acesso em 14 mai. 2014.
[38]A Cyber-riot. *The Economist.* Mai. 2007. Disponível em: http://www.economist.com/node/9163598. Acesso em 14 mai. 2014.

capacidade, cooperação e compartilhamento de informações entre a OTAN, países da OTAN e parceiros na defesa cibernética, visando educação, investigação e desenvolvimento no setor. O Centro oferece serviços defensivos no plano cibernético a toda organização filiada, tanto nos quarteis generais quanto para informações às forças deslocadas em operações e exercícios[39].

O caso seguinte, ocorreu na Geórgia em 2008. Primeiramente, é importante compreender que a relação entre o país e a Rússia é conturbada desde o início do século XX, quando a URSS invadiu o país, o qual havia declarado sua independência em 1918, mas foi reintegrado ao regime russo ao findar da Revolução Russa por volta de 1921. Com a desintegração da União Soviética, novamente os georgianos declararam sua independência, mas mantêm relações conflitivas com o país vizinho ainda hoje especialmente pelo controle do território da Ossétia do Sul[40].

Visando a retomada da Ossétia do Sul, o exército georgiano invadiu e tomou o controle da região. No dia seguinte, o exército russo deslocou-se até o local e expulsou rapidamente as forças da Geórgia, avançando ainda sob uma pequena parte do território georgiano. As ações nesse caso foram divididas em três partes: na primeira, assim como na Estônia, a ação escolhida foram ataques DDoS dirigidos a websites do governo e da mídia local; na segunda, a primeira parte continuou sendo aplicada e ampliou-se os ataques para maior número de alvos como instituições financeiras e de ensino, empresas, mídia ocidental (incluindo BBC e CNN). Os ataques a bancos inundaram o sistema bancário de transações falsas, o que fez com que outros bancos internacionais suspendessem as operações com os bancos georgianos, levando a paralizações. Ao mesmo tempo, o serviço de telefonia do país também foi suspenso, isolando a comunicação com o resto do mundo. (CLARKE; KNAKE, 2010, p.18-19).

Dessa forma, percebe-se que o objetivo primário era isolar e silenciar os georgianos, “produzindo efeitos psicológicos e de informações, reduzindo a capacidade de comunicar-se com o mundo externo, não apenas pela mídia e pelo governo, mas também pela população local” (FERREIRA NETO, 2012, p.82). À

[39]Informações obtidas diretamente do site da instituição, disponível em: https://www.ccdcoe.org/. Acesso em 10 mai. 2014.
[40]PRESIDENTE da Geórgia acusa Rússia de invadir seu território. *BBC BRASIL.* Ago. 2008. Disponível em: http://www.bbc.co.uk/portuguese/reporterbbc/story/2008/08/080808_ossetiapresidente_pu.shtml. Acesso em 12 mai. 2014.

época, o presidente polonês declarou que os ataques cibernéticos à Geórgia caracterizavam uma "agressão militar"[41]. Nota-se que se evitaram causar danos mais graves às redes SCADA do país, algo que os hackers tinham capacidade para faze-lo (CARR, 2010, p.115). Nesse caso, uma quebra no funcionamento dos sistemas de controle de infraestruturas teria sérias implicações as quais não eram a intenção no momento.

Apesar de, novamente, o governo russo ter negado sua responsabilidade nos ataques cibernéticos e, igualmente, ter se recusado a auxiliar na busca pela origem e não ter feito absolutamente nada para deter tais ataques provenientes de redes do país, especialistas em segurança cibernética, como CARR (2010, p.105-115), conseguiram encontrar vínculos entre a origem de alguns ataques de websites russos com uma organização criminosa russa, que por sua vez "estava interligada ao aparato de inteligência russo" (CLARKE, KNAKE, 2010, p.20, tradução nossa). Nas palavras dos autores:

> "Qualquer atividade cibernética em grande escala na Rússia, seja feita pelo governo, pelo crime organizado ou pelos cidadãos, é feita com a aprovação do aparato de inteligência do país e também dos chefes do Kremlin" (CLARKE, KNAKE, 2010, p.20, tradução nossa)

Por fim, a terceira fase representa a possibilidade do uso, pela primeira vez, de uma operação conjunta de um ataque contra redes de computadores com importantes operações tradicionais, demonstrando o "enorme potencial que traz essa nova dimensão" (FERREIRA NETO, 2012, p.82). Mais precisamente, "no mesmo momento em que o exército russo se movimentou, os guerreiros cibernéticos do país também o fizeram" (CLARKE; KNAKE, 2010, p.17, tradução nossa). Nesse sentido, a não responsabilidade oficial russa pelos ataques cibernéticos cria certa limitação para análise dessa coordenação de forças. No entanto, segundo relatos dos autores supracitados, durante a retomada russa da região da Ossétia do Sul, instalações afetadas pelos ataques cibernéticos, como por exemplo, órgãos da mídia e de comunicação, não sofreram ataques por meio cinéticos, levando a crer que o sucesso da ofensiva virtual deixou tais ações desnecessárias.

Além disso, a impossibilidade de comunicação entre as tropas georgianas durante a "guerra dos cincos dias"[42], e também com o mundo externo, foi um

[41]ESPINER, Tom. Georgia Accuses Russia of Coordinated Cyberattack. *CNet News*. Ago. 2008. Disponível em: http://news.cnet.com/8301-1009_3-10014150-83.html. Acesso em 09 mai. 2014.
[42]A denominação foi feita por Kornely K. Kakachia, e mais detalhes sobre a guerra entre a Rússia e a Geórgia na Ossétia do Sul podem ser encontrados em seu artigo. KAKACHIA, Kornely K. A guerra

facilitador para a retomada da região pelos russos. Ainda que o Kremlin negue envolvimento no caso, os ataques cibernéticos foram favoráveis à operação russa, levando a crer que ainda que os ciberataques tenham sido independentes e a coordenação destes com a ofensiva cinética tenha sido uma coincidência, no mínimo, os hackers russos sabiam o momento em que as operações terrestres teriam início, o que pode inferir em um prévio planejamento e conhecimento pela Rússia. Portanto, diante de tais possibilidades, é reconhecível que as capacidades cibernéticas podem vir a ser consideradas como um sistema operacional num ato de guerra, da mesma forma que os demais domínios cinéticos.

Por último, tem-se o incidente ocorrido no Irã em 2010. Mas primeiramente, é importante compreender o contexto dos acontecimentos. Os atos terroristas nos EUA em 11 de setembro de 2001 alavancaram uma GGcT, caracterizado por duas ofensivas abertas, uma no Afeganistão e outra no Iraque. Com a respectiva invasão dos norte-americanos a esses países, o Irã ganhou força e espaço na cena internacional, especialmente como potência regional. Isso porque seus dois principais inimigos na região – o Talebã no leste e Saddam Hussein no oeste – estavam controlados pela potência americana. Nesse sentido, o crescimento do Irã, juntamente com seu programa de enriquecimento nuclear, tornou-se uma ameaça ao ocidente, em especial à Washington, e também aos seus aliados Inglaterra e Israel, este último inimigo histórico de Teerã.

Assim, como uma guerra aberta ao Irã tornar-se-ia demasiadamente arriscada e perigosa, optou-se por um plano secreto de alcunha “Jogos Olímpicos”[43]. O programa iniciou-se em 2006, ainda na administração Bush filho, e teve como base o desenvolvimento e utilização de um vírus de computador para atacar outra nação. Talvez, essa tenha sido a arma cibernética mais sofisticada utilizada e divulgada até então. Nesse caso, não foi empregado um ataque DDoS como nas duas anteriores, mas sim uma ferramenta mais complexa, o vírus stuxnet.

O stuxnet era composto por códigos de programação extensos e complexos que tinham como finalidade reprogramar sistemas de controle industrial operados por SCADA. Ele ataca apenas motores que operam à determinada frequência e, ao

---

dos cinco dias. Relações Internacionais, n.20, Lisboa. 2008. disponível em: http://www.scielo.oces.mctes.pt/scielo.php?script=sci_arttext&pid=S1645-91992008000300003. Acesso em 10 mai. 2014.

[43]SANGER, David S. Obama Order Sped Up Wave of Cyberattacks Against Iran. *New York Times.* p.A1. Jun. 2012. Disponível emhttp://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all. Acesso em 16 mai. 2014.

encontrar tal frequência específica, altera o funcionamento do sistema computadorizado de modo a torna-lo inoperável. Especificadamente, o alvo era o programa nuclear iraniano, visando comprometer as centrífugas de enriquecimento de urânio do país (RID, 2013, p.32-33;42-53).

A maior parte das infecções oriundas do vírus, cerca de 60%, foi encontrada no Irã, o que indica que o país foi o alvo principal da operação. O resultado foi a danificação de um quinto das centrífugas nucleares iranianas, especialmente uma localizada na cidade de Natanz (ARAUJO JORGE, 2012). Os ataques, então, teriam ajudado a atrasar o programa nuclear iraniano na época. No entanto, a propagação do programa malicioso não foi feita através da internet, mas sim por dispositivos (pendrives) contaminados, visto que as centrífugas iranianas não operam com conexão. Ou seja, para sua efetividade, o ataque dependeu da participação humana, local e direta (propositalmente ou não) e de um dispositivo físico.

Por esses motivos, especialistas (por exemplo: CARREIRO, 2012) apontam que tal evento não pode ser considerado um ataque cibernético por não ter trafegado pelo ciberespaço, já que não utilizou a internet. No entanto, incorre-se no erro de perceber o espaço cibernético como sinônimo de internet, sem leva-lo em consideração também como um sistema computadorizado de redes interligadas. Da mesma forma, conforme se apontou na primeira seção deste capítulo através de Lionel Alford (2000), mesmo que um sistema computadorizado esteja isolado de conexão, ele pode vir a ser alvo de um ataque através de dispositivos físicos, como foi o caso. Ainda que o ataque pelo stuxnet não tenha causado explosões, graves danos ou tornado permanentemente inutilizável a infraestrutura iraniana, o ataque retardou o programa de enriquecimento de urânio do país, fazendo com que operasse com falhas e com efetividade menor do que programada.

Novamente, nesse caso, não houve responsabilidade oficial. Mas a complexidade do vírus, ao lado de notícias vinculadas em mídias internacionais, indica que os recursos e os conhecimentos requeridos para tal ofensiva não poderiam ser produzidos por simples organizações criminosas ou hackers independentes. Isso leva a crer que apenas algum Estado teria condições e capacidades para construir tal arma cibernética. Ainda, o interesse norte-americano e israelense em não permitir que o Irã alcance o patamar de potência nuclear, infere na participação desses Estados no ataque cibernético. Além do mais, em 2010, o diretor do serviço secreto exterior britânico (MI-6), John Sawers, em um discurso

público ressaltou a necessidade "de operações de inteligência para dificultar que países como Irã desenvolvam armas nucleares"[44].

Vale destacar que o stuxnet não foi a única ciberarma utilizada contra o país iraniano. Há, ainda, outros arsenais que teriam sido direcionados para Teerã, tais como o "duqu"[45] – o qual tem o objetivo de coletar informações e dados que possam ser úteis para ataques a sistemas SCADA –, o "stars"[46] – que teve como desígnio danificar sistemas do governo iraniano – e o "flame"[47] – o qual serve de espionagem em computadores que executam o sistema operacional da Microsoft Windows, podendo gravar áudio, capturar imagens, detectar tráfego de rede e digitação do teclado, além de obtenção de dados e informações. Nesse último exemplo, o programa foi encontrado e reconhecido oficialmente pela Equipe de Resposta ante Emergência Informática do Irã (MAHER)[48].

Portanto, ainda que os incidentes causados através do espaço cibernético tenham suas origens na década de 1980, o tema ganhou verdadeiro espaço na cena internacional a partir do século XXI. Nos casos apresentados, pode-se perceber que existiu certa violência nos ataques, ainda que não tenha sido de forma massiva e coletiva, mas sim específica e determinada. Além do mais, nota-se que os instrumentos cibernéticos tornaram-se um meio para se alcançar determinado fim, possuindo, então, caráter instrumental, seja para enfraquecer o inimigo – como no caso da Geórgia – seja para fins mais peculiares – como nos demais casos. Por fim, o caráter político também encontra-se presente nos casos na medida em que pode-se direcionar os ataques para a participação de governos mediante buscas por seus interesses. E, especificamente, no caso do Irã, é possível perceber uma guerra cibernética contínua contra o país.

Apreende-se que os responsáveis pela segurança cibernética de um Estado não devem se preocupar tão somente com suas redes militares, mas igualmente

---

[44]SIR John Sawers's speech – full text. *The Guardian.* Out. 2010. Tradução nossa. Disponível em: http://www.guardian.co.uk/uk/2010/oct/28/sir-john-sawers-speech-full-text. Acesso 16 mai. 2014.

[45]IRAN says it has controlled Duqu malware attack**.** *BBC News.* Tecnology**.** Nov. 2011. Disponível em: http://www.bbc.co.uk/news/technology-15721839. Acesso em 16 mai. 2014. Ver também, PERLROTH, Nicole. Reserchs find clues in malware**.** *New York Times.* p.B1. Mai. 2012. Disponível em: http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html. Acesso em 16 mai. 2014.

[46]Ibidem

[47]Também denominado "Skywiper". LEE, Dave. Flame: Massive Cyber-attack discovered, researchers say. *BBC News.* Tecnology. Mai. 2012. Disponível em: http://www.bbc.com/news/technology-18238326. Acesso em 16 mai. 2014.

[48]Disponível no site oficial da Equipe em: http://www.webcitation.org/682bfkhaU. Acesso em 16 mai. 2014.

com as redes civis e de infraestruturas críticas. No caso da Geórgia, mesmo não sendo direcionados para alvos bélicos, os ataques causaram efeitos psicológicos e barreiras à informação relevantes para as tropas e para a sociedade. A estratégia de manter os ataques sem responsabilidades oficiais é importante para proporcionar aos Estados parcerias com hackers e organizações criminosas. Convenientemente, ao invés do governo, esses grupos podem praticar os ataques e, se descobertos, levam a culpa, isentando o comando governamental. No caso da Rússia, esta alegou inúmeras vezes que os ataques lançados do seu território eram gerados por extremistas étnicos, os quais o governo não poderia controlar, mas mesmo assim se recusou a ajudar na busca, identificação e interrupção do ataque.

Em todos os casos observados, as ações não são oficialmente declaradas e, portanto, enquadram-se como operações encobertas. É possível entender, então, os conflitos cibernéticos como uma ofensiva discreta para alcançar fins que não poderiam ser obtidos por outros meios. Até mesmo porque, ainda que os ataques tradicionais vez ou outra sejam utilizados, a guerra convencional é cada vez mais depreciada moralmente e a opinião pública internacional é constantemente contra tais ações agressivas. Na mesma medida, um conflito armado aberto torna-se excessivamente arriscado e suscetível de contra-ataque imediato.

Assim sendo, a guerra cibernética surge como uma opção ainda não regulada definidamente pelo direito internacional e, mesmo que o fosse, poderia se apoiar em ações obscuras, seja de forma direta seja através das organizações por procuração. Ainda assim, pode-se afirmar que os métodos e armas utilizadas ainda devem evoluir e tem grande potencial para isso. Para além de uma visão superficial de desentendimentos entre nações ocidentais e orientais, os conflitos cibernéticos “devem ser examinados em um quadro emergente, e ainda cinzento,” sendo “mais um elemento complicador nas já complexas relações internacionais” (ARAUJO JORGE, 2012).

Enfim, após abordar neste capítulo a realidade da guerra cibernética no cenário internacional, iniciando-se pela apresentação dos conceitos e componentes básicos do tema, sem entrar nos pormenores técnicos da informática; depois de descrever suas principais características, fornecendo exemplos de como tais particularidades se manifestam no mundo concreto e apontando visões contrárias e favoráveis à existência da ciberguerra; conferiu-se, então, a cibernética como mais um elemento complicador nos estudos estratégicos e nas relações internacionais e

também como um novo e integrado domínio de conflito através das observações de casos na Sibéria em 1982, na Estônia em 2007, na Geórgia em 2008 e no Irã em 2010. Assim sendo, no próximo capítulo, o foco internacional será posto de lado e analisar-se-á a importância do meio cibernético para o Estado Brasileiro; delimitando as políticas e os órgãos responsáveis em sua formação, atuação e segurança, através de suas visões, políticas e estratégias, culminando na observação de desafios do país no campo cibernético.

4 A CIBERNÉTICA E O ESTADO BRASILEIRO

Após se abordar a realidade da guerra cibernética no cenário internacional, apresentando seus conceitos, componentes e características principais, além de algumas observações de casos que conferem a cibernética como um complicador das já complexas relações internacionais; o presente capítulo pretende analisar a importância do meio cibernético para o Estado Brasileiro, delimitando as políticas, as visões, as estratégias e os órgãos responsáveis em sua formação, culminando na elaboração de desafios para o país no campo cibernético.

Os primeiros relevantes esforços para esse novo ramo da segurança e defesa no país foram iniciados com a Estratégia Nacional de Defesa (END) de 2008, mas o tema já era brevemente tratado anteriormente, sendo esta data o marco mais importante para a pesquisa da atuação brasileira. Ademais, os debates, competências e atribuições estão envoltas sob o Ministério da Defesa, o Gabinete de Segurança Institucional da Presidência da República, a Secretaria de Assuntos Estratégicos e as Forças Armadas do Brasil (FAs), cabendo ao Exército Brasileiro o papel de força líder na condução deste setor.

4.1 A IMPORTÂNCIA E A VISÃO DA CIBERNÉTICA NO BRASIL: POLITIZADO OU SECURITIZADO?

O Brasil é cada vez mais um país de destaque nas relações internacionais. Por isso, vê-se como imprescindível o investimento em segurança nacional. Nesse quesito, encaixa-se a segurança cibernética. Os recentes casos[49] de espionagem de cidadãos, empresas e de chefes de governo brasileiros ressaltam a importância e a vulnerabilidade de seus sistemas. Além do mais, os próximos grandes eventos que devem ocorrer no país, como a Copa do Mundo e as Olimpíadas (entre outros), serviram como impulsionadores na criação de órgãos e políticas concernentes ao tema, como o Centro de Defesa Cibernética do Exército (CDCiber) e a Política Cibernética de Defesa (BRASIL, 2012b), visando a investigação de protestos sociais

[49] Ver (i) http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html; (ii) http://www1.folha.uol.com.br/mundo/2013/09/1335522-dilma-foi-espionada-pelos-eua-diz-tv.shtml; (iii) http://www1.folha.uol.com.br/mundo/2013/09/1339008-petrobras-foi-alvo-de-espionagem-de-agencia-dos-eua-afirma-programa-de-tv.shtml; Acesso em 03 fev. 2014.

internos e possíveis ameaças terroristas[50], além de preocupar-se com o aumento da proteção de dados confidenciais e de infraestrutura crítica.

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança para a Internet Brasileira (CERT.br)[51] , o Brasil possuí o maior número de internautas da América Latina, cerca de 50 milhões. Em 2013, o CERT.br recebeu notificações de 352.925 tipos de ataques no país, número que chegou a alcançar 466.029 em 2012. Comparando-se com o relatório de 2002, quando se reportou pouco mais de 25.000 ataques, os incidentes cibernéticos tiveram um aumento superior a 1.800% em uma década. Isso demonstra o crescimento vertiginoso não só de usuários de internet no país como também na quantidade e diversificação dos ataques virtuais. Ainda de acordo com as estatísticas de 2013, os incidentes reportados partiram majoritariamente de dentro do território nacional (61%), seguido por EUA (12%) e, depois, China (7%).

Em 2011, os incidentes reportados pelo Centro tinham como alvo, preferencialmente, empresas privadas e bancos. Já nos anos seguintes, os ataques estenderam-se para sites e sistemas governamentais, entre eles, os sites da Presidência da República e da Receita Federal. Essa situação revela uma potencial preocupação com a fragilidade do sistema de segurança cibernética do governo brasileiro. Por exemplo, um ataque que paralisasse o site da Receita Federal as vésperas do prazo de entrega das declarações de imposto de renda do cidadão brasileiro, poderia trazer grandes prejuízos tanto para o governo quanto para o cidadão. Assim:

> "a preocupação tanto com os conteúdos quanto com o tipo de uso, e a respectiva segurança da Internet, crescem em igual medida aos desenvolvimentos tecnológicos e ao número de usuários, observados, especialmente, ao longo dos últimos anos" (BRASIL, 2010b, p.31).

[50]O Brasil não possui, ainda, uma tipificação do crime de terrorismo. No entanto, diante dos grandes eventos que estão por vir no país, como Copa do Mundo e Olimpíadas, tramita no Congresso Nacional brasileiro desde meados de 2013 uma proposta para enquadrar o terrorismo, de maneira ampla, como ações que provoquem pânico generalizado, praticadas por motivos religiosos, ideológicos, políticos e de preconceito racial. Disponível em: http://www1.folha.uol.com.br/cotidiano/2013/06/1294541-congresso-comeca-a-discutir-tipificacao-do-crime-de-terrorismo.shtml. Acesso em 21 jan. 2014.

[51]O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato. Seus dados estatísticos estão disponíveis em: http://www.cert.br/. Acesso em: 02 mai. 2014.

Portanto, faz-se necessário uma categorização e tipificação das várias formas de conflito no ciberespaço, das possíveis vulnerabilidades, das ameaças e de suas fontes, "para que sejam alocadas responsabilidades aos cidadãos, ao Estado; sejam estabelecidas contramedidas e investigações criminais" (DUNN, 2010, p.1, tradução nossa). Conforme se apontou no primeiro capítulo, de acordo com Buzan et al (1998), dependendo de como se enquadra uma questão, as respostas a ela irão variar. Assim, quanto mais securitizado for um evento social, mais excepcional e extremo podem ser as respostas governamentais a ele. Tratar da mesma forma o ativismo, os crimes, o terrorismo e os atos de guerra cibernéticos seria um erro. Por isso mesmo, o Guia de Referência para a Segurança das Infraestruturas críticas da Informação (BRASIL, 2010a, p.129-139) conceitua e determina tais elementos.

Ainda que se posso afirmar que o tema não foi securitizado plenamente no Brasil, pode-se dizer que a cibernética é objeto de preocupação no âmbito da segurança e da defesa. Nesse caso, a hipersecuritização (securitização) de Hansen e Nissenbaum (2009) ainda é um processo em construção, estando localizado mais no âmbito das práticas de segurança diárias (politizado). Assim, a cibernética tem sido uma área priorizada recentemente pelo governo brasileiro, notando-se isso especialmente pelo que afirma Celso Amorim, ex-ministro das Relações Exteriores do Brasil e atual ministro da Defesa:

> "Ao contrário de cem anos atrás, tempo do Barão do Rio Branco, quando o Brasil comprava do exterior praticamente todos seus principais equipamentos de defesa sem a capacidade de nacionalizar sua produção, hoje o desenvolvimento de capacidades autônomas na indústria de defesa é um objetivo fundamental de nossa política. A Estratégia Nacional de Defesa, cuja segunda edição foi lançada no ano passado e agora acaba de ser apreciada pelo Congresso Nacional, define três áreas prioritárias desse esforço: a nuclear, a **cibernética** e a espacial" (AMORIM, 2013, p.308-309, grifo nosso).

Da mesma forma, o general do Exército Brasileiro e atual comandante do Centro de Defesa Cibernética no Brasil José Carlos dos Santos, em entrevista para a revista Época, ao ser perguntado se a cibernética será um novo campo das Forças Armadas, afirmou:

> "É uma nova governança. Eu diria que diversos países estão na mesma situação. Os Estados Unidos criaram seu comando cibernético em 2009. A Alemanha ativou seu centro de defesa cibernética neste ano, a Inglaterra no ano passado. O Brasil criou o Centro de Defesa Cibernética em agosto do ano passado. Essa era digital é um contexto novo. [...] Podemos, sim, contratar civis. Está dentro de nossas previsões a contratação de especialistas em regime de prestação de serviços. Basicamente estamos cuidando da formação do nosso pessoal. A partir de 2012, a matéria

> tecnologia para informação e comunicação se tornará obrigatória para todos os nossos futuros oficiais. Nas escolas de formação dos nossos sargentos, o assunto também será introduzido. É uma possibilidade contratar [hackers]. A imprensa diz que os Estados Unidos já fazem isso. Eles teriam até um grupo de hackers que trabalharia em prol do governo americano. Eles não se identificam como tal, mas trabalham. [No Brasil] São registrados milhares de incidentes de rede por dia. Logicamente um porcentual desses incidentes é de tentativas de intrusão em serviços internos do Exército. Recentemente, tivemos no Recife uma intrusão num serviço social, de distribuição de água. Um grupo, o FatalErrorCrew, conseguiu acessar um banco de dados dessa operação. Foi dado crítico? Bom, crítico, não. Mas mostrou uma vulnerabilidade. Eram dados de militares vinculados àquela operação" (SANTOS, 2011).

Dessa forma, percebe-se que no âmbito militar brasileiro há uma clara preocupação com a defesa e segurança cibernética dos sistemas virtuais e de infraestrutura do país, em especial aqueles ligados ao exército. A política adotada pelas Forças Armadas brasileiras é a de defesa-ativa, não buscando atacar outras nações, seguindo a linha pacifista histórica de posicionamento, visando primordialmente proteger os próprios sistemas e neutralizar possíveis ataques e intrusões.

Levando-se em consideração a elaboração de Buzan et al (1998), referente a categorização do tratamento de questões públicas – conforme visto no primeiro capítulo – podemos dividir o tratamento da segurança cibernética pelo Brasil em três etapas: até os anos 2000 (não politizado); na primeira metade dos anos 2000 (politizado) e a partir de 2008 (em processo de securitização).

Até o início do século XXI não foram criados documentos relevantes concernentes ao tema e nem debates ou preocupações quanto aos riscos e vulnerabilidades foram notados. Certamente, pelo fato da cibernética e seus elementos ainda estarem em processo de formação e evolução, juntamente com as TICs. A partir de então, conforme o Estado percebe a necessidade e importância de tal tecnologia, há uma institucionalização da questão, designação de capacidades e demarcação de conceitos.

Então, no ano 2000, tem-se o marco inicial do processo de politização do tema com o livro verde Sociedade da Informação no Brasil (BRASIL, 2000), do Ministério da Ciência e Tecnologia. O livro representa uma visão mais ampla para estabelecer "contornos e diretrizes de um programa de ações rumo à Sociedade da Informação no Brasil" (BRASIL, 2000, p.xv). O programa versa sobre as oportunidades e os riscos de uma sociedade em rede e informatizada; sobre economia, trabalho e comércio eletrônico; sobre universalização dos serviços de

internet como forma de cidadania; sobre como a informatização auxilia a educação; sobre transparência governamental para colocar o "governo ao alcance de todos"; além de abordar questões mais específicas de P&D e infraestrutura avançada. Basicamente, definem-se conceitos ligados a informática e propõem-se projetos de disseminação da internet pelo território nacional.

Em termos de segurança cibernética (até então denominado segurança da informação), no mesmo ano, o governo publicou o decreto 3.505 de 13 de junho de 2000[52], instituindo a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal. Aqui, percebe-se claramente a definição de pressupostos básicos, conceituações, objetivos, diretrizes, alocação de recursos e de responsabilidades. Principalmente, a legislação federal instituiu o Comitê Gestor da Segurança da Informação (CGSI), o qual serve de assessor e é subordinado à Secretaria-Executiva do Conselho de Defesa Nacional. Portanto, nota-se uma preocupação inicial com a segurança da informação do Estado.

Em seguida, através da lei federal 10.683 de 28 de maio de 2003[53], criou-se o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o qual tem como uma de suas competências coordenar as atividades de inteligência federal e de segurança da informação. O GSI/PR passou por diversas revisões de funções e atividades, tendo sido atualizado pela última vez com o Decreto 8.100 de 04 de setembro de 2013[54], sendo considerado por tal decreto órgão "essencial da Presidência da República".

Ainda, da estrutura do GSI/PR destacam-se dois órgãos "cujas atividades por eles desenvolvidas inserem-se no esforço de construção de estratégia da segurança cibernética" (MANDARIJO JR. 2009. p.104). Primeiramente, o Decreto Presidencial 5.772 de 8 de maio de 2006[55] criou o Departamento de Segurança da Informação e Comunicações (DSIC), com o objetivo de exercer exatamente as atividades de segurança da informação. O segundo órgão é a Agência Brasileira de Inteligência (ABIN), o qual atua nas vertentes de inteligência e contra inteligência em

[52]Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm. Acesso em 03 mai. 2014.
[53]Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2003/L10.683.htm. Acesso em 03 mai. 2014.
[54]Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8100.htm#art8. Acesso em 03 mai. 2014.
[55]Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Decreto/D5772.htm. Acesso em 03 mai. 2014.

prol do Estado, tendo como função, entre outras, “avaliar as ameaças internas e externas à ordem constitucional”[56].

Ademais, outros órgãos criados serviram para potencializar o surgimento da segurança cibernética, quais sejam o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC), o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Publica Federal (CTIR.gov), o Comitê Gestor da Internet (CGI), o Núcleo de Informação e Coordenação do Ponto BR (Nic.br) – este último mantendo também o já citado CERT.br –, o Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC.br) e o Centro de Estudos e Pesquisas em Tecnologias de Rede e Operações (CEPTRO.br), entre outros.

Assim sendo, até 2005, há um processo de politização do tema da segurança cibernética – inicialmente tecnicamente entendido como segurança da informação –, com a criação de órgãos, documentos oficiais, discussões, centros de estudos, determinação de recursos, etc. Portanto, o tema ainda não era visto como uma ameaça existencial propriamente dita, mas apenas um objeto de preocupação inicial e de discussão/debate político. A partir dessa data, há um processo de entendimento da cibernética como uma ameaça, se não plenamente existencial ao menos potencialmente existente e, portanto, em construção da securitização.

Nesse sentido, a Política de Defesa Nacional (BRASIL, 2005) menciona brevemente o tema em duas seções. Dessa forma, tem-se as primeiras citações diretas referentes a um ataque cibernético:

> “6.19 Para minimizar os danos de possível **ataque cibernético**, é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento. [...] XII - aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra **ataques cibernéticos** e, se for o caso, permitam seu pronto restabelecimento” (BRASIL, 2005, grifo nosso).

A partir de então, há uma maior produção de documentos legais brasileiros os quais tentam instigar o debate público de Defesa Nacional, incluindo então a segurança cibernética. Tais documentos serão melhor examinados na próxima seção, sendo eles o Glossário Militar das Forças Armadas de 2007, as Estratégias Nacionais de Defesa (END) de 2008 e 2012, o Guia de Referência para a Segurança

[56]Disponível na Lei 9.883 de 07 de dezembro de 1999.
Ver: http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm. Acesso em 03 mai. 2014.

das Infraestruturas Críticas da Informação de 2010, o Livre Verde: segurança cibernética no Brasil de 2010, o relatório Desafios Estratégicos para a Segurança e Defesa Cibernética de 2011, o Livro Branco de Defesa Nacional de 2012 e a Política Cibernética de Defesa de 2012. O que se faz a seguir é mostrar que o Estado brasileiro percebe a potencialidade e os riscos de ataques cibernéticos às infraestruturas críticas e da informação no país, alocando publicamente espaços em documentos legais que promovem a discussão e crescimento da importância do tema, tendo o Gabinete de Segurança Institucional da Presidência da República e o Exército Brasileiro como órgãos principais de atuação no setor cibernético.

4.2 RESPONSABILIDADES, POLÍTICAS E ESTRATÉGIAS CIBERNÉTICAS DO BRASIL

Primeiramente, vale ressaltar uma diferença descrita no Glossário das Forcas Armadas (BRASIL, 2007) entre defesa e segurança para, então, fazer sua aplicação e estruturação no ambiente cibernético brasileiro. O termo defesa é entendido como "o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança" (BRASIL, 2007, p.76), ou ainda, como uma "reação contra qualquer ataque ou agressão real ou iminente" (" (BRASIL, 2007, p.76). Por sua vez, segurança é colocada como uma:

> "1-Condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais. 2-Sentimento de garantia necessária e indispensável a uma sociedade e a cada um dos seus integrantes, contra ameaças de qualquer natureza. Condição que resulta do estabelecimento e conservação de medidas de proteção que assegurem um estado de inviolabilidade contra atos ou influências hostis" (BRASIL, 2007, p.235).

No nível cibernético, para Mandarino Jr. (2009, p.98), a segurança cibernética contempla ações que compreendem aspectos e atitudes tanto preventivas quanto repressivas, enquanto defesa cibernética refere-se a ações operacionais, de caráter ofensivo, caracterizadas por ataques cibernéticos. No entanto, apesar de algumas diferenças conceituais, não se pode isolar completamente um conceito do outro. Existe uma interligação de atribuições em relação ao setor cibernético que demanda atuação tanto em nível de defesa quanto no de segurança, haja vista que no meio cibernético a origem é de difícil determinação, os meios utilizados e os danos prováveis de um ataque podem atingir

tanto sistemas militares como também serviços públicos da sociedade. Nesse sentido, o Ministro da Defesa, Celso Amorim, em discurso de abertura no terceiro Seminário de Defesa Cibernética em outubro de 2012 pronunciou-se da seguinte maneira:

> "Não tenho dúvidas, por exemplo, de que a proteção de estruturas críticas do país – usinas hidroelétricas, linhas de transmissão, bases de dados do sistema financeiro, para não falar dos próprios meios das Forças Armadas – pertencem à Defesa. A identificação e perseguição de hackers ou crackers é tarefa da Segurança [pública]. Mas há áreas cinzentas entre uma e outra" (AMORIM, 2012).

Dessa forma, no Brasil, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e o Ministério da Defesa (MD) – acompanhados ainda pela Secretaria de Assuntos Estratégicos, pela Marinha do Brasil, pela Força Aérea Brasileira e, principalmente, pelo Exército Brasileiro – veem conduzindo as políticas, debates públicos e projetos do setor cibernético para o país. No tocante à segurança pública, a identificação de hackers em território nacional, por exemplo, ficam sob responsabilidade da Polícia Federal (PF) – subordinada ao Ministério da Justiça –, como atributos de crime comum. Ou seja, a PF estaria encarregada por ações de prevenção de incidentes e de repressão também no âmbito cibernético. No entanto, se levarmos em consideração a participação do Exército nas ações de segurança cibernética em grandes eventos que ocorreram no país, tais quais a Conferência Rio+20 em 2012, Copa das Confederações em 2013 e Copa do Mundo em 2014, notamos claramente essa mistura de atribuição de funções em operações "não guerra" designadas ao Exército.

Dessa forma, o GSI/PR e o MD destacam-se na construção de um ambiente politizado que caminha para a securitização acerca da cibernética, tornando-se os líderes na elaboração das diretrizes para esse setor. Nesse sentido, o GSI/PR tem como uma de suas funções coordenar a inteligência e a segurança da informação, transformando-o na engrenagem principal para a organização da estratégia da segurança cibernética no país (MANJARINO JR., 2009). Da estrutura do GSI/PR, destacam-se o DSIC e a ABIN.

O DSIC tem como atribuições, entre outras, regulamentar a segurança da informação e comunicações para toda a Administração Pública Federal (APF), realizar acordos internacionais de troca de informações sigilosas, ser o ponto de contato com a Organização dos Estados Americanos para assuntos de terrorismo cibernético e manter o centro de tratamento e resposta a incidentes nas redes de

computadores da APF. A ABIN atua nas tarefas de inteligência, por meio da produção de conhecimentos sobre fatos e situações de imediata ou potencial influência no processo decisório, na ação governamental, sobre a salvaguarda e sobre a segurança da sociedade e do Estado; e nas atividades de contra inteligência pela adoção de medidas que protejam os assuntos sigilosos relevantes para o Estado e a sociedade e que neutralizem ações de inteligência executadas em benefício de interesses estrangeiros.

A construção da securitização cibernética não ocorre tão somente por documentos legais e criação de órgãos da APF, mas também por meio de discursos públicos. Primeiramente, durante a 68ª Assembleia Geral das Nações Unidas, em discurso de abertura, a presidente do Brasil Dilma Rousseff proferiu as seguintes palavras:

> "As tecnologias de telecomunicação e informação não podem ser o novo campo de batalha entre os Estados. Este é o momento de criarmos as condições para evitar que o espaço cibernético seja instrumentalizado como arma de guerra, por meio da espionagem, da sabotagem, dos ataques contra sistemas e infraestrutura de outros países" (BRASIL, 2013).

Percebe-se, nesse caso, a conclamação internacional para a construção de uma governança global da internet e uma real preocupação com os riscos de um ataque cibernético, especialmente quando coloca os sistemas e infraestruturas como objetos de referência e, portanto, como algo existencialmente ameaçado. O discurso da presidente ainda demonstrou preocupação com a privacidade e os dados pessoais dos cidadãos brasileiros, alvo de espionagem pela agência americana National Security Agency (NSA) em 2013, colocando, então, também a sociedade brasileira como um objeto referencial.

Ademais, em 2014, foi aprovado o Marco Civil da Internet[57], projeto que estava trancado desde sua criação em 2009. Ainda que não tenha propriamente fins de defesa ou segurança nacional, a lei regula a utilização da internet no país, prevendo princípios, garantias, direitos, responsabilidades e deveres para usuários e empresas, tratando de neutralidade, privacidade, retenção de informações e dados, entre outros. Portanto, esse marco civil representa uma importante maior regulamentação interna e, igualmente, uma abertura ainda maior da discussão do tema para a sociedade.

[57]Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=912989&filename=PL@126/201. Acesso em 06 mai. 2014.

Ainda, na apresentação do Livro Verde: segurança cibernética no Brasil (BRASIL, 2010b), o então Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República, Jorge Armando Felix, não só apregoa a necessidade de garantir a segurança nacional, como também proclama a formulação de uma Política Nacional de Segurança Cibernética, expressando o tema como uma ameaça à segurança estatal:

> "Assim, motivado por esta missão e considerando a necessidade de assegurar dentro do espaço cibernético ações de segurança da informação e comunicações como fundamentais para a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação; a possibilidade real e crescente de uso dos meios computacionais para ações ofensivas por meio da penetração nas redes de computadores de setores estratégicos para a nação; e o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade; foi instituído Grupo Técnico para estudo e análise de matérias relacionadas à Segurança Cibernética. [...] Recomendo, portanto, a leitura desta obra, cuja publicação considero significativo incremento no arcabouço de documentos que objetivam garantir a Segurança Nacional, e convido-os a contribuir com propostas e sugestões para a evolução da mesma, visando formular, colaborativamente, à Política Nacional de Segurança Cibernética" (BRASIL, 2010b, p.5-6).

Ao final de suas palavras, ainda se percebe um chamamento à audiência pública para que participe e contribua com propostas e sugestões, levando o tema mais uma vez para a esfera da sociedade.

Em relação ao papel do MD, num primeiro momento, o Exército Brasileiro foi designado para conduzir o setor cibernético no país. No entanto, há previsão para a criação de um Comando de Defesa Cibernética das Forças Armadas – como acontece nos EUA com a USCYBERCOM[58] – no qual Exército, Marinha e Força Aérea trabalhariam integradamente. Mas por que motivos o MD atribuiu ao Exército Brasileiro a competência desse setor?

Primeiramente, é importante analisar a END de 2008, em que os primeiros esforços com viés político-estratégico foram feitos com relação ao setor cibernético. Segundo a respectiva estratégia, "o Ministério da Defesa e as Forças Armadas intensificarão as parcerias estratégicas nas áreas cibernética, espacial e nuclear" (BRASIL, 2008), colocando particular ênfase no "aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos" (BRASIL, 2008). Nota-se pelo documento, portanto, que a cibernética é colocada pela primeira vez como

[58]A USCYBERCOM é o Comando Cibernético dos Estados Unidos, subordinado ao Comando Estratégico do país, e tem como função primordial proteger a rede de computadores militar americana. Disponível em http://www.arcyber.army.mil/org-uscc.html. Acesso em 11 jun. 2014.

um setor decisivo para a conservação do país ao alegar que os "três setores estratégicos – o espacial, o **cibernético** e o nuclear – são essenciais para a defesa nacional" (BRASIL, 2008, grifo nosso). Contudo, o documento não atribuiu especificamente ao Exército a autoridade de ação nesse setor, estando 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).

Mesmo assim, como consequência da END de 2008, em 9 de novembro de 2009, o MD, por meio da Diretriz Ministerial 14, determinou as responsabilidades de coordenação e integração do setor cibernético ao Exército Brasileiro, no âmbito das Forças Armadas. Enquanto isso, o campo espacial ficou sob responsabilidade da Aeronáutica e o nuclear da Marinha. Como fruto dessa designação, o Exército projetou, além da instalação e ativação do Núcleo de Defesa Cibernética (NDCiber), também a criação do Centro de Defesa Cibernética (CDCiber), o qual já foi aprovado por decreto presidencial através da Portaria Nº 666, de 4 de Agosto de 2010[59].

O CDCiber, primeiramente, foi criado para a defesa de redes em grandes eventos, tendo seu primeiro teste na Conferência Rio+20, seguida pela Copa das Confederações em 2013 e Copa do Mundo em 2014. A partir de então, o Centro deve ganhar maior expertise e atuação ampla, podendo apoiar também instituições que trabalham com a internet no país, mantendo a rede mais segura de forma geral. Dessa forma, o Centro poderá contribuir na elevação da segurança e da capacidade de atuação em rede tanto na área militar quanto em diferentes setores do governo e da sociedade.

Em seguida, em 2010, foi lançado o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (BRASIL, 2010a), elaborado e organizado por especialistas de 13 órgãos da APF[60], propondo como objetivos gerais: (i) levantar e avaliar as potenciais vulnerabilidades e riscos que possam vir a afetar a segurança das infraestruturas críticas, identificando e monitorando suas interdependências; (ii) propor, articular e acompanhar medidas necessárias das infraestruturas; (iii) - estudar, propor e acompanhar a implementação de um sistema de informações com dados atualizados das infraestruturas; e, (iv) pesquisar e propor

[59]Disponível em: http://www.defesanet.com.br/cyberwar/noticia/1633/cdciber---portaria-de-criacao-do-centro-de-defesa-cibernetica-do-exercito. Acesso em 10 Dez. 2013.
[60]Quais sejam: "GSIPR/DSIC; Casa Civil/PR; Ministério da Defesa; Ministério das Relações Exteriores; Ministério da Saúde; Ministério do Planejamento, Orçamento e Gestão; Ministério da Ciência e Tecnologia; Banco Central do Brasil; Banco do Brasil; Caixa Econômica Federal; SERPRO, PETROBRÁS, e DATAPREV. (BRASIL, 2010a, p.20).

um método de identificação de alertas e ameaças da segurança de infraestruturas críticas da informação. Nesse caso, percebe-se novamente uma preocupação extremada com as infraestruturas críticas do país, colocando-as como uma ameaça existencial.

No mesmo ano do Guia, foi lançado o Livro Verde: Segurança Cibernética no Brasil (BRASIL, 2010b) o qual apresenta uma breve visão do país no que se refere às oportunidades e aos desafios em termos político-estratégicos, econômicos, sociais e ambientais, ciência, tecnologia e inovação, educação, legalidade, cooperação internacional, e segurança das infraestruturas críticas, tendo como foco central a segurança cibernética. Além do mais, contém diretrizes estratégicas para formulação de uma possível futura Política Nacional de Segurança Cibernética para o país (BRASIL, 2010b, p. 17,33).

Mais tarde, em 2012, é elaborado o documento que pela primeira vez aloca publicamente recursos para o setor cibernético. O Livro Branco de Defesa Nacional (BRASIL, 2012a) – que, apesar de aprovado na Câmara dos Deputados e no Senado, mas ainda não sancionado, é documento disponível no site do governo brasileiro – trata a cibernética como um desafio, denominando-a com um tipo de "conflito do futuro" (BRASIL, 2012a, p.28), e coloca a defesa cibernética propriamente como um novo tema no plano internacional. O livro também mira as infraestruturas do país como ameaça existencial ao afirmar que a "ameaça cibernética tornou-se uma preocupação por colocar em risco a integridade de infraestruturas [...] essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional" (BRASIL, 2012a, p.69).

O documento supracitado ainda defende que a proteção do espaço cibernético abrange variadas áreas, desde capacitação, inteligência, pesquisa científica, preparo e emprego operacional e gestão de pessoal até a proteção dos próprios ativos e capacidade de atuação em rede. Os projetos apresentados representam esforços de longo prazo, mas também são listadas ações de curto prazo como a construção da sede definitiva do CDCiber (já finalizada), a aquisição de infraestrutura de apoio, de equipamentos, de hardwares e softwares de defesa cibernética e capacitação de recursos humanos. A conclusão de todos os projetos de defesa cibernética existentes no Guia é prevista para 2035, com valor estimado em R$839 milhões (BRASIL, 2012a, p.200).

Sob a coordenação do Exército, expressivos avanços têm se realizado na capacitação de pessoal especializado e no desenvolvimento de soluções de alto nível tecnológico. Grande parte dos conceitos relacionados ao setor, assim como seminários, palestras, cursos de especialização e eventos partem de iniciativa desta Força. Há ainda, muito a ser produzido e organizado, inclusive dentro do Exército Brasileiro, mas a questão principal de preocupação atualmente é colocar em prática os esforços para o que chamam de defesa cibernética, termo que parece ser o preferido pelo Estado Brasileiro como forma de manifestação não bélica, seguindo sempre a linha pacifista histórica do país.

Outra publicação importante concernente ao tema em âmbito brasileiro foi a Política Cibernética de Defesa de 2012. A finalidade da Política é nortear "as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos" (BRASIL, 2012b). Esse documento solidifica o entendimento acerca das possibilidades e dos limites da atuação cibernética brasileira, tendo em vista a sensibilidade que esse espaço e ferramenta de poder possui. Mais uma vez, para além da atuação do MD, a audiência pública é chamada para colaborar com processo de construção do setor cibernético:

> "a) a eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa;" (BRASIL, 2012b).

Ainda, percebe-se uma preocupação na capacitação, agregação e gestão de pessoal, confirmando a potencial contratação de hackers, profissionais e especialistas em segurança da informação e comunicação proferida em trecho de entrevista apresentada anteriormente pelo Comandante José Carlos dos Santos (SANTOS, 2011) quando expõe como um de seus variados objetivos o de "capacitar e gerir talentos humanos necessários à condução das atividades do Setor Cibernético (St Ciber) no âmbito do MD" (BRASIL, 2012b);

Ademais, o documento cria o Sistema Militar de Defesa Cibernética (SMDC), órgão militar com o intuito de prevenir ataques aos sistemas de informática de todo o Brasil, o qual é coordenado pelo Estado-Maior das Forças Armadas, conforme segue:

> "O Estado-Maior Conjunto das Forças Armadas (EMCFA) é o órgão responsável por assessorar o Ministro de Estado da Defesa na

> implementação e gestão do SMDC, visando a garantir, no âmbito da Defesa, a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança desejados" (BRASIL, 2012b).

Dessa forma, o país insere-se no modelo de gestão cibernética das grandes potências, ainda que apenas inicialmente. Por enquanto, o objetivo é cuidar somente dos computadores vinculados ao Exército, mas a intenção futura é atuar na prevenção de ataques à completa rede informática de atuação estratégica brasileira. Objetivo ainda distante, que depende de investimentos e reconhecimento maiores, mas que parece ser possível de ser alcançado no longo prazo.

Por fim, tem-se a Estratégia Nacional de Defesa de 2012. Assim como o Livro Branco, a END 2012 não recebeu a sanção presidencial, mas é tida para fins do trabalho como documento importante, o qual também está disponível no site do governo brasileiro. Sendo uma atualização da END 2008, o último documento possui alguns pontos atualizados importantes que merecem ser citados.

Primeiramente, nessa nova estratégia o setor cibernético adquire uma seção exclusiva para apontamento de prioridades. Uma delas é expandir o CDCiber, comandado pelo Exército, para um comando maior de atuação integrada das Forças Armadas, ao afirmar que se deve "fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas" (BRASIL, 2012c). Outra prioridade é conduzir o tema para o debate acadêmico ao propor a necessidade de "fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional" (BRASIL, 2012c). Inclusive, neste ponto, propõe-se um estudo conjunto entre Ministros, Secretários e GSI/PR com vistas a "criação da Escola Nacional de Defesa Cibernética" (BRASIL, 2012c).

Ainda, a Estratégia de 2012 proclama a independência nacional de capacitação tecnológica autônoma, incluindo os setores espacial, cibernético e nuclear. Dessa forma, o país pretende desprender-se de tecnologia estrangeira. Essa preocupação pode ser notada após os casos de espionagem de cidadãos e chefes de governo já citados anteriormente, quando a presidente Dilma Rousseff anunciou ter determinado ao Serviço Federal de Processamento de Dados a

implantação de um sistema seguro de e-mail em todo o governo federal[61], além da projeção de criação de um Sistema Nacional de Segurança Cibernética próprio.

Uma das consequências das revelações de espionagem da NSA para com o Brasil foi o adiamento – ou cancelamento, haja vista que não se marcou oficialmente outra data – da visita da presidente brasileira a Washington em 2013, decisão que gerou certo constrangimento diplomático entre os países. No entanto, tal constrangimento já parece estar terminando por conta da visita do vice-presidente norte-americano Joe Biden ao Brasil durante os jogos da Copa do Mundo de 2014 a fim de estreitar relações bilaterais e reconstruir a confiança[62] entre os dois governos.

Ainda referente à prioridade de capacitação tecnológica autônoma, em entrevista ao jornal Correio Braziliense, o ministro da Defesa Celso Amorim expressou sua preocupação com a importação de tecnologia referente ao setor cibernético ao afirmar que:

> "Hoje, a tendência é comprar softwares importados, mas eles não vão garantir nossa defesa. Precisamos desenvolver tecnologia brasileira. Isso leva tempo, demanda investimentos, formação de pessoal e mudança de cultura. As pessoas acham mais fácil trabalhar com o que já existe, já conhecem. Mas, quando se trata da defesa e das redes do governo, só a tecnologia nacional pode garantir segurança máxima. Veja o caso da criptografia. Ela depende de um componente, o gerador de chaves, que é importado. E ele pode ser sabotado" (CORREIO BRAZILIENSE, 2013).

Por último, tanto a END de 2008 quanto a END de 2012 proclamam o intercâmbio militar – incluindo então o setor cibernético – com as Forças Armadas de nações amigas, particularmente com a América do Sul como forma de integração regional. Existem iniciativas nesse sentido, podendo ser citada a cooperação entre Brasil e Argentina, em matéria de defesa cibernética através do comunicado da reunião dos Ministros Celso Amorim e Arturo Puricelli[63], respectivamente.

Enfim, no campo da segurança cibernética, as ações ganharam maior investida a partir da criação do DSIC no GSI/PR, em 2006, e no campo da Defesa Cibernética, destaque maior passou a ser dado através da elaboração da END, em 2008. Os documentos referidos neste trabalho, acompanhados pela criação e

---

[61]MORAES, Maurício. Espionagem abre discussão sobre preparo do Brasil para uma guerra cibernética. *BBC Brasil.* São Paulo. Out. 2013. Disponível em: http://www.bbc.co.uk/portuguese/noticias/2013/10/131011_defesa_seguranca_cibernetica_brasil_mm.shtml. Acesso em 11 jun. 2014.

[62]ROMEIRO, Simon. Diplomacy and Soccer for Biden in Brazil. *New York Times.* p.A6. Jun. 2014. http://www.nytimes.com/2014/06/17/world/americas/for-biden-in-brazil-world-cup-and-diplomacy.html>?_r=0. Acesso em 21 jun. 2014.

[63]Disponível em http://www.defesanet.com.br/defesa/noticia/5668/brasil-argentina---comunicado-conjunto. Acesso em 11 jun. 2014.

atuação de órgãos estatais – no qual o GSI/PR e o MD possuem papel imprescindível – e pela atribuição de competências no que tange a segurança e defesa cibernéticas – nesse caso, destacando o Exército Brasileiro –, podem ser encarados como uma sistematização do processo de formação de ameaças existências no setor cibernético.

Na mesma medida, os breves discursos apresentados podem ser vistos como uma forma de alcançar a legitimação da população e a aceitação pública em busca da securitização, haja vista que seu processo torna-se mais aceitável em virtude da associação entre possíveis ataques cibernéticos em âmbito nacional com os ocorridos diariamente como crime comum. Portanto, conforme apontou Buzan e Hansen (2012, p.366), a segurança não é uma condição objetiva, mas sim um discurso que constitui identidades e ameaças. Nesse caso, parece claro o desenvolvimento, ainda que em prosseguimento, das identidades e ameaças cibernéticas, levando a uma securitização ainda incompleta do setor no país. Na seção que segue, serão apresentados alguns desafios e obstáculos para o desenvolvimento do campo cibernético no Brasil.

4.3 DESÁFIOS E OBSTÁCULOS NO CAMPO CIBERNÉTICO BRASILEIRO

Como foi possível perceber, existe no Brasil uma estrutura basilar pronta para atuar nas áreas de segurança e defesa cibernéticas. No entanto, ainda é superficial perante os desafios internacionais que se apresentam. Por isso, aliado ao crescimento das discussões e dos casos já citados referentes ao tema, o momento presente torna-se propício para acelerar medidas e projetos, aumentar o investimento e capacitação, para fins de formar e organizar um eficiente e amplo Sistema Nacional de Segurança e Defesa Cibernética. No entanto, alguns obstáculos mostram-se como verdadeiros problemas a serem superados para que se alcance esse desenvolvimento.

O primeiro óbice a ser citado é de questão cultural, fazendo referência ao apoio ao setor de defesa de modo geral. Defesa, no Brasil, foi majoritariamente um assunto ignorado ou marginalizado, especialmente entre os civis. Isso por que não se tem popularmente a real importância do que o setor de defesa representa para a nação, seja pelo fato do Brasil construir-se historicamente e diplomaticamente pela base pacifista seja pela hipótese remota de envolvimento intenso em uma guerra,

gerando uma sensação errônea de que não valeria a pena alocar investimentos maciços nessa área.

Agora, expanda essa visão especificamente para o setor cibernético. Se a defesa já seria pouco valorizada pela população, o que dizer de um setor novo e pouco conhecido? Como justificar, portanto, altos investimentos na cibernética quando existiriam no país muitas outras áreas carentes de recursos? Percebe-se através das ENDs que é dado enorme destaque à tecnologia no setor cibernético. Conforme aponta Bertonha (2009):

> "O papel da tecnologia tem sido, no último século e ainda mais hoje, fundamental para garantir a eficiência militar, e qualquer programa de defesa nacional que não contemple esses requisitos seria inócuo. [a END] enfatiza a todo instante essa necessidade e esse é um ponto forte do mesmo, indicando como seus elaboradores entenderam para onde caminha a guerra no século XXI" (BERTONHA, 2009, p.24).

No entanto, deve-se dispor de investimentos não somente em tecnologia, ainda que este seja um fator preponderante, mas também em recursos humanos, capacitação e operacionalização. É preciso compreender que investir em defesa não significa deixar de lado a linha pacifista brasileira, mas sim de que defesa nacional é um requisito fundamental para a ascensão econômica e política do país, evitando, dessa forma, ameaças à soberania, às riquezas e a segurança do Estado. Por isso, cada vez mais, defesa nacional e defesa/segurança cibernética devem ser temas de debate público para que se crie a devida consciência perante tão significativos temas.

Aliado a esta questão cultural, encontra-se um óbice no direito fundamental da pessoa, qual seja a privacidade. Nesse sentido, a discussão privacidade versus segurança ganhou destaque atualmente. Associam-se as atividades cibernéticas referentes à segurança e monitoramento a ações ilícitas de intrusão particular e de quebra de privacidade. Como separar essas questões haja vista que uma delas ultrapassa quase que obrigatoriamente os limites da outra? Por exemplo, se citarmos a China e a Coreia do Norte, países onde a liberdade e privacidade são restringidas, a segurança tem papel prioritário, mais por obrigação do que por possibilidade de escolha dos cidadãos. Nos EUA, com os recentes casos de espionagem da NSA de cidadãos norte-americanos e também de outras

nacionalidades tal debate ganhou força[64], pendente igualmente mais para o lado da segurança, muito em conta pelos diversos ataques terroristas ocorridos no país na última década.

No Brasil, a visão parece ser diferente. Nesse caso, retornamos ao primeiro obstáculo citado. A marginalização da questão defesa/segurança faz colocar a privacidade como um direito superior, tornando-se então, mais complicado o investimento maciço em um setor que pode ser visto superficialmente como de monitoramento e espionagem, como o cibernético, quando na verdade representa uma gama maior de atividades fundamentais à defesa nacional. Assim sendo, em virtude dos dois obstáculos citados anteriormente, percebe-se pouca valorização ou não priorização do setor cibernético na alocação de recursos financeiros, ainda que o Ministro Celso Amorim afirme que "reforços orçamentários razoáveis, embora longe do ideal, foram consignados ao setor" (AMORIM, 2012).

Essa constatação pode ser verificada pelo Livro Branco de Defesa Nacional, em que entre todos os projetos apresentados o de defesa cibernética é o que apresenta o menor valor global estimado (BRASIL, 2012a, p.200). Para ter uma comparação, enquanto se prevê R$839 milhões de gastos no período de 20 anos, nos EUA o valor proposto dentro do orçamento do Departamento de Defesa somente para 2014 é de cerca de R$10,7 bilhões[65], representando quase 3% do orçamento total anual – o que torna a segurança cibernética nos EUA a prioridade maior na área de defesa do país. Portanto, existe uma considerável diferença de investimento entre os países. No Brasil, tal investimento representa apenas 0,5% do total a ser gasto pelo Exército Brasileiro até 2035. Como se isso não bastasse, até a primeira metade do ano de 2013, o país gastou apenas 8,9% do que era previsto para o período com defesa cibernética[66]. Portanto, é imprescindível que seja dada a devida importância ao tema e que tais discussões apareçam cada vez mais

[64]OBAMA sacrifica privacidade dos americanos para manter a segurança**.** *Euronews.* Jun. 2013. Disponível em: http://pt.euronews.com/2013/06/07/obama-sacrifica-privacidade-dos-americanos-para-manter-a-seguranca/. Acesso em 16 jun. 2014.

[65]FLECK, Isabel. Investimento brasileiro para defesa cibernética representa 0,5% de orçamento do Exército para os próximos 20 anos. *Folha de São Paulo.* Folha Mundo. São Paulo. Ago. 2013. Disponível em: http://www1.folha.uol.com.br/mundo/2013/07/1310924-investimento-brasileiro-para-defesa-cibernetica-representa-05-de-orcamento-do-exercito-para-os-proximos-20-anos.shtml. Acesso em 16 jun. 2014.

[66]COSTA, Breno. Brasil gasta só 8,9% do previsto com defesa cibernética. *Folha de São Paulo*. Folha Mundo. Brasília. Ago. 2013. Disponível em: http://www1.folha.uol.com.br/mundo/2013/07/1310921-brasil-gasta-so-89-do-previsto-com-defesa-cibernetica.shtml. Acesso em 16 jun. 2014.

publicamente, para que a escassez de recursos seja revertida no permanente investimento e atuação do setor.

Ademais, o livro Desafios Estratégicos para a Segurança e Defesa Cibernética (BRASIL, 2011) compila artigos elaborados de acordo com as apresentações realizadas durante a reunião técnica sobre segurança e defesa cibernética em dezembro de 2010 em Brasília. A reunião foi organizada pela Secretaria de Assuntos Estratégicos juntamente com o Comando do Exército, buscando proporcionar aos servidores do governo federal conhecimentos sobre o assunto, identificando a atuação exercida pelas Forças Armadas, por instituições estatais e órgãos públicos e privados, entre outros. O livro aborda o setor cibernético em relação ao cenário internacional e sobre tendências globais, mas também foca sua análise em âmbito interno, em prol da formação de um Sistema de Segurança e Defesa Cibernética Nacional. Para fins do presente trabalho, vale ressaltar que foram apresentados desafios para o Brasil no que tange aos seguintes pontos:

> "a formulação de políticas públicas e de marco legal para o uso efetivo do espaço cibernético, especialmente no que concerne à manutenção das infraestruturas críticas do País; o estabelecimento de medidas que contribuam para a gestão da segurança da informação e comunicações e para a produção do conhecimento de inteligência; o estímulo das atividades de pesquisa e desenvolvimento para atender às necessidades do setor; a retenção de talentos; e o estabelecimento do perfil da carreira que deve ser de estado" (BRASIL, 2011, p.10).

Primeiramente, o desafio inicial que pode ser apontado é "assegurar o uso efetivo do espaço cibernético pelas Forças Armadas e impedir ou dificultar sua utilização contra interesses da defesa nacional" (CARVALHO, 2011, p.28). Para isso, vale destacar, é necessário criar o Comando de Defesa Cibernética das Forças Armadas, com a contribuição de civis e militares das três Forças, executando, assim, os objetivos do Sistema Brasileiro de Defesa Cibernética, além de elaborar a Política de Defesa Cibernética – objetivo já concluído em 2012.

Em seguida, aponta-se a necessidade de "capacitar e gerir talentos humanos para a condução das atividades do setor cibernético na defesa" (CARVALHO, 2011, p.29). Mais uma vez, nota-se aqui a preocupação com a contratação de profissionais especializados no assunto e, porque não, de hackers, conforme foi apontado pelo general José Carlos dos Santos (SANTOS, 2011) na primeira seção deste capítulo. Como pontos basilares desse desafio, é importante citar a criação de cargos e funções específicas para o setor, realizar periodicamente o Seminário de Defesa Cibernética no país, além de criar plano de carreira para

viabilizar e motivar a permanência de pessoal no setor público, conforme afirma Zuccaro (2011):

> "A preocupação com a retenção de talentos, qualquer que seja o campo de atividade e o segmento a explorá-lo, é invariavelmente pertinente. Em se tratando do campo cibernético existente no segmento governamental, tal preocupação é ainda mais justificada. O segmento empresarial é bastante atrativo, particularmente nas empresas estrangeiras, que drenam uma parte considerável dos brasileiros de alta competência nesse campo. Melhores salários, qualidade de vida, condições de trabalho e pesquisa são os principais fatores que explicam a migração de pessoas de qualificação diferenciada dos países em desenvolvimento para os efetivamente desenvolvidos" (ZUCCARO, 2011, p.70).

Ainda, a abordagem do assunto em âmbito acadêmico – tanto em instituições de nível superior civis quanto militares – também é de fundamental importância para o crescimento do setor. Outrossim, podem-se citar como desafios a inserção contínua da defesa cibernética nos exercícios de simulação de combate e nas operações conjuntas; a realização de campanha nacional de educação sobre Segurança e Defesa Cibernética por parte do governo federal com fins de alçar a condição de conscientização da sociedade brasileira sobre o tema (CARVALHO, 2011). Diante desses pontos, conforme aponta Mandarino Jr. (2011), é hora do Brasil preparar-se para dar proteção ao seu patrimônio informacional, alcançando isso através do setor cibernético. Nas palavras do autor:

> "O Brasil precisa estar preparado para proteger o seu patrimônio de informação, entendido aqui como o somatório de seus ativos de informação, suas informações críticas, seus sistemas de informação, suas infraestruturas críticas, incluindo a de informação, tudo aquilo, enfim, que pode ser identificado como componente da sociedade da informação presente no espaço cibernético. Para tanto, será necessário adotar medidas para a proteção mediante a elaboração de doutrina e a construção de estratégias de segurança e de defesa do espaço cibernético brasileiro, considerando ambos os conceitos complementares". (MANDARINO JR. 2011, p.46).

Por fim, Zuccaro (2011, p.67) ainda faz importantes considerações sobre a criação de um Marco Legal para o setor cibernético tanto interna quanto externamente. Para o autor, não deveria existir por parte do Brasil um interesse em construir um marco regulatório internacional para as ações dos governos nesse espaço, especialmente pelo fato de que os países mais avançados no desenvolvimento deste campo obteriam maiores vantagens – nesse caso, o autor não considera o Brasil no patamar mais adiantado, colocando-o num grupo secundário. Outro fator importante para essa negativa, é que a falta de responsabilização pelas atividades ofensivas no ciberespaço dificultam o controle e

eficiência das limitações regulatórias, visto que a maioria dos ataques não possuem atribuições diretas e seriam praticadas por "procuração"[67].

Mesmo assim, deve-se elogiar e estimular a participação do país nos debates internacionais sobre o assunto, tentando adquirir uma posição protagonista para que, mais à frente, obtenham-se maiores vantagens na conformação de um marco regulatório internacional. Nesse sentido, em 19 de dezembro de 2013, com a iniciativa do Brasil e da Alemanha, a Assembleia Geral da ONU aprovou a resolução GA/SHC/4094[68] denominada "O Direito à privacidade na Era Digital", a qual faz críticas às ações de espionagem, de vigilância eletrônica, de interceptação das comunicações digitais e de recolhimento de dados pessoais. O documento não possui caráter punitivo, mas tem um considerável peso político. Ainda que não represente concretamente um marco regulatório, significa uma forma principiante de definir regras e obrigações perante o direito internacional quanto a algumas atividades cibernéticas, mostrando, sobretudo, uma importante pró-atividade do Brasil perante o tema.

À exemplo da visita do vice-presidente norte-americano Joe Biden durante a Copa do Mundo de 2014, a chefe de Estado alemã, Ângela Merkel, encontrou-se com a presidente Dilma nas vésperas da abertura do evento para discutir também a espionagem da NSA em ambos os países, emitindo, inclusive, nota de repúdio a tais atividades. Apesar de possuir apenas uma importância simbólica, o encontro e a nota representam certa harmonia de posicionamento e maior parceria entre os países no tocante a questão cibernética.

Ademais, no campo do direito interno, a visão é oposta. Antes de se preocupar com questões externas, é preciso buscar o fortalecimento jurídico e doutrinário que defina as ameaças, riscos, atores e crimes cibernéticos. Nesse sentido, o Marco Civil da Internet no Brasil representa uma melhor maneira de regulamentação da rede de internet no país, fornecendo maiores responsabilidades e maior segurança aos usuários e provedores.

---

[67]Conforme se apontou no segundo capítulo do presente trabalho, as ações por procuração referem-se ao patrocínio ou financiamento estatal a organizações não oficialmente ligadas ao Estado, mas que praticam atividades – nesse caso, atividades cibernéticas ofensivas e/ou defensivas – que interessam diretamente ao governo daquele país. Dessa forma, o Estado não leva a responsabilidade por tais ações, mas sim, tais organizações.

[68]Disponível em: http://www.un.org/News/Press/docs/2013/gashc4094.doc.htm. Acesso em 10 jun. 2014.

A Pesquisa & Desenvolvimento e, por conseguinte, seu estímulo, são “dois celeiros naturais para o desenvolvimento de conhecimento e tecnologia no campo cibernético” (ZUCCARO, 2011, p.69). No Brasil, apesar de não existir grandes empresas nacionais com papel de enorme destaque no setor, vale ressaltar a empresa Dígitro situada em Florianópolis, a qual foi responsável pela produção de um software de fabricação nacional que filtra mensagens na internet e identifica manifestantes, como uma espécie de espionagem interna, tendo sido implantado, inclusive, pelo CDCiber e tendo sido muito utilizado na Copa das Confederações em 2013 e Copa do Mundo em 2014[69].

Como último e mais ambicioso ponto, mas ao mesmo tempo mais distante, almeja-se a formação de um Sistema Nacional de Defesa Cibernética, com ramificações e interligações que vão desde o nível político com o GSI/PR e com a APF (tomando conta da segurança da informação e cibernética), passando pelo MD em nível estratégico (preocupando-se com a defesa cibernética), culminando até mesmo nos baixos escalões de comando das Forças Armadas em nível operacional e tático (ficando a cargo da guerra cibernética), “com vista a engajar toda a sociedade na defesa dos interesses nacionais dentro do espaço cibernético” (CARVALHO, 2011, p.26).

Enfim, após abordar neste derradeiro capítulo a importância e a visão da cibernética para o Estado brasileiro, dividindo o tratamento da segurança cibernética pelo Brasil em duas etapas iniciais compreendidas primeiramente até os anos 2000 (não politizado) e subsequentemente pela primeira metade dos anos 2000 (politizado); depois de descrever as responsabilidades, políticas e estratégias cibernéticas adotadas no país, apresentando a atuação de diversos órgãos federais, em especial do GSI/PR e do MD, e alguns importantes decretos e documentos, caminhando para a construção de um processo de securitização ainda incompleto; tentou-se apresentar desafios e obstáculos para o devido desenvolvimento do setor no país e, por conseguinte, da conclusão da sua inicial securitização. Com o aumento significativo de sistemas e redes de informação, aumento crescente de acesso a internet e avanço nas tecnologias, crescem também as ameaças e risco de vulnerabilidades, apontando para a urgência de ações na direção da criação, manutenção e fortalecimento da cultura de segurança da informação e cibernética.

[69]SASSINE, Vinicius. Exército monitorou líderes de atos pelas redes sociais. *O Globo.* Brasília. Ago. 2013. Disponível em: http://oglobo.globo.com/brasil/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915. Acesso em 16 jun. 2014.

Vale ressalvar que este capítulo poderia ser assunto para uma tese completa. O tema apresentado ainda é novo, os trabalhos existentes na área são em pequeno número e também muito recentes, além de os conceitos expostos ainda confundirem-se constantemente diante da diversidade de avaliação de cada Estado e cada organização, haja vista a característica incipiente do setor. Considerando-se tais motivos, a elaboração do trabalho significou enorme desafio, mas, levando-se em conta o escopo de exigência de uma monografia, tentou-se de forma concisa apresentar os principais elementos, questões, órgãos e políticas que fazem parte do arcabouço brasileiro perante tão complexo tema.

5 CONSIDERAÇÕES FINAIS

Apesar de ser um tema novo para os Estados e para as relações internacionais, o setor cibernético adquire cada vez mais destaque nas políticas, estratégias, decisões e investimentos dos países. No que tange à agenda de segurança, o tema tem progredido rapidamente na categorização proposta por Buzan et al (1998), saindo do não politizado no século passado para alcançar uma securitização nos anos atuais. Assim, cada vez mais recursos são alocados para tal área; discursos são pronunciados demonstrando preocupação com ataques cibernéticos e com a proteção de infraestruturas críticas; especialistas e hackers são contratados por instituições governamentais e empresas privadas; seminários e palestras são oferecidos para incentivar a participação da sociedade; cursos e disciplinas são criadas em instituições de ensino para introduzir o tema e aperfeiçoar os recursos humanos. Além do mais, assegura-se a justificativa para utilização de medidas extraordinárias e – e, portanto, a legitimação do uso da força – em casos de um ataque cibernético grave, conforme foi apontado pelo Manual Tallin (SCHMITT, 2013).

No que se refere ao fenômeno da guerra, ainda que a guerra cibernética não torne alguns elementos da natureza tradicional da guerra obsoletos, as armas cibernéticas podem não só introduzir características particulares ao fenômeno como podem amplificar a força dos ataques cinéticos em guerras tradicionais. Ao introduzir novos fatores para a arte da guerra, os meios cibernéticos podem renovar as relações interestatais e os estudos de segurança internacional, de guerra e de relações de poder.

Ao mesmo tempo em que a guerra cibernética não altera os aspectos clausewitzianos das guerras tradicionais, quais sejam o político, o instrumental e o violento (ou o racional, o instrumental e o nacional), ela também adquire ares da nova natureza kaldoriana, sobretudo pelo fato dos ataques não terem origem bem determinada, não existir exércitos uniformizados, ocorrer o patrocínio e financiamento dos Estados a organizações militares cibernéticas ou não estatais, caracterizando o que se chamou de guerra por procuração.

Ainda, traços da natureza clausewitziana podem ser notados no que concerne em desarmar o adversário ao ponto de impedi-lo ou dificulta-lo em sua defesa ou da possibilidade de um ataque quando o domínio cibernético é utilizado

paralelamente ao cinético. Por outro lado, os ataques cibernéticos podem ocorrer a qualquer momento, não existindo mais a clara distinção entre onde começa e onde termina o conflito. A natureza kaldoriana da guerra, então, apresenta igualmente seus traços na guerra cibernética por esta se tratar de um conflito de caráter transnacional e globalizado.

De todo modo, o uso das armas cibernéticas pode servir para alcançar fins que dificilmente seriam obtidos por outros meios. Um ataque aéreo a uma instalação nuclear, por exemplo, dificilmente não teria responsabilização objetiva a um Estado, sem contar na exposição internacional pública de tais ofensivas. Nesse sentido, o Estado que pratica um ataque cibernético bem sucedido aproveita-se do anonimato e da distância física que o espaço cibernético oferece. Portanto, a cibernética tem tudo para remodelar as maneiras pela qual a arte de fazer a guerra começa, tem prosseguimento e termina.

Ademais, é imprescindível a cooperação interestatal e intraestatal – ou seja, em nível internacional e também em âmbito interno (entre empresas privadas e instituições públicas) – no que tange ao setor, a fim de combater as vulnerabilidades e determinar os riscos e ameaças, haja vista que essas são de natureza difusa, desconhecida e incipiente. Tem-se que o espaço cibernético é um novo e promissor campo para a prática de todo tipo de ato ilícito, seja de crime comum, seja de caráter bélico entre nações. A assimetria, a dificuldade de atribuição de responsabilidades e o paradoxo entre tecnologia e vulnerabilidade servem para facilitar essas práticas ofensivas através do ciberespaço. É como se o setor cibernético fosse ainda um território sem lei, pouco conhecido, sendo, portanto, um velho oeste dos tempos modernos.

A Escola de Copenhagen e seus preceitos construtivistas foram fundamentais para descrever o surgimento dos diferentes temas presentes nas discussões sobre a agenda de segurança, bem como suas evoluções e consequências. Mais especificamente, a teoria de securitização de Waever (1995), também abordada por Buzan (1998, 2012), serviu para diagnósticos mais específicos em relação à cibersegurança brasileira. A percepção da segurança é particular para cada realidade, e, nesse sentido, o setor cibernético inseriu-se como um assunto particular de análise, principalmente devido ao desenvolvimento e surgimento das novas TICs.

Quanto ao fenômeno da guerra, a natureza clausewitziana e a kaldoriana possibilitaram uma análise referente à guerra cibernética, de modo a apresentar ora características de uma, ora de outra. Os atores estatais, ainda que com níveis de prioridade diversos, tem se preparado para atuar no domínio cibernético, podendo ser considerado um novo recurso de poder e um novo e integrado campo de batalha. As observações de casos descritas e analisadas demonstraram como os recursos provenientes do setor cibernético podem se manifestar na realidade, tendo consequências físicas bastante reais.

Ainda, apesar de opiniões divergentes, as visões contrárias e favoráveis à existência da guerra cibernética, demonstradas pelos trabalhos de Clarke e Knake (2010) e Rid (2013), possuem argumentos originais e sensatos, sendo suas leituras importantes para que o debate de um tema tão novo e complexo seja mais bem aprofundado e ganhe maiores contribuições. No entanto, o posicionamento do presente trabalho foi voltado para a real existência do conflito virtual, acreditando-se ser a guerra cibernética uma realidade não só futura, mas também presente nas relações internacionais e estratégicas atuais.

Em relação a segurança cibernética no Brasil, existem três etapas de categorização, de acordo com aquela apresentada por Buzan et al (1998). Assim, tem-se inicialmente até os anos 2000, como não politizado; subsequentemente até a metade dos anos 2000, como politizado, e; finalmente, mais significativamente a partir de 2008, como em processo de securitização, com a criação da Estratégia Nacional de Defesa de 2008.

No caso brasileiro, o GSI/PR e o MD são os líderes na organização do setor cibernético do país. O Exército Brasileiro ficou como a Força responsável na atuação e consolidação da defesa cibernética brasileira. Assim sendo, as medidas adotadas pelo país representam uma afirmação da capacidade cibernética brasileira perante o mundo e uma preparação do país para defender seus interesses nesse espaço e proteger as infraestruturas críticas nacionais. No entanto, os investimentos ainda são iniciais e carecem de maiores esforços para que o Brasil equipare-se ao que é investido em grandes potências como EUA, China e Rússia, e venha a obter maiores vantagens no futuro.

Não se pode colocar o Exército Brasileiro como único responsável pelas atividades cibernéticas do país. O vertiginoso desenvolvimento de novas tecnologias, o exponencial crescimento de novas ameaças e a grande variedade de

estruturas e dados/ativos de informação a proteger faz com que seja necessário que cada empresa pública e privada, cada grupo e órgão busquem o fortalecimento de sua própria capacidade de defesa e segurança cibernéticas. Cada ator nacional deve ter a consciência da importância do setor cibernético e deve fazer sua parte. Um vasto território nacional, como o brasileiro, dificulta imensamente a abrangência de proteção feita por um único ator. Portanto, é imprescindível a colaboração entre serviço público e privado, o aperfeiçoamento do tema dentro do âmbito acadêmico e a conscientização da sociedade para com a importância do investimento em defesa nacional, incluindo, então, o setor cibernético.

Assim como o descobrimento da América ao findar do século XV e a exploração dos desconhecidos mares no mesmo período, o espaço cibernético é para o mundo contemporâneo um lugar ainda a ser desvendado, mas que mostra possuir grande potencial, capaz de transformar as relações de poder interestatais. Nesse caso, a disputa por uma "corrida cibernética" não se restringiria somente às grandes potências, como ocorrido durante a Guerra Fria ao se tratar da questão nuclear, mas também poderia beneficiar atores de menor expressão no sistema internacional diante do caráter assimétrico de seus elementos. Como uma espécie de colonialismo, aquele que fincar a bandeira do espaço cibernético mais rapidamente, criando raízes em seu solo, obterá maiores vantagens quando este campo for alvo de discussões internacionais mais robustas, ditando os rumos das regras, princípios e deveres que contornarão e disciplinarão tal setor.

O Brasil parece demostrar interesse em ser um dos protagonistas e, realmente, em alguns casos, age dessa forma. No entanto, se não investir pesadamente no desenvolvimento do setor no presente momento estará fadado a ser apenas um coadjuvante, deixando mais uma vez para as grandes potências o papel de liderança. Em âmbito militar, sem dúvida, a cibernética já é vista e utilizada como uma nova dimensão de combate, juntamente com os demais domínios (marítimo, aéreo, terrestre e espacial). Portanto, o espaço cibernético já pode ser considerado uma quinta dimensão nos conflitos modernos.

REFERÊNCIAS

ALFORD, Lionel D. **Cyber Warfare: Protecting Military Systems**. Acquisition Review Journal, Fort Belvoir, Fairfax County, VA, EUA, p. 100 – 120, 2000. Disponível em: http://www.dau.mil/pubscats/pubscats/AR%20Journal/arq2000/alford.pdf. Acesso em 01 maio 2014

AMORIM, Celso. **Discurso de abertura:** III **Seminário De Defesa Cibernética**. Brasília. Brasília: MD, 2012. Disponível em: https://www.youtube.com/watch?v=dkUcymtvcUk. Acesso em 10 jun. 2014.

_____. **Segurança Internacional: novos desafios para o Brasil.** Contexto Internacional. Vol. 35, No.1, Rio de Janeiro. pg.287-311. (Comunicação Oral). 2013. Disponível em: http://www.scielo.br/pdf/cint/v35n1/a10v35n1.pdf. Acesso em 16 abr. 2014.

ARAÚJO JORGE, Bernardo Wahl Gonçalves; **Estados Unidos, poder cibernético e a "guerra cibernética: Do Worn Stuxnet ao Malware Flame/Skywiper-e além*;*** Instituto Brasileiro de Relações Internacionais (IBRI); Boletim Meridiano 47; v.13, n. 131; 2012. Disponível em: http://seer.bce.unb.br/index.php/MED/article/view/7051/5623. Acesso em: 15 out. 2013.

AZAMBUJA, Darcy. **Teoria geral do estado**. São Paulo: Globo, p. 17-53. 1957. Disponível em: http://www.faroldoconhecimento.com.br/livros/Pol%C3%ADtica/AZAMBUJA,%20Darcy.%20Teoria%20geral%20do%20Estado.pdf. Acesso em: 17 abr. 2014.

BAKER, Stewart; WATERMAN, Shaun. IVANOV, George. **Sob Fogo Cruzado – infraestrutura crítica na era da guerra cibernética**. McAfee. p.1-42. 2013. Disponível em: http://www.mcafee.com/br/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf. Acesso em 11 jan. 2014.

BERTONHA, João Fábio. **Uma Política de Defesa Nacional**. Boletim Meridiano 47. n.103, p.24-28. 2009. Disponível em: http://periodicos.bce.unb.br/index.php/MED/article/view/757/471. Acesso em 15 set. 2013.

BRASIL. **Sociedade da Informação no Brasil: Livro Verde**. Tadao Takahashi (org.) Brasília: Ministério da Ciência e Tecnologia. 2000. Disponível em: http://livroaberto.ibict.br/bitstream/1/434/1/Livro%20Verde.pdf. Acesso em 03 mai. 2014.

_____. **Política de Defesa Nacional**. Ministério da Casa Civil. Subchefia para Assuntos Jurídicos. Decreto Nº 5484, de 30 de Junho de 2005. Brasília. 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm. Acesso em 10 jun. 2014

_____**. Glossário das Forças Armadas**. Ministério da Defesa. PORTARIA NORMATIVA nº 196, 22.02.2007-MD-MD35-G-01. 2007. Disponível em: http://www.hmab.eb.mil.br/downloads/outros/glossario_fa.pdf. Acesso em 10 jun. 2014.

_____. **Estratégia Nacional de Defesa**. Decreto Nº 6.703, De 18 de Dezembro de 2008**.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm. Acesso em 11 jun. 2014.

_____**. Guia de Referência para a Segurança das Infraestruturas Críticas da Informação.**. v.01. Brasília. Gabinete de Segurança Institucional da Presidência da República. 2010a. Disponível em: http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf. Acesso em 13 jan. 2014. Acesso em 10 jan. 2014.

_____. **Livro Verde: segurança cibernética no Brasil**. Claudia Canongia e Raphael Mandarino Junior (org.). Brasília: GSIPR/SE/DSIC. 2010b. Disponível em: http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf. Acesso em: 02 mai. 2014.

_____. **Desafios Estratégicos para a Segurança e Defesa Cibernética**. Cel Cav Otávio Santana de Rêgo Barros e TC Inf Ulisses de Mesquita Gomes (org.). Presidência da República. Secretaria de Assuntos Estratégicos. 2011. Disponível em: http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf. Acesso em 16 jun. 2014.

_____. **Livro Branco de Defesa Nacional.** 2012a. Disponível em: http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf. Acesso em 02 jun. 2014.

_____. **Política Cibernética de Defesa.** "Portaria Nº 3.389/MD, de 21 de dezembro de 2012." Edição: Ministério da Defesa. Diário Oficial [da] República Federativa do Brasil (Poder Executivo). p. 11-12. 2012b. Disponível em: http://www.jusbrasil.com.br/diarios/44578940/dou-secao-1-27-12-2012-pg-11. Acesso em 10 jun. 2014.

_____. **Estratégia Nacional de Defesa de 2012.** 2012c. Disponível em: http://www.defesa.gov.br/arquivos/2012/mes07/end.pdf. Acesso em 11 jun. 2014.

_____. **Discurso da Presidente, Dilma Rousseff, na abertura do Debate Geral da 68ª AGNU**. Nova Iorque/EUA. 2013. Disponível em: http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua. Acesso em 11 jun. 2014.

BULL, Heddley. **A sociedade anárquica**. Tradução Sérgio Bath, 1ª ed. Brasília: Editora Universidade de Brasília, Instituto de pesquisa de Relações Internacionais, p.13. 1977. Disponível em http://www.funag.gov.br/biblioteca/dmdocuments/0158.pdf. Acesso em 17 abri. 2014

BUZAN, Barry. **People, States and Fear: An Agenda for the International Security Studies in the Post-Cold War Era**. Boulder, Colorado: Lynne Rienner. 1991.

_____; HANSEN, Lene. **A evolução dos estudos de segurança internacional**. São Paulo. Editora Unesp. 576p. 2012.

_____; WAEVER, Ole;e WILDE, Jaap de. ***Security: a New Framework for Analysis*.** Londres, Lynne Rienner Publishers. 1998.

CANONGIA, Claudia; MANDARINO, Raphael. **Segurança Cibernética: o desafio da nova sociedade da informação**. Revista Parcerias Estratégicas do Centro de Gestão e Estudos Estratégicos (CGEE); v.14; n.29; pág 21-46. 2009. Disponível em: http://dsic.planalto.gov.br/artigos/101-artigo-sobre-seguranca-cibernetica-revista-parcerias-estrategicas-cgee. Acesso em 16 abr. 2014.

CARR, Jeffrey**. Inside Cyber Warfare: Maping the Cyber Underworld**. Sebastopol, O'Reilly Media; p. 318. 2010.

CARREIRO, Marcelo. **A guerra cibernética: ciberwarfare e a securitização da internet**. Revista Cantareira, Edição 17. Dossiê guerras, conflitos e tensões. p. 123-137. 2012. Disponível em: http://www.historia.uff.br/cantareira/v3/wp-content/uploads/2013/05/e17a9.pdf. Acesso em: 15 nov. 2013

CARVALHO, Paulo Sérgio Melo de. **Conferência de Abertura: o Setor Cibernético nas Forças Armadas Brasileiras**. In BRASIL. **Desafios Estratégicos para a Segurança e Defesa Cibernética.** Cel Cav Otávio Santana de Rêgo Barros e TC Inf Ulisses de Mesquita Gomes (org.). Presidência da República. Secretaria de Assuntos Estratégicos. 2011. Disponível em: http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf. Acesso em 16 jun. 2014.

CAVALCANTI, Elmano Pontes. **Revolução da informação: algumas reflexões**. Caderno de Pesquisa em Administração, São Paulo, v.1, nº1. 1995. Disponivel em: http://www.ancibe.com.br/artigos%20de%20si/artigo%20-

%20Revolu%C3%A7%C3%A3o%20da%20informa%C3%A7%C3%A3o%20-%20algumas%20reflex%C3%B5es.pdf. Acesso em 28 mar. 2014.

CLARKE, Richard; KNAKE, Robert. **Cyber War: The Next Threat to National Security and What to Do About It**. New York: HarperCollins. 2010.

CLAUSEWITZ, Carl von. **Da Guerra.** 1832. Disponível online em: http://pensamentosnomadas.files.wordpress.com/2012/11/da-guerra-carl-von-clausewitz.pdf. Acesso em: 18 Dez. 2013

CORNISH, Paul; LIVINGSTONE, David; CLEMENTE, Dave; YORKE, Claire. **On Cyber Warfare**. Chatam House Report. p.1-38. 2010. Disponível em: <http://www.chathamhouse.org/sites/default/files/public/Research/International. Acesso em 10 jan. 2014.

CORREIO BRAZILIENSE. **Celso Amorim diz que Brasil é vulnerável contra ataques cibernético**. Outubro de 2013. 2013. Disponível em: http://www.correiobraziliense.com.br/app/noticia/politica/2013/09/22/interna_politica,389429/celso-amorim-diz-que-brasil-e-vulneravel-contra-ataques-cibernetico.shtml. Acesso em 11 jun. 2014.

COUTO, Abel Cabral. **Elementos de Estratégia, Apontamentos para um Curso**. Volume I, IAEM, Lisboa. 1988.

DALLARI, Dalmo de Abreu. **Teoria Geral do Estado**. São Paulo: Saraiva. 2 ed. p. 29. 1998. Disponível em http://www.visionvox.com.br/biblioteca/e/Elementos-de-Teoria-Gera-do-Estado-Dalmo-de-Abreu-Dallari.pdf. Acesso em: 17 Dez. 2013.

DUNN, Myriam. **Cyberwar: concepts, status quo, and limitations**. CSS Analysis in Security Police. ETH Zurich. p.1-3. 2010. Disponivel em: http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-71.pdf. Acesso em: 11 jan. 2014.

FERNANDES, José Pedro Teixeira. **A ciberguerra como nova dimensão dos conflitos do século XXI**. p.53-69. 2012. Disponivel em: http://www.scielo.oces.mctes.pt/scielo.php?script=sci_arttext&pid=S1645-91992012000100005. Acesso em 20 nov. 2013.

FERREIRA NETO, Walfredo Bento. **Por uma geopolítica cibernética: apontamentos da Grande Estratégia Brasileira para uma nova dimensão da guerra.** Tese (Mestrado em Estudos Estratégicos da Defesa e da Segurança) **-** Programa de Pós-Graduação em Estudos Estratégicos.. Universidade Federal Fluminense, Rio de Janeiro. 178p. 2013.

HANSEN, Lene; NISSENBAUM, Helen. **Digital Disaster, Cyber Security and the Copenhagen School**. International Studies Quarterly nº 53, p. 1155-1175. 2009. Disponível em: http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf. Acesso em: 05 jan. 2014.

HOUGH, Peter. **Understanding Global Security**. Routledge. p.1-20. Disponível em: http://guessoumiss.files.wordpress.com/2011/08/understanding-global-security.pdf. 2004. Acesso em 31 mar. 2014.

KALDOR, Mary. **New and Old Wars: organized violence in a Global Era**. Polity Press. p.1-216. 1998.

_____. **Old Wars, Cold Wars, New Wars, and the War on Terror**. Cold War Studies Center, School of Economics, London. p.1-10. 2005. Disponível em: http://dspace.cigilibrary.org/jspui/bitstream/123456789/8613/1/Old%20Wars%20Cold%20Wars%20New%20Wars%20and%20the%20War%20on%20Terror.pdf?1. Acesso em 03 fev. 2014.

KIEVIT James; MELTZ, Steven. **Strategy and the Revolution in Military Affairs: From Theory to Policy**. 1995. Disponível em: http://www.au.af.mil/au/awc/awcgate/ssi/stratrma.pdf. Acesso em: 15 abr. 2014.

KLIMBURG, Alexander; **Mobilishing Cyber Power**. Survival; An IISS (International Institute for Strategic Studies) publication; vol.53. p.41-60. 2011. Disponível em: http://web.clas.ufl.edu/users/zselden/coursereading2011/Klimcyber.pdf. Acesso em 07 mai. 2014.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999. p.95.

LIBICKI, Martin C. **Sub Rosa Cyber War**. p.1-13. 2009. Disponível em: <http://www.ccdcoe.org/publications/virtualbattlefield/03_LIBICKI_Sub%20Rosa%20Cyber%20War.pdf>. Acesso em: 12 jan. 2014

LIND, Willian S. **The changing of war: into the fourth generation**. Marine Corps Gazette; Military Review. p.22-26.1989. Disponível em: https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf. Acesso em 31 mar. 2014.

MANDARINO Jr, Raphael. **Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético**. Monografia em Especialização em Ciência da Computação: Gestão da Segurança da Informação e Comunicações. Brasília, Universidade de Brasília-UnB. 2009. Disponível em: http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf. Acesso em 03 mai. 2014.

_____. **Reflexões sobre Segurança e Defesa Cibernética**. In BRASIL. **Desafios Estratégicos para a Segurança e Defesa Cibernética**. Cel Cav Otávio Santana de Rêgo Barros e TC Inf Ulisses de Mesquita Gomes (org.). Presidência da República. Secretaria de Assuntos Estratégicos. 2011. Disponível em: http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf. Acesso em 16 jun. 2014.

NISSENBAUM, Helen. Where Computer Security Meets National Security**. Ethics and Information Technology**, n. 7, p. 61-73. 2005. Disponível em: http://www.nyu.edu/projects/nissenbaum/papers/ETINsecurity.pdf. Acesso em: 05 jan. 2014

NYE JR, Joseph. **Cyber Power**. Harvard Kennedy School, Belfer Center for Science and International Affairs. 2010. Disponível em: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf. Acesso 19 dez. 2013.

_____.**Guerra e paz no ciberespaço**. Estado de São Paulo. 2012. Disponível em: http://www.estadao.com.br/noticias/impresso,guerra-e-paz--no-ciberespaco-,861242,0.htm. Acesso em 15 dez. 2013.

REED, Thomas. **At the Abyss: An Insider's History Of the Cold War.** 2004. Presidio Press. p.113-131.

RID, Thomas. **Cyber War Will Not Take Place**. Oxford University Press, London; p. 256. 2013.

RODRIGUES, Alexandre Reis. **Portugal e o espaço estratégico de interesse**. In: Jornal de Defesa e Relações Internacionais. Revista Segurança e Defesa. Loures: Diário de Bordo Editores. 2012. Disponível em: http://database.jornaldefesa.pt/politicas_de_defesa/portugal/JDRI%20009%20221112%20Portugal%20e%20o%20espa%C3%A7o%20estrat%C3%A9gico%20de%20interesse.pdf. Acesso em 28 dez. 2013.

RUDZIT, Gunther. **O debate teórico em segurança internacional: mudanças frente ao terrorismo?** Civitas – Revista de Ciências Sociais, v.5. n.2. 2005. Disponível em: http://revistaseletronicas.pucrs.br/ojs/index.php/civitas/article/view/5/1598. Acesso em 20 dez. de 2013.

SANTOS, José Carlos dos. G**eneral José Carlos dos Santos: Podemos recrutar "hackers"**. Revista Época. 2011. Disponível em? http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html. Acesso em 03 mai. 2014.

SCHMITT, Michael N. **Tallin Manual on the international law applicable to cyber warfare**. Cambridge University Press. p.1-215. 2013. Disponivel em: http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381. Acesso em 20 dez. 2013.

TANNO, Grace. **A contribuição da escola de Copenhague aos estudos de segurança internacional.** Contexto internacional., Rio de Janeiro, v. 25, n. 1, 2003. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292003000100002&lng=en&nrm=iso>. Acesso em 20 dez. 2013

VENTRE, Daniel. Ciberguerra. **Seguridad Global y Potencias Emergentes em un Mundo Multipolar**. XIX Curso Internacional de Defensa. Zaragoza: Imprenta Ministerio de Defensa. p.32-38. 2012. Disponível em: http://publicaciones.defensa.gob.es/docs/default-source/publicacionespdf/xix_curso_internacional_defensa.pdf. Acesso em 13 mai. 2014.

WAEVER, Ole, **Securitization and Desecuritization,** in Ronnie D. Lipshutz (Ed). Nova Iorque, Columbia University Press. 1995.

WEISS, Gus W. **The Farewell Dossier: Duping the Soviets.** 1996. Disponível em: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol39no5/pdf/v39i5a14p.pdf. Acesso em: 14 mai. 2014.

WENDT, Alexander. **Anarchy is what States Make of it: The social construction of power politics**. International Organization, Volume 46, n.2, p.391-425. 1992. Disponível em: http://ic.ucsc.edu/~rlipsch/Pol272/Wendt.Anarch.pdf. Acesso em 20 abr. 2014.

ZUCCARO, Paulo Martino. **Tendência global em Segurança e Defesa Cibernética – Reflexões sobre a proteção dos interesses brasileiros no ciberespaço**. In BRASIL. **Desafios Estratégicos para a Segurança e Defesa Cibernética.** Cel Cav Otávio Santana de Rêgo Barros e TC Inf Ulisses de Mesquita Gomes (org.). Presidência da República. Secretaria de Assuntos Estratégicos. 2011. Disponível em: http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf. Acesso em 16 jun. 2014.