UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS MINISTRO ALCIDES CARNEIRO
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
BACHARELADO EM RELAÇÕES INTERNACIONAIS

JOSILMA DE LIMA BARBOSA

DESAFIOS TRANSNACIONAIS PARA A SEGURANÇA E DEFESA DOS EUA NA ERA DA INFORMAÇÃO: o uso da tecnologia da informação como arma de ataque às ameaças virtuais

João Pessoa

2012

JOSILMA DE LIMA BARBOSA

DESAFIOS TRANSNACIONAIS PARA A SEGURANÇA E DEFESA DOS EUA NA ERA DA INFORMAÇÃO: o uso da tecnologia da informação como arma de ataque às ameaças virtuais

Trabalho de Conclusão de Curso apresentado ao Curso de Relações Internacionais da Universidade Estadual da Paraíba em cumprimento à exigência para obtenção do diploma de bacharela.

Orientadora: Profª. Drª. Luiza Rosa Barbosa de Lima

João Pessoa

2012

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA SETORIAL CAMPUS V – UEPB

B238d Barbosa, Josilma de Lima.

Desafios transnacionais para a segurança e defesa dos EUA na era da informação: o uso da tecnologia da informação como arma de ataque às ameaças virtuais. / Josilma de Lima Barbosa. – João Pessoa, 2012.

58f.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) – Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, Curso de Relações Internacionais, 2011.

"Orientação: Profª. Dra. Luiza Rosa Barbosa de Lima, Curso de Relações Internacionais".

1. EUA. 2. Revolução da informação. 3. Ameaças virtuais. 4. Tecnologia da informação e da comunicação. 5. Ciberterrorismo. I. Título.

21. ed. CDD 327

JOSILMA DE LIMA BARBOSA

DESAFIOS TRANSNACIONAIS PARA A SEGURANÇA E DEFESA DOS EUA NA ERA DA INFORMAÇÃO: o uso da tecnologia da informação como arma de ataque às ameaças virtuais

Trabalho de Conclusão de Curso apresentado ao Curso de Relações Internacionais da Universidade Estadual da Paraíba em cumprimento à exigência para obtenção do diploma de bacharela.

Aprovado em 05/07/2012

Professor(a) Luiza Rosa Barbosa de Lima (Orientador(a)) - UEPB

Professor(a) Gabriela Gonçalves Barbosa - UEPB

Professor(a) Maria do Socorro de Lucena Gomes - UNIPÊ

João Pessoa, 05 de julho de 2012.

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus. E a todos aqueles que acreditarem em minha vitória.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado forças para ter chegado até o fim desse curso, pois durante todo esse percurso houve grandes dificuldades e muitos percalços que seriam muito difíceis de serem resolvidos sem a presença dele em minha vida.

A minha mãe, e aos meus irmãos, em especial Janice e Jocenildo por terem me ajudado e acreditado em minha vitória.

Aos meus amigos de turma, mesmo aqueles que não conseguiram terminar junto comigo, meu muito obrigado por ter feito parte de minha história acadêmica.

Aos meus grandes e inesquecíveis colegas de classe Jeane Freitas, Marcílio Mendonça, Sibelle Macedo, Wemblley Lucena, Fernando Queiroga, Lídia Bruna, Thalita Franciely e Nivaldo Pires, pela força fundamental ao longo do curso.

Um agradecimento especial aos meus amigos Josileide Costa, Jeane Freitas e Ely Aislan, que foram indispensáveis em vida.

A professora Luiza Rosa pela paciência, incentivo e orientação, que tornaram possível a conclusão deste trabalho.

A todos os professores de Relações Internacionais da UEPB e aos que já passaram pela instituição, pela atenção, dedicação e consideração demonstradas ao longo de todo o curso, e que contribuíram para a minha formação acadêmica, em especial à Heleno Rotta, Luiza Rosa, Silvia Nogueira, Eliete Gurjão, Maria Lúcia Abaurre, Cristina Pacheco, Raquel Melo, Elias David, Leonardo, Giuliana Dias e Augusto Wagner.

A todos os funcionários da UEPB, em especial as secretárias Kaline Barbosa, Sandra Maranhão, Isabelle Carneiro, Fabíola Maia, pela presteza, atenção, e amizade.

À UEPB e a todos aqueles que contribuíram, de maneira direta ou indireta, para a realização deste trabalho.

RESUMO

Os Estados Unidos vêm enfrentando nesse início de século, várias tendências mundiais nas quais configuram sérios problemas para a segurança e a defesa do país. Dentre elas estão a globalização, a maior acessibilidade dos indivíduos a tecnologias, a proliferação de armas de destruição em massa, ameaças não-estatais e a emergência das tecnologias de informação e da comunicação. Ocorre que nesta última hipótese de destinação do desenvolvimento científico, empreendeu-se na produção de computadores, que a principio foram desenvolvidos para fins militares. Anos mais tarde também seria utilizado no setor civil. Essas máquinas tornaram-se potentes e com o auxílio da internet, elas se tornaram fundamentais no cotidiano das pessoas, das empresas, dos governos e das Forças Armadas do mundo inteiro. A tecnologia da informação está ajudando a disseminar poder que antes era prerrogativa apenas dos Estados e atualmente, é grande o número de atores-não estatais que vem ganhando força no cenário internacional pó meio de sua utilização. As informações influenciam o poder de uma maneira surpreendente, de forma que os governos de todos os tipos terão grandes desafios no o futuro, pois à medida que as tecnologias da informação e da comunicação se espalham de maneira acelerada, tais governos poderão ver seu controle se desgastar no decorrer deste século. Nesta conjuntura, surgem as ameaças virtuais, no qual vem provocando sérios problemas para a segurança e defesa nacional dos EUA. Portanto, para combater essas novas ameaças houve uma necessidade de adaptar as tecnologias militares para uma possível batalha no ciberespaço. Neste contexto, o presente trabalho pretende abordar os desafios enfrentado pelos EUA devido a emergência dessas novas ciberameaças que vêm causando insegurança e desordem no ciberespaço norte-americano, o perigo que elas podem causar às principais infraestruturas do país e de como a tecnologia da informação e da comunicação vêm sendo usadas como arma de ataque em seu combate.

PALAVRAS-CHAVE: EUA; Revolução da Informação; Ameaças Virtuais; Tecnologia da Informação e da Comunicação, Ciberterrorismo.

ABSTRACT

The United States is experiencing the beginning of this century, several global trends shape in which serious problems for security and defense of the country. These include globalization, the increasing availability of individual technologies, the proliferation of weapons of mass destruction, nonstate threats and the emergence of information technology and communication. It happens that in the latter case the allocation of scientific development, undertaken in the production of computers, which at first were developed for military purposes. Years later it would also be used in the civilian sector. These machines have become powerful and with the help of the internet, they became essential in the daily lives of individuals, companies, governments and armed forces worldwide. Information technology is helping to spread the power that was once the prerogative only of the States and currently is the large number of non-state actors that has gained strength in the international arena through its use powder. The information influences the power in a surprising manner, so that governments of all kinds have great challenges in the future, because as information technology and communication spread so rapidly, such governments can see if your control wearing during this century. At this juncture, there are cyber threats, which has caused serious problems for national security and defense of the United States. Thus, to combat these new threats there was a need to adapt military technology for a possible battle in cyberspace. In this context, this paper aims to address the challenges faced by the U.S. due to emergence of new cyber threats that are causing insecurity and disorder in the U.S. cyberspace, the danger they can cause the main infrastructure of the country and how the information technology and communication have been used as a weapon of attack in combating them.

KEYWORDS: U.S. Information Revolution; Cyber Threats, Information Technology and Communication, Cyberterrorism.

SUMÁRIO

INTRODUÇÃO

Na história da humanidade um fator sempre presente é a guerra. Tem havido grandes transformações nas suas ideologias, no armamento, nas suas causas, nas estratégias, mas as guerras são tão antigas quanto à própria existência do homem na terra.

A priori as guerras eram travadas essencialmente em terra firme, a exemplo da guerra do Peloponeso (431- 404 a. C.) que teve como grandes vencedores os espartanos, com seu poderoso exército que era considerado a grande máquina de guerra terrestre da Grécia Antiga (FUNARI, 2009, p.33). A guerra da Crimeia (1853-1856) foi um conflito ocorrido na península da Crimeia (no mar Negro, ao sul da atual Ucrânia), no sul da Rússia e nos Bálcãs onde o mar foi o principal campo de batalha. Já nas duas Grandes Guerras do século XX, tanto na Primeira Guerra Mundial (1914-1918), quanto na Segunda Guerra Mundial (1939-1945), viu-se o céu ser invadido por potentes aviões de guerras que provocaram grande destruição material e humana em várias partes do planeta. Durante a Guerra Fria (1947-1991) as duas potências, EUA e URSS militarizavam o espaço. E atualmente as possíveis guerras poderão ser travadas no ciberespaço.

Assim, o homem inicia o século no XXI no domínio de um quinto campo de conflito, denominado espaço cibernético, ou ciberespaço. Esse novo âmbito é um espaço desterritorializado, anárquico, intangível, que existe em um local indefinido, desconhecido, cheio de complexidade, no qual há grande possibilidade de serem travadas guerras virtuais em grande escala, principalmente entre Estados e organizações terroristas caracterizando a chamada guerra assimétrica.

Na era da informação a guerra cibernética deixou de ser ficção e virou realidade. Transformou-se em um dos maiores problemas enfrentados pelos governos e exércitos do mundo inteiro, em especial, para os Estados Unidos que sofrem constantes ataques cibernéticos. As ameaças virtuais põem em risco toda a infraestrutura de países que converteram seus sistemas de controle em redes de computadores. Hackers ou crackers[1] têm por escopo, atualmente invadir computadores, roubar senhas, provocar desordem no ciberespaço e gerar uma espécie de terrorismo informacional no mundo inteiro.

[1] Hackers são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. Já cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança. Mais informação em: <http://olhardigital.uol.com.br/produtos/digital_news/noticias/hackers_e_crackers_saiba_as_diferencas>.> Acesso em 15 jul. 2012

Para Nye (2011) outro aspecto proeminente do poder no século XXI é sua dimensão cibernética e informacional. Nye avalia que o poder cibernético pode ser uma forma de Hard Power (poder duro, ou de coerção). Nessa conjuntura, o autor ressalta a existência de divisões militares na China e que são especializadas em ataques cibernéticos. O escopo da estratégia chinesa de provocarem ataques cibernéticos, sobretudo nos Estados Unidos, seria para abalar sistemas de informação e diminuir a capacidade de comunicação do inimigo. O terrorismo cibernético e a espionagem informacional também são questões preocupantes oriundas da revolução tecnológica experimentada no século XXI. Em resposta a esses desafios, os Estados Unidos criaram a décima frota e a vigésima quarta força aérea, divisões do exército especializadas em defesa e ataque virtuais. (NYE 2011 apud MENDONÇA, 2011, p. 2)

A nova dimensão da guerra entre Estados e terroristas que estão cada vez mais utilizando-se das tecnologias da informação e provocante uma espécie de terrorismo virtual foi reconhecia pelo departamento da Defesa dos Estados Unidos, que criou recentemente o Comando Cibernético (Cyber Command), sob o comando estratégico. Na atual conjuntura mundial, o planeta encontra-se globalmente interconectado, e um ciberataque não identificado contra a infraestrutura governamental poderia gravemente prejudicar toda a base de um país, a exemplo disso, alguns especialistas estão temerosos, pois acreditam que a rede de energia elétrica pode ser um alvo particularmente suscetível de um ciberataque.

O presente trabalho tem por objetivo analisar as novas ameaças virtuais que põem em risco as infraestruturas chaves dos EUA, o impacto da tecnologia da informação e da comunicação na estratégia de segurança e defesa dos Estados Unidos, que são cada vez mais vinculadas aos meios militares norte-americanos no combate a essas ameaças. Elas vêm causando uma grande revolução nos assuntos militares e têm garantido o surgimento de novos tipos de armamentos, em especial os virtuais para combater as ameaças que desestabilizam o ciberespaço. Os Estados Unidos armam-se para uma possível guerra no campo do ciberespaço, não apenas com armas cibernéticas, mas há também a necessidade no desenvolvimento de armas convencionais, pois o governo norte-americano pronunciou que caso os ataques continuem, haverá retaliações e nelas poderão ser utilizadas também as armas convencionais aos agressores.

A escolha do assunto foi motivada pelo fato de os ataques cibernéticos estarem acontecendo constantemente em vários países, inclusive, no Brasil, mas o foco será os Estados Unidos pelo fato de serem estes os maiores alvos dos ciber ataques e também por serem a grande potência geradora do desenvolvimento de tecnologia da informação e do conhecimento.

Abordar-se-á, ainda sobre a nova Era da Informação como pano de fundo da emergência de novos atores, tais como as organizações terroristas, as novas ameaças, a exemplo do ciberterrorismo, num novo espaço operacional, o ciberespaço.

Neste contexto, encontra-se a necessidade de especificar a análise da ação militar em decorrência das ameaças virtuais existentes nos dias atuais e o problema da disseminação mundial de tecnologia e o perigo iminente em relação à segurança dos Estados Unidos deixando-os sempre em estado de alerta.

Por tanto, é importante mencionar a respeito dos métodos utilizados para alcançá-las. Em decorrência de revisões literárias sobre o assunto da Revolução da informação e de como esta está causando grandes transformações na política mundial, assim como a guerra cibernética como o mais novo paradigma da guerra do século XXI e o ciberterrorismo que é tão ameaçador quando o terrorismo convencional.

Tendo em vista a meta traçada e as condicionantes do presente trabalho, optar-se-á por uma abordagem qualitativa para a presente análise. Assim, neste sentido, a metodologia utilizada baseou-se, sobretudo em pesquisa bibliográfica, recorrendo a leituras temáticas sobre as questões abordadas e consulta sítios na internet.

Destarte, será analisado no primeiro capítulo a Revolução da Informação e as novas configurações de poder que vem se difundindo nesse início de século pelo sistema internacional. Os Estados Unidos, dentro desse contexto, também serão examinados, assim como a difusão das tecnologias da informação e da comunicação que se transformaram em poder ao parar nas mãos de protagonistas não-estatais causando um grande problema para o governo norte-americano, visto que, eles estão adquiriram poderes que antes eram exclusivos de Estados, e ainda a questão da soberania quem vem sendo redargüida nessa nova conjuntura mundial assim como a problemática do controle interno das informações nos Estados Unidos.

No segundo capítulo, mostrar-se-á, num primeiro momento, as ameaças cibernéticas que vem afligindo e pondo em alerta o governo e o exército norte-americano, passando por uma breve análise a respeito da guerra cibernética que poderá ser travada, não apenas entre os países, mas um único indivíduo poderá travar uma batalha com um país poderoso como os Estados Unidos, passando a abordar também o ciberterrorismo e as algumas estratégias que serão utilizadas pelo exército americano para combater esse mal que assola todo o território.

E por último, no terceiro capítulo, far-se-á uma abordagem a respeito das armas cibernéticas desenvolvidas pelos exército americano para combater as ameaças virtuais. Nesse contexto, um paradoxo que alerta sobre a importância e necessidade de estudo sobre a temática é que, ao mesmo tempo em que esse tipo de tecnologia é usado na segurança e

defesa dos Estados Unidos, ela também instiga outros países a usar os mesmos mecanismos para a defesa nacional, provocando assim, uma nova corrida armamentista

CAPÍTULO I

OS EUA NA ERA DA INFORMAÇÃO E AS NOVAS CONFIGURAÇÕES DE PODER NO SISTEMA INTERNACIONAL

A queda do comunismo e a derrocada do império soviético na década de 1990, finda o sistema bipolar que perdurou durante mais de quarenta anos no mundo. Com o fim do enfrentamento Leste-Oeste, o sistema internacional entrou numa nova fase de intensa transformação, caracterizando o período do pós Guerra Fria em uma época de incertezas e imprevisões, apresentando tendências multipolares diversificadas. A ameaça que antes era bem definida foi substituída por diversas outras, amorfas e dispersas, onde não há uma clara identificação de sua origem. Surgem novos Estados, multiplicam-se os conflitos locais e emergem no cenário internacional, protagonistas não-estatais que vão dividir o palco da política internacional com os Estados nesse início de século.

Essa nova fase, na qual o mundo se encontra, é baseada no conhecimento, na informação e nos rápidos avanços tecnológicos nos computadores, nas comunicações e nos transportes. Esse processo vem causando transformações significativas na política mundial, visto que tornou o planeta com um alto grau de interdependência e interconectividade, acarretando em sérios desafios aos governos do mundo inteiro, uma vez que, as distâncias, as barreiras físicas, econômicas, culturais e políticas estão sendo praticamente abolidas do mapa, pois a sociedade da informação e da comunicação desconhece o significado de fronteiras, barreiras e aduanas.

Assim, conforme aduz Ricardo Seitenfus (2004, p.3) os modernos meios de comunicação desconhecem as limitações fronteiriças. O fenômeno do fim do território – concebido como espaço estanque no interior da linha de fronteira – faz a interpenetração entre o endógeno e o exógeno apresentar-se como elemento fundamental da realidade contemporânea. Os cidadãos em rede levam novos atores à cena internacional.

A atual Revolução da Informação tornou-se o pano de fundo da emergência de novos atores no cenário internacional, com destaque às organizações terroristas que de acordo com Dupas (2004, p. 4) "repentinamente adquiriram o *status* de novos atores mundiais, concorrendo com os Estados, a economia e a sociedade civil e ainda disputa com os primeiros o monopólio da violência". Também fazem parte dessa estrutura as novas ameaças oriundas do ciberterrorismo e um novo espaço operacional, além dos já tradicionais, terra, mar, ar e

espaço, atualmente o ciberespaço é o quinto campo das possíveis batalhas que ocorrerão neste século.

Essas mudanças vêm sendo ocasionadas desde a Revolução Industrial no século XVIII, com os avanços nos meios de transportes e das comunicações. A máquina a vapor foi para a Primeira Revolução Industrial aquilo que o computador vem sendo para a Revolução da Informação, suas mais expressivas invenções, os maiores símbolos de cada uma das Revoluções que mudaram integralmente o *modus vivendi* da população mundial. Se a Revolução Industrial nascera na Inglaterra foi os Estados Unidos quem deram a luz a Revolução da Informação.

Castells (2008, p. 68) "afirma que a Revolução da Tecnologia da Informação é, no mínimo, um evento histórico da mesma importância da Revolução Industrial, provocando um padrão de descontinuidade nas bases da economia, sociedade e cultura".

A Era da Informação, realizada através da Internet e do progressivo desenvolvimento de novas tecnologias, multiplicou as vias de informação e deu origem ao aparecimento de novos espaços operacionais, onde os atores podem utilizar esta facilidade de distribuição de informação para "paralisar atividades estratégicas de uma ou mais sociedades" (SANTOS, apud VILELA, 2010, p. 06). Dada a acessibilidade geral à utilização das tecnologias, qualquer ator tem acesso a estas vias de informação e pode usá-las em seu proveito e de acordo com os seus interesses. (VILELA, 2010, p. 6).

Portanto, pode-se dizer que a era da informação teve seu advento na década de 1940, com o nascimento dos primeiros computadores eletrônicos digitais nos Estados Unidos em meio a Grande Guerra. Houve um grande incentivo para o desenvolvimento dessas máquinas, visto que elas estavam se tornando cada vez mais úteis em tarefas de desencriptação de mensagens inimigas e principalmente na criação de novas armas mais inteligentes. O mais famoso dos computadores produzidos na época foi o ENIAC[2]. Essa máquina era bem diferente dos protótipos de computadores que se conhece atualmente, era uma máquina gigantesca de 30 toneladas que media 30 metros de comprimento e ocupava um andar inteiro do prédio onde se localizava[3]. A partir de então, os Estados Unidos começam a empreender computadores cada vez mais potentes, e atualmente alguns deles se tornaram tão pequenos ao

[2] O **ENIAC** (Electronic Numerical Integrator and Computer) foi o primeiro computador digital eletrônico de grande escala. Criado em fevereiro de 1946 pelos cientistas norte-americanos John Eckert e John Mauchly, da Electronic Control Company. Desenvolvido em 1943 durante a II Guerra Mundial para computar trajetórias táticas que exigissem conhecimento substancial em matemática, mas só se tornou operacional após o final da guerra.

[3] Para mais informações: **História do Computador e da Internet**. Disponível em <http://www.tecmundo.com.br/mac-os-x/1697-a-historia-dos-computadores-e-da-computacao.htm#topo.> Acesso em 20 de mai. 2012

ponto de caberem na palma da mão, no entanto sua capacidade é incomparavelmente superior aos computadores produzidos na década de 1980, por exemplo.

Anos mais tarde, a rede mundial de computadores, ou internet, surgia em plena Guerra Fria. A internet foi desenvolvida, pelo Departamento de Defesa dos EUA e a antecessora da Internet, que na altura se designou por ARPANET (Advanced Research Project Agency Network); só começou a ser utilizada intensivamente durante a década de 1970, quando os computadores das organizações militares e das universidades foram interligados através da rede telefônica. No início dos anos de 1990, a Internet constituía já uma plataforma internacional e registrava mais de sete milhões de utilizadores em todo o mundo; contudo, foi nesta década que se assistiu ao crescimento desenfreado, não só do número de utilizadores, como dos conteúdos disponíveis e das tecnologias utilizadas para acesso a esta rede de comunicação global. Na década de 1990, este sistema tornou-se tão complexo que é impossível determinar quem o domina e ainda hoje, não se conhecem todas as ações mal intencionadas que se podem realizar sobre os computadores ligados a esta plataforma tecnológica. (BATISTA, Et al, 2003, p. 32).

Na conjuntura da Guerra Fria, o homem já havia conquistado um quarto campo de conflito: o espaço sideral. Assim como a terra, o mar, e o ar, americanos e russos também militarizaram o espaço a fim de atingirem pioneirismo na exploração desse âmbito. Ao longo dos séculos, explorar o espaço era algo inimaginável para qualquer ser humano. Contudo o homem conseguiu chegar aonde se achava que era o limite da terra, o céu, e caminhava a passos largos para um quinto campo de conflito que seria o ciberespaço.

De acordo com Almeida (2003, p. 20), a aplicação da violência tornou-se mais dependente das novas tecnologias, principalmente devido aos progressos advindos da microtecnologia, da biotecnologia, das tecnologias da informação e do domínio da tecnologia espacial.

Portanto, assim como os computadores tinham objetivos militares, a internet fora criada para o mesmo fim. Era mais uma forma dos militares americanos se comunicarem caso os meios convencionais de comunicações vissem a ser destruídos por inimigos.

Os avanços da tecnologia desenvolvidos durante o período da Segunda Guerra Mundial criou condições suficientes para o desenvolvimento das indústrias eletrônica e da informação, resultando nos computadores digitais, e mais tarde no raio laser. No futuro próximo, tanto o computador quanto o laser iriam servir de instrumentos para produzir potentes, aparatos de guerra tais como, vírus de computador, e as armas de energia dirigida (em inglês, em inglês, *directed energy weapons* –DEW), ou simplesmente e-bomb. Esta é uma

designação genérica para compreender desde o radar até a família das microondas de forte potência, também conhecidas como High Power Microwaves (HPM). (MARTINS, 2008, p. 99). Era a guerra do futuro que se anunciava.

Os computadores e a internet que foram criados para atender as necessidades militares passaram a ser aplicadas também em outros segmentos produtivos, numa transferência da esfera militar para o setor civil. As tecnologias surgiram pela necessidade de sobrevivência do homem na guerra, e as guerras são as maiores incentivadoras na descoberta de novas tecnologias, pois nos conflitos convencionais modernos o peso da tecnologia favorece o exército que a possui. Conclui-se que a existência da tecnologia é inerente a guerra. Assim, muitos produtos mais simples, como os enlatados e aparelhos celulares que atualmente são de utilidades civis nasceram em épocas de guerras. Essas tecnologias, principalmente as de informação evoluíram muito rapidamente, e hoje os computadores estão se tonando cada vez menores, mais potentes, mais baratos e mais fáceis de serem manipulados.

A rapidez na produtividade faz com que o intervalo entre o desenvolvimento de uma inovação tecnológica e a sua aplicação na produção de mercadorias ou no setor de serviços fosse cada vez menor. Com isso, os bens de consumo duráveis, especialmente aqueles ligados aos setores de tecnologia de ponta, como o de computadores, de produtos eletrônicos e de telecomunicações, a exemplo dos celulares, tornam-se rapidamente obsoleto em razão da velocidade com que são superados pela introdução de novas tecnologias. (LUCCI; BRANCO, 2002, p. 38). Isso também ocorre com os aparatos pertencentes às forças armadas, por exemplo, uma aeronave como a Lockheed F-104 Starfighter de interceptação e bombardeio nuclear que serviu na USAF (United States Air Force) de 1958 até 1967, hoje em dia, está completamente fora de uso. E o F-22, que é o caça mais moderno dos Estados Unidos na atualidade, logo será superado por outro muito superior a ele o F-35.

O progresso na ciência e a busca incessante do homem por maior produtividade e qualidade geram uma espécie de guerra de concorrência, e nela são constituídas as bases da aceleração tecnológica e as alterações ocorridas no mundo. E é nessa disputa acirrada por mercado consumidor que leva as indústrias a produzirem produtos cada vez mais rápido e modernos, isso consequentemente estimula ainda mais os avanços na tecnologia que se espalha pelo mundo tornando-o cada vez mais globalizado e praticamente sem fronteiras.

Portanto, devido a essa revolução na tecnologia, o mundo é hoje caracterizado por constantes mudanças que atinge todo o Sistema Internacional tornando-o totalmente instável. Isso dá origem a incertezas e riscos, que por vezes evoluem para crises profundas de difíceis

soluções para os governos contemporâneos. Essas mudanças são provocadas, sobretudo pelos saltos tecnológicos que fizerem com que o mundo se globalizasse e esse intenso processo de globalização que teve sua origem principalmente nos avanços nos meios de transportes e das comunicações, tem provocado um encurtamento das distâncias e um "encolhimento do mundo".

Para se ter uma ideia da dimensão do quanto à evolução da tecnologia vem provocando uma "diminuição" do planeta Joseph Nye faz uma interessante alusão a respeito de como a instantaneidade com a qual os acontecimentos ocorrem tem causado tal sensação: o Mayflower[4] levou três meses para cruzar o Atlântico. Em 1924, o voo transatlântico de Chales Lindenberg[5] demorou trinta e três horas. Cinquenta anos depois, o Concorde repetiu a travessia em três horas. Os mísseis balísticos podem fazer o mesmo em trinta minutos. (NYE, 2009, p. 1). Os vírus de computador podem contaminar os sistemas de informação em poucos segundos.

Contudo, as comunicações mundiais avançaram de uma maneira formidável, e hoje o mundo inteiro se conecta por meio de satélites, telefones, televisão, rádios, e vários outros meios de comunicação. A internet veio causando uma grande revolução nessa área, e grande parte de usuários espalhados pelo mundo encontram-se completamente dependentes dela. Atualmente, tanto indivíduos como grandes corporações dificilmente conseguiriam desempenhar suas tarefas sem a ajuda de computadores e da internet. As sociedades modernas encontram-se tão dependentes das tecnologias que, a interrupção nas redes de comunicação, por pelo menos um dia, provocaria um caos no mundo inteiro e um prejuízo econômico sem precedentes. A partir dos anos 1980, a internet conectou vários lugares do mundo numa rede de computadores e um incomensurável número de informações de todos os tipos são trocadas com uma velocidade impressionante, nunca antes imaginada pelo homem na "era analógica".

Para Magnoli, (2009, p. 417) no Vietnã foi travada a primeira guerra da "era da informação". A televisão foi um meio que influenciou bastante a população civil norte-americana durante a guerra. Isso ocorreu devido ao desenvolvimento nos diferentes meios de transmitir informação, como a televisão, o rádio, o telefone e o computador, e portanto fez com que ocasionasse uma série de alterações em todo mundo, isso resultou como fator dominante a disseminação de poder nas mãos da população de vários lugares no mundo.

---

4 Mayflower foi o famoso navio que, em 1620, transportou os chamados Peregrinos, do porto de Southampton, Inglaterra, para o Novo Mundo.

5 Charles Augustus Lindbergh foi um pioneiro da aviação estadunidense, famoso por ter feito o primeiro vôo solitário transatlântico sem escalas em avião, em 1927.

O avanço nas tecnologias da informação emergiu definitivamente nos meios militares na Primeira Guerra do Golfo, uma violenta conflagração militar ocorrida de janeiro a março de 1990. Waack (2009, p. 458) retrata bem esse entendimento quando profere que "essa tecnologia permitiu que o exército americano testasse não em exercícios, mas no campo de batalha, pela primeira vez, as doutrinas militares de informação em tempo real". Ainda na concepção de Waack:

> À revolução da informação seguiu-se uma revolução na doutrina militar americana, que já se vislumbrara como "exercício piloto" na Primeira Guerra do Golfo: trata-se do aperfeiçoamento da extraordinária capacidade de integração de vários sistemas, e da capacidade de transmissão de informações em tempo real do campo de batalha para qualquer dos níveis envolvidos em decisões bélicas. Na breve fase preparatória de bombardeios aéreos, durante a ação de 2003, os americanos empregaram quase que exclusivamente "armas inteligentes", ao contrário do que ocorrera em 1991. E dessa vez, quase sem oposição anti-aérea. (WAACK, 2009, p. 469).

O advento de armas cada vez mais potentes pode acarretar em sérias conseqüências para a humanidade. No caso da utilização de uma arma cibernética, que tem sua ação virtual, mas que seus planos e interesses são reais, os possíveis danos provocados por elas podem gerar grande caos caso um ataque seja direcionado as redes elétricas de um país. Contudo, armas produzidas com alta tecnologia de guerra estão sendo disseminadas facilmente para diversas regiões do planeta e consequentemente já encontram-se na posse de atores não-estatais, que já podem perfeitamente serem utilizadas para provocarem atos terroristas.

Este é um dos principais problemas enfrentados pelos Estados Unidos na atualidade, pois esta capacidade adquirida por outros países está sendo cada vez mais difundida e é de difícil controle para os governos de todas as partes do mundo, e não exclusivamente do norte-americano. A transmissão instantânea de informação e os avanços na internet acabaram por ultrapassar as fronteiras, sendo possível, hoje em dia, um único individuo disseminar um vírus letal para os sistemas informacionais pertencentes, e até mesmo roubar informações secretas do Pentágono, da CIA ou da OTAN, ou de grandes empresas como o Google e a Microsoft entre outras.

Portanto, é mister dizer que à medida que a tecnologia da informação se espalha de maneira célere pelo mundo e começa a baratear-se, os governos poderão ver seu controle se desgastar no decorrer do século XXI.

1.2 A TECNOLOGIA DA INFORMAÇÃO E A DIFUSÃO DE PODER

Esses avanços técnicos e científicos caracterizam a chamada "Terceira Revolução Industrial", também chamada de Revolução Técnico-Científica ou ainda Revolução da informação. As técnicas utilizadas para a fabricação dos componentes tecnológicos na atualidade são cada vez mais complexas e sofisticadas, por isso tem-se como umas das principais "matérias-prima" para a produção de chips, robôs, satélites, computadores, telefones celulares, etc., o conhecimento. (SENE; MOREIRA, 2002, p, 28). Os avanços da robótica e da engenharia genética são incorporados ao processo produtivo que depende cada vez menos da mão-de-obra e cada vez mais de alta tecnologia que são resultados dos esforços de mentes brilhantes através de seus conhecimentos científicos.

A Revolução da informação vem proporcionando uma difusão de informação em todo o mundo e o com ela tem ocorrido uma propagação de poder para protagonistas não-estatais que atualmente vem ganhando força no cenário internacional. Diferentemente do que pensam os realistas quando pronunciam que o Estado é o único ator relevante no sistema internacional, esses novos atores estão cada vez mais presentes na agenda internacional e tem preocupado os governos do mundo inteiro, pois à medida que as tecnologias se espalham, eles ganham poder e podem levar a um desgaste à soberania estatal.

Há quatro séculos, o estadista-filósofo Francis Bacon proferiu que conhecimento é em si mesmo um poder. Para Bacon o conhecimento científico tinha por escopo servir o homem e dar-lhe poder sobre a natureza. Ciência e poder do homem coincidem, uma vez que, sendo a causa ignorada, frustra-se o efeito. Pois a natureza não se vence, se não quando se lhe obedece. (BACON, 1973, p. 6). Quanto maior o conhecimento do ser humano mais poderoso ele se torna. Portanto, é exatamente essa difusão de informação que torna o indivíduo comum influente na política internacional atualmente.

A Revolução da Informação além de difundir tecnologia, conhecimento e interligar o planeta, ela também vem provocando transformações significativas na política mundial. Dois dos maiores problemas discutidos e enfrentados pelas autoridades governamentais no século XXI é o fluxo e o controle de informação, pois é cada vez maior a parcela de pessoas que tem acesso a ela. A Revolução da Informação tem como fundamento os rápidos avanços tecnológicos nos meios de comunicações, principalmente na internet na qual possibilita que milhões de informações circulem instantaneamente para qualquer parte do planeta fugindo completamente do controle dos governos.

Ademais, todo tipo de informação pode ser encontrada na internet hoje em dia. Pode-se aprender de tudo, inclusive, a fabricar bombas e armas caseiras com muita facilidade. Nos Estados Unidos, as facilidades com que são encontrados os boletins que disponibilizam os manuais militares norte-americanos na internet, deixam-os gratuitamente acessíveis, pronto para serem utilizados por qualquer pessoa e adicionados ao arsenal terroristas de conhecimento militar. A internet também fornece informações e contatos para que a Al Qaeda ou outros grupos terroristas recrutem combatentes às guerras.

A revolução da informação influencia o poder de uma maneira surpreendente, de forma que os governos de todos os tipos estão tendo sérias dificuldades para manter a segurança e a defesa interna do país devido à rapidez com que os fatos ocorrem. Os Estados Unidos que foram os grandes mentores da bomba atômica, não esperavam que a tecnologia nuclear fosse parar nas mãos de outros Estados, dando a estes poderes destruidores equiparados aos seus. A bomba foi criada em 1945 pelos norte-americanos e em 1949, a União Soviética testou seu primeiro artefato termonuclear. Os Estados Unidos entraram em pânico ao descobrir que seu maior rival já era igualmente a eles uma potência nuclear. Washington entra em transe paranóico, com suspeitas generalizadas de vazamentos de atos de traição Em 1961, já detinham a bomba, além de Estados Unidos e URSS, França, Grã-Bretanha, e em 1964, era a vez da China fabricar a sua própria bomba nuclear. (CÉSAR, 2008, p. 386). Ao contrário do que ocorreu no século XIX com o equilíbrio de poder, viu-se no século XX as armas nucleares produzirem uma forma maligna de "equilibro do terror" causando total insegurança no sistema internacional. A tecnologia disseminou-se rapidamente aos outros países, contrariando os interesses norte-americanos e provocando grande desconforto à posição de hegemonia destes.

A ciência permite que cada vez mais sejam produzidos aparelhos da mais alta tecnologia, e com a concorrência bastante acirrada, isso torna os custos do processamento e da transmissão ínfimos, ao ponto da população de todas as classes também ter acesso a essa tecnologia. Portanto, essa rapidez na disseminação de tecnologia e as facilidades no seu manuseio tornam-se efetivamente perigosas para toda a humanidade e provoca acima de tudo novos desafios aos Estados, visto que os ataques de 11 de setembro simbolizaram uma grande deficiência na segurança do país que é a maior potência bélica do planeta, e caracterizaram um novo tipo de ameaça advinda da tecnologia, pois ela foi parar nas mãos de protagonistas não-estatais, que por sua vez adquiriram poder; poder esse destrutivo que antes era privativo apenas aos governos.

O terrorismo existe há anos, mas ganhou notoriedade apenas com os atentados as torres gêmeas e ao Pentágono, nos eventos de 11 de setembro no qual chocou um mundo pela tamanha brutalidade e façanha por desafiar a potência norte-americana. Isso veio a mostrar que, como conseqüência da difusão de poder, as tecnologias dão condições suficientes países pobres, de regiões longínquas, como o Afeganistão e Iraque, tornarem-se altamente relevantes para os Estados Unidos.

O grupo terrorista Al Qaeda sempre repudiou a cultura ocidental e tudo que lhe é pertinente, no entanto utiliza-se das tecnologias oriundas do ocidente para propagar suas ideologias através de sua própria estação de noticiário de TV e também pela internet. Integrantes de grupos terroristas incitam jovens, inclusive crianças, a fazerem parte desses grupos como soldados e ainda fomentam a nutrir o ódio pela cultura ocidental, mormente em se tratando especificamente dos Estados Unidos.

Durante a guerra no Iraque, os terroristas investiram pesado na propaganda contra o ocidente e eles tiveram bastante êxito. A própria população foi a favor dos terroristas e contra a presença dos norte-americanos na região. Em qualquer guerra o controle da mídia é crucial para garantir o apoio popular, os próprios Estados Unidos fizeram isso quando quiseram invadir o Afeganistão em 2001, após os atentados, utilizando-se do slogan "*guerra contra o terror"* e garantir o apoio de sua população nessa empreitada. Os terroristas estão usando a tecnologia moderna e estão prestes a intensificar seu jogo de poder, agora no ciberespaço.

Nas guerras do Vietnã, Afeganistão e Iraque, os americanos empregaram as tecnologias da informação para empurrar até o limite a coordenação entre as forças de terra, ar e mar e entre as forças blindadas convencionais e as unidades de comandos infiltradas atrás das linhas inimigas. (MAGNOLI, 2009, p. 16).

A internet também é utilizada para promover benefícios em prol da população mundial. É bastante comum grupos ativistas convocaram pessoas para manifestações via internet. Jody Williams uma professora de inglês norte-americana e ativista, foi Premio Nobel da Paz em 1997 junto com sua organização por ter contribuído para a campanha internacional de proibição de minas terrestres. Ela organizou a campanha pela internet e conseguira lograr êxito, pois foi através dela que surgiu o tratado que proíbe as minas terrestres. (NYE, 2002, p. 84) Portanto, nessa atual conjuntura, os Estados terão que dividir o palco do cenário internacional com outros protagonistas e a política mundial não será mais território exclusivo de atores estatais.

No relevante fato ocorrido, e mencionado por Brigagão e Rodrigues foi que:

> Flagradas pelas câmeras do jornalismo internacional e noticiadas em escala global pelas agências de notícias e cadeias de tevês, as violações de direitos humanos provocam reações imediatas da opinião pública e forçam governos a tomar atitudes rápidas e energéticas. A divulgação em escala global de cenas de discriminação, de tortura e de chacinas num país pode derrubar secretários e funcionários de Estado e acelera processos legislativos e judiciais de proteção aos direito fundamentais. (BRIGAGÃO; RODRIGUES, 1998, p. 34).

Assim, o homem encerrou o século XX com esse poder de atravessar as fronteiras sem necessariamente sair do seu território. O ser humano foi capaz de criar uma poderosa rede de comunicação que une todo o planeta. A internet mudou o cotidiano das pessoas, produziu poderes para os cidadãos comuns. Mudou a forma de fazer compras, de fazer transações bancárias, de conhecer pessoas e principalmente a forma de fazer a guerra.

A internet além de útil, ele pode ser perigosa se for utilizada por pessoas que ensejem fazer determinadas práticas do mal. Por exemplo, é bastante comum, atualmente, ataques hackers em sites de governos, de grandes empresas e principalmente a sistemas bancários, onde conseguem roubar grandes quantias de dinheiro, causando prejuízos gigantescos.

Devido ao anonimato que a rede mundial de computadores proporciona, aliado a falta de legislação pertinente ao assunto, tal modalidade de delito aumenta consideravelmente no mundo contemporâneo, de forma a obrigar a população e as autoridades a buscar mecanismos de prevenção contra os criminosos. (CARLI, 2006). A falta de legislação é o principal problema enfrentado pelos governantes, pois não há como punir alguém que comete um crime cibernético se ainda não há leis para criminalizar esse tipo de conduta.

Além de roubar senhas, entrar nas contas bancárias alheias para roubar dinheiro, os hackers invadem a privacidade das pessoas, roubando imagens geralmente íntimas para extorquir dinheiros de seus donos, ou apenas para diversão. Assim como argumenta Hissa (2009) a cada clique do mouse, somos vigiados, seguidos e monitorados devido às tecnologias cada vez mais perversivas e onipresentes.

A agilidade com que os fatos acontecem no sistema internacional, na era da globalização, coopera ainda mais para a insegurança e instabilidade no mesmo, isso aumenta as dificuldades que os governos têm de adaptar respostas políticas eficazes, a, por exemplo, um ataque hacker a informações sigilosas ao Pentágono acontece de uma maneira muito mais acelerada que a política de segurança para evitá-la. A política internacional, não consegue evoluir com a mesma velocidade que as informações. O mesmo acontece com a legislação

internacional, visto que, a guerra moderna, é agora travada em geral, no computador e os tipos penais existentes são insuficientes para combater os cibercrimes.

Joseph Nye ilustra algo bastante interessante a respeito de como na globalização, os fatos ocorrem com grande rapidez:

> (...) a globalização moderna funciona num ritmo muito mais rápido do que suas modalidades anteriores. A varíola levou praticamente três milênios para se espalhar por todos os continentes habitados, chegando finalmente à Austrália em 1775. A Aids levou menos de três décadas para se espalhar da África para o mundo. E, falando em vírus metafóricos, em 2000 o vírus de computador "bug do amor" inventado por hackers nas Filipinas, precisou de apenas três dias para disseminar por todo o mundo. (...) (NYE, 2009, p. 248).

A revolução da informação acrescentou à globalização uma maior rapidez e intensidades nas questões da interligação mundial que a tornou ainda mais complexa, complicando e limitando cada vez mais o poder de ação dos Estados.

A modernização trouxe de fato muitos benefícios para a humanidade, porém com ela, vieram riscos não só para os estados como também para os indivíduos de toda parte do mundo. Essa modernização nas tecnologias informacionais e nas comunicações, está de fato mudando a natureza dos governos e da soberania e instituindo uma difusão do poder no Sistema Internacional.

Nas palavras de Barbeiro (2006, p. 117), os países também enfrentaram sérios desafios para inspecionar, controlar e proibir o uso de tecnologias sensíveis. Com a mesma tecnologia, como sensores, computação, comunicação e materiais, sendo cada vez mais desenvolvida para um espectro de aplicações tanto de aplicações comerciais como militares, a monitoração e o controle de exportação de componentes tecnológicos será mais difícil. Além do mais, *joint ventures*, mercados globalizados e a crescente proporção do capital do setor privado em pesquisa e desenvolvimento básico acabará por minar os esforços das nações para controlar esse tipo de tecnologia.

1.3 DESAFIOS À SOBERANIA AMERICANA E A PROBLEMÁTICA DO CONTROLE INTERNO DE INFORMAÇÕES

Soberania relaciona-se a poder, autoridade suprema pertencente a um Estado. O Poder do Estado é uno e indivisível. O Estado é para os realistas o ator central das relações internacionais e o poder o elemento central de sua análise. Para Waltz, o poder é a capacidade de influenciar o sistema internacional mais do que ser influenciado por ele, enquanto que Morgenthau afirma que os Estados procuram o poder visando à manutenção do *status quo*à

expansão ou o prestígio (NOGUEIRA; MESSARI, 2005, p. 29). Dentro dos limites territoriais do Estado, não há nenhum outro poder superior ao seu. Na sociedade internacional de nações, os Estados se reconhecem como iguais, todos são soberanos na ordem internacional. O termo soberania surge no final do século XVI juntamente com o Estado Moderno, sendo este decorrente da necessidade de neutralizar um contexto de instabilidade política, econômica e social presente no final da Idade Média. (FERRER; SILVA, p 2).

A questão da soberania estatal é um assunto bastante discutido e analisado na atualidade, pois ela está sendo intensamente redarguida no cenário internacional. Miranda (2004, p. 87) argumenta que alguns já a considera uma questão superada no mundo moderno e globalizado, pois a capacidade de ação autônoma do Estado estaria sendo continuamente superadas pela dinâmica das relações internacionais no plano econômico, tecnológico e mesmo jurídico. Esse forma de Estado, na qual se configura atualmente, nem sempre existiue um dia poderá desaparecer. Nada obstante, com a globalização, muitas pessoas discutem o "fim do Estado", visto que no atual período técnico-científico do capitalismo, com a aceleração dos fluxos que caracterizam a globalização, o Estado sofre transformações em seu papel, muito embora, falar em seu fim, pode ser precipitado e até perigoso. (SENE; MOREIRA, 2002, p. 116)

Sobre esse aspecto, Samuel Huntington faz uma observação interessante:

> (...) as fronteiras dos Estados se tornaram cada vez mais permeáveis. Todos esses desdobramentos levaram muitos a ver o fim progressivo do Estado Sólido, tipo "bola de bilhar", que supostamente foi a regra desde o Tratado de Westfália, e o surgimento de uma ordem internacional complexa, de múltiplos níveis, que parece mais com a idade média. (...) O enfraquecimento dos Estados e a aparição de "Estados fracassados" contribuem para uma quarta imagem de um mundo em anarquia. (HUNTINGTON, 2007).

É preocupante, para as autoridades governamentais norte-americanas e também dos demais países do globo, a maneira com a qual a soberania estatal vem sofrendo alterações devido aos efeitos da globalização e da revolução da informação. Para os realistas, mesmo com essas constantes mudanças os Estados vão continuar sendo os protagonistas mais importantes no cenário internacional, e os avanços da tecnologia continuarão sem sombra de dúvidas beneficiando os Estados mais ricos e poderosos. Esta revolução está tornando a política mundial mais complexa pelo fato de que, o mundo tornou-se globalizado e os problemas também se globalizaram e chegam a proporções assustadoras. Os protagonistas não-estatais já possuem tecnologias modernas capazes de provocar desordem nos sistemas de

informação de qualquer país. E uma das grandes ameaças no futuro será o fato de os terroristas transnacionais chegarem a possuir armas de destruição em massa, daí então o mundo inteiro entrará em colapso, visto que a sociedade internacional viverá sob o domínio do medo, pois não há uma maneira de impedir ou punir esses agentes já que eles não obedecem a nenhum tipo de legislação. A disseminação de tecnologia da informação parece ser inevitável. Ela está reduzindo o controle dos Estados além de afetar cada vez mais o poder entre os mesmos.

Atualmente os protagonistas transnacionais, a exemplo da Al Qaeda, uma organização fundamentalista islâmica internacional formam redes mundiais de ativistas que desafiam os métodos de defesa nacionais convencionais dos Estados. É uma organização forte que já tem em mãos armas altamente tecnológicas, e se utilizam da internet para promover o terror pelo medo e disseminar suas ideologias. Seus maiores alvos são os Estados Unidos, essa aversão é gerada pela insatisfação que este país produz no mundo islâmico com suas repugnantes ideologias ocidental e seu desprezível American Way Life totalmente adverso no mundo oriental. Essa forma de conflito tem sido denominado de guerra assimétrica[6].

Ainda que haja certa facilidade na disseminação de tecnologia da informação existente, devido a seu baixo custo, a obtenção e produção de novas informações geralmente requerem um grande investimento financeiro, algo bastante difícil para países como os africanos, mas não é impossível obtê-la. Contudo, à medida que se reduz os custos da produção de tecnologia e as barreiras de entrada aos mercados são facilitadas, ela pode reduzir o poder dos países mais ricos, ao contrário eleva o poder de países mais frágeis e de agentes não-estatais, e isso já é uma realidade atualmente.

A tecnologia da informação já chega às portas até mesmo de países totalitários e daqueles de sistemas fechados, com fronteiras quase intransponíveis. O que eles não esperavam é que não há barreira que a tecnologia não possa transpor. Estes países estão enfrentando grandes problemas pelo fato de ainda resistiram às informações e de tentaram manter um determinado controle sobre ela. Países, como a China podem controlar o acesso de seus cidadãos á internet e, inclusive, monitorar os seus usuários, contudo, é uma política bastante dispendiosa para qualquer país, principalmente àqueles com proporções continentais como a China e com a maior população mundial. (NYE, 2009, p. 281). A internet também propicia poder aos cidadãos a partir do momento que estes entram em contato com o universo

[6] Guerra Assimétrica é a guerra na qual os oponentes apresentam diversas características dispares tais como: nível de organização, objetivos, recursos financeiros, recursos militares, comportamento-obediência a regras. Em geral são guerras irregulares (guerrilhas), insurrecionais ou entre potências e Estados pequenos. As ações do mais fraco são geralmente indiretas e visam desgastar o mais forte.

da tecnologia, afinal, como disse Francis Bacon, conhecimento é poder. As sociedades de sistemas fechados e ditatoriais começam a perder o controle a partir do momento em que seus habitantes partilham dessa tecnologia com outros povos e começam a difundir ideais revolucionários que mobilizam a população na reivindicação de melhores condições de vida. Foi o que aconteceu no mundo árabe com a chamada Primavera Árabe que teve inicio na Tunísia e se propagou rapidamente para outros países da Região. E tudo isso foi auxiliado pelos meios de comunicação, principalmente da televisão e da internet.

Portanto, com essa evolução tecnológica, sobretudo nas telecomunicações, as fronteiras dos Estados ficam cada vez mais permeáveis. Embora haja resistência de alguns Estados ditatoriais em aceitar as tecnologias impondo restrições aos fluxos de informações, é cada vez mais difícil controlá-las.

A questão que os estudiosos do assunto em pauta fazem não é se o estado continuará existindo nos moldes atuais, de Estado soberano, e sim como sua centralidade e suas funções estão sendo modificadas com a rápida disseminação das informações. Muitos Estados passam constantemente por problemas relacionados à suas fronteiras, principalmente aqueles países com grandes extensões geográficas como os Estados Unidos, que recebe diariamente fluxos imensos de pessoas em seus aeroportos. Os Estados Unidos também são um país que tem o maior índice de violação de suas fronteiras virtuais. E não é só isso, é cada vez maior a lista de problemas com a qual o país convive todos os dias em suas fronteiras, e tornou-se um dos maiores desafios de controle internos dos Estados Unidos. Joseph Nye alega que:

> Conforme o 11 de setembro de 2001 ilustrou, os terroristas podem facilmente se infiltrar pelas fronteiras, e é mais fácil entrar com alguns quilos de agentes biológicos ou químicos mortais do que contrabandear toneladas de heroína e cocaína que chegam anualmente. Complicar a tarefa da governança nacional não é o mesmo que solapar a soberania. Os governos se adaptam. Entretanto, no processo de adaptação eles mudam o significado de jurisdição soberana, de controle e do papel dos protagonistas privados. (NYE, 2009. p. 288).

A rede terrorista Al Qaeda, que foi a grande protagonista dos atos terroristas do inicio do século XXI, que chocaram o mundo ao por em prova a segurança interna dos Estados Unidos e intimidando as autoridades norte-americanas, é exemplo claro de que qualquer pessoa, que possua tecnologia para fins maléficos, pode atravessar uma fronteira e provocar uma grande tragédia. Os ataques as Torres Gêmeas e ao Pentágono, envolveram indivíduos e grupos de vários países, e por incrível que possa parecer havia integrantes até mesmo no território dos Estados Unidos. Contudo, com a tecnologia da informação, as coisas

se complicam ainda mais para a segurança interna dos Estados, visto que as ameaças, na atualidade são virtuais, ou cibernéticas. Portanto se exigirá um esforço ainda maior dos Estados na era da informação, pois mesmo sendo a maior potencia bélica do planeta os Estados Unidos, não foram capazes de assegurar sua segurança nacional, talvez por acharem que já estavam seguros o suficiente ou quem sabe pelo fato de sustentarem o status de superpotência poriam medo em seus inimigos.

Para o realismo os atores não-estatais não possuem um status relevante nas relações internacionais, ou seja, sua influência é indireta e sempre por meio dos Estados. Dessa forma, sejam os grupos terroristas, sejam as Empresas Transnacionais (ETNs), sempre possuem uma base territorial, e, portanto, influenciam os Estados que, por sua vez, são os atores básicos das relações internacionais. Assim, as relações internacionais, na verdade, são relações interestatais. (SARFATI, 2005).

Na visão clássica do realismo, apenas os grandes e poderosos Estados têm importância do cenário internacional, porém isso está mudando, a emergência de grandes corporações multinacionais tem alterado a face da política internacional, devido a grande influência que estas causam, pois além de ultrapassar as fronteiras, elas, muitas vezes controlam mais recursos econômicos que muitos Estados-nações. Os liberais reconhecem que o Estado é o ator mais importante no sistema internacional, mas adotam a concepção de grande relevância que estas produzem no mundo e o poder que elas vêm adquirindo no decorrer dos anos é inegável. Destarte, com a difusão de tecnologia de informação o poder do Estado é compartilhado com pessoas, organizações não-governamentais e grupos terrorismos. Todos esses entes já desempenham papel de grande importância na política mundial.

No entanto, Organizações como Greenpeace, Anistia Internacional, Cruz Vermelha, Human Right Watch, dentre outras, atuam em várias atividades “voluntárias”, fora do âmbito do Estado. Estes são os principais atores não-governamentais que operam no mundo inteiro, os quais estabelecem verdadeiras redes e canais de interesses transfronteiriços que escapam ao controle das autoridades governamentais. O Estado-nação perdeu parte de sua soberania e teve algumas de suas tradicionais atribuições alteradas com a chegada desses novos atores no cenário internacional. Um outro exemplo são as empresas transnacionais que constituem o melhor exemplo de exercício de poder não-estatal, no caso econômico, nas relações internacionais. Algumas dessas empresas são tão poderosas economicamente que chegam a ter seu patrimônio maior do que o PIB de certos Estados. Empresas como a Coca-Cola, McDonald´s tem seu orçamento maior do que muitos países africanos. (BRIGAGÂO; RODRIGUES, 1998, p. 25-7).

Diante desses graves problemas que acarretaram a Revolução da Informação, os Estados Unidos resolveram investir intensamente na segurança do país, sobretudo no ciberespaço, que atualmente é o campo mais vulnerável. Portanto o Pentágono não está medindo esforços pra desenvolver o mais rápido possível uma nova geração de armas chamadas de armas cibernéticas ou virtuais capazes de alcançar inimigos militares que se comunicam em rede, mesmo quando essas redes não estão conectadas à internet. Além de estarem desenvolvendo armas convencionais para uma possível guerra no mundo real.

CAPÍTULO II

A AMEAÇA CIBERNÉTICA E A NOVA CONFLITUALIDADE NO CIBERESPAÇO

Atualmente existe uma grande dependência do homem em relação às novas tecnologias. É importante mencionar um paradoxo existente entre a relação homem-máquina, pois a tecnologia que "liberta é a mesma que aprisiona", pois nunca na história, o ser humano se tornou tão dependente das tecnologias como nessa nova era, e hoje o mundo vive sob forte influência do uso dos computadores e da internet. Isso proporciona um grande risco para a sociedade moderna porque tem estimulado uma constante atividade criminosa cometidas pelos crackers – considerados hackers do mal – e também por terroristas que se utilizam da tecnologia como instrumento para atacar alvos vulneráveis, com intenção de gerar pânico e violência de alguma forma, pois ataques virtuais podem causar grandes prejuízos materiais.

Há uma grande preocupação em relação à segurança interna dos Estados, já que as ameaças relacionadas à revolução da informação combinam tanto protagonistas governamentais quanto protagonistas transnacionais. Foi através da difusão dessa tecnologia que surgiram as novas ameaças à segurança dos Estados chamadas de ciber-ameaças. Na concepção de Nye (2009, p. 324) as Ciber-ameaças e uma potencial guerra cibernética ilustram as vulnerabilidades e a perda do controle cada vez maiores nas sociedades modernas. Por outro lado, o Major Visacro (2011, p. 53) diz que o advento da era da informação promoveu mudanças significativas na conduta da guerra. Mudanças que vão muito além da mera aquisição de moderna tecnologia. Embora não deva ser desconsiderada, a concepção de defesa alicerçada primordialmente no confronto ostensivo entre Estados Nacionais possui sua aplicação cada vez mais restrita.

Assim como aduz Garcia (2008, p. 1) se por um lado as novas tecnologias têm oferecido à humanidade inúmeros benefícios, por outro, disponibilizaram um novo e confortável meio para o cometimento de ilícitos civis e penais. As próprias estruturas da Internet e do espaço cibernético, bem como suas características essenciais, condicionam indivíduos ao cometimento de toda sorte de irregularidades e ilegalidades por suas vias. A intangibilidade, a volatilidade e a mobilidade das informações transmitidas e armazenadas na rede mundial de computadores, a instantaneidade e a fugacidade com que as conexões são estabelecidas, mantidas e encerradas, o alcance global da Rede, a possibilidade dos usuários agirem sem se expor fisicamente e de forma bastante discreta, em casa ou no trabalho, e a facilidade de preservação da verdadeira identidade de criminosos em sigilo, são exemplos de

peculiaridades inerentes a estas novas tecnologias que beneficiam a prática de condutas ilegais. Conforme salienta Verdelho:

> A convenção sobre cibercrimes do Conselho da Europa é o primeiro trabalho internacional de fundo sobre crime no ciberespaço. Foi elaborado por um comitê de peritos nacionais congregados no Conselho da Europa e consiste num documento de direito internacional publico. Embora tenha na sua origem, sobretudo países membros do Conselho da Europa, tem vocação universal. Na sua elaboração participam vários outros países (Estados Unidos da América, Canadá, Japão e África do Sul). E pretende-se que venha a ser aceite pela generalidade dos países do globo. (VERDELHO, et al., p. 10, 2003).

A facilidade na obtenção e no manuseio das tecnologias são os maiores aliados dos hackers e terroristas, e isso se transformou numa das maiores ameaças para a sociedade da informação e da comunicação, governo e forças armadas que se utilizam diariamente das redes de computadores. Este novo nível de terrorismo, praticado através de computadores e de sistemas de telecomunicações, tem por principal característica provocar temor, incertezas e desordem no sistema mundial. O terrorismo não é algo novo, porém houve uma mudança na maneira de como ele vem sendo praticado, devido ao uso das tecnologias da informação que foram disseminadas e amparadas por grupos dessa natureza.

A preocupação com esse tipo de ameaça já dura alguns anos e configura-se como um dos maiores desafios da atualidade. De acordo com Annunciação (2003, p. 9).), no ano de 1997, preocupado com a ameaça cibernética, o Departamento de Defesa dos EUA realizou um exercício para descobrir as dimensões de suas vulnerabilidades. A missão era de invadir os sistemas de computadores do próprio Departamento de Defesa e foi atribuída a um grupo de aproximadamente trinta pessoas. Para isso, foram utilizadas tecnologias comuns e softwares disponíveis no mercado ou obtidos pela Internet. O grupo logrou êxito em três meses: conseguiu invadir as redes não-secretas do Departamento e ficou em condições de causar sérios danos às comunicações e aos sistemas de energia.

Um dos incidentes mais repercutidos foi o que ocorreu na Estônia em 2007, no qual o país acusou a Rússia pelos ataques sofridos no país. Foi uma série de ataques que deixou os sites governamentais da Estônia fora do ar por algumas horas. Os ataques mostraram como os sistemas ligados à Internet são vulneráveis e serviu para deixar em alerta vários outros países

que tem seus sistemas controlados por redes e que podem ser futuro alvos de ataques cibernéticos. [7]

Vários outros ataques se sucederiam e foram atribuídos à guerra cibernética uma nova forma de guerra que estaria surgindo e motivando governos a se protegerem na Internet e aumentarem os gastos na segurança de todos os serviços ligados as redes. A Estônia é um dos países que mais depende das redes de internet nos seus sistemas bancários, comerciais, e governamentais, por esta razão, os ataques tiveram sérios danos ao país.

Os Estados Unidos, assim como a Estônia, partilham das mesmas vulnerabilidades, visto que seus principais serviços como as centrais hidroelétricas e nucleares, finanças, telecomunicações, transporte, saúde e defesa, são todos sistemas controlados através de redes, daí serem altamente vulneráveis a ataques cibernéticos. Para evitar um desastre de grandes proporções é preciso medidas eficazes de segurança em cibernética; o dispêndio não é nada generoso e o medo da guerra cibernética está fazendo os Estados Unidos e outros países que se sentem ameaçados pelos ataques a produzirem gastos elevados.

Um dos crimes cibernéticos de grande repercussão foi o que ocorreu com o *site Wikileaks*, que ganhou destaque mundial ao divulgar um vídeo de um ataque norteamericano ao Iraque. De acordo com o jornal *The New York Times* (2011), o site divulgou na *Internet* cerca 391.832 documentos secretos sobre a guerra do Iraque, 77 mil documentos confidenciais do Pentágono sobre a guerra do Afeganistão, além do trafego de informações entre o Departamento de Estado Americano e mais de 270 postos diplomáticos americanos ao redor do mundo. (ARAÚJO, 2011, p. 4),

Esses documentos repercutiram mundialmente, foram rechaçados pela opinião pública e pela mídia mundiais. Os Estados Unidos violaram todas as normas internacionais de direitos humanos durante a guerra do Iraque e do Afeganistão, na sua infundada "guerra ao terror" justificada após os ataques de 11 de setembro de 2001, no qual quase três mil pessoas perderam suas vidas nos violentos ataques terroristas, em contra partida a isso, quase 150 mil inocentes morreram, apenas na guerra do Iraque.

A volatilidade da Era da Informação demonstra a fragilidade com que são guardados dados sigilosos do Pentágono, OTAN, dos governos e de tantas empresas que dependem da tecnologia da informação hodiernamente.

[7]Mais informações em: Ataques digitais na Estônia. Disponível em: <http://informatica.hsw.uol.com.br/hacker-economia-eua1.htm > Acesso em 25de junho de 2012.

Contudo, o grupo denominado Anonymous também surge como uma nova ameaça virtual. Sem sede fixa, descentralizado e sem líder, qualquer pessoa pode fazer parte do grupo, que promovem protestos com o fim de requerer a liberdade de expressão e conteúdo online. Este grupo ficou conhecido em 2010, quando cobrou da sociedade destaque à revelação de informações confidenciais oficiais pelo Wikileaks em relação às atrocidades praticadas pelos Estados Unidos contra os iraquianos e afegãos nas guerras. Desde então, o grupo se caracterizou pela interrupção do serviço de sites, como o que ocorreu com as páginas de Visa e MasterCard depois que as empresas bloquearam o acesso a Assange.[8] E uma espécie de guerra virtual iniciou-se após o FBI fechar a empresa Megaupload em janeiro deste ano

Os ataques praticados pelo anonymous acontecem com grande freqüência em todas as partes do mundo, sobretudo as organizações norte-americanas. Os Anonymous não são um grupo estruturado. Há um núcleo central de pessoas que normalmente incentiva os ataques, nos quais qualquer cibernauta pode integrar-se, passando então a ser designado como Anonymous. Eles se consideram ativistas de internet ou hackivistas e não terroristas. Apresentam-se sempre com máscaras de Guy Fawkes[9]. Manifestam-se em prol de causas que beneficiem a sociedade como a liberdade de imprensa e são impulsionados por ideais libertários. Os participantes desse movimento se organizam em redes sociais e fóruns, pelo qual são estabelecidos os objetivos de ações e de como serão executados os planos de ataques.

A Internet torna-se uma arma digital nas mãos de indivíduos que ensejam provocar atos terroristas virtualmente, estes são chamados de ciberterroristas. Da mesma forma que os demais países do globo, os Estados Unidos estão temerosos em relação aos perigos que os ataques virtuais podem causar ao país. Os ciberterroristas já têm a capacidade de acessar qualquer informação dos sistemas do governo, e essa nova forma de terrorismo, o terrorismo via Internet é considerado uma ameaça para a integridade de um Estado.

Os anonymous também incitam manifestantes a protestarem contra as lei Stop Online Piracy Act (SOPA) e Protect IP Act (PIPA), caso sejam essas leis sancionadas, elas darão ao governo americano o direito de fechar sites de compartilhamento de conteúdo pirata baseados no exterior. Ambas as leis tem por objetivo acabar com a pirataria na internet, uma missão quase impossível na era da informação. O Presidente Obama se manifestou contra as duas

---

[8] Para mais informações ler: Entenda quem são os Anonymous e o LulzSec. Disponível em:< http://tecnologia.terra.com.br/noticias/0,,OI5200054-EI12884,00
Entenda+quem+sao+os+Anonymous+e+o+LulzSec.html > Acesso em 23 de junho de 2012.

[9] Guy Fawkes ou Guido Fawkes, como também era conhecido, foi um soldado inglês católico que participou da " conspiração da pólvora" na qual tinha-se a pretensão de assassinar o rei protestante Jaime I da Inglaterra, assim como todos os membros pertencentes ao parlamento durante uma sessão em 1605, objetivando o início de um motim católico.

leis, afirmando que elas podem atentar contra a liberdade de expressão na internet e vai gerar uma balbúrdia no campo real. [10]

Os Estados Unidos temem a ação de grupos como os anonymous, pois eles têm o apoio de pessoas de todas as partes do mundo e temem também que esses constantes ataques se tornam mais sérios ao ponto de danificar as principais estruturais do país proporcionando uma guerra cibernética.

2.2 CIBERWAR - NOVO PARADGMA DA GUERRA

Para Portela, "a guerra é, fundamentalmente o conflito armado que envolve Estados soberanos e cujo principal objetivo é solucionar uma controvérsia pela imposição da vontade de uma das partes na disputa". (PORTELA, 2010, p. 485). No entanto, Willian Lind apresenta a teoria de guerra de quarta geração[11] na qual o Estado perde o monopólio sobre a guerra (...). No seu fundamento se encontra uma crise universal da legitimidade do Estado, e essa crise significa que muitos países terão evoluída a guerra de Quarta Geração em seu território. (LIND, 2005, p. 14).

A próxima guerra pode acontecer não entre Estados soberanos e sim entre um Estado e outros protagonistas que insurgem nesse início de século. O ciberespaço é o novo campo de batalha e ciberguerra seu novo paradigma. A Guerra Cibernética corresponde ao uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil.[12]

A ideia de Guerra Cibernética, ou mais comumente, Ciberguerra, tem suas origens na própria definição e conceito de técnica cibernética. Com efeito, a palavra tem origem grega, *Kibernetiké* e significa a arte de controlar, exercida por um piloto sobre o navio e sua rota. Aquele que pilota é aquele e exerce o controle. Foi esse conceito que Nobert Wiener

[10] Mais informações em: http://g1.globo.com/tecnologia/noticia/2012/01/entenda-o-projeto-de-lei-dos-eua-que-motiva-protestos-de-sites.html

[11] Guerra de quarta geraçãoEsta teoria da guerra foi desenvolvida por William S. Lind e quatro oficiais do Exército e do Corpo de Fuzileiros dos Estados Unidos (USMC). É o termo utilizado pelos analistas e estrategistas militares para descrever a última fase da guerra na era da tecnologia da informação e das comunicações globalizadas.

[12] Fonte: CyberWar: Security, Strategy and Conflict in the Information Age, *Campen, Dearth and Goodden, ©AFCEA International Press 1996*

introduziu ao final da década de 1940, quando lançou o famoso "Cibernética ou controle e comunicação no animal e na máquina". (SAMPAIO, 2001, p. 2).

Annunciação (2003) diz que o entendimento de ciberguerra (ou guerra cibernética) ainda não é uniforme na literatura. Muitos autores interpretam a guerra cibernética como parte da guerra de informações. Segundo Nunes (1999), a guerra de informações pode materializar-se em: combate aos sistemas de comando e controle, segurança operacional, ciberguerra, guerra eletrônica, pirataria eletrônica ("hackers"), bloqueio de informação, guerra baseada na informação, ou mesmo, guerra psicológica.

Para Lewis, "A guerra é o uso da força militar para atacar outra nação e danificar ou destruir a capacidade e a vontade de resistir. A Guerra Cibernética implicaria um esforço por outra nação ou um grupo politicamente motivado para usar ataques cibernéticos para atingir fins políticos". (LEWIS, 2011, apud ARAÚJO, 2011, p. 5)

Á medida que a Internet evolui e fornece novos tipos de serviços e facilidades, ela também promove novos desafios e problemas que necessitam de resolução eficazes. O caso da segurança dos dados governamentais e das forças armadas dos Estados Unidos que estão ligados à world wide web; também designada por Cibersegurança, estão sendo ameaças pelos terroristas de computador que se aprimoram a cada dia. Os Estados, conjuntamente com os exércitos estão atualmente se concentrando em esforços para complementar a segurança física e lógica das redes de computadores, com medidas legislativas e outras para evitar ataques terroristas aos seus centros críticos.

O termo ciberespaço foi idealizado por Willian Gibson em 1984 em seu livro Neuromancer. Trata-se de um espaço que não existe fisicamente apenas virtualmente e é composto por computadores conectados a uma rede mundial que tornou-se palco do mais novo paradigma da guerra, a guerra cibernética. Ela é a mais nova ameaça que vem causando transtorno e grande preocupação aos organismos de segurança dos Estados Unidos, e de muitos outros países, inclusive o Brasil que vem sofrendo constantes ataques nos sites do governo[13], e os governantes do mundo inteiro têm demonstrado apreensão devido a serem alvos fáceis de hackers que constantemente atacam sistemas confidenciais comprometendo a infra-estrutura dos países.

De Acordo com Annunciação:

> A guerra cibernética também poderia ser usada dentro do conceito de guerra irrestrita, onde seriam atacados não só alvos estratégico-militares, mas

[13] O ataque de hackers realizado pelo grupo que se autodenomina "LulzSecBrazil" não causou, a princípio, nenhum estrago financeiro ao invadir os portais "www.presidencia.gov.br" e "www.brasil.gov.br", usados, em grande parte, para divulgação de material institucional.

> também os alvos civis de um país, a fim de causar uma desordem generalizada e difundir o medo. Após este ataque, seriam utilizadas outrastécnicas como ações terroristas, com o objetivo de minar a coesão interna, bem como a capacidade de resistência. Sampaio descreve uma lista de possíveis alvos dos ataques cibernéticos entre eles os computadores e programas com funções vitais, tais como: comando das redes de distribuição de energia elétrica, comando das redes de direção do tráfego aéreo, comando das redes de comunicação em geral, comando dos "links" com sistemas de satélites artificiais e comando das redes do Ministério da Defesa. Esses possíveis alvos são denominados por diversos autores como infra-estrutura crítica. (ANNUNCIAÇÃO, 2003, p. 6).

Esse novo tipo de ameaça levou o presidente Barack Obama criar o Comando de Operações Cibernéticas (Cyber Command), em Washington para defender o país desses ataques que vem ocorrendo com grande frenquência no país. Os norte-americanos acreditam que a Rússia e a China já teriam colocado na rede dos Estados Unidos, bombas lógicas, programas prontos para serem ativados e capazes de destruírem parte da infraestrutura do país. Um exemplo de guerra cibernética foi o que ocorrem em setembro de 2010 no Irã. O vírus *stuxnet*[14] danificou centrifugadoras do programa nuclear iraniano que tiveram panes irreversíveis. Não se sabe exatamente a origem dos ataques, mas as suspeitas recaem sobre os Estados Unidos e Israel. Segundo alguns especialistas, o stuxnet é um protótipo de uma arma virtual que pode levar a uma nova corrida armamentista.

A internet evoluiu a tal ponto que agora ela se configura como uma ameaça, não exatamente a internet em si, mas quem está por trás dela, o usuário que desfruta de sua grande capacidade de atravessar as barreiras virtuais sem dificuldades. Os worms e os vírus, que antes eram considerados simples incômodos, atualmente tornaram-se sérios desafios à segurança dos países. Por este motivo é que o Pentágono está acelerando os esforços para desenvolver uma nova geração de armas cibernéticas, capazes de alcançar inimigos militares que se comunicam em rede, mesmo quando essas redes não estão conectadas à internet.

Para se certificar da potência do vírus stuxnet, ele é capaz de invadir e reprogramar os controles automatizados de maquinários super modernas. Os stuxnet faz essas máquinas funcionarem a um regime tão excessivo que elas se autodestroem. Esse vírus e muitos outros não param de evoluir e podem ser realizados como ato de terrorismo industrial em qualquer parte do mundo. Uma outra ameaça que vem preocupando as autoridades governamentais é o vírus confincker. Ele atua infectando computadores comuns para formar uma super rede e já existem milhões de computadores infectados com esse vírus sem que os usuários percebam

[14] O stuxnet na realidade é um worm. (verme em português). É um programa malware, assim como o vírus, a diferente entre um e outro é que um vírus infecta um programa e precisa desse programa hospedeiro para se espalhar, enquanto um worm é um programa completo não depende de nenhum outro para se difundir.

isso. Não se sabe exatamente do que esse vírus é capaz, mas acredita-se que ele tem a capacidade de paralisar, por exemplo, o controle do tráfego aéreo de um país ou até mesmo alterar dados de um sistema judiciário. [15]

Muitos outros países, dentre eles o Brasil, estão preparando formas de se defender contra ataques cibernéticos ou efetuar ações ofensivas. O que não faltam são alvos para serem atacados, os mais suscetíveis são redes elétricas, fornecimento de água, hospitais, sistema bancários, etc. Hoje em dia, nada funciona de maneira isolada. No mundo moderno praticamente tudo é controlado a distância através de computadores e os crimes acompanham de perto toda essa evolução.

Richard Clark acredita que ataques cibernéticos mais sofisticados podem, por exemplo, descarrilar trens. Podem causar blackouts, não apenas cortando o fornecimento de energia, mas danificando os geradores de forma permanentes o que levariam meses para serem substituídos. Eles podem fazer coisas como provocar explosões em oleodutos ou gasodutos. Podem também causar panes nos sistemas de tráfegos aéreos fazendo com que aeronaves não decolem.

O caso dos Estados Unidos é bastante paradoxal, visto que ao mesmo tempo em que é a maior potência econômica, bélica e tecnológica do mundo é o país mais suscetível de ataques, pois mais do que qualquer outro país os Estados Unidos converteram todos seus sistemas ao controle de redes de computadores. As ferrovias norte-americanas, suas refinarias, pólos químicos, redes elétricas e o sistema bancários do país são controlados por meio de redes de computadores. E se algum hacker conseguir infiltrar-se em alguns desses sistemas provocará sérios danos ao país.

Portanto, a era da informação ocasiona certos riscos a sociedade moderna, devido à produção desenfreada das tecnologias que acabaram sendo utilizadas para práticas ilícitas. Segundo Richard Clark, ex-Conselheiro Especial para a Segurança no Ciberespaço do Governo Bush, existem vários tipos de crimes que podem ser praticados através da internet tais como, o estelionato cibernético que consiste numa ameaça de milhões de dólares por ano a bancos e ao cidadão comum. A espionagem cibernética onde acontece roubos de informações de empresas, roubam propriedades intelectuais, projetos de engenharias, formulas químicas e isso gerou um problema muito sério, pois esses ataques estão acontecendo constantemente em todos os países do

---

[15] Mais informação acessar: Ataques cibernéticos se tornaram armas de guerra. Disponível em: http://www.conjur.com.br/2011-mar-11/ideias-milenio-ataques-ciberneticos-tornaram-armas-guerra> Acesso em 25 jul. 2012

mundo, não configurando apenas um problema exclusivo dos Estados Unidos e sim um problema mundial.

Esses indivíduos, ou hackers, como são chamados no mundo cibernético, aproveitam-se da situação porque até agora não existem leis penais eficazes que possam punir esse tipo de crime, pois a burocracia para se aprovar uma lei é um processo lento enquanto os ataques hackers é tão rápido quanto o piscar dos olhos. E ainda existe a guerra cibernética na qual as nações podem atacar outras de diversas maneiras, a exemplo disso pode-se derrubar rede elétricas deixando um país sem energias durante horas ou mesmo podendo durar dias. Isso provocaria caos total no país podendo até mesmo este país responder a esses ataques de maneira convencional.

Segundo Nunes (1999), o conceito de ciberguerra, ainda que por vezes seja referido de uma forma diferenciada em relação ao conceito de guerra eletrônica, pode ser considerado como parte integrante do mesmo. A ciberguerra envolve, assim, a utilização de todas as "ferramentas" disponíveis ao nível da eletrônica e da informática para derrubar sistemas eletrônicos e de comunicações inimigos e manter os seus próprios sistemas operacionais intactos. Muitas das ações a serem desenvolvidas nesta área encontram-se ainda pouco definidas, devido fundamentalmente ao fato de se verificar um aparecimento contínuo de novos equipamentos e de ter sido apenas recentemente que os militares começam a encarar esta área tecnológica como uma nova forma de guerra. Alguns elementos característicos da ciberguerra aparecem aqui e ali de forma irregular e pouco sistematizada, à medida que as oportunidades da sua utilização vão surgindo. Os "cibersoldados"encontram-se normalmente confinados a Centros de Informação de Combate (CIC) equipados com monitores, computadores e outros equipamentos de alta tecnologia, mantidos por técnicos especializados. A sua missão consiste em fazer chegar aos respectivos comandantes os dados atualizados da situação verificada no campo de batalha

A guerra clássica, de concepção clausewitziana, tornou-se improvável devido ao alto grau de interdependência, sobretudo, econômica entre as nações. A guerra como um ato de violência destinado a forçar o adversário a submeter à vontade do outro, como proferia Clausewitz, parece ter perdido sua finalidade na atual conjuntura mundial. Parece paradoxal dizer que há uma crescente proliferação de ameaças e de conflitos no mundo, no entanto, muitos estudiosos das relações internacionais, principalmente os liberais, acreditam na impossibilidade da eclosão de uma guerra nos moldes das duas Grandes Guerras do século XX. Essa proliferação de ameaças e conflitos que afetam a segurança global tem produzido grande temor na população mundial, em estadistas e militares, e tem conduzidos estes dois

últimos a fazerem estratégias de segurança e de defesa eficazes para eliminar a ameaça advinda da era da informação.

CIBERTERRORISMO : A nova forma de crime no século XXI

A sociedade moderna apresenta vulnerabilidades em suas infraestruturas por ter um alto grau de dependência das redes de computadores, tornando alvos fáceis de atos terroristas, ou melhor, dos ciberterroristas. O conceito de ciberterrorismo foi utilizado pela primeira vez por Barry Collin, investigador no "*Institute for Security and Intelligence*", na década de 1980, para se referir à nova tendência do ciberespaço e do terrorismo, mas só a partir dos ataques às Torres Gémeas do World Trade Center em 11 de setembro de 2001, o "*FBI* divulgou inúmeros alertas sobre a responsabilidade e gravidade do ciberterrorismo", e foi também nesta conjuntura, que se intensificaram os ataques ciberterroristas, dos quais resultaram prejuízos avultados. (BATISTA, et al, 2003, p. 33).

De acordo com Mark Pollitt (1997), ciberterrorismom é a ação premeditada e realizada por hackers e crackers, contra informações, dados, sistemas e programas de computadores, com intenções políticas, econômicas, religiosas ou ideológicas resultando em violência contra alvos não combatentes de organizações ou agentes clandestinos.

O termo ciberterrorismo é a expressão usada para descrever os ataques terroristas realizados através da rede mundial de computadores, que tem por intuito provocar medo na população e causar danos a sistemas ou equipamentos nos países alvos. Os terroristas se aproveitam das fragilidades que apresentam tais sistemas e as facilidades que as novas tecnologias da informação trazem.

Os danos que esses ataques podem causar preocupam todos os países pelo fato de que praticamente tudo hoje em dia depende da internet para ser realizado. Há um perigo constante, pois ninguém sabe quando haverá um ataque e de onde pode originar tal ameaça. Assim,Nunes aduz que:

> A existência de um autêntico "calcanhar de Aquiles electrónico" e o receio de um ataque terrorista, tem vindo a gerar uma profunda reflexão em torno do facto de um actor individual, dotado de um computador e das necessárias competências técnicas, poder "deitar abaixo" a rede eléctrica de um País como os Estados Unidos. Esta assimetria, faz com que este País, detentor de uma superioridade militar convencional à escala global, tenha que desenvolver os mecanismos necessários para evitar o que muitos autores designam por "Pearl Harbour digital". (NUNES, 2009).

O FBI acredita que o ciberterrorismo, num futuro próximo, irá superar o terrorismo convencional. O problema é grave e requer medidas drásticas em relação à segurança e defesa do país. Robert Muller, diretor do FBI, fez apelo aos congressistas para que os mesmos aprovem uma legislação que ajude a combater as ameaças cibernéticas e que converta as agências de investigação e inteligência a "destinatários da informação". O Estado, mesmo sendo o principal ator das Relações Internacionais é regido por leis internas e internacionais, ele obedece a determinadas condutas que são impostas através de normas para que haja disciplina e respeito entre as nações, já que não há nenhuma autoridade suprema, legítima na ordem internacional. Contudo, essas organizações terroristas não se subordinam a nenhum tipo de legislação, assim, gera um outro problemas que preocupam as autoridades. Não são partes signatárias de tratados internacionais, recusa a obedecer todo e qualquer tipo de norma internacional, até mesmo do direito humanitário, no entanto, tais organizações buscam proteção nestas mesmas regras que repudiam. (WAISBERG, 2009, p. 2)

A identificação de membros pertencentes a esses grupos e a forma com a qual eles se estruturam são um grande problema, pois não há um exército uniformizado, não há um lugar fixo onde eles possam permanecer e isso dificulta bastante a ação do Estado em relação aos ataques, pois a cada dia eles se sofisticam e ganham mais adeptos.

Os ataques cibernéticos apresentam algumas vantagens em relação aos tradicionais ataques com bombas, evita-se a utilização de explosivos e que as organizações percam membros em missões suicidas, e ao mesmo tempo eles garantem a possibilidade de apenas um terrorista, munido exclusivamente de um computador conectado à Internet, fazer de forma anônima, e mais econômica, ataques as redes e a sistemas de informações de um determinado País.

Os exércitos do mundo inteiro estão se armando para uma possível guerra no ciberespaço. As armas são vírus potentes capazes de derrubar as redes elétricas de um país, por exemplo. Os EUA estão tendo despesas gigantescas para adaptar as tecnologias da informação de comunicação aos meios militares. Contudo, os EUA não estão desenvolvendo apenas armas virtuais, as tecnologias estão tão avançadas que o exército americano já usufrui de veículos aéreos não tripulados (VANT) e de canhões que também dispensa um condutor.

Portanto, como bem aduz Santos (2011), o desenvolvimento tecnológico exponencial que produziu a globalização da comunicação/informação e a globalização cultural veio conferir novas dimensões ao binômio “guerra/paz”. Na “Era da Informação” em que estamos mergulhados há pouco mais de vinte anos, a relação guerra/paz modificou-se de forma dramática, gerando

novos campos de combate, novos atores que se confrontam, novas armas, novas técnicas, tácticas e estratégias (SANTOS, 2011, p. 8).

CAPÍTULO III

APLICAÇÕES DA TECNOLOGIA DA INFORMAÇÃO E DA COMUNICAÇÃ NOS MEIOS MILITARES

Como resultado dos avanços das tecnologias a guerra muda constantemente de acordo com os progressos tecnológicos que a leva a importantes avanços na "arte da guerra". Na condição *sine qua non,* a tecnologia é sempre uma grande aliada dos exércitos que possui em seus arsenais de guerra. Essa nova era em que a ciência e a indústria unem-se para desempenhar papel essencial na produção de armas modernas, potentes e destrutivas, na qual a matéria-prima são as tecnologias da informação e da comunicação, que são capazes de criar e auxiliar no desenvolvimento de armas cada vez mais inteligentes, com um grande poder de precisão.

A tecnologia da informação e da comunicação tem provocado uma revolução nos assuntos militares, e o poder militar continua tendo grande relevância em setores decisivos das relações internacionais. Para os realistas a questão militar é a expressão mais alta do poder; o próprio poder econômico se submete ao poder militar, portanto é fundamental que o Estado esteja sempre forte militarmente, para que ele possa manter a estabilidade doméstica e a segurança em relação a agressões externas. O poder militar e econômico estadunidense possibilitam a consolidação de um poder político sobre os demais países que se encontram numa posição inferior a sua.

Os Estados Unidos ainda ostentam status de maior potencia bélica do planeta na atualidade. Como menciona Mann (2006, p. 31), o poderio norte-americano não tem rival, pois,

> (...) Quase todos os orçamentos militares do mundo estão se reduzindo, com exceção do norte-americano. Em 2001, este representava 36% do mundo inteiro – seis vezes maior que o da potência número dois, a Rússia, e sete vezes maior que o das três seguintes, França, Reino Unido e Japão. O orçamento americano de 2003 leva-o para mais de 40% do total mundial. Excede os gastos dos próximos 24 países juntos e é 25 vezes maior que os gastos somados de todos os sete "Estados Párias[16]" identificados pelos EUA como seus inimigos.

O teórico realista Edward Carr, saliente que o poder militar, sendo um elemento fundamental na vida do Estado, tornou-se não apenas um instrumento, mas um fim em si

[16] São considerados Estados Párias, todos aqueles que apresentam uma conduta contrária às normas internacionais de comportamento. São considerados Estados Párias Afeganistão, República da China, Iraque, Haiti, entre outros.

mesmo. E poucas dentre as guerras importantes dos últimos cem anos parecem ter sido travadas com o objetivo decidido e consciente de expandir o comércio ou o território. Travam-se as guerras mais sérias para tornar o próprio país militarmente mais forte ou, com mais frequência, para evitar que outro país se torne militarmente mais forte. (CARR, 2001, p. 146).

O instrumento de poder militar sempre foi algo crucial para a proteção da segurança nacional dos EUA, e no século XXI ele se torna ainda mais fundamental com a emergência das novas ameaças no ciberespaço. Essas novas ameaças desafiam o poder do Estado e sua soberania e mantê-los seguros é prioridade de qualquer Estado do sistema internacional. Os realistas salientam que o interesse nacional supremo dos Estados é manter a sua sobrevivência, e para sustentar essa sobrevivência é necessário um grande dispêndios nos assuntos militares.

É por esta razão que os Estados Unidos tendem a manter seu arsenal de guerra sempre renovado, amparado por aparatos da mais alta tecnologia, pois, na era da informação, onde a todo instante surgem novas ameaças que fazem com que suas forças armadas mudem de estratégias constantemente, é necessário que o exército esteja preparado para as mais diversas formas de ameaças. Destarte, o exército americano empenha-se em utilizar as tecnologias da informação e da comunicação nas suas estratégias e tem desenvolvido armas cibernéticas para combater os crimes praticados no ciberespaço.

Como esclarece o Major Nunes, no atual ambiente de informação, um ciber-ataque poderá assim ser considerado de nível estratégico se o seu impacto for tão importante que comprometa ou possa vir a comprometer a capacidade de um Estado assegurar as suas funções vitais como segurança e bem-estar para a sua população. Dentro deste contexto, tendo por base os seus efeitos, também as armas da guerra baseada na informação - Guerra de Informação – poderão ser consideradas como armas de "destruição massiva" (Libicki, 1996; Morris, 1995, apud Nunes, 1999), apresentando a sua utilização um enquadramento estratégico semelhante ao das Armas de Destruição Maciça (ADM). Devido à incerteza das consequências e ao potencial impacto de um ciberataque nas populações civis e na sociedade em geral, os Estados terão inevitavelmente de realizar uma avaliação dos riscos decorrentes da utilização de armas de informação por parte de atores hostis, nomeadamente por parte de grupos terroristas.

O potencial dessas novas tecnologias pode ser vistas nas duas guerras que iniciaram o século XXI, a do Afeganistão em 2001 e a do Iraque em 2003. Os Estados Unidos deram

um show de tecnologia e de violência nesses dois conflitos onde a grande maiorias de civis foram os maiores alvos.

Nas guerras modernas homens são substituídos por máquinas, robôs, e computadores que estão cada vez mais presentes nos conflitos da Era da Informação. Os soldados do futuro trabalham no manuseio de computadores sofisticados e não mais nos campos de batalhas tradicionais evitando assim baixas de soldados norte-americanos. Os EUA produzem esse tipo de tecnologia para proteger seu contingente militar, contudo, não há o mesmo interesse em relação aos povos de outros países. Os norte-americanos com seu poderio tecnológico-militar inigualável destruíram o Iraque, um país já arrasado com tantas guerras civis existente no próprio território e que não tinha chance alguma de lutar contra a máquina de guerra norte-americana.

O impacto do uso da tecnologia da informação e do conhecimento é superior a qualquer outra utilizada antes nos conflitos. Quando os Estados Unidos utilizaram a bomba nuclear em 1945 no Japão, não foi segredo alguns de onde as bombas se originaram, no entanto, um ataque cibernético de grande porte pode ser de difícil identificação caso ele venha a ser muito bem planejado.

Hackers são capazes de desviar correspondências eletrônicas confidencias de um país e lê-los e depois enviar para seus endereços de destino. Isso já ocorreu várias vezes com correspondências pertencentes ao pentágono e a OTAN. E estes organismos têm muita pressa em conter esse mal que cresce e assola o ciberespaço do país.

A intensa capacidade que têm atualmente os chips de computadores que aliam-se à tecnologia avançada de câmeras e sensores, tornou-se indispensável para que o exército tenha um bom desempenho nos conflitos atuais. Toda a comunicação entre os militares acontece em tempo real e a população mundial pode acompanhar em casa todos os acontecimentos ocorridos durante a guerra no exato momento em que elas estão acontecendo. Essas novas tecnologias podem conduzir uma guerra sem risco para os próprios soldados, mas podem significa aniquilação de civis inocentes. As armas inteligentes são precisas e podem acertar seu alvo com uma margem mínima de erro. Muitas dessas armas foram utilizadas na guerra do Golfo em 2003. Assim, como bem anuncia Waack,

> À revolução da informação seguiu-se uma revolução na doutrina militar americana, que já se vislumbrara como "exercício piloto" na primeira Guerra do Golfo: trata-se do aperfeiçoamento da extraordinária capacidade de integração de vários sistemas, e da capacidade de transmissão de informações em tempo real do campo de batalha para qualquer dos níveis envolvidos em decisões bélicas. Na breve fase preparatória de bombardeios

> aéreos, durante a ação de 2003, os americanos empregaram quase que exclusivamente “armas inteligentes” ao contrário do que ocorrera em 1991. (Waack, 2009, p. 469).

A tecnologia norte-americana evolui muito rapidamente e os aparatos de guerra tornam-se obsoletos com a mesma velocidade. O contingente de soldados dos Estados Unidos está diminuindo e tecnicamente eles estão se fortalecendo. As máquinas vieram de fato substituir o homem em diversas áreas e no meio militar isso não seria diferente.

A revolução da informação provocou uma Revolução nos Assuntos Militares (RAM). Segundo Turner (2000), a Revolução em Assuntos Militares pode ser definida como uma grande mudança na natureza da guerra, resultante do emprego de novas tecnologias as quais, combinadas com as dramáticas mudanças na doutrina, nos conceitos operacional e organizacional militares, alteram fundamentalmente o caráter e a conduta das operações militares. (TUNER, 2000, apud Longo, 2007).

A RAM foi impulsionada pelas novas tecnologias da informação e da comunicação. Satélites vigiam o mundo vinte e quatro horas por dia, aviões aéreos não tripulados já estão sendo utilizados nos conflitos modernos evitando morte de soldados, redes de sensores sofisticados, “aviões invisíveis” robôs soldados, essas são apenas algumas das tecnologias que podem ser encontradas nas atualidades. Porém se a guerra no ciberespaço é uma virtual, intangível, por que então os países investem tanto em armamentos convencionais?

Existe uma série de motivos para isso acontecer, um deles é o fato de que armas cibernéticas não garantem a segurança no mundo real, e como os ataques cibernéticos tem conseqüências concretas e graves, e os Estados Unidos já deixaram claro que poderão responder aos ciberataques de maneira convencional, caso eles venham a provocar dano de grande proporção no país.

3.1 ARMAS CIBERNÉTICAS PARA UMA GUERRA DIGITAL: Uma nova corrida armamentista?

Para combater as ameaças cibernéticas o governo norte-americano e o Pentágono estão empenhados em desenvolver armas cibernéticas capazes de infiltrar as redes militares dos inimigos mesmo quando estes não estão conectados a internet e derrubar as infraestruturas chaves desses países. O pentágono tem pressa na produção dessa nova geração de armas que vem causando uma grande revolução nos meios militares para tentar eliminar os crimes no ciberespaço que não para de crescer. Contudo, outros países já estão compelidos a desempenhar a mesma política de produção dessas armas, já que as ameaças partem de todos

os lugares e estão em todos os lugares, e essa conjuntura proporciona ao mundo ver novamente uma nova corrida armamentista e dessa vez, diferentemente do que ocorreu na Guerra Fria, onde apenas dois países disputavam a corrida armamentista, na atualidade muitos países pretendem se fortalecer militarmente, para se defenderem das ameaças cibernéticas que desafiam a segurança e a defesa dos países.

Assim, nas palavras de Wight (2002, p. 257) em virtude do progresso da ciência militar, a corrida armamentista teve continuidade pelo aprimoramento - e não pelo aumento - das armas. De corrida quantitativa, passou a ser qualitativa. Um ano após sua primeira utilização, a bomba atômica foi chamada de "arma absoluta"," uma descrição que talvez tenha fomentado o perigoso falso juízo de que ela não havia tomado seu lugar como um simples acréscimo à enorme variedade de armas já existentes, mas sim que as havia tornado desnecessárias.

A corrida armamentista, no período da Guerra Fria, atingiu proporções tais que na década de 1960 as duas potências já tinha em suas posses armas suficientes para destruir o mundo inteiro. Houve um gasto bélico desnecessário de ambas as partes, já que eram necessárias poucas dessas armas para conseguir tal proeza, devido a sua capacidade que era superior as bombas de Hiroshima e Nagasaki. No entanto, a peculiaridade da Guerra Fria era de que, em termos objetivos, não existia perigo iminente de guerra mundial. Mais que isso: apesar de retórica apocalíptica de ambos os lados, mas, sobretudo do lado americano, os governos das duas superpotências aceitaram distribuição global de forças no fim da Segunda Guerra Mundial, que equivalia a um equilíbrio de poder desigual mas não contestado em sua essência. (HOBSBAWM, 2009, p. 224).

A Guerra Fria possibilitou avanços importantes em tecnologias, sobretudo nas tecnologias espaciais nos quais criou condições para o homem militarizar o espaço e conquistar o quarto campo de conflito. Foram criados satélites para “vigiar” o inimigo dos quais destacam-se os satélites de comunicações, satélites científicos e satélites militares. Os satélites também são responsáveis por disseminar informação pelo mundo.

A revolução da informação tem proporcionado muita facilidade na difusão de tecnologia e de informação gerando uma guerra de informação no mundo, e tornando possível a emergência de novos tipos de insurgências informacional, oriundos a partir das tecnologias computacionais. A guerra no ciberespaço é atualmente uma realidade e todos os países, sobretudo os Estados Unidos, estão militarmente se fortalecendo para combater mais essa ameaça.

Existe uma grande probabilidade de haver um confronto com armas cibernéticas entre EUA e Irã ou Síria, segundo os planejadores militares norte-americanos, esta hipótese não está descarta e elas podem ser utilizadas, por exemplo, contra inimigos, cujos alvos sejam os sistemas de defesa aérea. O montante dos gastos divulgados pelo Pentágono sobre segurança cibernética e cibertecnologia (ofensiva e defensiva) é muito alto. Os EUA, atualmente deixam de investir no bem-estar social da população do país para investir em armamentos para melhor garantir a segurança nacional. É relevante mencionar que,

> No Iraque, durante os combates de 2007, as forças norte-americanas e a Agência de Segurança Nacional, usaram ferramentas cibernéticas para confundir sinais de celulares e computadores portáteis que os insurgentes utilizavam para coordenar seus ataques, segundo relatos publicados e confirmados por ex-funcionários norte-americanos. Operadores norte-americanos usaram técnicas cibernéticas para enganar o inimigo com informações falsas, em alguns casos levando rebeldes a emboscadas criadas por eles.[17]

As armas da era cibernética são intangíveis, virtuais, mas os danos são reais. Tal afirmação pôde ser comprovada com o ataque do vírus stuxnet as usinas nucleares do Irã que tiveram danos irreversíveis e prejuízos incalculáveis. Ele é considerado a primeira arma cibernética feita apenas com linhas de código, contudo não será a única. Funcionários do Departamento de Segurança Interna Norte-Americano afirmou que o vírus stuxnet é capaz de invadir um sistema automaticamente, roubar a fórmula do produto que está sendo fabricado, alterar todos os componentes que estão sendo utilizados, e ainda é surpreendentemente inteligente para dizer ao operador e ao software antivírus que tudo está operando em perfeita condições.

É assustador a sutileza com a qual ele invade o sistema e a devastação que ele provoca. Autoridades governamentais e militares temem que essa arma possa cair nas mãos de terroristas podendo eles a modificar e se tornar ainda mais letal, visto que os cibercriminosos já têm capacidade intelectual para tal façanha. Ele é uma ameaça para as principais indústrias como as usinas de abastecimento de água, as plataformas de petróleo, centrais elétricas, etc.

A era da informação alterou significativamente o papel dos Estados nas Relações internacionais, transformou a forma de fazer a guerra e influenciou o pensamento militar no século XXI. Atualmente não mais se recruta soldados pelo seu porte físico e sim pela sua

[17] Disponível em http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story_1.html acesso em 19 de maio de 2012.

capacidade intelectual. As forças armadas americanas por meio de anúncio estão recrutando hackers para tornarem-se cibersoldados para combater as ameaças virtuais eficazmente, pois é bem mais vantajoso para um país contratar esses gênios da computação que puni-los, e essa não é só uma política do governo dos Estados Unidos, outros países, como China, Rússia, Israel e Brasil estão seguindo esse modelo.

Os militares americanos já estão autorizados a realizarem ataques cibernéticos sobre seus inimigos para defender os interesses do país. Analistas políticos acreditam que as conseqüências desses ataques serão desastrosas e as ciberarmas são ainda mais perigosas que as convencionais devindo a sua alta proliferação e pelos estragos que elas podem causar.

As armas cibernéticas não são apenas as únicas novidades da tecnologia militar no século XXI. A cada dia surge uma nova arma, armas do tipo convencionais com efeitos super danosos para a população civil. Apesar de a guerra ser travada no ciberespaço, que é o campo "invisível", virtual, os Estados não dispensam nem descartam a possibilidade de um confronto real.

O medo traz as novas ameaças à segurança dos países fazem com que eles acabem se armando trazendo de volta o fantasma do período denominado de "*paz armada*" período entre 1871 e 1914, considerado crucial no preparo do cenário catastrófico da Primeira Grande Guerra, onde grande parte do orçamento da Europa foram gastos com armamentos, favorecendo uma corrida armamentista, o que levou o velho mundo a se transformar num verdadeiro campo de guerra.

Como aduz Herz (1950) no Dilema da Segurança onde se verifica o momento em que um Estado quer se garantir sua própria segurança, mas acaba sendo considerado como uma ameaça para os outros países. Em poucas palavras, o Dilema da Segurança configura-se da seguinte forma:

> Um Estado A procura garantir sua segurança e para isso adquire armas. Os demais Estados, que não tem como sondar as intenções do Estado A, sentem-se ameaçados e, por sua vez, também procuram adquirir armamentos para garantir sua segurança. Percebendo o armamento dos demais Estados, o Estado A confirma sua política original como correta e procura se armar ainda mais, de maneira a garantir sua segurança. Com isso, todos os Estados estão engajados em uma corrida armamentista que não tem saída nem vitorioso. O resultado disso é que, apesar de todos procurarem garantir sua própria segurança, tanto o Estado A quando os demais estão menos seguros depois da aquisição de armas do que antes. (Herz apud NOGUEIRA; MESSARI, 2005, p. 36).

Portanto, a obtenção de armamento não garante a segurança dos Estados e sim gera insegurança no mundo devido à corrida armamentista que instiga a proliferação de armas.

Na era da informação não é diferente das outras épocas. Os Estados continuam se armando e como as ameaças são muitas e diversificada os novos meios de combatê-las também os são.

O ciberterrorismo encontrou um novo cenário bélico, fazendo parecer obsoletas as armas utilizadas nas guerras convencionais, dado que o terrorista é um inimigo, muitas vezes sem rosto e sem fronteiras, tendo encontrado na Internet as facilidades e possibilidades que essa oferece (Pastor SÉRGIO GARCIA, apud BATISTISTA, 2003, et al).

As armas da era cibernéticas podem ser encontradas nas mais diversas formas. As aeronaves não tripuladas já são uma realidade. O X-47B é um avião bombardeiro, praticamente impossível de ser detectado por radar, daí ele ser chamada de "avião invisível". Foi desenvolvido para realizar operações completamente autônomas e é uma aeronave controlada por sistemas de informação.

Assim como diria Wiener, muito provavelmente e quase certamente, a ação de guerra por meio dos computadores pode configurar uma utilização dos mesmos como arma de destruição em massa. (SAMPAIO, 2001, p. 8)

As armas convencionais são tipos de armas que tem por objetivo de ataques as estruturas físicas, e as armas cibernéticas tem por objetivos atingir as estruturas lógicas, no entanto podem causas também danos físicos. Na era da informação também são encontradas outros tipos de armas nunca vistas antes em nenhuma outra guerra. Fala-se de armas de impulsos eletromagnéticos, são da categoria das armas de energia direta. A bomba eletromagnética não tem cheiro, nem cor, não produz fumaça, é invisível, e não causa mortes nem provoca nenhuma cratera sobre o solo caso seja utilizada. Mas então para que serve uma bomba que aparentemente parece ser inútil? Seus principais alvos são os cabos, as redes, os servidores, os circuitos de comunicações eletrônicas, os processadores, os comutadores, os servidores, os computadores, o coração dos *bunkers* - estes, difíceis de serem atingidos por outros meios. Conseqüências diretas? A interrupção momentânea ou definitiva das comunicações, das trocas de dados, dos sistemas de comando, dos aparelhos de detecção, de medida e de controle. Sua utilização visaria, no quadro de uma ofensiva aérea ou terrestre, a isolar o inimigo, a colocá-lo na incapacidade de controlar seus meios e suas forças ou de se informar sobre a situação da batalha em curso. (POUPÉE, 2003).

Direta ou indiretamente a tecnologia da informação influencia essas novas espécies de armas. Assim, versando sobre o assunto de tecnologia da informação, Castells salienta que

a entre as tecnologias da informação, compreende o conjunto convergente de tecnologias em microeletrônica, computação (software e hardware), telecomunicações/radiodifusão, e optoeletrônica. (SAXBY, 1990, MARX 1991, apud CASTELLS, 2008).

Os Estados Unidos estão desenvolvendo poderosos satélites equipados com raio laser capazes de danificar ou simplesmente sabotar satélites inimigos, sejam eles de utilidades militares ou de telecomunicações, prejudicando seriamente os outros países.

Na guerra de informação defensiva, os Estados Unidos em seu campo estratégico, abarca políticas de segurança nos quais podem ser usadas as armas cibernéticas como forma de retaliação. Assim como publicações de leis punitivas para esse tipo de crime, visto que as leis atualmente existentes não atingem o ciberespaço e por isso a necessidade de existirem leis que especifiquem diretamente os crimes virtuais.

A guerra é ato ilícito à luz do Direito das Gentes. Apenas começaram a existir normas proibitivas à guerra no século XX, e sua ilicitude veio a concretizar-se, apenas com o nascimento da Carta das Nações Unidas (Carta da ONU) celebrada em 1945 em São Francisco.

No século XXI surgem novos desafios ao Direito Internacional. A partir do momento em que protagonistas não-estatais começam a ganhar força e destaque no cenário internacional e iniciam um novo paradigma de guerra onde põe por terra a teoria clássica da guerra, onde os oponentes eram sempre estados soberanos. Porém a guerra chega a uma proporção tal que um único individuo pode ameaçar as principais infraestruturas de qualquer país através do ciberespaço e provocar uma guerra cibernética em larga escala.

CONCLUSÃO

No decorrer deste trabalho, foram apresentadas as novas ameaças que emergiram – com o advento da Revolução da Informação, oriunda nos Estados Unidos da América – nesse inicio de século, e no qual vem causando sérios desafios a política mundial. Nesse sentindo, buscou-se demonstrar as fragilidades que possuem a segurança e a defesa dos EUA quanto a questão cibernética no país e ainda os perigos que causam as novas tecnologias, sobretudo a da informação e da comunicação, quando utilizadas de forma inadequadas com intenção de provocar medo, insegurança e desordem, não apenas no espaço cibernético, mas em todo o sistema internacional. Vale ressaltar que em meio a tais ameaças, houve a necessidade do desenvolvimento de armas cibernéticas para combater as insurgências virtuais que vem ganhando força e destaque no cenário internacional.

Assim com aduz Joseph Nye sejam quais forem os efeitos futuros da interatividade e das comunidades virtuais um efeito político dos fluxos mais intensos da informação livre por meio de múltiplos canais já está claro: os Estados perderam grande parte de seu controle das informações sobre suas próprias sociedades. (...). A revolução da informação está tornando a política mundial mais complexa ao dar poder a protagonistas não-estatais, para o bem ou para o mal, e reduzindo o controle dos governos centrais, mas também está afetando o poder entre os Estados. (NYE, 2009, pp. 282-286)

Num primeiro plano, procurou-se abordar a respeito da Era da Informação, que teve seu advento nos EUA, ainda durante o período da Segunda Guerra Mundial com o nascimento do computador em seguida com o surgimento da internet na qual revolucionou os meios de comunicação. Assim como ocorreu com a Revolução Industrial, esta atual revolução vem promovendo uma série de transformações no mundo inteiro; proporcionou uma propagação de tecnologias no qual contribuiu para a emergência de novas ameaças, sobretudo as virtuais, que vem causando sérios desafios para os Estados nesse início de século, e ainda abala a soberania estatal.

A Revolução da Informação provocou uma evolução nas tecnologias da informação e da comunicação, desta feita, surgiram novas formas de crimes praticados através da internet. Estes são titulados, como estelionato cibernético, espionagem cibernética, e o mais grave deles é configurado como ciberterrorismo. A Era da Informação promoveu um mundo cada vez mais interligado e praticamente sem fronteiras e isso tem facilidade uma onde gigantesca de crimes virtuais praticados por atores não-estatais.

Contudo, a tecnologia da informação e da comunicação tem também apresentado resultados positivos, quando, nas palavras de Nye (2009), facilita as tarefas de coordenação e de fortalecimento do poder de ativistas de direitos humanos (...). Porém o grande problema é que nem todas as pessoas se utilizam da maneira correta dessas tecnologias, muitas delas aproveitam-se da falta de regulamentação no ciberespaço para cometerem crimes virtuais que já são praticados em larga escala no mundo inteiro.

O crescimento dos crimes virtuais é praticado devido as facilidades que as tecnologias da informação e da comunicação proporcionam aos seus usuários, por outro lado existem as dificuldades da aplicação de leis para a punição dos infratores, e ainda as burocracias legislativas não conseguem acompanhar a rapidez com que os crimes virtuais acontecem.

Destarte, não apenas leis estão sendo criadas para combater os crimes cibernéticos, mas os exércitos se munem de armas virtuais para eliminação desse mal que assola o mundo na atualidade.

Embora, a ciber-criminalidade exista atualmente, o ciberterrorismo ainda se apresenta apenas como uma hipótese, pois de acordo com Dorothy Denning, embora a probabilidade da ocorrência de um verdadeiro ataque ciberterrorista em larga escala não seja elevada, porém não é, de todo, impossível de acontecer. A autora considera que a ameaça ciberterrorista irá crescer devido ao desenvolvimento informático e tecnológico e que esta ameaça deve ser seriamente considerada. (VILELA, 2010, p.13). Por essa Razão, os Estados Unidos têm um extraordinário gasto anual com armamentos, pois não descartam a possibilidade de ocorrer uma guerra cibernética, além do mais, caso eles venham a ser atingidos por um ataque virtual que causem danos materiais ao país os agressores serão seriamente punidos, podendo assim a retaliação ser respondida com armas convencionais.

Portanto, conclui-se que, com a chegada da Revolução da Informação muitas transformações ocorrem no mundo e muitas ainda estão por vir. Essa revolução, assim como a Revolução Industrial trouxe vários benefícios para a população mundial e com ela veio também sérios problemas. O mundo se globalizou e os problemas também tornaram-se globalizados e tudo que ocorre num país consequentemente atingirá os demais devido ao elevado grau de interdependência entre os mesmos, fenômeno este que facilita os crimes virtuais que são capazes de ultrapassar qualquer fronteira.

Os Estados Unidos tentam se proteger desses ataques produzindo armas cada vez mais sofisticadas e inteligentes. Estão sendo desenvolvidas pelo Pentágono, não apenas armas virtuais, mas também armas convencionais, o que tem instigado outros países a

desempenharem a mesma política armamentista para combater os possíveis ataques ciberterroristas. Contudo, na atual conjuntura mundial assiste-se uma nova corrida armamentista, na qual difere da ocorrida do período de Guerra Fria pelo fato de que, não penas duas potências procuram se fortalecer militarmente, mas diversos países do globo destinam seus orçamentos na construção de armamentos para a segurança e defesa de seu território e atualmente do ciberespaço.

Portanto, entende-se que. utiliza-se a tecnologia para combater as próprias inovações tecnológicas.. Assim, como confere Vilela (2010), compreendendo que "o ciberterrorismo é, neste momento, uma das ameaças mais complexas que impende sobre o mundo ocidental", a defesa da informação passou, e adivinha-se que passará ainda mais a ser, uma ação estratégica. Neste sentido, dada a dependência dos sistemas de informação, os Estados já apostam numa postura mais pró-ativa nesta defesa e adivinha-se que apostem cada vez mais no controle e domínio do ciberespaço.

REFERÊNCIAS

ALMEIDA, Manuel António Lourenço de Campos. **Direito Humanitário e Conflitos Modernos**. Revista Militar, janeiro de 2003. Disponível em: <http://usacac.army.mil/CAC2/MilitaryReview/Archives/oldsite/portuguese/4thQtr03/almeida.pdf>. Acesso em: 21 mar. 2012.

ANNUNCIAÇÃO, João Wander Nascimento de. ***Ciberwar: Uma resposta genérica de ações defensivas para a MB.*** Disponível em: http://www.egn.mar.mil.br/arquivos/cepe/ciberwar.pdf. Acesso em: 09 de jun. 2012.

ARAÚJO, Paulo Sérgio de. **O USO DA TECNOLOGIA DA INFORMAÇÃO COMO ARMA DE ATAQUE.** Disponível em http://www.profissionaisti.com.br/wp-content/uploads/2011/11/O-USO-DA-TECNOLOGIA-DA-INFORMA%C3%87%C3%83O-COMO-ARMA-DE-ATAQUE.pdf> Acesso em: 05 de jun. 2012.

AMEAÇAS CIBERNÉTICAS: Novos níveis de violência. Disponível em: <http://www.dawnbible.com/pt/2011/1105-hl.htm>. Acesso em: 12 abr. 2012.

Ataques cibernéticos se tornaram armas de guerra. Disponível em: http://www.conjur.com.br/2011-mar-11/ideias-milenio-ataques-ciberneticos-tornaram-armas-guerra> Acesso em 25 jul. 2012

ANNUNCIAÇÃO, João Wander Nascimento de. **Ciberwar: Uma resposta genérica de ações defensivas para a MB.** Disponível em: <http://www.egn.mar.mil.br/arquivos/cepe/ciberwar.pdf>. Acesso em: 09 jun. 2011.

ATAQUES DIGITAIS NA ESTÔNIA. Disponível em**:** **<**http://informatica.hsw.uol.com.br/hacker-economia-eua1.htm**>.** Acesso em: 25 jun. 2012.

BARBEIRO, Heródoto. **O Relatório da CIA**: como será o mundo em 2020. Rio de Janeiro: Ediouro, 2006.

BATISTA, Gonçalo; RIBEIRO, Carlos; AMARAL, Feliciano. ***CIBERTERRORISMO***: A NOVA FORMA DE CRIME DO SÉC. XXI COMO COMBATÊ-LA?

BANCON, Francis. **Novum Organum ou Verdadeiras Indicações Acerca da Interpretação da Natureza.** São Paulo: Abril, 1973**.**

BILLO, Charles G. CHANG, Welton. Ciber Warfare: **An Analysis of the Means and Motivations of Selected nation States.** INSTITUTE FOR SECURITY TECHNOLOGY STUDIES AT DARTMOUTH COLLEGE. November 2004.

BRITO, Luis Vila de. ***A evolução tecnológica militar na Era da Informação.*** In: Revista Militar. Disponível em: <http://www.revistamilitar.pt/modules/articles/article.php?id=536>. Acesso em: 02 mar. 2012.

BRIGAGÃO, Clóvis; RODRIGUES, Gilberto. ***Globalização a olho nu***. São Paulo: Moderna, 1998.

BUZAN, Barry. HERRING, Eric. **The Arms Dynamic in World Politics.** Lynne Rienner Publishers.1998.

CARLI, Daniel Michelon De. ***Crimes Virtuais No Brasil - Uma Análise Jurídica***. Disponível em: <http://www-usr.inf.ufsm.br/~dcarli/elc1020/artigo-elc1020.pdf>. Acesso em: 24 abr. 2012.

CARR, Edward H. ***Vinte anos de Crise: 1919-1939***: Uma introdução aos estudos das relações internacionais. Brasília: UNB. 2ª edição, 2001.

CASTELLS, Manuel. ***A SOCIEDADE EM REDE***. Vol. 1. 11Ed. São Paulo: Paz e Terra, 2008.

CyberWar: Security, Strategy and Conflict in the Information Age, *Campen, Dearth and Goodden, ©AFCEA International Press 1996.*

CANABARRO, Diego Rafael. Resenha do livro ***Cyber War***: The Next Threat To National Security And What To do About It? Disponível em: <http://seer.ufrgs.br/ConjunturaAustral/article/view/20585/12058>. Acesso em: 13 mai. 2012.

CLAUSEWITZ, Carl von. ***Da Guerra***. São Paulo: Martins fonte. 2003.

CÉSAR, Luiz Fernando Panelli. "Tratado de Não-Proliferação Nuclear-TNP (1968)" In: ***História da Paz***. MAGNOLI, Demétrio (organizador). São Paulo: Contexto, p. 385-416, 2008.

DUPAS, Gilberto**.** ***O Poder dos Atores e a Nova Lógica Econômica***. Disponível em: <http://www.brasiluniaoeuropeia.ufrj.br/pt/pdfs/o_poder_dos_atores_e_a_nova_logica_economica_global.pdf>. Acesso em: 11 mai. 2012.

ENTENDA QUEM SÃO OS ANONYMOUS E O LULZSEC. Disponível em: <http://tecnologia.terra.com.br/noticias/0,,OI5200054-EI12884,00 Entenda+quem+sao+os+Anonymous+e+o+LulzSec.html >. Acesso em: 23 jun. 2012.

FERRER, Walkiria Martinez Heinrich, SILVA, Jacqueline Dias da**. A soberania no processo de globalização**: tradicionais conceitos e seus novos paradigmas. Disponível em: <http://www.diritto.it/pdf/26843.pdf. > Acesso em: 05 mar. 2012.

FUNARI, Pedro Paulo. "Guerra do Peloponeso" In:. MAGNOLI, Demétrio (org.). ***História das Guerras*****. São Paulo**: Contexto, p.p. 19-45, 2009.

GALLAGHER, Michael**. Especialistas temem guerra cibernética no futuro.** Disponível em: <http://www.bbc.co.uk/portuguese/celular/noticias/2012/04/120430_cyberguerra_futuro_fn.shtml>. Acesso em: 10 mai. 2012.

GARCIA, Flúvio Cardinelle Oliveira. **Ciberespaço:** Formas de regulamentação. Disponível em: <http://jus.com.br/revista/texto/11747/ciberespaco-formas-de-regulamentacao>. Acesso em: 05 jun. 2012.

GIBSON, William. **Neuromancer.** Disponível em: <http://www.libertarianismo.org/livros/wgneuromancer.pdf> Acesso em; 26 jul. 2012

GUGIK, Gabriel. **A História dos computadores e da computação**. Disponível em: <http://www.tecmundo.com.br/mac-os-x/1697-a-historia-dos-computadores-e-da-computacao.htm>. Acesso em: 12 abr. 2012.

HUNTINGTON, Samuel P. ***O Choque de Civilizações e a Recomposição da Ordem Mundial***. Rio de Janeiro: Objetiva, 2007.

HISSA, Carmina Bezerra ***Comércio*** **Eletrônico à Luz do Código de Defesa do consumidor.** Disponível em: <http://www.eumed.net/libros/2009a/491/Direito%20a%20Privacidade.htm>. Acesso em: 06 mai. 2012.

HOBSBAWM, Eric. A Era dos Extremos: O breve Século XX-1914-1991. São Paulo: Companhia das Letras. 2009.

KEOHANE, Robert O., NYE Jr., Joseph. *Power and Interdependence in the Information*. Foreign Affairs, v. 77, nº 5, set/out, Council of Foreign Relations, 1998. Disponível em: <http://www.scribd.com/doc/19106523/Keohane-e-Nye-Jr-Resenha>. Acesso em: 12 jun. 2011.

KOHN, Stephanie. **Hackers e Crackers**: as diferenças. Disponível em: < http://olhardigital.uol.com.br/produtos/digital_news/noticias/hackers_e_crackers_saiba_as_diferencas. > Acesso em 15 jul. 2012.

LAFER, Celso. **As Novas Dimensões do Desarmamento: os Regimes de Controle das Armas de Destruição em Massa e as Perspectivas para a Eliminação das Armas Nucleares.** Disponível em:< http.// www.iea.usp.br/artigos//>. Acesso em: 06 jun. 2011.

LIND, Willian S. **Compreendendo a Guerra de Quarta Geração**. Military Review. Janeiro-Fevereiro 2005. Disponível em: <http://www.ecsbdefesa.com.br/fts/MR%20WSLind.pdf> . Acesso em: 27 jun. 2012.

LOBATO, Pedro. **Ataques cibernéticos poderão ser considerados atos de guerra**. Disponível em: <http://b33p.com.br/2011/06/ataques-ciberneticos-poderao-ser-considerados-atos-de-guerra>. Acesso em: 27 mai. 2012.

LONGO, Wladimir Pirró e. **Tecnologia Militar**: Conceituação, Importância e cerceamento. Artigo publicado na revista TENSÕES MUNDIAIS, vol. 3, n. 5, pág. 111-143, Fortaleza/CE, 2007.

LUCCI, Elian Alabi. BRANCO, Anselmo Lázaro. Geografia: Homem e Espaço – As relações internacionais e a organização do espaço mundial. 18ª Ed. – São Paulo: Saraiva, 2002.

MAGNOLI, Demétrio. "Guerras da Indochina" In:. MAGNOLI, Demétrio (org.). ***História das Guerras*. São Paulo**: Contexto, p.p. 391-423.

MANN, Michael. ***O Império da Incoerência***: a natureza do poder americano. Rio de janeiro: Record, 2006.

MARTINS, José Miguel Quedi. **Digitalização e Guerra Local**: como fatores de equilíbrio internacional. 2008. 327 f. Tese (Doutorado em Ciência Política). Curso de Pós-Graduação em Ciência Política, Universidade Federal do Rio Grande do Sul. Porto Alegre.

MEARSHEIMER, John J. A Tragédia da política das grandes potências. Rio de janeiro: Gradiva, 2007.

MENDONÇA, Gustavo Resende. Resenha do Livro "**The Future of Power**", de Joseph Nye. Disponível em: < http://mundorama.net/2011/04/25/resenha-do-livro-%E2%80%9Cthe-future-of-power%E2%80%9D-de-joseph-nye-por-gustavo-resende-mendonca.> Acesso em 25 jun. 2012

MIRANDA, Napoleão. ***Globalização, Soberania Nacional e Direito Internacional***. R. CEJ, Brasília, n. 27, p. 86-94, out./dez. 2004.

MULCAHEY, Sean F. ***A dinâmica da mudança da vantagem militar na Era da Informação.*** 2004**.**

NYE, Joseph S. ***Cooperação e Conflitos nas relações internacionai:*** São Paulo. Gente. 2009.

_____. ***O Paradoxo do Poder Americano***. São Paulo: UNESP, 2002.

_____. ***The future of the power***. Nova York: PublicAffairs, 2011.

NETO, Ricardo Bonalume. **EUA miram ataques cibernéticos** Disponível em: <http://www.observatoriodaimprensa.com.br/news/view/eua-miram-guerra-cibernetica>. Acesso em: 07 jun. 2011.

NOGUEIRA, João Pontes. NOGUEIRA, Nizar Messari. **Teoria das Relações Internacionais: correntes e debates**. Rio de Janeiro: Elsevier, 2005.

NUNES, Paulo Fernandes Viegas. **Ciberterrorismo:** Aspectos de Segurança. Disponível em: <http://www.revistamilitar.pt/modules/articles/article.php?id=428>. Acesso em: 25 mai. 2012.

_____. **Imapcto das Novas Tecnologias no meio militar**: a guerra de informação. Disponível em: < http://www.airpower.au.af.mil/apjinternational/apj-p/2000/2tri00/nunes.htm> Acesso em: 01 fev. 2012.

OLIVEIRA, Flávio Rocha de. **Os Estados Unidos da América no Pós-Guerra - Transformação na Política de Segurança**. São Paulo. Plêiade. 2009.

PHISTER JR, Paul W. PLONISCHI, Igor G. **Aplicações Militares das Tecnologias da Informação.** Disponível em: <http://www.airpower.au.af.mil/apjinternational/apj-p/2004/4tri04/phister.html>. Acesso em: 04 jul. 2011.

POLLITT, Mark M.,October 1997, "**Cyberterrorism - Fact or Fancy?**", Proceedings of the 20th National Information Systems Security Conference, págs. 285-289. Disponível em: <http://www.cs.georgetown.edu/~denning/infosec/pollitt.html>. Acesso em: 02 abr. 2012.

PORTELA, Paulo Henrique Gonçalves. **Direito Internacional Público e Privado**. Bahia: Podivm, 2010.

POUPÉE, Karyn. **Nascem as armas eletromagnéticas.** Bibliotecadiplô. 2003. Disponível em: <http://diplo.org.br/2003-02,a565>. Acesso em: 22 de jun. 2012.

SAMPAIO, Fernando G. Ciberguerra. Guerra eletrônica e informacional: um novo desafio estratégico. Disponível em: <http://www.defesanet.com.br/esge/ciberguerra.pdf> Acesso em: 26 jun. 2012.

SANTOS, José Alberto Loureiro. **Conflitos na era da informação:** as revoltas árabes. Disponível em: http://www.acad-ciencias.pt/files/Mem%C3%B3rias/General%20Loureiro%20dos%20Santos/jalsantos_16_06_2011.pdf. Acesso em: 21 jul. 2012

SARFATI, Gilberto**.** ***Teorias das relações Internacionais***. São Paulo: Saraiva, 2005.
SENE, Eustáquio de. MOREIRA, João Carlos. **Trilhas da geografia**: Espaço geográfico mundial e globalização. São Paulo: Scipione, 2001.

SIETENFUS, Ricardo. ***Relações Internacionais.*** São Paulo: Manole, 2004.

SILVA, José Alexandre F. M. **Guerra de Informação**: Novos desafios para a Segurança e Defesa dos Estados. Academia Militar- Maio de 2008. Disponível em http://pt.scribd.com/doc/54810106/Guerra-de-Informacao-novos-desafios-para-a-Seguranca-e-Defesa-dos-Estados >. Acesso em: 01 fev. 2012.

TOTA, Pedro. "Segunda Guerra Mundial" In:. MAGNOLI, Demétrio (org.). ***História das Guerras*****. São Paulo**: Contexto, p.p. 356-388, 2009.

VERDELHO, Pedro, et al. **Leis do Cibercrime**. Vol.1. Lisboa: Centro Atlântico, 2003. 28p.

VILELA, Carolina Antunes Barata Pires. **Segurança**: Ameaças e Respostas: O ciber-terrorismo. Lisboa, Março de 2010. Disponível em: <http://www.fundacaorespublica.pt/cms/files/conteudos/carolina_vilela.pdf?PHPSESSID=5eed322c1da6c311f9d954f2b20a7300>. Acesso em: 30 mai. 2010.

VISACRO, Alessandro. **O Desafio da Transformação**. MILITARY REVIEW, Março-Abril 2011. Disponível em: <http://usacac.army.mil/CAC2/MilitaryReview/Archives/Portuguese/MilitaryReview_20110430_art010POR.pdf>. Acesso em: 23 abr. 2012.

WAISBERG, Tatiana. **O Papel do Direito Internacional na Guerra entre Israel e o Hamas**: inter armas silent leges? Revista Jus Vigilantibus, 2009. Disponível em: <http://jusvi.com/artigos/37981> Acesso em 25 jul. 2012

WIGHT, Martin. **A Política do Poder**. São Paulo: UNB, 2002.