Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Relações Internacionais

POLÍTICA DE DEFESA NACIONAL E ESTRATÉGIA NACIONAL DE DEFESA:

Percepções da Influência do Espaço Cibernético na Preparação e Conduta da Defesa

Autor: Willian Paulino

Orientador: Prof. Dr. Delmo de Oliveira Arguelhes

Brasília
2013

WILLIAN PAULINO

POLÍTICA DE DEFESA NACIONAL E ESTRATÉGIA NACIONAL DE DEFESA:

Percepções da Influência do Espaço Cibernético na Preparação e Conduta da Defesa

Monografia apresentada como requisito para a conclusão de Bacharelado em Relações Internacionais pela Faculdade de Ciências Jurídicas e Sociasi do Centro Universitário de Brasília – UniCeub .
Orientador: Prof. Dr. Delmo de Oliveira Arguelhes

BRASÍLIA
2013

WILLIAN PAULINO

POLÍTICA DE DEFESA NACIONAL E ESTRATÉGIA NACIONAL DE DEFESA:
Percepções da Influência do Espaço Cibernético na Preparação e Conduta da Defesa

Brasília, de de 2013.

BANCA EXAMINADORA

_____
Professor Dr. Delmo de Oliveira Arguelhes
Orientador

_____
Examinador

_____
Examinador

Dedicatória

Aos meus pais.

Agradecimentos

Agradeço ao orientador, Delmo Arguelhes, antes de mais nada, pela paciência e compreensão e ademais pela orientações que foram decisivas para a elaboração deste trabalho.

Agradeço também, aos colegas do Ministério da Defesa pelas sugestões e opiniões que, por vezes, ampliaram minha forma de compreender o meu próprio trabalho.

E embora seja atrevido tratar assunto que não pertence a nossa profissão, penso que não é incorreto abordar um terreno que outros, com maior presunção, ocuparam com ações.
Nicolau Maquiavel. A Arte da Guerra.

Resumo

Este trabalho teve por objetivo analisar a Política de Defesa Nacional e a Estratégia Nacional de Defesa brasileiras a partir do surgimento de um novo campo de batalha: o setor cibernético. Partindo disto, buscou compreender as expectativas subjacentes a estes documentos respondendo à seguinte pergunta: Como o Ministério da Defesa e as Forças Armadas se preparam para um novo teatro de operações, o espaço cibernético? Realizou um estudo exploratório das principais teorias de segurança internacional e teorias da guerra em si. Abordou ainda, o dilema de segurança formulado por Hobbes a luz da problemática da segurança cibernética, a questão da vigilância do ciberespaço e a problemática gerada por essa prática nos direitos individuais.

Palavras-chave: **s**egurança internacional, defesa nacional, estratégia, espaço cibernético.

Abstract

This study aimed to analyze the Brazilian National Defence Policy and the National Defence Strategy from the emergence of a new battlefield: the cyberspace. It aimed to understand the expectations underlying these documents answering the following question: How the Ministry of Defence and the Armed Forces are preparing for a new theatre of operations, cyber space? It conducted an exploratory study of the main theories of international security and theories of war itself. Also addressed the security dilemma formulated by Hobbes to light the issue of cyber security, the issue of surveillance of cyberspace and the problems generated by this practice in the individual rights.

Key words: international security, national defence, strategy, cyberspace.

Sumário

INTRODUÇÃO

> *Portanto, todas as artes praticadas na sociedade em função do bem de todos, todas as instituições nela estabelecidas mediante o respeito às leis e o temor de Deus seriam vãs se não se preparasse também a sua defesa, a qual, se eficaz, permite que sejam mantidas mesmo quando forem estruturadas com imperfeição.*
>
> A Arte da Guerra. Nicolau Maquiavel

Uma resultante da condição anárquica do sistema internacional é a preparação da defesa nacional. A ausência de regulação sobre os Estados faz com que se atribua aos próprios, enquanto entidades soberanas, que se regulem mutuamente como corresponsáveis pelo atendimento de sua segurança e de seus interesses. Dessa forma, uma consequência da estrutura da política internacional é o vislumbre constante da possibilidade de guerra. Ressalte-se que essa possibilidade não implica numa situação permanente de guerra, mas, sim, numa necessidade permanente de se estar preparado para ela.

A preocupação dos Estados com assuntos de segurança, por sua vez, demanda a criação e atualização das forças armadas, as quais sofrem direta influência do progresso econômico e técnico de uma sociedade. Essas preocupações são essenciais para a sobrevivência e ascensão de um Estado. Concomitantemente, o fator tecnológico pode ser decisivo no provimento da segurança. Contudo, trata-se de um componente apenas dessa atividade de preparação da guerra, sendo esta, um fenômeno eminentemente histórico e político indissociável de seu contexto. Enfim, "a guerra é uma simples continuação da política por outros meios" (Clausewitz, 2010: 27).

Com o avanço tecnológico ao longo dos séculos, os métodos de enfrentamento utilizados na guerra se alteraram, muitas vezes, impulsionados por avanços nas tecnologias que possibilitaram vantagens estratégias sobre os oponentes. Porém, em última instância, os motivos pelos quais se faz guerra, os objetivos da guerra e suas consequências podem ter variado em grau ou intensidade, mas sua natureza não mudou. Os objetivos fundamentais da guerra continuam sendo as mesmas de sempre, tendo sido muito bem apontadas por Clausewitz: "A guerra é, pois, um ato de violência destinado a forçar o adversário a submeter-se à nossa vontade" (Clausewitz, 2010: 7).

Partindo disso, serão apresentadas duas perspectivas propostas para a análise dessa questão, as chamadas revoluções nos assuntos militares (RAMs) e as guerras de quarta

geração (G4Gs) e, rever a perspectiva tradicional da teoria da guerra, desenvolvida por Carl von Clausewitz, a luz do debate moderno.

Neste contexto, será feito um estudo exploratório das consequências do surgimento de novas tecnologias e novas ameaças, especificamente no que se refere ao ciberespaço, nas dinâmicas de segurança internacional e, logicamente, as consequências para a política e estratégia de defesa nacionais enquanto instrumentos de políticas externa também.

Não é possível atingir o objetivo supracitado sem abordar, mesmo que superficialmente, o dilema da segurança *versus* vigilância. Este aspecto tem sua relevância aplicada na medida em que o espaço cibernético passa a exercer papel mais importante na vida dos cidadãos ao passo que se torna mais importante para o comando e controle de infraestruturas críticas e outras variáveis de grande importância para a segurança nacional.

Mais adiante, analisar-se-á como a política nacional de defesa prepara o Brasil para o uso dessas novas tecnologias para enfrentar essas novas ameaças e como o surgimento desse novo campo de batalha afeta a preparação e a condução da defesa nacional.

CAPÍTULO I

1.1 Segurança e Defesa – Conceitualizações Iniciais

Em função de seu caráter abrangente, os conceitos de segurança e defesa possuem inúmeros significados possíveis, fazendo-se necessária a especificação do sentido que se pretende dar a estes.

Em uma aproximação inicial, é preciso definir a que ou a quem se refere a segurança. Vale ressaltar que este conceito é altamente contestado, havendo diversas correntes de estudo sobre os diversos níveis de segurança. Contudo, pertinente ao presente trabalho, cabe definir apenas algumas dimensões fundamentais à determinação do objeto da segurança.

De acordo com Duroselle (2000: 135) constata-se uma mudança nas relações internacionais a partir do momento em que se descobre que o Estado deve afinar-se com um grande grupo de homens que formem uma comunidade e aceitem viver em conjunto.

A partir disso é que surge, no conjunto de Estados, o interesse nacional: a segurança. Segundo o autor, ela existe em dois graus:

> A segurança relativa consiste, por meio do poder, em alianças ou em qualquer outro tipo de ação que seja capaz de assegurar sua independência e sua integridade territorial, mesmo pagando o preço de uma guerra defensiva. A segurança absoluta, muito mais rara, consiste em se sentir a salvo não apenas da amputação territorial ou da perda da independência, como também a salvo de uma guerra indesejada.
>
> (Duroselle, 2000: 135-136)

Apesar de ainda não ser o conceito que se deseja adotar aqui, a proposta de Duroselle representa algo a ser considerado ao deixar em evidência o dilema de *paz* ou *liberdade* que se mostrou presente desde o início do Estado-nação moderno. Na medida em que era interesse dos homens de uma deterimanda comunidade manter sua independência mesmo que o custo disso fosse uma guerra. Por outro lado, observa-se o entendimento da segurança como uma ausência de preocupação com uma perda de território ou a perda da independência.

Quem aprofundou este conceito foi Barry Buzan que elencou, em princípio, quatro níveis onde o conceito de segurança pode ser aplicado: o internacional, o regional, o estatal e o individual (Buzan, 1991: 15).

Interessa a este trabalho a questão de segurança do indivíduo somente no que se refere ao relacionamento entre agente (indivíduo vinculado a valores, normas, regras e códigos de conduta da sociedade em que está inserido) e estrutura. Nesse sentido, a segurança deste indivíduo pode ser entendida como a ausência de ameaça a sua existência. Logo, trata-se de uma relação entre os indivíduos presentes no limite fronteiriço do Estado, da relação entre eles para com o Estado e, por outro lado, de como o Estado também pode ameaçar a segurança destes indivíduos.

O Estado, por sua vez, detem os meios legítimos de coerção sobre todos aqueles inseridos em sua delimitação fronteiriça. Depreende-se daqui uma relação de mútua dependêcia entre Estado e indivíduo. Explorando ainda mais essa lógica, cada um pode representar uma ameaça ao outro: o Estado pode ameaçar o indivíduo, em regimes autoritários, enquanto o indivíduo pode ameaçar o Estado enquanto faz parte de redes terroristas ou ao espionar em serviço de outros Estados, por exemplo (Alsina Jr., 2006: 24).

Essa relação reflexiva entre segurança individual e estatal, de acordo com Alsina Jr., determina, em linhas gerais, duas vertentes de estudo de segurança: a dos tradicionalistas (*Traditional Security Studies* – TSS) e a dos críticos (*Critical Security Studies* – CSS). Os tradicionalistas apresentam-se mais afinados com os postulados clássicos da vertente realista da teoria das Relações Internacionais, pois defendem o papel primordial do Estado-nação como provedor da segurança em seus níveis interno e externo. No caso da segurança externa, enfatiza-se a dimensão militar da segurança e a idéia de outro Estado soberano representar a ameaça externa. É importante ressaltar que os tradicionais assumem como pressuposto um sistema internacional anárquico, aos moldes do proposto por Hedley Bull no seu livro *A Sociedade Anárquica*, em 1977. A ausência de hierarquia entre os Estados nacionais territorialmente organizados é o que faz deste Estado o tutor, em última instância, da segurança de seu povo. Obviamente essa colocação de Hedley Bull é inspirada nos escritos de Hobbes que defendia a necessidade do Estado (o Leviatã) como um mal necessário para garantir a ordem e a segurança, fazendo com que se saísse do estado de natureza, onde os homens se matavam uns aos outros.

Hobbes defendia que, no estado de natureza, os homens poderiam todas as coisas e, consequentemente, todos os meios para atingir seus objetivos seriam válidos. O fato de o homem ser mal por natureza, de acordo com esse autor, resultaria num poder de violência ilimitado dos homens para com os próprios homens.

A partir disso, os homens recorreriam à violência sempre que quisessem um determinado bem. Por consequência, a manutenção desse bem implicaria na violência, esta

usada para garantir a segurança desse mesmo bem. Ressalte-se então que, de acordo com Hobbes (2002), o homem, no estado de natureza, estaria fadado a uma lógica do uso da força (violência) para manutenção de sua segurança e, naturalmente, o mais forte subjugaria o mais fraco até que surgisse outro ainda mais forte.

A mudança que possibilitaria a alteração do *status quo* desse estado de natureza seria o surgimento do Leviatã, ou, traduzindo a metáfora de Hobbes, o Estado. Os homens cederiam parcialmente sua liberdade em troca de segurança que seria provida pelo Estado por meio da vigilância e do controle de todos aqueles que se submetesse ao que ficou conhecido como o contrato social.

Transpor essa lógica para as relações internacionais não é algo tão difícil. O próprio Hobbes estabeleceu essa relação mesmo sem ter observados as dinâmicas de interação do Estado moderno: "Pois as Repúblicas, consideradas entre si mesmas, estão em estado de natureza, isto é, de hostilidade recíproca" (Hobbes, 2002: 7).

A lógica hobbesiana foi absorvida, principalmente, pelos tradicionalistas que adotam o estado de natureza para salientar a existência de um antagonismo entre os Estados (Bull, 2002: 81).

Os críticos, por sua vez, apontam a limitação dos tradicionalistas, por verem o Estado como entidade átoma e, por esse motivo, não sendo capaz de explicar, de maneira satisfatória, as diferentes facetas atinentes às questões de segurança. Em geral, os críticos acreditam que a proeminência dada ao Estado enquanto tutor da segurança é o grande limitador intelectual da proposta tradicional. Eles defendem um deslocamento do foco de estudo para a, por eles denominada, segurança humana em função de outras dimensões da segurança (econômica, política, ecológica etc.), não podendo ser dispostas sob a tutela do Estado. Os CSS afirmam que a visão tradicional desses assuntos acaba por criar um determinismo retroativo e, nesse sentido, os críticos procuram "questionar o *status quo*, afirmando que a visão tradicional da segurança acaba por reificar a realidade" (Alsina Jr. 2006:25).

O problema fundamental em relação à perspectiva crítica é a pretensão de englobar praticamente tudo como questão de segurança, pois, virtualmente, qualquer coisa pode representar ameaça à segurança do indivíduo. Levando isso em consideração, apesar de limitante, o ponto de vista tradicional mostra maior pertinência ao objeto de estudo deste trabalho.

Certamente, o Estado não é o unico elemento de qualquer estudo sobre segurança internacional, pois, obviamente, existem diversas fontes de insegurança que provêm de fora do escopo estatal, como é o caso do terrorismo, por exemplo. Entretanto, o Estado continua

sendo o principal elemento de qualquer estudo de segurança internacional. Assim, ao se tratar da questão de segurança, a sombra do Estado aparece de maneira onipresente. (Arguelhes e Ávila, 2011: 21-22).

Feitas estas considerações em relação ao debate em volta do conceito de segurança, passa-se à definição de defesa que, em certa medida, decorre da idéia de segurança, tendo, porém, caráter mais restrito. De acordo com Buzan, defesa, *stricto senso*, se refere à segurança militar externa. "Na prática, a agenda de segurança militar gira grandemente em torno da habilidade dos governos se manterem contra ameaças internas e externas, mas ela pode envolver também o uso de poder militar para defender Estados ou governos contra ameaças não-militares à sua existência como migrações e ideologias rivais" (Buzan *et al* 1998: 201). Contudo, se levarmos em consideração que o poder militar, personificado pelas Forças Armadas, responsáveis pela defesa do Estado, frequentemente possuem atribuições, ainda que subsidiárias, de provimento de segurança pública, estas são conceitualmente distintas das atribuições de defesa que se referem, no conceito aqui adotado, exclusivamente à *segurança militar externa*.

1.2 Da Segurança e da Defesa Internacional – Condicionantes Sistêmicos.

Será explorada aqui, em linhas gerais, a forma como a globalização - exaustivamente tratada em diversos outros trabalhos - afeta as questões que envolvem o objeto de estudo deste trabalho.

Terminada a Guerra Fria, inicia se um processo de reestruturação do sistema internacional. As questões de segurança passam então por importantes transformações, contudo, a posição de cada Estado na hierarquia de poder mundial continua sendo de grande relevância para sua política de defesa. Deve-se prestar especial atenção aos regimes internacionais de não proliferação, quase sempre fortemente incentivadas pelas principais potências do sistema.

Visando encurtar esta discussão, adotar-se-á uma definição conceitual de globalização uma tanto mais genérica proposta por David Held, que define globalização como a ampliação, aprofundamento e aceleração da interconexão, em escala mundial de todos os aspectos da vida social.

Segundo Held, a presente realidade global implicaria modificações nos padrões de interação e de construção da ordem, o que impossibilitaria pensar as relações de poder a partir de uma visão de poder estatal tradicional e, dessa forma, soberana. Embora não se pense que

o Estado está em vias de desaparecer, ele passa a ser obrigado a interagir com um grupo de atores não-estatais que freqüentemente assumem papel de grande relevância em seu cálculo estratégico (Held, 1995: 116).

Se, antes, os conflitos precisavam ser necessariamente posicionados em um dos dois lados do mundo bipolar, com o fim dessa ordem passaria-se, então, a uma regionalização dos conflitos. Talvez seja possível afirmar que a balança de poder atuaria agora em pequenas escalas regionais, o que ampliaria a possibilidade de desequilíbrios, também em menor escala.

Cria-se, portanto, uma dinâmica com grau de complexidade mais elevado. Desta forma sobrepõem-se varias camadas de governança que se estabelecem conforme o tipo de problema. Desse ponto de vista, "as questões de segurança e defesa estariam sujeitas a uma nova lógica, em que governos nacionais ver-se-iam compelidos a dar conta de demandas multifacetadas nos planos domestico, regional e global - tendo que lidar, muitas vezes, com ameaças de caráter não estatal" (Alsina Jr., 2006: 39).

Diante do exposto, como se colocaria a questão do poder militar, elemento crucial para o entendimento da defesa, no atual sistema internacional instável por natureza? É crescente a aceitação do axioma segundo o qual potências de primeira grandeza não entrariam em conflito armado ou, pelo menos, que esse acontecimento seria altamente improvável.

Para muitos analistas, a guerra estaria fora do leque de políticas aceitáveis. Em contrapartida, nas periferias do sistema internacional a instabilidade, consequente do processo de globalização, teria efeitos um tanto mais perversos pois os países de terceiro mundo precisariam enfrentar a possibilidade de conflitos externos e internos. Isto colocaria, de um lado, o centro pacífico e a periferia violenta.

Contudo, a interdependência em assuntos de segurança e defesa se coloca como uma realidade objetiva, colocando em xeque a idéia tradicional de Estado soberano e estrategicamente autônomo. O surgimento de novos atores e novas formas de atuação no sistema internacional amplia a complexidade do sistema internacional, talvez contribuindo ainda mais para seu caráter fundamentalmente imprevisível.

1.3 Definições de Guerra

Nesta seção, será apresentado um panorama acerca das três principais perspectivas da guerra hodierna.

As três perspectivas que serão apresentadas compartilham o objetivo de apresentar soluções práticas para a conduta da guerra, e o fazem a partir de ferramentas conceituais diferentes.

Estas perspectivas foram selecionadas em função de sua relevância para o entendimento e a própria elaboração das políticas de defesa do Brasil e de diversos outros Estados. É importante lembrar que os temas são motivos de intensos debates na academia. Essas abordagens oferecem oportunidade de tecer um painel amplo dos debates contemporâneos sobre os estudos estratégicos e políticas de defesa.

1.3.1 Teoria da Guerra de Clausewitz;

> Será que uma guerra é da mesma natureza que uma outra? Será que um objetivo de uma empreitada guerreira se distingue do fim político desta ultima? Qual é a medida das forças que se deve mobilizar em uma guerra? Qual a medida de energia que se deve desdobrar na conduta de uma guerra? De onde vêm as inúmeras pausas nas hostilidades, seriam elas partes importantes desta última, ou verdadeiras anomalias? Será que as guerras dos séculos XVII e XVIII com força moderada, ou as imigrações dos tártaros meio-civilizados, ou as guerras de destruição no século XIX estáo conformes à coisa em si? Ou será que a natureza da guerra está condicionada pela natureza das relações e quais são estas relações e estas condições? Os objetos que aparecem em respeito a estas condições não aparecem em nenhum dos livros escritos sobre a guerra particularmente naqueles que foram escritos recentemente sobre a conduta da guerra em seu conjunto, isto é, a estratégia. (CLAUSEWITZ, *apud* ARON, 1986: 100).

Neste fragmento trazido por Aron observa-se que a proposta de Clausewitz era analisar a guerra de um ponto de vista teórico e, a partir disso, descrever seu funcionamento geral entendendo as questões fundamentais da guerra e suas manifestações através da história tipificando aquilo que era fenômeno intrínseco à guerra e aquilo que era fenômeno político e social que se relacionava diretamente com as questões da guerra.

Clausewitz se ocupou da redação de sua maior obra *Da Guerra* de aproximadamente 1816 até 1830 e, entretanto, é importante ressaltar que o general prussiano considerava sua obra inacabada e que carecia de algumas revisões, contudo, o autor morreu antes de terminar sua revisão.

Nesta obra, sua análise fez uso de uma metodologia diálitica inspirada em Kant, mas que se desenvolve de maneira particular ao longo de *Da Guerra*. Ele analisa a guerra como resultado de duas vontades antagônicas; contrapõe o absoluto (ideal) e o real; as relações entre meios e fins; ataque e defesa e etc. É importante ressaltar que não se tratava de uma dialética aos moldes proposto por Hegel, pois não busca uma síntese através do conflito de contrários, mas busca o conhecimento discutindo pares de conceitos contrapostos para então colocar em destaque as principais características dos fatores contrastantes. (ARON, 1986: 108).

A partir destes pressupostos Clausewitz demontra que a guerra não é um fenomeno isolado, campacto e maciço, mas um fenômeno dinâmico que tem suas partes constitutivas influenciando-se mutuamente em interações recíprocas.

1.3.1.1 Definição Básica de Guerra

Carl von Clausewitz inicia o livro *Da Guerra* com um esforço de definir o que é a guerra. O autor faz isso dividindo o tema em pequenas partes que pretendem discriminar e definir os elementos da guerra para então buscar entender seu funcionamento em conjunto, num processo que parte do mais simples para o complexo, ou seja, o estudo da guerra se inicia a partir de sua forma mais simples, o duelo e, a partir dele, aumenta gradualmente sua escala de complexidade.

O duelo, essencialmente, consiste em tentar submeter o adversário à sua vontade fazendo uso de sua força física. Para tal, o objetivo imediato da guerra é abater o adversário a fim de torna-lo incapaz de resistir, obrigando-o a ceder aos seus interesses. "A guerra é, pois um ato de violência destinado a forçar o adversário a submeter-se à nossa vontade" (Clausewitz, 2010: 21).

Trata-se, então, de uma força fazendo frente a outra força e para tal faz uso da violência. Essa violência faz uso de ferramentas provindas das artes e das ciências. Evidencia-se aqui o caráter dual da guerra que não se define com uma ciência nem como uma arte, mas faz uso instrumental de ambos na busca por finalizar o adversário “ou colocá-lo em tais condições que ele se sinta ameaçado por essa probabilidade." (Clausewitz, 2010: 10)
"Forca, para contrapor a força oponente, veste-se das invenções da arte e da ciência" (Clausewitz, 2010: 75).

A escalada do duelo até o seu ponto mais alto culminaria no que Clausewitz chamou de guerra total onde o irrestrito poder militar de um Estado, visando destruir a resistência inimiga, mobilizaria toda a sua estrutura em função do esforço se guerra.

Clausewitz defende o caráter de menor importância para a guerra em si exercida pelas leis do "direito dos povos". Segundo ele, trata-se de uma restrição ínfima que se impõe a violência da guerra que não diminuem em nada a violência da guerra.

> "As almas filantrópicas poderiam então facilmente julgar que existe maneira artificial de desarmar e derrotar o adversário sem ver demasiado sangue, e que é para isso que tende a verdadeira arte da guerra. Por mais desejável que isso pareça, é um erro que é preciso eliminar. Num assunto tão perigoso como é a guerra, os erros devido à bondade da alma são precisamente a pior das coisas."
>
> (Clausewitz, 2010: 8)

Sobre o uso da violência na guerra, vale levar em consideração as colocações de Duroselle (2000: 148-160) sobre o que ele chamou de *poder*. De acordo com ele, o poder seria o conjunto de meios que um líder (chefe de Estado, General etc.) tem de aplacar a vontade de um adversário. Geralmente, esse poder está associado à capacidade de decidir quando usar a violência.

Sobre este aspecto Duroselle contribuiu bastante ao classificar elementos que devem ser considerados quando se vislumbra o uso da violência. São eles:

a) forças militares imediatamente disponíveis;

b) duração do conflito;

c) atitude do mundo exterior;

d) potencial a longo prazo de cada campo.

a) Quanto às forças militares imediatamente disponíveis, Durosselle ressalta a impossibilidade de se realizarem medidas rigorosas em relação a esse tema haja vista que esta questão está subordinada, em grande medida, ao "moral" das tropas.

b) A duração do conflito dependerá de três aspectos:

- A clareza do choque: Numa guerra tradicional, os elementos são claros. No caso de uma guerra de subversão, o autor defende que não pode ser longa;

- A possibilidade de renovação dos armamentos destruídos no choque inicial

- o tempo que levará o mundo exterior para intervir;

c) Atitude do mundo exterior: este aspecto se refere a segurança de que outros atores não intervirão. Durosselle ressalta que quanto maior a duração do conflito é bastante relevante no sentido de que a tendência a intervenção exterior aumenta proporcionalmente à duração do conflito.

d) O potencial: Se refere a probabilidade de ganhar e manter a vitória no local.

Duroselle (2000: 148-160)

Voltando ao Clausewitz, a lógica da política preside a guerra, mas a forma pela qual essa lógica pode ser expressa é a gramática dos meios. Em outras palavras, é importante reconhecer a guerra como continuação da política só que por outros meios. Por este exato motivo, a guerra está sujeita às condições sociais, desta forma, não se pode considerar a guerra um ato isolado: A guerra está inserida num contexto histórico, ou seja, na própria historicidade da política. "A política, além do mais, é o útero no qual a guerra se desenvolve..." (Clausewitz, 1984: 149).

É importante ressaltar que a guerra não é apenas um ato político, mas um instrumento da política enquanto meio de atingir determinados objetivos. Clausewitz chama a atenção para o fato de que enquanto meio, não pode se considerar a guerra isoladamente de seu fim e aconselha aos tomadores de decisões que se atentem para as mudanças na vontade política e suas possíveis consequencias na conduta da guerra.

Isso implica dizer que essa relação de subordinação entre política e guerra apresenta restrições e tendencias que serão seguidas no ato da condução da guerra. Desta forma, o leque de ações táticas e estratégicas utilizáveis é resultado da influência da sociedade política de um dado momento.

A definição de guerra é, então, contextual na medida em que precisa abrir espaço para o momento histórico em que está inserida. Este aspecto torna fundamental a flexibilidade anlítica, ao mesmo tempo em que deve demonstrar a direção para onde se deve avançar no "plano de guerra".

Para Clausewitz a guerra se divide em estratégia e tática. A estratégia visa alocar recursos de forma a alcançar a vitória, ou ainda, a paz. Por outro lado, a tática se preocupa em ter forças armadas treinadas e prontas para executar as manobras de combate.

Subjacente a essa separação conceitual entre tática e estratégia observa-se uma hierarquização dos níveis de planejamento da conduta da guerra. Enquanto a política define os objetivos de guerra, a estratégia define como alcançá-los (para que se tenha paz) e a tática observa a execução do que foi proposto pela estratégia. Apesar de parecer um detalhe sem importância, essa estrutura de pensamento está nas bases do pensamento estratégico brasileiro e de muitos outros países.

Um dos pontos centrais da teoria da guerra proposta por Clausewitz é aquilo que ficou conhecido como a "Trindade":

> A guerra, então, não é apenas um verdadeiro camaleão, que modifica um pouco a sua natureza em cada caso concreto, mas é também, como fenômeno de conjuntos e relativamente às tendências que nela predominam, uma supreendente trindade em que se encontra, antes de mais nada, a violência original do seu elemento, o ódio e a animosidade, que é preciso considerar como um cego impulso natural, depois, o jogo das probabilidades e do acaso, que fazem dela uma livre atividade da alma, e, finalmente, a sua natureza subordinada de instrumento da política por via da qual ela pertence à razão pura.
>
> (Clausewitz, 2010: 30)

Dois aspectos em relação a essa citação devem ser explicitados. A primeira é a analogia da guerra ao camaleão. Refere-se ao fato de que a guerra se altera apenas superficialmente, se adapta ao contexto histórico em que está inserida, mas mantém suas características mais profundas inalteradas.

Este aspecto é relevante para o que o trabalho de Clausewitz pretende ser, uma teria da guerra. Esta ressalva implica dizer que, em função de motivos conjunturais ou de contexto histórico, a guerra poderá assumir diversas formas mas sua natureza não se altera.

Em segundo lugar, a trindade em si. São elementos da trindade: a violência primordial ou a simples vontade de eliminar o inimigo; o jogo das probabilidades que supõe a imprevisibilidade inerente à guerra; e, por fim, a natureza subordinada de instrumento da política, ou seja, a instrumentalidade da guerra, trata-se de um meio para atingir um fim.

Seguindo adiante no texto, Clausewitz ilustra os três vértices da trindade de uma forma interessante. Atribui ao povo o aspecto da violência, ao Comandante e seu Exército a criatividade para lidar com a incerteza do combate e, finalmente, ao governo o aspecto de subordinação, pois a guerra está subordinada à vontade política expressa pelo Estado.

A trindade proposta por Clausewitz é o elemento de continuidade na guerra. A combinação de forças irracionais (violência), não racionais (probabilidade e acaso) e racionais (subordinação à vontade política) é o que permite identificar e analisar a guerra.

Ora, mas partindo disso, a guerra só poderia ser travada entre Estados? Com o fim da Segunda Grande Guerra, críticos da proposta de Clausewitz passaram a defender que com o aumento da importância do elemento não estatal na política internacional, a teoria clausewitziana teria fica obsoleta (Creveld, 1995).

Uma análise um pouco mais detalhada desse ponto de vista constata que ele não se sustenta por deixar de considerar um ponto essencial. A guerra consiste, antes de qualquer coisa, da violência, do acaso e da racionalidade. A conexão desses como a população, forças armadas (Comandante e seu exército) e governo, são secundários.

Qualquer seja a forma de organização (Estado, organização terrorista, líder tribal) para a execução da guerra, os três elementos da trindade primária estarão presentes.

O conjunto teórico elaborado por Clausewitz forma uma importante plataforma para a compreensão teórica da guerra e de sua conduta. Plataforma essa que tem influências profundamente arraigadas no pensamento brasileiro sobre as questões atinentes a guerra e que certamente são consideradas ao se preparar a conduta da defesa nacional.

1.3.2 Revolução nos Assuntos Militares (RAM)

A revolução nos assuntos militares tem dois estágios fundamentais de evolução histórica. O primeiro momento seria durante a Guerra fria. Momento em que ficou explícita a inadequação das estruturas das forças armadas e das doutrinas tradicionais ao então novo cenário de conflitos que precisava levar em consideração um inimigo com capacidade nuclear, ao longo dos anos 1940. Fazia-se necessário, então, desenvolver uma doutrina que empregasse melhor o uso ótimo dos próprios armamentos nucleares.

O aspecto revolucionário tem relação direta com os idéias marxistas-leninistas que enxergavam revolução como uma forma de progresso. No caso, o desenvolvimento tecnológico funcionaria como indutor da revolução pois traria vantagens táticas e estratégicas frente aos adversários.

Neste ponto, observa-se forte elemento ideológico no pensamento estratégico. O desafio seria articular o projeto de Forças Armadas com os preceitos ideológicos essencialmente ofensivos, haja vista que Lênin esperou o fim do imperialismo ocidental

através de uma guerra definitiva, de onde a milícia proletária sairia vencedora (Baumann, 1997:42-43).

Contudo, no estabelecimento do Estado Soviético e criação do Exército Vermelho constatou-se que seria necessário o resgate de práticas e mesmo de pessoal especializado do Exército Imperial. Aí se observa uma contradição interessante. Enquanto o exercito imperial adotava uma postura essencialmente defensiva, o Exército Vermelho deveria adotar uma postura ofensiva, coerente com a ideologia vigente naquele momento. Com a ascensão de Stalin a orientação ideológica se manteve enquanto, por outro lado, as instituições militares soviéticas eram estruturadas de acordo com preceitos doutrinários de Mikhail Frunze, que visionava o sucesso da revolução através de operações ofensivas (Rice, 1986).

Neste contexto, havia necessidade não apenas de produzir resultados operacionais, mas era importante estabelecer elementos normativos que conformariam Estado e exército soviéticos e apresentariam algum tipo de solução às contradições apresentadas. Deve se somar a isso ainda a novidade que representavam os armamentos atômicos que induziriam uma revisão de doutrinas e teorias militares.

Isto posto, pode se observar que, na perspectiva soviética, não se tratava apenas de adequar o treinamento dos combatentes aos postulados ideológicos de expansão da "Revolução Comunista" ou ainda de adaptar-se ao uso de novos armamentos. Nesse contexto, os soviéticos foram os primeiros a propor que evolução tecnológica poderia alterar os metodos de enfrentamento utilizados na guerra, o que tornaria necessário o aperfeiçoamento de organizações, técnicas e procedimentos (Proença Júnior, Diniz e Raza, 1999 *apud* Duarte, 2012).

A partir disso, foi concebida em 1958 uma primeira versão do que viria a ser considerada uma Revolução nos Assuntos Militares. Levava-se em consideração, além da tecnologia nuclear varia outras tecnologias que haviam avançado recentemente como, por exemplo, tecnologias de comunicação e de mísseis.

De acordo com Duarte, a primeira definição de RAM observou as seguintes alterações:

A primeira definição de RAM observou as seguintes alterações:

- Expansão do campo de batalha;
- Necessidade de condução de operações com maior profundidade e audácia, incluindo a necessidade de rápida penetração e destruição dos escalões de retaguarda do inimigo e suas instalações de comando e controle; e
- Elevação geral do tempo de operações.

Por sua vez, essas alterações demandavam uma série de adaptações doutrinárias e organizacionais, entre elas:

- Necessidade de ataques nucleares maciços em lugar da concentração maciça de forças convencionais;

- Necessidade de ataques profundos no território inimigo na abertura das trocas de uma guerra para, assim, dissuadir o uso de ataques nucleares sobre sua própria população e parque industrial;
- Importância de ações simultâneas por todo o teatro de operações oponente, romepndo, assim, sua coesã; e
- Grande ênfase em equipamento eletrônico, ao que se inclui equipamento de comando e controle, gerenciamento de logística e outros

(Tomes, 2000: 99 *apud* Duarte, 2012: 13).

O segundo momento da RAM deriva da experiência da guerra do Golfo (1990-1991) e acontece essencialmente nos EUA, em função de sua proposta de reforma de suas forças armadas em resposta a duas demandas que justaporiam um dilema de projeto de força. Por um lado, em função do fim da guerra fria as dimensões das forças armadas teriam que ser reduzidas, pois não havia mais um inimigo que justificasse o gigantesco orçamento do Departamento de Defesa norte americano. Por outro lado, era necessária a sustentação de uma estrutura preparada para o ambiente de incerteza e ambigüidade intrínsecos ao próprio sistema internacional.

Desse processo dialético culminou a proposta de reforma de todo o aparato de defesa dos EUA. A vitória no Golfo, que teve uma taxa de perda de menos de uma baixa americana para 3000 soldados adversários, deixou claro que a combinação entre ataques aéreos e ataques por mísseis altamente precisos seriam de primeira importância no cenário de guerras futuras. Ganhou ainda mais relevância a busca pela supremacia de informações, pois o grande desafio agora residiria na identificação precisa de alvos.

O que se observa é que a proposta de RAM entende que a guerra se desenvolveria através de inovações tecnológicas que causariam efeitos revolucionários na forma de emprego das Forças Armadas.

Cohen (1999) defende que evoluiriam três definições concorrentes de RAM. Segundo ele, as três representariam perspectivas diferentes de proposição de revolução militar e de conduta da política de defesa dos EUA.

A primeira corrente surge da definição dada pelo almirante William Owens que visava criar um "sistema de sistemas" que integraria ataques precisos de longa distância, comunicações e sensores das quatro forças norte-americanas.

Entendia-se então que a RAM estava fundada na combinação de inovações tecnológicas, operacionais e institucionais (Duarte, 2012).

O desafio que surge seria o de arquitetar um sistema geral e central que padronizasse protocolos entre as forças armada singulares, em outras palavras, tratava-se de um esforço de integração destas forças que enfrentaria ainda grande resistência corporativa da burocracia militar.

A segunda escola de RAM discorda da solução simples de arquitetura de "sistema dos sistemas" elaborada pelo Almirante Owens. Sua argumentação se baseia no entendimento de que a RAM seria um fenômeno complexo e não linear, além disso, esta revolução ainda não havia se manifestado plenamente, como defendia Owens. Isto posto, a política de defesa deveria promover a experimentação e inovação de maneira ampla, pois, assim como a primeira escola, a segunda entendia a RAM como produto consciente do esforço humano.

Nesta proposta evidencia-se um grande obstáculo. Trata-se da redução do orçamento, enfrentada em função do fim da guerra fria e, além disso, da resistência dos militares a experimentação nos termos desta proposta, pois as questões de segurança e defesa envolvem sempre uma dinâmica de ameaças, perigos e urgências que não permitem que se assumam riscos que não sejam estritamente necessários.

Esta escola chamou a atenção também para uma peculiaridade criada pelas armas nucleares. A guerra passou a necessitar muito mais de um elemento civil. Após o fim da segunda guerra ficou claro que os bombardeios estratégicos precisavam de um conhecimento sobre qual a melhor forma de se devastar a infraestrutura inimiga e devastar sua economia e não se tratava mais apenas de derrotar suas forças armadas (Buzan, 2012: 23-28), leve-se em consideração que a questão nuclear tornou duas coisas absolutamente necessárias: as armas convencionais e a limitação dos teatros de operação.

Em função disso, a escola em questão levantava a preocupação de as tecnologias, por estarem no setor civil, não caíssem em mãos de Estados inimigos. Assim, fazia-se necessário uma articulação entre as forças armadas e as corporações civis (Duarte, 2012: 19).

A terceira escola da RAM seria formada por veteranos da guerra do golfo e, em grande medida, por veteranos da guerra fria que defendiam que a a revolução já havia ocorrido na década de 80 e se passou, principalmente, no departamento de pessoal com as novas políticas de recrutamento e os novos centros de treinamento. Esta escola explicava o sucesso no Golfo a partir do emprego de forças voluntárias, profissionais e, consequentemente, altamente treinadas.

Das três escolas, esta era a mais pragmática e se preocupava principalmente com a manutenção da doutrina e sistema organizacional atual. Uma de suas grandes contribuições foi ter se antecipado na percepção de que terrorismo e insurgência poderiam evadir-se à capacidade de combate convencional (Duarte, 2012: 20).

A propostas destas três escolas tiveram oportunidade de serem testadas em campo nas guerras do Afeganistão e do Iraque onde os resultados abriram espaço para o debate sobre a quarta geração da guerra.

1.3.3 Gerações da Guerra

A proposta de Guerra de Quarta Geração (G4G) está intimamente ligada com as propostas de RAM. No entanto, esta ganhou maior visibilidade após os atentados de 11 de setembro, alguns autores defendem até que este atentado foi o marco inicial para a quarta geração da guerra.

De maneira similar a RAM, a G4G propõe uma vinculação causal histórica e futurista de mudança na guerra assim como sugere estar superada a teoria da guerra de Clausewitz, pois não se aplicaria mais a realidade hodierna.

De acordo com a proposta de G4G a guerra não seria mais trinitária, ou seja, diferia dos termos conceituais postos por Clausewitz. Desta forma, a guerra passaria a ocorrer fora do arcabouço do Estado-nacional. A partir disso, os autores supõem que se deva mudar toda a forma de se pensar a guerra e consequentemente mudar a forma como se prepara para ela.

Trata-se, em linhas gerais, de uma reorientação nas expectativas futuras de guerra, onde são incorporados outros elementos, principalmente os de abordagem culturalista que implicaria na concepção de um novo tipo de guerra.

Duas publicações lançaram as bases do pensamento sobre as gerações da guerra. A primeira escrita em 1989, pelo estadunidense William Lind em coautoria com os oficiais Keith Nightengale, John F. Schmitt, Joseph W. Sutton e Gary I. Wilson intitulada *The changing face of war: into the fourth generations* e a outra escrita em 1994 por Thommas Hammes intitulada *The evolution of war: the fourth generation.*

De acordo com esta teoria, a guerra moderna teria evoluído a partir de três gerações passadas e estaríamos vivendo a quarta geração da guerra. A primeira geração se refere as guerras napoleônicas e reflete as táticas da era dos mosquetes e das formações concentradas em linhas e colunas. À época essa formação era necessária em função das tropas sem formadas por conscritos não profissionais e então com pouco treinamento. Este tipo de enfrentamento veio a se tornar obsoleto com a invenção do rifle, embora alguns de seus elementos táticos ainda estejam presentes hoje (Lind *et al*,1989: 23).

A segunda geração se refere as guerras de unificação alemã. Suas táticas surgem em conformidade com as novas possibilidades de enfrentamento apresentadas pelos rifles e ainda pelas metralhadoras, obuses e arames farpados. É importante ressaltar que as mudanças dessa geração foram causadas unicamente pela mudança no fator tecnológico.

A terceira geração surgiria com a primeira guerra mundial e seria causada pela mudança de doutrina e organização militar. Seu expoente maior seria a maturação da *blitzkrieg* alemã. Nesta geração, a mudança viria a ser causada principalmente por novas idéias praticas de manobras.

Estaríamos vivendo atualmente a quarta geração da guerra. Muitos atores vislumbram seu marco inicial com o ataque as Torres gêmeas em 11 de setembro de 2001 (Hammes, 2006).

Esta proposta concebe a guerra passando por mudanças profundas, para as quais o ocidente deveria ainda se adaptar. Essas mudanças paradigmáticas tornariam necessário o desenvolvimento de novas formas de combate. Isso se daria em função de uma nova gama de tecnologias militares onde uma pequena rede de indivíduos munidos de "tecnologia" seriam capazes de atingir infraestruturas críticas, causando um dano desproporcional. Segundo Duarte as novidades seriam:

> *i)* incremento na atuação de pequenos grupos altamente dispersos e orientados por missões que envolvem toda a sociedade do inimigo; *ii*) a diminuição da dependência da logística concentrada e aumento na capacidade de explorar os recursos do inimigo; *iii)* a maior ênfase em operações de manobra, em decorrência do aumento ainda maior do poder de fogo; *iv*) a meta de colapsar o inimigo internamente, mas não destruí-lo fisicamente, recorrendo-se cada vez às operações psicológicas e ao uso da rede global de mídia e comunicações.
>
> (Duarte, 2012: 23).

A atual geração da guerra, além de incorporar elementos das outras gerações dá relevância substancial aos elementos psicológicos e morais. Muitos dos elementos desta geração da guerra sofrem influencia direta da guerra de guerrilha concebida por Mao Tsé-Tung, pois este estilo de guerra seria mais capaz de incorporar as novidades tecnológicas do século XXI.

A guerrilha utiliza meios de destruição em massa não nucleares de forma mais eficaz. Além disso, a evolução da biotecnologia, nanotecnologia, dos meios de comunicação, do ciberespaço poderia criariam um ambiente onde pequenas redes de indivíduos teriam força desproporcional, capaz de desestabilizar países inteiros (Hammes, 2007).

Martin Creveld, um dos teóricos das gerações da guerra, argumenta que o atual estágio dos armamentos nucleares e dos armamentos de destruição à distancia impossibilitaria a existência de guerras convencionais de grande porte, favorecendo a insurgência das guerrilhas modernas e da absorção desses moldes táticos pelas forças armadas convencionais (Creveld, 1995).

Um problema observado aqui é que se propõe uma readequação do presente em função de uma expectativa de futuro. Trata-se de um problema teleológico onde poderia-se estar proferindo uma profecia autorrealizável, pois se determinam as condições presentes em função de causas futuras de um evento (Arguelhes e Ávila, 2011: 24).

Outro problema é que os propositores da G4G tendem a supervalorizar as mudanças causadas pelas novas tecnologias de guerra. Confundem-se variações sensíveis com variações fundamentais na natureza da guerra. Certamente, a proximidade dos eventos dificulta inferir se estas mudanças são apenas contextuais ou se são de fato estruturais da realidade histórica.

1.4 Meios da Guerra e a Tecnologia

No tópico sobre a Guerra de Quarta Geração deixou-se sem resposta a seguinte questão: Será que uma mudança tecnológica ou de tipos de manobras seriam suficiente para alterar aspectos fundamentais da guerra?

Aqui, pretende-se explorar melhor a questão, a partir de uma perspectiva clausewitziana. Levando-se em consideração a historicidade da política e, consequentemente, da guerra, quando Clausewitz desenvolve seu raciocínio sobre os meios da guerra observa-se que a questão das tecnologias empregadas na guerra se enquadra nesse conceito e estão, assim como a guerra e a política, subordinadas ao contexto histórico no qual estão inseridas. Assim, rejeita-se a hipótese proposta pelos teóricos da G4G de que as mudanças tecnológicas teriam avançado a ponto de tornarem obsoleta a teoria da guerra de Clausewitz.

Ora, mas se a tecnlogia empregada na guerra tem sua relevância pautada pela sua capacidade de produzir resultados táticos e estratégicos, o único motivo pelo qual o analista ou o comandante se inclinam a entender o aspecto tencológico da guerra é a própria capacidade desssas tecnologias produzirem resultado na campanha e utilidade de uma determinada guerra para a política.

Partindo disso, é lógico deduzir que o aspecto tecnológico estaria então subordinado à uma estratégia da guerra. Talvez se trate apenas de um problema logístico, como propõem os estudiosos de estratégia brasileiros Proença Junior e Duarte (2005: 645-677).

O ponto de maior relevância aqui é que o processo que conforma, situa e usa uma tecnologia não está conformado no âmbito da teoria da guerra. A tecnologia teria relação mais direta com uma estratégia de guerra, mais específicamente ao aspecto logístico desta estratégia, que definirá como empregar a tecnologia tangível num determinado momento histórico.

CAPÍTULO II

2.1 A Guerra Digital

Cabe, inicialmente, distinguir os objetos analíticos que compõem o cerne dos estudos de segurança internacional, no que tange a segurança cibernética. Em linhas gerais, termos como "ciberespaço", "internet" e "web" vêm sendo utilizados sem a devida precisão conceitual, sendo tratados, muitas vezes, como sinônimos. A confusão semântica dessas palavras prejudica a pesquisa e, por consequencia, a análise.

O termo internet se refere a uma rede estruturada em três camadas principais. A primeira delas é física, composta por elementos que dão suporte às conexões, ao fluxo e ao armazenamento de dados. A segunda camada é composta por informação condificada em padrões técnicos e lógicos que viajam em formato digital. A terceira camada se estabelece a partir do uso e compartilhamento de dados que cria um vasto espaço de interação e formação de redes sociais, econômicas e políticas que se desenvolvem de maneira transnacional (Lucero, 2011: 34-41).

Por outro lado, web não é sinônimo de internet. De fato, a internet não depende da web para existir e continuaria existindo mesmo mesmo que a web deixasse de existir. Trata-se de uma uma aplicação visual, também conhecida como *World Wide Web* (WWW), voltada para a o desenvolvimento de *sites* que dão acesso ao conteúdo por meio de clique sobre *hyperlinks* (palavras, imagens, animações). Essa aplicação foi uma das responsáveis pela popularização pois facilitou o uso da internet para usuários não especializados concentrando nos *sites* várias ferramentas comunicacionais, como blogs, fóruns e chats.

O termo ciberespaço foi cunhado a partir da palavra "*cyberspace"* que traduzida seria "espaço cibernético" de onde se deriva o neologismo ciberespaço. O termo foi cunhado pelo autor de ficção científica William Gibson no livro *Neuromancer* (1991). O livro descreve uma distopia onde um conjunto de tecnologias profundamente arraigadas na sociedade acaba por alterar sua estrutura de funcionamento e princípios dos indivíduos.

A relevância desta obra reside no fato de ter se tornado uma das mais famosas obras de um subgênero da ficção-científica conhecido como *cyberpunk*. Este gênero literário serve de inspiração para vários movimentos ativistas que utilizam a internet para se manifestar como é o conhecido caso do Wikileaks e de seu fundador Julien Assange. No caso específico

de Julien Assange, há uma variação importante. O movimento que ele procura trazer é chamado de *cypherpunk* pois defende o uso de códigos criptografados para preservar a privacidade dos usuários e burlar qualquer tipo de vigilância (Assange *et al*, 2013).

De acordo com Lawrence Lessig (2006, p.9) a internet é o meio físico pelo qual os dados são transportados (texto de correio eletrônico, por exemplo) ou onde páginas são publicadas. O espaço cibernético estaria acima disso. Trataria-se, fundamentalmente, de um meio de comunicação estruturado onde a experiência humana estaria associada através da interação via internet. Silvana Monteiro (2007: 30) o define como "grande máquina abstrata, semiótica e social onde se realizam não somente trocas simbólicas, mas transações econômicas, comerciais, novas práticas comunicacionais, relações sociais, afetivas e sobretudo novos agenciamentos cognitivos". O ciberespaço é apontado também como "um domínio operacional marcado pelo uso da eletroeletrônica e do espectro eletromagnético com a finalidade de criação, armazenamento, modificação e/ou troca de informações através de redes interconectadas interdependentes" (Kuehl, 2009: 29). Nota-se que, apesar da diferença de perspectiva, não há grandes discordâncias entres os autores. Assim, define-se o ciberespaço através de suas caracteristicas físicas e os objetivos para os quais ele é utilizado.

Em 1996, John Perry Barlow, lançou um manifesto intitulado *Declaração de Independência do Ciberespaço*. O manifesto se dirigia aos "governos do mundo industrial" e sugere haver uma separação entre mundo real e o ciberespaço. Neste espaço, leis e autoridades não se aplicariam, nele seria desenvolvido um contrato social próprio, de acordo com as condições daquele "mundo".

É fato que o espaço cibernético vem sendo construído de acordo com o contexto social em que está inserido. Suas mudanças e evolução estabelecerão normas de funcionamento de acordo com valores implícitos, sejam eles de controle ou de liberdade (Sávio *et al*, 2005 *apud* Lucero, 2011: 37).

2.2 O Reconhecimento Internacional do Ciberespaço como Campo de Batalha

Até pouco tempo atrás o uso de computadores como armas ofensivas de guerra não passavam de uma trama encontrada em livros de ficção científica. Hoje se trata de uma realidade global. A internet se tornou alvo de vigilância governamental (Solce, 2008: 296).

Em outubro de 2006, numa reunião de comando das Forças Armadas dos Estados Unidos, o então secretário da força aérea americana, Michael W. Wynne, definiu o ciberespaço como um domínio "caracterizado pelo uso de eletrônicos e de espectro

eletromagnético para armazenar, modificar e intercambiar dados através de sistemas interconectados a associados a infraestruturas físicas". Nesta mesma ocasião foi anunciada a criação de um grupo de trabalho, subordinado à força aérea americana, com a missão de revisar e propor políticas e estratégias de ação (Solce, 2008: 296).

O discurso é uma demonstração clara do reconhecimento do ciberespaço como campo de batalhas, entretanto, observa-se que os EUA entendem esse processo como um modelo de incremento informacional dos sistemas de armamentos e não seria o caso de uma nova força armada especializada em combates informacionais.

De toda forma, é cedo ainda para afirmar qualquer coisa sobre a posição dos Estados Unidos, pois mesmo a força de trabalho criada para a ciberguerra ainda possui um *status* provisório, apesar de seu Diretor, Dr. Lani Kass, ser bastante enfático ao dizer que os EUA são os mais afetados pela ameaça cibernética e que, portanto, a defesa do espaço cibernético se trata de um ramo da guerra que é estratégico, tático e operacional (Lopez, 2006).

Contudo, a preocupação com o uso do espaço cibernético como campo de batalha antecede os acontecimentos supracitados e nos remetem ao início da popularização da internet, na década de 1990.

Em 1990, durante o governo Clinton, a questão da cibersegurança foi reconhecida como uma questão importante para infraestruturas críticas e, por outro lado, era extremamente relevante para a criação de comunidades, grupos organizados que combatiam regimes autoritários (Buzan, 2012: 373).

Em 1998 e 1999, a Rússia propôs que o Primeiro Comitê das Nações Unidas investigasse, entre outras coisas, a necessidade de regular armamentos de guerra de informação (Denning, 2000). Fica clara a preocupação de se reconhecer internacionalmente o espaço cibernético como campo de batalhar para que a partir disso se tornasse possível regulá-lo.

Apesar de carecer ainda de uma regulação internacional, o espaço cibernético já é reconhecido, se não juridicamente, na prática, como campo de batalha por vários Estados. Brasil, China e Coreia do Norte, EUA *et al* incluíram em suas estratégias e doutrinas militares o uso do ciberespaço, além de se ter notícia de terem criado também escolas de formação de pessoal para atuar na área. A China tem considerado rever toda a sua doutrina militar para criar uma quarta força militar especializadas em operações cibernéticas (Solce, 2008).

Por ter se desenvolvido, principalmente, para fins civis, as tecnologias utilizadas no setor cibernético são dominadas exatamente por empresas civis. Este aspecto requer alguma atenção dos militares que precisam trabalhar em parceria com essas empresas mas ao mesmo

tempo, tendo cuidado redobrado, para que esses trabalhos desenvolvidos em parceria não vazem para outros Estados.

Este ponto corrobora a tese de Buzan (2012) de que com o fim da guerra fria, o elemento civil utilizado na guerra passa a ganhar maior importância, pois essas novas tecnologias transcendem a *expertise* tradicional de combate militar, tornando-se um empreendimento muito mais civil do que pregava a literatura militar em tempos de segunda guerra ou guerra fria.

Por se tratarem de tecnologias relativamente baratas e em função do setor civil (geralmente empresas privadas) dominar esse tipo de tecnologia, há ainda a preocupação de que grupos terroristas, como a Al Qaeda, desenvolverem potencial cibernético e o usarem para atacar infraestruturas críticas dos países (Levine, 2006).

2.3 Os Estudos de Segurança Internacional e o Espaço Cibernético Pós 11 De Setembro

Depois dos atentados de 11 de setembro de 2011, a Guerra Global contra o Terrorismo (GGcT) elevou a preocupação com o ciberespaço para um novo e mais complexo nível.

Naquele momento, a utilização da internet por terroristas se tornou alvo de grande preocupação e por isso tornou-se também alvo de vigilância governamental. Segundo estudiosos pós-estruturalistas, críticos da GGcT, especialmente os mais influenciados por Foucault e por Carl Schimitt, (Walker, 2006 e Burke, 2007) essa vigilância que se impunha ao espaço cibernético era preocupante pois, legitimava a transgressão de direitos humanos e civis e acentuava a tensão entre a segurança e a liberdade. Leve-se em consideração que uma das preocupações da GGcT era com a formação de comunidades ligadas em rede, não mais tão afetadas por questões territoriais e, por esse mesmo motivo, se preocupava em vigiar a formação dessas redes (Buzan, 2012: 373).

Jacob Appelbaum resume as justificativas para a vigilância da internet estruturadas em quatro colunas, ou, nas palavras dele: "...Os Quatro Cavaleiros do Apocalipse da Informação: pornografia infantil, terrorismo, lavagem de dinheiro e a guerra contra algumas drogas" (Assange, 2012).

Outro aspecto a ser ressaltado é a questão da territorialidade, que durante a guerra fria era bastante clara e definida, mas que perdeu muito de seu significado quando o inimigo deixou de ser tão claro e coerente. O inimigo, o terrorista, se movimenta em silêncio até o momento em que ataca. Em função disso, tornou-se impraticável definir exatamente quem é o inimigo e, consequentemente, autoridades governamentais passaram a se concentrar em traçar

perfis de prováveis terroristas. Essa prática era constituída de atos proféticos, pois "procura identificar a ameaça futura e, a partir daí, produzir seu próprio sujeito" (Bigo, 2002; Jabri, 2006, *apud* Buzan, 2012).

Enfim, Buzan também aponta a dificuldade de reconciliar os ideais liberais com a necessidade de fornecer segurança e haveria, portanto uma autoridade soberana por um lado e, por outro, a crença numa liberdade individual. Há então uma contradição intrínseca a necessidade de prover segurança, o que fica explícito na necessidade de vigiar determinados grupos suspeitos em contraposição ao direito à privacidade dos indivíduos. Trata-se de um a lógica hobbesiana em seu formato mais elementar: em troca de alguma sensação de segurança é necessário que o povo abra mão de liberdades individuais como direito a privacidade e etc.

Um entendimento possível é que há, em vários aspectos, um conflito entre os conceitos de liberdade e segurança, se fazendo necessária uma busca pelo equilíbrio entre os dois, se é que isso é possível.

Salta aos olhos a questão da redução das liberdades civis em detrimento de um regime de exceção onde, basicamente, todos esses direitos são suspenso temporariamente, mas por tempo indeterminado. Se nos deixarmos levar por essa linha de raciocínio por um momento, não é necessário pensar muito para perceber alguns possíveis efeitos nefastos desse tipo de política.

Cabe lembrar, sobre a questão da vigilância do Estado, a abertura do livro *Teologia Política* (Schimitt, 2006): "Soberano é o que decide sobre a exceção". A exceção, de acordo com Schimitt, seria o momento em se abandona princípios elementaress do Estado Democrático de Direito em função de garantir, por exemplo, a segurança do "povo". Eventualmente a segurança do "povo" significará garantir a segurança da própria instituição, do Estado, em detrimento das liberdades individuais e interesses particulares de cada indivídio partícipe desse povo.

Evoca-se então a tese schimittiana segundo a qual a crise desse Estado Democrático de Direito, onde reside o conceito político de poder soberano, implica, necessariamente, na emergência de um poder total.

Ora, se a ameaça terrorista é amorfa, silenciosa e, muitas vezes, não detectável até o momento em que ataca, cria-se então uma justificativa para que se intensifiquem as ações dos agentes policiais (entenda-se aqui agente policial num sentido mais amplo, como agente do Estado com a função de vigiar e/ou levar à justiça) e se suspenda diversos direitos da população até o momento em que a ameaça seja eliminada. Mas a ameaça é invisível,

virtualmente qualquer pessoa pode ser uma ameaça e por esse mesmo motivo todos devem ser vigiados.

2.4 A Digitalização da Guerra

De fato, uma ciberguerra, nos termos de guerra que se enquadre no Direito Internacional Humanitário, ainda não foi declarada. Contudo, trata-se de uma possibilidade real que, pelo menos em parte, é pública e notória, leve-se em consideração que diversos Estados tem incorporado algum setor em suas forças armadas para se preparar para conflitos que envolvam a guerra cibernética. O caso do vírus Stuxnet que destruiu centrífugas nucleares no Irã e, de acordo com empresas de segurança cibernética como a McAffee e a Symantec, trata-se do mais poderoso vírus de computador já criado (Milevski, 2011).

Naturalmente, Estados com economias mais digitalizadas, como é o caso dos EUA, tem maior preocupação pelo motivo óbvio de que um ataque bem sucedido poderia comprometer seriamente sua economia. A mesma lógica se aplica a infraestruturas que tem seu sistema de comando e controle digitalizados. São as chamadas infraestruturas críticas.

No caso do Brasil, coube ao Gabinete de Segurança Insitucional da Presidência da República estabelecer uma definição para o termo infraestrutura crítica através da Portaria número 2, de 8 de fevereiro de 2008, publicada no DOU número 27 de 11 de fevereiro de 2008: “são consideradas infraestruturas críticas as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico e/ou político". A mesma portaria ainda define áreas que são prioritárias, pontuo: I - Energia; II – Transporte; III - Água; IV – Telecomunicações e V - Finanças.

Note-se que uma coisa que as cinco áreas prioritárias tem em comum é, no mínimo, o sistema de comando e controle, em alguma medida, digitalizado.

Um relatório divulgado pela empresa de segurança cibernética, McAffee, em 2012, avaliou a defesa das infraestruturas críticas de ciberataques nos EUA. O que chama a atenção é que, de acordo com o relatório, "as redes e sistemas de controle estão constantemente sob ataques cibernéticos, frequentemente de adversários de alto nível, como países estrangeiros" (Baker *et al,* 2012: 5). Um agravante que se apresenta aqui retoma a preocupação levantada por Buzan no que se refere a uma maior incorporação do elemento civil em questões de segurança nacional. Grande parte dessas infraestruturas críticas é administrada por empresas privadas, detidas, muitas vezes, por capital estrangeiro, ou seja, o elemento civil, privado e

internacional tem sua importância estratégica ampliada por agora ter se tornado uma questão de segurança nacional sendo alvo de sabotagem e espionagem.

O relatório aponta que além dos ataques que buscam desativar redes e sistemas de controle, é muito comum a tentativa de infiltração em busca de informações sigilosas.

Outro aspecto que vale ressaltar é a importância de atores não-estatais envolvidos. Se torna cada vez mais comum casos de ativismo pela internet, o que vem sendo chamado pela mídia de hackerativismo. É o caso do grupo Annonymous, que em sua versão brasileira fez ataques a sites do governo brasileiro, ou, o mais conhecido, o Wikileaks que vazou uma grande quantidade de documentos confidenciais americanos, alguns deles sobre o Brasil.

Por outro lado, tornou-se evidente em casos como o do Stuxnet que há interesse dos Estados em manter um braço não oficial de atuação. Um dos argumentos que leva a essa dedução é que os meios técnicos e economicos necessários para desenvolver uma ferramenta como o Stuxnet dificilmente seria viável a agentes externos ao Estado.

Pode-se dizer, então, que há alguma articulação entre o Estado e alguns atores não estatais, o que deixa em evidência a coexistência de pelo menos dois grupos de interesse no ciberespaço. Por um lado o Estado tenta cooptar os recursos humanos de elevado conhecimento técnico e por outro, os divérsos e heterogêneos movimentos ativistas na internet, interessados na ampliação das liberdades no ciberespaço e que rejeitam qualquer controle por parte do Estado.

> "Combatentes sem uniforme, sem formação, sem enquadramento, agem por surpresa e não sustentam por muito tempo contra uma tropa regular."
>
> (Aron, 1986: 198-199)

Não fosse a expressão "tropa regular" e a data em que foi escrita, a frase acima poderia muito bem descrever um *hackerativista*.

Ao fazer suas considerações e marcar alguns pontos de divergência sobre a teoria do guerrilheiro de Carl Schimitt, Aron (1986: 197-208) descreve um guerilheiro pela irregularidade, o alto grau de mobilidade, a intensidade do engajamento político e o caráter telúrico. Enquanto descreve o guerrilheiro do século XVIII, muitas de suas características saltaram aos olhos por se aproximarem muito da descrição de um *hacker*, ou de um cibersoldado.

Ora, mas se uma das características esperadas de um ataque cibernético é a sua irregularidade que se manifesta em função da sua carência de recursos ou da sua necessidade de manter em segredo sua identidade, ao mesmo tempo em que a mobilidade é um aspecto

intrínseco a esse tipo de combatente. É importante observar que da mesma forma que vários Estados incorporaram elementos de guerrilha a seus exércitos, vários Estados hodiernos tentam incoroporar *hackers* aos seus sistemas de defesa cibernética.

Quanto ao engajamento político e a forma de atuação em "bandos", observe-se grupos de *hackers* como os Annonymous ou os fundadores do Wikileaks em prol ideologia particular atacam sites de bancos, caso do primeiro e, este ultimo, vazando documentos confidenciais, colocando o governos dos EUA em situação complicada. Ressalte-se que alguns dos vazamentos do Wikileaks vieram de agentes do próprio Estado.

Até mesmo a dificuldade do direito internacional em tratar o assunto não tem grande novidade: "O direito internacional quis dar um estatuto aos irregulares ... ou resistentes." (Aron, 1986: 199).

Talvez não se possa afirmar que o *hackerativista* é a ressignificação do guerrilheiro, entretanto, a relação pareceu interessante o suficiente para que fosse citada.

CAPÍTULO III

3.1 A Defesa como Instrumento de Política Externa

Uma das áreas do conhecimento de menor estudo pela ciência política e pelas relações internacionais são a relação entre o plano interno e o plano externo do Estado. É claro que não se pretende aqui resolver este problema. Determinar em que medida fatores internacionais produzem efeitos sobre as burocracias internas a um determinado Estado e vice-versa, representa, talvez, um dos maiores desafios às áreas do conhecimento supracitadas. Então, devido a complexidade dessa questão, pretende-se aqui, chamar a atenção de se olhar mais atentamente para essa área de penumbra existente entre o funcionamento das instituições domésticas e o sistema internacional.

Ao analisar essa questão, observa-se inicialmente que o âmbito interno e externo se afetam mutuamente. Tratando-se dessas relações mutuamente constitutivas, deveria-se definir as linhas básicas do relacionamento entre política externa e a defesa nacional. Entretanto, esse alvitre é seriamente dificultado por dois aspectos principalmente:

> "o da determinação dos mecanismos que influenciam a articulação entre políticas públicas e a tradução para o plano doméstico dos efeitos sobre essas políticas decorrentes da nem sempre estável estrutura do sistema internacional."
>
> (Alsina Jr., 2006: 53)

Note-se que agravante a isso há o problema de essas relações se influenciarem mutuamente, o que torna a identificação das estruturas que influenciam nesse processo o principal ponto a ser definido para que se aprofunde nessa questão. Assim, a estratégia a se adotar aqui será a de contextualizar a inserção internacional do Brasil nos assuntos de segurança internacional, especificamente no que se refere a defesa cibernética, entretanto, sem deixar de observar as dinâmicas político-insitucionais internas ao país.

3.2 O Brasil e o Papel de suas Forças Armadas

Para que se entenda o contexto e as motivações para a criação dos altos documentos de defesa, a Política de Defesa Nacional e a Estratégia Nacional de Defesa, é necessário antes fazer algumas considerações, mesmo que superficialmente, sobre o papel das forças armadas no Brasil.

Observa-se, no caso brasileiro, um alto desinteresse nos assuntos de defesa por parte da sociedade civil. Alsina Jr. (2006: 49) ensaia que isso se deve, essencialmente, às históricas intervenções das Forças Armadas na política e, ademais, da ausência da securitização de ameaças externas.

Concomitantemente, a questão da seguraça pública ganhou grande dimensão hodiernamente. Este aspecto acabou por configurar elemento de pressão sobre as Forças Armadas brasileiras. Muitos políticos, parte da imprensa e mesmo acadêmicos tem defendido a militarização da segurança pública, em face dos altíssimos níveis de corrupção dentro das polícias e da alta criminalidade.

Em função disso, há algum entedimento, em uma parcela relevante da sociedade, que as ameaças ao Brasil estão no plano interno e não no plano internacional que é para onde as doutrinas militares se voltam.

Vale, ainda, abordar a estrutura institucional brasileira. Devido ao seu sistema político-partidário, há um grande desestímulo para que os detentores de mandatos parlamentares se interessem pelo desenvolvimento de políticas públicas mais complexas e de pouco apelo popular, como é a questão da defesa nacional. Agregue-se a isso o fato de o Brasil não vislumbrar nenhuma ameaça externa imediata à sua segurança nacional. Além disso, há, no Congresso Nacional, poquíssimos recursos humanos com capacidade de analisar esse tipo de política. Logo, geralmente, deputados e senadores, não estão em condições de analisar essas questões com propriedade. Resta então, pedir informações a militares e, com frequencia, a diplomatas mais entendidos de assuntos estratégicos.

É possível, a partir disso, deduzir a dificuldade que é tramitar qualquer questão que envolva a defesa nacional no parlamento brasileiro. A combinação de alta complexidade e desincentivo à classe política de buscar o aprofundamento nessas discussões acabou por renegar as questões de defesa quase que somente aos militares e a alguns diplomatas preocupados com o tema.

3.3 Os Altos Documentos de Defesa e o Ciberespaço

Uma tabela apresentada pelo Tenente Coronel Carneiro, especialista em Defesa Cibernética do Exército Brasileiro, em uma palestra realizada em Belo Horizonte em abril de

2013[1] expõe de maneira bastante clara como funciona o processo decisório, divido em níveis de planejamento, no que se refere à questão cibernética.

Nível de decisão	Designação	Estrutura
Político	Segurança cibernética	Gabinete de Segurança Institucional da Presidência da República
Estratégico	Defesa cibernética	Ministério da Defesa
Operacional	Guerra cibernética	Componentes das Forças Armadas
Tático		

Tabela 1: Processo decisório – espaço cibernético.

Cabe fazer algumas considerações sobre o processo. Ao GSI-PR compete a definição de uma política que se destina e definir quais são os problemas enxergados e sobre os quais os níveis mais baixos devem tomar providências, além de dar orientação básicas sobre como devem operar.

Logo abaixo, no nível de planejamento estratégico, precupa-se em "como fazer". São dadas diretrizes aos órgãos envolvidos sobre ações decorrentes, definindo como alocar recursos com vistas a atender o que foi colocado pela Política, além de serem definidos prazos e metas.

Por fim, o nível Tático/Operacional preocupa-se com a "execução" da Defesa Cibernética. É a quem cabe, de fato, realizar uma possível Guerra Cibernética, os soldados cibernéticos.

Os dois primeiros níves (político e estratégico) serão abordados nas próximas seções. O terceiro nível (tático e operacional) não será aborado devido a ser de cunho altamente específico e, majoritariamente, sigiloso.

[1] CARNEIRO, João Marinônio Enke. Os setores estratégicos da Estratégia Nacional de Defesa: O setor Cibernético. In VI Curso de Extensão em Defesa Nacional, 2013. Disponível em: http://www.defesa.gov.br/projetosweb/cedn/downloads.html. Acessado em 22/06/2013.

3.4 A Política de Defesa Nacional e a Segurança Cibernética

A Política de Defesa Nacional é um documento de alto nível do planejamento brasileiro de defesa que teve sua ultima atualização oficial por intermédio do Decreto Número 5.484 de 30 de junho de 2005 da Presidência da República.

Assume-se como pressuposto que uma política de defesa nacional se orientar basicamente a partir de ameaças provenientes do sistema internacional, leve-se em consideração que os vetores clássicos das relações exteriores são a diplomacia e a força militar do Estado-nação moderno (Alsina Jr., 2006: 33).

Proença e Diniz (1998) enumeram quatro elementos constitutivos de uma política de defesa que são descritos, abaixo.

- forças armadas: tem a função de gerar capacidade de combater, o que não implica o envolvimento de fato em um combate, podendo ser usado como instrumento gerador de vantagem numa barganha política;

- estrutura integrada de comando e planejamento militar: refere-se a capacidade de fazer com que as forças singulares tenha capacidade de agir de maneira integrada visando um mesmo objetivo. Este aspecto é, ainda hoje, foco de atenção do Ministério da Defesa, conforme será abordado mais adiante;

- institucionalidade governamental para a defesa: refere-se a teia de relacionamentos formais e informais que permeiam as Forças Armadas e as demais burocracias indiretamente relacionadas com o tema: e

- compatibilidade entre política declaratória e prática concreta: refere-se a coerência entra aquilo que é exposto pelo Estado como seus objetivos e aquilo que é realizado no plano concreto.

A criação deste documento, entretanto, está intimamente relacionada com a criação do próprio Ministério da Defesa e remonta a década de 1990.

O Ministério da Defesa (MD) foi criado durante o governo de Fernando Henrique Cardoso que, ao contrário dos governos anteriores, chega à presidência do Brasil num clima mais favorável, leve-se em considerção o sucesso do plano de estabilização econômica, o que conferiu ao então presidente, capital político e legitimidade para criação de tal órgão.

De toda forma, havia ainda que se enfrentar a resistência dos militares em criar esse órgão e convencê-los de que o Ministério da Defesa representaria grande avanço no sentido de possibilitar uma melhor atuação combinada e maior integração entre as três forças – sobretudo no aspecto logístico – questão comprovadamente muito importante para os

conflitos contemporâneos. Por outro lado, os militares se preocupavam com a redução do quadro de Oficiais-Generais que se seguiria a criação do Ministério da Defesa e também com a perda da influência política das forças, haja vista que os três ministérios das forças armadas passariam a ser representados por um único ministério civil.

Para pensar o Ministério da Defesa, criou-se o Comitê de Assuntos de Defesa que reuniu militares, diplomatas, acadêmicos e técnicos das áreas de orçamento e planejamento. Este comitê se valeu de um documento elaborado pela Secretaria de Assuntos Estratégicos, em 1994, denominado "Bases para uma Política de Defesa" que foi usado como subsídio para a definição genérica de um quadro internacional. A partir disso, se estabeleceu uma lista de prioridades, entre elas: a implantação do Sistema de Comunicações Militares por Satélite; a revitalização do Sistema de Controle do Espaço Aéreo; e a introdução de vetores de modernidade na Força Terrestre. Estimou-se um gasto de 10 bilhões de reais para atender estas iniciativas que só não foi mais bem sucedida em função da resitência das Forças Armadas em detalhar os projetos militares que estavam em andamento (Alsina Jr., 2006: 105).

Foi só em setembro de 1996, com a criação da Comissão de Relações Exteriores e Defesa Nacional (CREDEN) - decreto nº 1985, de 6 de maio de 1996, que se voltou a pensar na criação de uma Política de Defesa.

O embaixador Ronaldo Sardenberg, então Secretário de Assuntos Estratégicos (SAE) exerceu papel central no processo de criação da Política de Defesa Nacional. Documento que foi também muito relevante para a criação do próprio Ministério da Defesa.

O embaixador Sardenberg, que tinha reconhecida experiência no campo dos assuntos estratégicos e, além disso, bom trânsito com o Presidente Fernando Henrique, elaborou um texto, que serviria de base para os trabalhos da CREDEN, intitulado "Apontamentos Tentativos para a Concepção Estratégica e Política de Defesa Nacional. Assim, a Política de Defesa Nacional beneficiou-se bastante de aportes oferecidos pela SAE sendo finalmente criada em 7 de novembro de 1996 (Alsina Jr., 2006: 112-117).

Em 2005, durante o governo Lula, o documento sofreu uma atualização no sentido de rever o conceito de segurança para uma visão de sentido mais cooperativista, conforme adotado pela ONU e OEA[2] (Pereira, 2010)

[2] Até o momento em que este texto é escrito, encontra-se sob avaliação do Congresso Nacional uma nova atualização da Política Nacional de Defesa. Entretanto, por não haver mudança significativa no documento, especialmente no que se refere ao objeto de estudo deste trabalho, não se levou em consideração o novo documento que tem sua minuta disponível em: https://www.defesa.gov.br/index.php/ultimas-noticias/3869-24072012-defesa-politica-estrategia-e-livro-branco-de-defesa-nacional-conheca-os-documentos-enviados-pela-presidenta-da-republica-a-apreciacao-do-congresso-nacional

O documento define quais são as aspirações do país em relação a sua segurança e defesa nacional. É composto, basicamente, de duas partes, uma política que estabelece um marco conceitual, que define a visão a ser adotada dos ambientes internacional e nacional e quais são os objetivos da defesa. A segunda parte consiste de orientações estratégicas a se adotar, ou seja, dá orientações e diretrizes que devem ser adotadas.

Já na introdução deste documento define-se que a preocupação brasileira se volta, preponderantemente, para o campo externo e que se encontra em consonância com a política externa brasileira.

No primeiro item, "O Estado, A Segurança e a Defesa", onde são definidos conceitos adotadas pela Política, o que vale destacar é que a política demonstra adotar um conceito de segurança ampliado e passou a abranger os campos político, militar, econômico, social e ambiental, apesar de defender que a defesa externa permanece como primordial das Forças Armadas e, ainda, no âmbito interestatal. Fica explícita uma visão de sistema internacional mais alinhada à vertente realista da teoria das relações internacionais, ou seja, aos TSS conforme exposto no capítulo 1. Assim, orienta-se para o provimento de uma segurança militar externa.

Já no segundo item "O Ambiente Internacional" a PDN faz menção direta à questão da segurança cibernética que é entendida como uma questão de segurança nacional. Aponta-se a questão dos avanços da tecnologia da informação *et al* como um fator que trouxe maior eficiência aos sistemas militares e em consequencia disso criaram-se vulnerabilidades que podem ser exploradas no sentido de interferir ou, até mesmo, desativar estes sistemas à distância. O reconhecimento dessa possível ameaça já é um passo importante para que ela seja trabalhada e minimizada, na medida do possível.

Fica clara a preocupação com ataques cibernéticos de origem em outros Estados, especialmente, os dotados de meios ofensivos superiores. Essa idéia de defesa de inimigos mais capacitatos perpassa todo o documento sem que se identifique exatamente de onde viria essa ameaça.

É demonstrado no item 6.19 que versa sobre "Orientações Estratégicas" uma preocupação em minimizar efeitos de um possível ataque cibernético aperfeiçoando dispositivos de segurança e adotando procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento. O item 7.1 paragrafo XII retoma este aspecto.

Em vários momentos da PDN é demonstrada uma preocupação com o desenvolvimento tecnológico do país e a redução da dependência tecnológica além da

superação das restrições unilaterais de acesso a tecnologias sensíveis (tópico 4.13 p. 13). No caso específico da segurança cibernética, essa preocupação com o desenvolvimento tecnológico nacional aponda uma quase desconfiança da tecnologia comprada no exterior. Leve-se em consideração que um aparato de defesa cibernética, em geral, teria um código tão complexo que tornaria difícil encontrar uma *backdoor*, ou seja, uma falha de segurança que permitiria a invasão do sistema por algum progrmamador que estivesse ciente dessa falha.

A PDN mostra que a preocupação brasileira com o setor cibernético é no sentido de fundar capacidade de defender as infraestruturas associadas ao espaço cibernético no país. Assim, identifica-se uma fragilidade e orientar as Forças Armadas a trabalhar suas capacidades a partir disso, sobretudo, dando ênfase ao desenvolvimento nacional dessas tecnologias.

Infere-se também que a PDN se preocupa com invasões potenciais com capacidade para desativar os sistemas ligados ao espaço cibernético. Entretanto, não se elabora sobre o possível atacante, se um agente estatal ou um *hacker*, por outro lado, a linha entre esses dois é bastante tênue sendo, quase sempre, impossível diferenciar sua atuação exceto quando há diferença óbvia na quantidade de recursos necessários para realizar um determinado ataque.

Outro aspecto que corrobora essa proposição são os relatos de Jacob Appelbaum (Assange *et al*, 2013: 55-56). Segundo ele, universidades estadunidenses realizam campeonatos de guerra cibernética simulada com observação da Marinha dos EUA na intenção de aprender as técnicas desenvolvidas por *hackers* além de recrutar essas pessoas para trabalhar para o governo. É importante observar aqui a parceria entre o governo, universidades e empresas. Receita que os Estados Unidos tem usado para induzir seu desenvolvimento tecnológico em diversas áreas.

Voltando ao caso brasileiro, fica claro o reconhecimento do espaço cibernético como campo de passível de ataque e que sua defesa merece atenção num nível elevado por se tratar de uma questão de segurança nacional. Por isso a preocupação com o desenvolvimento de tecnologia nacional. Mas como desenvolver essa tecnologia nacional? E talvez mais importante do que isso, como dar um salto tecnológico que nos coloque em nível de igualdade com outros países do mundo que já vem investindo neste setor a muito mais tempo? Acredita-se que a melhor forma de se fazer isso seja por meio do trinômio: Forças Armadas, Empresas e Academia.

Por outro lado, o ciberespaço também é reconhecido como campo de ataque para o qual as forças armadas podem desenvolver material ofensivo que certamente não será obtido através de compras em outros países. Em síntese e respondendo a questão proposta por este

trabalho, observa-se que pouco se fala no desenvolvimento de uma capacidade ofensiva no campo cibernético. A atenção da PDN se volta a intenção de se desenvolver capacidades de defesa cibernética. Saliente-se um apecto presente em todo o documento que é o desenvolvimento de capacidades defensivas e, apesar de não identificar ameaças, o documento parece se preparar para a defesa de um ataque partindo de uma potência maior, ideia que perpassa todas as áreas da PDN que se prepara para um ataque provindo de uma potência (ou uma coalizão de potências) com capacidade ofensiva maior, em outras palavras, a Política de Defesa Nacional orienta as Forças Armadas a se prepararem para impedir um ataque cibernético que afete as infraestruturas críticas brasileiras. Contudo, esse plano se estabelece em dois níveis, um ativo e outro reativo. O primeiro, conforme já abordado, se dedica a impedir um ataque, o segundo nível se prepara para a falha do primeiro que seria, para o caso de algum sistema de comando e controle ser desativado tenha-se um plano de reativação no menor intervalo de tempo possível.

3.3 A Estratégia Nacional de Defesa e a Segurança Cibernética

No ato de seu lançamento, a Estratégia Nacional de Defesa (END) chamou a atenção de analistas, observadores e da mídia (desta mais superficialmente). Houve bastante consenso de que esta representaria algum avanço na área.

A END, documento publicado por meio do Decreto Presidencial número 6.703, de 18 de dezembro de 2008, se propõe a definir como e quais atitudes serão tomadas, em médio e longo prazo, para atender às vontades nacionais definidas pela Política de Defesa Nacional. Nas palavras do diplomata Paulo Roberto de Almeida, a END deve servir como "um guia operacional e um manual de reequipamento de suas Forças Armadas, com vistas à execução dos objetivos básicos nacionais." (Almeida, 2010: 5).

Assim, enquanto a Política de Defesa Nacional define o que se quer da Defesa, a Estratégia Nacional de Defesa lança esforços no sentido de definir como e quando serão alocados os recursos de forma a atingir os objetivos definidos na política. Isto posto, a END está num nível hierarquico imediatamente inferior à PND e, neste sentido, não pode ir contra o que esta última postula.

De acordo com Moreira Franco, atual ministro da SAE, um país tem duas formas de preparar suas defesas:

> Uma é olhar para fora, definir claramente quas são as ameaças e, com isso, estruturar a defesa; a outra é olhar para dentro, visualizar as necessidades e vulnerabilidades internas e externas e desenvolver capacidades dissuasórias que contraponham eventuais riscos à segurança nacional (Franco, 2012).

A END deixa bem claro que se alinha à segunda alternativa, pois, define que a defesa do Brasil se orientará a partir do desenvolvimento de capacidades, não identificando, pelo menos de modo explicito, quais são as ameaças e vulnerabilidades que se apresentam ao Brasil. Diante disso, a nossa grande estratégia se baseia no argumento da própria instabilidade inerente ao sistema internacional e no aumento da importância do país no mundo para orientar sua estratégia nacional de defesa (com grandes poderes vem grandes responsabilidades).

Em toda a leitura do documento se observa a preocupação com o princípio da independência nacional, uma ideologia nacional desenvolvimentista, como fator primordial em matéria de segurança e defesa revelando o forte caráter nacionalista deste documento. Este aspecto não poderia deixar de se manifestar ao tratar da aquisição de equipamentos ou o desenvolvimento de tecnologias. Quanto a estes aspectos também se apregoa uma autonomia absoluta independente do altíssimo custo que isso pode representar.

Levando-se em consideração que "o conceito de ameaça é, por definição, fundacional e operativamente anterior à formulação que objetiva a segurança" (Saint-Pierre, 2011) nota-se um importante aspecto a ser ressaltado é que a elaboração deste documento não se baseia na definição de ameaças mas na construção de capacidades pelo país. Entratanto devido a grande dificuldade de se apontar ameaças à segurança do Brasil num contexto internacional. Ora, mas se é a identificação de uma ameaça o que permite que um país oriente sua defesa, como um país sem ameaças imediatas pode preparar sua defesa? Resta ao Brasil se preparar para as intempéries do sistema internacional baseando o desenvolvimento de seu aparato de defesa no desenvolvimento de suas capacidades.

A END se estrutura a partir de três eixos: reorganização das forças armadas, reestruturação da indústria brasileira de material de defesa e política de composição dos efetivos das Forças Armadas. O grande argumento para justificar essa revisão estrutural das Forças Armadas e da própria burocracia de defesa brasileira é a idéia de uma crescente importância do Brasil no cenário internacional o que exigiria uma maior responsabilidade com questões externas ao país.

O primeiro eixo, o que se refere à reorganização das forças armadas estabelece algumas mudanças no papel do próprio Ministério da Defesa e do alto comando das três forças.

Dessas novas diretrizes dadas às três forças cabe chamar a atenção que três setores de maior necessidade de serem desenvolvidos, a saber: setor cibernético, o espacial e o nuclear ficando sob responsabilidade, respectivamente, do exército, aeronáutica e marinha. Um maior aprofundamento sobre o primeiro setor estratégico será abordado mais adiante.

No momento, é conveniente abordar, mesmo que superficialmente, os outros dois eixos estruturantes da END para que não se perca de vista uma visão do todo da estratégia.

O segundo eixo se refere à reestruturação da indústria brasileira de material de defesa que tem em sua agenda um estímulo à integração regional da indústria de defesa além de visar o desenvolvimento de tecnologias para equipar as Forças Armadas.

O terceiro eixo se refere à política de composição de efetivo das forças. A estratégia reafirma a necessidade de se manter o serviço militar obrigatório e que este deve funcionar como espaço republicano, seja lá o que isso signifique.

Depreende-se que a Estratégia Nacional de Defesa tem como um de seus principais objetivos a modernização das Forças Armadas e fica clara uma vontade de levar o país a um salto tecnológico que coloque o aparato brasileiro de defesa em pé de igualdade com outras potências intermediárias do sistema internacional.

A Estratégia entende que, através desse desenvolvimento tecnológico a ser desenvolvido, o Brasil se veria menos constrangido ou subordinado a imposições de outros países do sistema internacional: "Não é independente quem não tem domínio das tecnologias sensíveis, tanto para a defesa, quanto para o desenvolvimento" (END, p.9).

A END procura deixar bem claro também que sua orientação, essencialmente pacífica, gira em torno do desenvolvimento de uma capacidade dissuasória. Ou seja, desenvolver e equipar as Forças Armadas brasileiras na medida em que sua capacidade defensiva torne altamente custosa uma intervenção direta no território Brasileiro. Isto posto, a intenção da reforma no aparato de defesa brasileiro é pacífica e interessada na proteção do próprio território.

Observa-se aqui uma inflexão entre a PDN e a END. Enquanto a PDN dá grande ênfase a capacidade defensiva, a END dá maior atenção a capacidade dissuasória. Embora uma não exclua a outra, uma força dissuasória no setor cibernético implicaria efetivamento no desenvolvimento de uma capacidade de ataque, de represália. Trata-se de um aspecto sutil mas que no caso específico do setor cibernético, faz toda a diferença, leve-se em consideração

que um aparato de defesa cibernética tem pouco ou nenhuma semelhança com um aparato de ataque. Enquanto um fuzil é fuzil e pode ser usado para atacar ou defender, um vírus é um armamento com a finalidade de se propagar e corromper os sistemas enquanto um antivirus é uma ferramenta de busca concebido para eliminar vírus com uma metodologia completamente diferente da usada por um vírus.

A Estratégia coloca como um de suas principais diretrizes o fortalecimento e aperfeiçoeamento desses setores estratégicos. Argumenta-se que o fortalecimento desses setores assegurará uma atuação mais flexível das Forças que terão sua capacidade de atuar em rede e com o uso de uma tecnologia independente de tecnologias estrangeiras.

A questão da atuação mais flexível parece estar associada à ideia de gerações da guerra, conforme apresentado no primeiro capítulo. Defende-se que a flexibilidade é "a capacidade de empregar forças militares com o mínimo de rigidez pré-estabelecida e com o máximo de adaptbilidade à circunstância de emprego da força" (END, p. 23). Implantar esta forma de operar em instituições que tanto prezam pela organização e disciplina é o primeiro desafio que se apresenta. Por outro lado, parece-me que trata-se de uma tentativa de implantar técnicas de guerrilha nas forças regulares, o que sugeriria uma preparação para um conflito assimétrico, onde esse tipo de combate tem melhores resultados.

O eixo estruturante da END que diz respeito à forma de organização das Forças Armadas, identifica três setores cujo desenvolvimento é decisivo para a defesa nacional: o nuclear, o cibernético e o espacial. A estratégia, sob justificativa de sistematizar uma estratégia de defesa integrada atribuiu a cada Força um desses setores decisivos, que ficaram conhecidos também como setores estratégicos da END. A saber, o setor nuclear, sob responsabilidade da Marinha do Brasil, o setor cibernético sob responsabilidade do Exército Brasileiro e o setor espacial, obviamente, à Força Aérea Brasileira.

O desenvolvimento da defesa cibernética é um tópico que tem como pré-requisito a interoperabilidade, no mínimo, entre o Exército e a Aeronáutica, leve-se em consideração que o setor aeroespacial ficou a cargo da Força Aérea e o sistema de comunicação em rede necessita, em grande medida, de satélites. Isto torna inevitável um trabalho conjunto as três forças, o que contribui para atingir um dos objetivos postulados pela PND que seria aumentar a integração e interoperabilidade das três forças.

A END determina ainda que as capacitações cibernéticas deverão ter como parte prioritária as tecnologias de comunicação, inclusive por meio de veículos espaciais, entre as forças, de forma que se assegure a capacidade de atuação em rede.

Outro aspecto para o qual a END chama a atenção é a necessidade de aperfeiçoar dispositivos e procedimentos de segurança visando reduzir a vulnerabilidade dos sistemas cibernéticos relacionados com a Defesa Nacional, são os casos dos sistemas da Casa Civil e do Gabinete de Segurança Institucional da Presidência da República, do Ministério da Defesa, Ministério das Comunicações e Ministério da Ciência, Tecnologia e Inovação. Vislumbra-se ainda a hipótese de restabelecimento destes sistemas em caso de impossibilidade de se evitar um ataque.

Observa-se a intenção de se adotar uma estratégia híbrida que envolve ações preventivas e a preparação para ações reativas, ou seja, como reagir se atacado. Porém, o foco é a defesa dessas infraestruturas e o desenvolvimento da capacidade defensiva, o que se faz com foco em aparatos de inteligência e, consequentemente, vigilância.

De fato, a PDN e a END, no que se refere ao espaço cibernético, se mostram bastante alinhadas, com exceção de pequenas nuânces, como a questão do poder dissuasório. Observa-se, entretanto, uma maior proeminência dada ao setor cibernético na Estratégia. Este aspecto salta aos olhos e pode demonstrar uma diferente hierarquização das prioridades nos diferentes momentos de concepção de cada documento.

Por fim, vale destacar a criação de uma organização encarregada de "desenvolver a capacitação cibernéticas nos campos industrial e militar" (END, p. 33). O que mais tarde viria a ser o Núcleo do Centro de Defesa Cibernética (CDCiber), inaugurado em 6 de agosto de 2010. Núcleo este que tem como síntese de sua missão “Coordenar e Integrar”. Criado para atender determinações da END, o núcleo ainda se encontra e fase de estabelecimento.

CONCLUSÃO

Com a ausência de uma ameaça clara ao Estado brasileiro fica difícil orientar a sua defesa. Mais difícil ainda, é justificar o investimento de recursos na criação de um novo ramo da guerra, o espaço cibernético. Contudo, como foi demonstrada nesta pesquisa, a preocupação com o setor cibernético justifica basicamente por dois motivos: *i*) a condição anárquica do sistema internacional que o torna imprevisível; *ii)* o resultado devastador que um ataque bem sucedido às infraestruturas críticas, especialmente, por meio dos sistemas de comando e controle que residem no espaço cibernético.

O progresso econômico e técnico de uma sociedade resulta na cobiça internacional e chama a atenção de outros países com interesses adversos. Assim, a preocupação dos Estados com assuntos de segurança precisam estar a altura de sua importância no mundo pois essas questões são essenciais para sobrevivência e ascensão contínua de um Estado. Por esses motivos, a capacitação tecnológica é um fator decisivo no provimento da segurança, lição que se aprende observando milhares de anos de história da guerra: uma vantagem tecnológica pode representar a proeminência de um país no mundo.

Apesar dessa importância crucial da tecnologia, nega-se a ideia de que ela tenha capacidade de mudar a própria natureza da guerra, pois trata-se de um componente de nível tático/estratégico, ou seja, apenas um elemento da preparação para a guerra que exerce influência direta nos métodos de enfretamento, não alterando o fato desta ser um fenômeno histórico e político indissociável de seu contexto, ou ainda, "...uma continuação da política por outros meios" (Clausewitz, 2012: 27).

A Política Nacional de Defesa representa um grande avanço por trazer clareza conceitual a ser utilizada pelo país, além disso, aponta um norte para onde o país deve se orientar. Algo que não é fácil com a ausência de ameaças claras e objetivas como é o caso do Brasil.

A PND foi importante também por abrir espaço para uma Estratégia de Defesa Nacional que, apesar de ser excessivamente ambiciosa, representa um avanço para o Brasil no sentido de contribuir com nossa defesa de maneira pragmática e organizada.

Por fim, é importante chamar a atenção para o aspecto que seja talvez o mais intrigante deste trabalho: o clássico dilema da segurança *vs*. vigilância. Como em várias outras áreas da segurança, o setor cibernético, a medida em que se torna objeto de preocupação torna-se também, inevitavelmente, objeto de vigilância. Talvez o grande desafio que se afigura agora

seja definer até que ponto se deve dar poder de vigiar ao Estado? Esta questão não poderá ser respondida sem detalhados debates que temo não serem passíveis de resultados faceis ou agradáveis. De fato, esse desafio não se apresenta somente para o Brasil pela própria caracteristica universalizante do espaço cibernético. Isso porque, não se tem mais hoje um carro ou um telefone, se tem um computador sobre rodas e um computador capaz de fazer chamadas de voz e todos, de uma forma ou de outra, ligados ao espaço cibernético. Isto implica dizer que todos somos afetados pelas ações estatais nesta área.

Isto posto, chama a atenção a falta de material bibliográfico debatendo específicamente a problemática do espaço cibernético e sua influência no provimento da segurança e da defesa, o que torna este trabalho desafiador mas que ao mesmo tempo contribui para a dificuldade de se elaborar uma conclusão mais precisa, haja vista que não é possível escrever nada mais do que uma aproximação inicial ao assunto.

BIBLIOGRAFIA

ALMEIDA. Paulo Roberto. A Arte de NÃO Fazer a Guerra: Novos Comentários à Estratégia Nacional de Defesa. Revista Geopolítica, v. 1, n.º 2, Ponta Grossa, 2010.

ALSINA Jr., Política Externa e Política de Defesa no Brasil: Síntese Imperfeita. Brasília: Câmara dos Deputados, Coordenação de Publicações, 2006.

ANCONA, Clemente. Tática/estratégia. In Enciclopédia Eunaudi volume 14: Estado/guerra. Lisboa: Casa da Moeda / Imprensa Nacional, 1989.

ARGUELHES, Delmo de Oliveira & ÁVILA, Carlos Dominguez. História da América do Sul e cultura estratégica: estão conflitos do passado presentes hoje? In OLIVEIRA, Marcos Aurélio Guedes de (org). Comparando a defesa sul-americana. Recife: Editora Universitária UFPE, 2011.

ARON, Raymond. A guerra é um camaleão. In Pensar a Guerra, Clausewitz – volume 2: a era planetária. Brasília: Edunb, 1986.

ASSANGE, Julian; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie. Cypherpunks : Liberdade e o Futuro da Internet. São Paulo : Boitempo, 2013.

BAKER, Stewart e WATERMAN, Shaun. Sob fogo cruzado: Infraestrutura crítica na era da guerra cibernética. Relatório McAfee, 2012. Disponível em: <mcafee.com.br>. Acesso em 15.dez.2012.

BULL, Hedley. A sociedade Anárquica, Um estudo da ordem política mundial. Universidade de Brasília, Imprensa Oficial do Estado de São Paulo, 2002.

BURKE, Anthony. *Beyond Security, Ethics and Violence: War Against the Other,* Londres: Routledge, 2007.

BUZAN, Barry. People, states and fear: an agenda for international security studies in the post cold war era. Boulder: Lynne Rienner Publishers, 1991.

BUZAN, Barry; WEAVER, Ole; DE WILDE, Jaap. Security: a new framework for analysis. Boulder: Lynne Rienner Publishers, 1998.

CARNEIRO, João Marinônio Enke. Os setores estratégicos da Estratégia Nacional de Defesa: O setor Cibernético. In VI Curso de Extensão em Defesa Nacional, 2013. Disponível em: <http://www.defesa.gov.br/projetosweb/cedn/downloads.html>. Acessado em 22/06/2013.

CLAUSEWITZ, Carl Von. Da Guerra. São Paulo: Editora WMF Martins Fontes, 2010.

COHEN, E. *American views of the revolution in military affairs. Mideast security and policy studies,* v. 8, 1999.

COUTAU-BÉGARIE, Hervé. Tratado de Estratégia. Rio de Janeiro: Escola de Guerra Naval, 2010.

CREVELD, Martin Van. *The transformation of war: the most radical reinterpretation of armed conflict since Clausewitz*. Nova York: Free Press, 1995.

DENNING, Dorothy E. *CYBERTERRORISM Testimony before the Special Oversight Panel on Terrorism*. The Terrorism Research Center, Georgetown University, Washington D.C., 2000.

DUARTE, Érico Esteves. As Falácias em Torno da Proposta de Guerra de Quarta Geração. In: Encontro Nacional da Associação Brasileira de Estudos de Defesa (ENABED), 4., 2010. Anais...Brasília, 2010.

_____. Tecnologia Militar e Desenvolvimento econômico: Uma Análise Histórica. Rio de Janeiro: IPEA, 2012.

DUROSELLE, Jean-Baptiste. Todo Império Perecerá. Brasília: Editora da Universidade de Brasília, 2000.

FRANCO, Moreira. A defesa nacional no dia a dia do cidadão. Correio Braziliense de 30.ago.2012.

GIBSON, William. Neuromancer. São Paulo: Editora Aleph, 1991.

HAMMES, Thomas X. *Countering evolved insurgent networks*. Marine Corps Gazette, vol. 91, n.º 10. Quantico: Marine Corps Association, 2007.

HAMMES, Thomas X. *The Sling and the Stone: on war in the 21st century.* Minneapolis: Zenith, 2006.

HELD, David. *Democracy and the Global Order: From the modern state to Cosmopolitan Governance.* Stanford University Press, 1995.

HOBBES, Thomas. O Leviatã. Lisboa, Imprensa Nacional, 2002.

KUEHL, Dan. *From Cyberspace to Cyberpower: Defining the Problem*. In: KRAMER, Franklin; STARR, Stuart; WENTZ, Larry *Cyberpower and National Security*. Washington, Estados Unidos: National Defense University Press, 2009

LESSIG, Lawrence. *Code and Other Laws of Cyberspace.* Nova York: Basic Books, 1999.

LEVINE, Barry. The man who put Al-Qaeda on the Web, Newsfactor Mag. Online 2006. Disponível em: <http://www.globalsecurity.org/org/news/2006/060729-alqaeda-web.htm> Acesso em: 15.jan.2013.

LOPEZ, C. Todd. Senior Leaders Discuss Fighting in Cyberspace, INTERCOM, novembro de 2006. Disponível em: <http://public.afca.af.mil/shared/media/document/AFD-061220-041.pdf> Acesso em: 15.jan.2013.

LEWIS. James A. *Thresholds for Cyberwar*. Center for Strategic International Studies, 2010.

LUCERO, Everton. Governança da Internet: aspectos da formação de um regime global e oportunidades para a ação diplomática / Everton Lucero – Brasília: Fundação Alexandre de Gusmão, 2011.

MILEVSKI, Lukas. *Stuxnet and Strategy: A Special Operation in Cyberspace?* JFQ / issue 63, 4ª quartier 2011. Disponível em: <ndupress.ndu.edu> Acesso em: 15.jan.2013.

MONTEIRO, Silvana Drumond. Ciberespaço: o Termo, a Definição e o Conceito. DataGamaZero – Revista de Ciência da Informação. Vol. 8, n. 3, jun. 2007. Disponível em: <http://dgz.org.br/jun07/Art_03.htm>. Acesso em: 10.jun.2013.

PEREIRA, Priscila Rodrigues. Política de Defesa Nacional, Estratégia Nacional de Defesa e Livro Branco de Defesa: um processo não linear. Mundorama, 2010. Disponível em: <http://mundorama.net/2010/12/01/politica-de-defesa-nacional-estrategia-nacional-de-defesa-e-livro-branco-de-defesa-um-processo-nao-linear-por-priscila-rodrigues-pereira/> Acesso em: 10.mai.2013

PROENÇA Jr., Domício *ET alli*. Guia de Estudos de Estratégia. Rio de Janeiro: Jorge Zahar Editor, 1999.

PROENÇA Jr., Domício; DINIZ, Eugênio. Política de Defesa no Brasil: uma análise crítica. Brasília: Editora Universidade de Brasília, 1998.

PROENÇA JÚNIOR, D.; DUARTE, É. *The Concept of Logistics derived from Clausewitz: All That is Required so That The Fighting Force Can Be Taken as a Given.* Journal of Strategic Studies, v. 28, n. 4, 2005.

RICE, C. *The Making of Soviet Strategy*. *In*: PARET, P. (Ed.). *Makers of modern strategy*. Princeton University Press, 1986.

SAINT-PIERRE, Héctor Luis. "Defesa" ou "segurança"?: reflexões em torno de conceitos e ideologias. **Contexto int.**, Rio de Janeiro, v. 33, n. 2, Dec. 2011 . Disponível <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292011000200006&lng=en&nrm=iso>. Acesso em: 23 de junho 2013.

SCHMITT, Carl. Teologia Política. Belo Horizonte: Del Rey, 2006.

SOLCE, Natasha. *Battlefield of Cyberspace: The Inevitable New Military Branch.* 18 Alb. L.J. Sci. & Tech., 2008.

TEIXEIRA JR., Augusto Wagner Menezes & LUCENA SILVA, Antonio Henrique. Contribuições de Barry Buzan para a evolução dos Estudos Estratégicos Pós-Guerra Fria: Dinâmica Armamentista, Polaridade e a *Regional Security Complex Theory*. Encontro Nacional da Associação Brasileira de Estudos de Defesa (ENABED), 4., 2010. Anais...Brasília, 2010.

WALKER, R. B. J. *Lines of Insecurity: International, Imperial, Exceptional. Security Dialogue,* v. 37, n. 1, 2006.