UNIVERSIDADE DA FORÇA AÉREA BRASILEIRA

PROGRAMA DE PÓS GRADUAÇÀO

MESTRADO EM CIÊNCIAS AEROESPACIAIS

Jaceguai de Magalhães

A FORÇA AÉREA BRASILEIRA E A GUERRA CIBERNÉTICA:
A Necessidade do Domínio do Ciberespaço

RIO DE JANEIRO

Dezembro de 2010

Jaceguai de Magalhães

A FORÇA AÉREA BRASILEIRA E A GUERRA CIBERNÉTICA:
A Necessidade do Domínio do Ciberespaço

Dissertação apresentada ao Programa de Pós-graduação da Universidade da Força Aérea como requisito parcial para a obtenção do título de Mestre em Ciências Aeroespaciais.

ORIENTADOR: Prof. Dr. Luiz Carlos Fumiaki Miwa

RIO DE JANEIRO
Dezembro de 2010

AGRADECIMENTOS

Agradeço aos meus orientadores pela paciência e confiança em meu trabalho, a Deus por manter tudo justo e perfeito e, em especial, a minha esposa, Élen, e filha, Ana Carolina, pelo apoio e compreensão pelas longas horas de ausência.

“Quanto mais conhecemos, mais amamos.”
Leonardo da Vinci

RESUMO

O objetivo da presente pesquisa é diagnosticar a realidade da Força Aérea Brasileira (FAB) quanto ao desenvolvimento de ações de Guerra Cibernética. Para atingir tal objetivo, este trabalho baseou-se em pesquisas que apresentaram a Guerra Cibernética como uma forma de guerra voltada à consecução dos objetivos nacionais. Além disso, a Guerra Cibernética pode ser utilizada de forma sinérgica com métodos tradicionais de Guerra Cinética, aumentando a eficiência de seus resultados e a sua eficácia, como, por exemplo, no caso da Guerra Centrada em Redes. O trabalho teve início com a fundamentação da Guerra Cibernética, prosseguindo com o estudo das ações realizadas pela China, pelos Estados Unidos da América e pela Rússia, de forma a fornecer parâmetros para a análise das ações realizadas pela FAB. Por fim, chegou-se ao diagnóstico de que a Guerra Cibernética, no âmbito da FAB, encontra-se em um estágio inicial de desenvolvimento, se comparado aos países citados, carecendo de mais desenvolvimento a fim de diminuir vulnerabilidades presentes, devido à incorporação da tecnologia da informação a diversos sistemas.

Palavras-chave: Ataques digitais. Guerra Cibernética. Guerra da Informação. Paralisia. Centros de Gravidade.

ABSTRACT

The objective of this research is to diagnose the Brazilian Air Force's reality in the development of Cyber Warfare activities. To achieve this goal, this work was based on researches that presented Cyber Warfare as a form of war aimed at the achievement of national objectives. In addition, Cyber Warfare can be used synergistically with traditional methods of Kinetics War, increasing the efficiency of its results and its effectiveness, such as in the case of network-centric warfare. The work began with the characterization of Cyber War, continuing the study of actions taken by China, the United States of America and Russia in this field in order to provide parameters for the analysis of actions taken by Brazilian Air Force. Finally, we arrived at a diagnosis that the Cyber Warfare, under Brazilian Air Force, is at an initial stage of development, when compared to the countries mentioned here, requiring a better development to reduce vulnerabilities due the incorporation of information technology in several systems.

Key-words: Digital Attacks. Cyber Warfare. Information War. Paralysis. Center of Gravity.

LISTA DE ABREVIATURAS E SIGLAS

BANT	- Base Aérea de Natal
BASV	- Base Aérea de Salvador
Bda Inf L	- Brigada de Infantaria Leve
BRICs	- Bloco de países formado por Brasil, China, Índia e Rússia
C2	- Comando e Controle
C2W	- do inglês *Command and Control Warfare* (Guerra de Comando e controle)
C3I	- Comando, Controle, Comunicações e Inteligência
C4IVR	- Comando, Controle, Comunicações, Computação, Inteligência, Vigilância e Reconhecimento (C4ISR, na sigla em inglês)
CAV	- Controle Aéreo Avançado
CCABR	- Centro de Computação da Aeronáutica de Brasília
CCARJ	- Centro de Computação da Aeronáutica do Rio de Janeiro
CCASJ	- Centro de Computação da Aeronáutica de São José dos Campos
CERT.BR	- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CG	- Centros de Gravidade
CIA	- Central de Inteligência Americana
CINDACTA 3	- Terceiro Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo
COMAER	- Comando da Aeronáutica
COMAR 3	- Terceiro Comando Aéreo Regional
COMAR 7	- Sétimo Comando Aéreo Regional
CTIR	- Centro de Tratamento de Incidentes de Segurança em Redes
DDOS	- *Distributed Denial of Service* (negação de serviço distribuida)
DNS	- *Domain Name Service* (serviço de nome de domínio)
DTI	- Diretoria de Tecnologia da Informação da Aeronáutica
E3	- Envelope de Emprego Efetivo
EEAR	- Escola de Especialistas da Aeronáutica
END	- Estratégia Nacional de Defesa
EUA	- Estados Unidos da América

FAB	- Força Aérea Brasileira
GC	- Guerra Cibernética
GCR	- Guerra Centrada em Redes
GOV	- Governo Federal Brasileiro
IPS	- *Intrusion Prevention System* (sistema de prevenção a invasões)
JTDIS	- *Joint Tactical Information Distribution System* (Sistema de Distribuição de Informações Táticas Conjuntas)
OCR	- Operações Centradas em Rede
OODA	- Ciclo de Observação, Orientação, Decisão e Ação de Jonh Boyd
PAGL	- Prefeitura de Aeronáutica do Galeão
PDA	- Processamento de Dados Administrativos
PLA	- *People's Liberation Army* (Exército Popular de Libertação)
PND	- Política Nacional de Defesa
PSYOP	- Operações psicológicas, da sigla em inglês
RAM	- Revolução em Assuntos Militares
SBCT	*Striker Brigade Combate Team* (Brigada de Ataque de Time de Combate)
SI	- Sistemas de Informação
SIGPES	- Sistema de Informações Gerenciais de Pessoal
SILOMS	- Sistema Integrado de Logística Manutenção e Serviços
STI	- Sistema de Tecnologia da Informação do Comando da Aeronáutica
TI	- Tecnologia da Informação
UNIFA	- Universidade da Força Aérea

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

De uma forma cada vez mais abrangente, a vida moderna vem utilizando-se dos avanços e facilidades oferecidas por tecnologias informatizadas. No mundo atual, a tecnologia da informação está cada vez mais presente no dia-a-dia das pessoas e organizações, o que torna impossível imaginar a manutenção do modo de vida atual sem a presença da informática, que, embora crie vantagens incalculáveis, cria vulnerabilidades, antes inexistentes.

A Tecnologia da Informação (TI) trouxe à humanidade um fator diferencial em seu desenvolvimento ao longo da história, pois a sua utilização possibilitou, de forma não antes concebida, o gerenciamento e a troca de informações, atuando, de forma exponencial, na produção de conhecimentos e como ferramenta fundamental na execução de praticamente todas as atividades da atualidade.

Essa atuação da TI tomou vulto ainda mais elevado com a utilização de computadores em rede e, hoje, com a interligação global através da *internet*, atingiu níveis elevadíssimos de integração que evidenciam, cada vez mais, o ganho de seus benefícios. Porém, como efeito colateral, trouxe uma dependência de sistemas interligados em rede, o que veio a criar uma vulnerabilidade que passou a ser alvo de exploração nos dias atuais.

Essa vulnerabilidade é explorada por um ramo novo da Arte da Guerra conhecido como Guerra Cibernética (GC), a qual tem se tornado matéria cada vez mais presente nos estudos militares de diversas nações, que identificaram nela um meio eficiente a ser utilizado no esforço de combate.

Seguindo essa linha, conflitos da atualidade demonstraram o poder dessa nova forma de guerrear. Portanto, evidenciaram a necessidade do entendimento dessa nova fonte de poder por parte das Forças Armadas que pretendam estar inseridas, de forma destacada, no cenário moderno, trazendo a necessidade de estudos científicos que venham desmistificar o assunto.

Como exemplo de estados que têm dado significativa importância na área de Guerra Cibernética, conforme Carr (2009), destacam-se a China, a Rússia e os Estados Unidos, que, embora de modos distintos, possuem incluídas na composição doutrinária de suas Forças Armadas o tema Guerra Cibernética.

Assim, conforme sinalizado por Forças Aéreas de outros países, é necessário que a Força Aérea Brasileira (FAB) estude essa nova forma de guerrear, o que leva à questão-problema que orientou toda a pesquisa científica:

Qual o cenário vivido pela Força Aérea Brasileira no desenvolvimento de ações de Guerra Cibernética?

A fim de responder essa questão, o objetivo geral deste trabalho é diagnosticar a situação em que a FAB se encontra quanto ao desenvolvimento de ações de Guerra Cibernética. No intuito de atingi-lo, foram estabelecidos, como marcadores intermediários, os seguintes objetivos específicos, que serviram para o alcance do objetivo geral:

a) discutir os fundamentos da Guerra Cibernética;
b) caracterizar ações que podem ser realizadas por Forças Aéreas utilizando-se de princípios de Guerra Cibernética; e
c) analisar a Força Aérea Brasileira quanto às ações de Guerra Cibernética.

Este trabalho justifica-se pelo fato da Guerra Cibernética, com a recente explosão e desenvolvimento da Tecnologia da Informação (TI), ter-se tornado uma realidade no mundo contemporâneo, apresentando-se como um meio eficiente ao esforço de combate de Nações, Exércitos, Grupos Organizados e, até mesmo, indivíduos. Diversos conflitos recentes demonstraram ao mundo o poder de destruição causado por atividades executadas no ambiente cibernético, portanto é de vital importância à Forca Aérea Brasileira (FAB) o domínio de tal recurso de forma a incorporá-lo em seu arsenal.

Porém, para que efetivamente essa arma venha a ser utilizada de forma eficaz e eficiente pela FAB, é necessário a sua utilização sistematizada e planejada, o que, devido aos recentes avanços tecnológicos e a relativa novidade do assunto, traz uma grande necessidade de estudos científicos sobre o tema.

Assim, o estudo do referido tema torna-se investido de importância, pois auxiliará na composição de um conhecimento necessário ao aumento do nível de poder da Força Aérea Brasileira. Caso esta força venha a desconsiderar tal assunto, estará deixando, não apenas, de usar uma arma de elevado potencial ofensivo, mas também, principalmente, estará se colocando em uma posição de grande vulnerabilidade.

Para estudar esse assunto, de elevada importância, será utilizada, como referencial teórico, a teoria de Armistead (2004) que, em seu trabalho, apresentou a informação como um elemento do poder, antes limitada pelo fator tecnológico. Na atualidade, tal limite foi ultrapassado com o desenvolvimento do ambiente cibernético, o que fez com que a informação proporcionasse um significativo aumento do nível de poder quando utilizada de forma adequada.

Ainda, de acordo com Armistead (2004), a explosão da computação, das telecomunicações e da tecnologia de mídia modificou a visão desse poder, tornando a informação, com seu componente cibernético, o seu elemento mais importante.

Dessa forma, conforme Armistead:

> Lições aprendidas após a Operação Tempestade no Deserto apontam ao fato de que a nação que puder controlar o fluxo de informações irá vencer o conflito. Quer essa informação esteja na forma de inteligência militar, propaganda, comprimento de ondas eletrônicas ou fluxo de dados computadorizados, a habilidade para manipular informação será a conquista primária dos conflitos futuros. (ARMISTEAD, 2004, p. 14).

Assim sendo, conforme Armistead (2004), o poder é definido como a habilidade de um determinado elemento fazer com que outro realize algo que não faria de outra forma, servindo, assim, o domínio do fluxo de informações no ambiente cibernético, quando utilizado para este fim, como um fator vital a toda Força Armada que intencione elevar seu nível de poder de forma a obter a preponderância nos campos de batalha.

Diversos autores vêm realizando estudos acerca da Guerra Cibernética, e durante este trabalho suas obras serão utilizadas para fornecer uma revisão de literatura que possibilitará a verificação da situação da FAB quanto ao desenvolvimento de ações nesta área.

Nesse sentido, Bobbit (2003) citou que a guerra cibernética é uma modalidade relativamente nova, que vem acompanhando a emergência de uma nova forma de ordem constitucional, fruto de uma revolução dos meios militares que venceram a Longa Guerra (período englobando o início da Primeira Guerra Mundial, em 1914, até novembro de 1990 após a unificação da Alemanha) trazendo à tona o Estado-Mercado em detrimento do Estado-Nação. Essa revolução militar, ainda segundo Bobbit (2003), é entendida num sentido mais amplo que meramente a tecnologia de ponta, ela é consequência de um fenômeno triplo dos armamentos nucleares e demais armas de destruição em massa, telecomunicações internacionais e poder da computação rápida.

Analisando a forma de lutar em diversas ocasiões da história, Hanson (2002) alega que o Ocidente alcançou a preponderância militar de diversas maneiras, que transcendem a superioridade em matéria de armas e que nada têm a ver com moralidade ou genes. Segundo ele, “a guerra à moda ocidental é tão letal justamente por ser tão amoral – raramente perturbada por preocupações com rituais, tradições, religião ou ética, por nada além da necessidade militar” (HANSON, 2002, p. 41).

A preponderância militar ocidental, de acordo com Hanson (2002), é baseada em uma forma de guerrear direcionada às colisões de choque, sem restrições ao emprego de seus meios em uma batalha decisiva e, historicamente, apoiada em sua superioridade tecnológica. O domínio de fatores tecnológicos sempre serve como apoio à vitória obtida por meio de uma batalha direta e quando nações não ocidentais infringiram derrotas às nações ocidentais, tal feito acorreu com a utilização de tecnologia ocidental.

Com o desenvolvimento das linhas estratégicas de guerra, diversos conceitos foram inseridos no arcabouço estratégico-militar da atualidade, dentre eles o da paralisia de Fuller (1926), o ciclo OODA de Boyd (OSINGA, 2007), o do Modelo dos Cinco Anéis de Warden (1995) e o de Guerra Paralela de Warden (1995). Tais conceitos mostram-se intimamente ligados ao conceito de Guerra Cibernética.

Demonstrando a utilização da Guerra Cibernética no cenário moderno, Rattray (2001) definiu que o pensamento militar moderno integrou o uso da tecnologia da informação para aprimorar tradicionais formas de guerra, citando como exemplo a influência decisiva, durante o sucesso americano na guerra do golfo, da integração de sistemas de informação com uma sofisticada capacidade de força convencional.

Dessa forma, as forças armadas necessitam adaptar-se ao novo ambiente de guerra em que Sistemas de Informação servem como armas e alvos. Rattray (2001) complementa que a perspectiva de guerra no Ciberespaço apresenta-se como uma oportunidade militar, mas, também, envolve novos riscos significativos de segurança nacional.

Citando a Guerra do Golfo, Rattray (2001) relatou que prover informações precisas e em tempo mostrou-se um desafio aos comandantes americanos durante a execução de operações. Os Estados Unidos atacaram a inteligência, rede de

comunicações e comando iraquiano para cegar seus oponentes no campo de batalha e desconectar a população de sua liderança.

Nesse sentido, Warden (1995), cita o que Clausewitz considerava impossível, ou seja, o ataque simultâneo a vários alvos ao mesmo tempo, hoje, com a Tecnologia da Informação, tornou-se possível, sugestionando uma nova mudança de era na História da Guerra.

De acordo com Arquilla e Ronfeldt (1993), a Guerra Cibernética apareceu como um desenvolvimento de estratégias de guerra baseadas na informação, que agora, com o advento da informática, obtiveram as ferramentas necessárias para aumentar o seu potencial de forma substancial.

Tal potencial foi observado por diversos países, entre eles EUA, China e Rússia, que observaram, segundo Carr (2009), não só a necessidade de defender-se contra essa nova arma, mas, também, uma grande oportunidade de aumentar o seu nível de poder.

Em uma demonstração da concretização da Guerra Cibernética em seu potencial, segundo Alberts, Garstka e Stein (1999), surgiu o conceito de Guerra Centrada em Redes, que é uma filosofia de combate que tem seu foco no poder de combate adquirido pelo elo formado entre os diversos elementos participantes de uma rede de combate. Tal compartilhamento, ainda segundo os autores citados, forneceu um elevado nível de poder às forças armadas que o vem utilizando.

Porém, tal nível de poder trouxe, segundo Alberts, Garstka e Stein (1999), vulnerabilidades que são objeto de ataques por parte de grupos engajados em guerras assimétricas e irregulares, como, por exemplo, os grupos terroristas.

Segundo Uda (2009), o terrorismo cibernético é algo cada vez mais presente na sociedade moderna, com elevado potencial de perigo, que traz a toda nação, e por consequência a suas Forças Armadas, um potencial de perigo, que gera um desafio de grande monta na execução de medidas que contraponham essa ameaça.

Assim, esse embasamento teórico foi utilizado para fornecer informações de grande valia para a resposta da questão-problema apresentada. Porém para que este objetivo seja alcançado, foi utilizada a metodologia descrita a seguir.

Para a realização do presente estudo a metodologia adotada foi a pesquisa exploratória bibliográfica e documental.

A pesquisa baseou-se em livros, artigos científicos, entrevistas na *web*, documentos eletrônicos, doutrinas de Forças Aéreas e documentações normativas, entre outras fontes, a respeito do tema específico, bem como temas relacionados, com a finalidade de obter informações necessárias à fundamentação teórica da Guerra Cibernética, bem como para a caracterização de ações que podem ser realizadas utilizando-se este conceito.

Feita tal atividade, foram estudados casos específicos referentes às ações realizadas por diversos países, de modo a fornecer parâmetros de comparação que possibilitem analisar as ações realizadas pela FAB, viabilizando, assim, o diagnóstico da sua realidade no desenvolvimento de ações de Guerra Cibernética, objetivo geral do trabalho.

Para atingir esse objetivo, esta dissertação foi estruturada de forma que no Capítulo 2 são apresentados os fundamentos conceituais da Guerra Cibernética, prosseguindo o Capítulo 3 com a apresentação da Guerra Cibernética na estratégia de Guerra Moderna.

A seguir, no Capítulo 4, são evidenciadas ações efetivas realizadas pela China, Rússia e EUA com relação à Guerra Cibernética, de forma a se fornecer parâmetros passíveis de comparação com relação à situação da Força Aérea Brasileira.

O Capítulo **Erro! Fonte de referência não encontrada.**, descreve a metodologia utilizada para atingir os objetivos específicos, e, consequentemente, o objetivo geral da dissertação, prosseguindo o Capítulo 6 com a análise dos dados obtidos, primeiro em seus aspectos estratégicos e doutrinários, e, depois, com relação à situação da Guerra Cibernética na FAB.

Assim, com o tema do trabalho situado, o momento mostra-se oportuno para passar à discussão a respeito dos fundamentos teóricos da Guerra Cibernética.

2 FUNDAMENTOS DA GUERRA CIBERNÉTICA

O conceito de Guerra Cibernética está relacionado ao campo da Tecnologia da Informação (TI). Portanto, sofre constantes modificações em um pequeno espaço de tempo, que são marcas pelo que hoje é conhecido como Revolução da Informação.

Segundo Arquilla e Ronfeldt (1993), a Revolução da Informação é o avanço da informação computadorizada, da tecnologia da comunicação, de inovações organizacionais e da teoria de gerenciamento pelo qual o mundo vem passando na atualidade. Essa Revolução da Informação alterou a forma como as organizações têm se projetado para tirar vantagens da nova forma de coleta, armazenamento, processamento, transmissão e apresentação das informações, transformando-as em um recurso estratégico tão valioso na era pós-industrial, quanto o capital e o trabalho foram para a era industrial.

Esse aumento da dependência da sociedade moderna com relação à informação refletiu-se no meio militar, dando origem a um fenômeno em que Sistemas de Informação (SI) “podem atualmente servir tanto como arma como alvo” (RATTRAY, 2001, p. 1), gerando uma “Guerra da Informação”.

Portanto, para discutir o conceito de Guerra Cibernética, é necessário primeiro conceituar a Guerra da Informação, que é o grande conjunto do qual a Guerra Cibernética é uma categoria.

2.1 A GUERRA DA INFORMAÇÃO

Uma abordagem típica na definição de Guerra da Informação é que ela “é simplesmente o uso da informação para atingir os objetivos nacionais” (STEIN, 1995, p. 32).

Segundo LIBICKI (1995), a Guerra da Informação é representada por sete categorias diferentes, a saber:

a) guerra de inteligência;
b) guerra eletrônica;
c) guerra de comando e controle;
d) guerra de *hacker*;
e) guerra psicológica;

f) guerra de informações econômicas; e

g) guerra cibernética.

Portanto, embora o objeto desse trabalho seja a Guerra Cibernética, mister se faz que uma análise da Guerra da Informação seja realizada, uma vez que aquela acaba por herdar as características inerentes a esta. Vale ressaltar, ainda, que, entre os diversos autores, por vezes, os dois conceitos misturam-se vindo a ser utilizados como sinônimos.

Observa-se, nessa divisão, a presença de dois conceitos muito semelhante que merecem ser diferenciados, que são os conceitos de Guerra Hacker e a Guerra Cibernética.

Segundo Uda (2009), a diferença entre os dois conceitos está ligada principalmente na finalidade das atividades. Na Guerra Hacker os objetivos de seus autores estão diretamente relacionados a objetivos relacionados a crimes cibernéticos, na busca de objetivos relacionados a interesses de pessoas, organizações e instituições.

Já a guerra cibernética, ainda de acordo com Uda (2009), está relacionada à consecução de objetivos nacionais, ou seja, interesses estatais estão diretamente ligados às atividades, sejam elas defensivas ou ofensivas, numa alusão à consecução dos objetivos políticos de uma nação.

Ainda sobre a conceituação de Guerra da Informação, segundo Stein (1995), verifica-se que o mesmo trata do assunto sem subordinar a Guerra da Informação, ao elemento tecnológico, o que possibilita verificar que a importância da informação para os conflitos não é uma exclusividade do mundo moderno.

Embora cada vez mais a Guerra da Informação venha ganhando importância na doutrina militar, em épocas passadas ela já era considerada um fator preponderante para a vitória.

As guerras travadas pelos Mongóis, nos séculos XII e XIII, foram um exemplo passado da Guerra da Informação, quando o império Mongol veio a se tornar o maior império, em termos territoriais, já conhecido na história da humanidade. A forma de lutar dos Mongóis, para Arquilla e Ronfeldt (1993), foi o

mais próximo que se chegou à condução de uma Guerra da Informação[1] na sua forma mais pura.

> Examinar o costume militar Mongol, dessa forma, será instrutivo para desenvolver os fundamentos para travar uma guerra semelhante no mundo pós-moderno. O uso desse exemplo, também, reforça o ponto de que a Guerra da Informação não depende de alta tecnologia, mas principalmente de como o conflito é concebido e da interação estratégica. (ARQUILLA; RONFELDT, 1993, p. 34, tradução nossa).

Descrevendo o conflito, Arquilla e Ronfeldt (1993), afirmam que o sucesso militar dos Mongóis, basicamente, ocorria pelo fato dos mesmos descobrirem exatamente onde o inimigo estava e quais eram seus planos, enquanto mantinham a sua posição e planejamento em segredo. Desse modo, os mesmos foram capazes de sobrepujar o que havia de melhor nos maiores exércitos da China Imperial, do Islã e da Cristandade, apesar da sua inferioridade numérica crônica.

Uma maneira de ilustrar essa vantagem obtida pelos Mongóis é compará-la a um jogo de xadrez no qual os Mongóis atuavam com peças em menor número e poder, porém podiam antecipar todos os movimentos de seus adversários. Assim, os seus oponentes, mesmo possuindo maior número de peças, não conseguiam transformar tal característica em vantagem, sendo, invariavelmente, derrotados.

Essa vantagem era conseguida pelos Mongóis devido ao fato dos mesmos possuírem uma rede de mensageiros e espiões, que mantinham seu comando constantemente atualizado das informações necessárias e possibilitavam uma cadeia de Comando e Controle. Além disso, a estratégia de combate Mongol primava pela destruição da rede de comunicações do inimigo, cegando-o, para depois desferir-lhe um ataque direto em seu coração.

Os Mongóis utilizavam, com maestria, técnicas de guerra psicológica e de inteligência, o que levava, segundo Arquilla e Ronfeldt (1993), a que os mesmos nem sempre se vissem obrigados a travar batalhas, pois atingiam seus objetivos militares sem a necessidade do combate físico. Porém, quando era necessário o combate, este era travado de forma excepcionalmente coordenada pelos mesmos, que direcionavam seus ataques para destruir os planos de seus oponentes.

---

[1] Os autores, no original, fazem referência à “guerra cibernética na sua forma mais pura”, tratando, no caso, guerra cibernética como sinônimo de Guerra da Informação, porém, modernamente, para conceituar-se guerra cibernética, é necessária a presença do ambiente cibernético, que no século 12 e 13, obviamente, ainda não havia sido desenvolvido.

Lutando dessa forma, o exército Mongol venceu um exército Polonês-Prussiano que era quatro vezes maior, pois os Mongóis, ao saberem dos planos e posições inimigas, movimentaram seus efetivos reduzidos entre as linhas de deslocamento Polonesa-Prussiana, destruindo seus inimigos por partes, derrotando-os sem que os mesmos sequer tomassem conhecimento do quê os havia atacado.

Em termos estratégicos, os Mongóis primeiro buscavam interromper as comunicações inimigas, e depois atacar diretamente em seus centros de gravidade (CG). Analisando a situação, Chambers (2003) concluiu que, de forma contrária a Clausewitz, os Mongóis davam pouco valor à necessidade de destruir as forças inimigas antes do avanço. Também, suas campanhas não eram “lineares”, eles atacavam onde desejavam e onde as circunstâncias eram favoráveis.

“Claramente as chaves do sucesso Mongol foram comando, controle, comunicação e inteligência superiores” (ARQUILLA; RONFELDT, 1993, p. 36, tradução nossa).

O exemplo Mongol, além de demonstrar como a informação pode ser utilizada para vencer uma guerra, mostra, também, que a mesma deve ser vista como um meio para atingir determinado fim, ou seja, serve para alertar quanto à necessidade de uma força militar dominar a utilização da informação como arma de guerra, evidenciando que esta força deve estar focada nos fins a serem alcançados, muito mais que na tecnologia utilizada.

O uso da informação para alcançar os objetivos bélicos continuou e a evolução tecnológica, pela qual a sociedade moderna vem passando, modificou a forma como a informação começou a ser tratada nos meios militares.

Nos dias atuais, segundo Schwartau (1996), os sistemas de informação alcançaram um nível tal de interligação por meio de redes que praticamente todo o funcionamento de uma sociedade moderna é dependente dessa estrutura, o que veio a possibilitar o conceito de Guerra da Informação, apresentado a seguir:

> Guerra da Informação é a aplicação de força destrutiva, em grande escala, contra meios e sistemas de informação, contra computadores e redes que suportam sistemas de controle de tráfego aéreo, transações de bolsa de valores, registros financeiros, câmbio, *internet*, telefonia, registro de crédito, transações de cartões de crédito, programas espaciais, de ferrovias, hospitalares de monitoração de pacientes e farmácia, de controle de processos de manufatura, publicação de jornais, indústria de seguros, utilitários de distribuição de energia e tudo que dependa profundamente de computadores. (RATTRAY, 2001, p. 12, tradução nossa).

Esse conceito demonstra a força com que a tecnologia infiltrou-se nos diversos meios de informações modernas, aparecendo como um fator a ser levado em consideração caso se deseje utilizar o exemplo dos mongóis na utilização da informação, só que, na atualidade, contando com o suporte da Tecnologia da Informação, trazendo à tona a disciplina da Guerra Cibernética, a qual será discutida no próximo tópico.

2.2 A GUERRA CIBERNÉTICA

O conceito de guerra cibernética foi proposto, originariamente, por Arquilla e Ronfeld, que enunciaram: “Guerra Cibernética refere-se à condução e o preparo de operações militares de acordo com princípios relacionados à informação.” (ARQUILLA; RONFELDT, 1993, p. 30, tradução nossa)

Tal conceito, embora englobe os componentes militares e da informação da Guerra Cibernética, torna-se um pouco vago por não fazer referência ao “elemento computadorizado” da disciplina em questão. Em um maior desenvolvimento das teorias de Guerra Cibernética, foi apresentado o conceito de Guerra Cibernética Estratégica como “um meio do estado e de organismos não estatais atingirem seus objetivos por meio de ataques digitais aos centros de gravidade adversários.” (RATTRAY, 2001, p. 14, tradução nossa).

Nesse conceito, mais recente, é verificada a inclusão do “elemento computadorizado”, através do termo digital, e de uma questão importante ao estudo em voga, que é a inclusão do componente estratégico da guerra cibernética ao indicar os centros de gravidade adversários como objetivos.

A conceituação de Rattray é muito importante por, também, trazer à tona a possibilidade da guerra nos dias atuais poder ser travada não somente por estados, mas também por elementos não estatais, numa alusão à substituição do Estado-Nação pelo Estado-Mercado, conforme preconizado por Bobbitt (2003).

Os conceitos apresentados, embora de grande importância e valia, são abrangentes, por isso, para facilitar o entendimento da questão, deve-se adicionar aos dois conceitos apresentados, aquele concebido por Parks e Duggan (*apud* DUTRA, 2007):

> Guerra Cibernética é o sub-conjunto da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes.

> Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra Cibernética é a *Internet* e as redes a ela relacionadas, as quais compartilham mídia com a *Internet*. A definição militar mais próxima para o nosso termo, guerra cibernética, é uma combinação de ataques a redes de computadores, defesa de redes de computadores e possivelmente, operações especiais de informação.
> Nós definimos guerra cinética como sendo a guerra praticada no "mundo real". Todos os tanques e navios e aviões e soldados tradicionais são os protagonistas da guerra cinética.

Como se pode perceber, o uso da tecnologia da informação foi integrado ao pensamento militar e, de acordo com Uda (2009), ataques cibernéticos ofensivos, na guerra de redes, tornam o ataque convencional mais efetivo. Em outras palavras, um sistema de defesa integrado ou um sistema de armas pode ser corrompido usando-se ataques cibernéticos. Os exércitos modernos tendem a ser mais e mais dependentes de computadores e redes computadorizadas, assim, tornando-se mais vulneráveis a esses ataques.

Complementando essa ideia, Rattray (2001) enumerou seis setores considerados críticos e passíveis de ataques cibernéticos, devido à sua dependência de Sistemas de Informação, a saber:

a) segurança nacional;
b) serviços públicos vitais;
c) outros serviços públicos;
d) utilidade pública (transporte e serviços de saúde);
e) usuários comerciais gerais; e
f) operadores e provedores de serviço de rede comercial.

Nota-se que os setores listados podem ser incluídos nos centros de gravidade do Modelo dos Cinco Anéis elaborado por Warden que versa sobre a escolha de alvos a serem atacados com o objetivo de alcançar a vitória.

Esse ponto reforça a importância do ambiente cibernético devido ao fato dele se "embrenhar nos demais recursos dos poderes militar, econômico, social e político, em alguns casos diminuindo suas forças, em outros aumentando-as." (ARMISTEAD, 2004, p. 11, tradução nossa).

Percebe-se que os objetivos da Guerra Cibernética coincidem com os da Guerra Cinética, porém existem diferenças entre as duas formas, diferenças essas que, embora possam não afetar o resultado final esperado, a vitória, tem forte influência no processo de condução da Guerra. Assim pode-se dizer que "a Guerra

Cibernética é a arte de lutar sem lutar; de derrotar o inimigo sem sangrá-lo.” (CARR, 2009, p. 2, tradução nossa)[2].

Para verificar essa diferença processual na condução da Guerra Cibernética é necessário definir os tipos de ataques cibernéticos realizados, conforme definição de Rattray (2001):

a) ataques mecânicos – requerem que o adversário obtenha acesso físico direto ao alvo. Os resultados desse tipo de ataque, geralmente são mais observáveis do que os resultados conduzidos por meios eletrônicos;
b) ataques eletromagnéticos – os componentes eletrônicos e sistemas de informação e redes são vulneráveis ao embaralhamento e ao estrago produzido por energia eletromagnética direcionadas a eles; e
c) ataques digitais – A maior parte da atenção dada aos ataques estratégicos cibernéticos diz respeito às ameaças de invasões e transtornos de sistemas computacionais e redes que suportam infraestruturas avançadas de informação. O efeito desejado de tais ataques pode variar entre a total paralisia, o desligamento intermitente dos sistemas de informação e redes, erros de dados aleatórios, roubo de informações, monitoramento e controle ilícito de sistemas, acesso a dados e inclusão de informações falsas. Adicionalmente, atacantes podem empreender uma inserção de componentes de sistemas corrompidos na infraestrutura adversária de informação, possibilitando ao atacante monitorar acesso, prejudicar ou destruir redes e sistemas adversários.

Como pode ser observado, o ataque digital, especificamente, é o que ocorre no mundo dos computadores e de seus acessórios, e a utilização desses três tipos de ataques poderá ser simultânea, o que deve ser bastante considerado, pois, segundo Rattray (2001), essa utilização simultânea será sinérgica.

> Os níveis de esforço físico, velocidade, trânsito envolvido e caminhos de transmissões possíveis são muito diferentes para ataques digitais do que para ataques tradicionais. No entanto, ataques digitais causam mais transtornos e/ou destruição do que ataques mecânicos e eletromagnéticos. (RATTRAY, 2001, p. 19, tradução nossa).

---

[2] Ao propor essa conceituação, o autor deixou claro que o fez baseado em Sun-tzu.

Ainda segundo Rattray (2001), ataques digitais não violentos, para atingir objetivos políticos, devem ser entendidos como uma nova forma de guerra, na qual sua condução é feita com o menor gasto possível de vidas humanas e recursos econômicos, buscando subjugar o inimigo sem luta.

O uso de ataques digitais deve ser entendido como uma nova forma de guerra que utiliza o conceito de microforça. Neste conceito, aparatos bélicos de tamanho relativamente pequeno geram efeitos devastadores de paralisia e neutralização de Centros de Gravidade do inimigo, sem a destruição causada por armas como as químicas e as nucleares, por exemplo, (BOBBITT, 2003).

Assim:

> O Próximo passo é maximizar o uso de sua própria informação sobre alvos, limitar a capacidade do inimigo de desenvolver informações a respeito da força atacante e minimizar o esforço físico gasto, essa poderá ser a forma de travar a guerra cibernética como uma microaplicação de força. (RATTRAY, 2001, p. 22, tradução nossa).

Os ataques digitais adquirem essa característica menos violenta, sem perder a eficácia, principalmente, devido às diferenças do ambiente cibernético para outros ambientes de Guerra, conforme a definição a seguir (RATTRAY, 2001):

a) os demais meios podem modelar o ambiente, porém não o criam. O ambiente cibernético é criado pelo homem. Assim o ambiente cibernético é muito mais mutável;
b) a Guerra Cibernética pode ser mais difícil de detectar; e
c) exige cooperação civil-governamental.

Um grande exemplo de governo que forçou sua vontade contra adversários, sem derramamento de sangue, no domínio cibernético, segundo Carr (2009), foi a situação que o referido autor chamou de primeira guerra da rede mundial (*World Wide Web*), no qual China e Estados Unidos da América (EUA) travaram combates com cerca de 80.000 *hackers* chineses engendrando ataques aos EUA entre 1999 e 2001.

Note-se que a partir de então, “grande parte do foco da Republica Popular da China tem sido a espionagem cibernética de acordo com a sua estratégia militar de mitigar a superioridade tecnológica militar dos EUA.” (CARR, 2009, p. 2, tradução nossa).

Verifica-se o aparecimento de outro fator de fundamental diferença entre a Guerra Cibernética e a Guerra Cinética – a participação dos elementos não

estatais. Estes elementos ganharam importância destacada, pois nos dias atuais “Grupos, Organizações, Estados-Nação e até indivíduos podem influenciar a política, em um nível sistêmico, utilizando a informação” (ARMISTEAD, 2004, p. 13, tradução nossa).

Assim, a Guerra Cibernética não é travada apenas entre exércitos e estados, a cada dia, mais elementos não estatais têm se tornado autores de atividades ligadas a esta modalidade de guerra. Essa situação, segundo Armistead (2004), vem ocorrendo desde o fim da Guerra Fria, período no qual as Nações-Estado estão perdendo poder em detrimento de corporações de abrangência mundial com poder por vezes maior que o de nações.

Alguns pontos-chave dessa nova era, que indicam o fortalecimento desse componente não estatal no ambiente da guerra, mais especificamente a cibernética, foram listados por Armistead (2004) conforme a seguir:

a) comunicação geral e aberta com grande ênfase na velocidade;
b) censura branda ou inexistente, o indivíduo controla seu fluxo de informações;
c) confiança e qualidade emergirão, mas não inicialmente; e
d) enfraquecimento das Nações-Estado e fortalecimento das redes.

O fortalecimento dos elementos não estatais, não só ampliou o leque de ameaças, como também colaborou para o surgimento de uma nova classe de soldados - o guerreiro digital. Esse novo personagem, segundo Liang e Xiangsui (1999), está assumindo o papel de um modelo de soldado que nunca tinha sido questionado por milhares de anos - o guerreiro forjado em aço e sangue.

> O incessante crescimento da tecnologia cibernética exige um significativo esforço de readaptação, numa escala grandiosa, de militares que foram criados e formados dentro de uma concepção da guerra mecanizada. É precisamente por este motivo que algumas nações com visão prospectiva, ao invés de única e simplesmente priorizarem os cortes de efetivos, estão enfatizando: a elevação da qualificação técnica do seu pessoal; o incremento do nível de tecnologia avançada e semiavançada incorporada ao seu armamento; e a atualização do pensamento militar e doutrinário. (LIANG; XIANGSUI, 1999, p. 49).

A política de arregimentação desses novos guerreiros digitais tem variado de país para país, de acordo com as especificidades de cada um.

A Rússia baseia-se na mobilização de sua “população altamente preparada de *Hackers* patrióticos que são mais que desejosos em lutar por seu país pelo domínio do Ciberespaço.” (CARR, 2009, p. 35)

Segundo Liang e Xiangsui (1999), a China tem priorizado a formação de seus quadros militares, o que tem refletido numa significativa redução de números absolutos do efetivo militar, devido à gradual substituição de soldados tradicionais por soldados da era digital. É bom salientar, ainda, que por diversas ocasiões os chineses lançaram mão de seus *Hackers* nacionais.

Uma forma diferente de convocar soldados cibernéticos foi citada por Carr (2009), que disse haver fortes indícios de que Mianmar, em uma determinada situação, chegou a terceirizar ataques cibernéticos, o que seria um indício do aparecimento de uma nova classe de mercenários cibernéticos.

> A era dos “fortes e valentes soldados defensores da nação” já está ultrapassada. Num mundo em que até mesmo a guerra nuclear talvez se torne um jargão militar obsoleto é bem provável que um jovem pálido e franzino, usando um par de óculos de grau, esteja mais bem preparado para ser um soldado moderno do que um jovem forte e musculoso. A maior evidência dessa assertiva, talvez seja o relato de uma ocorrência que circula nos meios militares ocidentais. Como parte de um exercício de segurança, um tenente da Força Aérea dos EUA, utilizando um computador doméstico ligado à *Internet* através de uma linha discada comum, conseguiu penetrar na rede de computadores do Comando Combinado do Atlântico, colocando uma divisão naval inteira de joelhos. (LIANG; XIANGSUI, 1999, p. 50).

Assim, apesar de diferenças na condução da guerra cibernética em relação a outras formas tradicionais, verifica-se que aquela permanece mantendo a eficácia necessária, porém com possibilidades elevadas de aumentar os seus índices de eficiência. O que obriga a toda força armada, do mundo moderno, adequar-se a esse novo conceito, para não ser sobrepujada por outra força que o tenha feito.

Para a Força Aérea Brasileira, o domínio do ambiente cibernético mostra-se como uma necessidade, não só pela possibilidade que o mesmo traz em termos de multiplicação de forças, mas também pelo aparecimento de novas ameaças, estatais ou não, que podem afetar o cumprimento de sua missão.

Com o conhecimento da conceituação de Guerra Cibernética, em um campo teórico, mostra-se necessário o estudo de como essa nova forma de guerrear poderá ser efetivamente realizada. Portanto, o próximo passo será a apresentação de métodos e técnicas comumente utilizadas no processo de condução da Guerra Cibernética.

2.3 MÉTODOS E TÉCNICAS DE GUERRA CIBERNÉTICA

Até o presente momento, este trabalho tratou da Guerra cibernética em termos conceituais, porém para que se possa corroborar a afirmativa apresentada por Rattray (2001) de que o uso da tecnologia da informação para aprimorar formas de guerrear foi integrado ao pensamento militar, deve-se verificar como tais ações poderão ser realizadas com a utilização de diversas técnicas e métodos.

A guerra cibernética não é uma solução universal a ser utilizada aleatoriamente. Como todo tipo de guerra, deve ser objeto de estudos que indiquem a sua aceitabilidade, praticabilidade e adequabilidade. Rattray (2001, p. 142, tradução nossa) cita que “adversários considerando usar Guerra Cibernética para atingir centros de gravidade devem determinar como preparar, implementar e terminar os conflitos da melhor maneira para alcançar seus fins políticos.” Nesse caso, ainda de acordo com o autor citado neste parágrafo, para implementar a Guerra Cibernética, os seguintes fatores devem ser observados:

a) atacantes devem utilizar extensiva inteligência sobre a dependência de seus adversários em relação à infraestrutura de informação, incluindo suas vulnerabilidades;

b) atacantes devem desenvolver ferramentas e técnicas específicas para aumentar as vulnerabilidades da infraestrutura de informação dos alvos;

c) ataques digitais podem ocorrer sozinhos, em conjunto com meios convencionais ou junto à utilização de armas de destruição em massa;

d) um maior período para preparo de um ataque pode, potencialmente, criar uma maior vantagem em termos de precisão, surpresa e sincronização; e

e) na falta de meios adequados para prover ataques precisos, os atacantes podem ser forçados a utilizar ferramentas e técnicas, como a infiltração de *softwares* maliciosos, que executem um ataque de negação de serviço para causar disrupção colateral expressiva de sistemas que não eram alvos de ataques intencionais. Nesse caso, atenção especial deve ser dada ao fato de tal ataque poder vir a se tornar impossível de parar.

> Para serem efetivos, os atacantes devem ganhar entendimento da informação disponível limitando a visibilidade de seus esforços de inteligência, a fim de não despertar ações defensivas. Defensores devem controlar informações acerca de suas vulnerabilidades e suas ações enquanto dissemina tal informação para habilitar ações de proteção. (RATTRAY, 2001, p. 136, tradução nossa).

Verifica-se que o estudo da Guerra Cibernética é, intensamente, voltado às ações ofensivas, isso ocorre, pois “a ofensiva define a defesa – eixo da segurança no ciberespaço, assim a defesa sempre olha para o passado.” (CARR, 2009, p. 39, tradução nossa).

Nas guerras estratégicas passadas, segundo Rattray (2001), os defensores tinham ligeira vantagem em relação aos atacantes, pois, ao saberem de suas fraquezas, poderiam se proteger melhor, exigindo um grande trabalho de inteligência dos atacantes, o que não ocorre com o advento da Guerra Cibernética.

Essa modificação na relação entre defesa e ataque ocorreu, pois “a guerra cibernética é revolucionária porque não tem linha de batalha, a inteligência é intangível e os ataques vêm sem avisos não deixando tempo para preparar defesas.” (UDA, 2009, p. 100, tradução nossa).

Segundo Rattray (2001), os ataques digitais procuram expor informações, corromper informações, roubar serviços ou negar serviços. Assim um ambiente de defesa deve propiciar integridade, autenticidade, antinegação, confidencialidade e disponibilidade.

Embora pareça claro o que se necessita para compor uma defesa cibernética adequada, tal ação tem se mostrado complexa a começar pela dimensão de tal aparato uma vez que “a mensuração de ataques cibernéticos ainda é difícil, pela falta de experiência histórica ou métricas de análise.” (RATTRAY, 2001, p. 120, tradução nossa).

> As ferramentas tecnológicas para defender infraestruturas de informação têm se mostrado de reduzida capacidade para, de qualquer forma, prevenir proativamente ataques digitais baseados em invasões de rede. O tempo requerido pelos defensores para determinar se a disrupção a um determinado sistema de informações ou rede foi resultante de um ataque malicioso, impede severamente a defesa ativa. A maioria das ferramentas defensivas existentes detecta atividades digitais suspeitas baseadas em métodos de reconhecimento calçados em ataques digitais previamente catalogados. (RATTRAY, 2001, p. 129, tradução nossa).

A defesa citada anteriormente é baseada em um modelo tradicional que, segundo Rattray (2001), segue os seguintes passos:

a) estabelecer defensor;
b) controlar acesso;
c) monitorar;
d) responder;
e) mitigar efeitos; e

f) prevenir futuros acessos.

Tal modelo apresenta a deficiência de estar sempre atuando reativamente, portanto sempre atrasado em relação a ataques inéditos, ainda mais se for considerada a filosofia básica dos principais atores na condução da guerra cibernética, hoje conhecidos como *Hackers*:

> Os *hackers* procuram a falha do dia zero, que consiste em achar uma vulnerabilidade, em *software*, que ainda não foi descoberta, mantendo dessa forma a defesa sempre atrasada em relação ao ataque. (CARR, 2009, p. 40, tradução nossa).

Para Carr (2009), o custo de ataque na Guerra Cibernética é muito baixo, exigindo recursos computacionais reduzidos e disponíveis em abundância, ao contrário da defesa que se torna cara, dispersa, irregular, inconsistente e de difícil coordenação. Assim ele propõe um modelo diferente a ser seguido para o estabelecimento da defesa que foi denominado pelo mesmo de *Cyber Early Warning Model,* traduzindo-se para Modelo de Alerta Cibernético Antecipado (MACA), o qual prioriza a prevenção em detrimento da reação.

Tal modelo baseia-se nas seguintes fases:

a) tensão latente – é identificado um estado de tensão entre dois ou mais atores que podem levar a conflitos entre os mesmos;
b) reconhecimento cibernético – é iniciado um profundo estudo das força, fraquezas e possibilidades relativas ao ambiente cibernético envolvendo os atores em questão;
c) evento iniciador – é atingido determinado ponto a partir do qual os ataques são iniciados ou a partir de quando uma ação é obrigatória;
d) mobilização cibernética – as forças necessárias são reunidas de forma a alcançar uma massa decisiva contra pontos decisivos; e
e) ataque cibernético – os ataques são realizados.

Uma aplicação prática desse modelo pôde ser observada no caso do conflito entre Rússia e Geórgia, em especial em 2008 que, segundo Carr (2009), ocorreram conforme o descrito a seguir.

Existiam tensões políticas entre a Rússia e a Geórgia mesmo antes da queda da União Soviética. No final dos anos 80, líderes oposicionistas georgianos pressionaram pela sua independência da União Soviética. Em 1989, nacionalistas da Abcásia – província autônoma da Geórgia no mar negro – fizeram demandas pela criação de uma república Soviética separada. Essa demanda gerou conflitos

entre georgianos étnicos, vivendo na Abcásia, e nacionalistas abcasianos suportados pela União Soviética.

Depois da queda soviética, as tensões na Abcásia continuaram a aumentar. Em 1992, nacionalistas abcasianos continuaram a pressionar pela independência e militantes atacaram prédios governamentais em Sukhumi – sua capital. Em resposta, a polícia da Geórgia e unidades da Guarda Nacional foram enviadas para reaver o controle. As tensões entre Geórgia e Rússia sobre a Abcásia continuam até os dias atuais e são enormemente responsáveis pela deflagração dos conflitos na Ossétia do Sul em 2008.

A deflagração do conflito na Ossétia do Sul, em 2008, foi acompanhada de ataques cibernéticos paralelos a *sites* da *web* do governo da Geórgia (Figura 1). *Hackers* pró-rússia promoveram ataques a *sites* da Geórgia e coordenaram suas ações através de uma rede de *sites* de *hackers* frequentados por criminosos cibernéticos e *hackers* russos. Adicionalmente, *hackers*, supostamente pró-russos, lançaram o StopGeorgia.ru, um *site* dedicado a recrutar *hackers* simpatizantes para a milícia cibernética russa. O StopGeorgia.ru proveu estes simpatizantes com uma lista de *sites* da *web* georgianos a serem atacados, bem como instruções de como lançar diversos tipos de ataques cibernéticos. *Sites* da Geórgia foram desfigurados com propaganda antigeorgiana ou foram colocados fora do ar com ataques do tipo *Distributed Denial of Service* (DDoS).

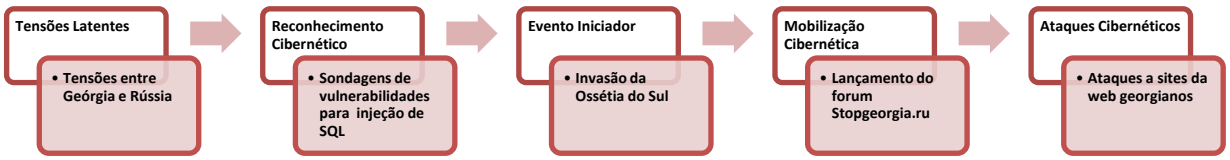

Figura 1: Estágios dos ataques cibernéticos a *sites* da *web* georgianos.
Fonte: Carr (2009, p. 183, tradução nossa).

Segundo Carr (2009), a sofisticação dos ataques realizados em eventos de guerra cibernética é altamente dependente da habilidade do atacante e da quantidade do reconhecimento realizado. A quantidade de técnicas, métodos e ferramentas disponíveis para tais fins é ainda desconhecida e a complexidade

aumenta exponencialmente com a possibilidade de agrupamento entre esses diversos recursos, de acordo com a ocasião apresentada.

O conhecimento desses recursos é fundamental para a realização de ações ofensivas, bem como para a implementação de atividades de caráter defensivo.

Feito o estudo acerca de como a Guerra Cibernética pode ser implantada, mostra-se necessário verificar o contexto teórico estratégico no qual a Guerra Cibernética está incluída, habilitando-a como uma nova forma de guerra.

3 A GUERRA CIBERNÉTICA NA GUERRA MODERNA

Hanson (2002) defende que o Ocidente[3] obteve, ao longo de sua história, uma supremacia nos campos de Batalha, e embora tenham ocorrido diversos reveses, devido a diversos fatores, na Grande maioria das Guerras entre o Oriente e o Ocidente, no final, este venceu utilizando batalhas baseadas nas colisões de massa em batalhas decisivas.

Diferenciando a forma ocidental de lutar, da oriental, Hanson (2002) cita que esta estava baseada essencialmente na busca da manobra e da dissimulação, essência dos estratagemas, evitando o choque frontal e decisivo, base da luta à maneira ocidental, que não deixou de incorporar em sua estrutura, embora não de forma prioritária, a busca da manobra e da dissimulação.

Em diversos confrontos entre exércitos equipados com armas de equivalente desempenho, como no caso da Guerra das Malvinas entre Argentina e Inglaterra, segundo Hanson (2002), o lado que obteve a vitória, mesmo tendo inferioridade numérica, o fez por ter uma "abordagem cultural comum da guerra – uma tradição holística que transcendia morteiros e jatos, e uma tradição muito diferente da de seus respectivos, e algumas vezes corajosos, adversários." (HANSON, 2002, p. 634).

Basil H. Liddell Hart publicou, sete anos após a Segunda Guerra Mundial, o livro ***Paris; Or the Future of War***, no qual, segundo Fadok (1995), ele recorda a derrota mítica de Aquiles por seu oponente Paris por meio de um ataque de precisão cirúrgica com uma flecha bem dirigida.

> Atacar as vulnerabilidades do inimigo (em vez de seus pontos fortes) poderia e deveria servir como modelo de conduta na guerra, nos anos que viriam. Os campos de morte da Primeira Guerra Mundial teriam feito certamente preferível uma estratégia de paz; as tecnologias de voo e a mecanização pareciam torná-la possível, também. Assim, começou a busca por essas vulnerabilidades fundamentais da nação inimiga, que fossem cruciais à sua sobrevivência e que estivessem protegidas pelo escudo e espada de suas forças armadas. Ao longo desse caminho, os teóricos do poder aéreo reintroduziram a ideia de paralisia no dicionário da estratégia militar. (FADOK, 1995).

Os pioneiros do poder aéreo, segundo Fadok (1995), enfatizavam a "terceira dimensão" que a arma aérea acrescentava ao campo de batalha. A capacidade do avião de erguer-se sobre o desgaste da batalha de superfície levou

[3] Neste caso, refere-se a EUA e Europa.

muitas pessoas a especularem que o poder aéreo poderia derrotar uma nação inimiga e suas forças armadas, incapacitando ou paralisando o potencial de fazer a guerra. Infligir a paralisia, por meio do ataque aéreo, ao calcanhar de Aquiles da nação inimiga parecia prometer a vitória decisiva a um custo significativamente inferior, em termos de vida e de dinheiro.

Percebe-se então, uma evolução do conceito de guerra partindo das grandes colisões de massa para uma guerra menos violenta baseada em ataques precisos que podem derrotar o inimigo com um maior grau de eficiência. Não, necessariamente, destruindo-o, mas causando-lhe a paralisia.

Conceituando a paralisia estratégica, Fuller (1926) apresenta a ideia da ordem tríplice como “um fundamento tão universal que pode ser considerado axiomático para o conhecimento em todas as suas formas” (FULLER, 1926, tradução nossa).

Os seres humanos, para Fuller (1926), são constituídos de corpo, mente e alma, portanto as guerras, que são atividades humanas, devem estar sujeitas a uma constituição similar. Assumindo como base de seu estudo a ordem tríplice, Fuller (1926) demanda três esferas da guerra: física, mental e moral. Essas esferas tratam, respectivamente:

a) da destruição da força física do inimigo (poder de combate);
b) desorganização de seus processos mentais (poder de pensamento); e
c) desintegração de sua vontade moral de resistir (poder de resistência).

Fuller (1926) acrescenta que as forças que operam nessas esferas fazem isso de maneira sinérgica, não isolada: “o que certamente ganha a guerra é a combinação suprema dessas três forças agindo como uma força única.” (FULLER, 1926, tradução nossa).

Esta ordem tríplice, segundo Fadok (1995), revela-se útil para começar a compreender a essência da paralisia estratégica. Para ele, a paralisia do adversário consiste em dimensões físicas, mentais e morais e como estratégia, acarreta o intento não letal de incapacitar fisicamente e desorientar mentalmente o inimigo de modo a induzir seu colapso moral.

Embora a intenção não letal, segundo Fadok (1995), não elimine a ação destrutiva ou impeça que haja resultados fatais, ela atua, sempre que possível, para mitigar esses resultados negativos. Esses efeitos físicos, de acordo com a estratégia geral, podem ser de curto ou longo prazo.

Segundo Fuller (1926), os valores dos princípios de guerra eram objeto de grandes debates e muitas autoridades estabeleceram que a guerra não tinha princípios, porém , indo de encontro a Clausewitz (2010), Fuller definiu o seguinte:

> O valor dos princípios reside em seu poder para eliminar o próprio individuo quando decisões têm de ser tomadas, e assim nos ajuda a manter o equilíbrio que só é possível quando a mente está sintonizada com a lei da economia de forças. (FULLER, 1926, tradução nossa).

Segundo Fadok (1995), a contribuição da lei da economia de forças para a definição de paralisia estratégica é a ideia de despender esforço mínimo para produzir efeito máximo – “algo que Paris fez muito bem contra o pesadelo que Aquiles era para ele.” (FADOK, 1995).

Assim pode-se definir paralisia estratégica como:

> Uma opção militar com dimensões físicas mentais e morais que tem a intenção de incapacitar, em vez de destruir o inimigo. Ela busca o efeito político máximo ou benefício político máximo possível com o mínimo custo ou esforço militar necessário. Além disso, tem por objetivo uma decisão rápida por meio de uma batalha de manobra dirigida contra a capacidade física ou mental que tem o adversário de manter ou controlar seu esforço de guerra, para diminuir sua vontade moral de resistir. (FADOK, 1995).

Para Fuller (1926), a força de um exército está em sua organização controlada por seu cérebro, portanto para derrotar esse exército é necessário paralisar seu cérebro. Portanto o meio mais eficaz e eficiente para derrotar o inimigo, com economia de força militar, seria o efeito instantâneo de um tiro na cabeça ao invés de um lento sangramento causado por ferimentos sucessivos, mas leves, no corpo.

O conceito de paralisia tomou mais força ainda com o surgimento da Arma Aérea devido a suas características intrínsecas, como velocidade, manobrabilidade e capacidade de penetração, características estas ainda mais presentes no ambiente cibernético.

Aliada a estas características, nota-se que com a inclusão da tecnologia da informação, de forma geral, na sociedade moderna, foi evidenciada uma nova forma de levar a paralisia ao inimigo, elegendo a Guerra Cibernética como um grande campo para a aplicação deste conceito.

A noção da paralisia ficou impregnada na doutrina militar britânica e americana, refletindo nos pensamento de estrategistas atuais, dentre eles John Boyd.

John Boyd, segundo Osinga (2007), foi um piloto, americano que criou dentre outras, a teoria das Manobras Transientes que, baseada em sua experiência como piloto de caça na Guerra da Coréia, defendia que rápidas mudanças de direção tornariam a resposta inimiga inadequada à nova situação.

Boyd defende uma guerra psicológica e temporal, ao contrário de uma guerra física e espacial. Seu objetivo militar é “quebrar a vontade e o espírito do comando inimigo, criando situações operacionais e estratégicas surpreendentes e perigosas” (LIND, 1979, tradução nossa).

Para criar as situações citadas no parágrafo anterior, segundo Fadok (1995), precisa-se operar com um andamento ou ritmo mais rápido que o do adversário. Dito de maneira diferente, a guerra de manobra de Boyd tem por objetivo deixar o inimigo impotente, negando-lhe tempo para colocar-se mentalmente à altura das circunstâncias da guerra, que se desenvolvem rapidamente e, naturalmente, são incertas.

Segundo Osinga (2007), Boyd, de acordo com sua análise da história militar antiga e moderna, identificou quatro qualidades basilares para o êxito:

a) iniciativa;
b) harmonia;
c) variedade; e
d) rapidez.

Em conjunto, segundo Osinga (2007), essas características permitem que a pessoa se adapte ao ambiente incerto e cheio de atritos da guerra, e dê forma a esse ambiente.

Boyd, de acordo com Fadok (1995), confere a Clausewitz o crédito de reconhecer a necessidade de melhorar a própria adaptabilidade na guerra, diminuindo os próprios atritos. Além disto, tomando emprestado de Sun Tzu, Boyd insiste em que a pessoa pode usar o atrito para configurar o conflito a seu favor, criando e explorando os atritos que o oponente enfrenta. Então, ele relaciona esta ideia de minimizar o atrito entre as forças amigas e maximizar o atrito inimigo com suas qualidades fundamentais de iniciativa, harmonia, variedade e rapidez.

> Para maximizar o atrito do inimigo, deve-se planejar atacar com uma multiplicidade de ações que se possam executar com a maior rapidez. De maneira semelhante à ideia contemporânea de guerra em paralelo, esta combinação letal de ações rápidas e múltiplas serve para sobrecarregar a capacidade do adversário de identificar e tratar adequadamente estes acontecimentos, que parecem extremamente ameaçadores. Reduzindo de

> maneira constante a capacidade de resistir do oponente, física e mental, também se termina por esmagar sua capacidade moral de resistir. (FADOK, 1995)

Para Boyd, segundo Fadok (1995), ocorre uma grande perturbação quando se leva ao inimigo, rápida e repetidamente, uma combinação de acontecimentos ambíguos (mas ameaçadores) e enganadores (mas não ameaçadores). Esses diversos acontecimentos, comprimidos no tempo, geram rapidamente anomalias entre as ações que o oponente acredita ameaçarem sua sobrevivência e aquelas que realmente o fazem. O inimigo precisa eliminar esses desencontros entre a percepção e a realidade, se pretende que suas reações permaneçam relevantes ou em outras palavras, se ele pretende sobreviver.

Boyd defende uma conduta inversa a de Clausewitz, segundo Fadok (2009), de destruir os centros de todo o poder e movimento, atacando as conexões morais-mentais-físicas que unem centros de gravidade não cooperativos “destruindo a harmonia interna do inimigo e as suas conexões com o mundo real, produzindo paralisia e fazendo com que as resistências entrem em colapso” (FADOK, 1995).

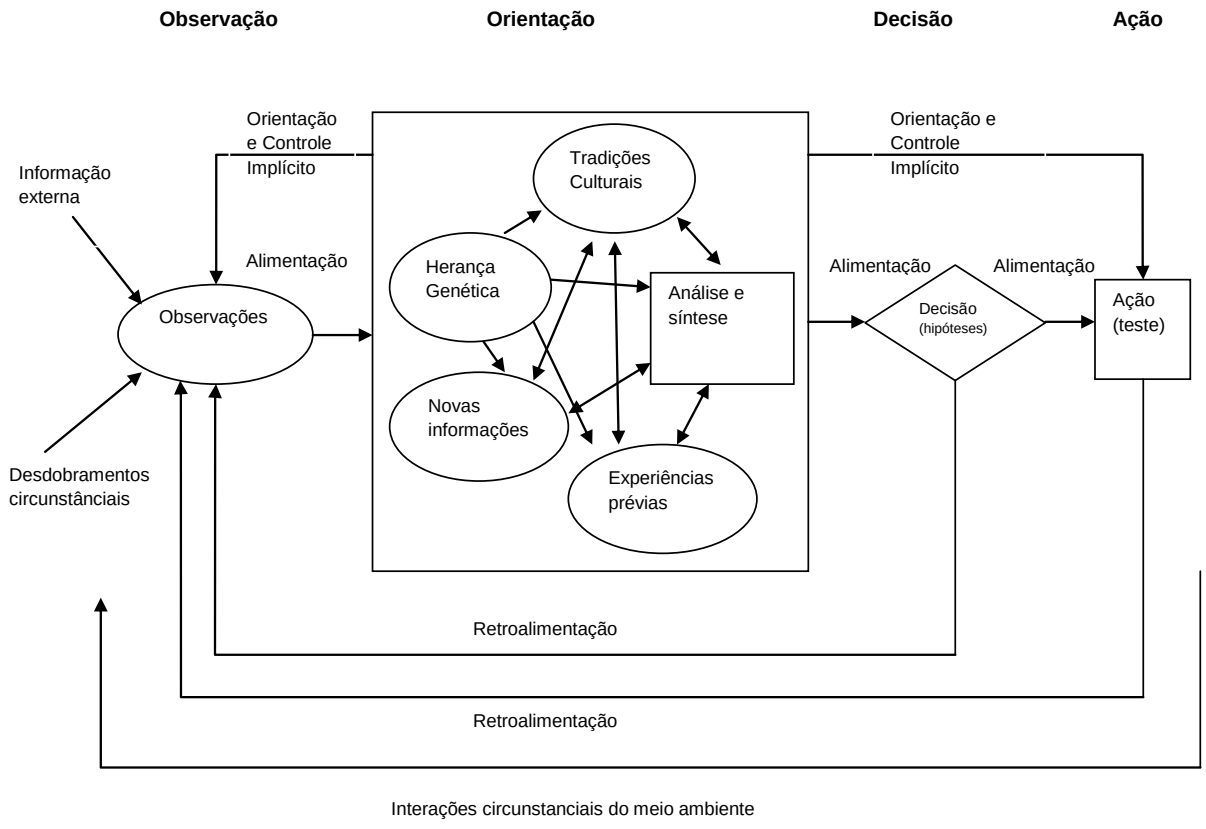

Figura 2: Ciclo OODA real.
Fonte: Osinga (2007, p. 231, tradução nossa).

Boyd, segundo Osinga (2007), é associado ao ciclo OODA (Figura **2**), apresentado no trabalho de Boyd denominado: ***A Discourse on Winning and Losing***. Geralmente o ciclo OODA é entendido como observação, orientação, decisão e ação, e é equivalente a um ciclo de decisão no qual, de forma genérica, é sugestionado que o sucesso da guerra depende da habilidade de executar o ciclo OODA mais rapidamente que o inimigo.

A tecnologia da informação, nesse sentido, e conforme características apresentadas no decorrer deste trabalho, apresentou-se como uma grande ferramenta de apoio a execução desse processo de exame do mundo real, por possibilitar a manipulação de grande volume de dados de forma sistematizada, possibilitando a execução do ciclo OODA em maior velocidade.

Segundo Fadok (1995), Boyd propõe que o êxito no conflito surge de infiltrar-se no ciclo OODA do adversário e ali permanecer. O comandante militar pode fazer isso de duas maneiras suplementares.

Primeiro, ele precisa minimizar seu próprio atrito por meio da iniciativa e da harmonia de resposta. Esta diminuição do atrito de seu lado age de modo a diminuir seu próprio ciclo (isto é, a fazer com que seu próprio ciclo de decisão-ação se torne mais veloz).

Segundo, ele precisa maximizar o atrito de seu oponente por meio da variedade e da rapidez das respostas. Este aumento no atrito inimigo age de maneira a aumentar o ciclo do adversário (isto é, tornar mais lento o ciclo de decisão-ação dele).

Em conjunto, essas manipulações do atrito garantem uma operação contínua dentro do ciclo OODA inimigo, de maneiras ameaçadoras e imprevisíveis. Inicialmente, isto produz confusão e desordem no campo inimigo. Afinal, produz pânico e temor que se manifestam simultaneamente na paralisia da capacidade de enfrentar e na disposição para resistir.

Traduzindo ao campo militar, o ciclo OODA está intimamente ligado ao processo de comando e controle de uma força armada, e conforme apresentado por (COIMBRA, 2009), atingir este processo é uma forma de levar a derrota ao inimigo, por privá-lo de suas capacidades de direção, ou seja, leva-se o inimigo à paralisia.

Assim, da mesma forma que a Tecnologia da Informação apresenta-se como uma ferramenta que possibilita a execução do ciclo OODA de forma mais rápida, apresenta-se também como uma ferramenta para interferir no ciclo

adversário e, acima de tudo, como uma vulnerabilidade ainda mais presente com a interligação dos recursos de informática em rede.

Fica, dessa forma, evidenciada a importância do domínio da Guerra Cibernética por parte de uma Força Armada que deseje realizar suas atividades de Comando e Controle de forma vantajosa em relação a seus adversários.

Complementando as ideias de Boyd surge outro teórico moderno bastante influente no campo militar, John Warden, que desenvolveu o conceito de Guerra Estratégica como sendo o esforço para derrotar o inimigo através de ataques aos centros de gravidade, sem necessariamente necessitar atacar suas forças militares em campo (WARDEN, 1995).

Warden (1995) cita que não se pode pensar estrategicamente se o processo iniciar-se com aeronaves, surtidas ou armas individualmente, ou mesmo com toda a força militar inimiga. Ao invés disto, deve-se focar na totalidade do inimigo, depois em nossos objetivos e, então, no que deve ser feito ao inimigo antes que nossos objetivos se tornem os dele.

Os estrategistas e planejadores operacionais, conforme Warden (1995), devem se livrar do conceito que o objetivo central da guerra é colidir com as forças militares inimigas. Na guerra estratégica, “a colisão pode acontecer, mas não é sempre necessária, deve, normalmente, ser evitada, e é quase sempre o meio para um fim e não o fim por si só” (WARDEN, 1995, tradução nossa). (WARDEN, 1995)

> Finalmente, como estrategistas do século XXI, nós devemos desmistificar a guerra em uma extensão considerável. Napoleão e Clausewitz estavam certos quando eles falaram sobre fricção, névoa e moral. Eles estavam certos, no entanto, em um tempo que comunicações eram quase inexistentes, armas tinham pouco mais alcance e precisão do que aquelas das Legiões Romanas, a maioria dos movimentos era feita à velocidade do passo de uma caminhada, batalhas eram vencidas ou perdidas dependendo do resultado de dezenas de milhares de encontros, quase pessoais, entre soldados que podiam ver um ao outro quando atiravam e a guerra era largamente confinada à colisão de homens e navios em ponto limitado do tempo e espaço. (WARDEN, 1995, tradução nossa).

Nessas circunstâncias, de acordo com Warden (1995), a moral estava para o físico em uma relação de 3 para 1. De forma diferente, nos dias atuais, os combatentes tornaram-se gerenciadores de grandes equipamentos como tanques, aeronaves, peças de artilharia e navios, tornando-se dependentes destes.

Como efeito dessa dependência, segundo Warden (1995), ocorre que sem esses mecanismos, a capacidade de afetar o inimigo aproxima-se de zero.

Warden, não quer dizer com isso que o físico esta para o moral na razão de 3 para 1, mas afirma que pelo menos em igualdade de condições parece provável.

O advento do poder aéreo e das armas de precisão, segundo Warden (1995), tornaram possível destruir o lado físico do inimigo sem, contudo, causar o desparecimento da moral, da névoa e da fricção, o que permite pensar em guerra, de uma forma genérica, como a forma de uma equação na qual: físico x moral = êxito.

Nos dias atuais, segundo Warden (1995), as entidades estratégicas, seja uma indústria estatal, seja uma organização guerrilheira, estão altamente dependentes dos meios físicos, fazendo com que a equação penda para o lado físico. Neste, mesmo com altíssimos níveis de moral, a falta de recursos físicos impossibilitará o êxito.

Segundo Warden (1995), os objetivos são a chave para o sucesso, e os mesmos devem ser definidos muito além de espancar o inimigo ou derrotar suas forças militares, pois no final de tudo é necessário lembrar que se vai à guerra não para ter uma boa luta, mas sim para obter algo de valor político para a organização[4].

No nível estratégico, Warden (1995), define que:

> ...nós obtemos nossos objetivos causando determinadas mudanças em uma ou mais partes do sistema físico inimigo fazendo com que o mesmo decida adotar nossos objetivos, ou nós tornamos fisicamente impossível para ele se opor a nós. O último nós chamamos paralisia estratégica. (WARDEN, 1995, tradução nossa).

A Guerra Estratégica, seguindo Warden (1995), é uma guerra para fazer com que o inimigo faça o que você quer que ele faça. Levada ao extremo ela pode até ser uma guerra para destruir o inimigo, porém o sistema como um todo é que é o alvo. Esse sistema é composto pelos elementos do Modelo dos Cinco Anéis (Figura 3) que são, em ordem de prioridade, os seguintes:

a) liderança;
b) elementos orgânicos essenciais;
c) infraestrutura;
d) população; e
e) forças desdobradas.

---

[4] Warden (1995) reitera que esse é objetivo estratégico, e que embora possa ser usada atitude semelhante para os níveis táticos, estes, ainda, têm como objetivo principal enfrentar o inimigo.

Se o sistema for devidamente identificado, segundo Warden (1995), será percebido que as força militares serão apenas um apêndice sem utilidade se não forem suportadas por sua liderança, elementos orgânicos essenciais, infraestrutura ou população. Nesse sentido, não é dito que as forças militares não devem ser atacadas, existem momentos em que elas deverão ser alvos, pois fazem parte do sistema. A grande observação é que os planejadores devem iniciar o seu trabalho pelo todo, para então de forma dedutiva chegar aos pequenos detalhes na identificação dos Centros de Gravidade.

Figura 3: Modelo dos Cinco Anéis.
Fonte: Warden (1995).

Descrevendo como usar o modelo dos cinco anéis, Warden (1995) cita que o conceito de Centro de Gravidade é simples conceitualmente, porém de difícil execução, pois existirão mais de um e cada um deles tem um efeito diferente sobre os demais. Em alguns casos, é importante notar, que ocasionalmente os centros de gravidade estarão apenas indiretamente relacionados com a capacidade inimiga de conduzir operações militares.

Todo estado e toda organização militar tem um conjunto único de centros de gravidade ou vulnerabilidades, e o modelo dos cinco anéis é um bom ponto de partida na sua identificação. “Estes centros de gravidade, que também são anéis de vulnerabilidades, são absolutamente críticos para o funcionamento do estado.” (WARDEN, 1995, tradução nossa).

O anel mais crítico, para Warden (1995), é o da liderança, pois ele representa a estrutura de comando do inimigo. Esta estrutura, ao longo da história tem se mostrado como o ponto mais sensível, por ser ela a responsável pela coordenação de todos os esforços bem como pelo direcionamento das ações. Embora, hoje, atingir a figura do comandante tenha se tornado algo de difícil execução, as comunicações de comando tornaram-se essenciais, e estas são vulneráveis a ataques.

Assim, segundo Warden (1995), quando a estrutura de comando e controle é atingida, como aconteceu no Iraque por ocasião da Guerra do Golfo, a liderança tem grande dificuldade em dirigir a guerra, demonstrando que quando o líder não pode ser atingido diretamente, ele deve ser pressionado de forma indireta para, por fim, realizar concessões. “O comandante inimigo irá normalmente chegar a estas conclusões como um resultado do grau de destruição imposto aos anéis circundados” (WARDEN, 1995, tradução nossa).

O próximo anel mais importante, segundo Warden (1995), é o dos elementos orgânicos essenciais, que são aqueles elementos indispensáveis ao sistema. Eles não são, necessariamente, diretamente relacionados ao combate, porém a sua privação irá causar o colapso do sistema, como, por exemplo, a privação de energia e combustível em um país moderno.

A privação desses elementos essenciais poderá levar a liderança a realizar concessões, pois:

> - danos aos elementos essenciais levam ao colapso do sistema.
> - danos aos elementos essenciais tornam fisicamente difícil ou impossível manter determinada política, ou lutar.
> - danos aos elementos essenciais têm repercussões na política e economia interna que são muito caros para suportar. (WARDEN, 1995, tradução nossa)

O terceiro anel mais importante, segundo Warden (1995), é o da infraestrutura, que embora na essência e nos resultados seja semelhante ao segundo anel, difere-se deste por existirem mais instalações de infraestrutura e maior redundância, o que irá exigir mais esforços para causar danos suficientes a causar efeitos.

O quarto anel mais importante, segundo Warden (1995) é a população que, “objeções morais deixadas à parte” (WARDEN, 1995, tradução nossa), é difícil de ser atacada diretamente, e a intensidade deste ataque deve ser tremenda, para que venha a surtir efeitos.

Ataques feitos indiretamente à população, segundo Warden (1995), obtêm efeitos quando a população do país alvo possui, relativamente, pouco interesse no resultado da Guerra, como no caso do Vietnã do Norte e dos Estados Unidos na Guerra do Vietnã.

> Teóricos anteriores, como Giulio Douhet, pensaram que a guerra poderia ser vencida infringindo tal grau de perdas à população civil que a moral iria quebrar-se, causando a subsequente capitulação. Historicamente, obviamente, ele estava sobre solo sólido; cidades sitiadas, normalmente, rendiam-se, quando o sofrimento e o pânico tornavam-se demasiados para os civis sustentarem. Muitos, no entanto, argumentam que os bombardeios da Inglaterra e da Alemanha durante a Segunda Guerra Mundial, na verdade enrijeceram a moral civil. (WARDEN, 1995, tradução nossa).

O último anel, segundo Warden (1995), é o das forças militares desdobradas, pois embora exista a tendência de pensar sobre elas como o mais importante dos anéis, conceitualmente, as Força Armadas são meios para atingir determinado fim, e um de seus fins é exatamente proteger os anéis internos. Portanto o efeito da destruição das forças armadas leva a uma concessão, de última instância, decorrente do fato dos demais anéis ficarem desprotegidos. O ataque ao anel militar é o mais difícil, pois este existe, e está preparado, exatamente para a defesa e o ataque.

Na maioria dos casos, segundo Warden (1995), a totalidade dos anéis é existente, porém não é possível atingir mais do que um ou dois dos anéis externos através de meios militares, devido à limitação destes para determinados atores, para estes, que não podem utilizar armas contra os centros estratégicos do inimigo, “o único recurso disponível é o ataque indireto através de guerra não convencional ou psicológica” (WARDEN, 1995, tradução nossa).

Percebe-se que o conceito dos aneis de Warden traz a possibilidade de vencer uma guerra sem que haja necessariamente o embate físico, uma vez que, para atingir os centros de gravidades dos anéis internos, podem ser utilizadas formas altenativas à guerra cinética, como por exemplo, e cada dia mais presente, a Guerra Cibernética.

Mais uma vez, o grau de inclusão da Tecnologia da Informação nos diversos setores da sociedade, indica que é possível atingir um dos elementos dos anéis de centros de gravidade, sem a necessidade do embate físico direto, mas através dos sistemas que controlam o funcionamento destes elementos. Ou seja, pode-se levar a paralisia ao inimigo através da Guerra Cibernética.

Para Warden (1995), o requisito mais importante do ataque estratégico é o correto entendimento do sistema inimigo. Com o sistema identificado, o próximo problema é a forma de reduzi-lo a um determinado nível, ou até mesmo paralisá-lo. A menos que existam motivos para prolongar a guerra, o Ataque Paralelo é a linha de ação a ser adotada.

O ataque paralelo, de acordo com Warden (1995), sobrecarrega o inimigo, levando-o à paralisia, sendo diferente do ataque em série, que permite ao inimigo a execução de diversas ações para mitigar os efeitos do golpe sofrido.

No passado, segundo Warden (1995), a abordagem paralela não era viável devido à necessidade de concentrar forças, o que demandava muito tempo, tornando praticamente impossíveis operações simultâneas.

> Tecnologia tornou possíveis ataques simultâneos nas vulnerabilidades inimigas de todo nível estratégico e operacional. Este processo paralelo de guerra, colocado em oposição à antiga forma serial, torna-se bastante real, o que Clausewitz chamou de forma ideal de guerra, o ataque de golpes em todo lugar ao mesmo tempo. Para Clausewitz, o ideal era uma sombra platônica na parede do fundo de uma caverna, nunca para ser conhecida por mortais. A sombra materializou-se, e nada mais será o mesmo. (Warden, 1995, tradução nossa).

No ambiente cibernético o ataque paralelo encontra campo fértil para ser realizado. Uma vez que a interligação de sistemas atingiu um nível global e a velocidade do tráfego de dados é feita, praticamente, em tempo real, pode-se lançar o ataque paralelo de forma a atingir o sistema de comando e controle (Ciclo OODA) do inimigo, levando-se o mesmo à paralisia.

Se a escolha de um ataque for feita corretamente, torna-se possível atingir inimigos poderosos através de seu calcanhar de Aquiles, sem a necessidade do combate direto e frontal, porém com o objetivo da vitória.

Assim, com o desenvolvimento das teorias estratégicas de guerra, verifica-se que esta, a cada vez mais, vem sendo tratada menos em termos de força bruta e mais como aplicação de força adequada aliada à precisão direcionada a alvos devidamente selecionados. Tal evolução está intimamente ligada ao desenvolvimento do Poder Aéreo, porém nos dias atuais, o desenvolvimento tecnológico e o aumento de sua abrangência, possibilitaram o aparecimento de um novo poder: o poder cibernético.

Com o desenvolvimento da tecnologia, segundo (Fadok 1995), os ciclos OODA serão cada vez mais rápidos, e a utilização dos ataques paralelos a alvos selecionados corretamente nos Centros de Gravidade dos Cinco Anéis irá fazer com

que forças desenvolvidas levem rapidamente forças mais fracas à paralisia. Uma concretização desta assertiva foi verificada através do conceito de Guerra Centrada em Redes (GCR), o qual será tratado na sequência.

3.1 GUERRA CENTRADA EM REDES

Segundo Alberts, Garstka e Stein (1999) Guerra Centrada em Redes (GCR) diz respeito a um novo comportamento humano e organizacional, baseado na adoção de uma nova forma de pensar aplicada às operações militares - pensar centrado em redes.

A GCR, de acordo com Cebrowski e Garstka (1998), tem seu foco no poder de combate que pode ser gerado pelo elo entre a estrutura de redes com o empreendimento militar. Ela é caracterizada pela capacidade de forças dispersas geograficamente criarem uma consciência situacional de alto nível do campo de batalhas, que poderá ser explorada, via autossincronização e outras Operações Centradas em Redes (OCR) [5], para atingir o intento dos comandantes.

Segundo Alberts, Garstka e Stein (1999), GCR suporta velocidade de comando, conversão superior de informação de posição em ação, e é transparente à missão, tamanho da força e geografia. Assim sendo, GCR, tem o potencial de gerar a junção dos níveis estratégico, operacional e tático da guerra. Resumindo, GCR não é especifica sobre tecnologia, mas, sim genérica sobre uma forma emergente de resposta militar para a era da informação.

A Figura 4 mostra os elementos necessários para gerar poder de combate para o empreendimento centrado em redes. Pode-se perceber pela figura, que tudo começa com a infraestrutura, e a partir de então são habilitadas a criação do compartilhamento do conhecimento e da consciência situacional do campo de batalha. Este conhecimento e consciência são alavancados por uma nova abordagem de comando e controle e forças autossincronizadas. O resultado, representado na base da Figura 4, está no aumento do ritmo das operações, reação aprimorada, menores riscos, menores custos e melhoria da efetividade de combate.

---

[5] Operações Centradas em Rede vêm do inglês *Network-Centric Operations*.

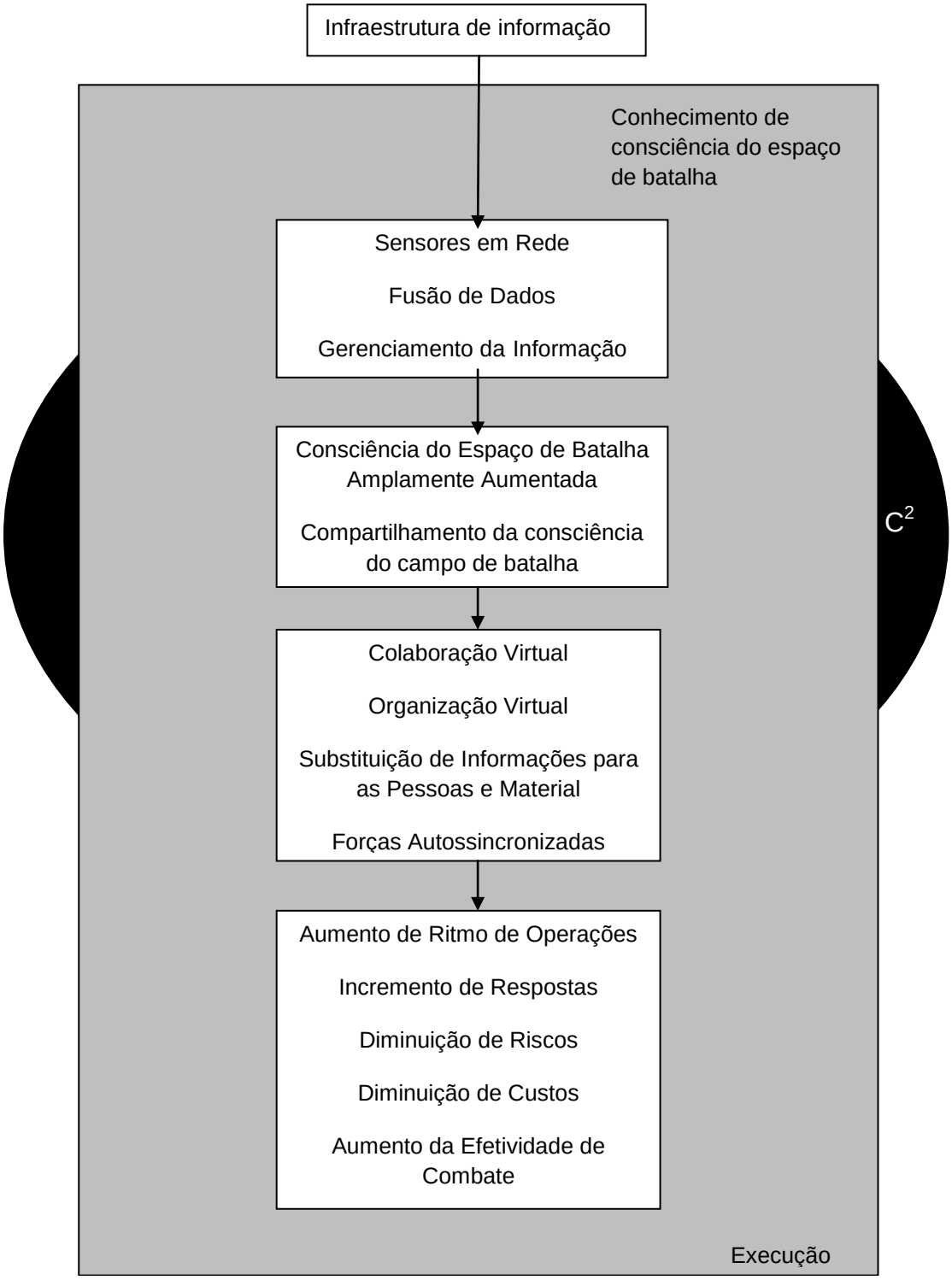

Figura 4: O Empreendimento de Guerra Centrada em Redes das Forças Armadas.
Fonte: Alberts, Garstka e Stein (1999, p. 89, tradução nossa)

Nesse sentido, em termos práticos para uma Força Aérea esse conceito de Guerra Centrada em Redes é exemplificado pela operação em pacotes de aeronaves compartilhando informações entre os diversos sensores envolvidos tanto

de aviões de caça, de ataque, de controle e alarme em voo e baseados no solo, sob a coordenação de um centro de comando e controle.

O conceito apresentado apresenta alguns pontos chaves, que segundo Alberts, Garstka e Stein (1999), são descritos a seguir.

Primeiro, o uso de forças dispersas geograficamente. No passado, devido a limitações nas capacidades de comunicação, movimentação e projeção de efeitos, as forças necessitavam ser alocadas em proximidade. Como resultado, uma força dispersa era relativamente fraca, e era incapaz de responder rapidamente a um ataque ou a montar uma ofensiva com rapidez. A tecnologia da informação possibilitou liberar as forças de combate da dependência das restrições físicas do campo de batalha, possibilitando às forças do futuro a serem mais efetivas em movimento.

Tal perspectiva, de liberação das restrições geográficas, permite a mudança de uma abordagem baseada na massa das forças pela massa dos efeitos, independente da concentração de forças prévia. Com a falta de necessidade da prévia concentração de forças ocorrem grandes vantagens para as forças em campo, como rastros menores, maior segurança e menor necessidade de transporte de desdobramentos, dentre outras.

O segundo conceito chave é o fato das forças serem inteligentes. Impulsionadas pelo conhecimento derivado da consciência situacional compartilhada do campo de batalha e de um entendimento compartilhado das intenções do comandante, essa força poderá ser capaz de se autossincronizar, operando com menores rastros para o inimigo, e sendo mais efetiva quando operando autonomamente. Tal força depende de uma alimentação constante de informações acuradas e oportunas, além de poderosas ferramentas de processamento e expertise necessária para colocar as informações do campo de batalha em contexto e transformá-las em conhecimento do espaço de batalha.

O terceiro conceito chave é que ocorre o elo efetivo entre as entidades no campo de batalha, o que significa que:

a) forças dispersas e distribuídas podem gerar sinergia; e
b) responsabilidade e trabalho podem se realocados de forma dinâmica para adaptar-se à situação.

O elo efetivo, de acordo com Alberts, Garstka e Stein (1999), requer o estabelecimento de uma infraestrutura de informações de alta performance e

robusta, para prover todo o empreendimento de combate com um serviço de informação de alta qualidade.

A GCR aumenta a sinergia entre os atores envolvidos, segundo Alberts, Garstka e Stein (1999), isto ocorre devido a sua natureza dinâmica. GCR provê os comandantes com a flexibilidade de empregar uma vasta gama de abordagens de comando, desde conceitos existentes até conceitos emergentes, com o da autossincronização. Esta flexibilidade operacional será necessária para vencer os desafios da era da informação.

Fica evidente que a GCR fornece às forças que a utilizam no campo de batalha, uma oportunidade, antes inconcebível, de consciência situacional e agilidade no processo de tomada de decisão, que possibilita a gestão do combate de forma a multiplicar o poder das forças empregadas, bem como o seu uso mais eficiente proporcionando uma maior eficácia. Portanto a GCR não pode deixar de ser levada em consideração por Forças Armadas empenhadas em tirar o máximo proveito do ambiente cibernético.

Ao analisar a Guerra Centrada em Redes, fica evidente que as teorias de paralisia, ciclo OODA, centros de gravidade e guerra paralela tornam-se cada vez mais factíveis e ganham maior evidência.

Isso ocorre, principalmente, porque na GCR ocorre um elo entre as entidades, que segundo Alberts, Garstka e Stein (1999), irá aumentar a efetividade do combate, e para verificar esse aumento de poder é necessário primeiro analisar a força de combate de uma plataforma atuando sozinha, conforme a seguir:

Conforme Alberts, Garstka e Stein (1999), para haver um engajamento com sucesso, o seguinte deve ocorrer, com certa quantidade de tempo:

a) primeiro, o alvo deve ser detectado;
b) segundo, ele precisa ser identificado;
c) terceiro, a decisão de engajar deve ser tomada;
d) quarto, a decisão deve ser transferida para uma arma; e
e) quinto, a arma de ser apontada e disparada.

Associando-se estes passos com um engajamento em particular, há um desgaste de tempo e do alcance do engajamento. O tempo exigido varia grandemente em função da mobilidade do alvo e se o mesmo usa contramedidas. O consumo do tempo depende do alcance dos sensores e armas, raio mortal do

armamento, tempo requerido para comunicar e processar informação e tempo requerido para o processo de decisão.

O combatente centrado em plataforma (que atua isoladamente), de acordo Alberts, Garstka e Stein (1999), age em um engajamento no qual a capacidade de sensoriamento e engajamento estão na mesma plataforma, e que possui apenas uma capacidade limitada de armas para serem empregadas através de informações gerada por outras plataformas. Tal modelo serve tanto para um combatente no solo, em um tanque, voando um avião ou comandando um navio.

Atuando isoladamente, o Envelope Efetivo de Emprego (E3), dessa plataforma será, normalmente menor que o do alcance das armas e dos sensores, conforme Alberts, Garstka e Stein (1999), o que está representado na Figura 5. Tal redução ocorre, principalmente, devido ao tempo gasto durante todo o processo de engajamento citado anteriormente.

Exemplos, dessa situação, são operações de combate aéreo nas quais a consciência operacional dos pilotos de caça é adquirida por meios de sua própria aeronave, isoladamente, e através de informações transmitidas de aeronaves de Controle Aéreo Avançado (CAV), via voz. Ocorre que o alcance efetivo é menor que o alcance do armamento devido diversos fatores, dentre outros, o tempo gasto para identificar se o alvo é inimigo ou amigo.

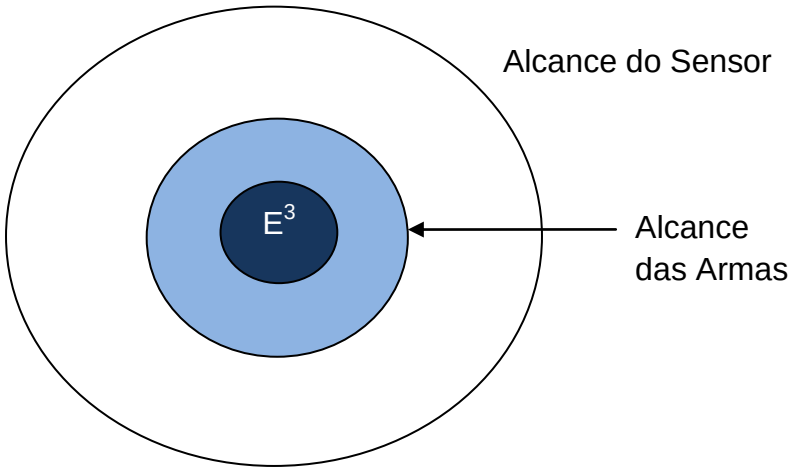

Figura 5: Envelope do Engajamento Centrado em Plataforma.
Fonte: Alberts, Garstka e Stein (1999, p. 97, tradução nossa).

Percebe-se, que no caso específico de aeronaves de caça operando orientadas às plataformas, o alcance dos sensores de bordo é limitado, além de possuir o efeito negativo de mostrar sua posição.

Além disso, o comando e controle transmitido por voz, passa pelo atraso do tempo de transmissão e interpretação da mensagem por parte do controlador e do piloto, que também devem dedicar sua atenção a outras atividades como o voo e o combate propriamente dito.

Alberts, Garstka e Stein (1999), lembram ainda que diversos alvos não são passados ao piloto, pela simples limitação da metodologia de transmissão utilizada.

Ao contrário desta situação, conforme Alberts, Garstka e Stein (1999), em operações centradas em redes, as capacidades de sensoriamento, comando, controle e engajamento são amplamente compartilhadas por *links* digitais.

Assim a fonte de poder é consideravelmente aumentada em uma operação centrada em rede, derivada em parte pelo aumento de conteúdo, qualidade e agilidade no tempo de transmissão do fluxo de informações entre os links dos nós da rede.

A Figura 6 mostra graficamente como o E3 proporcionado pela GCR é aumentado. No caso (a) são mostradas aeronaves operando em conjunto sem integração e no caso (b) operando com integração, portanto passando a ter um significativo aumento de seu E3.

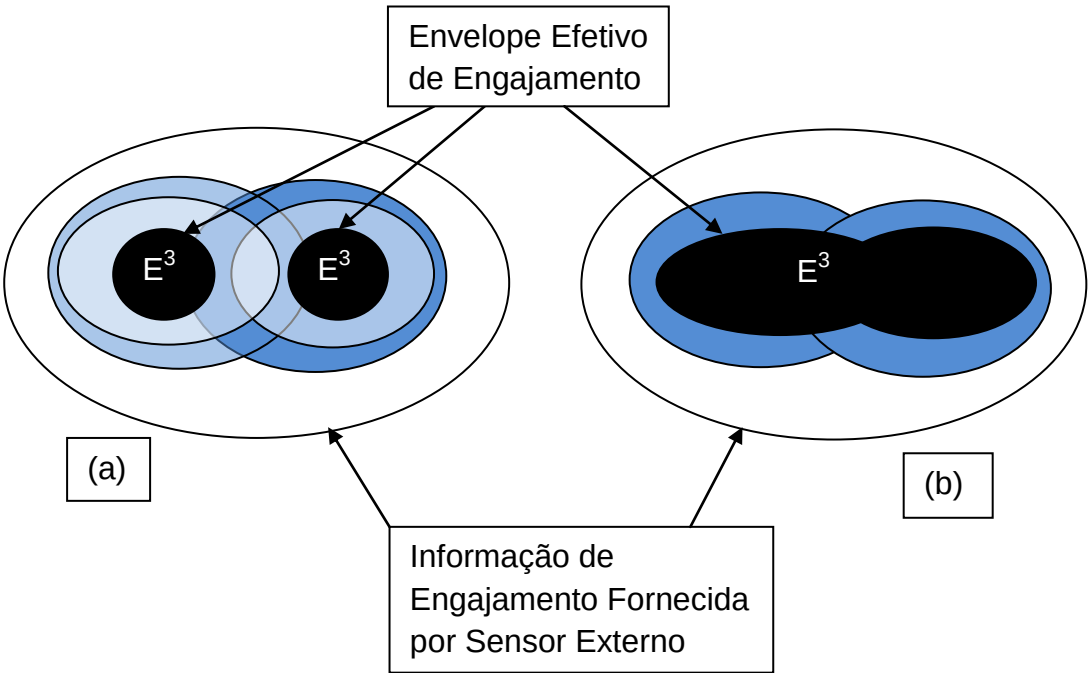

Figura 6: Poder de Combate com Valor Aumentado Devido GCR.
Fonte: Alberts, Garstka e Stein (1999, p. 102, adaptação nossa).

Segundo Alberts, Garstka e Stein (1999), em relação à Figura 6, no caso (a) o E3 da plataforma é menor que o alcance do armamento, devido aos fatores já

discutidos e no caso (b) o E3 é igual ao conjunto do alcance dos armamentos das plataformas envolvidos, devido às facilidades fornecidas pelo compartilhamento de dados via redes.

Alberts, Garstka e Stein (1999), citam que a Força Aérea Americana fez testes nos quais aeronaves F-15C, operando com a filosofia de GCR, tiveram um aumento de efetividade de 100% em relação a aeronaves do mesmo tipo operando sem esta filosofia.

Embora esteja evidente que a GCR, segundo Alberts (1996), oferece oportunidade potencial de prover um grande aumento de poder, não existe garantia de que apenas ligando em rede os elementos do espaço de batalha sem a doutrina e a organização apropriada haverá aumento da efetividade. Na verdade, existe a possibilidade indesejada, de, ao colocar-se o ambiente de batalha em rede sem a doutrina, organização e treinamento adequado, haver uma degradação do desempenho.

Junte-se a isso que, com a utilização da Guerra Centrada em Redes, ocorre o aparecimento de vulnerabilidades decorrentes da transmissão de dados passível de ser interceptada e acessada por potenciais inimigos.

Como um exemplo dessa vulnerabilidade, pode-se citar a notícia publicada no Portal Terra (2009) que narra como aviões não tripulados americanos foram alvos de *hackers* no Iraque, conforme o relato a seguir, extraído do próprio portal.

Rebeldes iraquianos estariam usando há mais de um ano um software, que normalmente é utilizado para interceptar downloads via satélite, para roubar informações enviadas pelas aeronaves não tripuladas do exército americano. Com as informações, os grupos extremistas estariam descobrindo com antecedência determinadas operações militares dos Estados Unidos na região.

Segundo reportagem publicada pelo jornal The Wall Street Journal, o exército americano desconfia que o Irã esteja por trás destas operações. Os rebeldes xiitas iraquianos estariam usando o software SkyGrabber, que custa cerca de US$ 25 na *Internet*, para interceptar os vídeos enviados automaticamente pelos aviões para as bases militares americanas. De acordo com uma fonte próxima ao assunto entrevistada pelo jornal americano.

Um representante da empresa responsável pelo software que os rebeldes iraquianos estariam utilizando, a russa SkySoftware, afirmou que não tinha

conhecimento de que o programa poderia ser usado desta forma. "O SkyGrabber foi desenvolvido para interceptar músicas, fotos, vídeos e outros materiais que as pessoas colocam na internet, e não dados militares ou comerciais, apenas conteúdos legais", escreve Andrew Solonikov por *email* ao jornal americano.

O SkyGrabber é um programa que intercepta *downloads* realizados via satélite por outros usuários, sem necessidade de conexão com a *internet*, apenas uma antena via satélite.

O problema foi descoberto por militares americanos no Iraque no final de 2008, quando um *laptop* apreendido junto com um militante xiita preso continha arquivos com diversas imagens de vídeos enviados pelos aviões não tripulados, conhecidos como Predator. Em julho deste ano, mais arquivos de vídeos com imagens interceptadas dos aviões foram encontrados em laptops de outros rebeldes, levando alguns oficiais a concluírem que diversos grupos rebeldes estariam tendo acesso regular aos vídeos.

Segundo a fonte entrevistada pelo The Wall Street Journal, os militares encontraram "dias e dias, horas e mais horas" de arquivos com imagens interceptadas. "Estas imagens já fazem parte do material deles", disse a fonte ao jornal.

Para os repórteres do The Wall Street Journal, estas interceptações marcam o surgimento da guerra cibernética nas áreas de conflitos sob intervenção americana, e também apontam uma potencial vulnerabilidade das aeronaves não tripuladas, principal argumento utilizado pelo presidente Barack Obama para convencer a população sobre a viabilidade do envio de mais tropas ao Iraque e ao Afeganistão. Os vídeos roubados também mostram, segundo o jornal, que os adversários dos americanos continuam encontrando maneiras simples de enfrentar a sofisticada tecnologia militar dos Estados Unidos.

O exército americano afirma estar trabalhando para evitar novas interceptações, com soluções como codificar as imagens, mas admite ainda não ter certeza se o problema foi completamente resolvido. Adversários militares dos Estados Unidos também teriam interceptado imagens enviadas por aviões não tripulados em outros locais de combate, como Afeganistão e Paquistão.

Tal fato serve de alerta para Forças Armadas que estão trabalhando na incorporação da Guerra Centrada em Redes em suas operações. Pois embora tal filosofia forneça um alargamento do horizonte estratégico, operacional e tático, traz,

também, vulnerabilidades, uma vez que a concentração das informações fornece um alvo valioso ao inimigo, que muito mais do que impedir ou interceptar essas transmissões, poderá vir a interceptá-las e modificá-las ou mesmo transmiti-las a seu favor. Como os Ingleses fizeram com os códigos Alemães na Segunda Guerra Mundial.

Portanto, o que foi exposto indica que o caminho para implantação do conceito de GCR deve ser ricamente povoado de análises e experimentos a fim de prover um melhor entendimento de como uma Força Armada poderá aproveitar o seu imenso potencial.

Nos dias atuais, diversas forças armadas vêm utilizando o conceito de GCR em suas Forças Armadas, o que lhes forneceu um elevado potencial militar no que diz respeito à Guerra Convencional. Esse desequilíbrio acabou gerando uma maior utilização da Guerra Irregular, assim, o ambiente cibernético, como fonte de poder, tornou-se também uma vulnerabilidade que gera grandes desafios de segurança, dentre eles os relacionados ao terrorismo, mais especificamente, o terrorismo cibernético, assunto tratado a partir do presente momento.

3.2 TERRORISMO CIBERNÉTICO

A conceituação de Terrorismo Cibernético encontra diversas interpretações e, segundo Uda (2009), é algo cada vez mais presente na sociedade moderna com elevado potencial de perigo, o que torna a segurança cibernética um dos maiores desafios frente ao desafio do ambiente competitivo do século XXI.

Nesse, ponto, é necessário diferenciar os conceitos de Crime Cibernético, Terrorismo Cibernético, e Guerra Cibernética.

a) Crime Cibernético – segundo Uda (2009), Crime Cibernético é toda a gama de crimes já existentes e que apresentam a singular característica de serem praticados no ambiente cibernético, como roubos, pornografia infantil, contrabando, lavagem de dinheiro, vandalismo e terrorismo praticado contra civis. Nestes casos, a lei de cada país da o tratamento específico em seu ordenamento jurídico.
b) Terrorismo Cibernético – Uda (2009) apresenta o conceito, fornecido pelo FBI, no qual o Terrorismo Cibernético é qualquer ataque politicamente motivado e premeditado contra informação, sistemas de

computadores, programas de computadores e dados que resulte em violência contra alvos não combatentes realizados por grupos subnacionais ou agentes clandestinos.

c) Guerra Cibernética - “um meio do estado e de organismos não estatais atingirem seus objetivos por meio de ataques digitais aos centros de gravidade adversários.” (RATTRAY, 2001, p. 14, tradução nossa).

Pode-se perceber que o Crime Cibernético possui intersecção com o Terrorismo Cibernético, e este, por sua vez, acaba por ter uma sobreposição com o a Guerra Cibernética, portanto será mantido o foco no estudo sobre o terrorismo em seu aspecto cibernético.

Os ataques terroristas cibernéticos, segundo Arquilla, Ronfeldt e Zanini (2009), causam violência física e grandes danos. Dentro deste, contexto, o antigo fenômeno do terrorismo continua a manter o seu apelo para seus perpetradores por três razões principais:

a) o seu apelo de ser a arma dos fracos – uma sombria maneira de travar guerra atacando assimetricamente para causar danos ao adversário e, tentar, derrotar uma força ostensivamente superior;

b) o terrorismo tem o apelo de ser um modo de reivindicar identidade e atenção do comando – terroristas, normalmente, recorrem à violência como um fim que por si só gera identidade ou mancha a identidade do inimigo; e

c) terrorismo, em alguns casos, tem o apelo de ser um caminho para alcançar uma nova ordem mundial destruído premeditadamente o presente.

Segundo Arquilla, Ronfeldt e Zanini (2009), nas duas primeiras motivações ou razões, o terrorismo pode envolver retaliação ou retribuição por erros passados, enquanto a terceira é sobre revelação, renascimento e a chegada de uma nova era. A primeira é altamente estratégica; ela tem um sentido prático, e os objetivos podem ser limitados e específicos. Em contraste, a terceira pode encampar uma forma, sem limitações e transcendental, de alterar o mundo através do terrorismo.

Independente da motivação, o terrorismo passou a ser matéria obrigatória no preparo de uma Força Militar, pois institucionalmente as Forças Armadas têm como missão básica a manutenção da soberania e integridade territorial de um país,

bem como a manutenção de suas instituições, que podem ser afetados por ataques terroristas direcionados a um estado como um todo.

Tais ataques tornaram-se mais abrangentes e letais às instituições, dentre outros fatores, com o surgimento da era da informação. Segundo Arquilla, Ronfeldt e Zanini (2009), este aparecimento trouxe mudanças na doutrina, organização e estratégia que levam a crer o aparecimento de um **novo terrorismo** em sintonia com essa era. Suas principais hipóteses, nesse sentido, são:

a) Organização - terroristas continuarão a mover-se de uma estrutura hierárquica para uma de redes, da era da informação;
b) Doutrina e Estratégia - terroristas irão, provavelmente, ganhar novas capacidades para atos letais; e
c) Tecnologia – terroristas provavelmente estão aumentando o uso de tecnologias avançadas da informação, para uso ofensivo e defensivo, assim como para dar suporte para sua estrutura organizacional. Apesar da grande especulação sobre terroristas usando técnicas de guerra cibernética para interromper o uso da Rede Mundial, eles, usualmente, tem fortes motivos para mantê-la em funcionamento, como, por exemplo, para efetuar a troca de mensagens entre os membros de uma organização.

“Resumindo, o terrorismo está seguindo em uma direção que chamamos de guerra da rede.” (ARQUILLA, RONFELD e ZANINI, 2009, p. 135, tradução nossa). Com isto a guerra irregular tornou-se endêmica e viciosa por todo o mundo.

Segundo Lesser (1998), a preponderância militar de um país, em termos de força convencional, irá motivar seus adversários a recorrerem ao terrorismo como uma resposta assimétrica. Os avanços tecnológicos e o tráfico ilícito podem tornar mais fáceis o acesso de terroristas a Armas de Destruição em Massa.

Os terroristas, para Arquilla, Ronfeldt e Zanini (2009), estão migrando de uma, ultrapassada, estrutura hierárquica, para outra em rede, e estão, crescentemente, aumentando o uso de avançadas tecnologias de comunicação para prover uma estrutura de comando, controle e coordenação, que irão provê-los com a capacidade de montar operações à distância.

Tal aumento na capacidade de operação dos terroristas tem aumentado sensivelmente a necessidade do preparo das instituições de um país, e nesse sentido com grande ênfase às Forças Armadas, para o combate a esta ameaça.

De acordo com Littleton (1995), atualmente existem duas camadas distintas de terroristas, uma caracterizada por profissionais altamente preparados e outra constituída de amadores. A possibilidade de negação, isto é, de não assumir a autoridade por determinados ataques, provida pela utilização de amadores, tornou-se um grande potencial para gerar ataques terroristas cada vez mais violentos e mortais.

Segundo Arquilla, Ronfeldt e Zanini (2009), diversos especialistas sugerem que a informação será um alvo chave, pois embora ela ofereça uma atividade menos letal, ela oferece teatros de operações adicionais para os terroristas.

Isso ocorre, pois para Arquilla, Ronfeldt e Zanini (2009), a revolução da informação está alterando a natureza do conflito, particularmente em dois aspectos:

a) a revolução da informação está favorecendo e fortalecendo organizações organizadas em redes, normalmente dando-lhes vantagens em relação às organizações organizadas hierarquicamente. O aparecimento das redes significou que o poder está migrando para atores não estatais, os quais são capazes de organizar-se em redes multiorganizacionais alastradas.
b) com o aprofundamento da revolução da informação, os conflitos serão de comunicações e informações, de forma cada vez mais crescente. Mais do que nunca, os conflitos irão girar em torno do conhecimento e do poder suave. Os adversários irão enfatizar operações de informações e gestão de percepção, ou seja, medidas orientadas à mídia que objetivam atrair mais do que coagir, o que afetará como a sociedade e os militares vêm os conhecimentos sobre si mesmos e sobre os adversários.

As ameaças da era da informação, conforme Arquilla, Ronfeldt e Zanini (2009), serão provavelmente mais difusas, dispersas, ambíguas e multidimensionais em relação às ameaças tradicionais. O espectro dos conflitos será moldado em suas extremidades pelas seguintes dinâmicas:

> - Guerra Cibernética – um conceito que refere a guerra militar orientada a informações – está se tornando um importante aspecto na extremidade militar do espectro, na qual a linguagem normalmente tem sido sobre conflitos de alta intensidade.
> - Guerra de Redes aparece, de forma crescente, na extremidade da sociedade do espectro, na qual a linguagem tem sido normalmente sobre

> conflito de baixa intensidade, operações de guerra irregular e modos de conflito e crime não militares. (ARQUILLA; RONFELDT, 1993, tradução nossa).

Enquanto a Guerra Cibernética, usualmente assume forças militares combatendo entre si, conforme Arquilla, Ronfeldt e Zanini (2009), Guerra de Redes envolve mais forças irregulares, paramilitares e não estatais, portanto, pode-se observar, que os dois tipos tratam basicamente do mesmo assunto, diferenciando-se, na figura de seus atores.

Para ser mais preciso, segundo Arquilla, Ronfeldt e Zanini (2009), Guerra de Redes refere-se a um modo emergente de conflito e crime a nível da sociedade, envolvendo medidas muito semelhantes à guerra tradicional, na qual os protagonistas, organizações estruturadas em rede, têm utilizado doutrinas, estratégias e tecnologias em sintonia com a era da informação. Então, a Guerra de Redes da era da informação difere de modos de conflitos e crimes nos quais os protagonistas preferem uma organização hierárquica, formal e isolada.

O surgimento dessa ameaça terrorista no ambiente cibernético trouxe a tarefa complementar para as forças armada se prepararem para o, se assim pode ser dito, terrorismo convencional e também terrorismo cibernético.

A estrutura organizada em rede, utilizada atualmente pelos terroristas, conforme Arquilla, Ronfeldt e Zanini (2009), possui um organograma horizontal. Neste, idealmente, não há comando e liderança singular e central, não há quartéis generais, ou seja, sem uma cabeça a ser afetada, pois ela possui pouca hierarquia e possivelmente vários líderes. O processo de decisão e as operações são descentralizados, aceitando a iniciativa local e autonomia.

Para que a estrutura organizada em redes possa funcionar, segundo Arquilla, Ronfeldt e Zanini (2009), precisa haver objetivos, interesses e princípios compartilhados, além de doutrina e ideologia global. Outro fator de sucesso para a estrutura em rede, é que ela deverá depender de uma estrutura para comunicações densas de informações funcionais, mais do que outros tipos de organizações.

Esses fatores, em conformidade com Arquilla, Ronfeldt e Zanini (2009), são providos pelas últimas tecnologias de informações e comunicações, como o celular e a *Internet*, que tem sustentado os agentes de Guerra de Redes, além de fornecer-lhes excelentes perspectivas com o enorme potencial de desenvolvimento das tecnologias citadas.

Arquilla, Ronfeldt e Zanini (2009), salientaram que a tecnologia da informação e a *Internet* não são os únicos aspectos a serem observados quando se fala sobre a guerra de redes. Atenção especial deve ser dada aos usuários, aos novos e antigos sistemas e ao fato de que a guerra de redes não ocorre na *Internet, pois* a sua conduta e ganho depende muito mais dos efeitos que ocorrem no mundo real, ou seja, Guerra de Redes não é Guerra da Internet.

Um aspecto importante a ser considerado quando se analisa a Guerra de Redes, segundo Arquilla, Ronfeldt e Zanini (2009), é o seu elevado potencial de realizar operações em enxame, que ocorrem quando diversos pequenos módulos da rede convergem suas forças para um alvo específico, provenientes de diversas direções.

As estruturas em rede bem construídas, segundo Arquilla, Ronfeldt e Zanini (2009), são normalmente muito sólidas em termos defensivos, isso ocorre pois as mesmas são redundantes e possuem comando e controle disperso, o que dificulta o ataque das mesmas. Além disso, são difíceis de ser atingidas, uma vez que ao atacá-las e rompê-las, provavelmente tal feito estará sendo feito em apenas uma parte da estrutura, sem atingir o sistema como um todo.

Uma das dificuldades de lidar com atores da Guerra de Redes, de acordo com Arquilla, Ronfeldt e Zanini (2009), é o espaço cinzento entre a definição de uma ação como defensiva ou ofensiva, fazendo com que a esta ação orbite entre diversos lados de diversos padrões duais como: guerra ou paz, guerra ou crime, civil ou militar e ataque ou contra-ataque, dentre outros.

Tal indefinição torna difícil para estados, e especificamente suas forças armadas, lidarem com essa estrutura, Pois os mesmos baseiam-se em um ideal de soberania e autoridade tradicionalmente ligado à racionalidade burocrática que define claramente a divisão de negócios e problemas por seus respectivos responsáveis.

Para combater organizações baseadas em rede, Arquilla, Ronfeldt e Zanini (2009), apresentam três aspectos:

a) hierarquias têm dificuldade em combater redes;
b) são necessárias redes para combater redes; e
c) aquele que dominar o modelo de redes primeiro e melhor irá ganhar maior vantagem.

O conceito de guerra de rede, conforme Whine (1998), é consistente com os padrões e tendências das organizações terroristas do Oriente Médio que tem se tornado as mais ativas na atualidade. O aparecimento de arranjos em rede nas organizações terroristas é parte de um movimento mais amplo de mudança de organizações patrocinadas por estados, para grupos com patrocínio privado. Tais grupos têm usado a TI para guiar seus elementos dispersos, ou seja, para estas organizações a TI não é apenas um meio de ataque e defesa, mas também um meio de suporte à própria organização.

Mesmo para países, teoricamente, afastados do foco do terrorismo cibernético, como o Brasil, tal situação já tem se mostrado um motivo de preocupação, como no caso em que, segundo (CARR, 2009, p. 203), Tom Donahue, um analista sênior da CIA, citou, em uma conferência proferida em 18 de janeiro de 2008, a ocorrência de um ataque cibernético que causou um enorme *blackout* em um país estrangeiro. Posteriormente, uma rede de televisão americana noticiou que esse país era o Brasil conforme o relato a seguir:

> Diversas fontes proeminentes de inteligência confirmaram que ocorreram uma série de ataques cibernéticos no Brasil: um no norte do Rio de Janeiro em janeiro de 2005 que afetou três grandes cidades e dezenas de milhares de pessoas, e outro evento, muito maior, iniciado em 26 de setembro de 2007.
> Este, no estado do Espírito Santo, afetou mais de três milhões de pessoas em dúzias de cidades durante um período de dois dias, causando importantes disrupções. Em vitória, uma das maiores produtoras de minério de ferro do mundo teve sete usinas colocada fora do ar, custando à compania sete milhões de doláres. Não está claro quem fez e qual o motivo. (CBS, 2009, tradução nossa). (CBS, 2009)

Verifica-se com essa declaração que existem três verdades a respeito da guerra cibernética, em particular o terrorismo cibernético, segundo Uda (2009, p. 8):

a) a ameaça é real;

b) há possibilidade de mais de um ataque; e

c) ataques serão direcionados à infraestrutura crítica.

Para contrapor ações do terrorismo cibernético, Arquilla, Ronfeldt e Zanini (2009) indicam que a natureza de dupla mão da conectividade em redes de informação, como a *Internet,* implica que os perigos impostos pela guerra cibernética são simétricos. Ou seja, quanto maior for o grau de utilização de tecnologia da informação para fins ofensivos, maior será a sua exposição a ataques similares por parte de forças contraterroristas.

Para Arquilla, Ronfeldt e Zanini (2009), o ponto chave para o contraterrorismo é identificação tecnológica e organizacional da rede terrorista. Uma vez que tais estruturas forem identificadas, então será possível inserir e disseminar falsas informações, sobrecarregar sistemas, interceptar e direcionar o tráfego de mensagens, excluir acesso e impor outras ações destrutivas e disruptivas impedir e prevenir operações terroristas.

Portanto, é necessário que os Estados estabeleçam sua capacidade, em termos de Guerra Cibernética, para garantir a defesa de sua estrutura, contra ataque de terroristas cibernéticos, pois “o sucesso dos futuros conflitos dependerá menos de bombas e balas e mais de bits e bytes.” (COLEMAN, 2007).

Fica evidente assim, que embora o terrorismo tenha ganho grande fôlego com o advento da era da informação, e o aparecimento do terrorismo cibernético, o mesmo também ganhou as vulnerabilidades existentes no ambiente cibernético, o que exige o preparo adequado das forças que lutam em sua contraposição, ou seja, é necessário que as forças armadas se adaptem a essa nova realidade, para que o inimigo não ganhe um grande diferencial de poder.

Com o desenvolvimento do tema a respeito de Guerra Cibernética, percebe-se que os seus efeitos possuem uma abrangência muito elevada. Aliado a isso, nota-se que uma característica intrínseca da Guerra Cibernética é o seu elevado potencial de negação, que aumenta a dificuldade de identificar a verdadeira natureza do conflito - se é um ato de crime, terrorismo ou guerra.

Tal dificuldade traz à tona o assunto referente à condição legal de se responder a um ataque cibernético internacional como um ato de guerra, o qual será tratado a seguir.

3.3 O ATAQUE CIBERNÉTICO COMO ATO DE GUERRA

Um dos assuntos mais debatidos no Direito Internacional, segundo Sklerov (2009), é quando um estado pode responder legalmente a um ataque cibernético em autodefesa. Enquanto a Direito de Guerra é composto de princípios conhecidos e amplamente aceitos, aplicar esses princípios à Guerra Cibernética é uma tarefa difícil.

Esta dificuldade, de acordo com Sklerov (2009), ocorre devido ao fato das leis de guerra terem sido feitas como resposta a guerras convencionais entre

estados. Conforme a Carta das Nações Unidas (1945), uma nação pode usar a força para autodefesa contra um ato de agressão, mas diz isto se referindo a conflitos armados.

Segundo Carr (2009), a Lei do Conflito Armado é utilizada gomo um guia para determinar o que é ou não Guerra Cibernética, tal determinação deve ser conforme a certas regras: a Lei do Conflito Armado aplica-se somente quando o conflito já foi iniciado, e incidentes cibernéticos que correspondam com o conflito armado devem ser atribuídos a governo específico.

Conforme Carr (2009), tais restrições tornam impraticáveis a aplicação da Lei do Conflito Armado à Guerra Cibernética, devido a sua essência. Assim não há uma entidade legal conhecida como Guerra Cibernética, o único dispositivo definido, pelo entendimento internacional, é o direito de autodefesa de uma nação quando for atacada, e tal dispositivo referindo-se a ataques armados.

Quando se avalia um ataque armado sob o paradigma do ataque entre nações, segundo Sklerov (2009), torna-se mais fácil avaliar o escopo do ataque e identificar o atacante. Infortunadamente, quando um ataque cibernético esta em progresso, torna-se difícil para um estado realizar esta avaliação. Esta dificuldade tem tornado os Estados relutantes a responder ataques cibernéticos em autodefesa, devido ao temor da violação das leis de guerra.

Portanto, uma Força Armada em seu preparo para utilização do espaço cibernético, deve adaptar todo o seu ordenamento legal de forma a balizar as suas ações referentes à Guerra Cibernética de forma a torná-la legalmente factível, e assim perder o temor de atuar no ambiente cibernético.

Segundo Sklerov (2009), tal temor não é necessário, pois as leis internacionais dão ao estado o direito de:

> 1. Abordar e responder a ataques cibernéticos como atos de guerra a não apenas como questões criminais.
> 2. Usar defesas ativas, não apenas passivas, contra redes de computadores em outro estado, que pode ter, ou não, iniciado o ataque, mas negligenciou o seu dever de prevenir que ataques cibernéticos partissem de suas fronteiras. (SKLEROV, 2009, p. 46, tradução nossa)

Existe, de acordo com Sklerov (2009), um dilema legal imposto, pois o ponto de vista prevalecente, de estados e acadêmicos, é que os estados devem tratar os ataques cibernéticos como uma questão criminal. Primeiro pela incerteza se este ataque, sequer, pode ser tratado como armado, e depois porque a lei da guerra

requer que um Estado atribua um ataque armado a um Estado Estrangeiro, ou a seus agentes, antes de responder com a força.

Esta visão, segundo Sklerov (2009), é limitada, pois a defesa ativa é uma forma de força eletrônica, portanto esta visão impõe a obrigação de defesa passiva, que nem sempre é suficiente e adequada, além disto, ao tratar os ataques como crime, seus executores são colocados sob o arcabouço do ordenamento jurídico de seu país.

Assim essa visão limitaria a utilização de uma defesa cibernética ativa, limitando um ator obrigado a atuar sob os ditames legais a atuar defensivamente, o que conforme discutido nos tópicos anteriores, proporcionaria uma grande desvantagem.

Acima de tudo, conforme Sklerov (2009), essa imposição do modelo defensivo reativo de resposta de crise ocorre, pois é virtualmente impossível atribuir autores de ataques cibernéticos durante a sua execução, e tal tarefa de identificação de autores é algo muito custoso e dependente de cooperação internacional.

Este arranjo legal acaba por possibilitar que Estados utilizem o estratagema de executar ataques cibernéticos por via de sua população civil, que assim estaria protegida pelo próprio sistema legal deste, tornando assim os ataques impossíveis de ser revidados de forma legal.

Para fugir deste dilema, de acordo com Sklerov (2009), os estado devem utilizar defesa ativa, porém a lei internacional ainda não provê, aparentemente, suporte legal a tal atividade. “Afortunadamente, o Direito da Guerra é robusto o suficiente para prover tal direcionamento aos estados; apenas um precisa examiná-lo completamente.” (SKLEROV, 2009, p. 48, tradução nossa).

O Direito da Guerra, de acordo com Sklerov (2009), é dividido em duas principais áreas. O *jus ad bellun*, conhecido como o direito da gestão do conflito, que é a base jurídica internacional para um governo realizar a sua transição da paz para a guerra e o *jus in bello,* que é conhecido como direito do conflito armado, que governa o uso da força durante o conflito, propriamente dito.

Para Sklerov (2009), a análise se um estado pode ou não responder a ataques cibernéticos através de defesa ativa, predominantemente, reside no jus ad bellun.

Historicamente, segundo Sklerov (2009), a transição da paz para a guerra era uma prerrogativa da soberania, porém com a Carta das Nações Unidas, passou

a existir a figura da ratificação por parte da ONU. É exatamente esta carta o documento que possui os modelos que permitem uma moderna análise do *jus ad bellum*.

No artigo 2, inciso 4 da Carta das Nações Unidas está consignado o seguinte:

> Todos os Membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1945).

Na análise de Sklerov (2009), este artigo criminaliza o uso e a ameaça da força por parte dos Estados. Assim os Estados não devem ameaçar ou efetivamente usar a força contra outro Estado, a menos que apareça uma exceção dentro da própria Carta. Tal posição é imposta pelo artigo 2, inciso 3 desse documento.

"Todos os Membros deverão resolver suas controvérsias internacionais por meios pacíficos, de modo que não sejam ameaçadas a paz, a segurança e a justiça internacionais." (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1945).

Segundo Sklerov (2009), existem apenas duas exceções que suportam o uso da força; autorização do Conselho de Segurança da ONU, e defesa própria.

É na segunda exceção, segundo Sklerov (2009), que reside o lapso de interpretação que permitirá o uso de uma defesa ativa como uma resposta a um ato de guerra. O artigo 51 diz o seguinte:

> Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva no caso de ocorrer um **ataque armado** contra um Membro das Nações Unidas, até que o Conselho de Segurança tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos Membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao Conselho de Segurança e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer tempo, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1945, grifo nosso)

A justificativa legal proposta por Sklerov (2009), e alvo de discussões, é que não há definição formal de ataque armado, podendo-se ai encaixar a Guerra Cibernética.

Embora esteja aberta a possibilidade de usar a Guerra Cibernética como autodefesa, tal ação deverá ser baseada em alguns princípios consolidados pelo ordenamento jurídico internacional que para Sklerov (2009) são os seguintes:

a) proporcionalidade, a força aplicada para a defesa deverá ser proporcional ao potencial ofensivo da força atacante; e
b) necessidade, existe a impraticabilidade de ser usado um meio alternativo, pacífico, de autodefesa.

A autodefesa possui um subconjunto conhecido como autodefesa antecipada, que segundo Sklerov (2009), é já a longo tempo consolidado como o um princípio do Direito Internacional. Este princípio tem o seu embasamento na eminência de um ataque, que quando identificada, autoriza um Estado usar meios restritos no momento imediatamente anterior a um ataque.

> Nos dias atuais, a eminência permite que Estados empreguem legalmente o uso em antecipação a um ataque, no momento que (1) evidências demonstrarem que um agressor comprometeu-se a realizar um ataque armado e (2) o atraso da resposta atravancará a capacidade de um defensor montar uma defesa adequada. (SKLEROV, 2009, p. 51, tradução nossa).

Assim iminência é um conceito relativo, que atua como o seguinte:

> Estados fracos podem agir legalmente antes dos mais fortes, na presença de ameaças idênticas, porque eles correm maiores riscos com a passagem do tempo. No mesmo caminho, poderá ser necessário conduzir operações defensivas contra grupos terroristas muito antes de um ataque planejado, porque poderá não haver outra oportunidade para alvejar terroristas antes que eles ataquem.... Em outras palavras, cada situação apresenta um caso específico de oportunidade na qual um Estado pode evitar um ataque eminente. (SCHMITT, 2003, tradução nossa). (SCHMITT, 2003)

Até o presente momento o estudo está focado nos atores estatais, porém uma Força Armada, para a aplicação do *jus ad bellum*, como embasamento da Guerra Cibernética, deve pautar sua ação em uma análise levando-se em conta a relação do ator não estatal e o Direito da Guerra.

Segundo Sklerov (2009), como regra geral, o Direito Internacional trata cada estado como soberano e proíbe outros estados de travarem guerra contra eles ou de interferir em seus assuntos domésticos. Uma vez que um estado abre mão desses direitos quando ele ataca outro, ele não o faz quando atos realizados por pessoas, dentro de suas fronteiras, são criminosos.

Mesmo que o *jus ad bellum* tenha certa previsão para ataques realizados por elementos não estatais, segundo Carr (2009), historicamente essa previsão é escassa. No entanto com o crescimento do terrorismo transnacional, os Estados estão se vendo obrigados a expandir suas normas tradicionais para absorver os ataques terroristas.

A relação entre os elementos não estatais e o direito de responder a um ataque cibernético, como um ato de guerra, segundo Carr (2009), reside no grau de comprometimento desse governo com a luta pela prevenção de realização de tais ataques a partir de seu território, e de como este governo se relaciona com os atores não estatais realizando ataques a outros países.

“Existe um princípio a muito estabelecido no Direito Internacional que o estado é responsável por realizar ações adequadas para prevenir o uso de seus domínios para a prática de atos criminosos contra outras nações e povos.” (SCHMITT, 2003, tradução nossa).

Portanto um estado deve fortalecer as suas instituições para combater essa ações criminosas, tal preparo deve refletir em suas Forças Armadas, que devem atuar legitimadas pela lei.

Pode-se perceber que o embasamento legal, quanto à Guerra Cibernética, é permeado de tópicos que podem ser frutos de estudos aprofundados, porém ficando nítido que o Direito Internacional já possibilita o enquadramento da legalidade da Guerra Cibernética.

Feito isto, percebe-se que a Guerra Cibernética é uma realidade no que diz respeito à sua utilização como forma de atingir os objetivos políticos de uma nação, ou seja, como uma forma de travar uma guerra.

Colocado o embasamento teórico, a seguir será estudado como China, EUA e Rússia, vem realizando ações de Guerra Cibernética, a fim de fornecer parâmetros de comparação ao diagnóstico da Força Aérea Brasileira.

4 AÇÕES DE FORÇAS ARMADAS NA ÁREA DE GUERRA CIBERNÉTICA

Com o intuito de verificar o preparo de diversas forças aéreas com relação ao tema, foi feita uma pesquisa direcionada às forças de países que, segundo quase a totalidade da bibliografia existente, são mais desenvolvidos em relação à Guerra Cibernética, ou seja, Federação Russa, China e Estados Unidos da América.

Embora, de acordo com o objetivo geral do trabalho de diagnosticar a situação da FAB nas ações de Guerra Cibernética, pareça mais adequado utilizar os países do Cone Sul como parâmetros de comparação, em uma pesquisa preliminar destes, não foram identificadas ações contundentes na área de Guerra Cibernética que possibilitassem obter meios adequados a uma análise.

Assim, além do critério de desenvolvimento em assuntos militares cibernéticos, um critério que norteou a inclusão de China e Rússia foi o fato dos mesmos, junto com Brasil e Índia, formarem o bloco dos BRICs, compondo as partes mais desenvolvidas em termos militares, dentre esses países, sendo de grande interesse à realidade da Força Aérea Brasileira.

A inclusão dos EUA justificou-se exatamente pela sua posição como grande potência militar da atualidade, e por ser o país mais desenvolvido em ações no meio cibernético.

Portanto, a seguir serão verificadas as ações de Guerra Cibernética nos países selecionados de acordo com o critério estabelecido.

4.1 CHINA

A tecnologia da informação é uma área que, segundo Carr (2009), difere da capacidade industrial e dos equipamentos militares, pois nenhuma nação pode clamar pelo seu domínio. Como um resultado disto, TI e sua contraparte militar, a Guerra Cibernética, apresenta um grande apelo para o Exército Popular de Libertação (PLA, da sigla em inglês)[6], que possui grande abundância de recursos no

[6] Exército Popular de Libertação são as forças armadas da República Popular da China.

tamanho de sua população e no número de pessoas formadas com alta qualidade em matemática e ciências.

Ainda segundo Carr (2009), em abril de 2001, quando uma aeronave EP-3 de vigilância de sinais colidiu com uma aeronave militar Chinesa, resultando na morte do piloto Chinês, uma população raivosa de *hackers* Chineses lançou ataques contra redes americanas. Estes eventos não passaram desapercebidamente dos oficiais do PLA, que observaram como guerreiros cibernéticos poderiam afetar a dependência tecnológica de uma força superior em um esforço para ganhar uma vantagem assimétrica.

Assim a análise do caso chinês traz à tona a utilização da Guerra Cibernética como forma de contrapor um estado menos poderoso militarmente, China, frente a outro mais forte, EUA.

As doutrinas Americana e Chinesa em Guerra da Informação possuem diferenças “os EUA tendem a focar no aspecto da Guerra de Informações baseada em ataque a redes de computadores, enquanto os Chineses tomam uma perspectiva mais ampla, enfatizando pilares como *PSYOP*, contradição e engano.” (FERRIS, 2001 apud YOSHIHARA, 2001).

Respondendo a pergunta- o que explica o intenso interesse chinês em Guerra da Informação? - Yoshihara (2001) argumenta que claramente os chineses identificaram as implicações da revolução da informação.

> Primeiro, a China reconheceu a importância da alta tecnologia e a força crescente da informação na era da globalização e da interdependência. Segundo, a China aspira a ser participante majoritário em termos políticos e econômicos em uma comunidade global na qual o poder da informação possui um lugar crítico nas relações entre estados. Assumindo-se que o desenvolvimento econômico localiza-se na mais alta prioridade nacional, a integração Chinesa no sistema econômico internacional, altamente fundamentado na informação, fortaleceu o apelo pela informação. Terceiro, como um corolário do ponto anterior, os Chineses acreditam que, como a China tem aumentado a abrangência de seu poder nacional, o mundo eventualmente irá mudar de um mundo unipolar para outro multipolar, no qual a República Popular da China estará em igualdade de condições. Ou seja, a habilidade de competir economicamente e de travar uma guerra de alta tecnologia com TI será um componente crítico da força nacional Chinesa. (YOSHIHARA, 2001, p. tradução nossa)

Assim é verificado que se pode usar o exemplo chinês, como de um país emergente em busca de uma posição de destaque mundial, e que nesse sentido está preparando suas forças Armadas para atuar no ambiente cibernético.

Um problema, identificado pelos chineses no curso de seu preparo, inerente à tecnologia em uma força militar tecnologicamente avançada é sua

dependência da tecnologia, portanto ficando a questão de “como utilizar fraqueza para derrotar força e como conduzir uma guerra contra inimigos mais fracos utilizando a superioridade em informações para atingir a vitória com um menor custo.” (PUFENG, 1995, p. tradução nossa).

O governo Chinês vê a Guerra Cibernética, segundo Thomas (2000), como uma verdadeira Guerra Popular, significando que ele pode recrutar especialistas de sua população civil, a qual possui um grande nível de preparo, e poderá vir a se tornar um fator decisivo.

Segundo Carr (2009), a China, assim como os EUA, vê os futuros conflitos como de engajamento limitado, ao invés de uma Guerra total, assim o objetivo não é esmagar o inimigo, mas sim tornar os custos da guerra inaceitáveis para o mesmo, causando-lhe uma paralisia.

Essa visão, de forma clara, mostra uma abordagem possível de ser adotada por uma país mais fraco frente a outro mais forte, fazendo, de certa forma, um equilíbrio de forças.

Segundo Thomas (2009), o termo cibernético não tem seu uso amplamente difundido na China, que geralmente utiliza o termo informática, no entanto, este pode ser utilizado como sinônimo de cibernético, assim como ataque de informação é utilizado como ataque cibernético.

Ainda de acordo com Thomas (2009), a China define Guerra Cibernética de forma ampla como uma luta entre lados opostos fazendo uso de tecnologia de rede e métodos para lutar por uma vantagem em termos de informações no campo político, militar e tecnológico. Complementa, ainda, que para os chineses, a guerra cibernética poderia ser uma série de ações como vigilância, defesa e suporte de redes realizadas por lados opostos utilizando a tecnologia de rede na área de comando de combate, controle de armas, suporte ao combate, suporte logístico, reconhecimento de inteligência e gerenciamento de combate.

De uma perspectiva estratégica e militar, conforme Mckenzie (2000), a Guerra Cibernética promete compensar as grandes, antiquadas e convencionais forças armadas Chinesas. Primeiro a Guerra da Informação possibilita aos chineses lutarem a partir de uma posição de relativa fraqueza, particularmente contra inimigos de forças militares amplamente superiores, como os EUA e o Japão. Na terminologia atual, TI provê “capacidade assimétrica” para estados e atores não estatais. Enquanto a definição de guerra assimétrica tem variado e evoluído através dos

tempos, o conceito básico é utilizar métodos e capacidades heterodoxas para minar ou evitar as forças inimigas enquanto inflige estragos desproporcionais nas fraquezas inimigas.

> Em uma confrontação hipotética entre Estados Unidos e China, o atraso das forças Chinesas iria, indubitavelmente, trazer a derrota. Então os Chineses não podem esperar lutar nos termos Americanos, eles devem descobrir outros meios para intimidar ou derrotar os EUA. A Guerra Cibernética provê Pequim com a capacidade potencial de alcançar diretamente o solo Americano, o qual está muito distante das limitadas capacidades de projeção militar Chinesa. Os Chineses poderiam atacar a infraestrutura critica nos Estados Unidos para influenciar ou manipular a percepção pública e, assim, enfraquecer o desejo político da América de intervir ou lutar. Esta necessidade de atacar fraquezas, com a finalidade de derrotar um inimigo superior, é um conceito central e ainda influente da filosofia de guerra popular de Mao Tsé-Tung, e tem um forte espaço nos pensadores Chineses. (YOSHIHARA, 2001, p. tradução nossa)

A tecnologia cibernética avançou potencialmente o pensamento chinês no que diz respeito à antecipação. Os acadêmicos militares chineses professam que aqueles que não pretendem perder a iniciativa em conflito de curta duração, acharão maior facilidade em obter os objetivos da guerra através de uma campanha, ou batalha, única mais do que em qualquer outro tempo da história. A ideia dos ataques repentinos modificou-se. “Não é apenas através da surpresa, como significava antigamente, também significa que um lado não poderá reagir, mesmo que a situação seja conhecida, porque o outro lado possui uma tecnologia mais avançada.” (THOMAS, 2009, p. 467, tradução nossa).

Fica evidente que a China incorporou em seu pensamento militar o tema Guerra Cibernética, conferindo importância capital ao mesmo na condução de uma guerra.

Como resultado desse pensamento, segundo Krekel (2009), analistas Chineses têm argumentado que a preparação e a mobilização são mais importantes do que já foram anteriormente. O preparo para a guerra, para incluir o recrutamento de talento em informação, deverá ser feito com antecipação. Assim, se uma operação cibernética mostrar-se necessária, poderá ser realizada intempestivamente com o uso de elos civil-militares.

Lançar ataques para ganhar a iniciativa inclui atacar o centro de gravidade inimigo e enfraquecer a sua eficiência de combate dos sistemas de informação e das armas computadorizadas. Isto permitirá alguém enfraquecer a superioridade inimiga em informação e reduzir a sua capacidade holística de combate.

Segundo Thomas (2009), em maio de 2006, a China publicou a sua Estratégia Estatal de Desenvolvimento da Informatização, que embora não seja especificamente militar, é em muitos aspectos uma contraparte para a Estratégia Militar Nacional para Operações no Espaço Cibernético. A primeira clama pelo seguinte:

a) prover uma infraestrutura cibernética nacional;
b) fortalecer as capacidades para a inovação independente em tecnologias cibernéticas;
c) otimizar a infraestrutura da industria cibernética;
d) realizar um progresso efetivo na construção de uma sociedade e economia nacional orientada à informática;
e) estabelecer novos modelos de industrialização;
f) construir uma política nacional aperfeiçoada e sistemas para o processo de informatização;
g) aumentar a capacidade de aplicar tecnologias cibernéticas entre a população;
h) promover a informatização da economia nacional;
i) popularizar o governo eletrônico;
j) estabelecer uma avançada cultura de *internet*; e
k) acelerar a informatização social.

Tal ação mostra o comprometimento político com assuntos ligados à tecnologia da informação, atuando no caso de forma abrangente, e obrigatoriamente obrigando o preparo das Forças Armadas Chinesas para a condução da Guerra Cibernética.

Para entender a estratégia cibernética Chinesa, é necessário compreender a definição Chinesa de estratégia. De acordo com Thomas (2009), a Enciclopédia Militar Chinesa define estratégia como um julgamento analítico de fatores como condições internacionais, hostilidades políticas bilaterais, economia militar, ciência e tecnologia e geografia na medida em que eles se aplicam à preparação e direção do plano geral militar ou de guerra.

Percebe-se na definição Chinesa de estratégia, que a mesma possui uma percepção de julgamento analítico de fatores aplicáveis ao plano de guerra, diferindo do conceito Americano, que de acordo com Thomas (2009), é um conceito de um

conjunto de ideias para o emprego de instrumentos de força militar para atingir objetivos militares.

De acordo com Li Binngyan (2004 apud THOMAS, 2009, p. 468 – 469), o uso da informação é crucial no processo cibernético para influenciar ou controlar a direção de um processo decisório oponente. A estratégia militar deve absorver metodologias, incluindo teorias cibernéticas e de informação, para atrair o inimigo a adotar uma estratégia que irá levar a China a obter os maiores ganhos.

Um grande desafio da doutrina Chinesa é realizar a integração entre o Arsenal Cibernético de Alta Tecnologia com Estratagemas Militares Tradicionais.

Nesse ponto, segundo Thomas (2009), Dai Qingmin, o maior especialista Chinês em Guerra da Informação, escreveu que a China deverá pretender usar pacotes de elétrons como ela outras vezes no passado usou sua força. Segundo ele, estratagemas, como **matar com uma espada emprestada** e **exaurir o inimigo no portão e atacá-lo de acordo com a sua facilidade,** sugerem como operações de informação podem ser implementadas, ainda, sugeriu diversas estratégias específicas, citadas a seguir.

a) embaralhar ou sabotar informações ou sistemas de informação inimigos;
b) sabotar uma estrutura global operacional de informação inimiga;
c) enfraquecer a capacidade de informação inimiga para a luta;
d) dispersar as força, armas e fogo inimigo enquanto concentra a sua própria;
e) dissimular a tentativa de reconhecimento inimigo e realizar preparações suficientes para as próprias tentativas;
f) confundir ou desviar um inimigo e criar excelente oportunidades de combate para si próprio;
g) dar ao inimigo uma falsa impressão, enquanto, simultaneamente, lança-lhe um ataque de informações;
h) cegar ou ensurdecer um inimigo com toda sorte de falsa impressão;
i) confundir a mente inimiga ou cause disrupção ao pensamento inimigo;
j) fazer um inimigo acreditar que o que é falso e verdadeiro e o que é verdadeiro é falso; e
k) fazer um inimigo apresentar-se com um julgamento ou ação errônea.

Segundo Thomas (2009), Dai Qingmin quebrou com a tradição Chinesa quando advogou a obtenção da iniciativa e da superioridade em informações, atacando primeiro. Esta estratégia ofensiva ativa contradiz a tradicional estratégia Chinesa de defesa ativa, e indica novas missões para forças cibernéticas e de informações.

A China, dessa forma, incorporou a Guerra Cibernética em sua doutrina militar de acordo com os seus princípios básicos, porém realizando adaptações necessárias, que possibilitam a utilização desse ambiente de guerra decorrente do aparecimento da era da informação.

Existem diferenças evidentes na forma como o Ocidente e Oriente verificam a combinação entre tecnologias, devido as suas diferentes culturas militares e sociais, assim, de acordo com Thomas (2009), o povo oriental enfatiza o estratagema, enquanto o povo ocidental enfatiza a tecnologia, dessa forma, tradicionalmente, os soldados ocidentais recorrem à tecnologia quando em dificuldades enquanto o oriental recorre aos estratagemas para suplantar a deficiência tecnológica.

De acordo com Thomas (2009), a China já é um competidor cibernético para os Estados Unidos, e tem feito avanços significativos em absorver suas capacidades cibernéticas em sua concepção estratégica, tornando-se mais ativa e, talvez, mais ameaçadora. Além disto, continua Thomas (2009), a China vem realizando extensivo reconhecimento computacional nos EUA e em outros países, o que leva a lembrança de um ditado antigo que diz que “um exército vitorioso primeiro vence e depois procura a batalha” (THOMAS, 2009, p. 475, tradução nossa).

O caso chinês tornou bem claro a possibilidade de um estado utilizar a Guerra Cibernética como ferramenta de grande potencial no jogo de equilíbrio de forças entre nações, evidenciando a necessidade do preparo das Forças Militares nesse ambiente, não só para fins dissuasórios, mas também, obrigatoriamente, para fins defensivos.

Finalizando, cita Thomas (2009), que a habilidade chinesa de esconder a forma de seus ataques tornará difícil o reconhecimento de uma ação preventiva que possa vir a se desenrolar, esse comportamento, de certa forma mais ligado ao campo psicológico, traz a tona a análise de outra abordagem realizada, a ser estudada no caso Russo.

4.2 FEDERAÇÃO RUSSA

A Federação Russa, segundo Carr (2009), tem sido o país mais ativo na implementação de ataques cibernéticos contra seus adversários, dentre eles, Chechênia, Quirguistão, Estônia, Geórgia e Ingushétia. Ainda segundo Carr (2009), embora os ataques a estes países não tenham sido comprovadamente efetuados com a sanção do Kremlin, todos eles foram ferramentas na promoção da política da Federação Russa, além do Kremlin nunca ter agido para impedi-los, portanto, beneficiando-se deles.

O interesse militar russo no desenvolvimento da Guerra Cibernética remonta aos meados dos anos 90, quando o Subcomitê de Segurança da Informação da Duma[7], segundo Carr (2009), expressou sua suspeita a respeito de placas de telecomunicações fabricadas nos EUA, adquiridas pelos russos, e que se suspeitava possuírem um dispositivo que quando acionado, poderia derrubar todo o sistema de telefonia russo. Ainda segundo o autor citado, tal desconfiança não era exclusividade russa, pois o próprio EUA recusou-se a comprar placas eletrônicas de um fabricante de defesa chinês (Huawei), essencialmente pela mesma razão.

Tal situação deixa bem evidente, que a Guerra Cibernética é uma realidade, e que países dependentes da aquisição de tecnologia externa, bem como subordinados à nova ordem comercial imposta pela globalização, devem se preparar para ataques cibernéticos, que já podem até terem sido preparados para ser realizados, quando necessários.

A história do desenvolvimento da doutrina russa, iniciada com a verificação da necessidade descrita anteriormente, foi apresentada por Billo e Chang (2004) e deu-se conforme o descrito a seguir:

A construção doutrinária militar russa iniciou-se com a Revolução em Assuntos Militares[8] (RAM) ocorrida nos anos 80,quando as Forças Armadas Russas, trabalhando conjuntamente com especialistas do setor de Tecnologia da Informação

---

[7] A **Duma** é o nome dado à Assembleia Nacional da Rússia, criada em 1906 pelo Czar Nicolau II, substituída pelo Soviete supremo na sequência da revolução de 1917 e restabelecida com a queda do estado soviético, em 1991.

[8] Revolução em Assuntos Militares, é uma constatação feita por militares que informação e tecnologia de informação devem ser consideradas como armas para atingir os objetivos nacionais pela via militar. (GOLDEBERG, 2005, tradução nossa)

e comunidade acadêmica, desenvolveram uma doutrina de guerra cibernética[9] robusta na qual o arsenal de guerra cibernética, composto de códigos de programas, recebeu uma atenção proeminente.

A literatura aberta atual bem como diversas declarações publicadas por especialistas em inteligência, apontam a Rússia como uma nação-estado que possui habilidades em Guerra Cibernética próxima às dos EUA colocando-a entre as mais desenvolvidas nações em termos de Guerra Cibernética.

> De acordo com a análise oficial americana, a Rússia é um exemplo de um país pesadamente envolvido com o desenvolvimento da sua capacidade em Guerra Cibernética. De quinze critérios enumerados pelo Conselho de Defesa e Ciência americana em seu relatório de proezas técnicas, a Rússia foi listada como tendo capacidade relevante em sete categorias e uma boa capacidade em quatro. Este desempenho continua, mesmo apesar das atuais dificuldades econômicas. (DEFENSE SCIENCE BOARD TASK FORCE, 1996, p. tradução nossa)

Segundo Billo e Chang (2004), a doutrina de Guerra Cibernética russa, aparentemente, parece ser produto do medo da superioridade americana no campo cibernético. Ainda, segundo os autores citados neste, o Ex Ministro da Defesa da Rússia, Sergey Ivanov, disse que o governo russo estava apoiando o desenvolvimento de um regime internacional de leis para prevenir o uso de tecnologia da informação incompatível com o propósito da missão de assegurar a segurança e estabilidade internacional.

Nos anos 80, os militares russos, segundo Billo e Chang (2004), iniciaram um estudo visando a Revolução em Assuntos Militares[10], inicialmente referindo-se à utilização de Comando e Controle eletrônico nas unidades militares e depois na avaliação do impacto de vírus de computadores, e outros tipos de armas cibernéticas, como bombas lógicas, dentre outras.

O setor tecnológico e a comunidade acadêmica em conjunção com os militares russos, desenvolveram uma doutrina em Guerra Cibernética, segundo Billo e Chang (2004), superior a de qualquer outro país, à exceção dos EUA.

Os russos reconheceram que a guerra de informações requer a condução simultânea de medidas ofensivas e defensivas para ser coroada de sucesso, assim

---

[9] Na doutrina oficial, o governo russo, escolheu referir-se à Guerra Cibernética e Guerra da Informação como Operações de Informação.

[10] Revolução em Assuntos Militares, é uma constatação feita por militares que informação e tecnologia de informação devem ser consideradas como armas para atingir os objetivos nacionais pela via militar. (GOLDEBERG, 2005, tradução nossa)

“o fato da Guerra da Informação prover um novo meio de afetar a população civil e militar, modificou os seus princípios, táticas e condições de uso em relação à guerra convencional.” (BILLO e CHANG, 2004).

Ainda segundo Billo e Chang (2004), armas de software receberam uma grande atenção na doutrina russa de Guerra Cibernética. O desenvolvimento e utilização deste tipo de arma exige planejamento de longo prazo, preparo técnico e inteligência sobre alvos, tudo isto possuído por órgãos do serviço secreto russo como a Agência Federal de Comunicações e Informações Governamentais e o Serviço Federal de Segurança da Federação Russa que substituiu a conhecida KGB, e atualmente engloba a agência citada anteriormente.

Portanto a Rússia, após identificar a necessidade de preparo na área de Guerra Cibernética, introduziu-a em sua doutrina, tornando a uma arma poderosa, cujo poder já foi demonstrado.

Numa demonstração da proficiência russa em termos de guerra cibernética, Carr (2009) cita a rapidez com que a Rússia moveu-se da exploração de redes de computadores para o ataque a rede de computadores durante a segunda guerra da Chechênia (1997-2001), em um esforço para controlar o fluxo de informação, colocando diversos *sites* fora do ar.

A evolução militar russa com a inclusão da Guerra Cibernética, ocorreu, como no caso chinês, de uma forma ligada à linha estratégica geral, portanto se no caso chinês a evolução foi seguindo a linha do estratagema, mais voltado para o lado psicológico, no caso russo ela tomou um lado mais voltado ao campo cognitivo.

Tal fato demonstra que uma Força Armada não precisa modificar radicalmente sua filosofia de guerra para incorporar os conceitos de Guerra Cibernética, mas deve adequar-se a esse ambiente, tirando o máximo proveito. A evidência dessa situação foi observada no desenvolvimento da doutrina militar russa, que será tratada na sequência.

Durante os primórdios da inclusão da Guerra da Informação, na doutrina Russa, verificou-se o aparecimento da Fundação para Política Eficiente (FPE), que segundo Carr (2004), foi criada por Gleb Olegovich Pavlovski, nascido em Odessa em cinco de março de 1951.

Pavlovski, ainda de acordo com Carr (2004), se autoidentificava como um tecnologista político, o que faz um perfeito senso nos dias atuais do mundo

conectado. Ele era um tecnologista do oriente considerado um precursor, criando programas para a internet russa nos dias iniciais de existência da mesma.

A FPE era uma força inicial da internet russa. Segundo Carr (2004), o *site* original da FPE, FEP.ru (do inglês Foundation for Effective Politics – FEP), não está mais ativo, porém informações de arquivo mostram o mesmo em atividade entre 1998 e 2007. O *site* influenciava especialistas em operações de *Internet*, provendo exemplos de *sites*, desenvolvidos anteriormente, dando suporte a figuras políticas russas e suas campanhas. “No entanto, artigos contemporâneos da imprensa acusam Pavlovsky de disseminar a desinformação através das mesmas vias.” (CARR, 2009, p. 163, tradução nossa).

Anos mais tarde, segundo Carr (2009), o Kremlin passou a favorecer as editoras Newmedia Stars de Konstantin Rykov’s, bem como o dni.ru, o vzglyad.ru e o portal de vídeo rossiya.ru, tendo Rykov recebido um assento na Duma[11].

Em 2007, Maskim Zharov, um dos autores de *Chronicles of Information Warfare,* segundo Carr (2009), publicou um manual de instruções para *bloggers* que desejassem lutar contra os inimigos da Rússia.

Apesar das trocas de interesse por parte dos governantes, Pavlovsky continuou a ser uma voz influente na política russa. Segundo Carr (2009), sua organização criou a editora Yeropa, que publicou o *Chronicles of Information Warfare,* um livro que cobre informações de como implementar a política do Kremlin através de diversos métodos, incluindo ataques a computadores adversários, explicando como usar a informação como arma para lutar contra os inimigos da Rússia, como a Geórgia.

> Apesar da FPE, não ser parte das forças armadas da Federação Russa, ela é parte da voz oficial do Kremlin e um elemento chave na execução de uma resposta contra um discurso antikremlin, ou ações contra oponentes internos e externos. Desde que Guerra Cibernética é frequentemente categorizada como Guerra da Informação, a FPE é uma importante, pouco conhecida, organização a observar. (CARR, 2009, p. 164, tradução nossa)

Percebe-se que a Rússia percebeu o aspecto cognitivo das questões cibernéticas mais do que as demais nações. Alguns políticos russos sentiram que a desintegração da União Soviética ocorreu devido a ataques cognitivos ou operações

---

[11] A **Duma** é o nome dado à Assembleia Nacional da Rússia, criada em 1906 pelo czar Nicolau II substituída pelo Soviete supremo na sequência da revolução de 1917 e restabelecida com a queda do estado soviético, em 1991.

de informação deliberadas. “Diversos livros russos tratam da Terceira Guerra Mundial como uma guerra da informação na qual o ocidente conquista a União Soviética.” (THOMAS, 2009).

Segundo Leonenko (1995 apud THOMAS, 2009, p. 477), enquanto os chineses utilizam estratagemas para alterar a razão dos responsáveis por decisões, os russos preferem um conceito conhecido como controle reflexivo, um processo em que os atores controladores transmitem aos seus alvos diversos motivos e razões que levem a estes últimos a tomarem decisões sugestionadas pelos controladores.

Segundo Thomas (2009), a tarefa chave do controle reflexivo é localizar o elo fraco do filtro do oponente e explorá-lo. Assim, durante um conflito, os dois oponentes analisam suas próprias ideias e aquelas percebidas nos inimigos e então tentam influenciar um ao outro. Um reflexo refere-se à criação de certo modelo de comportamento no sistema em que se pretende assumir o controle.

O controle reflexivo explora fatores morais, psicológicos e outros fatores como a característica pessoal dos comandantes, assim, em uma guerra, que empregue o controle reflexivo, o lado com maior capacidade de refletir, isto é, com a maior capacidade de imitar ou predizer os pensamentos do outro lado, terá uma maior probabilidade de vitória.

De acordo com Thomas (2009), Leonenko integrou a tecnologia da informação e a teoria do controle reflexivo. Ele notou que o uso de computadores poderia auxiliar na utilização do controle reflexivo, uma vez que a velocidade de processamento dos dados e do calculo das opções poderiam facilitar a transmissão de motivos e bases, pela entidade controladora, para o sistema controlado, que estimulariam a decisão desejada. A grande meta do controle reflexivo é induzir o inimigo a tomar uma decisão desfavorável a ele. Usando tais princípios, talvez por estudar as ações russas, as forças iugoslavas enganaram os sensores da OTAN, nos Balkans, fazendo-a atacar alvos falsos sobre Kosovo.

Finalmente, segundo Leonenko (apud THOMAS, 2009), diversas decisões são tomadas por computadores, assim são feitas automaticamente, sem a intervenção humana, o que indicaria que vivemos em um ambiente muito mais aterrorizante do que se pensa, no qual decisões são tomadas por máquinas incapazes de avaliar o que está ocorrendo e de perceber a reação das pessoas. Assim, a forma de pensar do inimigo é moldada pela inteligência de combate e uma coleção de imagens feitas de conceitos, conhecimento, ideia e experiência.

O conceito de controle reflexivo de Leonenko contém diversos elementos de outro conceito russo, o da arma de informações que “é uma peça especialmente selecionada de informação capaz de causar mudanças em processos de informação de sistemas de informações (físico, biológico, social, etc) de acordo com a intenção de uma entidade utilizando a arma.” (MARKOV, 1996 apud THOMAS, 2009, p. 479, tradução nossa).

Assim, conforme as definições, a arma de informação, assim como o controle reflexivo, pode ser aplicada na modelagem e tomada de decisões de diversos tipos de conflitos, podendo ser usada, também, em processos sociais e sistemas.

Fica evidente, que o caso Russo fornece uma nova perspectiva de análise para a implantação da doutrina de Guerra Cibernética em uma Força Armada, tornando-a uma ferramenta poderosa para consecução dos objetivos finais.

De acordo com Thomas (2009), não existem definições Russas de Guerra da Informação e de Operações de Informações que utilizem o termo cibernético, embora diversos falem sobre informática. Geralmente, teóricos militares Russos vêm tópicos relacionados à informação em duas categorias: informações técnicas e informações psicológicas. A Rússia não separa os tópicos relacionados à informação como a China e os EUA o fazem, como operações psicológicas, operações de redes de computadores, segurança operacional e assim por diante.

Na maioria dos países o aspecto técnico é o de maior interesse, mas na Rússia o aspecto psicológico e o que chama mais atenção. Segundo Prokof’ev (2003 apud THOMAS, 2009, p. 480), a principal ameaça para a segurança de uma nação no século XXI é a segurança psicológica.

Inicialmente a política de Segurança de Informações Russas, conforme Thomas (2009), em contraste à abordagem Chinesa, tinha seu foco no desenvolvimento de uma doutrina de segurança de informações, nas leis de segurança de informações internacionais, no programa Rússia Eletrônica e no estudo de programas cibernéticos americanos, as autoridades russas acompanhavam de perto o desenvolvimento cibernético Americano.

A Doutrina de Segurança de Informações Russa foi desenvolvida no ano de 2000, e segundo Thomas (2009), ela apresenta propósitos, objetivos e direções básicas da política de segurança de informações Russa.

A doutrina Russa, segundo Thomas (2009) é bem abrangente e dentre outros aspectos aborda:

a) os interesses nacionais Russos na esfera de informações;
b) ameaças à segurança de informações;
c) identificação de ameaça internas e externas;
d) discussão a respeito da tensão entre a necessidade da livre troca de informações e a necessidade de restrição à disseminação de informações específicas;
e) discussão à de sistemas de telecomunicações, defesa, legais; e de situações de emergência; e
f) direção para instituições federais detentoras de poder estatal; e o balanço entre interesses individuais, da sociedade e do estado na esfera de informações.

De acordo com Thomas (2009) a doutrina Russa define segurança da informação como a proteção estatal dos interesses nacionais na esfera de informações definida pela totalidade do equilíbrio entre os interesse individuais, sociais e estatais. A segurança de informações na esfera de defesa foi apontada na doutrina e envolve o seguinte:

a) a infraestrutura de informações dos elementos centrais de comando e controle militar e os elementos de comando e controle das ramificações das Forças Armadas e das instituições de pesquisa do Ministério da Defesa;
b) os recursos de informações dos empreendimentos do complexo de defesa e instituições de pesquisa;
c) o software e hardware dos sistemas automatizados de comando e controle das Forças, armamentos e equipamentos militares mobiliados com facilidades computacionais; e
d) recursos de informação, sistemas de comunicação e infraestrutura de informações de outras forças, elementos e componentes militares.

Mais uma vez verificamos as direções políticas da nação, indicando o caminho do preparo cibernético para as forças armadas, que devem estar preparadas para contrapor as ameaças impostas pelo ambiente cibernético, independente da sua direção filosófica estratégica.

Em 2006, analistas Russos defenderam a necessidade da política militar da Federação Russa ser atualizada, tal necessidade, segundo Thomas (2009), ocorreu devido ao risco que a segurança militar passou a correr com o desenvolvimento, a manufatura, introdução e lançamento de armas cibernéticas.

Para os especialistas Russos, segundo Thomas (2009), o uso de armas de informação é uma chave para o sucesso. Estes esforços são mais direcionados para a ruptura das informações adversárias do que para a obtenção da supremacia em informações. Os alvos destas rupturas não são apenas os armamentos e líderes no campo de batalha, mas também o espírito do cidadão médio.

Por fim, o seu talentoso corpo de matemáticos, segundo Thomas (2009), coloca a Rússia em posição de manter seu elevado poder cibernético pelos próximos anos. As Nações-estado devem esperar encontrar a presença eletrônica Russa nos campos de batalha virtual, de forma aberta ou disfarçada por princípios de controle reflexivo. Além disso, a Rússia tem sido agressiva ao impelir o entendimento internacional a respeito do assunto tecnológico da informação.

Assim a Rússia serve não só como exemplo a ser analisado como padrão de inclusão doutrinária da Guerra Cibernética, mas também serve como catalisadora dessa ação por parte dos países que não adotaram a linha de inclusão da Guerra Cibernética em seu pensamento militar, uma vez que podem vislumbra nela um potencial adversário.

Tal necessidade, de contrapor forças antagônicas que levam ao desenvolvimento doutrinário, fica claro na competição entre a Federação Russa e EUA, cuja doutrina será analisada a seguir.

4.3 ESTADOS UNIDOS DA AMÉRICA

Nos anos 90, segundo Rattray (2001), os Estados Unidos entraram em um período cheio de novas oportunidades e desafios, como nos anos 20, o otimismo tecnológico e econômico era novamente ascendente, assim, o explosivo crescimento da computação em rede e de meios revolucionários de telecomunicações transformaram as atividades comerciais e influenciaram a vida diária de diversas pessoas.

Os anos 90, conforme Rattray (2001), também, presenciaram o desenvolvimento de novas possibilidades, totalmente inéditas, para a condução da

guerra através do uso da Tecnologia da Informação. Assim como o Avião criou um novo setor para o combate, o ciberespaço, de forma crescente, começou a servir como local de operações militares. Quanto mais um ator dependia de sua infraestrutura de informação, maior o potencial de esta servir como valoroso centro de gravidade para ataques e defesa.

O ano de 1991 marcou a confluência de eventos centrais para o aparecimento da preocupação americana a respeito da Guerra Cibernética Estratégica. A primeira Guerra do Golfo, denominada por muitos como a primeira Guerra Cibernética, segundo Rattray (2001), proveu um impulso substancial para que a segurança nacional Americana passasse a entender a relação entre o uso da força e a era da informação.

Tal ocasião, não serviu apenas para os americanos como marco da necessidade do domínio da informação nos campos de batalhas, serviu também para todos os países com forças armadas atuantes e comprometidas com o seu desenvolvimento frente os novos desafios.

Porém a preocupação americana com a exploração das telecomunicações e da informação não apareceu repentinamente, já, durante a Segunda Guerra Mundial, o Presidente Roosevelt, segundo Capaso (1997), gerenciava as telecomunicações americanas através do Comitê de Comunicações de Guerra. Até o fim da metade do século, o governo Americano focou-se em garantir que a AT&T provesse uma capacidade de telecomunicações suficiente para atender os requisitos militares, porém sem protegê-la contra ataques externos.

A crescente dependência estratégica Americana na sua infraestrutura de informação, bem como sua vulnerabilidade em telecomunicações, tornou-se de grande preocupação durante a Guerra Fria. Autoridades Americanas tornaram-se bastante preocupadas com a perda, para seus adversários Soviéticos, de “informações econômicas estratégicas sob a forma privada, de dados não classificados a respeito de desenvolvimentos tecnológicos e planos industriais de processos e investimentos” (LIPSCOMB, 1979, p. tradução nossa). Como resultado disto, o Presidente Carter emitiu a Diretiva Presidencial 24 estabelecendo esforços para aprimorar a proteção de informações de segurança nacional e de comércio governamental, tanto classificada como não classificada.

A Guerra Cibernética, segundo Rattray (2001), emergiu no âmbito militar como um conceito fortemente associado à Revolução em Assuntos Militares[12] (RAM). Dois níveis de significativa mudança confrontaram o pensamento militar estabelecido. No curto prazo, a integração de inteligência avançada, vigilância e sistemas de reconhecimento com sistemas d´armas invisíveis, de longo alcance e de precisão deveriam estabelecer o domínio nos futuros engajamentos no campo de batalha tradicional. No longo prazo, pensadores da RAM salientaram a importância de um conceito frouxamente articulado conhecido como Guerra Cibernética**,** enfatizando a habilidade de degradar e até mesmo paralisar um sistema de comando, controle, comunicações e inteligência (C^3I) oponente.

No final dos anos 90, defensores da RAM clamaram pela troca da guerra centrada na plataforma pela guerra centrada em rede para atingir a superioridade de informação. Estes defensores continuaram a focar o "uso de comandantes, atiradores e mídia de redes altamente capacitadas para atingir o poder de uma força verdadeiramente integrada." (CEBROWSKI e GARSTKA, 1998, tradução nossa)

De acordo com Fredericks (1997), o Departamento de Defesa lutou bravamente nos anos 90 com a definição e escopo do que constituiria a Guerra da Informação. A diretiva classificada TS3600.1 desse departamento, intitulada *Information Warfare*, publicada em 1992 proveu o primeiro quadro oficial.

Em 1993, segundo Ratray (2001), o Presidente do Estado Maior Conjunto publicou o *memorandum* ***Command and Control Warfare*** (C2W) que definiu C2W como "a estratégia militar que implementa a Guerra Cibernética no campo de batalha e que integra a destruição física. Seu objetivo é decapitar a estrutura de comando inimiga do corpo de suas forças de combate" (EUA, 1990, tradução nossa). Este *memorandum* salienta tanto ações ofensivas para conquistar a iniciativa quanto à proteção do próprio comando e controle, englobando, para estes fins, operações de segurança, operações psicológicas, dissimulação militar, guerra eletrônica e destruição. (EUA, 1990)

Observa-se, então, a crescente inclusão da Guerra Cibernética na doutrina americana, chegando, nesse ponto, a mesma a ser vista como um meio de

---

[12] Revolução em Assuntos Militares é uma constatação feita por militares que informação e tecnologia de informação devem ser consideradas como armas para atingir os objetivos nacionais pela via militar. (GOLDEBERG, 2005, tradução nossa)

levar o inimigo à paralisia, e de atingir os Centros de Gravidade, consequentemente colocando o ambiente cibernético no topo da discussão militar.

> Guerra Cibernética ofensiva começou a ser vista após a Guerra do Golfo como um meio potencial de minimizar a exposição e o dano colateral em situações que de outro modo exigiriam o uso de forças convencionais. Discussões sobre o uso de técnicas digitais de Guerra de Informações para atacar alvos além do campo de batalha tradicional começaram a ocorrer fora do governo. Trabalhos, como o de Alvim e Heidi Toffler (Guerra e Antiguerra: Sobrevivência na Aurora do Terceiro Milênio), receberam atenção crescente dentro dos círculos de segurança nacional. Os Toffler identificaram uma grande variedade de desafios militares apresentados pela era da informação, incluindo o ataque digital para romper a infraestrutura de informação e a gestão da percepção, como meios disponíveis para adversários estatais e não estatais. (RATTRAY, 2001, p. 316, tradução nossa).

No contexto da intensificação dos debates Americanos a respeito da eficácia de sanções aplicadas, especificamente ao Iraque, os analistas de segurança nacional começaram a identificar diretamente como a Guerra Cibernética poderia ser usada para aguçar a dor infligida nos adversários, atacar alvos como os dados de produção e marketing de uma empresa, acessar contas bancárias (que poderiam ser esvaziadas) e negar acesso a estas, causando um efeito devastador.

Dentro do campo militar, especificamente, durante os anos oitenta as Forças Armadas, tanto dentro do Estado Maior Conjunto como individualmente, formularam doutrinas para guiar as operações envolvendo Guerra Cibernética.

A Força Aérea, conforme Rattray (2001), foi a primeira força a lidar com a formulação de uma doutrina voltada para a Guerra Cibernética. A Força Aérea identificou a Guerra Cibernética como prioridade em abril de 1993, depois da emissão por parte do Departamento de Defesa de sua diretiva inicial.

Assim a Força Aérea renomeou o Centro de Guerra Eletrônica da Força Aérea para Centro de Guerra da Informação da Força Aérea (AFIWC, da sigla em inglês), designando para esse centro, segundo Rattray (2001), o foco no domínio da informação no campo de batalha.

Tal situação ocorreu com mais intensidade no âmbito da Força Aérea, devido ao fato dessa ser a mais dependente, nos dias atuais, do ambiente cibernético, e por ser ela, também, a que incorporou em maior intensidade os conceitos apresentados de Fuller, Boyd e Warden.

Portanto, tornou-se fator determinante à Força Aérea Americana, e todas aquelas que operam similarmente à sua doutrina, adotar ações direcionadas ao domínio do espaço cibernético.

Em uma cúpula de Oficiais Generais de quatro estrelas da Força Aérea, em agosto de 1994, segundo Rattray (2001), os mesmos concordaram que as operações ofensivas, em termos de Guerra Cibernética, seriam multiplicadoras para futuras forças, porém sérias preocupações defensivas já se faziam presentes. A maior parte da discussão da Força Aérea a respeito do assunto centrou-se na importância da Guerra Cibernética no aprimoramento da capacidade das forças Americanas de explorar as vantagens da tomada de decisão no campo de batalha provendo um melhor suporte às forças amigas enquanto rompe os sistemas inimigos.

A Força Aérea formalizou os seus primeiros esforços nos fundamentos de sua doutrina com a publicação, pelo Departamento da Força Aérea, do artigo *Cornestones of Information Warfare* em agosto de 1995. Segundo Henning (1997), este artigo descreveu a Guerra Cibernética de uma maneira que lidava com a informação propriamente dita como um setor separado, arma poderosa e alvo lucrativo.

Ainda, de acordo com Henning (1997), aquele artigo recomendou que a Guerra Cibernética não fosse incorporada como uma missão de uma tarefa[13], aproximando a Guerra Cibernética ao conceito de tarefa[14] para que a força aérea pudesse cumprir sua missão de controle da soberania do espaço aéreo[15] além da aplicação, aprimoramento e suporte à Força. O artigo identificou a possibilidade da utilização de um ataque digital estratégico de forma análoga ao ataque aéreo estratégico.

O progresso dos esforços da Força Aérea para integrar a Guerra Cibernética em sua coluna vertebral foi refletido por sua Doutrina Básica no ano de 1997 quando a mesma enunciou o seguinte:

---

[13] Os termos aqui utilizados, para facilitar o entendimento e evitar erros de interpretação, foram adaptados à Doutrina Básica da Força Aérea Brasileira (BRASIL, 2005), embora nas fontes de pesquisa tenham sido utilizados termos diferentes, devido às diferenças de nomenclatura doutrinária.

[14] Os termos aqui utilizados, para facilitar o entendimento e evitar erros de interpretação, foram adaptados à Doutrina Básica da Força Aérea Brasileira (BRASIL, 2005), embora nas fontes de pesquisa tenham sido utilizados termos diferentes, devido às diferenças de nomenclatura doutrinária.

[15] Os termos aqui utilizados, para facilitar o entendimento e evitar erros de interpretação, foram adaptados à Doutrina Básica da Força Aérea Brasileira (BRASIL, 2005), embora nas fontes de pesquisa tenham sido utilizados termos diferentes, devido às diferenças de nomenclatura doutrinária.

> A guerra é normalmente associada com diferentes ambientes como ar, terra, mar e espaço. Adicionalmente, a informação agora é considerada outro ambiente, no qual diversos aspectos da guerra podem ser conduzidos. A Força Aérea dos Estados Unidos conduz guerra aérea, espacial e de informações para alcançar seus objetivos de Comando de Força Conjunta (JFC [da sigla em inglês]). Adicionalmente, forças aéreas e espaciais cumprem uma grande variedade de funções relacionadas á informação, classicamente descritas como inteligência, vigilância e reconhecimento (ISR, [da sigla em inglês]). Estas funções podem ser conduzidas independentemente de operações terrestres e navais e podem complementar, apoiar ou ser apoiada por operações terrestres e navais. (EUA, 1997, tradução nossa). (EUA, 1997)

A Doutrina Básica da Força Aérea dos Estados Unidos (EUA, 1997) continuou a destacar a tomada de decisões contra os adversários através de um comando e controle, mais efetivo. Ela descreve, ainda, a Guerra Cibernética envolvendo diversas atividades, como guerra psicológica, dissimulação militar, combate eletrônico e ataques tanto físicos como cibernéticos.

Exemplos de Alvos de Guerra Cibernética

Liderança
- Pessoal Chave
- Apoio de PDA
- Comunicação estratégica
- Força de Base

Infraestrutura Civil
- Comunicações (*links*/nós)
- Indústria
- Finanças
- População

Infraestrutura Militar
- Comandantes
- Comunicação de C2 (*links*/nós)
- Tropas
- Coletores de inteligência

Sistemas de armas
- Navios / Aviões
- Artilharia
- Munições guiadas de precisão
- Defesa Aérea

Figura 7: Alvos de Guerra Cibernética.
Fonte: Rattray (2001, p. 328, tradução nossa).

O papel do Estado Maior Conjunto na formação doutrinária aprimorou-se com a publicação de *Information Warfare – Strategy for Peace – The Decisive Edge for War* (EUA, 1996). Neste documento está registrado que a Guerra Cibernética aplica-se a todas as fases e escopo de operações militares, bem como a todos os níveis da guerra.

Tal situação evidenciou que a doutrina militar americana incorporou a Guerra Cibernética, não apenas isoladamente por parte de suas forças, mas de forma integrada, através de seu Estado Maior Conjunto em consonância com o direcionamento moderno de operações conjuntas.

Descrevendo a possibilidade de Guerra Cibernética ofensiva, o Estado Maior Conjunto citou o seguinte:

> Guerra Cibernética Ofensiva emprega disciplinas tradicionais de gestão de percepção como operações psicológicas e ataques a sistemas de informação para produzir efeitos sinérgicos contra elementos remanescentes de sistemas de informações adversários, *links* de transferência de informações e nós de informações. (EUA, 1996, tradução nossa). (EUA, 1996)

Os exemplos de alvos de Guerra Cibernética, delineados no documento citado no parágrafo anterior, estão retratados na Figura 7, indicando claramente o desejo de travar guerra de informações estratégica.

Na era industrial pós Segunda Guerra Mundial, a superioridade militar americana, segundo Barry e Zimet (2009), estava estruturada nos seguintes fatores:

a) sua força industrial;
b) tecnologia superior em armas e comando,controle, comunicações, computação, inteligência, vigilância e reconhecimento (C4IVR); e
c) uma robusta infraestrutura militar.

Os americanos não puderam permanecer inertes com a mudança da sociedade e a chegada da era da informação. Foram obrigados a adaptar o seu pensamento militar, servindo de exemplo a todos os países inseridos no contexto mundial moderno.

Com a passagem da era industrial para a era da informação, conforme Barry e Zimet (2009), a difusão da tecnologia da informação tendeu a modificar os parâmetros de combate. Armamentos de precisão e Operações Centradas em Redes (OCR) deram aos Estados Unidos uma vantagem decisiva nos campos de batalha, porém, na guerra irregular trouxe um revés, pois, como um grande empreendedor da infraestrutura do ciberespaço os EUA passaram a estar abertos a todos que possuam meios para acessar o tal ambiente.

O ciberespaço, de acordo com Barry e Zimet (2009), tornou-se um fundamento sensível para a estrutura militar nacional e internacional, pois os militares possuem seus tanques, navios e aeronaves, mas tem limitado impacto na conectividade provida por meios comerciais da qual a supervia expressa de informações é dependente.

A Figura 8 caracteriza a conectividade do *Backbone* de comunicações globais demonstrando que apenas uma pequena parte do tráfego é realizada por infraestrutura fechada a acessos exteriores e que principalmente, há uma interconexão entre o tráfego de dados militares e a estrutura comercial, bem como a estrutura de forças aliadas.

O espaço cibernético, cada vez mais, foi ganhando importância, dentro das forças armadas americanas culminando com o aparecimento do conceito de Poder Cibernético Militar, descrito a seguir:

> Poder Cibernético Militar é o domínio do ciberespaço para a aplicação de conceitos operacionais visando cumprir missões e objetivos militares, incluindo assistência humanitária e a desastres, alcançar estabilidade, segurança, transição e reconstrução, operações de influência e combates. (BARRY e ZIMET, 2009, p. 285, tradução nossa)

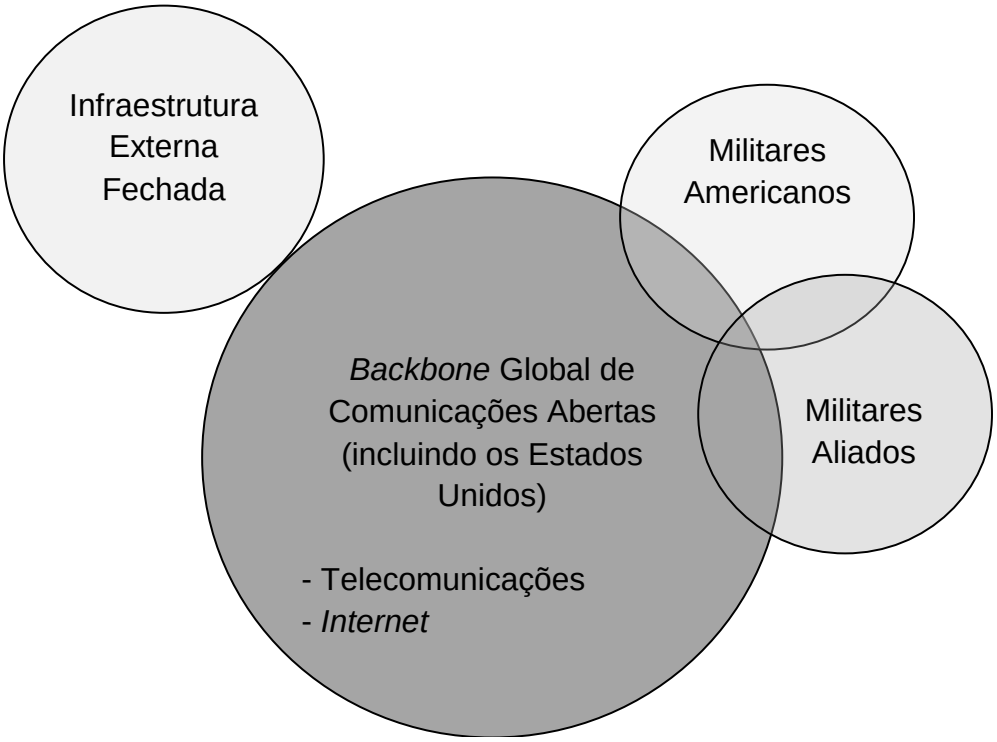

Figura 8: Conectividade do Espaço Cibernético.
Fonte: Barry e Zimet (2009, p. 288, tradução nossa).

Normalmente, segundo Barry e Zimet (2009), o Poder Cibernético Militar é utilizado para dar apoio a outros domínios como o marítimo, o aéreo e o terrestre, porém, provavelmente, em um futuro próximo o Poder Cibernético Militar Conjunto será utilizado para obter a prevalência contra um inimigo, exclusivamente em seu domínio cibernético.

A Figura 9 demonstra, de forma adicional, esse conceito. Nota-se que a base do triangulo apresenta o domínio do ciberespaço, incluindo tipos de redes (aberta e fechada) e seus requisitos. O segundo nível apresenta funções, conceitos e estratégias habilitadas pelo conceito operacional de poder militar cibernético, incluindo operações centradas em redes e operações de informação, além de funções administrativas. O terceiro nível demonstra a utilização do poder cibernético em todas as fases de um plano de campanha conjunto.

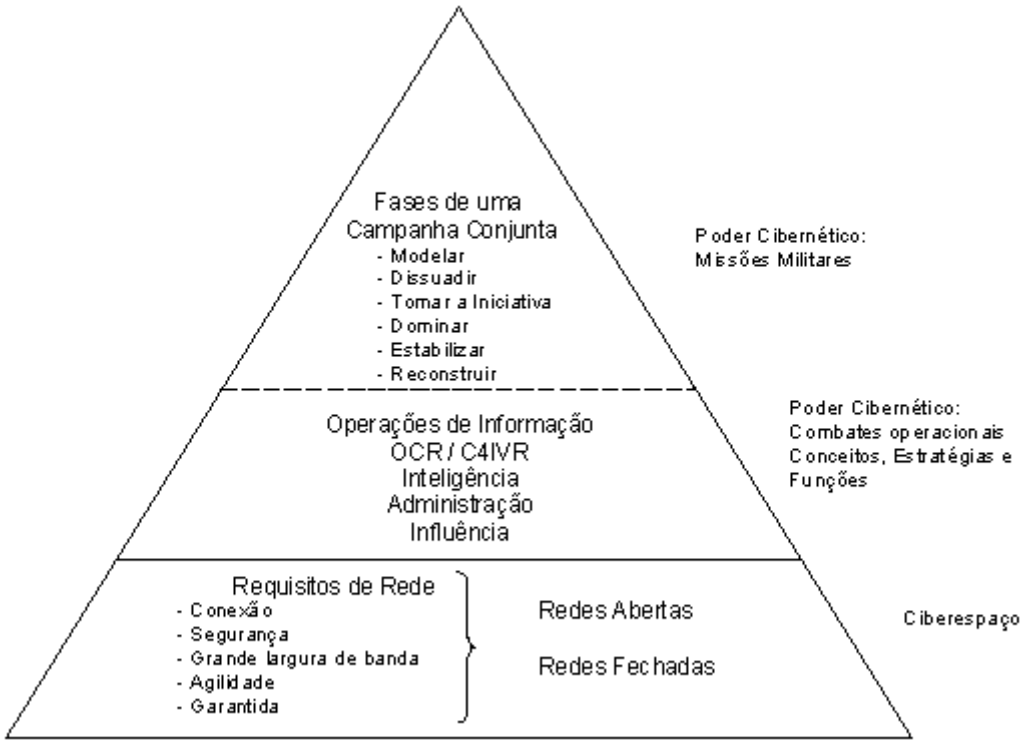

Figura 9: Poder Cibernético Militar / Suporte do ciberespaço para conceitos operacionais, estratégia e funções.
Fonte: Barry e Zimet (2009, p. 290, tradução nossa).

O Departamento de Defesa (EUA, 2005), na definição do escopo das operações realizadas por forças conjuntas no período de 2012 a 2020 definiu ações fundamentais a serem tomadas, que traduzidas, segundo Barry e Zimet (2009), para o espaço cibernético são:

a) operações de informação;
b) OCR, um conceito de guerra transformador, cujo escopo, doutrina e tecnologia estão em desenvolvimento e cuja ampla utilidade é ainda objeto de debates;
c) funções normais, de rotina de negócios e administrativas usando ferramentas cibernéticas;
d) operações de inteligência usando ferramentas cibernéticas; e
e) operações de influência utilizando ferramenta cibernéticas.

Em comparação às doutrinas chinesa e russa apresentadas anteriormente, percebe-se que a incorporação da doutrina americana aos conceitos de Guerra Cibernética é feita de forma mais pragmática, refletindo a filosofia estratégica americana de ataques rápidos e decisivos apoiado em seu poderio militar.

Seguindo essa abordagem prática, desenvolveu-se o conceito de Operações Centradas em Redes (OCR) representando um poderoso conjunto de conceitos de combate e capacidades militares que possibilitam a combatentes tirar total vantagem de toda informação disponível. Uma de suas definições é a seguinte:

> A condução de operações militares utilizando sistemas de informações em rede para gerar uma Força Militar flexível e ágil que atue sob uma orientação de um comandante comum, independente do espaço geográfico ou disposição organizacional dos elementos individuais e na qual o foco do combatente é mantido à distância de preocupações individuais, unitárias e de plataformas para dar prioridade para a missão e responsabilidades da equipe, grupo de trabalho ou aliança. (FEWELL e HAZEN, 2003, tradução nossa). (FEWELL e HAZEN, 2003)

Conforme Alberts, Garstka e Stein (1999) os princípios das OCR, como articuladas pelo Departamento de Defesa, são:

a) uma robusta força interligada em rede aumentará o compartilhamento de informações;
b) compartilhamento de informações aprimorará a qualidade da informação e a consciência situacional compartilhada;
c) consciência situacional compartilhada habilitará colaboração e autossincronização além de melhorar a sustentabilidade e velocidade do comando; e
d) esses, por sua vez, aumentarão drasticamente a eficácia da missão.

Segundo Barry e Zimet (2009), esse princípios irão possibilitar a atuação das forças dentro de um desempenho e velocidade que irão interferir no ciclo de observação, orientação, decisão e ação (OODA) do adversário.

No sentido de tornar factível a implementação do conceito de OCR, segundo Barry e Zimet (2009), o Departamento de Defesa está obtendo verdadeiras integrações entre as diversas Forças e trouxe a OCR para o centro emergente da estratégia Americana. Porém, embora esforços e recursos estejam sendo aplicados neste sentido, muitos dos compartilhamentos de dados e comunicações (táticos, operacionais e estratégicos) no Iraque e Afeganistão permanecem sendo realizados de forma hierárquica, usando radiodifusão e limitando os usuários. “O Departamento de Defesa deverá ver essa meta [da OCR] tornando-se realidade, em uma década ou mais.” (BARRY e ZIMET, 2009, p. 294, tradução nossa).

Além das barreiras culturais e diferenças organizacionais, a complexidade da infraestrutura de informação envolvida é uma realidade presente, segundo Barry e Zimet (2009), os sistemas de dados do Departamento de Defesa chegam a cerca

de 3,5 milhões de computadores, 10.000 redes locais de computadores, 1.500 bases em 65 países conectados por 120.000 circuitos de suporte de telecomunicações, 35 sistemas primários de rede sobre 3 arquiteturas baseadas em roteamento, transmitindo informações ostensivas, secretas e ultrassecretas.

Além de toda esta miríade, apresenta-se o maior desafio à tecnologia de rede que são os combatentes, desdobrados nas forças naval, terrestre, aérea e espacial realizando missões por todo o mundo, e seu suporte de integração a inteligência. Todos esses meios sob o manto da OCR reflete a Rede de Informações Global (GIG, na sigla em inglês), que é o grande desafio do Departamento de Defesa para as próximas décadas. Tal desafio já consumiu bilhões de dólares e vários outros ainda serão gastos.

Como pode ser observado, o investimento em OCR exige somas vultosas, o que cria a exigência de países com menor poder econômico criarem soluções alternativas que possam fornecer meios de usufruir as benesses deste modo de combater a um custo acessível e factível.

Para Kramer (2009), OCR é uma abordagem fundamental tomada pelas Forças Armadas Americanas, que tem obtido grandes sucessos em sua utilização, porém, gera a seguinte questão: Focando tão pesadamente nas capacidades centradas em redes, não estará os Estados Unidos criando vulnerabilidades que poderão ser exploradas por seus oponentes em seu detrimento?

Desde a Guerra do Golfo em 1991, segundo Kramer (2009), as forças convencionais Americanas, que estão fundamentadas na centralização de redes, tornaram-se extremamente poderosas, o que leva a seus inimigos a levarem em conta a utilização de meios assimétricos no caso de conflito com os EUA, e nesse sentido ataques a redes de computadores, tanto militares como civis, podem ser essa assimetria.

Uma pergunta levantada por Libicki (2009) foi: Poder Cibernético, particularmente o militar, é relevante? Embora tal pergunta possa parecer estranha, Libicki (2009) argumenta que o Poder Aéreo nos seus primórdios também sofria fortes indagações, pois para provar sua utilidade, naquela época, e ainda nos dias atuais, necessitava demonstrar sua influência para as forças de superfície.

De forma análoga, o Poder Cibernético, necessita, nos dias atuais, demonstrar sua real influência: “Se controle, influência ou competência no meio cibernético tiverem pouco haver com o emprego do poder militar em setores

convencionais, então, ninguém necessitará do Poder Cibernético, exceto, talvez, como fanfarronice.” (LIBICKI, 2009, p. 275, tradução nossa).

A interligação em rede parece ser a essência do espaço cibernético por duas razões: primeiro porque cibernético refere-se a controle, e o controle requer *feedback*; segundo, porque espaço assume o meio no qual há movimento omnidirecional, em contraste com o fluxo monodirecional caracterizado pelos encanamentos de água. “Em outras palavras, se não houver interatividade, não haverá nenhum ciberespaço.” (LIBICKI, 2009, p. 276, tradução nossa).

> Esta distinção é crucial e normalmente ignorada. Muitos defensores da transformação militar através da interligação de redes atribuem poderes mágicos para seus aspectos de interatividade, argumentando que a interligação permitirá comando e controle mais ágil, possibilitando aos combatentes realizarem seu ciclo de observação, orientação, decisão e ação mais rapidamente do que os inimigos, ou autossincronização, eliminando a necessidade de comando e controle hierárquico e facilitando a tática superior do enxame [conforme preconizado pela guerra centrada em redes[16]], assim trazendo o poder para o cume. (LIBICKI, 2009, p. 276, tradução nossa)

Para Libicki (2009), esses efeitos não seriam possíveis se o único resultado obtido pela interligação de redes das Forças Armadas fosse a recepção mais rápida de informações, o que poderia ser obtido por diversas formas de difusão, não necessariamente a cibernética.

Nesse sentido, para verificar a questão central da efetividade da utilização do Poder Cibernético com a interligação em rede, para Libicki (2009), é necessário basear-se em resultados de experiências, muito mais do que resultado de combates recentes, pois, apesar da discussão a respeito da Revolução em Assuntos Militares[17] (atualmente chamada de transformação), a digitalização das Forças Armadas tem caminhado a passos lentos.

Soldados na invasão do Iraque, segundo Talbot (2004), que operassem abaixo do nível de comando de companhia tinham pouca ou quase nenhuma conectividade digital; “Eles, costumeiramente, tomavam conhecimento sobre os inimigos da forma tradicional, ou seja, indo ao encontro deles.” (TALBOT, 2004, tradução nossa). (TALBOT, 2004, p. tradução nossa)

---

[16] Para mais detalhes sobre Guerra Centrada em Rede ver Fewell e Hazen (2003) e Cebrowski e Garstka (1998).

[17] Revolução em Assuntos Militares é uma constatação feita por militares que informação e tecnologia de informação devem ser consideradas como armas para atingir os objetivos nacionais pela via militar. (GOLDEBERG, 2005, tradução nossa)

Esse questionamento levantado acerca da real validade do Poder Cibernético serve como alerta aqueles países em busca de sua capacitação nessa área, que, embora necessária, não é mágica, deve vir decorrente de profundo estudo e pesquisa seguida de um rigoroso processo de avaliação.

Nesse sentido, nas forças armadas americanas, experiências têm sido feitas com a finalidade de verificar a efetividade da Guerra Centrada em Redes. Duas delas foram, segundo Libicki (2009), particularmente produtoras de efeitos quantitativos a respeito da efetividade militar: O experimento da *Striker Brigade Combat Team* (SBCT) e do *Joint Tactical Information Distribution System* (JTIDS), também chamado Link-16.

A SBCT, também conhecida como Brigada de Ataque, segundo Gonzales (2005b), é uma das mais novas unidades do Exército Americano. Na composição desta unidade estão intrinsecamente incluídas capacidades de comando e controle e comunicações avançadas e, talvez, os mais importantes elementos desta Brigada, ou seja, sua nova concepção operacional e sua estrutura organizacional.

A SBCT, segundo Gonzales (2005b) utiliza um conceito de Centralização em Rede que se aproxima bastante do conceito de OCR, além de apresentar uma estrutura organizacional inovadora.

Essa inovação é observada pela presença de um Esquadrão de Reconhecimento, Vigilância e Aquisição de Alvos, uma companhia orgânica de inteligência militar e outras capacidades para gerar a sua própria consciência situacional e para rapidamente realizar a fusão de sensores de dados e relatórios possibilitando a geração de consciência situacional, de alta qualidade, a respeito do inimigo.

A experiência da SBCT, basicamente, consistiu na comparação de desempenho entre uma Brigada de Ataque e uma Brigada de Infantaria Leve (Bda Inf L)[18] – força padrão do atual exército americano. Segundo Libicki (2009), as diferença de desempenho foram dramáticas, e, algumas, são apresentadas a seguir:

---

[18] Abreviatura prevista no Manual de Abreviaturas, Siglas e Símbolos do Ministério da Defesa Brasileiro (BRASIL, 2008b).

a) a Bda Inf L foi capaz de identificar menos de 10% das forças com as quais combateu, antes do engajamento, enquanto a SBCT identificou 80%;
b) decisões que levavam 2 dias para serem tomadas pela Bda Inf L, tomaram três horas da SBCT;
c) a SBCT causou 10 vezes mais vítimas; e
d) no final, a SBCT obteve sucesso em conquistar a cidade atacada, enquanto a Bda Inf L falhou na conquista.

Embora os resultados apresentados, indiquem a superioridade da Brigada de Ataque, Libicki (2009) chamou atenção para o fato de que “a vitória favorece os maiores Batalhões” (NAPOLEÃO BONAPARTE apud LIBICKI, 2009), o que foi observado nesta experiência, não apenas pela superioridade numérica do efetivo SBCT, mas também pela superioridade qualitativa em relação aos seus equipamentos.

Segundo apresentado por Libicki (2009), a SBCT possuía maior número de atiradores de elite, veículos de transporte em maior quantidade, veículos com maior poder de fogo e, principalmente, maior número de unidades de reconhecimento, portanto, embora tenha ficado clara a superioridade do poder da SBCT, ainda não foi conclusiva a medida da participação do conceito de OCR em sua composição.

A experiência do JTIDS, segundo Gonzales (2005a), consistiu na realização de missões de combate entre aeronaves F-15, efetuando missões apoiadas apenas em comunicações de voz, e F-15, utilizando o JTDIS, que consiste em um sistema que permite link de dados entre os diversos elementos envolvidos nas operações.

Os resultados obtidos nesta experiência, que contou com cerca de 12.000 surtidas de treinamento, segundo Libicki (2009), foram menos expressivos, talvez porque a plataforma utilizada, F-15, possua embutida alta tecnologia, além de operações aéreas serem realizadas em grande velocidade não deixando margens a grandes diferenças em termos temporais.

O resultado obtido, diferente da razão 10 para 1 da experiência da SBCT, foi de 2,6 para1 a favor dos F-15 equipados com o JTDIS. Segundo Libicki (2009), os pilotos envolvidos, apontaram alguns fatores que levaram aos mesmos a obter esta vantagem, conforme descrito a seguir:

a) consciência situacional individual e compartilhada, sobre o inimigo, mais completa e adquirida com maior rapidez;
b) uma superioridade em termos de informação, ao conhecer as formações inimigas com maior velocidade e profundidade;
c) maior tempo de decisão disponível para os pilotos, líderes e alas, possibilitando maior dedicação ao voo propriamente dito;
d) obter o conhecimento antes dos engajamentos;
e) maior habilidade de se autossincronizar, atuando como um enxame, “formulação clássica da centralização em rede” (LIBICKI, 2009, p. 282, tradução nossa);
f) melhor geometria de interceptação;
g) maior letalidade do tiros de mísseis; e
h) mais tiros por engajamento.

> É razoável acreditar que a habilidade de “ver” o alvo com maior velocidade e mais cedo no ciclo de engajamento tem um efeito apreciável na eficácia da missão. Porem é certamente plausível que o conhecimento extra que foi fornecido ao piloto apontaria os mesmos efeitos se fossem fornecidos por grande largura de banda ou por fusão de dados. (LIBICKI, 2009, p. 283, tradução nossa)

Segundo Libick (2009), os resultados dos testes a respeito da efetividade da OCR ainda não são conclusivos, algo que, ocorreu também com o Poder Aéreo, que, até os dias de hoje, ainda não chegou a resultados em termo de custo e benefício sobre a morte de 50.000 pessoas, pertencentes à Oitava Força Aérea, durante a Segunda Guerra Mundial.

Independente da conclusão a respeito da contribuição das Operações Centradas em Redes, as Força Armadas Americanas continuam seu trabalho pelo desenvolvimento de sua capacidade cibernética, conforme pode ser observado na Figura 10 que mostra os programas cibernéticos das diversas Forças Singulares dos EUA.

Segundo Barry e Zimet (2009) a Força Aérea dos Estados Unidos, é a força americana que mais tem atuado e avançado na área cibernética, chegando a colocar o Poder Cibernético em igualdade de posição com o Poder Espacial e o Combate Aéreo, considerando o espaço cibernético como uma quinta dimensão.

A Força Aérea considera, segundo Barry e Zimet (2009), a superioridade do espaço cibernético como um pré-requisito para operações de combate militares em todos os domínios.

Força	Conceitos	Aquiteturas	Sistemas	Organização
Força Aérea	Espaço Cibernético como um domínio de combate	C2 Constellation	Assurance, Data integration, global information grid (GIG)	Cyberspace Command
Exército	Informação e cognição como um domínio	LandWarNet	Future Combat Systems, Warfigther Information Network-Tactical, GIG	1st Information Operations Command, Network Enterprise Technology Command
Marinha	Operações de Informação, operações Centradas em Rede	FORCEnet	Navy MarineCorps Intranet (NMCI), GIG	Naval Network Warfare Command
Corpo de Fuzileiros Navais	Operações Centradas em Rede e Guerra	Marine Air Ground Task force – Information Operations	NMCI, GIG	Marine Corps Systems Command

Figura 10: Sumário de programas cibernéticos da Forças Armadas dos Estados Unidos.
Fonte: Barry e Zimet (2009, p. 301, tradução nossa).

Tal afirmação fornece um requisito a ser incluído por Forças Aéreas desejosas de incluir a Guerra Centrada em Rede em sua doutrina, pois, por se tratar de operação conduzida no espaço cibernético, necessita da superioridade nesse ambiente para garantir as operações nos demais meios, podendo tal afirmativa ser comparada de forma análoga com a necessidade da superioridade aérea exigida nas operações convencionais da Guerra Cinética.

Segundo Barry e Zimet (2009), a Força Aérea Americana, considera cinco corolários, chamados de **Cinco Mitos**, para o espaço cibernético:

> - O coletor de informações e o serviço provedor de informações devem ser funções organizacionais separadas e não conjuntas.
> - O domínio do ciberespaço vai bem além da Internet. A Força Aérea considera o ciberespaço um domínio físico, através da interligação entre o espectro eletromagnético e sistemas eletrônicos, ao invés de um domínio virtual.
> - A batalha para obter a superioridade cibernética em qualquer conflito deverá ser travada em uma rede distribuída ao invés de apenas em uma localização na qual poderia estar um elemento de coordenação central.
> - O controle dos efeitos gerados por armas cibernéticas são controláveis, e o desafio de atingir alvos e efeitos colaterais não são diferentes do que os criados por explosivos e meios destrutivos cinéticos.
> - A defesa do domínio cibernético requer uma abordagem holística da rede ao invés de apenas um aumento de segurança em cada nó individual. (BARRY e ZIMET, 2009, p. 300, tradução nossa)

Finalmente, como demonstração clara da importância dada pela Força Aérea Americana, com relação à Guerra Cibernética, segundo Barry e Zimet (2009), foi a criação provisória do Comando do Espaço Cibernético como a 8ª Força Aérea, posteriormente transferida para a 24ª Força Aérea, ativada em 18 de agosto de 2009, como parte do Comando Espacial da Força Aérea, responsável por operações cibernéticas, com a missão de efetuar o preparo para travar guerras no espaço cibernético defendendo as redes de computadores nacionais, executando operações criticas e atacando redes de computadores adversárias.

É notório o desenvolvimento dos EUA nas questões relacionadas à Guerra Cibernética, que se encontra profundamente incluída no âmbito de sua doutrina militar, fornecendo ferramentas para, de forma sinérgica, aumentar o já vasto poder militar americano.

Como pôde ser observado, cada um dos países analisados possuem estratégias diferentes na abordagem da Guerra Cibernética, porém em uma verificação holística consegue-se perceber pontos de congruência entre as diversas abordagens, os quais identificam o cerne da implantação da doutrina de Guerra Cibernética. Esses pontos focais serão tratados no próximo tópico.

4.4 PONTOS FOCAIS DE GUERRA CIBERNÉTICA NA CHINA, RUSSIA E EUA

A análise do caso Americano, Chinês e Russo fornece uma ferramenta útil para identificar o estágio atual da Guerra Cibernética. Isso ocorre, pois durante essa analise ficaram evidenciados alguns pontos em comum referente a estes países, e que servem para nortear a condução da Guerra Cibernética por parte outros países, servindo como pontos focais, conforme descritos a seguir:

a) ênfase na formação de pessoal especializado e capacitado na área de Guerra Cibernética, que em posse de uma tecnologia adequada e de uma estruturação organizacional, tornam-se um força militar a ser levada em consideração.
b) a Guerra Cibernética foi incluída nas doutrinas militares e faz parte de suas operações militares. Estes países já realizaram e realizam atividades de emprego real da Guerra Cibernética em consonância com suas atividades militares tradicionais, evidenciando a importância do assunto para o campo militar;
c) a Guerra Cibernética, embora de formas diferentes, é uma ferramenta no posicionamento doutrinário militar desses países. A china utiliza a Guerra Cibernética como uma forma para auxiliar na aquisição de sua posição emergente no atual status mundial, e, assim como a Rússia, como uma forma de levar uma guerra assimétrica a um adversário mais forte. Já os EUA, enxergam a Guerra Cibernética como uma forma de manter a sua hegemonia militar. Assim fica evidente que, em todos os casos, a Guerra Cibernética está sendo utilizada como ferramenta para a consecução dos objetivos nacionais.
d) todos estes países vislumbram os conflitos futuros como limitados, portanto o domínio dessa forma de lutar mostra-se como alternativa viável de poder;
e) o comando e controle das modernas forças armadas são dependentes do ambiente cibernético que têm o seu potencial de operação evidentemente elevado, porém acabam por servir como alvo, uma vez que a interferência no ciclo OODA poderá trazer uma consequente paralisia;

f) a Guerra Cibernética reflete a doutrina estratégica de cada país, sendo mais voltada ao aspecto psicológico na China, ao aspecto cognitivo na URSS e ao aspecto pragmático dos EUA;
g) a melhor forma de conduzir uma defesa cibernética é a preventiva, e deve-se dar ênfase às atividades ofensivas;
h) existe um grande desafio a ser levado em conta, que é a integração entre a doutrina da Guerra Cibernética e a adotada tradicionalmente pelas forças armadas;
i) a competição gerada pela necessidade de melhor colocar-se em relação a seus adversários potenciais têm levado ao desenvolvimento da Guerra Cibernética nesses países;
j) a Guerra Cibernética é levada como uma alternativa ao confronto cinético direto, atuando de forma sinergética em relação aos poderes militares tradicionais, terrestre, naval e aéreo;
k) existe uma grande preocupação nacional quanto a defesa cibernética, o que ocorre devido ao aumento crescente da dependência desses países com relação à tecnologia da informação de forma abrangente em sua sociedade, aumentando sua vulnerabilidade;
l) o ambiente cibernético é tratado como um quinto ambiente. Neste, os combates podem ser travados, vindo a se comparar ao ambiente terrestre, naval, aéreo e espacial;
m) existe a necessidade da aquisição da superioridade no ambiente cibernético, a fim de se garantir uma adequada situação de segurança que habilite a liberdade de ação nos demais ambientes;
n) a Guerra Cibernética é utilizada para aumentar ainda mais o diferencial de poder com relação a adversários mais fracos;
o) a Guerra Cibernética pode ser utilizada para implementar um desequilíbrio de forças;
p) a Guerra Cibernética pode ser utilizada para contrapor um situação assimétrica de inferioridade de força; e
q) a Guerra Cibernética é fruto de profundos estudos para a sua sistematização e sua utilização, refletindo em grande participação acadêmica neste preparo;

Portanto fica evidenciado que embora operem de formas diferentes, existem pontos comuns nas doutrinas militares desses três países que acabam evidenciando a realidade e importância do tema Guerra Cibernética para o meio militar utilizá-la como ferramenta para auxílio da busca dos objetivos políticos.

Com a identificação dos pontos focais referente à Guerra Cibernética, nesses países, que se encontram mais adiantados nesse quesito, pode-se, agora analisar os dados obtidos, conforme apresentado no próximo capítulo.

5 METODOLOGIA

O assunto Guerra Cibernética é algo relativamente novo no âmbito das Forças Armadas e, como não poderia deixar de ser, coberto de crenças e misticismos que cercam todos os ramos do conhecimento ainda não explorados com profundidade.

Assim, procurou-se estudar a Guerra Cibernética que, por ser uma atividade nova e estar ligada a uma tecnologia em constante evolução, ainda apresenta conceituações não sedimentadas que necessitam de um maior conhecimento.

Para explorar o tema, foi necessário realizar pesquisas em diversos livros e em artigos científicos que abordassem o assunto. As principais obras utilizadas como fontes de estudos foram as escritas por Armistead (2004), Carr (2009), Fuller (1926), Kramer, Starr e Wentz (2009), Rattray (2001), Uda (2009) e Warden (1995), dentre outras.

O material consultado não se limitou apenas ao específico de Guerra Cibernética. Para uma melhor compreensão do assunto, foram utilizados materiais que tratam dos seguintes assuntos, dentre outros: Guerra da Informação, Segurança em Redes, História Militar, Estratégia Militar, Invasões de Hacker e Terrorismo Cibernético.

Além dos livros e artigos consultados foram utilizadas outras fontes que trataram do assunto, como entrevistas na *web*, documentos eletrônicos de caráter histórico, doutrinas de Forças Aéreas e documentações normativas.

Para dar início às atividades de pesquisa, fornecendo uma fundamentação teórica, foi estabelecido o objetivo específico de discutir os fundamentos da Guerra Cibernética, o que foi feito através da conceituação de Guerra da Informação e da Guerra Cibernética, conforme a teoria existente, realizada no Capítulo 2.

Prosseguindo a atividade, foi estabelecido um segundo objetivo específico de caracterizar ações que podem ser realizadas por forças Aéreas utilizando-se de princípios de Guerra Cibernética.

Para atingir tal objetivo, foi necessário estabelecer uma ligação entre os conceitos teóricos da Guerra Cibernética e suas aplicações na Guerra Moderna, o que foi feito no Capítulo 3, com o estudo da estratégia moderna de guerra, focado

nas teorias da paralisia, do ciclo OODA e dos anéis de Warden, de forma a fornecer uma melhor compreensão da importância do ambiente cibernético para os conflitos da atualidade.

Com o estudo acerca das teorias de guerra realizado, passou-se, então, a apresentação de formas concreta de emprego dessas teorias de guerra relacionadas à Guerra Cibernética, através da apresentação do conceito de Guerra Centrada em Redes (GCR), que estudada em suas potencialidades e vulnerabilidades, evidenciou a importância, na atualidade, acerca do assunto terrorismo cibernético, que foi tratado na sequência.

Assim com o estudo do terrorismo cibernético e da aplicação convencional da Guerra Cibernética, através da Guerra Centrada em Redes, apresentou-se a necessidade da pesquisa para verificar o enquadramento legal da Guerra Cibernética, fornecendo elementos de sua tipificação legal, no âmbito do Direito Internacional, que viessem a legitimá-la como uma forma de guerra.

Assim a caracterização de ações que podem ser realizadas seguindo princípios de Guerra Cibernética, finalizou-se com o estudo de ações realizadas pelos EUA, China e a federação Russa (Rússia), através de suas Forças Armadas, na área de Guerra Cibernética.

A escolha desses países se deu pela presença de Rússia e China no bloco dos BRIC, ao qual o Brasil faz parte, e por ser o EUA, reconhecidamente, o país mais desenvolvido na área cibernética.

Seguindo a pesquisa, foi estabelecido um terceiro objetivo específico, para analisar a Força Aérea Brasileira quanto às ações de Guerra Cibernética. Tal análise foi feita utilizando-se como referência os dados obtidos no estudo dos casos dos países citados, bem como todas as demais informações obtidas no decorrer da dissertação.

Dessa forma, atingindo os objetivos específicos, foi possível alcançar com êxito o objetivo geral de diagnosticar a situação em que se encontra a FAB quanto ao desenvolvimento de ações de Guerra Cibernética, o que poderá ser verificado no decorrer do próximo capítulo.

6 ANÁLISE DA GUERRA CIBERNÉTICA

Para realizar esta fase do trabalho, será feita uma análise estratégica e doutrinária acerca de aspectos gerais da Guerra Cibernética, contextualizando a sua importância para uma Força Armada, em particular para a arma aérea, como uma fonte de poder a ser utilizada em termos ofensivos e defensivos.

Após, de forma a atingir o objetivo geral do trabalho, será realizado um diagnóstico das ações da Força Aérea Brasileira em relação à guerra cibernética.

Esse diagnóstico será realizado tomando-se como parâmetros de comparação, quando aplicável, os pontos focais apresentados no item 4.4, tudo à luz da fundamentação teórica, realizada no capítulo 2, bem como todas as considerações realizadas.

6.1 ANÁLISE ESTRATÉGICA E DOUTRINÁRIA

Com o moderno desenvolvimento tecnológico, ficou evidente que a guerra cibernética ganhou importância destacada na doutrina militar, isto ocorreu, principalmente, devido ao fato do componente cibernético mostrar-se como um fator multiplicador de poder, bem como uma vulnerabilidade a ser explorada e defendida.

A guerra cibernética apresenta-se como uma alternativa à obtenção dos objetivos políticos através do uso da força, conforme definição de guerra feita por Clausewitz (2010). Essa alternativa tem demonstrado algumas características, que a tornam uma realidade no contexto bélico, conforme analisadas a seguir.

Uma primeira característica, a ser verificada, é que a guerra cibernética apresenta-se como uma solução viável, de baixo custo relativo, como um fator de peso na balança de poder entre dois oponentes.

Esse baixo custo relativo pode ser observado pela possibilidade de uso, em grande escala, de recursos, humanos e materiais, facilmente compartilhados entre os meios civis e militares, com grande utilização em tempos de paz, o que aumenta significativamente a eficiência da aplicação desses recursos.

Outro fator, a ser considerado, é que em um conflito entre dois atores, geralmente, aquele que tem maior disponibilidade de recursos tecnológicos tende a obter uma vantagem significativa. Neste sentido, a guerra cibernética possui a função de mitigar tal desnível.

Isso ocorre, pois, conforme foi verificado na fundamentação teórica, o ambiente cibernético possui uma característica marcante que o difere dos demais, ou seja, ele é totalmente artificial, criado pelo ser humano, portanto sofrendo maior influência deste.

Tal característica, por mais contraditória que possa parecer, aumenta a influência do fator humano, o que em determinado aspecto, se não chega exatamente a igualar o poder relativo, fornece a possibilidade de atores, com menor acesso a recursos tecnológicos, de elevado custos, a investir em seus recursos humanos de forma a minimizar uma situação de desequilíbrio. Esta situação, conforme observado no item 4, foi observada e explorada por China e Rússia com relação aos EUA, e serve de exemplo para uma Força Aérea carente de recursos, como a brasileira.

Mais um aspecto, a ser observado quanto ao ambiente cibernético, é que após o término da Primeira Guerra Mundial, talvez em resposta ao massacre ocorrido nas trincheiras europeias, o aparecimento dos carros de combate e do poder aéreo, as estratégias de guerra evoluíram do choque frontal entre as forças para ataques específicos que viessem a trazer os resultados desejados.

Seguindo essa linha, verificou-se que a guerra deveria ter como lei fundamental a economia de forças, assim, para derrotar o inimigo, seria necessário o ataque ao cérebro do mesmo, numa analogia ao corpo humano, pois este ataque iria produzir o efeito de paralisar todo o restante do corpo, sem a necessidade de embates na busca da aniquilação do inimigo.

Como resposta a esta necessidade, desenvolveram-se os conceitos estratégicos de paralisia, ataques paralelos e centros de gravidade, dentre outros. Tais conceitos, para serem viabilizados, dependiam de uma estrutura de comando e controle que possibilitasse a utilização eficaz de um número elevado de meios de forma simultânea, tal estrutura teve como arcabouço teórico o conceito do ciclo OODA de Boyd, que no ambiente moderno de guerra, foi estruturado sobre uma estrutura de tecnologia da informação.

Essa situação traz a importância da análise do ciclo decisório (ciclo OODA) presente em todos os campos da sociedade e especificamente útil para os combates. Nota-se que para este ciclo completar-se é necessário observar para depois orientar, decidir e finalmente agir, ocorrendo ele de forma cíclica e ininterrupta.

Seguindo este modelo, verifica-se que a vitória será alcançada por aquele que conseguir realizar esse ciclo de forma mais ágil, ou seja, mais rápida. Isso ocorre, pois a partir do momento que um dos lados, envolvido no conflito, estiver executando o ciclo mais rapidamente, irá gerar um volume tal de informações a serem processadas pelo ciclo adversário, que o mesmo irá atingir o seu limite de trabalho causando uma paralisia do processo decisório, e a consequente derrota.

Para atingir o ciclo de comando e controle do adversário, bem como defender o próprio ciclo, é necessário que se realize uma adequada escolha de alvos a serem atingidos. Estes devem estar localizados em Centros de Gravidades chaves.

Tais centros são na verdade fonte de poder, portanto de suma importância para os estados. Assim, de acordo com este modelo, para atingir a vitória, um oponente deve visualizar o sistema como um todo, e deve focar suas ações nos elementos mais importantes, que quando atingidos, acabarão a causar, por fim, a ruptura do ciclo OODA inimigo, sua paralisia e, por conseguinte, sua derrota.

Uma forma prática para se atingir os centros de gravidade do inimigo, é a utilização de ataques paralelos, nos quais diversos alvos de variados centros de gravidade são atacados de forma praticamente simultânea, negando ao inimigo a possibilidade de recuperação, fazendo com que o mesmo entre em um processo de paralisia.

A ação de ataques paralelos foi uma característica possibilitada pelo advento da moderna Tecnologia da Informação, pois antigamente tal ação, embora identificada, era considerada impossível de ser realizada devido às restrições tecnológicas. O poder desse tipo de ataque traz à tona uma substituição da metodologia de ataques seriais em ondas por uma metodologia de ataques paralelos simultâneos. Tais ataques, embora mais letais, são muito mais complexos para ser viabilizados.

Essa complexidade traz, dentre outros fatores, a necessidade da aquisição, disseminação e compartilhamento de informações, com grande velocidade e volume, nas operações militares, o que, na atualidade, só é possível com a utilização do ambiente cibernético.

Tal dependência gerou, de forma ambígua, duas situações para os oponentes envolvidos na guerra atual.

Por um lado, a utilização do ambiente cibernético tem fornecido uma vantagem incomparável aos atores que a estão utilizando em suas forças militares, fornecendo-lhes um nível de poder muito superior em relação aos que não possuem tal condição.

Por outro lado, o próprio ambiente cibernético, quando altamente presente nos atores que o utilizam, acaba por gerar uma vulnerabilidade intrínseca, devido a sua característica de interconexão a um ambiente de acesso generalizado. Assim constitui-se como alvo viável para aqueles que não possuem, necessariamente, um grande poder militar.

Tal dualidade, obrigatoriamente, elege o ambiente cibernético como um centro de gravidade a ser atacado e ser defendido, portanto fundamentando a importância do domínio da guerra cibernética por parte das Forças Armadas.

Mais especificamente, para as Forças Aéreas, que por definição, são responsáveis pela Superioridade Aérea, que pode ser traduzida pelo controle do espaço aéreo, a guerra cibernética mostra-se como fator de fundamental importância.

Um aspecto que vem ao encontro dessa afirmativa, é que a Força Aérea, comparativamente às Forças Naval e Terrestre, é a que possui maior dependência da TI, o que pode ser observado, dentre outros fatores, pelo elevado grau de informatização dos sistemas embarcados dos modernos vetores de combate aéreo.

Aumentando ainda mais o grau de dependência cibernética das Forças Aéreas com relação ao ambiente cibernético, é notório o fato de estas estarem, a cada dia mais, tornando-se dependentes de sofisticadas estruturas informatizadas de comando e controle baseadas em radares, comunicações, computadores e redes, dentre outros aspectos.

Tal situação trouxe uma inovação doutrinária na estratégia da guerra, pois, como é concebida, nos dias atuais, a superioridade aérea é o fator primário a ser conquistado em uma campanha militar devido a características, dentre outras, como o alcance geral do ambiente aéreo, sem limites, conforme Seversky (1988).

A inovação doutrinária verificada no caso em voga, e observada em especial pelos americanos, é que, devido à dependência da Força Aérea com relação ao ambiente cibernético, torna-se fator preponderante que, anteriormente à superioridade aérea, seja obtida a superioridade cibernética.

Essa constatação evidenciou a necessidade da discussão da guerra cibernética por parte das Forças Aéreas, que devem tratar a situação, além de uma necessidade defensiva, como uma oportunidade de aumentar o seu poder agregado, tornando-se fundamental à consecução de seu objetivo final que é manter o controle do espaço aéreo de interesse de sua nação.

A não observância do trato do assunto cibernético, no âmbito de uma Força Aérea, irá colocá-la em situação de vulnerabilidade frente a seus potenciais inimigos, uma vez que sistemas de vital importância ao funcionamento da mesma, tanto em termos administrativos como operacionais, estarão sendo colocados em posição de risco.

Outra oportunidade apresentada pelo ambiente cibernético, e intimamente ligada a uma Força Aérea, é que novas potencialidades fizeram-se presentes, como uma possibilidade de realizar a integração e o compartilhamento de dados, em tempo real, nos campos de batalha, conhecido como Guerra Centrada em Redes.

Tal filosofia de combate fornece à força que o utiliza uma vantagem substancial, pois possibilita o uso coordenado dos recursos aumentando a sua efetividade, dando um poder de combate diferencial.

Isso ocorre, pois, com a difusão de informações através do campo de batalha, aumenta-se a consciência situacional por parte dos atores envolvidos na batalha, o que por si só gera uma situação favorável indo de encontro ao ensinamento de Sun Tzu (2004, p. 8) que disse: “se conheces os demais e te conheces a ti mesmo, nem em cem batalhas correrás perigo”.

Para uma Força Aérea, que possui características, intrínsecas a seus vetores, como velocidade, flexibilidade, mobilidade, alcance e penetração, a Guerra Centrada em Redes apresenta-se como um fator diferencial na integração e disseminação de informações pelo Teatro de Operações, que devido a essas características tende a tomar contornos dispersivos.

Exemplificando essa situação, nota-se que um avião de caça voando próximo a um grande número de inimigos e amigos, a uma velocidade por vezes superior a do som, necessita de consciência situacional de uma área que pode assumir proporções de altura que podem variar de 0 a 40.000 pés e de superfície de raio de diversas milhas náuticas.

Tal consciência encontra na Guerra Centrada em Redes, um vasto recurso a ser explorado, que se aplicado corretamente aumentará em muito a vantagem de uma Força Aérea envolvida em combates aéreos.

Esse poder, embora de grande valor, traz, também, o aparecimento de vulnerabilidades, decorrentes da emissão das informações de combate por todo o campo de batalha, que podem ser utilizadas por adversários em condições de inferioridade, o que traz a obrigatória preocupação de segurança quando da sua aplicação, bem como se apresenta como uma oportunidade a ser explorada.

Essa possibilidade de exploração do ambiente cibernético contra atores de maior poder, além de apresentar-se como algo a ser explorado por forças convencionais, evidencia outra grande preocupação, em evidência nos dias atuais, particularmente após os eventos de 11 de setembro de 2001, que é o fortalecimento do terrorismo cibernético.

A motivação dos grupos terroristas e o seu grau de periculosidade são variáveis, porém os mesmos utilizam o terrorismo cibernético como forma viável de atores em inferioridade realizarem ações em oposição a um adversário mais poderoso. Essa capacidade pode ser usada, inclusive, de forma velada por um estado para realizar ações de forma dissimulada em seu proveito, protegendo, de forma indireta os seus executores, ao colocá-los sob seu arcabouço legal em detrimento de serem tratados como agentes de uma guerra.

Essa situação, quando colocada no nível de uma Força Aérea, toma importância ao colocar em risco sua função básica, que é a manutenção da soberania do espaço aéreo do interesse de sua nação. Esse incremento do grau de importância ocorre, pois, em última instância, é a Força Aérea de uma nação quem deve zelar pelo uso de seu espaço aéreo.

Tome-se como exemplo os danos impostos pelos ataques terroristas conhecidos como o onze de setembro. Estes ataques demonstraram que a nação possuidora da mais poderosa Força Aérea do planeta mostrou-se incapaz de impedir a utilização de meios aéreos civis, no interior de seu território, como arma contra ela mesma.

Embora o evento analisado não tenha sido um ataque cibernético, propriamente dito, ilustra bem como uma interferência no sistema de defesa e tráfego aéreo de um país pode ser utilizada a favor das intenções inimigas, sejam elas provenientes de inimigos convencionais em uma guerra nos moldes

tradicionais, bem como proveniente de inimigos não convencionais como no caso do terrorismo.

Essa situação ocorre, pois os modernos sistemas de defesa e tráfego aéreo são altamente dependentes de informações que, em última instância, geram consciência situacional utilizando a troca de informações através do ambiente cibernético.

Portanto, mesmo uma Força Aérea de uma nação pacífica, que utilize doutrinariamente suas forças armadas de forma defensiva, deve preocupar-se em manter eficazes suas defesas cibernéticas. A não observância desse aspecto poderá impedir o cumprimento de sua função fundamental do controle do espaço aéreo.

Assim além de verificarmos o grande potencial ofensivo da Guerra Cibernética, tanto em ataques cibernéticos, propriamente ditos, bem como na sua utilização em sinergia com outras formas de guerra, nota-se a necessidade de sua utilização para fins defensivos.

Essa afirmação demonstra o grande potencial dissuasório da Guerra Cibernética, pois o seu domínio tem a qualidade dupla de persuadir tanto pelo potencial ofensivo que a mesma pode imprimir a um adversário, bem como pela condição de negar que este utilize o ambiente cibernético em seu favor. Tal situação vem a reforçar a posição da Guerra Cibernética como uma forma viável de guerra nos dias atuais.

A postura dissuasória da utilização, imposta pela utilização da Guerra Cibernética, é totalmente dependente da orientação política-estratégica adotado pelos atores que a utilizam. Essa variação estratégica de acordo com a situação, de cada ator, ficou bem evidenciada nos casos analisados de China, Federação Russa (Rússia) e Estados Unidos da América, conforme descrito na sequencia.

Na China, ficou evidente, que a Guerra Cibernética tem sua importância determinada, principalmente, como uma alternativa à sua baixa capacidade de projeção de poder. Assim o ambiente cibernético, atua como um meio que possibilita aos chineses atingirem seus inimigos à distância.

Na doutrina militar chinesa, em consonância com a filosofia oriental, a guerra cibernética é levada a cabo utilizando métodos de dissimulação, camuflagem e estratagemas que afetem o processo decisório inimigo, em um aspecto mais psicológico, de forma favorável aos chineses.

Numa analogia ao ciclo OODA, pode-se dizer que os chineses atuam, com predominância, na tarefa de afetar as capacidades de observar e orientar do ciclo inimigo, numa tentativa de afetar o seu funcionamento.

Na Federação Russa, mais especificamente na Rússia, a Guerra Cibernética ganhou importância como forma de contrapor o poderio militar americano, assim, a Rússia armou-se de um poderoso arsenal cibernético, o qual tem sido constantemente utilizado em suas operações de Guerra.

Doutrinariamente, os russos dão maior importância ao aspecto cognitivo da Guerra Cibernética, atuando na direção de conduzir as decisões adversárias a seu favor. Tais ações são feitas recheadas de dissimulação, e utilizando o conceito do controle reflexivo, que leva o inimigo a tomar a ação desfavorável, através de uma imagem própria (russa) devidamente refletida a ele.

Utilizando-se o conceito do ciclo OODA, percebe-se que a atividade russa é direcionada, principalmente à orientação e à decisão, de forma a levar o inimigo a tomar linhas de ações favoráveis aos russos.

Os Estados Unidos, como detentores da vanguarda tecnológica mundial, perceberam no ambiente cibernético uma oportunidade de potencializar o seu já imenso poderio militar, de forma a atingir uma posição hegemônica, evidenciada em todas as últimas ações de Guerras Regulares na qual suas forças estiveram presentes.

Conceitos como o da Guerra Centrada em Redes estão em pleno desenvolvimento no âmago das Forças Armadas Americanas e em especial na Força Aérea, e embora ainda não se tenha conseguido identificar a verdadeira medida da influência da Guerra Cibernética na composição do poder militar americano, com certeza essa tem fornecido meios para manutenção de sua superioridade mundial.

Tal dependência do ambiente cibernético levantou o alerta americano para sua vulnerabilidade nesse setor, pois embora possa parecer inconcebível, a própria estruturação do ambiente cibernético abre grandes brechas à aplicação da Guerra Assimétrica.

O imenso poderio militar americano encontra ecos em sua doutrina que busca os combates decisivos e rápidos, portanto para alcançar seu objetivo, dentro do modelo do ciclo OODA, os americanos atuam no mesmo como um todo, ao

possuírem os meios necessários a atuar nos centros de gravidade internos dos inimigos, de forma paralela, para causar a paralisia.

Porém se for necessário identificar a posição, no ciclo OODA inimigo, em que sua atuação tem prioridade, poder-se-ia apontar os aspectos da decisão e ação contra o inimigo, tirando deste a possibilidade de completar o ciclo, consequentemente, causando-lhe a derrota.

Portanto, as variações estratégicas de acordo com a situação de cada Força Armada, demonstra que a guerra cibernética é tratada por estes países como uma forma de guerrear em um quinto ambiente, concorrendo com o aéreo, o terrestre, o naval e o espacial.

A Guerra Cibernética se tornou uma realidade atual, ficando evidente que deve ser levada em consideração por qualquer Força Aérea que intencione manter-se atualizada em nível de poder, evidência essa comprovada pela atenção dada à mesma por parte de poderosas nações, como China, EUA e Rússia.

Assim verificados os aspectos estratégicos da guerra cibernética, e sua importância para uma Força Aérea, será agora verificada a situação da Força Aérea Brasileira neste quesito.

6.2 A GUERRA CIBERNÉTICA NA FAB

Para dar início ao diagnóstico da Força Aérea Brasileira em suas ações voltadas para a Guerra Cibernética, é necessário primeiro contextualizar a posição política-estratégica da FAB no contexto da nação brasileira.

A Constituição da República Federativa do Brasil (BRASIL, 1988), prevê o seguinte:

> Art. 142. As Forças Armadas, constituídas pela Marinha, pelo Exército e pela Aeronáutica, são instituições nacionais permanentes e regulares, organizadas com base na hierarquia e na disciplina, sob a autoridade suprema do Presidente da República, e destinam-se à defesa da Pátria, à garantia dos poderes constitucionais e, por iniciativa de qualquer destes, da lei e da ordem. (BRASIL, 1988)

Já desse artigo, percebe-se que a destinação das Forças Armadas Brasileiras, e, por conseguinte, da Força Aérea Brasileira, é a defesa da Pátria em todos os seus aspectos, portanto todo assunto, como a Guerra Cibernética, que afete a defesa nacional deve ser alvo de atenção por parte dos militares brasileiros.

Assim, seguindo essa orientação constitucional, a doutrina de Guerra Cibernética, de forma positiva, já foi reconhecida pelos mais altos níveis militares brasileiros, o que foi demonstrado pela Política de Defesa Nacional, de 2005, do Ministério da Defesa, que em seu item XII estabelece a seguinte diretriz estratégica: “aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, permitam seu pronto restabelecimento.” (BRASIL, 2005).

Tal diretriz colocou a Guerra Cibernética no escopo das Forças Armadas Brasileira, de forma positiva, por demonstrar o reconhecimento da importância do ambiente cibernético para as ações militares, e acabou por dar legitimidade para as atividades cibernéticas.

Ainda sobre esta diretriz, percebe-se que em seu cerne está a preocupação com a postura de utilizar a Guerra Cibernética para a Defesa Nacional, porém, de forma sintonizada aos potenciais desta forma de guerra verificado nos países analisados no item 4, não limita a sua utilização estratégica a uma postura operacional defensiva, mas sim aos interesses nacionais.

Nos países analisados, como parâmetros para o caso brasileiro, a Guerra Cibernética não é tratada apenas como recurso defensivo necessário, mas sim como uma importante ferramenta no posicionamento estratégico, sendo considerada como elemento importante a ser considerado no balanço de poder em relação a seus potenciais adversários.

Observa-se que um grande fator, que impulsionou a inclusão da Guerra Cibernética na doutrina militar dessas nações, foi a competição gerada entre os diversos envolvidos, o que deve ser observado pelo Brasil, pois a Guerra Cibernética demonstrou sua necessidade nas três situações de poder relativa possíveis, conforme descrito a seguir;

a) situação de superioridade – neste caso a Guerra Cibernética é utilizada para consolidar ainda mais a posição de superioridade de um ator, aumentando o seu poder dissuasório e a eficiência no alcance da vitória, que pode ser medida em termos de custo com relação aos aspecto de vidas, recursos financeiros e recursos materiais, dentre outros;

b) situação de igualdade – neste caso o ambiente cibernético pode servir como um fator de desequilíbrio, mais eficaz e eficiente, na relação de equiparação de poder apresentada; e
c) situação de inferioridade – nesta situação, a guerra cibernética apresenta campo fértil a ser explorado em situações de Guerra Assimétrica, por fornecer ferramentas de custo relativo baixo, porém de elevado potencial destrutivo.

O direcionamento doutrinário das forças militares dos países analisados incorporou os aspectos da Guerra Cibernética, que passou a ser utilizada como ferramenta para a consecução dos objetivos nacionais, ou seja, com o status estratégico, servindo, inclusive, como alternativa ao confronto direto cinético.

Nesse aspecto, o Brasil, conforme visto em sua Política Nacional de Defesa, define que a Guerra Cibernética deve ser considerada estrategicamente, desde que vá de encontro aos interesses da Defesa Nacional, ou seja, adotando-se uma postura dissuasória defensiva.

Essa postura é corroborada pela Estratégia Nacional de Defesa (END), de 2008, que possui as seguintes diretrizes relacionadas à Guerra Cibernética:

> 1. Dissuadir a concentração de forças hostis nas fronteiras terrestres, nos limites das águas jurisdicionais brasileiras, e impedir-lhes o uso do espaço aéreo nacional.
> Para dissuadir, é preciso estar preparado para combater. A tecnologia, por mais avançada que seja, jamais será alternativa ao combate. Será sempre instrumento do combate.
> 4. Desenvolver, lastreado na capacidade de monitorar/controlar, a capacidade de responder prontamente a qualquer ameaça ou agressão: a mobilidade estratégica.
> 6. Fortalecer três setores de importância estratégica: o espacial, o cibernético e o nuclear. Esse fortalecimento assegurará o atendimento ao conceito de flexibilidade.
> Como decorrência de sua própria natureza, esses setores transcendem a divisão entre desenvolvimento e defesa, entre o civil e o militar.
> 22. Capacitar a indústria nacional de material de defesa para que conquiste autonomia em tecnologias indispensáveis à defesa. (BRASIL, 2008a)

Percebe-se nestas diretrizes a orientação no sentido de dissuadir estando preparado para o combate, o que em termos de Guerra Cibernética indica a necessidade de possuir uma capacidade ofensiva que possibilite responder a qualquer ameaça ou agressão.

Outro ponto a ser observado na END é a inclusão do setor cibernético dentre os setores de importância estratégica, direcionando a necessidade da

cooperação civil-militar em sintonia com a Indústria Nacional na busca do desenvolvimento cibernético que atue em favor da autonomia brasileira.

Colocado o direcionamento a ser adotado pelas Forças Armadas, no que diz respeito à Guerra Cibernética, será agora analisado como são tratadas as ações de Guerra Cibernética no âmbito da FAB, a fim de fornecer um diagnóstico da atual situação.

Seguindo essa linha é preciso, inicialmente, verificar como o assunto é tratado pela legislação que direciona doutrinariamente todas as ações a serem realizadas pela Força Aérea Brasileira, ou seja, a Doutrina Básica da Força Aérea Brasileira, DCA 1-1 (BRASIL, 2005).

Inicialmente, a DCA 1-1 estabelece a missão-síntese da FAB que “é manter a soberania no espaço aéreo nacional com vistas à defesa da Pátria.” (BRASIL, 2005)

Como já analisado, o controle do espaço aéreo, nos dias atuais, é profundamente dependente do ambiente cibernético, principalmente, nas áreas de controle de tráfego aéreo, nas atividades administrativas ou na utilização de vetores aéreos profundamente dependentes da TI, todos de fundamental importância ao poder aéreo.

Verifica-se, assim, o grande grau de aderência da FAB ao ambiente cibernético, o que a torna alvo potencial de ataques digitais, que poderão vir a atingir sensivelmente o cumprimento de sua missão, o que obriga o trato da Guerra Cibernética por parte desta força.

Prossegue a DCA 1-1 definindo que “o principal objetivo da guerra é impor uma vontade ao adversário” (BRASIL, 2005), portanto como visto na fundamentação teórica, bem como na análise de China, EUA e Rússia, a Guerra Cibernética é um meio a ser utilizado na consecução deste objetivo, o que reforça ainda mais a necessidade de seu trato no âmbito da FAB.

Corroborando a necessidade do domínio acerca dos conflitos no ambiente cibernético por parte da FAB, o ambiente cibernético apresenta-se como um quinto ambiente bélico, portanto como cita o item 3.9 da DCA 1-1, o poder militar deve ser empregado de forma a responder a um pensamento militar unificado, o que deve incluir ações referentes ao ciberespaço.

Dentre as Forças Armadas, devido às características elencada e discutidas por teóricos do Poder Aéreo como Douhet (1987), Seversky (1988),

Mitchell (apud RATTRAY, 2001), Warden (2010) e Boyd (apud OSINGA, 2007), dentre outros, é a Força Aérea é a mais dependente e vulnerável no que diz respeito ao Comando e Controle.

Como os sistemas de Comando e Controle modernos são altamente dependentes de recursos computacionais, torna-se imperativo à Força Aérea Brasileira prover a sua segurança, para não correr o risco de ter seu ciclo OODA afetado, levando-a a derrota.

Nesse sentido, percebe-se que China, EUA e Rússia, não só verificaram a necessidade de prover a adequada proteção de seus sistemas de C2, bem como identificaram ai um centro de gravidade a ser afetado, colocando tal atividade em alinhamento ao seu pensamento estratégico, portanto servindo de exemplo à FAB para adotar tal linha de ação.

Tal atividade de Combate aos Sistemas de Suporte ao C2, já está presente na doutrina da FAB, portanto demonstrando um alinhamento desta força em relação ao que já foi verificado pelos países citados.

Como pode ser observado, a FAB vem apresentando um posicionamento doutrinário que já reconhece a importância da Guerra Cibernética para a realização de sua missão, porém tal atividade ainda mostra-se defasada frente ao direcionamento teórico da atualidade e das forças mais avançadas neste quesito.

Uma indicação desta defasagem é a conceituação da DCA 1-1 no que diz respeito à Guerra Cibernética colocando-a como um subtipo da Guerra de Informações da seguinte forma:

> O conceito de Guerra Cibernética, ainda que por vezes seja abordado de uma forma diferenciada em relação ao conceito de Guerra Eletrônica, pode ser considerado como parte integrante do mesmo. A Guerra Cibernética envolve, assim, a utilização de todas as “ferramentas” disponíveis ao nível da eletrônica e da informática, para a indisponibilidade dos sistemas eletrônicos e de comunicação inimigos e para manutenção dos nossos próprios sistemas operacionais. (BRASIL, 2005, p. 19)

Tal posicionamento doutrinário indica uma necessidade de revisão, pois, como explicitado por Libicki (1995), o conceito de guerra cibernética está localizado como um subtipo da Guerra da Informação, assim como a Guerra Eletrônica, portanto, embora semelhantes, são distintos e dessa forma devem ser tratados.

Seguindo esta linha, o posicionamento das Forças Armadas dos países estudados (EUA, China e Rússia), coloca a Guerra Cibernética em um nível estratégico. Desta forma, a mesma é tratada como fonte de poder necessário ao

domínio de um novo ambiente, assim colocando a necessidade da superioridade cibernética no mesmo patamar de outros ambientes como o terrestre, o naval e o aéreo.

Cabe ressaltar, que como a Tecnologia da Informação embrenha-se por toda estrutura de uma força militar moderna, os países estudados verificaram a necessidade de adquirir a superioridade cibernética, de forma similar à consolidada necessidade da aquisição da superioridade aérea, possibilitando assim o fornecimento de condições ideais para operações seguras a serem realizadas tanto na terra, na água como no ar, o que indica um caminho a ser adotado pela FAB.

Salienta-se que, de acordo com a END, a Força Aérea Brasileira deverá trabalhar pelo desenvolvimento de sua capacidade de operar em rede, o que irá aumentar substancialmente o seu potencial de combate, demonstrando a necessidade de utilizar, de forma conjunta, as formas cinéticas e cibernéticas de guerra.

Visto como o assunto Guerra Cibernética, está inserido doutrinariamente no âmbito da FAB, prosseguindo o diagnóstico, deve ser verificado como efetivamente as ações de Guerra Cibernética estão sendo tratadas por esta força.

Seguindo esse contexto é preciso, inicialmente, verificar como está estruturado o trato da Tecnologia da Informação na FAB.

Nesse sentido, verifica-se que os assuntos referentes à Tecnologia da Informação, no âmbito da aeronáutica, são regidos pelo Sistema de Tecnologia da Informação do Comando da Aeronáutica (STI) que possui a seguinte finalidade:

> Apoiar o cumprimento da missão de todas as Organizações do COMAER com os recursos de tecnologia da informação, de acordo com a Política e as diretrizes do COMAER, e com os padrões e práticas internacionais, no que for aplicável, contribuindo para a eficácia do processo de tomada de decisão nos seus diversos níveis. (BRASIL, 2004, p. 8).

Portanto, toda a atividade de Guerra Cibernética está subordinada ao STI, e deverá ser analisada a luz desse sistema.

Tal situação indica uma sistematização da Tecnologia da Informação na qual a Guerra Cibernética deve ser incluída, a fim de prover direcionamentos que venham a viabilizar a estruturação da Guerra Cibernética no âmbito da FAB.

Para nivelar-se aos países mais desenvolvidos na área cibernética militar, o STI deve estar atuando no sentido de dar ênfase à formação de pessoal especializado e capacitado a gerir a Guerra Cibernética e fornecer a tecnologia e

estrutura organizacional adequada para possibilitar a utilização militar do ciberespaço.

Essa necessidade de estruturação para a Guerra Cibernética impõe-se não somente pelo fato do domínio desse fator servir como fator de multiplicação da capacidade militar de uma Força Aérea, conforme identificado pelos países analisados, mas por tal situação apresentar-se como uma obrigatoriedade frente à necessidade de implantar uma defesa contra ataques digitais.

Tal fato ocorre, pois, nos dias atuais, cada vez mais a TI está se inserindo na sociedade moderna, evidenciando, assim, diversas vulnerabilidades identificadas nos Centros de Gravidade, conforme os anéis de Warden.

Exemplificando essa dependência, no caso da Força Aérea Brasileira, podem-se citar as seguintes atividades, dentre outras, profundamente dependentes do ambiente cibernético:

a) Sistema de Logística e Manutenção;
b) Sistema de Gerenciamento de Pessoal;
c) Sistema de Pagamento de Pessoal;
d) Sistema de Controle de Tráfego Aéreo;
e) Sistema de Defesa Aérea; e
f) Sistema de Comando e Controle.

Fica assim evidenciada a necessidade da estruturação da Defesa Cibernética a fim de propiciar a manutenção dessas funções fundamentais ao funcionamento da Força Aérea Brasileira.

Nesse sentido, as atividades de estruturação, para atuação nesse ambiente, foram iniciadas no âmbito das Forças Armadas Brasileira, encontrando-se a Guerra Cibernética em seus estágios embrionários, cabendo ao Exército Brasileiro coordenar essas atividades.

> Foi realizado, no período de 21 a 24 de junho de 2010, no Estado-Maior do Exército Brasileiro e no Centro de Instrução de Guerra Eletrônica, também do Exército, o I Seminário de Defesa Cibernética.
> O evento contou com a participação de militares das três forças e convidados de empresas e órgãos da Administração Pública Federal.
> Foi dividido em duas partes, sendo os dois primeiros dias destinados à realização de palestras de alto nível, ministradas por gestores de órgãos governamentais e empresas com envolvimento nos ramos financeiro, energético, cibernético e de telecomunicações, abertas a todos os participantes. Nos dois últimos dias, as atividades foram restritas ao pessoal das três forças, divididos em grupos de trabalho (GT) para elaborar um plano de desenvolvimento na área.
> **O seminário pode ser visto como um primeiro passo para o desenvolvimento das atividades relacionadas à Guerra Cibernética**,

> incluindo integração das Forças Armadas. A Guerra Cibernética foi uma das áreas estratégicas identificadas pelo Ministério da Defesa, sendo atribuída ao Exército a responsabilidade de coordenar ações para permitir o desenvolvimento nesta área. (CENTRO DE COMPUTAÇÃO DA AERONÁUTICA DO RIO DE JANEIRO, 2010c, grifo nosso). (CENTRO DE COMPUTAÇÃO DA AERONÁUTICA DO RIO DE JANEIRO, 2010c)

Tal situação mostra-se como um aspecto positivo por evidenciar o reconhecimento da necessidade do preparo quanto à Guerra Cibernética, e o fato de tal reconhecimento estar sendo tratado pelas Forças Armadas Brasileiras, de forma abrangente. Com isto, demonstra-se uma preocupação com uma situação observada pela tríade de países analisados, que é a dificuldade apresentada pelo desafio da integração da doutrina de Guerra Cibernética às doutrinas tradicionais.

Isso ocorre, pois a doutrina militar tem, como principal fonte de desenvolvimento, as experiências bélicas testadas em combates reais, realizados pelas próprias forças armadas ou vivenciadas por outras. Assim, de forma análoga ao que aconteceu com o Poder Aéreo, que ainda encontra-se em consolidação, o Poder Cibernético carece de experiências de combate reais, em maior número, para que sua efetividade possa ser realmente evidenciada e incorporada de forma prática à doutrina militar.

Tal busca, de casos que possibilitem uma correta identificação das características dessa forma de guerra, encontra, ainda, maiores dificuldades de ser realizada devido à volatilidade do ambiente cibernético e dificuldade imposta no rastreamento das atividades cibernéticas.

Na falta desses exemplos reais, cresce, ainda mais, a importância das Forças Armadas investirem em estudos científicos que possam fornecer elementos que possam substanciar a sua estruturação, conforme identificado por EUA, China e Rússia, que possuem grande participação do meio acadêmico no preparo para a Guerra Cibernética.

Seguindo a necessidade de implantar uma eficaz defesa cibernética, a FAB, de acordo com o STI, possui organizações chamadas de Elos Especializados do STI que, dentre outras, possuem as seguintes competências:

> a) Estabelecer procedimentos adequados para a identificação, a avaliação e o gerenciamento dos riscos associados à segurança dos sistemas de TI sob sua área de responsabilidade;
> b) Estabelecer um plano de resposta a incidentes envolvendo a segurança dos sistemas de TI sob sua responsabilidade; e
> c) Estabelecer procedimentos que garantam aos seus técnicos de TI, inclusive aos colaboradores terceirizados, o conhecimento das normas

> de segurança da informação, respeitadas as particularidades de cada cargo ou função exercida. (BRASIL, 2006)

Neste contexto, o Centro de Computação da Aeronáutica do Rio de Janeiro (CCA-RJ) é o elo especializado que vem atuando diretamente na área de Guerra Cibernética, e que criou em sua estrutura o Centro de Tratamento de Incidentes de Segurança em Redes (CTIR.FAB), que possui a seguinte missão:

> Definir e coordenar ações em resposta a eventos que comprometam a segurança na rede, através da identificação do incidente nos sistemas computacionais, trabalhando em conjunto com os demais centros de computação, com os especialistas em segurança e com o CTIR Gov na definição e apoio a implementação das ações aplicáveis em toda a rede do Comando da Aeronáutica.. (CENTRO DE COMPUTAÇÃO DA AERONÁUTICA DO RIO DE JANEIRO, 2010a)

O CTIR.FAB, irá atuar na defesa da infraestrutura de redes da FAB e para tal irá fornecer os seguintes serviços:

> Serviços reativos
> - Análise de logs
> - Tratamento de incidentes
> Serviços proativos
> - Prevenção de ataques IPS
> - Análise de vulnerabilidades
> - Implementação de recursos de segurança
> Serviço de gerenciamento de qualidade
> - Treinamentos
> - Emissão de normas
> - Assessoria em Gestão de Continuidade de Negócios (CENTRO DE COMPUTAÇÃO DA AERONÁUTICA DO RIO DE JANEIRO, 2010a)

O CTIR.FAB já se encontra em funcionamento e no que diz respeito à defesa contra ataques direcionados à Infraestrutura de TI já apresenta alguns resultados, conforme Figura 11, Figura 12 e Figura 13. Tal situação mostra um aspecto positivo, por evidenciar a preocupação da FAB quanto à necessidade de implantar uma defesa adequada ao ambiente cibernético, porém, algumas considerações devem ser realizadas.

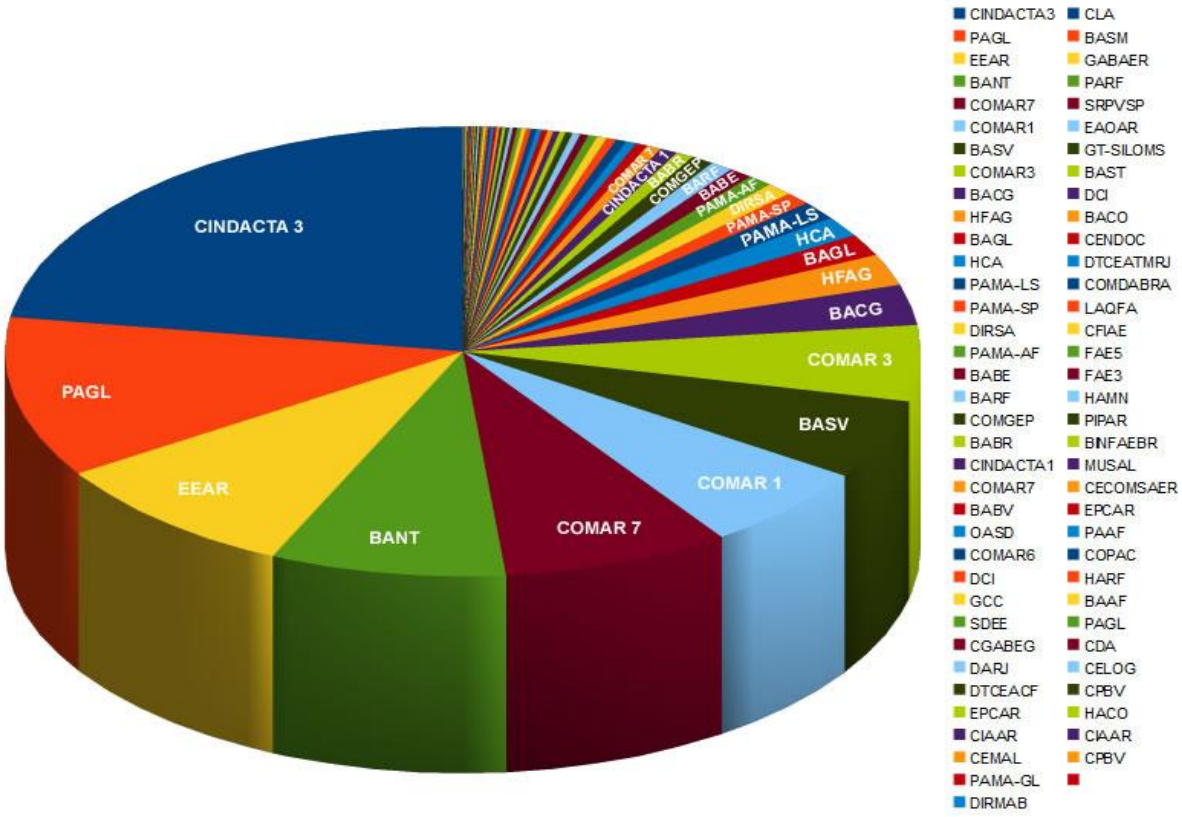

Figura 11: Gráfico de detecção de infecções por Organizações Militares no mês de junho 2010.
Fonte: Centro de Computação da Aeronáutica do Rio de Janeiro (2010b).

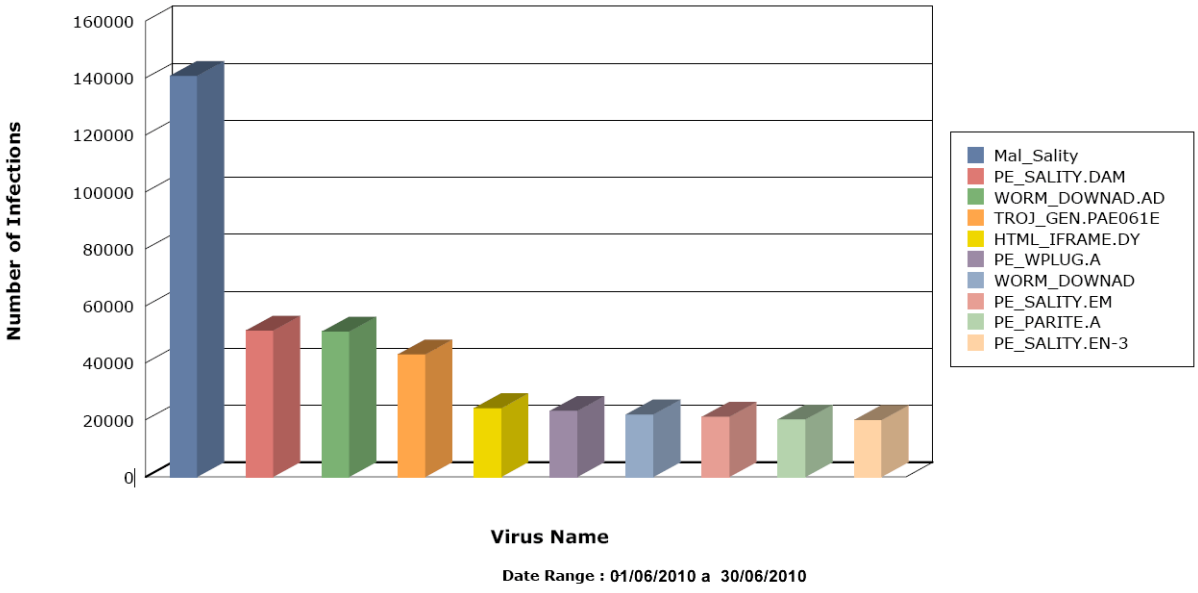

Figura 12: *Ranking* dos 10 vírus mais detectados
Fonte: Centro de Computação da Aeronáutica do Rio de Janeiro (2010b)

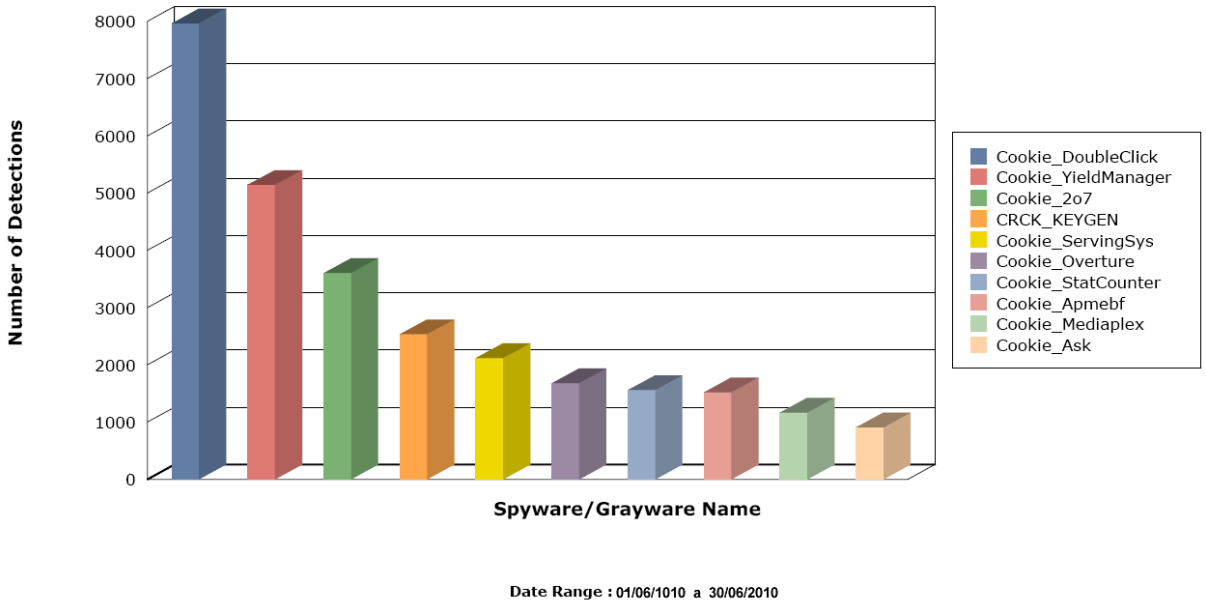

Figura 13: *Ranking* dos 10 spywares mais detectados
Fonte: Centro de Computação da Aeronáutica do Rio de Janeiro (2010b)

Um primeiro ponto, a ser analisado, é que em consonância com o observado por EUA, China e Rússia, a guerra cibernética é uma realidade, com ações reais já sendo realizadas. Nesse sentido ao analisarmos a Figura 11, pode-se observar que a Organização Militar na qual foi identificado o maior número de detecções é o CINDACTA 3 (Terceiro Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo).

A evidência de tal constatação é que tentativas de infecção estão sendo detectadas, possibilitando o seu adequado tratamento, porém, por outro lado, indicam o fortalecimento da necessidade de se preparar uma defesa robusta no que diz respeito ao ambiente cibernético.

Essa necessidade adquire força, nesse caso, pelo fato do CINDACTA 3 ser a organização responsável pelo comando e controle da defesa aérea de toda região sul do Brasil, portanto um ponto sensível a ser atingido por potenciais inimigos, mais fortes, iguais ou mais fracos, na busca de vulnerabilidade críticas a serem atingidas em um eventual conflito.

Essa defesa, como pode ser constatada, deve ser implementada visando não só possíveis ataques provenientes de conflitos regulares, mas também de conflitos irregulares. Nota-se neste sentido que o ataque por si só não fornece a sua origem, portanto trazendo à tona a necessidade de um eficaz trabalho de inteligência

no sentido de identificar seus autores de forma a possibilitar uma reação mais adequada.

Outra constatação, evidenciada pelas Figura 11, Figura 12 e Figura 13 é que existe a identificação de ataques às Organizações militares provenientes de ataques utilizando recursos previamente identificados, vírus e *spyware* listados, porém salienta-se que devem ser realizadas ações na identificação de recursos ainda não conhecidos.

Isto acontece, pois conforme já colocado, os atacantes sempre buscam a utilização de ataques ainda não conhecidos, que podem demandar um elevado tempo até serem identificados, tempo este que, de acordo com o potencial do ataque, poderá fazer com que o ataque venha a infligir danos de elevada monta.

Portanto, é oportuno salientar que a estrutura de funcionamento do CTIR.FAB é, ainda, voltada para o modelo tradicional de defesa reativa

Na análise dos pontos focais em relação às ações de Guerra Cibernética realizadas por EUA, China e Rússia, foi identificado que estes consideram a forma preventiva como sendo a mais apropriada para conduzir a defesa cibernética. Além disso, as Forças Armadas desses países conduzem suas ações cibernéticas de forma a dar grande ênfase ao potencial ofensivo das mesmas.

Assim, conforme observado, o modelo de defesa cibernética da FAB, opera, ainda, de forma reativa necessitando de um maior desenvolvimento para atuar de forma preventiva. Para isso será necessário um grande desenvolvimento, no sentido de fornecer à Força Aérea Brasileira um considerável poder cibernético, que possibilite a sua utilização, de forma efetiva, em prol da Defesa Nacional.

Assim comparando-se aos países que se encontram mais adiantados em relação à guerra cibernética, nota-se que a Força Aérea Brasileira, na atualidade necessita aprofundar o tratamento do assunto, fazendo com que o ambiente cibernético venha a se tornar realidade como fonte de poder.

Essa fonte de poder possui o potencial de ser utilizado em situações assimétricas, tanto de superioridade e de fraqueza, bem como em situação de simetria. É bom salientar, que a utilização ofensiva da guerra cibernética, fornece ferramentas não só com relação a conflitos regulares, como também irregulares.

Outro fator observado, é que, com a utilização da Tecnologia da Informação, nos diversos setores da FAB, torna-se obrigatória a implementação de uma defesa cibernética adequada, tal defesa objetiva contrapor ataques

provenientes de conflitos simétricos e assimétricos, bem como regulares e irregulares.

A não implementação de uma correta defesa cibernética poderá tornar a Força Aérea Brasileira vulnerável a ataques cibernéticos direcionados a sua estrutura de Comando e Controle, bem como a sua infraestrutura, dentre outros pontos. Tal situação poderá permitir que forças adversárias, até mesmo relativamente inferiores em termos militares tradicionais, possam vir a suplantar o poder militar cinético da FAB, apenas com a utilização de ataques digitais direcionados aos centros de gravidade.

Assim, utilizando os conceitos teóricos fornecidos na fundamentação teórica e os parâmetros retirados na pesquisa de ações realizadas pelos EUA, China e Rússia, pode-se diagnosticar que as ações de Guerra Cibernética na FAB, de forma geral, encontra-se em estágios iniciais, se comparadas aos países citados, limitadas, ainda, a uma estrutura defensiva reativa, embora já possua sua importância refletida nos níveis políticos, estratégicos e doutrinários.

CONCLUSÃO

O presente trabalho foi conduzido com o objetivo geral de responder a questão-problema: qual o realidade vivida pela da Força Aérea Brasileira no desenvolvimento de ações de Guerra Cibernética?

Para responder esta questão, e realizar o devido diagnóstico das ações de Guerra Cibernética, inicialmente, foram estudados os fundamentos da Guerra Cibernética de forma fornecer subsídios para as análises realizadas.

Nesta tarefa, verificou-se que a Guerra Cibernética é um ramo da Guerra da Informação, existindo esta no ambiente da Guerra, mesmo antes do advento da informática. Nesse sentido, por exemplo, já os mongóis nos séculos XII e XIII, utilizaram seus conceitos de forma a obterem a vitória sem a necessidade do real envolvimento em combates, ou para obterem condições privilegiadas, aumentando seu poder agregado, e possibilitando aos mesmos a vitória, mesmo quando em inferioridade numérica.

Com o desenvolvimento tecnológico moderno, ficou evidente que a Guerra da Informação ganhou importância destacada na doutrina militar, principalmente devido à incorporação do componente cibernético, que além de proporcionar um multiplicador de poder, forneceu também vulnerabilidades a serem exploradas e defendidas.

Com isto a Guerra Cibernética passou a ser tratada estrategicamente por parte das Forças Armadas de diversos países que verificaram neste método de guerra um grande potencial de poder a ser adquirido e utilizado em favor de suas missões.

Tal situação foi evidenciada, principalmente, após conflitos como a Guerra do Golfo e com o evidente aumento de dependência da sociedade moderna em relação a sistemas de informação, objeto da Guerra Cibernética.

Discutindo o conceito de Guerra Cibernética, ficou claro que a mesma trata de ações de cunho militar realizadas no ambiente cibernético, e que tais ações devem ser voltadas para atingir os centros de gravidade adversários, possibilitando a consecução dos objetivos políticos, ou seja, a Guerra Cibernética possui um valor estratégico.

Outro dado, de vital valor, apresentado na discussão conceitual é que, dentre os diversos tipos de ataques cibernéticos, o ataque digital é o que causa

efeitos mais devastadores, com menos violência e o que tem o menor custo de execução, portando, deve ser objeto de destacada atenção.

A Guerra Cibernética tornou-se uma realidade atual, ficando evidente que deve ser levada em consideração por qualquer nação que intencione manter-se atualizada em nível de poder, evidência essa comprovada pela atenção dada à mesma por parte de poderosas nações, como China, EUA e Rússia.

Outro aspecto, evidenciado, foi que na Guerra Cibernética as ações ofensivas tomam importância evidente, em detrimento de ações defensivas, pois além de diversos fatores, como custo e complexidade, é o ataque que ocasiona a vitória.

Corroborando essa postura ofensiva, foi demonstrado que o modelo defensivo ideal é o modelo que acaba utilizando ações ofensivas, de forma a evoluir de uma postura reativa, para uma postura preventiva, muito mais compensadora.

Prosseguindo na fundamentação da Guerra Cibernética, foi necessária a identificação de como a integração deste novo modelo de guerra pode ser realizada ao pensamento militar, de forma a obter ecos na estratégia militar.

Assim verificou-se que a Guerra Cibernética está altamente atrelada a diversos conceitos estratégicos como paralisia, ciclo OODA, ataques paralelos e centros de gravidade. Esta postura estratégica, muito semelhante à do poder aéreo, a coloca em nível estratégico de igualdade se levada em comparação aos poderes aéreos, terrestres, navais e espaciais.

Como forma concreta da utilização estratégica da Guerra Cibernética, apresentou-se a Guerra Centrada em Redes, filosofia que prima por uma robusta estrutura de Comando e Controle baseada no compartilhamento de informações, o que gera uma um elevado nível de poder, fornecendo vantagens substancias a seus utilizadores.

Esse aumento de força acabou por evidenciar uma grande questão dupla quanto à Guerra Cibernética: ela fornece um elevado nível de poder, a ser explorado, e uma grande vulnerabilidade, a ser defendida, obrigando sua implantação sistematizada e controlada.

Essa vulnerabilidade, na atualidade, reforçou a atuação do terrorismo internacional sob a égide do terrorismo cibernético, o que leva, em certa medida, a atenção das Forças Armadas quanto às questões terroristas que possam afetar a Segurança Nacional.

Observou-se, em seus fundamentos, que a Guerra Cibernética é um modelo de Guerra a ser levado em consideração na estratégia militar, e que até mesmo o Direito Internacional fornece subsídios à tipificação de ataques cibernéticos como ato de Guerra.

Com a fundamentação teórica em Guerra Cibernética, colocada a bom termo, ficou evidente a presença de três estados nos quais tal teoria tem se mostrado mais consolidada e estão sendo colocadas em prática: China, Federação Russa (Rússia) e Estados Unidos da América.

Assim passou-se à busca do segundo objetivo intermediário através da caracterização de ações, utilizando os princípios de Guerra Cibernética, realizadas por Forças Armadas de diversos países. Tal caracterização foi realizada utilizando-se como parâmetros a China, a Rússia e os EUA, este por sua posição hegemônica, em termo de poder militar, e os demais por serem os países, do BRICs, mais avançados militarmente.

Nessa caracterização ficou evidente que, nos países estudados, a Guerra Cibernética foi incluída em sua doutrina sendo realizada em consonância com a estratégia individual de cada país.

Na China e Rússia, ficou evidente que a Guerra Cibernética é utilizada, principalmente, como uma ferramenta para mitigar sua inferioridade militar em relação aos EUA.

Alem disto, os três países utilizam o ambiente cibernético para efetuar ataques contra seus inimigos, de forma a obter a superioridade cibernética, e aumentar o poder de suas forças tradicionais, baseadas em ataques cinéticos. Observa-se que em todos os casos, o objeto principal da Guerra Cibernética tem sido as estruturas de Comando e Controle.

Outro fator de destaque, observado nos Países estudados, foi a atenção que os mesmos dão ao preparo de suas forças no que diz respeito a pessoal, tecnologia e doutrina, além da grande interação com o ambiente civil, principalmente na figura do meio acadêmico.

Ainda como destaque, observa-se a grande preocupação que China, EUA e Rússia possuem com relação à estruturação de suas defesas estratégicas contra ataques cibernéticos, colocando esse tipo de defesa como uma das principais necessidades.

Com a fundamentação teórica realizada e a instituição de um parâmetro de comparação, passou-se à análise da Força Aérea Brasileira com relação às ações de Guerra Cibernética.

Nesta análise verificou-se que a Guerra Cibernética já possui seu valor reconhecido pelos níveis estratégicos, que emitiram diretrizes que visam o fortalecimento da Força Aérea Brasileira com relação ao assunto.

Nesse direcionamento percebeu-se a grande preocupação dada à utilização da Guerra Cibernética para constituir a estrutura dissuasória defensiva do Brasil. Neste contexto, a Força Aérea deverá estar preparada para efetivamente realizar suas defesas e apta a projetar sua força como resposta a uma agressão.

Assim dentro do escopo da Força Aérea Brasileira, a Guerra Cibernética ganhou força no que diz respeito à necessidade de estruturar e defender sua estrutura de Comando e Controle, incluindo a utilização de operações centradas em rede.

Além disso, verificou-se a necessidade de prover a devida segurança aos diversos sistemas em uso, de forma a possibilitar seu funcionamento adequado.

Quanto às ações efetivamente realizadas pela FAB, na busca do seu preparo em termos de Guerra Cibernética, essas estão em seus momentos iniciais, e na atual conjuntura se encontram calcadas em uma defesa reativa.

Assim com o estudo dos fundamentos da Guerra Cibernética, das ações realizadas por diversos países nessa área e da realidade da Força Aérea Brasileira pôde-se chegar à solução do problema geral de realizar um diagnóstico da situação da FAB quanto à guerra cibernética.

Esse diagnóstico da realidade permite inferir que a Guerra Cibernética é um método de guerra de domínio obrigatório por parte da Força Aérea Brasileira, com sua importância reconhecida pelos mais altos níveis militares, e com suas ações efetivas em um estágio inicial de implantação, limitadas em sua eficácia, no presente momento, a ações defensivas reativas.

Ao alcançar o objetivo proposto, tornou-se evidente a necessidade de futuras pesquisas que se aprofundem em outros campos, tais como uma pesquisa voltada à Guerra Cibernética, especificamente em um ambiente não convencional e uma pesquisa indicando estratégias a serem adotadas na realização de ataques cibernéticos, dentre diversas outras.

Finalmente, com o diagnóstico da Guerra Cibernética na Força Aérea Brasileira, ficou evidente que o caminho a ser trilhado ainda é longo, para que essa Força possa atuar efetivamente no meio cibernético em prol da Defesa da Nação, o que possibilitará ao Brasil agir conforme o enunciado em sua Estratégia Nacional de Defesa:

“Defendido, o Brasil terá como dizer não, quando tiver que dizer não.” (BRASIL, 2008a, p. 8)

REFERÊNCIAS

ALBERTS, D. S. **INFORMATION AGE TRANSFORMATION:** getting to a 21s century millitary. 2. ed. Washington: DoD, CCRP, 1996. 155 p.

ALBERTS, D. S.; GARSTKA, J. J.; STEIN, F. P. **NETWORK CENTRIC WARFARE:** Developing e Leveraging Information Superiority, 1999. Disponível em: <http://www.dodccrp.org/files/ncw_report/report/ncw_0801.pdf>. Acesso em: 01 outubro 2010.

ARMISTEAD, L. **Information Operations:** warfare and the hard reality of soft power. Washington: Brassey's Inc, 2004. 277 p.

ARQUILLA, J.; RONFELD, D.; ZANINI, M. **TERRORISM AND COUNTERTERRORISM:** Understanding the New Security Environment. 3. ed. New York: Mc Graw-Hill, 2009. 134 - 157 p.

ARQUILLA, J.; RONFELDT, D. **Cyberwar is Coming!**, 1993. Disponível em: <http://www.rand.org/pubs/reprints/2007/RAND_RP223.pdf>. Acesso em: 05 junho 2010.

BARRY, C. L.; ZIMET, E. **Cyberpower and National Security**. Washington: Potomac Books, Inc, 2009. p. 285 - 308 p.

BILLO, C. G.; CHANG, W. **Cyber Warfare:** an analysis of the means and motivation of selected nation states, 2004. Disponível em: <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf>. Acesso em: 27 setembro 2010.

BOBBITT, P. **A guerra e a paz na história moderna:** o impacto dos grandes conflitos e da política na formação das nações. Tradução de Cristiana Serra. Rio de Janeiro: Campus, 2003. 883 p.

BRASIL. **Constituição da República Federativa do Brasil**, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 19 nov 2010.

BRASIL, Ministério da Defesa. **Política de Defesa Nacional:** Diretrizes, 2005. Disponível em: <https://www.defesa.gov.br/pdn/index.php?page=diretrizes>. Acesso em: 25 julho 2010.

_____ **Estratégia Nacional de Defesa**. Brasília: [s.n.], 2008a.

_____ **MD 33-2:** Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas. Brasília: [s.n.], 2008b.

BRASIL, Ministério da Defesa, Comando da Aeronáutica. **NSCA 7-7:** Estrutura e competências do Sistema de Tecnologia da Informação do Comando da Aeronáutica (STI). Brasília: [s.n.], 2004.

_____ **DCA 1-1:** Doutrina Básica da Força Aérea Brasileira. Brasília: [s.n.], 2005.

_____ **NSCA 7-13:** Segurança de Sistemas de Tecnologia da Informação no Comando da Aeronáutica. Brasília: [s.n.], 2006.

CAPASO, P. F. **TELECOMUNICATIONS AND INFORMATION ASSURANCE:** America´s Achilles Heel?, 1997. Disponível em: <http://pirp.harvard.edu/pubs_pdf/capasso/capasso-p97-1.pdf>. Acesso em: 29 setembro 2010.

CARR, J. **Inside Cyber Warfare**. Sebastopol, CA: O'Reilly, 2009. 212 p.

CBS. **Cyber War:** Sabotaging the System - 60 Minute - CBS News, 2009. Disponível em: <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml>. Acesso em: 28 julho 2010.

CEBROWSKI, A. K.; GARSTKA, J. J. **NETWORK-CENTRIC WARFARE:** Its Origin and Future, 1998. Disponível em: <http://www.kinection.com/ncoic/ncw_origin_future.pdf>. Acesso em: 10 julho 2010.

CENTRO DE COMPUTAÇÃO DA AERONÁUTICA DO RIO DE JANEIRO. **CTIR - Centro de Tratamento de Incidentes de Segurança em Redes**, 2010a. Disponível em: <http://www.ctir.intraer/index.php>. Acesso em: 01 junho 2010.

_____ **CTIR:** Indicadores, 2010b. Disponível em: <http://www.ctir.intraer/index.php?pag=indicadores>. Acesso em: 27 julho 2010.

_____ **I Seminário de Defesa Cibernética**, 2010c. Disponível em: <http://www.ccarj.intraer>. Acesso em: 27 julho 2010.

CERT.BR. **Cartilha de Segurança para Internet**, 2006. Disponível em: <http://cartilha.cert.br>. Acesso em: 24 julho 2010.

CHAMBERS, J. **The Devil's Horsemen:** The Mongol Invasion of Europe. New York: Book Sales, 2003. 200 p.

CLAUSEWITZ, C. V. **Da Guerra**. 3. ed. São Paulo: Wmf. Martins Fontes, 2010.

COIMBRA, D. S. **A INFLUÊNCIA DAS ATIVIDADES DA GUERRA CIBERNÉTICA EM UM SISTEMA DE COMANDO E CONTROLE**. Rio de Janeiro: Escola de Comando e Estado-Maior da Aeronáutica, 2009.

COLARIK, A. M. . J. L. J. **Cyber Warfare and Cyber Terrorism**. Hershey: Information Science Reference, 2008. 565 p.

COLEMAN, K. G. **Department of Cyber Defense:** An organization whose time has come!, 2007. Disponível em: <http://www.technolytics.com/Dept_of_Cyber_Defense.pdf>. Acesso em: 27 julho 2010.

DCSINT, US Army Training and Doctrine Command. **Critical Infraestructure:** Threats and Terrorism, 2006. Disponível em: <http://www.fas.org/irp/threat/terrorism/sup2.pdf>. Acesso em: 24 julho 2010.

DEFENSE SCIENCE BOARD TASK FORCE. **Report of the defense Sciense Board Task Force on Information Warfare - Defense**, 1996. Disponível em: <http://www.acq.osd.mil/dsb/reports.htm>. Acesso em: 02 setembro 2010.

DHANJANI, N.; HARDIN, B.; RIOS, B. **HACKING:** The Next Gneration. Sebastopol: O'reilly, 2009. 279 p.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA. **DTI:** Organograma, 2010. Disponível em: <http://www.dti.intraer/documentos/organograma/Microsoft%20PowerPoint%20-%20ORGANOGRAMA%20DTI.pdf>. Acesso em: 27 julho 2010.

DOUHET, G. **O Domínio do Ar**. Rio de Janeiro: INCAER, 1987.

DUTRA, A. M. C. **Introdução à Guerra Cibernética:** a necessidade de um despertar brasileiro para o assunto, 2007. Disponível em: <http://www.sige.ita.br/IX_SIGE/Artigos/GE_39.pdf>. Acesso em: 17 julho 2010.

EUA, Air Force Doctrine Center. **INFORMATION OPERATIONS:** Air Force Doctrine Document 2-5, 1998. Disponível em: <http://www.globalsecurity.org/military/library/policy/usaf/afdd/afdd2-5.pdf>. Acesso em: 30 setembro 2010.

EUA, Chairman of the Joint Chiefs of Staff. **COMMAND AND CONTROL WARFARE**, 1990. Disponível em: <http://www.dod.gov/pubs/foi/reading_room/732.pdf>. Acesso em: 30 setembro 2010.

EUA, Department of Air Force, Air Force Doctrine Center. **AIR FORCE BASIC DOCTRINE**, 1997. Disponível em: <http://www.globalsecurity.org/military/library/policy/usaf/afdd/afdd1.pdf>. Acesso em: 30 setembro 2010.

EUA, Department of Defense. **CAPSTONE CONCEPT FOR JOINT OPERATION**, 2005. Disponível em: <http://www.dtic.mil/futurejointwarfare/concepts/approved_ccjov2.pdf>. Acesso em: 01 outubro 2010.

EUA, Joint Staff. **INFORMATION WARFARE - A STRATEGY FOR PEACE - The Decisive Edge for War**, 1996. Disponível em: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA318379&Location=U2&doc=GetTRDoc.pdf>. Acesso em: 01 outrubro 2010.

FADOK, D. S. **John Boyd e John Warden:** A busca da paralisia estratégica pelo poder aéreo. Maxwell Air Force Base: Air University Press, 1995. 61 p.

FEWELL, M. P.; HAZEN, M. **NETWORK-CENTRIC WARFARE - Its Nature and Modelling**, 2003. Disponível em: <http://www.dsto.defence.gov.au/publications/2596/DSTO-RR-0262.pdf>. Acesso em: 01 setembro 2010.

FREDERIKS, B. E. **INFORMATION WARFARE AT THE CROSSROADS**, 1997. Disponível em: <http://www.dtic.mil/doctrine/jel/jfq_pubs/1816pgs.pdf>. Acesso em: 12 agosto 2010.

F-SECURE CORP. **F-Secure Security Center**, 2010. Disponível em: <http://www.f-secure.com/en_US/security>. Acesso em: 24 julho 2010.

FULLER, J. F. C. **The Foundations of Science of War**, 1926. Disponível em: <http://www.cgsc.edu/carl/resources/csi/fuller2/fuller2.asp>. Acesso em: 18 setembro 2010.

GEERS, K. **Cyberspace and the Changing Nature of Warfare**, 2008. Disponível em: <http://www.scmagazineus.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/>. Acesso em: 17 junho 2010.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. São Paulo: Atlas, 2008.

GOLDEBERG, I. K. **GLOSSARY OF INFORMATION WARFARE TERMS**, 2005. Disponível em: <http://www.psycom.net/iwar.2.html>. Acesso em: 30 setembro 2010.

GONZALES, D. E. A. **Network-centric operations case study:** air-to-air combat without Link 16, 2005a. Disponível em: <http://www.rand.org/pubs/monographs/2005/RAND_MG268.pdf>. Acesso em: 01 outubro 2010.

GONZALES, D. E. A. **Network-centric operations case study:** the Striker Brigade Combat Team, 2005b. Disponível em: <http://www.rand.org/pubs/monographs/2005/RAND_MG267-1.pdf>. Acesso em: 01 outrubro 2010.

HANSON, V. D. **Porque o ocidente venceu:** Massacre e cultura - da Grécia antiga ao Vietnã. Tradução de Fernanda Abreu. Rio de Janeiro: Ediouro, 2002. 703 p.

HENNING, P. R. **AIR FORCE INFORMATION WARFARE DOCTRINE:** Valuble or Valueless?, 1997. Disponível em: <http://www.au.af.mil/au/awc/awcgate/acsc/97-0604c.pdf>. Acesso em: 15 setembro 2010.

KRAMER, F. D. in **CYBERPOWER AND NATIONAL SECURITTY**. Washington: Potomac Books, Inc, 2009. p. 3 - 42 p.

KRAMER, F. D.; STARR, S. H.; WENTZ, L. K. (Eds.). **CYBERPOWER AND NATIONAL SEGURITY**. Washington: Potomac Books, Inc, 2009.

KREKEL, B. **CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOTATION**. McLean: Northrop Grumman, 2009.

LESSER, I. O. E. A. **COUNTERING THE NEW TERRORISM**. Washington: RAND, 1998. 181 p.

LIANG, Q.; XIANGSUI, W. **A guerra além dos limites:** conjecturas sobre a guerra e a tática na era da globalização. Beijing: Pla literature and Arts Publishing House, 1999. 255 p.

LIBICKI, M. C. **What is Information Warfare?**, 1995. Disponível em: <http://www.dodccrp.org/files/Libicki_What_Is.pdf>. Acesso em: 10 maio 2010.

LIBICKI, M. C. in **CYBERPOWER AND NATIONAL SECURITY**. Washington: Potomac Books, Inc, 2009. p. 275 - 284 p.

LIND, W. S. **Military Doctrine, Force Structure, and The Defense Decision-Making Process**, 1979. Disponível em: <http://www.airpower.maxwell.af.mil/airchronicles/aureview/1979/may-jun/lind.html>. Acesso em: 02 outubro 2010.

LIPSCOMB, G. **PRIVATE AND PUBLIC DEFENSES AGAINST SOVIET INTERCEPTION OF U.S. TELECOMUNICATIONS:** Problems and Policy points, 1979. Disponível em: <http://pirp.harvard.edu/pubs_pdf/lipscom/lipscom-p79-3.pdf>. Acesso em: 30 setembro 2010.

LITTLETON, M. J. **INFORMATION AGE TERRORISM:** Toward Cyberterror, 1995. Disponível em: <http://edocs.nps.edu/npspubs/scholarly/theses/1995/Dec/95Dec_Littleton.pdf>. Acesso em: 07 outubro 2010.

MCKENZIE, K. F. J. **THE REVENGE OF THE MELIANS:** asymetric threat and the next QDR. Washington: National Defense University, 2000.

NYS, N. Y. S. O. O. C. S. **Automated Information Systems Security Policy Glossary**, 2010. Disponível em: <http://www.cscic.state.ny.us/lib/glossary/>. Acesso em: 24 julho 2010.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Carta das Nações Unidas**, 1945. Disponível em: <http://www.onu-brasil.org.br/documentos_carta.php>. Acesso em: 09 outubro 2010.

OSINGA, F. P. B. **Science, Strategy and War:** The strategic theory of John Boyd. New York: Routledge, 2007.

PORTAL TERRA. **Aviões não-tripulados dos EUA são alvo de hackers no Iraque**, 2009. Disponível em: <http://tecnologia.terra.com.br/interna/0,OI4162955-EI4799,00-Avioes%20naotripulados%20dos%20EUA%20sao%20alvo%20de%20hackers%20no%20Iraque.html>. Acesso em: 09 outubro 2010.

PUFENG, W. **THE CHALENGE OF INFORMATION WARFARE**, 1995. Disponível em: <http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm>. Acesso em: 28 setembro 2010.

RATTRAY, G. J. **Strategic Warfare in Cyberspace**. Cambridge: MA, 2001. 517 p.

SCHMITT, M. N. **PREEMPTIVE STRATEGIES IN INTERNATIONAL LAW**, 2003. Disponível em: <http://libertyparkusafd.org/lp/Hale/Special%20Reports/Preventive%20War%20Doctrine/Preemptive%20Strategies%20and%20International%20Law.pdf>. Acesso em: 09 outubro 2010.

SCHWARTAU, W. **Information Warfare:** Cyberterrorism: Protecting your personal security in the eletronic age. 2. ed. Nova Iorque: Thunder's Mouth Press, 1996. 768 p.

SEVERSKY, A. P. D. **A Vitória pela Força Aérea**. Rio de Janeiro: INCAER, 1988.

SKLEROV, M. J. **INSIDE CYBER WARFARE**. Sebastopol: O'Reilly, 2009. 45 - 75 p.

STEIN, G. J. **Information Warfare**, Maxwell AFB, Spring 1995. Disponível em: <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/stein.htm>. Acesso em: 17 junho 2010.

SYMANTEC CORP. **Symantec Security Response Website**, 2010. Disponível em: <http://www.cscic.state.ny.us/lib/glossary/>. Acesso em: 24 julho 2010.

TALBOT, D. **How Technology Failed in Iraq**, 2004. Disponível em: <http://www.technologyreview.com/printer_friendly_article.aspx?id=13893&channel=computing&section=>. Acesso em: 01 outrubro 2010.

THOMAS, T. L. **LIKE ADDING WINGS TO THE TIGER:** Chinese Information War Theory and Practice, 2000. Disponível em: <http://fmso.leavenworth.army.mil/documents/chinaiw.htm>. Acesso em: 28 setembro 2010.

THOMAS, T. L. in **CYBERPOWER AND NATIONAL SECURITY**. Washington: Potomac Books, Inc, 2009. p. 465 - 488 p.

TZU, S. **A Arte da Guerra**. 34. ed. Rio de Janeiro: Record, 2004. 112 p.

UDA, R. T. **Cybercrime, Cyberterrorism and Cyberwarfare:** Crime, Terror, and War without Convencional Weapons. LaVergne: Xlibris Corporation, 2009. 243 p.

WARDEN, J. **The enemy as a System**, 1995. Disponível em: <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm>. Acesso em: 17 junho 2010.

WARDEN, J. **The Air Campaign**. Lexington: toExcel, 2010. 181 p.

WHINE, M. **Islamist Organizations on the Internet**, 1998. Disponível em: <http://www.ict.org.il/Articles/tabid/66/Articlsid/716/Default.aspx>. Acesso em: 10 outubro 2010.

YOSHIHARA, T. **CHINESE INFORMATION WARFARE:** A Phantom menace or emerging Threat?, 2001. Disponível em: <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub62.pdf>. Acesso em: 28 setembro 2010.

GLOSSÁRIO

BACKBONE – espinha dorsal de comunicações, é o canal principal responsável por toda interconexão de comunicações.

BANNERS – curta mensagem publicitária em um *site* da *internet*, normalmente, com um *link* para a página do anunciante.

BOTNET – rede de computadores infectada que pode ser controlada remotamente por um servidor de comando e controle.

CIBERESPAÇO – do inglês *cyberspace*, diz respeito a computadores, redes e conjuntos de redes de computadores interligados. Neste conjunto de meios, dados trafegam, são armazenados, processados e acessados.

CIBERNÉTICA – ciência que tem por objeto o estudo comparativo dos sistemas e mecanismos de controle automático, regulação e comunicação nos seres vivos e nas máquinas.

CIBERPIRATA – *hacker* ou pirata eletrônico, comumente utilizado para denominar pessoa com profundo conhecimento de informática que eventualmente os utiliza para violar sistemas ou exercer outras atividades ilegais.

COMMAND AND CONTROL WARFARE **(C2W)** – Guerra de Comando e Controle.

DISTRIBUTED DENIAL OF SERVICE **(DDOS)** – ataque distribuído de negação de serviço.

DOMAIN NAME SERVICE **(DNS) –** serviço de nome de domínio, é o serviço responsável em transformar os endereçamentos da web em nome de fácil entendimento humano e vice-versa, como exemplo 10.10.1.10 poderá ser traduzido pelo DNS como www.portal.intraer.

E-MAIL – mesmo que *email,* mensagem de correio eletrônico.

FIRMWARE – Programas de computadores gravados nos dispositivos.

GUERRA CINÉTICA – modalidade de guerra travada no mundo real, envolvendo tropas, aviões, carros de combate e demais meios não virtuais.

HACKERS – ver ciberpirata.

INTRUSION PREVENTION SYSTEM **(IPS)** – Sistema de Prevenção de Intruso. É um dispositivo de segurança de rede que monitora o tráfego e/ou atividades dos sistemas em busca de comportamentos maliciosos ou não desejáveis, em tempo real, para bloquear ou prevenir essas atividades.

LOG – registro, normalmente automatizado, de atividades realizadas em determinado sistema.

SITE – conjunto de páginas *Web* que fazem parte de um endereço eletrônico acessado pelos navegadores de rede do tipo do *Internet Explorer*.

SOFTWARE – Programas de computadores.

SPAMMER – Pessoa que envia spam.

SPYWARE – *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

VÍRUS – programa, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos.

WEB – ver World Wide Web.

WORLD WIDE WEB **(WWW) –** conhecida rede mundial de computadores, denominada de *Internet*.

WORM – programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador

APÊNCICE A - RECURSOS PARA ATAQUES DIGITAIS

Neste tópico serão abordados os principais recursos disponíveis, conhecidos na atualidade, para ações ofensivas de guerra cibernética, lembrando que tais recursos podem e devem ser utilizados em conjunto, no sentido de maximizar os resultados pretendidos.

1 Adware

Segundo o DCSINT (2006), é toda aplicação de *software* onde *banners* de propaganda são mostrados enquanto o programa está em execução. Os autores dessas aplicações incluem o código adicional que disponibiliza essas propagandas, que podem ser vistas através de uma janela ou da barra que aparece na tela do computador. A justificativa para a utilização do *adware* é que ele ajuda a recuperar custos do desenvolvimento dos programas e para mantê-los reduzidos aos usuários.

A crítica quanto à utilização do *adware* reside no fato do mesmo incluir código que pode rastrear uma informação pessoal do usuário e passá-la a terceiros sem autorização ou conhecimento. Esta prática é conhecida como spyware, e será tratada no decorrer deste trabalho.

2 Boato *(Hoax)*

E-mail que, segundo o CERT.BR (2006), possui conteúdo alarmante ou falso e que, geralmente, tem como remetente ou aponta como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de *e-mail*, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

3 Bomba Lógica (*Logic Bomb*)

“Uma rotina programada que destrói dados através da formatação de discos rígidos ou da inserção aleatória de lixo nos arquivos de dados.” (DCSINT, 2006).

4 Bot

Segundo a F-Secure Corp (2010), é um programa malicioso que, uma vez instalado em um sistema computadorizado, permite ao atacante escravizar o sistema em uma rede de sistemas escravizados de forma similar, conhecida como "*botnet*". Os computadores individuais em uma *botnet* podem ser referenciados como bot ou zumbi.

Um tipo especial de bot, conhecido como *IRCbot*, é um programa que conecta a um canal de *Internet Relay Chat* (IRC) como um usuário normal ou um *botnet*. Tal canal é utilizado nas salas de bate-papo difundidas pela *internet*.

O termo "*bot*" também é utilizado de forma mais genérica para programas que realizam operações automatizadas como escanear páginas da *web*, calcular estatísticas e assim por diante. Estes programas, geralmente, não são considerados maliciosos.

5 Botnet

Uma *Botnet*, segundo a F-Secure Corp. (2010), é uma rede de computadores infectada por *bots,* que pode ser controlada remotamente por um servidor de comando e controle. Cada computador infectado é conhecido como um computador zumbi ou zumbi. Um atacante ou grupo de atacantes exploram os recursos coletivos de uma *botnet* para realizar uma ação maliciosa principal como enviar milhões de *spam*, realizando assim um ataque do tipo DDoS, dentre outros.

6 Cavalo de Tróia (*Trojan Horse*)

De acordo com o CERT.BR (2006), é um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo e etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

7 Código Malicioso (*Malware*)

"*Software* ou *firmware* que é intencionalmente inserido em um Sistema de Informações Gerenciais para uma função desautorizada." (NYS, 2010).

Segundo a Symantec Corp. (2010), códigos maliciosos destrutivos utilizam ferramentas populares de comunicação para se espalhar, incluindo *worms* enviados através de *e-mail* e mensagens instantâneas, cavalos de tróia inseridos por *sites* da *web* e arquivos infectados por vírus, baixados de conexões ponto-a-ponto. Estes códigos, ainda, fazem buscas para explorar vulnerabilidades existentes nos sistema fazendo sua entrada de forma "quieta e silenciosa".

8 *Denial of Service* (DoS)

Este é um tipo de ataque que, segundo a F-Secure Corp. (2010), é conduzido através da *internet*, onde uma quantidade enorme de dados é enviada a um sistema computadorizado ou outro recurso (programas, *websites* ou redes), com o objetivo de sobrecarregá-lo ou interromper o seu funcionamento. Ataques DoS são tipicamente conduzidos por um único sistema computadorizado ou pequeno grupo destes sistemas e podem ser realizados de diversas maneiras.

Mesmo que um ataque DoS não resulte em uma interrupção total, muitos recursos serão direcionados para lidar com o mesmo, assim a performance do sistema será significativamente degradada ou outros usuários estarão impossibilitados de utilizar o sistema ou recursos até que o ataque tenha terminado.

9 *Distributed Denial of Service* (DDoS)

Segundo a F-Secure Corp. (2010), é um tipo de ataque conduzido pela *internet* usando recursos combinados de diversos computadores para bombardear e, frequentemente, interromper o funcionamento de um sistema computadorizado ou outro recurso ligado. Existem diversos tipos de ataques DDoS, que irão variar na maneira como o ataque é conduzido.

Ataques DDoS são, usualmente, realizados por *botnets*, uma vez que recursos combinados de todos os computadores de uma rede podem gerar uma

quantidade terrível de dados, suficiente para sobrecarregar a maioria das defesas dos objetivos, em segundos.

Em um exemplo de como um ataque DDoS é conduzido, um atacante explora uma vulnerabilidade em um sistema de computador e o transforma no seu mestre DDoS usando um *Software* de Controle Remoto. Mais tarde, o invasor usa o sistema mestre para identificar e controlar zumbis com a finalidade de realizar ataques.

10 Engenharia Social

Método de ataque onde, segundo o CERT.BR (2006), uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

11 Exploit

“Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um *software* de computador.” (CERT.BR, 2006).

12 Falsa Identidade

Método, segundo o CERT.BR (2006), onde o falsificador atribui-se identidade ilegítima, podendo se fazer passar por outra pessoa, com objetivo de obter vantagens indevidas, como por exemplo, obter crédito, furtar dinheiro de contas bancárias das vítimas, utilizar cartões de crédito de terceiros, entre outras.

13 Ferramenta *Hack*

Ferramentas que, segundo a Symantec Corp. (2010), podem ser usadas por um *hacker* ou usuário não autorizado para atacar um computador, obtendo acesso indevido através de alguma forma de identificação, até mesmo através do sistema de digitais.

Embora algumas ferramentas *hack* possam ser válidas para funções legítimas, sua capacidade de facilitar acessos não autorizados as transforma em um risco.

Ferramentas *hack* são também usualmente utilizadas para obter informações ou obter acesso a servidores que sub-repticiamente utilizam métodos para contornar ou ultrapassar mecanismos de segurança óbvios herdados de sistemas onde elas estão instaladas ou facilitar a tentativa de desabilitar um computador alvo, prevenindo então sua utilização normal.

Ferramentas *hack* também podem ser usadas como programas para facilitar ataques a computadores de terceiros como parte de um ataque DoS direto ou distribuído. Um exemplo de ferramenta *hack* é um armazenador de teclas pressionadas – um programa que rastreia e armazena as teclas pressionadas por um indivíduo e pode mandar essa informação a um hacker.

14 Harvesting

"Técnica utilizada por *spammers*, que consiste em varrer páginas w*eb*, arquivos de listas de discussão, entre outros, em busca de endereços de *e-mail*." (CERT.BR, 2006)

15 Keylogger

Programa, de acordo com o CERT.BR (2006), capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um *site* de comércio eletrônico ou *Internet Banking*, para a captura de senhas bancárias ou números de cartões de crédito.

16 Pharming

Segundo a F-Secure Corp. (2010), é um tipo de ataque de engenharia social onde um *site* fraudulento é usado para enganar um usuário fazendo-o fornecer informações pessoais sensíveis, como sua conta bancária ou detalhes de

sua conta de correio eletrônico. Um ataque de *Pharming* tipicamente depende de um "envenenamento de DNS" que envolve o plantio de um arquivo de servidor do usuário ou um servidor DNS com informações falsas.

Neste caso, o envenenamento de DNS redireciona os usuários de *site* legítimo para uma cópia sob o controle do atacante. Assim toda informação inserida pelo usuário no *site* falso estará comprometida.

Um ataque de *Pharming* poderá também ser usado em conjunção a uma tentativa de *phishing* (técnica tratada na sequência deste trabalho). Neste caso uma mensagem mal direcionada leva o usuário a acessar de forma insuspeita o *site* malicioso.

17 Phishing

Segundo o CERT.BR (2006), é também conhecido como *phishing scam* ou *phishing*/*scam*. É uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, este tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na *Internet*. Atualmente, o termo também se refere a mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

18 Porta dos Fundos (*Backdoor*)

"Programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado." (CERT.BR, 2006)

19 Rootkit

Conjunto de programas que, segundo o CERT.BR (2006), têm como finalidade esconder e assegurar a presença de um invasor em um computador comprometido. É importante ressaltar que o nome *rootkit* não indica que as

ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *Administrator*) em um computador, mas sim para manter o acesso privilegiado em um computador previamente comprometido.

20 Scam

"Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras." (CERT.BR, 2006).

21 Scan

"Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores." (CERT.BR, 2006).

22 Scanner

Programa utilizado, conforme o CERT.BR (2006), para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

23 Screenlogger

"Forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado." (CERT.BR, 2006)

24 Sniffer

Segundo o CERT.BR (2006), é um dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis

(como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

25 Spam

"Termo usado para se referir aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas." (CERT.BR, 2006).

26 Spyware

De acordo com o CERT.BR (2006), esse termo é utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

27 Trapdoor

"Um ponto de entrada secreto e não documentado, em programa de computador, usado para autorizar acesso sem os métodos normais de autenticação." (NYS, 2010).

28 Vírus

Programa, ou parte de um programa de computador, normalmente malicioso, que, segundo o CERT.BR (2006), se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

29 Web Bug

"Imagem, normalmente muito pequena e invisível, que faz parte de uma página *Web* ou de uma mensagem de *e-mail*, e que é projetada para monitorar quem está acessando esta página Web ou mensagem de e-mail." (CERT.BR, 2006).

30 Worm

Programa, de acordo com o CERT.BR (2006), capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.

Verificamos que a gama de recursos disponíveis para ações de Guerra Cibernética é bem extensa, ainda mais se for levado em consideração que os mesmos podem ser utilizados de forma combinada. Essa verificação serve como grande alerta a uma força militar quanto à possibilidade de usar este arsenal em seu favor, bem como quanto à grandiosidade do trabalho de defesa a ser implementado.

Uma vez colocado os recursos disponíveis para ações ofensivas, fica a necessidade de apresentar um fator fundamental a ser levado em consideração, que é a aquisição de inteligência sobre os alvos, discutido no próximo tópico. Tal fator tem se mostrado essencial para viabilizar a condução da Guerra Cibernética, não só para que os ataques digitais venham a ter sucesso, bem como para implementação de uma defesa.

APÊNDICE B - COLETA DE INTELIGÊNCIA

Para executar com sucesso um ataque contra uma organização, ou implementar uma defesa, os autores dessa atividade devem primeiro realizar um processo de reconhecimento para adquirir inteligência, sobre o seu adversário, de diversas formas.

Segundo Dhanjani, Hardin e Rios (2009) muitos métodos tradicionais para obter inteligência sobre alvos ainda funcionam nos dias de hoje, como busca no lixo, busca em banco de dados públicos e busca em máquinas de pesquisa. No entanto novos métodos que são baseados na coleta de informações através de tecnologias, como aplicações de redes sociais, estão se tornando mais comuns.

É evidente que toda força, que intencione utilizar a Guerra Cibernética, deve executar esforços no preparo de sua estrutura de inteligência, de forma a capacitar-se para fornecer informações, adequadas e úteis, à condução da guerra no ambiente cibernético.

Estas informações não devem se limitar, apenas, a aspectos técnicos a respeito de como atingir o adversário, mas devem, também, ser direcionadas no sentido de identificar, corretamente, o quê deve ser atingido.

Além deste viés ofensivo, é necessário, também, conhecer as técnicas de coleta de informações de inteligência, para a execução de um plano próprio de contrainteligência visando negar suas próprias informações ao adversário.

Do ponto de vista do atacante, é extremamente importante realizar o reconhecimento da forma mais dissimulada possível. De acordo com Dhanjani, Hardin e Rios (2009), uma vez que a aquisição de informação é um dos primeiros passos que o atacante deve realizar, ele deve tomar as devidas precauções para não realizar nada que possa alertar o alvo. Essas informações acerca do alvo, sempre auxiliam o atacante de alguma forma.

Portanto, serão apresentadas, a seguir, principalmente técnicas que não envolvem o envio de pacotes de rede sobre os alvos, e, portanto, mais difíceis de serem identificadas e rastreadas via sistemas de informações. Todas de acordo com o apresentado por Dhanjani, Hardin e Rios (2009).

1 Engenharia de Segurança Física

Obter informações através de meios físicos é uma tática tradicional que atacantes vem utilizando a algum tempo. Alguns exemplos de informações que um atacante pode obter através desses métodos, incluem diagramas de rede, informações financeiras, plantas, listas telefônicas e informações decorrentes de conflitos entre funcionários e de comunicações entre os mesmos.

2 Procura no Lixo

É um método de aquisição de informações onde o atacante realiza buscas através do acesso direto ao lixo de determinada organização. Embora esta técnica não seja nova, é ainda utilizada com sucesso para obter grande volume de inteligência.

3 Visita Direta ao Alvo

Atacantes, normalmente vão à locação do ataque para obter mais informações sobre o alvo. É consenso que atacantes podem obter muito conhecimento sobre uma organização apenas caminhando por ela e escutando a conversa de seus componentes.

4 Google Earth

O Google Earth é um *software* de mapeamento gratuito fornecido pela Google. Um atacante pode utilizá-lo para visualizar fisicamente o local, antes de visitá-lo pessoalmente, obtendo conhecimento espacial do alvo. Assim o atacante terá maior facilidade Mara misturar-se com os integrantes da organização, se já possui um conhecimento prévio dos caminhos utilizados pelos mesmos.

5 Engenharia Social de *Call Centers*

Engenharia social é a arte de obter informações de pessoas que não querem fornecê-las. Jornalistas, autoridades policiais e advogados utilizam estas

habilidades por profissão. Eles estudam técnicas para intimidar ou simpatizar com as pessoas de forma que estas acabam por fornecer informações. Atacantes cibernéticos usam técnicas similares para obter informações sensíveis de vítimas acima de qualquer suspeita.

Os *Call Centers* são uma excelente ferramenta para realizar tal empreendimento, por possuírem acesso a uma gama variada dos componentes de uma organização, além de poderem realizar a pesquisa de forma contínua.

6 Ataques Hackers a Ferramentas de Busca

Ferramentas de busca, por definição, são utilizadas achar e localizar informações na *Internet*. Adicionalmente a isto, os atacantes têm meios de usar estas ferramentas para identificar e localizar vulnerabilidades e dados confidenciais através das ferramentas de busca, além de poderem realizar tais atividades sem a necessidade de se expor.

6.1 Ataque *Hacker* Utilizando o Google

Atacantes podem utilizar o Google para obter informações básicas como listas de contato, documentos internos e estruturas organizacionais de alto nível, bem como localizar potenciais vulnerabilidades nas aplicações *web* da organização.

6.2 Ataque *Hacker* Automatizado a *Sites* de Busca

Um atacante pode utilizar uma ferramenta chamada SEAT (da sigla em inglês, *Search Engine Assessment Tool*)[19], desenvolvida pela empresa Midnight Research Labs, para automatizar os ataques hackers ao Google, Yahoo e MSN, dentre outras atividades.

---

[19] Tal ferramenta pode ser obtida no *site* http://midnightresearch.com/projects/search-engine-assessment-tool/.

7 Extraindo Metadados de Documentos Online

Metadados são dados sobre outros dados, como, por exemplo, os documentos Word do Microsoft Office. Tais dados podem conter informações sensíveis, como os usuários que manipularam determinados arquivos. Utilizando ferramentas de buscas e aplicativos, como o SEAT, é possível buscar documentos que possuem metadados e extrair informações destes.

8 Buscando Códigos Fonte

Diversos desenvolvedores, na tentativa de solucionar problemas, colocam códigos fontes (textos em linguagem de programação, utilizados para fazer um aplicativo) em sites de discussões na tentativa de solucioná-los, tais códigos fornecem preciosas informações a respeito da organização.

9 Exploração de Redes Sociais

Os atacantes podem utilizar as redes sociais, Facebook, Myspace e Twitter, dentre outras, para levantar informações a respeito de uma organização através de seus componentes.

Tal levantamento pode ser realizado por meio da engenharia social associada a diversos mecanismos presentes nas redes sociais como, por exemplo, a recuperação de senhas esquecidas.

Normalmente, tal recuperação é fornecida com respostas a respeito do usuário, respostas estas, costumeiramente, ligadas a informações pessoais que podem ser obtidas do próprio usuário, ou até mesmo com observação minuciosa dos dados disponibilizados na rede.

Essas redes sociais fornecem informações valiosas aos atacantes ao expor a rotina de seus usuários, fornecendo informações a respeito de localização e atividades, dentre outras.

10 Rastreamento de Funcionários

Os atacantes não, necessariamente, necessitam atacar diretamente as organizações. Eles podem atacar o seu elo mais fraco, que são seus funcionários. Obtendo informações do quadro de funcionários de uma determinada organização, os atacantes podem elaborar a correta forma de abordagem a um determinado componente de forma a obter informações necessárias a ataques contra a organização como um todo.

Fica evidente, a grande disponibilidade de métodos para aquisição de inteligência, porém os mesmos não serão de valia nenhuma para uma instituição, em sua estruturação para a condução da guerra Cibernética, se os mesmos não forem adquiridos observando-se um critério de seleção de informações. Assim ao coletar informações e necessário responder a pergunta: Quais informações são importantes?

> Qual informação é importante para um atacante e qual não é? Toda informação que um atacante puder encontrar poderá ser utilizada por alguma razão. Da perspectiva de um atacante, toda informação é importante. Algumas podem ser mais críticas do que outras. Informações que podem ser consideradas críticas para um atacante podem incluir:
> - Uma informação identificável pessoal de um funcionário, como telefone residencial e de trabalho, endereço de trabalho e residencial, histórico criminal, número de seguro social e relatórios de crédito;
> - Arquitetura de redes, incluindo o número de servidores *web* e de *email*, sua localização e a versão do *software* que elas usam;
> - Arquivos da organização, incluindo arquivos de banco de dados, diagramas de rede, documentação e artigos internos, planilhas e assim por diante;
> - Informações das organizações como fusões e aquisições, parceiros de negócios, serviços de hospedagem e assim por diante;
> - Informações organizacionais, incluindo organogramas detalhando a estrutura organizacional e a cadeia hierárquica; e
> - Interações de trabalho detalhando informações como quem se da bem no trabalho, a frequência com a diretoria se reporta com a gerência, qual a frequência com que os gerentes se comunicam com seus subordinados, com se comunicam (via email, telefone e BlackBerry) e assim por diante.
>
> As informações explicitadas aqui podem ser públicas ou privadas. Atacantes que realizaram suas pesquisas preliminares são grandemente recompensados. Toda informação obtida durante o reconhecimento pode beneficiar o ataque de alguma forma, inclusive com a utilização de informações públicas para ganhar informações internas sensíveis. (DHANJANI, HARDIN e RIOS, 2009, p. 22 -23, tradução nossa).

Salienta-se que as técnicas apresentadas não esgotam o assunto, são somente uma amostragem de métodos existentes, e disponíveis para uma Força

Militar realizar a fundamental tarefa de inteligência, sem a qual, será praticamente inviabilizada a Guerra Cibernética.

A aquisição de inteligência, por si só, não habilita uma Força Militar a multiplicar sua força com a utilização dos conceitos de Guerra Cibernética, para tal feito, é necessário que a referida Força realize a Guerra Cibernética em consonância com doutrinas de guerra que a norteiem em suas atividades, conforme apresentado no próximo item.