UMA VISÃO DA EVOLUÇÃO DAS GUERRAS MODERNAS: A AMEAÇA DA GUERRA CIBERNÉTICA NO CONFLITO DE QUARTA GERAÇÃO

"Ao nos aproximarmos do século XXI, nossos inimigos ampliaram os campos de batalha – do espaço físico para o espaço cibernético... Em vez de invadir nossas praias ou lançar bombardeios, esses adversários podem tentar empreender ataques cibernéticos contra os nossos sistemas militares críticos e a nossa base econômica... Se quisermos que nossos filhos cresçam em segurança e liberdade, devemos adotar, em relação a essas novas ameaças do século XXI, o mesmo rigor e determinação que aplicamos aos piores desafios à segurança deste século."

Ex-Presidente norte-americano Bill Clinton
Discurso na formatura de turma da Academia Naval
Estados Unidos da América (EUA)
22 de maio de 1998

ALEXANDRE ARTHUR CAVALCANTI **SIMIONI***
Capitão de Corveta (FN)

SUMÁRIO

INTRODUÇÃO

Ao entrarmos neste novo milênio, a emergência de novas ameaças globais e seus reflexos têm sido uma preocupação para todos os Estados no campo da segurança internacional, especialmente no que diz respeito aos conflitos de caráter multidimensional, ou seja, aqueles que envolvem ações em terra, mar, ar, espaço exterior, espectro eletromagnético e ciberespaço.

Uma característica que marcou o século XX e que continua presente neste início do século XXI é a distinção entre guerra e paz, que se tornou cada vez mais obscura. Exemplo disso foi a Segunda Guerra Mundial, que não começou com declarações de guerra (exceto em alguns poucos lugares) e tampouco terminou com declarações de paz. Após esse período, o mundo presenciou uma fase tão difícil de classificar, seja como guerra seja como paz, que o neologismo "guerra fria" teve de ser inventado para descrevê-lo. (HOBSBAWM, 2007)

No auge desse período da bipolaridade havia uma corrente de estudiosos que des-

* Chefe da Divisão de Trabalhos Acadêmicos do Centro de Instrução Almirante Sylvio de Camargo.

crevia o século XX como sendo de "pequenas guerras", pois, como a guerra convencional existente entre Estados tornou-se praticamente impossível de eclodir em função da ameaça nuclear, verificava-se, então, uma expansão dos conflitos na periferia, que passaram a ser denominados como de "baixa-intensidade", "guerrilhas", "irregulares", "assimétricos" etc[1].

Fig 1: Ciberwar
Fonte: www.infowars.net

Com o colapso da União das Repúblicas Socialistas Soviéticas (URSS) em 1991 e, consequentemente, com a desestabilização do concerto internacional pela ruptura do equilíbrio entre as potências mundiais[2], o mundo passa a presenciar o surgimento de um outro cenário denominado de nova ordem mundial, caracterizado pela superação da bipolaridade Leste-Oeste e pela ratificação da hegemonia militar norte-americana[3], capaz de declarar guerra a qualquer outro Estado, em qualquer lugar do globo, sem temer represália.

No imediato pós-Guerra Fria, acreditava-se em *uma era de paz e prosperidade*, pois, como na visão idealista de Francis Fukuyama, "um mundo feito de democracias liberais teria menor incentivo para as guerras"[4]. Porém, esta esperança de um mundo sem guerras "catastróficas" de caráter global, como as vivenciadas no século XX, foi dissolvida ao presenciarmos conflitos como os de Somália, Ruanda, Bósnia, Kosovo, Chechênia, Afeganistão e Iraque. Donald Kagan (*apud* SILVA, 2004) já apontava que "há mais de dois séculos a única coisa mais comum que as previsões sobre o fim da guerra tem sido a própria guerra (...) [uma vez que] estatisticamente, a guerra tem sido mais comum que a paz" na história da humanidade.

---

[1] Havendo, neste momento, uma inversão da máxima de Clausewitz – "a guerra é a continuidade da política por outros meios" –, já que neste período a política é a continuidade da guerra, pois a guerra pelas armas nucleares se torna improvável. (TEIXEIRA DA SILVA, 2006)

[2] Caracterizada pela ameaça da Mútua Destruição Assegurada entre os EUA e a URSS por armas nucleares.

[3] Como nas palavras de Chomsky (2003): "Nunca houve na história nada remotamente parecido com o quase monopólio de meios de violência em larga escala em poder de um único país".

[4] Como esclarece Saraiva (2007): "Francis Fukuyama (1992) decretou o Fim da História, no início dos anos 90, por meio da publicação de um artigo de mesmo nome em um periódico americano, o The National Interest, ainda em 1989. Sua teoria tornou-se ícone para os liberais e neoliberais, que muito bem souberam usufruir de suas conclusões. Segundo ele, os conflitos, ao longo da história, sempre estiveram relacionados a questões ideológicas. Nesta lógica, com a derrota do comunismo e a afirmação do capitalismo como modelo triunfante, estava fadada a era da bipolaridade e de antagonismos entre as nações, prevalecendo a tendência da homogeneização de ideias e ações. Conferia às ciências naturais a responsabilidade de uniformizar as sociedades, a modernização e o desenvolvimento tecnológico, tornando possível a acumulação de riquezas e favorecendo potencialmente o processo de homogeneização das sociedades, no momento em que esta tecnologia fosse incorporada, independentemente de origens históricas ou culturais, favorecendo a modernização econômica, tornando todas organizações sociais parecidas. Como consequência desse processo, estavam a aproximação maior entre os povos e a disseminação de uma cultura consumista universal, movendo o mundo em direção ao capitalismo".

Portanto, o que irá marcar o início desta nova ordem mundial é a insegurança global, na qual temas como narcotráfico, crime organizado, corrupção, lavagem de dinheiro, ameaças ecológicas, ameaças aos direitos humanos, ameaças financeiras, ameaças no cyberespaço, pandemias globais e o novo terrorismo internacional passaram a fazer parte da pauta da nova agenda de segurança, por colocarem em risco a integridade dos povos, a estabilidade dos Estados e os esforços pela paz e pela segurança mundial[5].

No campo militar, o fim da Guerra Fria encerrou o período em que o planejamento estava ancorado em ameaças claramente definidas. Sabia-se, naquele momento, quem eram os "amigos" e quem eram os "inimigos". Com isso, era possível prever o dimensionamento da capacidade militar do oponente, bem como realizar o monitoramento de suas atividades, a fim de saber, com certa precisão e previsibilidade, o grau de ameaça. Atualmente, já não se sabe mais quem são os novos "inimigos". Com isso, as Forças Armadas deixaram de ser a principal ameaça à Segurança Nacional de um Estado, representando, dessa forma, uma mudança/evolução dos conceitos de guerra aceitos desde a Paz de Westfália[6].

Ainda que continuem existindo disputas territoriais, os conflitos estão cada vez mais ligados à apropriação indevida de recursos, ao controle de capitais, às sanções comerciais e a outros fatores econômicos. Esses novos fatores passaram a representar um novo modelo de ameaça às seguranças social, política, econômica e militar dos Estados. Assim, no início do século XXI, encontramo-nos em um mundo em que as operações armadas já não estão essencialmente nas mãos do Estado ou dos seus agentes autorizados e as partes beligerantes não têm características, *status* e objetivos em comum, exceto quanto à vontade de utilizar violência. (HOBSBAWM, 2007)

Diante dessa situação, o mundo passa a vivenciar uma época caracterizada pelas incertezas, em que as ameaças tornaram-se difusas, não sendo mais possível responder, com certa precisão, às perguntas básicas do estudo da Situação Militar do Inimigo – "o quê, quando, onde e com que valor" –, presentes em qualquer planejamento militar.

Outro fator de extrema relevância durante o período da Guerra Fria foi o extraordinário desenvolvimento científico-tecnológico em todas as áreas, motivado pela corrida armamentista entre os EUA e a URSS, o que vem trazendo, desde aquele momento, graves consequências para a segurança internacional. Diante desta nova realidade tecnológica, alguns países começaram a reduzir o efetivo de suas Forças Armadas e iniciaram a elevação da qualificação técnica de suas tropas, tendo em vista o avanço das tecnologias incorporadas aos armamentos, bem como das atualizações do pensamento militar e doutrinário que acabaram ganhando notoriedade após a Segunda Guerra do Golfo (1990-1991), com o aparecimento dos conceitos de Re-

[5] O processo de consolidação desta nova ordem mundial fica caracterizado no período de tempo existente entre dois fatos históricos que representaram pontos de inflexão no pensamento político-estratégico em nível mundial: a dissolução da União Soviética em 1991 e os atentados nos EUA em 2001, como expresso nas palavras da secretária de Estado norte-americano Condoleeza Rice: **"A queda do Muro de Berlim e a queda do World Trade Center representam o início e o fim de um longo período de transição."** (O destaque é nosso)

[6] Este Tratado de 1648 marca o fim das guerras privadas e o declínio das tropas de mercenários, proporcionando o desenvolvimento dos Estados Nacionais soberanos – com seus Exércitos e Marinhas permanentes – e o início das Relações Internacionais.

volução em Assuntos Militares (RAM)[7] e Revolução nos Assuntos Militares em Curso (RMC)[8], em um período denominado de Pós-Modernismo Militar (PMM).

Observa-se, a partir dos conceitos da RAM, uma rápida evolução tecnológica aplicada aos teatros de operações, em função da automação, abrangência, multifuncionalidade, da precisão e do poder de combate das tropas. Dessa forma, verifica-se uma expansão virtual do campo de batalha, tendo em vista a possibilidade de se conduzir as ações à distância, empregando os conceitos de *Network Centric Warfare*[9] e de C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance and Recconnaissance*), conjugados com as ações no cyberespaço e no espaço sideral[10].

Constata-se uma tendência "civilista" da guerra, ou seja, o aparecimento de "guerreiros não militares" penetrando na ambiência militar . . . É o surgimento de um novo modelo combatente: o guerreiro digital

Em paralelo a tal situação, constata-se uma tendência "civilista" da guerra, ou seja, o aparecimento de "guerreiros não militares" penetrando na ambiência militar, permitindo, desta forma, o emprego de uma multiplicidade de meios militares e, principalmente, não militares, sendo o *hacker* o primeiro a aparecer nesse ambiente, pelo alto impacto de suas ações. É o surgimento de um novo modelo combatente: o guerreiro digital. (LIANG e XIANGSUI, 1999)

Os atentados ao World Trade Center e ao Pentágono em 11 de setembro de 2001, levando à morte cerca de 3 mil pessoas de 88 nações, bem como as imagens inesquecíveis da destruição de dois ícones (capitalista e militar) do Estado norte-americano, marcaram de forma contundente as ameaças deste novo

---

[7] RAM – "São mudanças de paradigma na natureza e na condução das operações militares que tornam obsoletas ou irrelevantes certas capacidades de algumas forcas armadas da época, ou que criam novas capacidades em novas dimensões da guerra, ou ambos os casos." (EGN, p.3-1)

Segundo o chefe do Estado-Maior das Forças Armadas dos EUA em 2002, General Myers, "[...] não é a modernização das armas e equipamentos de combate que caracteriza a transformação; é a mudança intelectual e organizacional". Para aprofundar o assunto ver: CÔRTES, M.H.C. *A defesa nacional diante do pós-modernismo militar*. 2000 e Simpósio sobre Revolução ou Evolução de Assuntos Militares, promovido pelo Centro de Estudos Político-Estratégicos da Escola de Guerra Naval, 2002.

Uma nova concepção sobre o tema da RAM é apresentada em Blackwater: a ascenção do exército mercenário mais poderoso do mundo, de autoria de Jeremy Scahill (2008). Nesse livro, o autor mostra que a verdadeira Revolução em Assuntos Militares ocorre em função da "implementação da operação de privatização e terceirização das guerras" no período posterior ao 11 de Setembro.

[8] Fundamentadas em forças que têm por base os enormes avanços das tecnologias de informação. Para aprofundar o assunto ver: GARCIA. Francisco Proença. "A transformação dos conflitos armados e as forças da Revolução nos Assuntos Militares". Portugal. Revista Militar, 2005.

[9] Para aprofundar o assunto ver: Botelho, Tomás de Aquino Tinoco. "A guerra centrada em rede". O Anfíbio, 2004.

[10] Para aprofundar o assunto ver: HENRIQUES, José António Zeferino. "As grandes linhas geopolíticas e geoestratégicas da guerra e da paz". Grupo de Estudo e Reflexão de Estratégia, Edições Culturais da Marinha de Portugal. Lisboa. Cadernos Navais, Nº 17 – Abril/Junho, 2006.

século, com ações de proporções globais e ilimitadas, expressas sob múltiplas formas, meios e métodos de ataque, nutridos por motivações políticas, étnicas e religiosas.

Uma das consequências desses ataques foi o fato de os responsáveis legítimos pelo uso da força e pela declaração formal de guerra terem deixado de ser, a partir daquele momento, os Estados, passando a ser, também, atores não estatais. Outra consequência diz respeito à multiplicidade de armas empregadas neste novo tipo de guerra, que podem ser bombas, agentes bioquímicos, aeronaves como mísseis, vírus de computador etc.

Diante desse cenário, conclui-se que a diversidade de meios empregados por estas organizações não estatais tem ampliado o conceito de guerra, sobretudo a ambiência das atividades relacionadas com a guerra. Ou seja, as guerras deste início de século poderão ser caracterizadas pelo uso da força das armas e por outros meios que não a força das armas; os novos princípios de guerra não prescrevem mais "o emprego da força armada para compelir um inimigo à nossa vontade", e, sim, "a utilização de todos os meios, militares e não militares, letais e não letais, para compelir um inimigo aos nossos interesses". (LIANG e XIANGSUI, 1999)

As organizações transnacionais, também denominadas de "*Estado-Rede*" por Manuel Castells (1999), caracterizam-se por não possuírem território, população ou infraestrutura, mas, sim, por possuírem armas e inteligência e empregarem ações de "guerra não militar" para atacar a comunidade internacional. Nesse caso, as fronteiras nacionais, as legislações, regras de combate e os princípios éticos não têm qualquer efeito restritivo sobre suas ações; ao se deparar com esse tipo de oponente, não há como se realizar uma declaração formal de guerra, bem como também não haverá um campo de batalha definido. Contudo, sabe-se que a destruição não será, de forma alguma, inferior àquela de uma guerra tradicional. Estas características do conflito multidimensional ensejam um novo conceito de guerra, prescrevendo a prontidão de todos os meios disponíveis, a prevalência da informação e a presença do campo de batalha em todos os lugares. (LIANG e XIANGSUI, 1999)

Diante deste novo cenário, surge um novo "paradigma da guerra", pois, diante da impossibilidade de se combater de forma convencional Estados com uma capacidade militar muito superior, os atores internacionais de menor capacidade militar, no intuito de mudar esta ordem política ou de se defender das ações destes Estados, têm que, em última análise, realizar uma reavaliação de sua doutrina militar, empregando táticas, armas e métodos na forma de guerra assimétrica[11], buscando minimizar esta diferença entre as capacidades bélicas pelo emprego de meios não convencionais.

---

[11] Definido pelo Glossário das Forças Armadas do Brasil como sendo: 1. "**Conflito caracterizado pelo emprego de meios não convencionais contra o oponente** – normalmente pela parte que se encontra muito inferiorizada em meios de combate. 2. **Conflito armado que contrapõe dois poderes militares que guardam entre si marcantes diferenças de capacidades e possibilidades** – trata-se de enfrentamento entre um determinado partido e outro, com esmagadora superioridade de poder militar sobre o primeiro. Neste caso, normalmente o partido mais fraco adota majoritariamente técnicas, táticas e procedimentos típicos da guerra irregular." (o destaque é nosso). A Doutrina Básica da Marinha esclarece sobre o assunto que "a guerra assimétrica é empregada, genericamente, por aquele que se encontra muito inferiorizado em meios de combate em relação aos de seu oponente. A assimetria se refere ao desbalanceamento extremo de forças. Para o mais forte, a guerra assimétrica é traduzida como forma ilegítima de violência, especialmente quando voltada a danos civis. Para o mais fraco, é uma forma de combate".

Portanto, pode-se inferir que as guerras neste início de século apresentarão ao mundo "novas" formas de combate, empregando, para tal, todos os meios disponíveis. Verificar-se-á também que o campo de batalha se expandirá para uma dimensão que é virtualmente ilimitada[12] em função do desenvolvimento tecnológico. Como propõem os coronéis chineses Qiao Liang e Wang Xiangsui (1999), a verdadeira mudança na nova dimensão do campo de batalha decorre do que é chamado de "espaço não natural".

A partir dessa nova teoria, os conceitos de dimensão, peso, terra, mar e ar perdem seus significados até então aceitos. Dentre eles, o cyberespaço irá despertar maior atenção às guerras do futuro, onde os conflitos em redes interativas se tornarão uma realidade, bem como ocorrerão em paralelo às guerras tradicionais, havendo, portanto, uma sobreposição e interação dos campos de batalha tecnológico e convencional. Da mesma forma, acredita-se que o campo de batalha do futuro não apresentará distinção entre tecnologia militar e civil, bem como entre o combatente militar e o civil, ocorrendo, como será visto a seguir na teoria da Guerra de 4ª Geração, uma superposição entre o que se considera campo de batalha, áreas de paz ou neutras. Este novo conceito de guerra irá significar a fusão de todas as armas e a eliminação de todas as fronteiras entre as ambiências militar e não militar.

Considerando tal contexto, diversos segmentos da sociedade passaram a se dedicar ao estudo dessas novas ameaças do século XXI, inclusive da tecnologia cibernética, pela sua característica destrutiva à infraestrutura crítica de uma nação. Diversos Estados, entre eles o Brasil, têm procurado adequar os instrumentos colocados à sua disposição para o enfrentamento dessas novas ameaças, tanto no âmbito interno, por meio do preparo e adequação de suas instituições, quanto no âmbito externo, por meio da cooperação internacional.

O Brasil, por meio de suas ações da política externa, vem procurando, nestes últimos anos, projetar-se para maior presença internacional, de forma a angariar maior inserção e poder na arena das decisões mundiais. Porém, ao buscar esta posição no concerto internacional, é preciso que o Estado esteja preparado para a entrada em um mundo de competição global sujeito a qualquer tipo de retaliação, inclusive cibernética.

Nesse aspecto, mesmo havendo uma baixa probabilidade de que ocorram ataques dessa ordem em solo brasileiro, existe esta possibilidade. Dessa forma, o Estado brasileiro, de maneira alguma, pode se tornar complacente. Para tanto, deve manter a regulação dos dispositivos legais atualizada, como a Constituição Federal, a Política de Defesa Nacional, a Estratégia Militar de Defesa etc., bem como fortalecer os órgãos do Estado que participam ativamente no combate dessas possíveis ameaças. A participação em fóruns internacionais com o propósito de fomentar a cooperação internacional, por intermédio de acordos bilaterais e multilaterais em todas as áreas, inclusive do cyberespaço, é de suma importância para que se possa detectar, com antecedência, qualquer tipo de ameaça. Nesse contexto, o sucesso nesse tipo de confronto dependerá exclusivamente da eficácia das ações desenvolvidas pelo Estado para que possa adaptar-se ao atual contexto tecnológico.

No campo militar, Vidigal (2004) nos ensina que, apesar do papel tradicional das Forças Armadas ter sido sempre o de enfrentar Forças regulares inimigas, "[...] o contexto atual indica a necessidade de

[12] Exemplo disso são os satélites, submarinos com mísseis balísticos, a guerra eletrônica e a guerra psicológica. (LIANG e XIANGSUI).

ampliação do emprego das Forças Armadas do país em inúmeras situações antes não previstas". Ou seja, as Forças Armadas devem possuir a capacidade de combater, efetivamente, as novas ameaças deste século, sejam elas no plano convencional ou no espaço virtual. Isso implica uma mudança de mentalidade e a quebra de paradigmas, bem como o contínuo estudo prospectivo de cenarização, visando proporcionar o preparo e o dimensionamento adequados das forças[13].

Uma das máximas militares é a de que se deve sempre, em tempo de paz, preparar-se para a guerra, buscando-se, sempre que possível, prever "como será a próxima guerra". E isso está se tornando cada vez mais difícil, em função dos motivos expostos até agora. Para melhor compreensão deste fenômeno da guerra, um grupo de autores, entre eles William Lind (2007), apresentou alguns conceitos sobre as formas e técnicas de como as guerras modernas se desenvolveram ao longo da história, sob a denominação de Quatro Gerações de Guerras ou Guerra de Quarta Geração (G4G).

Porém, naquele momento, esses conceitos não atraíram muito a atenção dos pensadores militares. Somente após os atentados de 11 de setembro, alguns dos idealizadores dessas teorias defenderam que os ataques da Al Qaeda concretizavam suas previsões, principalmente após a afirmação de um dos principais estrategistas deste grupo terrorista estar empregando os conceitos da G4G contra os EUA. Comprovou-se, de fato, que um *website* da Al Qaeda foi um dos únicos locais no qual a G4G foi cuidadosamente discutida. (HAMMES, 2007).

Neste momento, valemo-nos das palavras de Epitácio Pessoa: "Até que o perigo da guerra deixe de ameaçar o mundo, será criminoso, perante a nação, o governo que não se preparar e se acautelar para enfrentá-la". (Em 7 de abril de 1920)

BREVE HISTÓRICO SOBRE AS GERAÇÕES DE GUERRA

Quem quer que seja o primeiro a reconhecer, entender e implementar uma mudança de gerações, pode obter uma vantagem decisiva. Ao contrário, uma nação que seja lenta ao adaptar-se a uma mudança de geração estará sujeita a uma derrota catastrófica.

William S. Lind

A doutrina atual apresenta o desenvolvimento militar moderno em três gerações distintas de guerras, sendo a Quarta Geração apenas objeto de estudo e reflexão pelos estudiosos do tema, não sendo completamente aceita pela comunidade militar.

A Guerra de 1ª Geração (G1G) caracterizou-se pela rigidez das táticas e por formações lineares, em terra ou no mar, na era do mosquete de carregar pela boca e de cano não raiado. Estendeu-se no período da se-

Fig.2: Alusão às Guerras Napoleônicas na Guerra de 1ª Geração
Fonte: www. shuzak.com/

[13] Como nos alerta Liddell Hart na dificuldade de quebra de paradigmas e mudança de mentalidade: "Mais difícil do que colocar uma ideia nova na cabeça dos militares é dela [da cabeça] retirar os conceitos antigos".

Fig.3: Blitzkrieg alemã durante a Segunda Guerra Mundial.
Fontes: www.achtungpanzer.com, www.2worldwar2.com e www.talkingproud.us e www.bbchs.k12.il.us/

gunda metade do século XVII até o início do século XIX, tendo seu clímax nas campanhas napoleônicas.

A Guerra de 2ª Geração (G2G) caracterizou-se pelo emprego do poder de fogo dos novos armamentos produzidos nas indústrias no pós-Revolução Industrial. As táticas eram traçadas baseadas no fogo e movimento, porém permanecendo, ainda, essencialmente lineares. O poder de fogo em massa substituiu a quantidade de soldados no campo de batalha. A evolução da G2G culminou com a Primeira Guerra Mundial. Durante esse conflito, foram empregados os instrumentos que permitiram o desenvolvimento da Guerra de 3ª Geração (G3G), como o carro de combate, o submarino e a aviação.

A Guerra de 3ª Geração (G3G) caracterizou-se pela mudança das táticas militares, baseadas em manobras ao invés do atrito, surgindo os primeiros conceitos da Guerra de Manobra[14]. As táticas da G3G foram as primeiras verdadeiramente não lineares, buscando-se a aproximação indireta, conforme descrita pelo estrategista Liddell Hart, ao invés de procurar o contato direto para sua destruição. Portanto, a Guerra de Manobra, ao contrário da Guerra de Atrito, visa incapacitar sistematicamente o seu sistema de combate, por meio da obtenção de uma posição vantajosa, em vez de ir ao encontro direto. Alguns componentes do sistema de combate do inimigo podem permanecer intactos, porém não funcionarão como parte do todo; com isso, o sistema de combate não possuirá coesão.

A adição de elementos de nova tecnologia, como os carros de combate, permitiu uma grande mudança do nível operacional na Segunda Guerra Mundial, como verificado na Blitzkrieg[15], na qual ocorre a mudança das bases da arte operacional de lugar para tempo. Esta mudança foi indiscutivelmente sedimentada após o trabalho do coronel aviador norte-americano John Boyd sobre a teoria do ciclo OODA (Observação-Orientação-Decisão-Ação) dos pilotos americanos na Guerra da Coreia[16].

---

[14] "[...] uma filosofia de combate que preconiza a destruição da coesão do inimigo por meio de uma série de rápidas, violentas e inesperadas ações, as quais criam uma turbulenta e rápida degradação da situação, a qual o inimigo não pode suportar ou administrar." (EGN, FI-504)

[15] Ataque-relâmpago realizado pelas forças alemãs durante a Segunda Guerra Mundial.

[16] O Coronel John Boyd desenvolveu uma das bases teóricas da Guerra de Manobra, durante o desempenho dos pilotos norte-americanos na Guerra da Coreia, sobre o combate em inferioridade numérica. Ele observou que, durante os conflitos, os adversários passam por repetidos ciclos, compostos das fases da OBSERVAÇÃO-ORIENTAÇÃO-DECISÃO-AÇÃO (O-O-D-A) e que o partido potencialmente vitorioso seria aquele que possui o ciclo sensivelmente mais rápido que o de seu adversário, pois faria com que o inimigo não conseguisse reagir ante as ações tomadas pelo adversário, quebrando sua coesão e capacidade de lutar como força organizada.

A GUERRA ASSIMÉTRICA E A GUERRA DE 4ª GERAÇÃO

"Se o inimigo tiver sua vontade de lutar afetada, então sua capacidade militar, sem importar quão poderosa seja, passa a ser irrelevante."

Mao Tsé Tung

De forma geral, as doutrinas militares atuais preveem quatro tipos diferentes de guerra: a guerra convencional, a guerra de destruição em massa, a guerra irregular e a guerra assimétrica.

Como a guerra nuclear – vista como uma guerra de destruição em massa – tornou-se cada vez mais improvável após a Segunda Guerra Mundial, os conflitos armados evoluíram para uma forma irregular, substituindo a forma convencional de combate. Porém, os atentados de 11 de setembro sugeriram a evolução para um novo tipo de guerra, em face das características apresentadas pelo terrorismo contemporâneo, substituindo os conceitos aceitos da Guerra Irregular e recebendo, a partir de então, a denominação de Guerra Assimétrica[17].

Este novo tipo de guerra foi reconhecidamente aceito por alguns estudiosos americanos e europeus, que apresentaram a Guerra Assimétrica com a denominação de Guerra de Quarta Geração (G4G), e pelos coronéis chineses Liang e Xiangsui, apresentando-a como Guerra Além dos Limites ou Guerra Irrestrita. Nesse novo tipo de guerra, como propõem os coronéis chineses, os meios empregados na condução da guerra transcendem as atividades militares, sendo possível empregar todos os meios disponíveis, incluindo meios militares e civis, letais ou não, usando qualquer método para compelir o inimigo a fazer a sua vontade.

Diante disso, os teóricos chineses afirmam que a Guerra Assimétrica pode se manifestar das seguintes formas: guerra psicológica; guerra econômica; guerra com armamento usual; guerra radiológica, nuclear ou radioativa; guerra biológica, bacteriológica ou virótica; guerra cibernética, eletrônica ou informática; e guerra química. Dessas formas, a preponderante é a guerra psicológica, tendo em vista que, neste tipo de conflito, o que se busca é atingir o moral do adversário. Diante disso, pode-se afirmar que todos os outros tipos de guerra são decorrentes de suas ações e, mais do que isso, todos os outros tipos de guerra serão subordinados à guerra psicológica.

Como apresentado na introdução deste texto, o termo G4G vem sendo usado para designar o conflito multidimensional, empregando todas as redes disponíveis – políticas, econômicas, sociais e militares – para atacar diretamente as mentes dos oponentes responsáveis pelas tomadas de decisões. Pode-se afirmar, ainda, que a G4G foi influenciada pelas evoluções das gerações de guerras do passado e estão pautadas em algumas ideias centrais, a saber:

A primeira ideia central está na dimensão do campo de batalha. Na G4G, este campo de batalha inclui toda a sociedade inimiga. A segunda ideia central é uma decrescente dependência na logística centralizada. A terceira ideia central é maior ênfase na guerra de manobra, em que o efetivo da tropa e o poder de fogo não serão mais fatores de vantagem esmagadora. A quarta ideia cen-

[17] Uma dúvida frequente versa sobre as diferenças entre Guerra Assimétrica e Guerra Irregular. Segundo Teixeira (2006), quando um tipo de guerra ocorre no interior de um Estado, geralmente suas ações estão relacionadas às questões de libertação nacional, de insurgência, intolerância racial ou de revolução. Nesse caso, empregam-se métodos específicos de combate e, por se apresentarem sob uma forma típica de manifestação, recebem a denominação, na literatura militar, de Guerra Irregular ou de Resistência ou, ainda, Guerra de Guerrilhas.

tral está pautada na destruição da capacidade de coesão do inimigo internamente, em vez de destruí-lo fisicamente. Os alvos incluem o apoio da população à guerra, assim como a oposição à cultura inimiga por meio de operações psicológicas, em que a correta identificação do centro de gravidade[18] do inimigo passa a ser o objetivo principal, pois é a fonte de todo o poder físico e mental, ou seja, o que sustenta sua força e resistência. (LIND, 2007) Conclui-se, portanto, que a G4G apresenta-se como uma guerra não linear, em um campo de batalha não definido, não havendo distinção clara entre guerra e paz, tampouco entre civis e militares.

A doutrina militar dos EUA aponta para quatro formas prováveis de guerra no futuro: Guerra Cibernética, Guerra de Precisão, Operações Combinadas e as *Military Operations Other Than War* – MOOTW[19], que abrange uma série de operações em que os militares são empregados, porém não necessariamente como os protagonistas da operação. Porém, segundo Liang e Xiangsui, a guerra cibernética será a forma básica de guerra futura.

A G4G apresenta-se como uma guerra não linear, em um campo de batalha não definido, não havendo distinção clara entre guerra e paz, tampouco entre civis e militares

GUERRA DE INFORMAÇÃO

"A obtenção de cem vitórias em cem batalhas não é o expoente da excelência. Subjugar o exército inimigo sem combater constitui o verdadeiro expoente da excelência"

Sun Tzu

Ao analisar a evolução da sociedade e da guerra, Alvin e Heidi Toffler (1995) apresentaram a teoria da evolução da civilização e das guerras em ondas de inovação. A primeira onda de evolução ocorreu com a Revolução Agrária, quando houve a mecanização da cultura. Os produtos eram advindos da produção agrícola e se constituíram na causa das guerras travadas naquele período. A segunda onda adveio da industrialização, abrangendo as duas Revoluções Industriais, proporcionando mudanças na forma de condução das guerras, em função do aparecimento das máquinas e das armas de destruição em massa, atingindo seu ápice durante a Segunda Guerra Mundial. Após este conflito, o mundo passa a vivenciar o grande impulso tecnológico decorrente dos avanços na área da Tecnologia da Informação (TI). Nesse contexto, a humanidade vivencia a terceira onda, também denominada como Era da Informação, na qual o valor econômico passa a ser criado a partir do conhecimento, assumindo posição central na criação de riqueza dos Estados. Dessa forma, o conflito na Era da Informação visará degradar o recurso da produção da riqueza do oponente – o conhecimento.

[18] Definido por Clausewitz como: "[..] o centro de todo o poder e movimento, do qual tudo depende. É o ponto sobre o qual todas nossas energias devem ser direcionadas". (EGN,FI-504)

[19] Na qual traduziremos como Operações de Não Guerra. Para aprofundar o assunto ver: "Military Operations Other Than War", J-7 Operations Plans and Interoperability Directorate, Joint Doctrine, Joint Force Employment. USA.

Surgem, nesse momento, os primeiros conceitos modernos da Guerra da Informação (*Information Warfare*).

A Guerra da Informação pode ser entendida, no nível estratégico, como o uso da informação para atingir os objetivos nacionais. Como nos ensina o professor George Stein (1995), a informação, tal como a diplomacia, a competição econômica ou o emprego da força militar, é um aspecto-chave do Poder Nacional.

Diante disso, entende-se que a Guerra de Informação Estratégica (GIE) pode ser interpretada como um conflito de nível social ou de nação contra nação, conduzido, em parte, por meio do cyberespaço, visando atingir, como principal alvo, a mente das pessoas responsáveis pelas decisões, por meio de ataques à Infraestrutura Global de Informações de um Estado, caracterizado pelo conjunto de sistemas de comunicações, redes de computadores e serviços informatizados.

No nível operacional, a Guerra de Informação se apoiará na conquista dos objetivos estratégicos, influenciando a habilidade do adversário em tomar decisões de uma maneira tempestiva e eficaz. Ou seja, é a degradação do ciclo OODA do adversário.

Para tanto, a Guerra da Informação pode materializar-se por meio de: combate aos sistemas de comando e controle, segurança operacional, guerra cibernética, guerra eletrônica, pirataria eletrônica (*hacking*), bloqueio de informação, guerra baseada na informação e a guerra psicológica. (NUNES, 1999)

A doutrina brasileira prevê quatro níveis na condução dos conflitos, a saber: político, estratégico, operacional e tático. Porém a teoria da guerra além dos limites aponta para uma supracombinação desses níveis nas guerras do futuro. Ou seja, a combinação homem-máquina poderá realizar ações que afetem desde o nível tático até o nível

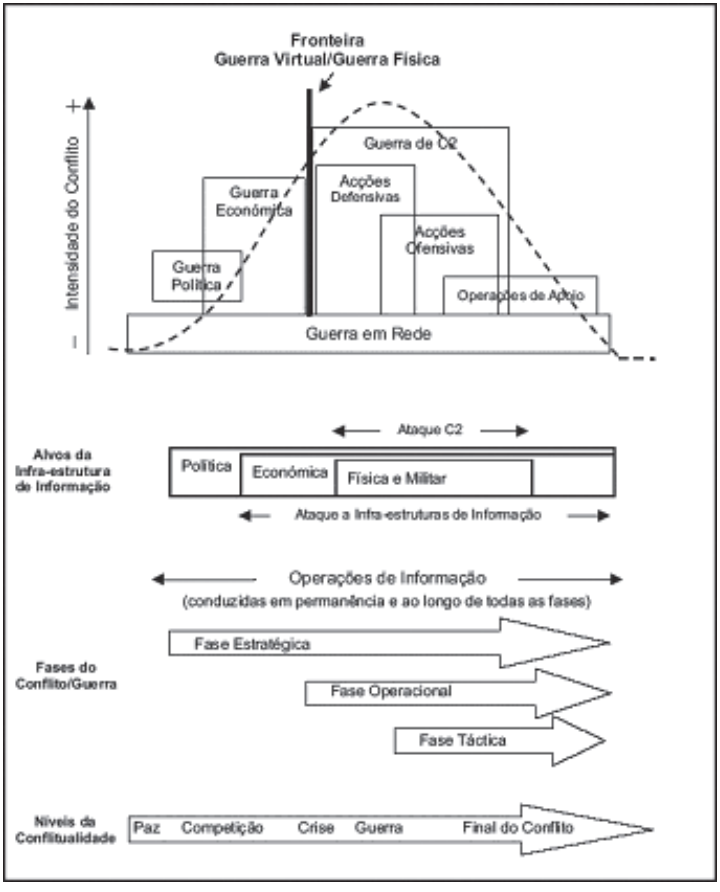

Fig. 4: Relação da Guerra da Informação com os níveis de condução das guerras
Fonte: Caldarella (1995); Waltz (1998) *apud* NUNES (2006)

político. Um exemplo disso são os ataques realizados pela *Al Qaeda* na última década, que, geralmente por meio de métodos táticos em suas ações, refletem no nível estratégico dos Estados atingidos. Para os autores chineses, na guerra militar e não militar não existem ambiên-cias que não possam ser ultrapassadas, não existem meios que não possam ser usados, como também não existem campos de ação e métodos que não possam ser combinados. Outro exemplo refere-se ao emprego de *hackers*, pois suas ações poderão permear e causar danos em todos os níveis, do político ao tático. A representação gráfica abaixo sintetiza a relação das Operações da Guerra da Informação entre os diversos níveis na condução dos conflitos.

Dessa forma, conforme nos ensina Nunes (2006), a Guerra da Informação é conduzida em todos os níveis desde o período de paz. Durante a escalada da crise entre dois atores internacionais, são desenvolvidas ações de informações, essencialmente na sua Infraestrutura de Informação Nacional e de Defesa, sendo de caráter político-econômico. Com o início do conflito, os ataques da Guerra de Informação passam a ser direcionados para a Infraestrutura de Informação de Defesa do adversário, privilegiando os ataques na sua estrutura de Comando e Controle. Ao término do conflito, estas ações irão apoiar-se na consolidação dos objetivos iniciais, atuando no nível da Infraestrutura Global de Informação do Estado.

No campo militar, as Forças Armadas encontram-se cada vez mais dependentes da velocidade e da funcionalidade oferecidas pelas redes de computadores em todas as áreas, desde os sistemas de comunicações aos sistemas de armas, visando garantir a sua operacionalidade no campo de batalha.

Atualmente, estima-se que mais de 90% das comunicações militares utilizam ligações de dados comerciais (NUNES, 2006). Portanto, quanto mais dependente o adversário for dos sistemas de informação para a tomada de decisão, mais vulnerável estará aos ataques da Guerra da Informação.

Como exemplo desta dependência tecnológica cita-se a complexidade de interconexões que envolvia o sistema de mísseis Patriot, empregado pelos norte-americanos na 2ª Guerra do Golfo para interceptar os mísseis Scud iraquianos. O conjunto de sistemas envolvia satélites do tipo DSP[20] para identificação do alvo. Ao detectar um míssel Scud, o satélite enviava um sinal de alarme para uma estação receptora localizada na Austrália; esta estação retransmitia o sinal para um Posto de Comando (PC) localizado nos EUA e, a partir deste, o sinal era enviado para o comando das forças norte-americanas em Ryadh. Somente após esse "longo" trâmite de mensagens o comando de disparo era encaminhado para as bateri-

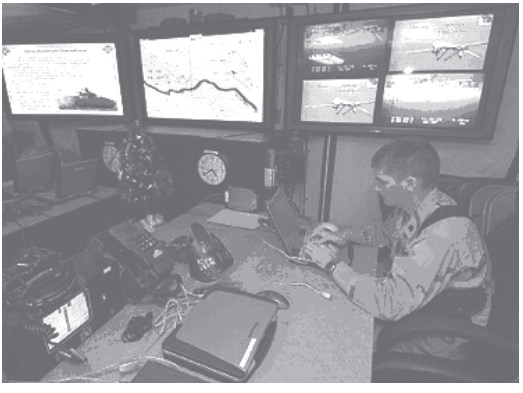

Fig. 5: Guerra da Informação
Fonte: www.nzz.ch

[20] Os Satélites DSP (Defense Support Program) foram desenvolvidos na década de 1970. Sua configuração original previa o seu posicionamento em órbitas geoestacionárias, sendo dotados de sensores para prover alarme contra mísseis além do horizonte. (LIANG e XIANGSUI, 1999)

as de mísseis Patriot. O tempo total entre a detecção e o comando de disparo era de apenas 90 segundos, porém passíveis de serem interferidos por ações da Guerra de Informações, particularmente da vertente da guerra cibernética, ao longo desse processo. Não foi por acaso que o primeiro objetivo norte-americano a ser atacado na Guerra do Golfo foi o sistema de comunicações iraquiano, com o intuito de causar uma paralisia estratégica no seu ciclo OODA, perdendo, desta forma, sua operacionalidade no campo de batalha.

GUERRA CIBERNÉTICA

"Trazer a guerra cibernética para os sistemas militares é tão importante quanto os poderes naval, terrestre e aéreo."
Jornal do Exército Popular da China, em 1999

A Guerra Cibernética pode ser definida como um subconjunto da guerra da informação e se caracteriza pelo uso dos meios computacionais para ações ofensivas por meio de penetração nas redes de computadores de alvos estratégicos, a fim de infligir no inimigo o enfraquecimento das suas defesas convencionais, destruir sua coesão e diminuir sua capacidade de controle, comunicações e reação ou, ainda, de condutas defensivas por meio de ações próativas e reativas, visando coibir a atividade do atacante na infraestrutura de redes. (BEZERRA et al., 2004)

Como apresentado anteriormente, o funcionamento dos principais sistemas de informação das sociedades modernas está interligado por redes de computadores, formando a Infraestrutura Global de Informações de um Estado. Dessa forma, em um cenário de hostilidades e/ou beligerância entre dois atores internacionais, a exploração das redes de computadores por meio de ataques cibernéticos tem por objetivo impedir que este adversário empregue eficazmente o seu potencial de comando e controle, bem como buscar atingir os setores críticos da sua infraestrutura nacional, causando em sua população e em seus líderes o sentimento de insegurança e derrota diante de um inimigo invisível e desconhecido. Ou seja, o resultado alcançado por ataques cibernéticos pode proporcionar que uma nação inteira seja conduzida à capitulação, sem que, no entanto, haja qualquer manobra política ou militar para tal. (BEZERRA et al., 2004; DUTRA, 2007)

Diante disso, pode-se inferir que os alvos compensadores para uma guerra cibernética são as redes de computadores e sistemas que gerenciam e controlam os seguintes serviços críticos de um Estado:

a. redes de telecomunicações;
b. energia elétrica;
c. saúde pública, emergência e água potável;
d. sistema financeiro; e
e. redes de comando e controle do governo.

Segundo Bezerra *et al*. (2004), um ataque bem-sucedido nas redes dos sistemas de telecomunicações permitirá uma descontinuidade das informações em todos os níveis do governo e da sociedade civil, gerando insegurança, pânico e incerteza com relação à real situação do conflito. No que concerne aos sistemas de energia elétrica, saúde pública, emergência e água potável, estes sistemas são considerados essenciais para a população de modo geral. Em relação ao sistema financeiro, visa causar uma quebra na estrutura econômica do país, levando ao caos financeiro nacional, podendo, inclusive, ter reflexos na solidez desse país na economia internacional. Um ataque cibernético sobre as redes de Comando e Controle do Governo terá como objetivo atingir o seu

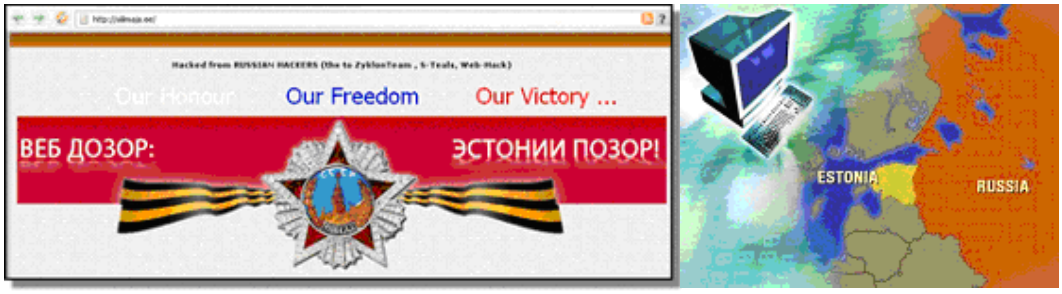

Fig. 6: Site da Estônia após ataques cibernéticos – Fontes: www.viruslist.com e www.abcnews.com

ciclo OODA, reduzindo a capacidade de recuperação e respostas a esses ataques.

Existem diversos casos de ataques cibernéticos no cenário internacional, sendo dos mais recentes os ataques realizados à Estônia em 2007, com repercussão internacional em função do alto impacto que estes ataques tiveram naquele país, demonstrando a enorme fragilidade de um Estado diante de ataques nesta nova dimensão da guerra.

Em 17 de maio de 2007, a Estônia anunciou que havia recebido um ataque cibernético sem precedentes na história. Um país com aproximadamente 1,4 milhão de habitantes e com mais de 1 milhão de computadores orgulhava-se da eficiência dos serviços *on-line* prestados pelo Estado, não havendo, portanto, a tradicional burocracia dos papéis, e por terem realizado as primeiras eleições nacionais pela internet. No entanto, o país sofreu, durante um período de três semanas, três ondas sucessivas de ataques cibernéticos, interrompendo os serviços de internet e praticamente imobilizando o governo. Os ataques cibernéticos atingiram *sites* governamentais, partidos políticos, companhias, bancos e empresas de comunicações. Inicialmente, as investigações levaram o governo da Estônia a indicar a Rússia como autora do ataque. O motivo seria uma represália do governo russo à remoção de uma estátua na capital do país em homenagem aos soldados soviéticos mortos na Segunda Guerra Mundial. A característica dos ataques foi do tipo DDoS[21] (ataque de negação de serviço), com origem em *botnets*[22], no qual os *sites* recebem uma quantidade muito grande de acessos ao mesmo tempo, impossibilitando seu funcionamento. Os ataques só foram mitigados em função da estreita colaboração entre as equipes de resposta a incidentes de segurança informática, denominadas de CSIRT (*Computer Security Incident Response Team*), demonstrando a incapacidade dos Estados em evitar ou controlar ataques

[21] "Distributed Denial of Service – Técnica de sabotagem baseada em um esquema de esgotamento dos recursos disponíveis num determinado serviço internet e que resulta na sua paralisação. Este esgotamento é conseguido por um número simultâneo de 'pedidos' muito superior ao dimensionamento previsto do sistema. Esses 'pedidos', indistinguíveis do verdadeiro tráfego, são normalmente realizados de forma automática a partir de uma botnet." (SANTOS, 2007)

[22] "Conjunto de computadores, por vezes da ordem das centenas de milhar, previamente infectados por um worm ou vírus, geograficamente dispersos e sob controle de um agente criminoso. Normalmente usadas para envio massivo de correio eletrônico não solicitado (Spam) ou roubo de identidade, estas 'redes' começam a ser utilizadas em ataques mais sofisticados, como o DDoS. O verdadeiro dono do computador infectado não conhece a atividade criminosa feita a partir da sua residência ou local de trabalho." (SANTOS, 2007)

Fig. 7: Alusão aos guerreiros cibernéticos chineses e à nova dimensão de combate
Fontes: www.therawfeed.com e www.foxnews.com

desta magnitude. Esses acontecimentos na Estônia fizeram a Organização do Tratado do Atlântico Norte (Otan) refletir a respeito de considerar, a partir daquele momento, ataques virtuais como ações militares, em função da dimensão dos danos causados. (CARDOSO, 2007; SANTOS, 2007)

Portanto, torna-se evidente que a evolução da Guerra Cibernética dentro do contexto da Guerra de Informação impõe uma nova realidade, apontando para um novo Paradigma da Guerra. Como sugere Cardoso (2007), as guerras modernas já não obedecem à concepção clausewitziana da matriz trinitária ou trindade paradoxal (Estado, Forças Armadas, população), típica do anterior sistema internacional, em função das incertezas e assimetrias permanentes.

Dessa forma, verifica-se que EUA, China, Rússia e Taiwan são os Estados que estão mais avançados no que tange às capacidades, estratégias e doutrinas destinadas a preparar as forças militares e não militares para o envolvimento em guerras cibernéticas, criando unidades especialmente dedicadas ao tema, indicando o espaço cibernético como um novo teatro de operações. Atualmente, considera-se a tecnologia empregada na condução da guerra cibernética tão secreta quanto foi o desenvolvimento da bomba nuclear durante a Segunda Guerra Mundial, em função do impacto de suas ações.

Como propõe Nunes (2006), o emprego de Operações de Informação, como a Guerra Cibernética, poderá ser muito mais fácil, mais eficiente e, provavelmente, será politicamente aceitável, em especial aos olhos da comunidade internacional, se comparável ao emprego e às consequências das operações militares convencionais.

Além disso, analisando-se os custos operacionais para implementar uma Guerra Cibernética, verificar-se-á que estes são praticamente insignificantes quando comparados aos custos que envolvem operações militares tradicionais. (DUTRA, 2007)

Diante desse contexto, acredita-se que o tema merece atenção especial pelo Estado brasileiro, como já vem ocorrendo desde 2000 com a criação do Comitê Gestor da Segurança da Informação (CGSI), o qual tem assessorado a Secretaria-Executiva de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação, o que, possivelmente, trará, a médio prazo, grandes implicações tanto para a Política de Defesa Nacional quanto para a Estratégia Militar de Defesa.

Fig. 8: Alusão a civis e militares atuando na Guerra de Informação – Fonte: www.sandia.gov e www.government.zdnet.com

CONSIDERAÇÕES FINAIS

No passado, um comandante podia ter certeza de que a próxima guerra iria reunir as características das guerras do passado e do presente. Com isso, era possível analisar táticas apropriadas ao passado e adaptá-las ao presente. O comandante de hoje não conta mais com essa possibilidade. Ele sabe apenas que aquele que não se adaptar corretamente às experiências da última guerra certamente perderá a próxima.

General alemão
Franz Uhle-Wettler

Torna-se imperioso para o Brasil aprofundar as pesquisas nesta nova dimensão da guerra, visando proporcionar o estabelecimento de uma política de segurança da informação para o País

Apesar das incertezas do futuro, a guerra continuará a existir pela busca de poder, podendo-se inferir, com certa precisão, que os princípios da Guerra de 4ª Geração apresentados tornar-se-ão regra nos conflitos deste início de século. O mundo presenciará guerras entre atores não estatais e os Estados, guerras assimétricas, sem regras, sem princípios, sem frente ou retaguarda. Em contrapartida, essas guerras da Era da Informação serão marcadas pelo emprego de um novo tipo de Força Armada, dotada de alta tecnologia e com utilização do cyberespaço. Dessa forma, a guerra cibernética passa a ser considerada como uma variante da guerra assimétrica, objetivando a paralisia estratégica do oponente. (CARDOSO, 2007; GARCIA, 2005)

Com base nos cenários prospectivos da (in)segurança internacional, acredita-se que haja uma grande probabilidade de os conflitos acontecerem também fora da ambiência militar, elevando, dessa forma, o contexto da Guerra de Informação para um Paradigma da Guerra, eliminando por completo a distinção entre os sistemas militares e civis (NUNES, 1999; 2006).

Diante desta situação, torna-se imperioso para o Brasil aprofundar as pesquisas nesta nova dimensão da guerra, visando proporci-

onar o estabelecimento de uma política de segurança da informação para o País.

Segundo Dutra (2007), a criação de centros de pesquisa e estudo da segurança das informações é o primeiro passo na criação de metodologias e disseminação da cultura de segurança computacional. Além disso, considera-se primordial o estabelecimento de parcerias público-privada e civil-militar no intuito de formar grupos de análise de risco, gerência de crises, de forma a identificar as ameaças ao sistema, as suas vulnerabilidades e as contramedidas a serem adotadas, bem como coletar todos os indícios e provas, colaborando, assim, com uma eventual investigação. O autor cita o exemplo do modelo americano de pesquisa – os *think tanks*[23] – criado pelo US National Defense Research Committee, o qual está baseado na sinergia de esforços entre os diversos setores do Estado na busca de soluções para as diversas ameaças que enfrenta o Estado.

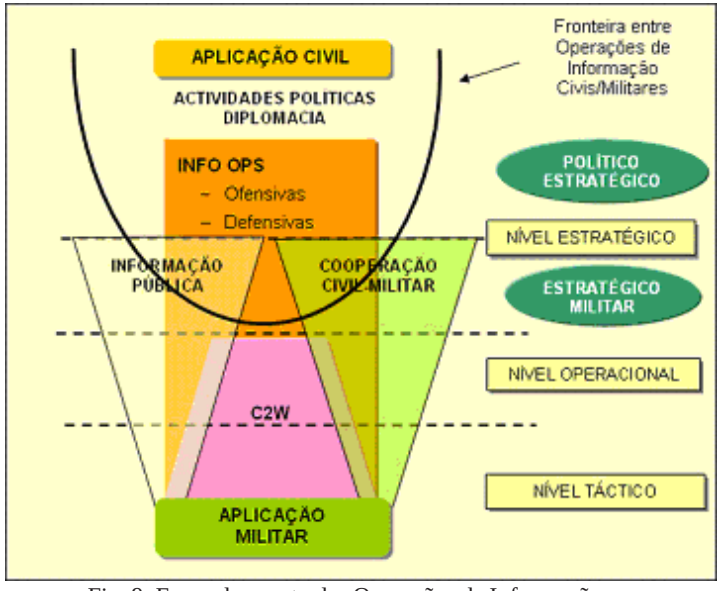

Fig. 9: Enquadramento das Operações de Informação na Doutrina Otan (AJP-01).
Fonte: NUNES (2006)

Desde a década de 1990, os EUA adotaram medidas mais incisivas para garantir a segurança da informação no ambiente cibernético. Cita-se, como exemplo, a Diretiva Presidencial (PDD-63) de 1999, determinando realizar todas as medidas necessárias para eliminar as vulnerabilida-des a ataques cibernéticos nas infraestru-turas críticas. Em 2000, criaram o Cyber National Informaton Center, reunindo o Governo e o setor privado na defesa de sistemas de computadores. Após os ataques de 11 de setembro de 2001, foi criado o National Infrastructure Protection Center (NIPC). No mesmo ano, a Postgraduate School (US Navy) criou dez cursos específicos de segurança cibernética. Já em 2003, os EUA publicaram a National Strategy to Secure the Cyberspace – a estratégia de segurança nacional do cyberespaço –, estabelecendo como prioridade nº 1 o estabelecimento do National Cyberspace Security System, que tem como missão precípua recuperar uma rede atacada, detectar, analisar e responder a um ataque cibernético. (SILVA e TARANTI, 2003)

[23] "Os *think tanks* são centros de pesquisa e de formação de pesquisadores, em que 'especialistas das ciências sociais, economistas, matemáticos, engenheiros e físicos são chamados a compartilhar seus conhecimentos', fazendo surgir uma nova função, a do 'militar intelectual', diz Mattelart, que serve de conselheiro aos órgãos de defesa e circula com intimidade pelos corredores do Pentágono e do Departamento de Estado." (DUTRA, 2007)

Segundo Nunes (2006), a Otan, ao longo da última década, tem aprimorado o desenvolvimento de políticas, doutrinas e procedimentos destinados a integrar as capacidades civis e militares no ambiente da informação, integrando no seu planejamento de defesa as Operações de Informação como prioridade, inclusive sendo capaz de ser o esforço principal na condução das operações militares. Para tanto, a Otan divide as Operações de Informação como sendo de caráter ofensivo[24] e defensivo[25], devendo estas ser coordenadas no mais alto nível da operação, para que a sua condução reflita a orientação político-estratégica do Estado.

Verifica-se, portanto, que as Operações de Informação na Otan também estão presentes em todo espectro do conflito (paz, crise e guerra) e nos diversos níveis de condução das operações (político, estratégico, operacional e tático). (NUNES, 2006)

Por fim, considera-se fundamental que o Brasil continue desenvolvendo suas capacidades defensivas a ataques cibernéticos, por meio de identificação de suas vulnerabilidades críticas, em todos os níveis. Para tanto, o emprego de medidas ativas de defesa, como o uso de senhas, *firewalls*, sistemas de autenticação, uso de *software* de monitoramento etc., torna-se imprescindível. Além disso, o incentivo à formação acadêmica, o desenvolvimento de *softwares* nacionais de criptografia e a redução da dependência de tecnologia externa devem ser prioridade do governo em função do caráter transnacional dos ataques cibernéticos. Sugere-se, ainda, a criação de grupos do tipo do CSIRT com cooperação internacional, visando às coordenações e ações necessárias na resposta a um ataque cibernético. (SILVA e TARANTI, 2003; SANTOS, 2007)

No entanto, a condução de ações de guerra de informação defensivas não nega a possibilidade do desenvolvimento de processos de ações ofensivas, visando à defesa dos interesses nacionais. Entre essas medidas, destacam-se: programas de quebra de senha, programas de observação, obtenção de informação, identificação do alvo; programas de ataque; programas de marcação de alvos; programas de comportamento virulento, cavalos de troia; programas de sobrecarga do sistema; manipulação direta de dados; e, por fim, bombas lógicas. (DUTRA, 2007)

🗁 CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<GUERRAS> Guerra futura; Guerra de manobra; Informação na guerra; Política internacional; Guerra assimétrica; Guerra cibernética;

[24] As Operações de Informação Ofensivas procuram "influenciar a informação e os sistemas de informação disponíveis de um potencial adversário, durante uma situação de paz, crise ou conflito, na consecução de determinados objetivos, ou em resposta a uma ameaça específica". (NUNES, 2006)

[25] As Operações de Informação Defensivas procuram "assegurar o acesso permanente e a utilização efetiva da informação e dos sistemas de informação durante uma situação de paz, crise ou conflito e proteger a informação crítica da Aliança, de forma a atingir determinados objetivos". (NUNES, 2006)

BIBLIOGRAFIA

BEZERRA, E. K.; NAKAMURA, E.T.; LIMA, M.B.; RIBEIRO, S.L. O espaço cibernético e seu emprego como agente de instabilidade de uma nação: uma visão sobre a guerra cibernética. Texto apresentado na I Conferência Internacional de Perícias em Crimes Cibernéticos. 2004. Disponível em: http://portal.ibta.com.br/cursos/ibtanews/ibtanews_2/artigo.htm. Acesso em: 05/set/2008.

BOTELHO, Tomás de Aquino Tinoco. "A guerra centrada em rede". *O Anfíbio*. Revista do Corpo de Fuzileiros Navais, nº 23, Edição 2004.

CARDOSO, Luís Sousa. "Os ciberataques e a soberania nacional". *Revista Planeamento Civil de Emergência*. Portugal. Nº 19, 2007. Disponível em: http://www.cnpce.gov.pt/?p=160. Acesso em: 13/set/2008.

CASTELLS, Manuel. A sociedade em rede. São Paulo. Ed: Paz e Terra, 1999.

CASTRO. Luiz Fernando Damaceno Moura e. "Estônia sofre ataque virtual". Resenha. PUC MINAS. *Conjuntura internacional*. 02 de julho de 2007.

CHOMSKY, Noam. *O império americano: Hegemonia e Sobrevivência*. Rio de Janeiro. Ed. Elsevier, 2004.

CORTÊZ, Marcos Henrique Camillo. "A defesa nacional diante do pós-modernismo militar". Trabalho apresentado no I Seminário sobre Defesa Nacional. Centro de Estudos Estratégicos da Escola Superior de Guerra. Rio de Janeiro, 20 nov, 2001.

CRUZ, Eduardo Lucas de Vasconcelos. "Tecnologia militar e indústria bélica no Brasil". *Security and Defense Studies Review*, Vol.6 nº 3, 2006. Disponível em: www.ndu.edu . Acesso em: 29 de setembro de 2008.

DUTRA, André Melo Carvalhais. "Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto". Instituto Tecnológico da Aeronáutica. (S/D) Disponível em: www.sige.ita.br/IX_SIGE/Artigos/GE_39.pdf . Acesso em: 29/set/2008.

GARCIA. Francisco Proença. "A Transformação dos conflitos armados e as forças da Revolução nos Assuntos Militares". Portugal. *Revista Militar*, 2005. Disponível em: http://revistamilitar.pt/modules/articles/print.php?id=25. Acesso em: 26/09/2008.

HAMMES, Thomas X. "A guerra da quarta geração evolui, a quinta emerge". *Revista Militar Review*. Set-Out, 2007.

HENRIQUES, José António Zeferino. "As Grandes Linhas Geopolíticas e Geoestratégicas da Guerra e da Paz". Grupo de Estudo e Reflexão de Estratégia, Edições Culturais da Marinha de Portugal. Lisboa. *Cadernos Navais*, Nº 17 – Abril - Junho, 2006. Disponível em: http://www.marinha.pt/NR/rdonlyres/38E34C39-2810-405A-9757-D6F68DDDC394/3758/n171.pdf. Acesso em: 19/09/2008.

HOBSBAWM. "Globalização, Democracia e Terrorismo". São Paulo. Ed. Schwarcz, 2007.

LIANG, Qiao; XIANGSUI, Wang. *A Guerra Além dos Limites: Conjecturas sobre a Guerra e a Tática na Era da Globalização*. Beijing: PLA Literature and Arts Publishing house, 1999.

LIND, William S. "Compreendendo a Guerra de Quarta Geração". *Revista Militar Review*. Jan-Fev, 2005.

_____. A face mutável da guerra: rumo à quarta geração. 2007. Disponível em: www.midiasemmascara.com.br/artigo.php?sid=5919. Acesso em: 10/Fev/2008.

MACEDO, Mônica. "A automatização do campo de batalha". *Revista Comciência*. 2002. Disponível em: http://www.comciencia.br/reportagens/guerra/guerra06.htm. Acesso em: 25/09/2008.

NUNES, Paulo Fernando Viegas. "Impactos das Novas Tecnologias no Meio Militar. A Guerra da Informação". Artigo apresentado pelo autor durante o Congresso Internacional da Imprensa Militar em Lisboa de 13 a 16 de setembro de 1999. Disponível em: www.airpower.maxwell.af.mil/apjinternational/apj-p/2000/2tri00/nunes.htm. Acesso em: 10/Set/2008.

_____. “Operações de Informação: Enquadramento e Impacto Nacional”. *Revista Militar*. Portugal. 2006. Disponível em: http://revistamilitar.pt/modules/articles/print.php?id=137. Acesso em: 22/09/2008.

RIQUET FILHO, Luciano Fabrício. Guerra Estratégica de Informações: um novo meio de fazer guerra. Escola de Guerra Naval. Rio de Janeiro, 2003.

SANTOS, Lino. Cibersegurança – a resposta à emergência. *Revista Planeamento Civil de Emergência*. Portugal. Nº 19, 2007. Disponível em: http://www.cnpce.gov.pt/?p=160. Acesso em: 13/set/2008.

SARAIVA, Graziele Oliveira. A política externa norte-americana e o discurso anti terrorismo. Porto Alegre, 2007. Disponível em: http://www4.fapa.com.br/monographia/artigos/3edicao/GRAZIELE.pdf . Acesso em: 20/09/2008.

SCAHILL, Jeremy. *Blackwater: a ascenção do exército mercenário mais poderoso do mundo*. São Paulo. Ed. Companhia das Letras, 2008.

SILVA, Marcio Moreira da; TARANTI, Christian Giorgio Roberto. A ameaça Cibernética e segurança da Informação. 2003.

SILVA, Antonio Ruy de Almeida. “Vencendo a Guerra e Perdendo a Paz”. *Revista do Clube Naval*. Rio de Janeiro, 2004.

STEIN, George. “Guerra de Informação”. *Revista Airpower*, 3º Trimestre, 1995. Disponível em: www.airpower.maxwell.af.mil/apjinternational/apj-p/1995/3tri95/pstein.html. Acesso em: 12/Mar/2008.

SZAFRANSKI, Richard. “Uma teoria da Guerra da Informação: preparação para 2020”. *Revista Airpower*, 3º Trimestre, 2005. Disponível em: www.airpower.maxwell.af.mil/apjinternational/apj-p/1995/3tri95/pszafra2.html. Acesso em: 02/Set/2008.

TEIXEIRA, Alexandre Peres. Guerra assimétrica global: a batalha do século XXI e a capitulação do direito internacional. UNB. Brasília, 2006.

TEIXEIRA DA SLVA, Francisco Carlos. As múltiplas faces do terrorismo e a probabilidade de ocorrência de atentados no Brasil. Encontro de Estudos: Terrorismo, Brasília: Presidência da República, Gabinete de Segurança Institucional, Secretaria de Acompanhamento Estudos Institucionais, 2006.

TOFFLER, Alvin; TOFFLER Heidi. *Guerra e Antiguerra: sobrevivência na aurora do terceiro milênio.* Rio de Janeiro. Ed: Biblioteca do Exército, 1995.

VIDIGAL, Armando F. “A Missão das Forças Armadas para o Século XXI”. *Revista Marítima Brasileira*. Rio de Janeiro, 4º trimestre, 2004.