Artigo Científico

A Tecnologia da Informação e a Ameaça Cibernética na Guerra Irregular do Século XXI.

Alvaro de Souza Pinheiro(*)

O que terroristas, adolescentes e soldados profissionais têm em comum na atualidade? É a necessidade em comunicações ágeis nas suas operações táticas!
(Mathew J. Sheffer, "Awareness Through Agility: Teenagers as a Model for Terrorist Development of Situational Awareness", "IO Sphere", Professional Journal of the Joint Information Operations Warfare Command, San Antonio / Texas, Winter 2007)

RESUMO

O chamado Conflito de 4ª Geração, também identificado como Conflito Irregular Assimétrico, característico da Guerra Irregular, passa por um efetivo processo de evolução, no qual a Tecnologia da Informação é fator preponderante. No contexto mais moderno de sua conceituação, dentre as operações e atividades doutrinariamente inseridas na Guerra Irregular, estão as Operações de Informação. Essas, por sua vez, englobam cinco grandes competências: as Operações em Rede Computadorizada; a Guerra Eletrônica; a Simulação Militar; as Operações de Segurança e as Operações Psicológicas. Na atualidade, organizações revolucionárias não estatais de diferentes matizes vêm empregando a Tecnologia da Informação em Conflitos de 4ª Geração, dela extraindo o máximo de vantagem. Esses movimentos revolucionários estão sendo identificados como Insurreições de 2ª Geração, a fim de serem diferenciados daqueles do período da Guerra Fria. Particularmente, Operações Psicológicas Cibernéticas estão sendo otimizadas por diferentes forças irregulares. Indiscutivelmente, os EUA são o Estado Nacional onde a Tecnologia da Informação está mais desenvolvida. A evolução conhecida como "Revolução nos Assuntos Militares", materializada na 1ª Guerra do Golfo Pérsico, hoje, dá lugar ao conceito de Guerra Rede-Cêntrica. Entretanto, este conceito implica mais do que simplesmente incorporar as últimas tecnologias. Também tem como objetivo interferir na forma como as missões serão cumpridas, como as unidades vão se organizar para o combate, como se relacionarão entre si, e como serão eficiente e efetivamente apoiadas. No contexto da evolução da Guerra Irregular no Sec XXI, tendo como foco a Tecnologia da Informação, avultam os conceitos da Guerra Cibernética e da Segurança da Informação. Esses se baseiam na utilização ofensiva e defensiva de informações e sistemas de informação para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes computadorizadas.

No Brasil, levando em consideração o incremento da sua estatura político-estratégica, fica cada vez mais evidente que as atividades de Guerra Cibernética e Segurança da Informação são parcelas relevantes da defesa dos interesses vitais do Estado Nacional Brasileiro.

Palavras-chave: Guerra Irregular. Conflito de 4ªGeração. Operações de Informação. Insurreições de 2ª Geração. Operações Psicológicas Cibernéticas. Guerra Cibernética. Segurança da Informação. Infra-estrutura Crítica Nacional.

ABSTRACT

The so called Fourth Generation Warfare also identified as Asymmetric Irregular Conflict, characteristic of Irregular Warfare (IW), is living an effective process of evolvement, in which Information Technology (IT) is a relevant factor. In its most modern concept, doctrinally, among different kind of operations and activities, IW comprises Information Operations (IO).

(*) O autor é General-de-Brigada do Exército Brasileiro, doutor em Ciências Militares e especializado em Política, Estratégia e Alta Administração do Exército, ambos pela Escola de Comando e Estado-Maior do Exército (ECEME). É especialista em Operações Especiais e Guerra Irregular. (EMail: pinheiroa@terra.com.br).

IO have five great competences: Computer Network Operations (CNO); Eletronic Warfare (EW); Military Deception (MD); Operations Security (OPSEC); and Psychological Operations (PSYOP). Currently, different kind of non state revolutionary organizations are employing IT in Fourth Generation Warfare, extracting from it maximum of advantage. These revolutionary movements are identified as Second Generation Insurgencies, in order to be differentiated from those of the Cold War Period. Particularly, Cyber Psychological Operations (CYOP) are being optimized by different irregular forces. Unquestionably, USA is the Nation State where IT is most developed. The evolution known as Revolution of Military Affairs (RMA), materialized in the First Persian Gulf War, nowadays, gives place to the concept of Network Centric Warfare (NCW). However, NCW implies more than just incorporating latest technologies; it also addresses how missions are accomplished, how units are combat organized, how they relate to one another, and how they are efficiently and effectively supported. In the context of the IW improvement in the 21st Century, focusing IT, the concepts of Cyber Warfare (CW) and Information Security (IS) stands out. These concepts are based upon the offensive and defensive employment of information and systems of information to deny, exploit, corrupt or destroy adversary's values based upon information, systems of information and computer networks.

In Brazil, considering the improvement of its political strategic height, it's more and more evident that CW and IS activities are a relevant portion on defending the vital interests of the Brazilian Nation State.

Key-words: Irregular Warfare. Fourth Generation Warfare. Information Operations. Second Generation Insurgencies. Cyber Psychological Operations. Cyber Warfare. Information Security. National Critical Infra-structure.

1 A GUERRA IRREGULAR DO SÉCULO XXI

O chamado Conflito de 4ª Geração, também identificado como Conflito Irregular Assimétrico, característico da Guerra Irregular, é consensualmente considerado por analistas militares de diferentes países como o Conflito Armado do Século XXI.

Até porque, há que se considerar que essa modalidade de conflito passa por um processo efetivo de evolução, no qual a implementação da Tecnologia da Informação é fator preponderante.

Segundo o mais atualizado conceito doutrinário, desenvolvido pelo Comando de Operações Especiais dos EUA (U.S. Special Operations Command – SOCOM), atualmente adotado pela OTAN, Guerra Irregular é "uma luta intensa entre atores estatais e não estatais pela legitimidade e influência sobre relevantes populações. Favorece aproximações indiretas e assimétricas, embora possibilite o emprego de todo o espectro de capacitações militares, bem como de outras, a fim de erodir a vontade, o poder e a influência de um inimigo" - Irregular Warfare, Joint Operating Concept (JOC), Version 1.0, Jan 2007.

Destacam-se como suas características básicas: a Guerra Irregular não procura a derrota do adversário pelos meios de confrontação primordialmente militar; enfatiza o emprego de métodos não convencionais e indiretos para subverter, atritar e exaurir um adversário; e busca ganhar o apoio da população para viabilizar a erosão do poder, da influência e da vontade do adversário.

Há que se ter em mente, entretanto, que a Guerra Irregular ou Assimétrica poderá vir a ocorrer, e, via de regra, ocorrerá,

simultaneamente, a uma Guerra Convencional.

Na atualidade, estão doutrinariamente inseridas no contexto da Guerra Irregular as seguintes operações e atividades: Insurreição; Contra-Insurreição (COIN); Terrorismo; Contraterrorismo (CT); Guerra Não Convencional (UW); Operações Psicológicas (PSYOP); Atividades de Inteligência e Contra-Inteligência; Operações de Informação (IO); Comunicações Estratégicas (SC); Operações de Estabilidade, Segurança, Transição e Reconstrução (SSTR); Operações de Defesa Interna no Estrangeiro (FID); Operações Civil Militares (CMO); Atividades criminosas transnacionais e de imposição da lei (LE).

Em todas essas modalidades de operações e atividades, quaisquer que sejam os ambientes operacionais e a natureza das facções em litígio, estarão sempre presentes – como estiveram, desde a bíblica Batalha de Jericó – com diferentes níveis de capacitação, as três funções científico-tecnológicas operacionais básicas, quais sejam: o "Sensoriamento" (obtenção de informações sobre terreno, condições meteorológicas e inimigo); o "Processamento" (tomada da decisão e sua implementação); e a "Atuação" (neutralização da ameaça).

Da mesma forma, mesmo num contexto de Conflito Irregular Assimétrico, as atividades de Inteligência (Humana, de Imagens, e de Sinais) e de Contra–Inteligência serão sempre imprescindíveis ao processo decisório, em quaisquer dos níveis: político-estratégico, operacional ou tático.

2 AS OPERAÇÕES DE INFORMAÇÕES NOS ATUAIS CONFLITOS DE 4ª GERAÇÃO

Sendo uma das modalidades de operações doutrinariamente compreendidas pela Guerra Irregular, as Operações de Informação (Information Operations - IO) englobam cinco grandes competências: as Operações em Rede Computadorizada (Computer Network Operations – CNO); a Guerra Eletrônica (Eletronic Warfare - EW); a Simulação Militar (Military Deception - MILDEC); as Operações de Segurança (Operations Security - OPSEC); e as Operações Psicológicas (Psychological Operations - PSYOP).

O objetivo primordial das Operações de Informação é proporcionar aos comandantes, em todos os níveis, um conhecimento atualizado e fidedigno da situação em presença, qualquer que seja o ambiente operacional. Esse conhecimento é indispensável ao gerenciamento de qualquer campo de batalha, independente da natureza do conflito em presença. Efetivas estimativas da situação são, inequivocamente, indispensáveis para a tomada de decisões oportunas, adequadas e pertinentes.

O comprometimento dos EUA como Estado Nacional que lidera a pesquisa, o desenvolvimento e o emprego de operações dessa natureza fica demonstrado pela recente evolução do antigo Joint Information Operations Center em Joint Information Operations Warfare Command (JIOWC), San Antonio, Texas. Trata-se de um Grande Comando Combinado, responsável pelo planejamento, integração e sincronização das Operações de Informação em apoio aos Grandes Comandos Combinados Operacionais dos EUA, ao redor do globo. O JIOWC está diretamente subordinado ao U.S. Strategic Command (USSTRATCOM).

Especialistas nessa área têm verificado que organizações revolucionárias não estatais, integradas por forças irregulares, vêm empregando a Tecnologia da Informação (Information Technology – IT) em Conflitos de 4ª Geração, dela extraindo o máximo de vantagem. Inclusive, os movimentos revolucionários que, na atualidade, demonstram a capacitação de maximizar, em seu proveito, as Operações de Informação, estão sendo identificados como Insurreições de 2ª Geração, a fim de serem diferenciados daqueles do período da Guerra Fria, (Second Generation Insurgencies) ou,

ainda, como Conflitos Assimétricos de 2ª Geração (Second Generation Asymetric Warfare). Dentre estas organizações, destacam-se: o Hezbollah, o Movimento Talibã e a Al Qaeda, nos respectivos Teatros de Operações do Líbano, Afeganistão e Iraque.

A diferença básica entre as Insurreições ditas de 1ª Geração e as de 2ª é que as primeiras eram conduzidas longe da observação da mídia; muito pouco se divulgava sobre as campanhas em curso ou a respeito de seus sucessos ou reveses. As de 2ª Geração são desenvolvidas tendo como fundamento essencial o "oxigênio" da publicidade, tremendamente disponível na atualidade, e que quando não adequado e oportunamente aproveitado conduz o movimento revolucionário a uma inexorável derrota em curto prazo.

Os Conflitos Assimétricos de 1ª Geração eram conduzidos longe da observação da mídia. Atualmente, os de 2ª Geração se desenvolvem em torno do "oxigênio" da publicidade, o qual, se não oportuna e adequadamente aproveitado, leva o movimento evolucionário a uma derrota inexorável.

Nesse contexto, é possível identificar com clareza o desenvolvimento das chamadas Operações Psicológicas Cibernéticas (Cyber Psychological Operations – CYOP), também identificadas por pessoal especializado como Mensagens Guiadas de Precisão (Precision Guided Messages – PGM) que, basicamente, são operações desenvolvidas com suporte da Informática, visando, objetivamente, atacar e influenciar atitudes, comportamentos e posturas dos combatentes − de todas as facções em presença − e da população de uma maneira geral. As CYOP são caracterizadas pela velocidade, precisão e criatividade. Diariamente, é possível, em diferentes ambientes operacionais, verificar-se como incidentes de natureza diversificada são, imediatamente após sua ocorrência, reportados pela Internet, ou por telefones celulares ou ainda por vídeo mensagens, bem antes que órgãos de comunicação social dotados de credibilidade possam verificar a autenticidade daqueles reportes.

Organizações como a Al Qaeda e o Hezbollah têm desenvolvido CYOP extremamente eficientes e eficazes, não apenas para o público externo, como também para o público interno, como se pode perceber, por exemplo, nas atividades de recrutamento nas comunidades muçulmanas em diferentes países do Oriente Médio.

Com tais recursos cibernéticos, o emprego das Operações Psicológicas ganha uma dimensão que extrapola o ambiente operacional, atingindo até mesmo outros continentes, com repercussões tremendamente relevantes em todos os níveis do conflito em presença. Apesar de tudo isso, analistas internacionais avaliam que as Operações de Informações do Exército dos EUA, no que se refere à contrapropaganda, têm deixado muito a desejar. E em função dessa idiossincrasia, já há quem advogue, no próprio Departamento de Defesa, a separação das Operações Psicológicas, que passariam a constituir um Comando de mesmo nível que o JIOWC.

3 OS EUA, A REVOLUÇÃO DA INFORMAÇÃO E A GUERRA REDE-CÊNTRICA

Já há algumas décadas que o mundo vem procurando se adaptar aos dramáticos progressos desenvolvidos, principalmente, na tecnologia da informação e das comunicações, particularmente a partir do emprego intensivo da Internet.

Esses extraordinários avanços motivaram transformações radicais na criação de novos modelos de negócios, que efetivamente deram origem a uma nova "Economia da Informação". Em todo o mundo, empresas diversificadas passaram a trocar bens, serviços, e informação por meios

altamente eficientes e eficazes que praticamente ignoram fronteiras geográficas, criando novas e muito bem fundamentadas associações geopolíticas, num mundo cada vez mais globalizado.

Indiscutivelmente, os EUA são o Estado Nacional mais desenvolvido no que se refere à Tecnologia da Informação. E este tremendo salto científico-tecnológico, conhecido como Information Revolution, se deveu, inequivocamente, ao emprego com finalidade militar.

Nessa área, o grande laboratório foi a Operação Desert Storm, na 1ª Guerra do Golfo Pérsico. E aquele tremendo êxito alcançado, com base na Tecnologia da Informação, propiciou uma evolução que passou a ser conhecida como a Revolução nos Assuntos Militares (Revolution in Military Affairs – RMA).

Na atualidade, o conceito de RMA foi substituído pelo de Guerra Rede-Cêntrica (Network Centric Warfare - NCW). Trata-se de um conceito operacional que, apesar de emergente, foi testado em exercícios de campanha e jogos de guerra convencional, já vem sendo exaustivamente empregado nos diversos cenários onde estão se desenvolvendo operações militares no contexto da "Guerra Global contra o Terror". O que se pretende é consolidar todas as evoluções até agora desenvolvidas, propiciando aos sistemas de comando e controle (C4ISR - Comando, Controle, Comunicações, Computadores, Inteligência, Vigilância e Reconhecimento), em todos os níveis, uma perspectiva de consciência situacional, até agora inédita e improcedente, do campo de batalha, qualquer que seja o ambiente operacional em presença. Entretanto, não se trata apenas de incorporar as últimas tecnologias, o espectro abrangido vai muito além.

O NCW tem como objetivo interferir na forma como as missões serão cumpridas; como as unidades serão organizadas para o combate; como elas se relacionarão entre si, em curso de operações; e como serão apoiadas no combate e logisticamente. O fundamento básico do NCW é a difusão simultânea de informações (digitalizadas) a diferentes escalões, propiciando uma acentuada aceleração no ritmo das operações, significativo incremento na sincronização das ações desenvolvidas pelos diferentes sistemas operacionais (Comando e Controle; Inteligência; Manobra; Apoio de Fogo; Mobilidade, Contra-Mobilidade e Proteção; Defesa Anti-Aérea; e Apoio Logístico); considerável redução das baixas em combate; e otimização das condições para a manutenção da iniciativa das ações em relação ao inimigo.

Na verdade, as experiências desenvolvidas nos Centros de Operações Táticas (COT) dos Grandes Comandos Divisionários, Grandes Unidades valor Brigada e Unidades valor Batalhão, particularmente nas operações contra forças irregulares no Iraque e no Afeganistão, bem como nos sistemas de comando e controle das Forças de Operações Especiais, tanto nesses Teatros quanto em operações contraterrorismo em diferentes partes do globo (inclusive na Colômbia), estão demonstrando que, ao mesmo tempo em que compartilhar informações simultaneamente se constitui num valioso incremento ao poder de combate, isto carrega consigo uma série de implicações de grande complexidade, as quais ainda não estão adequada, oportuna e plenamente resolvidas.

Compartilhar informações simultaneamente, ao mesmo tempo em que se constitui num valioso incremento ao poder de combate, carrega consigo uma série de implicações de grande complexidade, as quais ainda não estão adequada, oportuna e plenamente resolvidas.

Mesmo assim, em julho de 2008, o Exército dos EUA divulgou a ativação de seu primeiro Network Warfare Battalion (NWB). Esta unidade não operará como um

todo e independentemente, mas sim, por meio de destacamentos operacionais, frações que serão alocadas ao comando de Grandes Comandos e Grandes Unidades, visando o apoio às operações de combate nos Teatros do Iraque e do Afeganistão, bem como às operações contraterrorismo em diferentes partes do mundo. Estará também em condições de participar de Operações Cibernéticas (Cyber Operations) junto a elementos da U.S. Air Force e U.S. Navy, bem como de outros países.

Este Batalhão tem como seu escalão imediatamente superior a 704 Military Intelligence Brigade, que por sua vez está subordinada ao U.S. Army Intelligence and Security Command (INSCOM). Esta subordinação demonstra, por si só, que o grande objetivo das ações a serem desencadeadas é prioritariamente focado no Sistema Operacional de Inteligência e Contra-Inteligência.

Muito embora esse primeiro Batalhão seja da Força Terrestre, todas as demais Forças estão decisivamente engajadas no esforço conduzido pelo Departamento de Defesa para o desenvolvimento de sistemas ofensivos e defensivos de Guerra Cibernética (Cyber Warfare). Segundo dados divulgados por especialistas, as Forças Armadas dos EUA possuem, atualmente, dezenas de milhares de profissionais engajados em atividades dessa natureza. E a tendência natural é que outras unidades especializadas valor Batalhão, e mesmo valor Brigada, venham a ser ativadas.

4 A AMEAÇA CIBERNÉTICA NO MUNDO

Em fevereiro de 1999, a editora oficial do Exército de Libertação do Povo divulgou um livro de autoria de dois coronéis − altos oficiais de política da Força Aérea da China − Qiao Liang e Wang Xiangsui. Traduzido para o inglês pela Central Intelligence Agency (CIA) em 228 páginas, o livro recebeu o título de "Unrestricted Warfare" (Guerra Irrestrita). Inicialmente, não recebeu muita publicidade; porém os dramáticos eventos de 11 de setembro de 2001 mudaram radicalmente esse perfil, porque, naquele momento, ficou claro para o mundo que a guerra irrestrita deixou de ser teórica e transformou-se numa dramática realidade.

Este livro, até hoje, chama a atenção da mídia ocidental por advogar o emprego de uma multiplicidade de meios militares e, particularmente, não militares, para um ataque aos EUA, na eventualidade de um conflito. A violação de sites da Internet; o ataque cibernético às redes informatizadas de comunicações, transportes, e instituições financeiras, dentre outras; o desencadeamento sistemático do terrorismo, seletivo e indiscriminado, e da guerra psicológica, por meio de exploração da mídia; o potencial aproveitamento da guerrilha urbana; e a ameaça de que Pequim pode vender armas de destruição em massa para países e organizações que apóiem o terrorismo, destacam-se entre as táticas, técnicas e procedimentos preconizados naquela obra.

Os autores ressaltam que: "na guerra irrestrita, a primeira regra é a de que não existem regras. Nada é proibido." E que

> "... trazer a Guerra Cibernética para os sistemas militares é tão importante quanto os Poderes Naval, Terrestre e Aéreo."

Tudo dentro do contexto de uma Guerra Estratégica da Informação, que tem como seus vetores principais: a Guerra Cibernética e a Segurança da Informação.

O conceito mais difundido de Guerra Cibernética no mundo ocidental é o preconizado por Campen, Dearth e Godden na obra "Cyber War: Security, Strategy and Conflict in the Information Age". Segundo esse conceito, a "Guerra Cibernética corresponde ao uso ofensivo e defensivo de informações e sistemas de informação para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes

computadorizadas." Os Estados Nacionais, de uma maneira geral, têm procurado desenvolver estruturas sistêmicas que lhes proporcionem adequados níveis de Segurança da Informação, sobretudo, com relação às atividades militares diretamente relacionadas com a Defesa Nacional e com os demais componentes de sua infra-estrutura crítica (transportes, energia, telecomunicações, saúde, águas, finanças etc.).

China e Rússia vêm se destacando dentre alguns países que estão encarando como ação estratégica estatal a formação do que analistas estão identificando como "guerreiros cibernéticos". Fontes especializadas asseguram que os chineses estão decisivamente engajados nas tecnologias de desenvolvimento de vírus e worms, bem como na abertura de brechas de segurança na Internet. São inúmeros os países que consideram o "ambiente cibernético" com uma nova dimensão do combate, assim como o mar, a terra, o ar e o espaço sideral. O computador pessoal transformou-se numa arma perigosa, eficiente e eficaz, mesmo quando utilizado por adolescentes. E a tecnologia "hacker" transformou-se num poderoso instrumento bélico. Nos EUA, são inúmeros os episódios de invasão em redes de sistemas de infra-estrutura nacional crítica, inclusive penetrando no Sistema de Comando e Controle do Pentágono. Tudo com base em capacitações que se encontram facilmente disponíveis em todo o mundo.

Em fevereiro de 2003, o Governo dos EUA expediu a "National Strategy to Secure the Cyberspace", que determina como 1ª prioridade o estabelecimento do National Cyberspace Security Response System. Este, não somente recupera um determinado sistema objeto de um ataque, como também detecta, analisa e responde. A estrutura da Cyber Warning Information Network (CWIN) tornou-se operacional a partir de junho de 2003, possuindo 30 nódulos que possibilitam ao governo e a indústria compartilhar informações relacionadas a ataques cibernéticos e outras ameaças a sistemas computadorizados.

Além da capacitação para interceptar comunicações de satélites regionais em praticamente todo o mundo, os EUA desenvolveram junto ao Canadá, Grã Bretanha, Austrália, e Nova Zelândia, o "Projeto Echelon" que possibilita, em condições ótimas, o monitoramento de telefones, fax, telex, rádio e Internet, em qualquer parte do planeta.

5 O BRASIL E AS SUAS VULNERABILIDADES CIBERNÉTICAS

Uma realidade incontestável, que é ratificada a cada momento no contexto da atual conjuntura internacional, é que a tecnologia da Guerra Cibernética e da Segurança da Informação não se compra, nem se importa, desenvolve-se.

Não obstante os esforços envidados no sentido de se estabelecer uma perspectiva mais integrada da infra-estrutura crítica, em função de uma atuação mais presente das agências reguladoras, objetivo a que se propõe o Departamento de Segurança da Informação e Comunicações do Gabinete da Segurança Institucional da Presidência da República, o que se observa em termos de Brasil é, de uma maneira geral: a obsolescência dos sistemas; a presença de sistemas de proteção importados; a inexistência de testes adequados nos planos de contingência; e em determinadas áreas, como é o caso da infra-estrutura das telecomunicações, excessiva presença da privatização por empresas estrangeiras.

Segundo analistas especializados, a inexistência de uma cultura padronizada na Segurança da Informação fica caracterizada pela vulnerabilidade da coordenação de ações conjuntas, pelo tímido estabelecimento de padrões e normas nacionais, bem como por uma legislação que necessita adequar-se aos crimes da Informática e Segurança da Informação.

A elevação do Brasil a patamares adequados passa por um maior incentivo à formação acadêmica de recursos humanos

especializados em: resposta a incidentes; verificação de vulnerabilidades; teste e correção de procedimentos e, onde há que se enfatizar, redução da dependência externa e diferentes áreas de pesquisa. Em termos de criptografia nacional, é impositivo o desenvolvimento de códigos nacionais, o incremento das atividades de cripto-análise e a regulamentação de códigos e auditorias. Apesar da NBR 17799 (código de práticas para a gestão de Segurança da Informação), é impositiva a elaboração de diretrizes, regras e procedimentos que regulem como uma organização controla, protege e distribui informações sensíveis.

No "Jornal do Brasil", de 31 de julho de 2008, o colunista político Mauro Santayana divulgou uma denúncia muito grave da Associação dos Engenheiros da Petrobrás. Segundo aquela Associação, quem detém todas as informações sobre o potencial brasileiro de combustíveis fósseis é a Empresa Halliburton, dos EUA. Ainda, que a Agência Nacional do Petróleo (ANP) teria contratado, sem licitação, uma subsidiária daquela multinacional (Landmark Digital and Solutions) para administrar o banco de dados das reservas e explorações da Petrobrás. Confirmada a denúncia, fica caracterizado um verdadeiro crime lesa Pátria, envolvendo a ruptura da segurança de uma informação estratégica, vital aos mais relevantes interesses nacionais.

Na verdade, em função de sua crescente estatura político-estratégica, fica cada vez mais evidente que as atividades de Guerra Cibernética e Segurança da Informação são parcelas relevantes da defesa dos interesses vitais do Estado Nacional Brasileiro.

Não há dúvida que a Nação pode pagar um preço muito alto menosprezando a segurança dos seus sistemas de informações. E, ineqüivocamente, o processo de gerenciamento dessas atividades deve ser liderado pelas Forças Armadas, em função de sua sedimentada cultura de Segurança Nacional, bem como pelo excepcional padrão de qualidade dos recursos humanos e pelo potencial de conhecimento (pesquisa e desenvolvimento) já existente nos seus Centros Tecnológicos.

REFERÊNCIAS

"Irregular Warfare Special Study", Joint Warfighting Center / USJFCOM, Aug 2006.

"Information Assurance: Trends in Vulnerabilities, Threats, and Technologies", edited by Jacques S. Gansler and Hans Binnendijk , Center for Technology and National Security Policy / NDU, Jan 2005.

"Unrestricted Warfare", Qiao Liang and Wang Xiangsui, PLA Literature and Arts Publishing House, Beijing, Feb 1999.

"Information Operations: The Challenges of Second Generation Insurgencies", David Sloggett, "IO Sphere", Winter 2007.

"The Network Warfare Battalion", James Dunnigan, "Strategy Page" / " News As History", July 12, 2008.

"Ameaça Cibernética e Segurança da Informação", CC (EN) Marcio Moreira da Silva / Diretoria de Telecomunicações da Marinha e Cap (Eng) Christian Giorgio Roberto Taranti / Centro Tecnológico da Aeronáutica., Exposição efetuada no Ministério da Defesa em 15 Jul 2003.

"O Brasil Ganha uma Visão Mais Integrada da Infra-Estrutura Crítica", Livro Branco da 2ª. Conferência de Segurança de Governo (SECGOV 2006), Brasília / DF, VIA FORUM, Edição 2 – ANO 1 – Nr 2 – Dez 2006 – Distribuição Seletiva.