SIMPÓSIO - VIGILÂNCIA DE FRONTEIRAS 2011

28 – 29 Junho 2011, Brasília - DF

Estudo sobre a Guerra de Informação na China

José Ricardo Rodrigues Teixeira **Alves**[1]
Capitão de Mar-e-Guerra (RM1-EN)

""Atacai-o onde não estiver preparado. Executai as vossas investidas somente quando não vos esperar."
Sun Tzu

1 - Propósito

O propósito deste artigo é situar a Guerra de Informação[2] (GI), pela análise da conjuntura e de cenários decorrentes e, posteriormente, situar a Guerra Cibernética[3] (GC).

2 – Introdução: conceitos pertinentes associados à GI

2.1 – Aspectos operacionais:

As tecnologias de informação e das comunicações, integradas, desencadearam uma verdadeira revolução, iniciando uma nova era, cujas características são o transporte instantâneo de dados imateriais e a proliferação das conexões virtuais e redes eletrônicas. A Internet constitui o coração, a encruzilhada e a síntese dessa mutação em curso. As "infovias" representam, na era atual, o que as estradas de ferro

---

1 O autor exerceu a função de Superintendente de Apoio aos Sistemas, na Diretoria de Telecomunicações da Marinha (1999 – 2003), cursou a Escola de Guerra Naval: C-PEM Curso de Política e Estratégia Marítimas, onde desenvolveu a monografia "A Guerra de Informação (Information Warfare – IW): O Cenário do Futuro" (2003); e MBA COPPEAD em Gestão Internacional, onde desenvolveu a monografia "Guerra na Rede – Estudo de Formas de Organização e Comportamento Organizacional das Ameaças Difusas" (2003), orientado pelo Prof. Doutor Francisco Carlos Teixeira da Silva (UFRJ). e também exerceu a função de Superintendente de Sistemas na Diretoria de Sistemas de Armas da Marinha (2003 – 2005), quando passou à reserva remunerada. Prestou sérvios como Monitor de Tecnologias de Informação e Comunicações para o PNUD (Programa das Nações Unidas para o Desenvolvimento), atuando sob a direção da Assessoria Especial do Ministério do Esporte nos XV Jogos Pan-Americanos Rio 2007 (2007), e como Coordenador de Avaliação de Projeto (para o mesmo PNUD), atuando sob a direção da Diretoria de Tecnologias Educacionais (DITEC) subordinada à Secretaria de Estado de Educação do Estado do Paraná (SEED-PR) no Projeto Paraná Digital (2008-2009). Também prestou serviços para a Organização dos Estados Ibero-americanos para a Educação, a Ciência e a Cultura (OEI) – Fundo Nacional de Desenvolvimento da Educação (FNDE) – Coordenação Geral de Tecnologia da Informação (CGETI), como Analista de Processos de Negócio apoiando o desenvolvimento de sistemas, desenvolvendo metodologia de mapeamento e modelagem de processos (2010 – 2011). Atualmente presta serviços como consultor de segurança de informações digitais (política de segurança e análise de risco) e como analista de processos de negócio.

2 Para o propósito deste artigo, será utilizado o conceito de GI difundido pela "School of Information Warfare" da "National Defense University",2 dos EUA [1].

> *"... é uma abordagem do conflito armado que focaliza o gerenciamento e o uso da informação sob todas as suas formas e em todos os níveis, para conquistar uma decisiva vantagem militar".*

Outras abordagens:

A definição apresentada acima é coerente com aquela apresentada em relatório do Congresso norte-americano [2]:

> *"GI envolve ações empreendidas para obter superioridade de informação afetando-se a informação do adversário, seus processos baseados em informação, seus sistemas de informação e suas redes baseadas em computadores enquanto se defende a própria informação, os processos baseados em informação, os sistemas de informação e as redes baseadas em computadores. GI é definida como Operações de Informação conduzidas em tempo de paz, crise e conflito para atingir e promover objetivos específicos sobre adversário(s) específico(s)".*

Também encontra forte correlação com outra definição, disseminada pela Marinha Americana (DoD, 201, Enc. 2-1):

> *"GI é o uso de informação para dar suporte à estratégia de segurança nacional com o objetivo de estabelecer e manter vantagem decisiva atacando-se a infra-estrutura de informação do adversário através da exploração, negação e influência, enquanto se protege os sistemas de informações amigos. GI é implementada na estratégia militar nacional por GC[2](Guerra de Comando e Controle)".*

3 guerra desenrolada no espaço cibernético [2], envolvendo a utilização de ferramentas disponíveis na eletrônica e na informática para interferir nos sistemas eletrônicos e de comunicações inimigas, além de manter os próprios sistemas operacionais. Utiliza-se de centros de informações de combate com profissionais e equipamentos de alta tecnologia, cuja finalidade consiste em fazer chegar aos comandantes os dados utilizados na situação verificada no campo de batalha. Seus efeitos são muito semelhantes ao da pirataria eletrônica. A GC designa atividades no espaço cibernético. Ela pode incluir ataques dissuasórios de informação e negação da habilidade do inimigo de fazer o mesmo, além de incluir operações ofensivas ou operações destinadas a obter a SI campo de batalha.

Espaço Cibernético: É o conjunto formado por todas as interconexões de seres humanos (cibernauta[3]) através de computadores e telecomunicações, sem considerar a geografia física (é um "espaço virtual"). Termo cunhado por William Gibson, em 1984, no romance "Neuromancer". É muitas vezes usado como uma metáfora para descrever domínios não-físicos[3] (ou seja, "virtuais"), criados por sistemas de computadores. Da mesma forma que o domínio físico, contém objetos (arquivos, mensagens, gráficos etc.) e diferentes modos de transporte e disponibilização ("protocolos") [3]. Também pode ser definido como o conjunto de pessoas, sítios e computadores que compõe a Internet [4].

foram para a era industrial: fatores de impulso e intensificação das trocas.

Mesmo na guerra moderna, o uso crescente de computadores propiciou a criação de um universo onde a sua aplicação é ampla e decisiva, caracterizando-se pela multiplicidade qualitativa e quantitativa das informações que empregam. Os avanços tecnológicos dessa era, ao serem incorporados a forças militares, traduzindo-se na utilização de novos conceitos associados à informação, impõem uma nova postura para agregar o valor desses avanços de forma eficiente.

Hoje, com a internacionalização dos conflitos e a globalização da economia mundial, a Guerra de Informação (GI), assume importância significativa, sendo foco de debates nos âmbitos militar e civil. Analisando-a no contexto da evolução histórica da arte da guerra, destaca-se uma evolução marcada por fatos extremamente relevantes que deram início a verdadeiras eras, que não distorcem os princípios da guerra, enunciados por Clausewitz ou Sun Tzu, mas otimizam a utilização dos recursos disponíveis de forma que esses princípios são assegurados eficazmente, se traduzindo em vitória.É uma abordagem multifacetada, e sua maior expressão seria a Guerra de Manobra[4] (GM). A utilização da Tecnologia da Informação (TI) na arte de combater também "encurtou" o espaço físico. Guerrear, portanto, significa agir mais rápido que o oponente, não permitindo sua reação e quebrando, conseqüentemente, sua coesão e sua capacidade de lutar como força organizada, num espaço hexa-dimensional (naval, terrestre, aérea, espacial, eletrônica e cibernética) [5].

Na GM, a velocidade é vital para a vitória. Traduz-se em agir antes que o inimigo possa reagir, a fim de causar desequilíbrio. Retira-se dele a capacidade de percepção e, portanto, sua compreensão sobre a realidade no campo de batalha. Ele estará fadado a tomar decisões erradas e será derrotado. É necessário atacar de forma intensa, coordenada e precisa (*swarming*[5]). Não se trata apenas de velocidade física (embora a guerra, atualmente seja hexa-dimensional), mas também velocidade na tomada de decisões. Percebe-se que as guerras do século XXI não possuem forças inimigas bem definidas, nem envolvem diretamente Estados-nação. Essa concepção é uma evolução do conceito tradicional de forças combinadas. É a Guerra Centrada em Redes[6] (GCR), onde não somente a tecnologia tem um papel importante, mas a gestão da informação e do conhecimento e a estrutura organizacional passam a ter um papel fundamental.

A obtenção da Superioridade de Informação (SI) implica em um potencial de utilização da GC, entre outras modalidades de guerra.

A Tabela 1 ilustra a variação na velocidade da tomada de decisões, sob a forma do impacto das transformações no campo de batalha sobre o ciclo OODA (Observar, Orientar, Decidir e Agir). A Figura 1 ilustra a evolução da capacidade de acesso da informação ao longo da história.

---

[4] É um estilo de guerra que procura superar um problema através de uma posição vantajosa, ao invés de ir de encontro direto do mesmo, procurando acumular a destruição cumulativa do arsenal inimigo. O objetivo é incapacitar o inimigo, visando incapacitar sistematicamente o seu sistema de combate. Desta forma, o sistema perderá a coesão. O sucesso não dependerá somente de técnicas e procedimentos, mas da capacidade de entender as características do sistema inimigo, do emprego da surpresa e da velocidade, sem as quais não se pode concentrar poder contra fraquezas, e do tempo, o qual passa a ser uma arma.

[5] A tradução literal seria "enxame de abelhas". Conceito doutrinário, sendo aperfeiçoado nos EUA. Estabelece um novo paradigma ao defender que o uso de TI, num contexto de GI, mudará a natureza dos conflitos atuais. [6] É uma maneira estruturada e coordenada de engajar o inimigo de todas as direções, com todos os meios disponíveis de utilização de força e fogo, de distâncias próximas ou grandes. Depende, para seu sucesso, de uma miríade de unidades pequenas, conectadas em rede, onde a sinergia provocada pelo uso de TI será o diferencial que se traduzirá em vitória [7].

[6] Guerra Centrada em Redes. Define-se GCR como a habilidade que forças dispersas, geograficamente ou hierarquicamente, possuem de criar um alto nível de consciência situacional, que pode ser explorada para se atingir os objetivos da guerra [8].

GCR é a forma de materializar (parametrizar, modelar, planejar, executar etc.) os conceitos de GI. Tornam-se necessárias mudanças nos conceitos de operação, doutrina, organização, concepções de comando, treinamento e outros elementos organizacionais, para que se obtenha fluxo adequado de informações funcionais.

Abandona o conceito de guerra centrada em plataformas, onde se concentram os sensores, as armas e os decisores (Comando e Controle - C^2). A visão norte-americana propõe uma rede independente de sensores (somente), com comando próprio, uma rede independente de atiradores, também sob comando próprio e uma rede de decisores (C^2). Elementos de redes diferentes falam entre si (relacionamentos horizontais), sem necessidade de se reportar ao nível superior. Estabelece, portanto, uma nova forma de estrutura organizacional do tipo rede (onde todos os elementos estão fortemente conectados em rede de computadores), para forças militares em combate.

A hipótese central da GCR é que este conceito aplicado a uma força armada será capaz de gerar poder de combate crescente por possuir melhor sincronização de efeitos no campo de batalha, pela obtenção de maior velocidade de comando e letalidade, além de ter maior possibilidade de sobrevivência e possuir capacidade de resposta crescente. Considera-se que, a posse de mais e melhores informações, resulta na obtenção de melhor consciência compartilhada e melhores níveis de interoperabilidade e ações sincronizadas.

É uma concepção futurista de organização de combate.

TEMPO					
Ciclo OODA	**~1780**	**~1850**	**~1940**	**~1990**	**~2000**
Observação	Luneta	Telégrafo	Rádio e radar	Sensores	Redes integradas
Orientação	Semanas	Dias	Horas	Minutos	Contínua
Decisão	Meses	Semanas	Dias	Horas	Imediata
Ação	1 estação	1 mês	1 semana	1 dia	Minutos

Tabela 1 - Transformações no campo de batalha em relação ao ciclo OODA

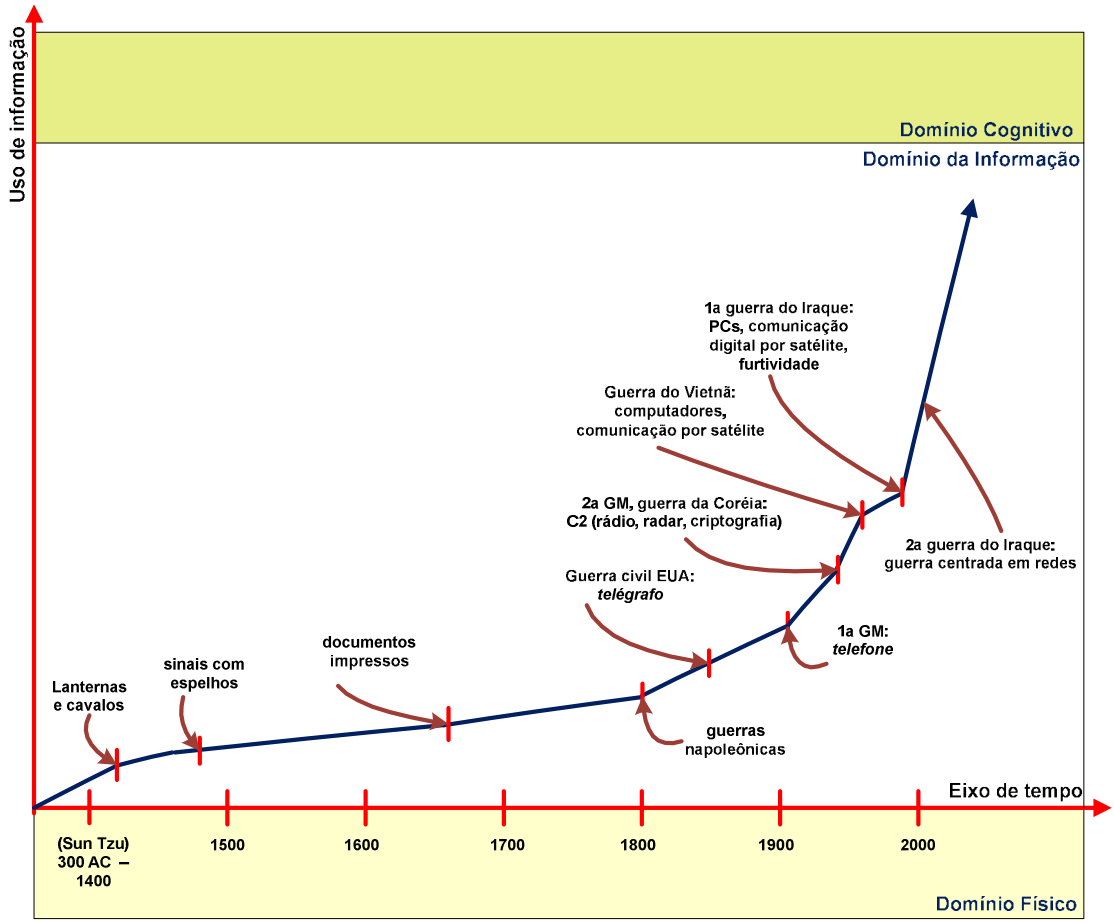


Figura 1 - Capacidade de acesso à informação.

Alves [9] e Nunes [10] subdividem a GI em envolventes: GC^2 (desenvolve-se por intermédio de ações que dificultam a capacidade de tomar decisões do inimigo), SegOp[7] (destina-se a garantir a preservação dos próprios segredos, assim como do local onde eles residem. Obtém-se pela proteção adequada das informações digitais através de estabelecimento de Políticas de Segurança de Informações Digitais: segurança de redes, segurança de acesso, segurança de conectividade, criptografia, segurança das instalações e segurança do pessoal), Guerra Eletrônica (GE - visa neutralizar os sistemas de C^2 do inimigo, atuando sobre as suas comunicações e sensores, enquanto assegura-se a integridade dos próprios sistemas), pirataria eletrônica (*hacking* - consiste numa ação de "guerrilha eletrônica", através da qual qualquer pessoa pode participar, conectando-se à Internet), bloqueio de informação (obtido através

[7] Segurança Operacional.

da destruição física ou lógica da infra-estrutura de comunicações[8] do inimigo), Guerra Psicológica (GP - a mente humana é o alvo do ataque, buscando-se quebrar a vontade de lutar do oponente) e GC.[9]

Seriam utilizadas armas de três classes: **armas de efeito físico**; **armas de efeito de sintaxe** (tem como objetivo atacar a lógica operacional de um sistema de informação, introduzindo atraso ou comportamento indesejável no seu funcionamento. São de complexidade média, possuem foco de ataque estrutural, e de emprego de modelo estatístico na escolha de alvos. Tem por objetivo adquirir o controle ou desativar as redes que conectam os sistemas de informação. Como exemplo, podemos citar os vírus de computador, vermes e cavalos-de-tróia); e **armas de efeito de semântica** (têm como objetivo destruir a confiança que os utilizadores possuem no sistema de informação e na rede que os suporta, além de influenciar a sua interpretação da informação que neles circula. O foco de utilização será comportamental, obtido pela manipulação, modificação e destruição dos modelos de decisão, da percepção e da representação da realidade, construída através da utilização de um sistema de informação pertencente a um sistema de comando e controle).

Após analisarmos o conceito da GI, é necessário inseri-lo em um contexto adequado. Como será demonstrado, este contexto é o da Guerra Assimétrica[10] (GA).

Observando a assimetria no contexto mundial, ao se analisar, atualmente, um tipo qualquer de conflito, algumas premissas parecem importantes:

a) todas as nações do globo estão sendo confrontadas com um modelo de poder econômico e militar sem paralelo na história mundial, e contra o qual nenhuma nação tem meios de defesa;

b) as declarações de guerra não mais existem;

c) as guerras atuais não são semelhantes às do passado;

---

8 os satélites, as ligações por cabo e as torres de microondas que canalizam a informação para o interior do território inimigo.

9 A GC é considerada como a guerra desenrolada no espaço cibernético [11], envolvendo a utilização de ferramentas disponíveis na eletrônica e na informática para interferir nos sistemas eletrônicos e de comunicações inimigas, além de manter os próprios sistemas operacionais. Utiliza-se de centros de informações de combate com profissionais e equipamentos de alta tecnologia, cuja finalidade consiste em fazer chegar aos comandantes os dados utilizados na situação verificada no campo de batalha. Seus efeitos são muito semelhantes ao da pirataria eletrônica. Ela pode incluir ataques dissuasórios de informação e negação da habilidade do inimigo de fazer o mesmo, além de incluir operações de informação.
Espaço cibernético: É o conjunto formado por todas as interconexões de seres humanos (cibernauta - "Astronauta" do espaço cibernético, isto é, um usuário da Internet - quando desempenha funções militares, recebe o nome de "guerreiro cibernético" - tradução proposta de "cyberwarrior") através de computadores e telecomunicações, sem considerar a geografia física (é um "espaço virtual"). Termo cunhado por William Gibson, em 1984, no romance "*Neuromancer*". É muitas vezes usado como uma metáfora para descrever domínios não-físicos (ou seja, "virtuais"), criados por sistemas de computadores. Da mesma forma que o domínio físico, contém objetos (arquivos, mensagens, gráficos etc.) e diferentes modos de transporte e disponibilização ("protocolos"). Também pode ser definido como o conjunto de pessoas, sítios e computadores que compõe a Internet [4].

10 é a forma de se impor ao inimigo (superior militarmente) usando recursos capazes de alterar o curso da guerra, como por exemplo GI e armas não convencionais.
As assimetrias observadas, para um lado, são: poder econômico e financeiro (muitos recursos versus poucos), capacidade bélica, estruturação organizacional (hierarquia versus rede).
As assimetrias do outro lado são: objetivação (número quase infinito de alvos versus poucos alvos para o adversário), resultados (indiferença de resultados a curto e médio prazos contra a necessidade de resultados expressivos do adversário a curto prazo) e comportamental (não sujeição a nenhuma regra, inclusive admitindo-se o suicídio na ação versus um adversário preso a regras e a convenções).
O terrorismo, considerado a pior das ameaças difusas não é uma assimetria propriamente dita, mas a utiliza para obter sucesso na execução de suas ações. Possuem recursos financeiros e capacidade bélica muito inferiores ao de um Estado-Nação que os desfavorecem, mas detêm estrutura organizacional do tipo rede, objetivação (número quase infinito de alvos em potencial a serem atacados), resultados e comportamento como características favoráveis.
As formas de GA são: 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.
São características da GA:
a) desgaste visando a imobilização operacional do adversário: é uma guerra dos fracos contra os fortes. O desgaste tornará o oponente incapaz de uma vontade política. Ao término desta guerra se tem muito mais uma vitória política do que uma vitória militar;
b) ofensiva: não sendo guerras revolucionárias elas perdem o caráter defensivo;
c) global: é onde reside a sua eficácia, traduzindo-se em maior determinação e em melhor delimitação de objetivos;
d) atemporalidade: não tem começo. Só historicamente é que se define o tempo da guerra. Os envolvidos têm interesse em prolongar um falso período de paz, antes da definição explícita de seu início.
e) delineamento indefinido: não distingue objetivamente entre alvo civil e militar, entre armas e não armas, entre espaço de guerra e de paz.
f) mobilidade: apresenta um sentido claro para se desencadear as ações militares. A luta pode surgir em qualquer uma das seis dimensões anteriormente definidas. A liberdade de operação sobre o espaço e tempo, constitui a própria força. O espaço é ilimitado. Não existem frentes de combate nem retaguarda. O espaço não é ocupado, mas "contaminado", exigindo a presença do adversário. É uma guerra de movimento e não de poder de fogo.
g) assimetria de designação de alvos: haverá muita dificuldade no emprego de determinados tipos de armamento, por um lado, enquanto que, no outro, haverá ampla possibilidade de se empregar qualquer facilidade como arma;
h) preponderância para o combate estratégico: o combate se dá no plano estratégico-militar, mas o combate aos militantes se dá nos planos operacional e tático.

d) as alianças são as de conveniência momentânea; e
e) o aparecimento das ameaças difusas, num mundo que passa por um processo de globalização.

Pode-se entender que a utilização da informação pode afetar a habilidade de realização de Operações de Informação militares (OpInf[11]), onde se trabalha a natureza da informação: a forma de abstração da realidade e as dinâmicas que se desenvolvem entre os domínios resultantes dessa abstração. Esta abstração divide a realidade em três domínios[12] (domínio físico, domínio da informação e domínio cognitivo) é a base da habilidade apontada. Destaca-se que a informação possui domínio próprio diferenciado do domínio físico. Mas é somente no domínio cognitivo onde a vantagem informacional se desenvolve e se estabelece a vitória.

As dinâmicas específicas através das quais estes domínios interagem são descritas como primitivas (sensoriamento,[13] consciência,[14] decisões, observações - dados, compreensões,[15] ações, informação, compartilhamento, sincronização,[16] conhecimento e colaboração). Essas dinâmicas se traduzem em ações no domínio físico, originadas por decisões no domínio cognitivo, transmitidas ao domínio físico pela informação.[17] Forma-se, assim, um ciclo OODA, orientado à GI. Este modelo está representado nas Figura 2 e 3.

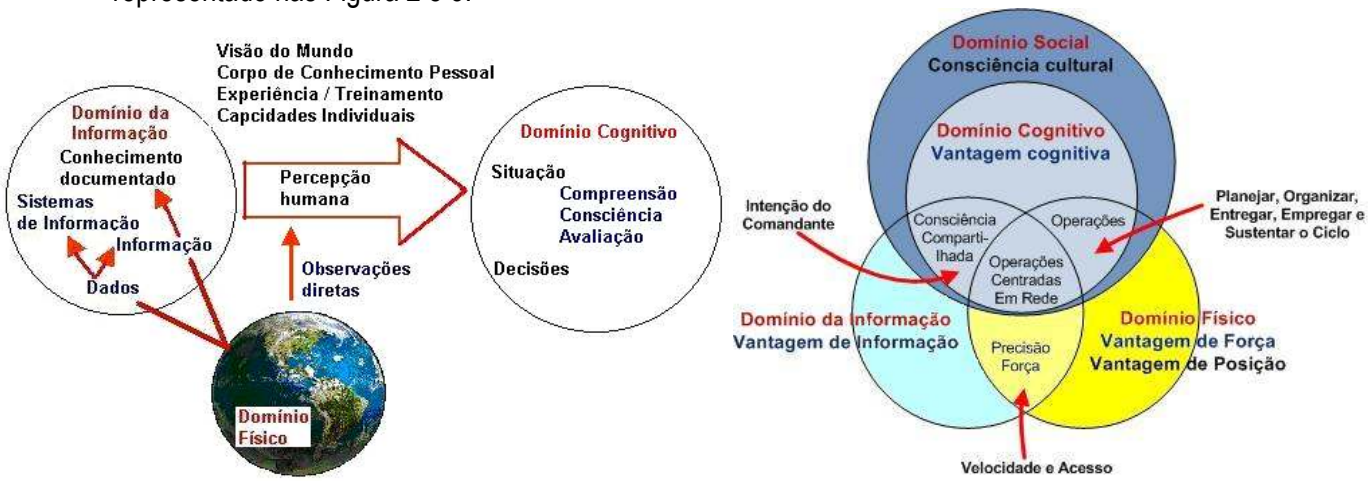


Figura 2. Modelo de abstração da GI. [8]

---

11 Envolvam ações executadas para afetar informação de adversário e sistemas de informação enquanto defendendo se é própria informação e sistemas de informação. Elas se aplicam através de todas as fases de uma operação, alcance de operações militares, e a cada nível de guerra. Elas são um fator crítico na capacidade de articulação do Comandante das Forças Combinadas para alcançar e sustentar o nível de superioridade de informação requerida para as operações combinadas decisivas.
OpInf agregam valor em sofisticação crescente, conectividade e confiança em tecnologia da informação. As OpInf tem como alvo informação ou sistemas de informação a fim de afetar o processo baseado em informação, seja humano ou automatizado. As OpInf podem incluir operações de GE, operações de GP, ataques físicos, ou operações especiais de ataque a redes (GC).

12 os estudiosos de GI adaptaram o modelo descrito na taxonomia de Bloom (que descreve a dinâmica do aprendizado), para descrever a dinâmicas envolvidas no processamento de dados, informação e conhecimento, necessárias à análise de domínio da GI.

13 Tradução proposta de "sensing".

14 Tradução proposta de "awareness".

15 Tradução proposta de "understanding".

16 Tradução proposta de "synchronization".

17 Daí a sua importância.

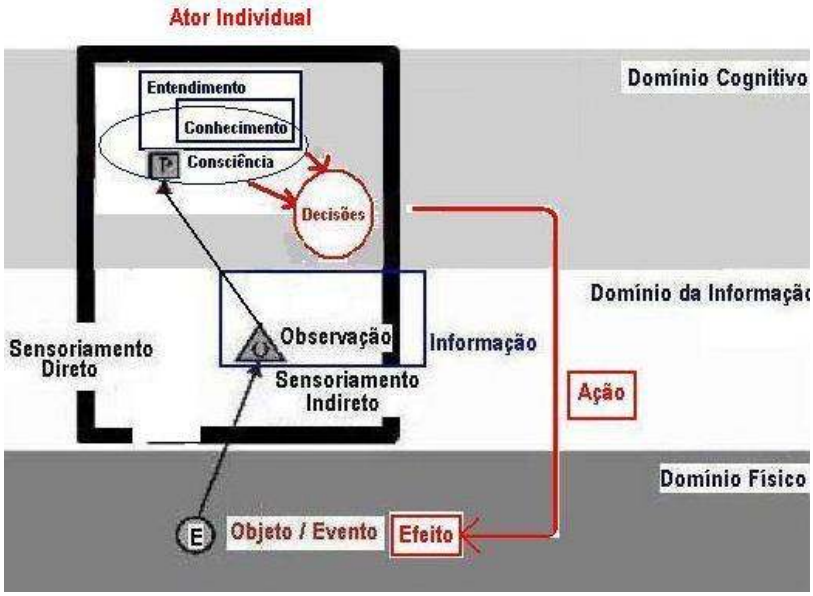


Figura 3. Relação entre domínios e ciclo OODA. [8]

Nota-se que:

a) o sensoriamento age sobre o domínio físico, mas pertence ao domínio da informação. Os sensores geram dados que, ao serem processados, se transformam em informação. Nesta dinâmica se inserem praticamente todas as atividades de GE;

b) a informatização do campo de batalha se inicia no sensoriamento e no processamento posterior. Também pode incluir a automação dos processos, análise de risco e outras atividades de suporte à tomada de decisão (informatização: movimento vertical ascendente);

c) a decisão é tomada a partir do estado de consciência sobre o campo de batalha, considerando conhecimento anterior adquirido. Esta dinâmica se desenvolve no domínio cognitivo;

d) a ação é modelada de modo a produzir o efeito desejado (Operações Baseadas em Efeito – OBE[18]) dentro do risco que se pretende assumir (devidamente quantificado). Se desenvolve a partir do domínio cognitivo, é virtualizada no domínio da informação e é realizada no domínio físico (virtualização: movimento vertical descendente); e

e) a SI é produzida no domínio da informação, onde a guerra é informatizada e virtualizada. A SI leva em consideração três dimensões que formam um cubo: Relevância, Acuracidade (ou acurácia) e Oportunismo. A SI das duas forças são comparadas desde o planejamento das ações e durante a execução dos combates até o término destes. A vitória é obtida pela SI alcançada. Portanto, em uma GA, as OpInfo têm por objetivo obter a SI, pela redução das assimetrias existentes no domínio da informação (que irão se refletir na redução de assimetrias no domínio cognitivo (melhor e mais rápido ciclo OODA) e conseqüentemente, no domínio físico (fracos enfrentando fortes) e. A Figura 4 ilustra este cubo.

[18] Formam um conjunto de ações coordenadas que possuem a finalidade de formatar o comportamento de inimigos, aliados ou neutros em períodos de paz, crise e guerra [12]. GCR é um modo de guerrear, enquanto OBE são ferramentas de implementação deste modo (especialmente, Guerra Nodal, que são ataques a nós críticos da rede de C^2 do inimigo). Utiliza as seguintes premissas: ações geram efeitos (resultados ou impactos criados, no ciclo de Boyd do adversário - entre Orientação e Decisão - pela aplicação de poder militar ou outro tipo de poder), não somente sobre o inimigo, mas sobre quem as observa; efeitos podem ocorrer simultaneamente nos diversos níveis de condução da guerra; efeitos não podem ser isolados, possuindo as características e serem correlacionados e cumulativos e que efeitos possuem uma natureza dual (física e psicológica) [13].
As OBE utilizam quatro ingredientes-chave da GCR, como garantia de sucesso: opções (habilidade de conectar capacidades separadas geograficamente), agilidade (a responsividade das forças conectadas em rede com consciência compartilhada e velocidade de comando provê a agilidade de adaptação às ações do adversário, permitindo a formatação respectiva e reorientação das próprias ações), coordenação (consciência situacional compartilhada e entendimento das intenções do comandante, acrescidos de sincronização de efeitos, permite coordenação de ações e efeitos complexos) e mobilização do conhecimento (mobilização de conhecimento e "expertise" para auxiliar a tomada de decisões em todos os níveis).

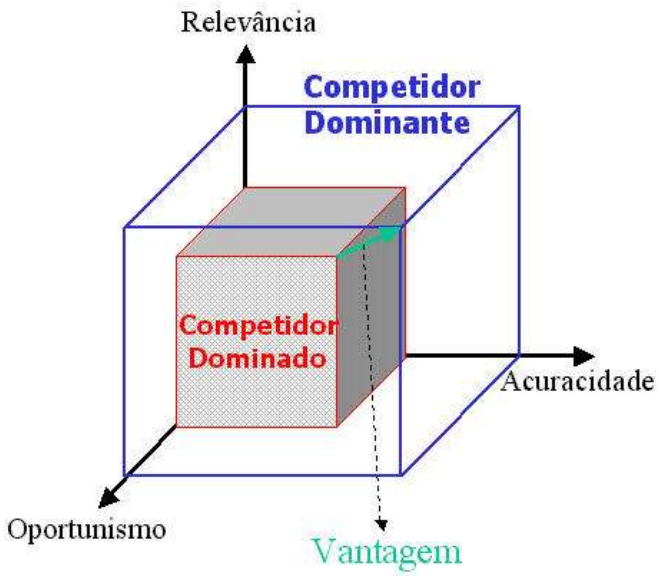


Figura 4. As dimensões da SI.

2.2 –Características da Guerra Cibernética:

Segundo Dutra [14] apud Parks e Duggan[19] e Cahill, Rozinov e Mulé[20] algumas características de guerra convencional (combate cinético) não possuem significado na GC, tornando-se necessário enumer novas características:

a) **efeito cinético** (a GC deve produzir efeitos no espaço cinético);

b) **dissimulação e visibilidade** (medidas ativas podem ser adotadas para se dissimular no espaço cibernético, mas qualquer coisa que se faça é visível);

c) **mutabilidade** (não existem leis de comportamento imutáveis no espaço cibernético, excetuando-se aquelas que necessitam de uma ação no mundo real);

d) **disfarce** (se alguma entidade no espaço cibernético possui a autoridade, acesso, ou habilidade necessários para por em prática qualquer ação que um atacante deseje realizar; o objetivo do atacante é assumir a identidade dessa entidade, de alguma forma);

e) **dualidade** (armamento utilizado tem emprego dual);

f) **compartimentação** (tanto o atacante, como o defensor de um sistema, controlam uma pequena parcela do espaço cibernético que utilizam);

g) **usurpação** (quem controlar a parte do espaço cibernético que o oponente utiliza, pode controlar o oponente);

h) **incerteza** (o espaço cibernético não é consistente, nem confiável); e

i) **proximidade** (limitações físicas de distância e espaço não se aplicam ao espaço cibernético).

Pode-se concluir, aos listar estas características, que [15]:

a) ataques cibernéticos são possíveis somente porque sistemas de informação possuem falhas: falhas em protocolos de rede, protocolos de comunicação, de sistema operacional e falhas adicionadas por pessoas (que utilizam, administram ou mantém estes sistemas);

b) GC operacional tem a sua importância (a ponto de não poder ser menosprezada), a ponto de ser considerada por alguns autores (mas não todos), como um multiplicador de força: ataques ocorrem porque vulnerabilidades foram exploradas. Predição de efeitos de ataques cibernéticos é impossível, assim como estabelecer a previsão de qualquer ataque. Também não inutilizam permanentemente equipamentos, nem

---

[19] PARKS, R. C., DUGGAN, D. P. **Principles of Cyberwarfare**. Proceedings of the IEEE Workshop on Information Assurance, West Point, NY, p 122 – 125, 2001. Trabalho apresentado no Seminário de Segurança da Informação da Academia Militar do Estados Unidos da América, 2001, West Point, NY.

[20] CAHILL, T. P.; ROZINOV, K.; MULÉ, C. **Cyber Warfare Peacekeeping**. Proceedings of the IEEE Workshop on Information Assurance, West Point, NY, p 100 – 107, 2003. Trabalho apresentado no Seminário de Segurança da Informação da Academia Militar do Estados Unidos da América, 2003, West Point, NY.

causam baixas. Apenas produzem efeitos temporários. Também podem não responder satisfatoriamente se for utilizada como apoio a uma operação cinética no mundo físico (apoio a um ataque aéreo, atacando-se uma estação de radar, por exemplo), pois pode não responder satisfatoriamente se desdobramentos se apresentarem durante a missão. No entanto, a característica de negação de uso (mesmo temporário) pode ser usada em qualquer caso e com precisão. Mas deve-se manter prudência em utilizar somente GC para apoiar operações cinéticas, por exemplo, pois não se pode garantir uma janela de negação de uso que pode ser necessária para se apoiar uma operação como esta;

c) GC estratégica não parece ser decisiva: não se pode prever, com precisão, a extensão da destruição que se causará com um ataque cibernético a nível estratégico. Também não se consegue avaliar, com precisão, os desdobramentos políticos que tal ataque causaria (é difícil elaborar a escalada de uma crise, somente se utilizando GC a nível estratégico). Em crises bilaterais é impossível impedir que uma terceira parte se envolva. Certamente não causaria o mesmo efeito de ataques aéreos, por exemplo, sobre uma sociedade. Quando um ataque é lançado (ou uma atividade de exploração utilizada na preparação para ataque é descoberta) vulnerabilidades são identificadas e corrigidas, impedindo a extensão do ataque ou a sua repetição. Portanto, a possibilidade de exercer coerção a nível estratégico cai a cada dia;

d) dissuação (coerção) cibernética estratégica nunca funcionará tão bem quanto a nuclear[21]. Além disso, pode-se incluir nesta discussão outros aspectos: a identificação da origem dos ataque não é uma tarefa fácil, nem precisa, não se consegue estabelecer a extensão dos danos causados por um ataque cibernético, para garantir que a coerção foi levada a cabo; os ataque não podem ser repetidos; hackers externos à crise não podem ser simplesmente afastados e controlados; a retaliação cibernética pode ser mal interpretada; é difícil estabelecer um limite preciso para se estabelecer uma resposta cibernética;

e) as respostas a ataques cibernéticas devem ponderar muitos fatores: a determinação do alvo do ataque sofrido (de difícil determinação); o que o alvo atingido revela sobre o atacante; a intensidade da resposta cibernética; se será utilizada resposta cinética e com que intensidade; se um Estado-nação deve responder a ataques "independentes" realizados por civis (hackers comuns – *rogue operators*); se a dissuação deve ser estendida aos aliados, em determinados casos; estabelecimento do limiar que permite a associação de um ataque cibernético a um ato de guerra[22]; determinar se ataques a alvos civis (estratégicos) que produzem efeitos colaterais (baixas entre civis) podem ser considerados crime de guerra e sujeitos a julgamento em tribunal internacional;

f) os efeitos de uma operação cinética tendem a saturar acima de um determinado custo, o que não acontece, geralmente, com ataques cibernéticos, o que fornece uma grande vantagem ao atacante; e

g) a avaliação dos ataques cibernéticos é específica e deve considerar três eixos: intensidade do ataque (se ataques mais intensos proporcionarão maior danos ou se há um limiar de saturação), duração dos ataques (quanto mais um ataque se alonga, mais ataques subseqüentes se tornam mais difíceis de realizar) e evolução temporal (em relação ao tempo, o número de vulnerabilidades deve decrescer, mas sistemas se tornam mais complexos, admitindo mais vulnerabilidades, embora sejam mais complexos de lidar).

Estas características moldam a atuação no espaço cibernético, dando-lhe conotações especiais (mundo virtual *versus* mundo físico), pois há atuações no domínio cognitivo e no domínio da informação, além de produzir efeitos no domínio físico. Como exemplos imediatos, pode-se citar impacto imediato sobre os princípios de guerra convencionais (objetivo, ofensiva, massa, economia de força, manobra, unidade de comando, segurança, surpresa)[23] e sobre iniciativas de utilização de GC como estratégia de dissuação em crises, principalmente.

2.3 – Taxonomia da GI:

Todas as características listadas permitem a apresentação do modelo proposto por Waltz [16]. Na

---

21 a dissuação cibernética produz efeitos que a situa acima daqueles provocados por meios econômicos e diplomáticos, mas abaixo da dissuação provocada por força física e, evidentemente, pela força nuclear, em termos de "níveis de beligerância"

22 geralmente, a varredura de redes, não é considerada um ato de guerra, quando se identifica que foi efetuada por uma organização militar de outro país. Mas é considerada crime (civil) em vários países.

23 os princípios da guerra variam de nação a nação. São adaptados às doutrinas militares nacionais. Por exemplo, os EUA definem "simplicidade", mas não definem como princípios de guerra: moral, mobilidade, mobilização política, liberdade de ação (China).

Figura 5, ilustra-se o modelo de informação na guerra. Nele está descrito um modelo unidirecional elementar de conflito, aplicado a dois atores. Um atacante A engaja um defensor B que deve determinar a reação adequada. O objetivo de A é influenciar e coagir B para que as ações deste sejam favoráveis ao objetivo de A (rendição, erro forçado, retirada de forças, fim de hostilidades, etc.). O atacante pode usar a força ou outro tipo de influência para atingir seu objetivo. Três fatores influenciam a decisão de B e as ações subseqüentes, como reação ao ataque de A:

a) ***a capacidade de B de agir***: a habilidade de B em responder é um fator físico, que pode ser medido em termo de capacidade para comandar e intensidade de força. Guerra de atrito se baseia na premissa de que a degradação da capacidade de luta de B forçará B a tomar decisões que o farão sucumbir à iniciativa de A. Capacidade é uma medida que depende de muitos componentes, incluindo os Centros de Gravidade (características estratégicas, capacidades militares, de onde a força deriva a sua liberdade de ação, intensidade física ou vontade de lutar);

b) ***a vontade[24] de B para lutar***: a vontade é um fator humano, uma medida da determinação do tomador de decisão de B e sua inclinação em relação às ações alternativas que percebe. Este é o elemento mais difícil para o atacante, para mensurar, modelar ou influenciar. A força de vontade para atingir um objetivo estabelecido ou propósito transcende critérios de decisão objetivos. A força de vontade de um tomador de decisão pode exercer pressão, não importando o nível de risco, reagindo até de maneira irracional (em termos militares);

c) ***a percepção de B***: a consciência da situação por parte da perspectiva de B é um fator de informação abstrata, medida em termos de precisão, completude, confiança, incerteza ou oportunismo. As decisões tomadas por B são determinadas pela percepção da situação (ataque de A sobre B) e pela percepção da própria capacidade para agir. Baseado nestas percepções e na percepção de ações alternativas disponíveis e suas conseqüências imaginadas e na sua força de vontade, B responde.

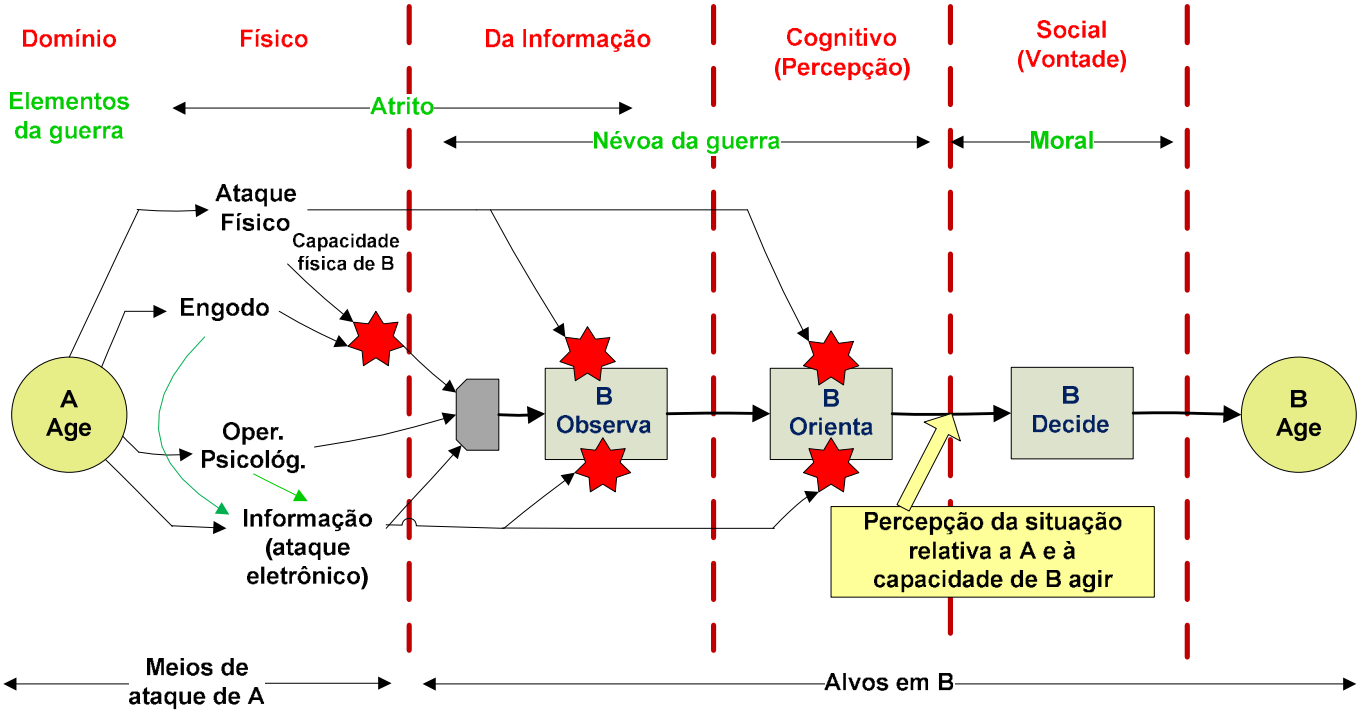


Figura 5. Modelo básico dos processos de informação em um conflito entre o atacante A e o defensor B. [16]

Para que A possa influenciar a decisão a ser tomada por B, pode atacar sua capacidade em reagir. Isto reduzirá as opções disponíveis para B, influenciando diretamente sua vontade. O atacante A pode, também, influenciar a percepção de B sobre a situação (atacando seus sensores e suas

[24] não vontade simples, mas também pode-se incluir o termo militar "moral".

comunicações – GE). Enquanto não puder atacar ou controlar diretamente sua vontade, os ataques à sua percepção ou à sua capacidade podem prover os meios para acessar a sua vontade, ou mesmo limitá-la[25].

O modelo descrito na Figura 5 ilustra os meios pelos quais, A pode influenciar a capacidade de B e o fluxo de informação que permite a B ter a consciência da situação sobre o conflito. O fluxo de informações que emana de A atravessa quatro domínios das decisões e ações de B (domínio físico, domínio da Informação, domínio Cognitivo - percepção e domínio Social – vontade/moral). O modelo permite explorar as alternativas que A tem para influenciar a consciência situacional de B. O modelo ilustra quatro opções disponíveis para A: ***ataque físico***; ***engodo***; ***ataque psicológico*** e ***ataque "informacional"***, dentro do ciclo OODA de B. A eficácia seria atingida ao se quebrar a vontade de lutar de B, sem que A tenha que lutar (Sun Tzu).

A GI estabelece um novo paradigma, pois não se conduz o conflito somente no domínio físico. Ele se desenvolve principalmente no domínio Cognitivo onde as informações são coletadas e reunidas (digitalização), onde as decisões são tomadas (incluindo aí a influência do domínio Social) e as ações (e suas alternativas) são implementadas (virtualização) para produzir efeitos no domínio Físico. Portanto a GI expande o conflito para além da realidade física, para uma região onde não há fronteiras físicas, onde não se pode distinguir o que militar do que é civil e onde se lida com "ativos intangíveis" que devem ser mensurados (para poderem ser controlados).

Quanto à formas de guerra de informação, podem ser citadas: guerra na rede (*netwar* – através do ativismo civil), guerra política (influência sobre decisões e políticas emanadas por lideranças governamentais), guerra econômica e guerra de comando e controle (GC).

Os componentes e objetivos da operações[26] na GI estão mostrados na Figura 6, que utiliza o conceito de OpInfo em um contexto de GC. Estas podem ser classificadas como:

a) **exploração de informação (direta ou indireta)**: operações de exploração de redes, bases de dados, acessos, direitos, vulnerabilidades, meios de transmissão, características de emissões eletromagnéticas (MAGE[27]), engenharia social, *phishing*, etc.;

b) **ataque e defesa da informação**: operações psicológicas, engodo, medidas de segurança de informações digitais, GE, destruição física, ataque à informação (*hacking*, viroses, etc.).

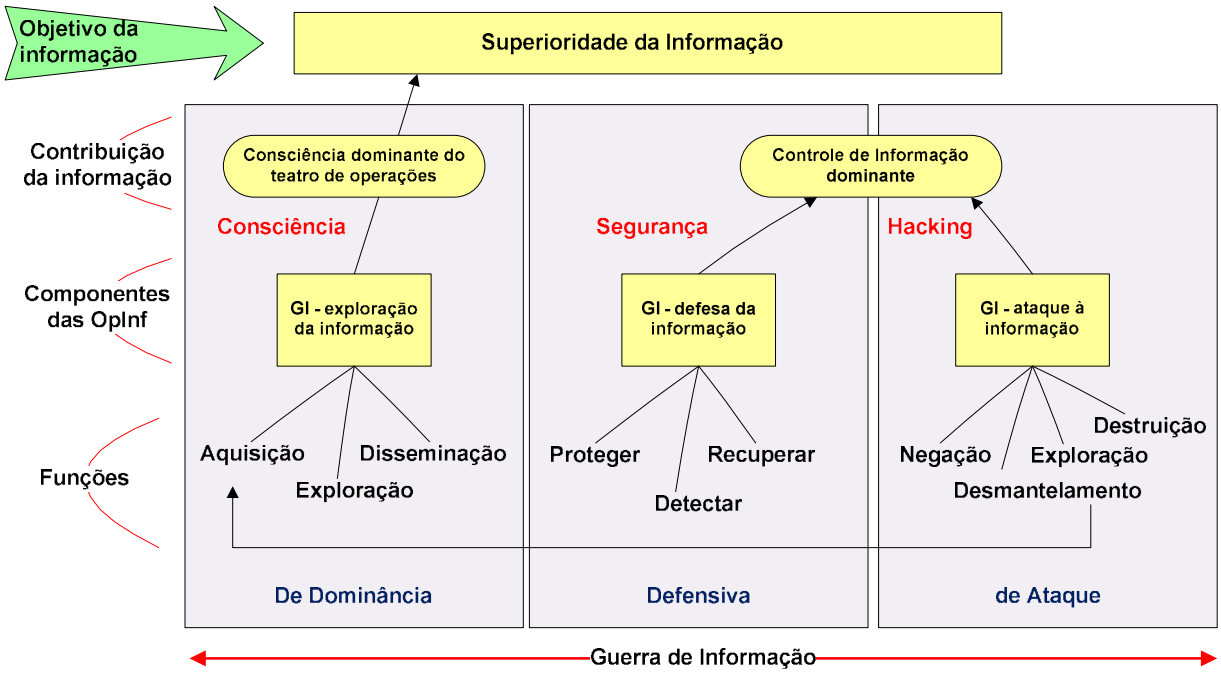


Figura 6. Os componentes e objetivos das operações na GI. [16]

[25] gerenciamento de percepção.
[26] incluindo funções das OpInf.
[27] Medidas de Apoio a GE.

Uma taxonomia funcional pode ser construída com base nos objetivos da GI, funções (táticas de contramedidas) e efeitos sobre alvos designados em infra-estruturas. A taxonomia está ilustrada na Figura 7 e é estruturada em três ramos que são as propriedades essenciais dos processos de segurança de uma infra-estrutura de informação e os objetivos associados (contramedidas).

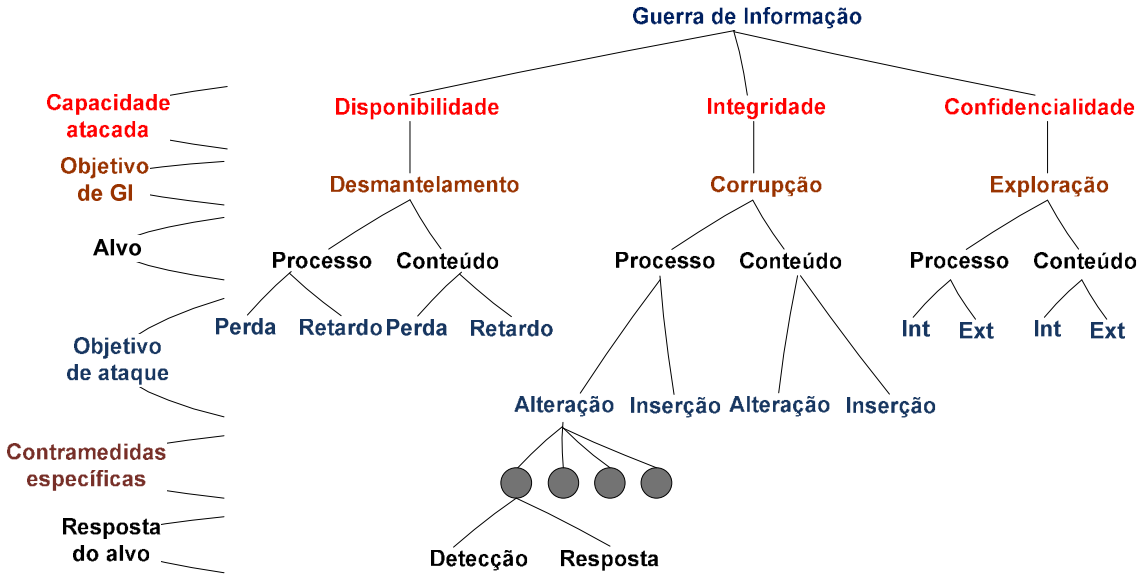


Figura 7. Taxonomia funcional da GI. [16]

2.4 – Aspectos organizacionais:

Em termos organizacionais (para que a gestão do conhecimento seja eficaz), é importante salientar como as organizações brasileiras / estrangeiras (envolvidas nas atividades de guerra) utilizam a informação (em termos de processos de colaboração, arquitetura e da estrutura de conhecimento montada). É preciso estratificar a maneira como a informação é tratada organizacionalmente. De forma mais específica, é preciso entender a dinâmica do aprendizado organizacional, a fim de determinar a habilidade de se obter vantagem cognitiva.

De acordo com o modelo de Boisot, o conhecimento é representado em três dimensões: difusão, abstração e codificação no Espaço-I, conforme ilustrado na Figura 8. [17] [18] [19] [20].

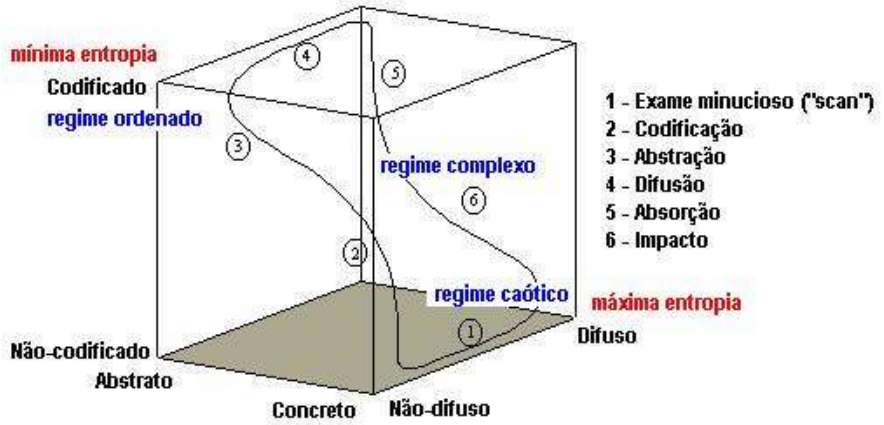


Figura 8. Ciclo de aprendizado social no Espaço-I.

No ciclo de aprendizado, há várias fases:

a) **exame minucioso**: identificação de ameaças e oportunidades em dados disponíveis, mas nebulosos (denominados "sinais fracos"). Exame de padrões desses dados numa visão única e idiossincrática em que eles se transformam pela posse de indivíduos ou pequenos grupos. Esse exame pode ser muito rápido, quando os dados são bem codificados e abstraídos, ou muito lento e aleatório, quando os dados não são codificados e são de contexto específico;

b) **solução de problemas**: processo de estruturação e coerência a tais visões (codificação). Nesta fase as

soluções são encontradas numa forma definida e após a eliminação da incerteza inicial. Essa fase tem início na região de não-codificação do Espaço-I e é freqüentemente associada a risco e conflito;
c) **abstração**: generalização da aplicação de visões recentemente classificadas em uma gama mais larga de situações. Isto envolve a redução às características mais essenciais, conceituando-as. Solução de problemas e abstração trabalham freqüentemente em conjunto;
d) **difusão**: compartilhamento de novas visões concebidas em uma população determinada. A difusão de dados bem codificados e abstraídos para uma população grande serão tecnicamente menos problemáticos do que compartilhamento de dados não-codificados e de contexto específico. Só o compartilhamento de contexto pelo transmissor e receptor pode acelerar a difusão de dados não codificados. A probabilidade de se obter um contexto compartilhado é inversamente proporcional ao tamanho da população;
e) **absorção**: aplicação das novas visões codificadas em uma forma "aprender fazendo" ou "aprender usando". Com o passar do tempo, tais visões codificadas adquirem uma "névoa" de conhecimento não codificado que ajuda a guiar sua aplicação em circunstâncias particulares;
f) **impacto**: inclusão de conhecimento abstrato em práticas concretas. Produz impacto em regras técnicas ou organizacionais, ou em práticas comportamentais. Absorção e impacto trabalham freqüentemente em conjunto.

O maior valor isolado de um item no Espaço-I é aquele que possui maior grau de codificação, abstração e mínima difusão (valor isolado).[28] O plano inferior da Figura 4 é formado por competências básicas (que dificilmente se difundem) e o plano superior, por sistemas modulares (que rapidamente se difundem). O vértice superior esquerdo é representado por regimes ordenados,[29] e o diagonalmente oposto, por regimes caóticos.[30] O volume intermediário é formado por regimes complexos.[31]

Deve-se acrescentar agora as características culturais das organizações ao tratarem a informação. Os diferentes tipos de instituição podem ser posicionadas no modelo de Boisot, em torno de quatro classificações básicas (burocráticas, feudais, de mercado e clãs), conforme demonstrado na Figura 9. O detalhamento das classificações propostas está mostrado na Tabela 2.

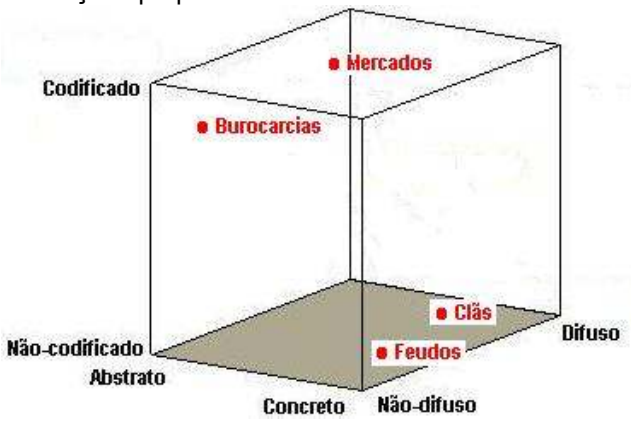


Figura 9. Instituições no Espaço-I.

[28] Mínima entropia.
[29] Ambiente informacional caracterizado por altos níveis de codificação, abstração e número de agentes pequeno em interação.
[30] Ambiente informacional caracterizado por pequenos níveis de codificação e abstração e um número grande de agentes em interação.
[31] Ambiente informacional caracterizado ou por altos níveis de codificação e abstração ou por um número pequeno de agentes em interação (ou exclusivo).

	informação não-difundida	informação difundida
informação estruturada	**Burocracias:** • Difusão limitada e sob controle central; • Reações impessoais e hierárquicas; • Submissão a objetivos superiores; • Coordenação hierárquica; • Sem necessidade de compartilhamento de valores e crenças.	**Mercados:** • Informação largamente difundida, sem controle; • Relações impessoais e competitivas; • Sem objetivos superiores - cada um por si; • Coordenação horizontal através de regulamentação; • Sem necessidade de compartilha-mento de valores e crenças.
informação não-estruturada	**Feudos:** • Difusão limitada pela falta de codificação nos relaciona-mentos; • Reações impessoais e hierárquicas (feudal / carismática); • Submissão a objetivos superiores; • Coordenação hierárquica; • Necessidade de compartilhamento de valores e crenças.	**Clãs:** • Informação difundida, mas limitada por falta de codificação nos relaciona-mentos; • Relações pessoais e não-hierárquicas; • Objetivos são compartilhados por processos de negociação; • Coordenação horizontal através de negociação; • Necessidade de compartilhamento de valores e crenças.

Tabela 2 - Características dos tipos de instituição

Portanto, pode-se concluir que a existência de codificação produz arranjos organizacionais importantes (hierárquicos ou burocráticos - verticais - e "achatadas" - horizontais). A ausência de codificação produz clãs e feudos.

O modelo proposto por Hofstede[32], enuncia os conceitos descritos na Tabela 3:

	alta redução de incerteza	baixa redução de incerteza
pequena distância ao poder	Fluxo de trabalho: burocrático	Estrutura não-burocrática implícitamente estruturada
grande distância ao poder	Burocracia completa	Burocracia pessoal

Tabela 3 - Modelo de Hofstede.

Integrando os dois modelos (Boisot e Hofstede), tem-se a Tabela 4:

		Hofstede	
		alta redução de incerteza	**baixa redução de incerteza**
Boisot	**informação codificada**	Força de trabalho: burocrática Modelo implícito: vertical **Modelo Boisot**: Burocracia	Estrutura não-burocrática implícitamente estruturada Modelo implícito: mercado **Modelo Boisot**: Mercado
	informação não-codificada	Burocracia completa Modelo implícito: pirâmide **Modelo Boisot**: Feudo	Burocracia pessoal Modelo implícito: família **Modelo Boisot**: clã
		informação altamente difundida	**informação pobremente difundida**
		Boisot	

Tabela 4 - Integração de modelos.

Acrescentando-se, a este entendimento, os conceitos propostos por Aston (Tabela 5), e, ainda, a suposição de que em uma organização "territorial" onde transações externas e internas ocorrem exigindo

[32] Geert Hofstede , um professor e consultor holandês, mostra uma abordagem para compreender valores diferentes de culturas diversas. Essa abordagem começou com uma pesquisa envolvendo dezesseis mil funcionários de uma corporação multinacional que funciona em mais de quarenta países, e desde então tem sido ampliada. Decompõe a cultura nacional em cinco dimensões: distância do poder, evitar a incerteza, individualismo-coletivismo, masculinidade-feminilidade e orientação curto-prazo longo-prazo.

postura adaptativa a essas situações, pode-se seguir o seguinte modelo (Tabela 6):

Dimensões de Aston	Dimensões associadas de Hofstede
Estruturação de atividades	Redução de incertezas
Concentração de autoridade	Distânca ao poder

Tabela 5 - Modelo de Aston.

	Interna à empresa	Externa à empresa
Interna à região	**Feudos:** • Sede corporativa • TI1	**Clãs:** • Serviços de suporte • TI2
Externa à região	**Burocracias:** • Filiais ou escritórios • TI3	**Mercados:** • Redes de fornecedores • TI4

Tabela 6 - Modelo adaptativo.

Destaca-se, nesta descrição, a utilização de uma aplicação de TI específica para cada caso.

No entanto, as forças da globalização e a diversidade da força de trabalho chamam cada vez mais a atenção para a possibilidade de influência da cultura sobre a tomada de decisão. Fons Trompenaars define cultura, especificamente, como "a forma pela qual um grupo de pessoas resolve problemas". Partindo-se desta premissa, é somente razoável esperar que assim como as culturas variam, o mesmo ocorre com as tendências e processos de tomada de decisão [21].

Do modelo de Hofstede, de diferenças de valores em culturas nacionais, as dimensões da distância ao poder e individualismo-coletivismo têm implicações especiais na tomada de decisão. Os funcionários de culturas com alta distância ao poder (por exemplo, as FFAA brasileiras, atualmente) podem esperar que seus supervisores tomem as decisões e que estejam menos inclinados do que os individualistas em termos de serem envolvidos nos processos de tomada de decisão. Entre os sinais de bons gerentes em culturas que destacam e respeitam diferenças de "status", pode-se enumerar a disposição de agir como especialistas na solução de problemas e a disposição de ser decisivo. Um gerente que parece desconfortável tomando decisões, sem o envolvimento e consenso do grupo, pode ser visto menos favoravelmente.

Os valores relativos ao individualismo-coletivismo também afetam as tendências culturais de participação na tomada de decisão. Nas culturas coletivistas, a tomada de decisão tende a ser muito orientada para o grupo e a ser executada com todo o empenho para se obter consenso. Isto resulta em mais tempo gasto para tomar a decisão, mas tipicamente uma implementação mais rápida e fácil. A compreensão e o comprometimento oriundos deste processo são muito vantajosos para a implementação. Por outro lado, a decisão nas culturas individualistas tem orientação mais decisiva de poupar tempo ao fazer uso de votação para solucionar desacordos. O resultado geralmente é uma decisão mais rápida e uma implementação mais lenta. Os problemas de implementação geralmente envolvem atrasos causados por mal-entendidos e falta de comprometimento. Por exemplo, no Japão coletivista, muitas empresas usam o sistema "ringi" - uma abordagem de decisão em grupo, na qual os funcionários indicam aprovação escrita de propostas antes de sua implementação. Na França, mais individualista, é comum as decisões serem tomadas no nível mais alto da corporação e serem passadas aos outros níveis hierárquicos inferiores para serem implementadas.

A cultura também pode influenciar a determinação da decisão ser ou não ser necessária, isto é, pode influenciar nas opiniões das pessoas quanto à necessidade de mudança ou não de uma situação existente. Os norte-americanos tendem a perceber as situações como problemas a serem resolvidos e querem fazer algo a respeito. Outras culturas, como a tailandesa e a indonésia, estão mais propensas a aceitar as situações como são. Para fazer planos, um tomador de decisão precisa poder visualizar o futuro, acreditar que pode influenciá-lo e achar que é conveniente fazê-lo. As diferenças culturais de atitudes em relação ao tempo vão financiar as decisões de planejamento. O estereótipo do "sonho americano" e a pressa em direção ao futuro, por exemplo, podem ser um contraste forte com a tendência

dos franceses de respeitar e valorizar o passado. O grau de detalhe do planejamento, assim como o esquema de tempo das decisões e planos, podem ser afetados por essas diferenças culturais, como a orientação no tempo.

No entanto, as instituições que utilizam TI, a decisão é liberada do confinamento das reuniões face a face. As pessoas que trabalham nesses ambientes tendem a estar mais focadas em tarefas e a evitar os conflitos interpessoais e outros problemas comuns nas deliberações face a face. Mas, há o risco das decisões se tornarem mais impessoais e talvez menos motivadoras em termos de comprometimento com a implementação e o acompanhamento.

Portanto, pode-se concluir que, numa organização, as decisões são tomadas recebendo-se a influência da cultura organizacional, enquanto que os dados são interpretados segundo influência da cultura individual. A Tabela 7 ilustra esta conclusão:

		Hofstede	
		alta redução de incerteza	**baixa redução de incerteza**
Hofstede	pequena distância ao poder	alemães, finlandeses e israelenses **Burocracias**	ingleses, escandinavos e holandeses **Mercado**
	grande distância ao poder	latinos, países mediterrânicos e islâmicos, japoneses **Feudos**	Hong-Kong e Singapura **Clã**

Tabela 7. Influência da cultura organizacional.

Outro aspecto importante a ser analisado é a rejeição à informação. Um modelo alternativo ao proposto por Hofstede e Boisot é o modelo proposto por Thompson e Wildavsky. Eles reconhecem a mitologia da era, que se atravessa uma "era da informação", numa "sociedade da informação". No entanto, eles notam paradoxalmente que o comportamento mais significante das pessoas em relação à informação é a rejeição. Eles descrevem quatro tipos de rejeição (mutuamente exclusivos) associados com quatro estratégias de formação de organizações. Essa descrição está apresentada nas Tabelas 8, 9 e 10.

Tipo de rejeição	Exemplo	Caracterização
Absorção de risco	"O que você não sabe não vai machucar você".[33]	Fatalismo, aceitação de um mundo no qual a vida é uma loteria.
Rede pessoal de relaciona-mentos informais[34]	"Quando eu tenho vontade de ler um livro eu escrevo um".[35]	Há tantos dados que são todos rejeitados em prol de uma rede pessoal de relacionamentos informais.
Proteção de paradigma	"Estas teorias absurdas do Prof. Ohm ..."[36]	Uma hierarquia poderosa cuja estrutura é ameaçada fecha seus postos elevados para rejeitar informação que questiona sua fundação.
Expulsão	"Se foi bom bastante para Moisés é bom bastante para mim".[37]	Não hierárquico; um grupo do tipo seita fecha seus postos elevados para proteger seus filiados vulneráveis, dos estranhos predatórios.

Tabela 8 - Exemplos de rejeição à informação.

[33] Ditado popular.
[34] Tradução proposta de "Networking".
[35] Benjamin Disraeli, sobrecarregado por dados.
[36] A reação de estabelecimentos científicos por ocasião da primeira tentativa para publicar a Lei de Ohm.
[37] Extrato de canção popular cristã fundamentalista americana que rejeita o princípio evolucionista de Darwin".

Tipo de rejeição à informação	Cultura	Categoria Hofstede
Absorção de risco	Fatalismo (clã)	Baixa capacidade de evitar incertezas
Rede pessoal de relaciona-mentos informais	Mercados	Baixa masculinidade
Proteção de paradigma	Hierarquias	Baixa individualidade
Expulsão	Seitas	Baixa distância ao poder

Tabela 9 - Exemplos de rejeição à informação em função da cultura.

Tipo de rejeição à informação	Países correspondentes	Países opostos
Absorção de risco	Singapura, Hong Kong	Grécia, Portugal
Rede pessoal de relaciona-mentos informais	Suécia, Dinamarca	Japão
Proteção de paradigma	Paquistão, Taiwan	EUA, Austrália
Expulsão	Israel, Áustria	Filipinas, México

Tabela 10 - Exemplos de países em relação a rejeição à informação.

Portanto, pode-se concluir que, mesmo vivendo a "era da informação", numa "sociedade da informação", não se encontrará facilidades de implementação de qualquer idéia que vise a melhorar a estrutura organizacional de uma instituição, mesmo que esta nova estrutura seja orientada a informação e mesmo que valores culturais estimulem o processo de mudança.

Também se percebe que o caminho a percorrer para a implementação de uma RAM[38], é bem específico para cada cultura, para cada indivíduo, onde o tratamento e a rejeição à informação têm um resultado determinante. Portanto não basta implementar uma RAM baseada em TI. É preciso estabelecer uma estratégia de implementação adequada às FFAA em questão. Mesmo assim, não se garante que a implementação será um sucesso ou se obterá, sempre a SI em um conflito, após esta implementação.

Conclui-se que a estrutura e dinâmica organizacionais podem favorecer ou não a eficácia da utilização da GI. Portanto, não é qualquer organização que poderá tirar proveito do uso adequado de GI. Ou seja, a organização das FFAA devem se adaptar para que possam se tronar vitoriosos nas guerras travadas no século XXI.

3 – Análise de Conjuntura

Neste item será analisada a conjuntura onde está inserida a República Popular da China (2ª economia do plante, mas um terço da economia americana), para que se possam construir cenários prováveis de conflito, onde a GI e a GC obterão papéis relevantes.

3.1 – Ambiente Macro-econômico:

- **dados coletados:**

	2007	2008	2009	2010
população	1,31 bilhões	1,32 bilhões	1,33 bilhões	?
PIB China (US$)	0,974 trilhões	1,2 trilhões	3,7 trilhões	5,9 trilhões
Crescimento PIB (%)	13	9	6,1	10,3
PIB EUA (US$)	14,7 trilhões	14,3 trilhões	13,8 trilhões	14 trilhões
inflação	1,50%	4,80%	5,90%	-0,70%[39]

Tabela 11. Dados gerais.

[38] Revolução em Assuntos Militares.

[39] estimada em 5% para 2011.

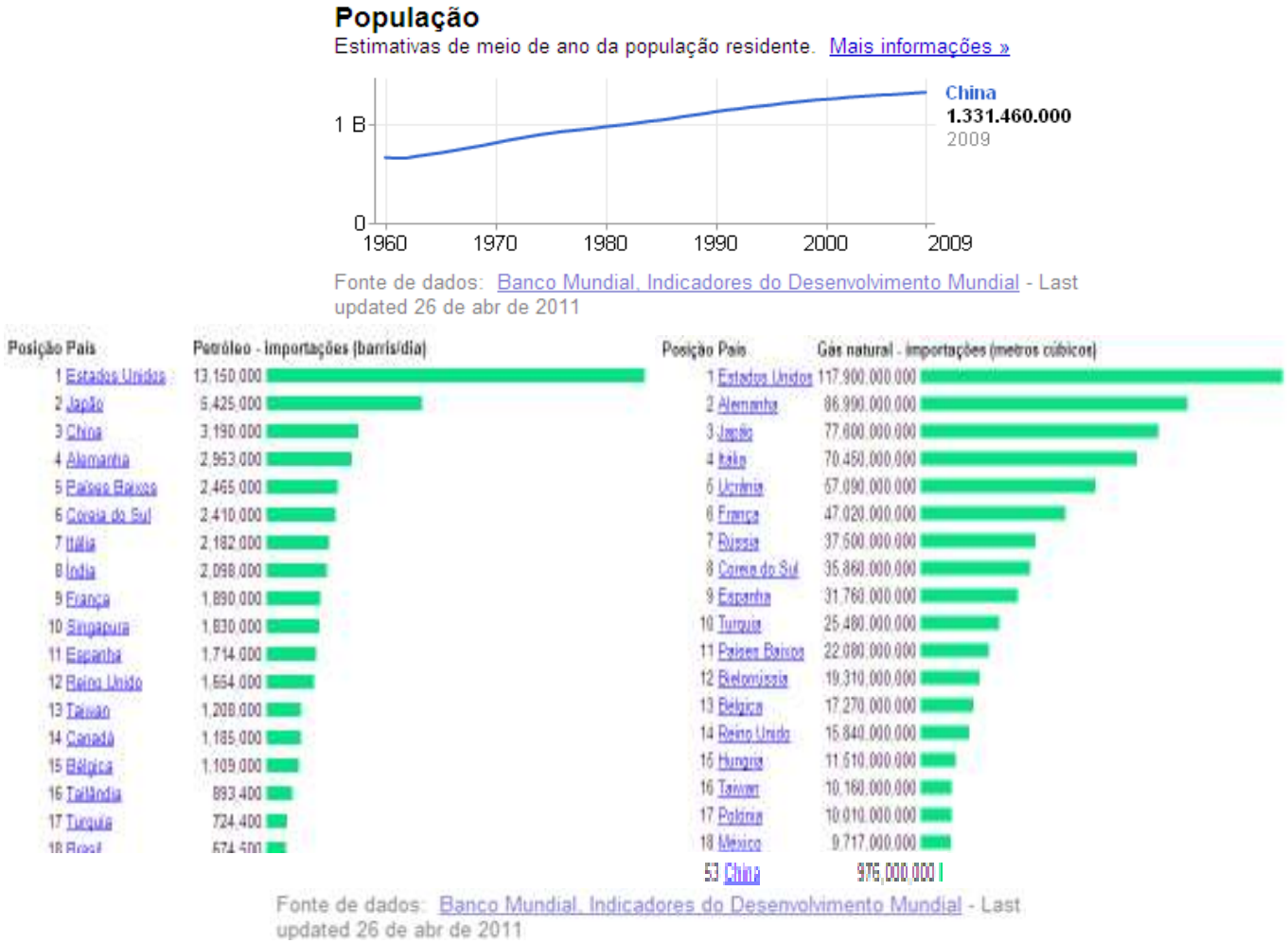
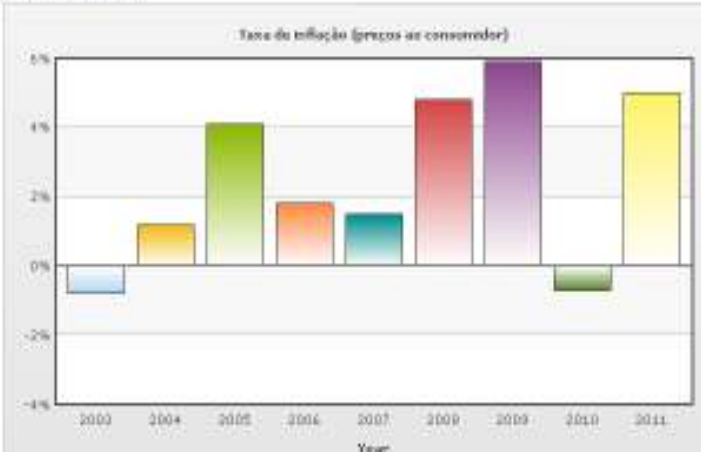


Figura 10. Dados gerais.

Produção de gás natural[40]: 82,94 bilhões de m^3 (2009) – 9º país produtor mundial;
Consumo de gás natural[41]: 87,08 bilhões de m^3 (2009) – 9º país consumidor mundial;

Taxa de inflação (preços ao consumidor): 5% (2010 est.)
-0,7% (2009 est.)



Ano	Taxa de inflação (preços ao consumidor)	Posição	Mudança Porcentual	Data da Informação
2003	-,80 %	214		2002 est.
2004	1,20 %	183	-250,00%	2003 est.
2005	4,10 %	132	241,67%	2004 est.
2006	1,80 %	42	-56,10%	2005 est.
2007	1,50 %	28	-16,67%	2006 est.
2008	4,80 %	118	220,00%	2007 est.
2009	5,90 %	96	22,92%	2008 est.
2010	-,70 %	14	-111,86%	2009 est.
2011	5,00 %	140	-814,29%	2010 est.

Fonte: CIA World Factbook - A menos que indicado de outra maneira, toda a informação en esta página es correta até Março 11, 2011

Tabela 12. Inflação.

[40] CIA World Factbook.
[41] ibid.

- **Reservas estrangeiras e desvalorização do iuane:**

O momento-chave da escalada chinesa [22] deu-se em março de 2009, quando o primeiro-ministro Wen Jiabao bateu na sagrada solidez do dólar. "Emprestamos uma enorme quantidade de recursos aos EUA. E é claro que estamos apreensivos com a segurança dos nossos ativos. Para falar francamente, estamos um pouco preocupados". Obrigou os EUA a responder, reafirmando algo que até ali ninguém pusera em dúvida: a capacidade de os EUA honrarem os títulos que emitem. Foi uma espécie de jogo de cena dos chineses, que detêm 1,4 trilhão de dólares em bônus emitidos pelo Tesouro americano, dos 2 trilhões que possuem em reservas estrangeiras (só no ano passado compraram mais 400 bilhões de dólares em T-Bonds). Boa parte desse patrimônio amealhada a partir de 2007. Exatamente por ser a maior detentora desses títulos é que não interessaria à China pôr publicamente em dúvida a solidez desses ativos. Mas não deixou passar a oportunidade para fragilizar os EUA diante do mundo, obrigando-os – suprema ironia – a reafirmar a segurança dos seus títulos como se fossem um desses países caloteiros. Este acúmulo de reservas de deve, de certo modo, a um iuane desvalorizado: como o câmbio não é flutuante, sua moeda mexeu-se relativamente pouco nos últimos anos, apesar do volume monstruoso de ingresso de capital estrangeiro no país e do azul radiante de sua balança comercial. Nos últimos meses, as autoridades chinesas passaram a reagir de forma cada vez mais irritada quando os EUA repetem a velha reclamação de que o país manipula o iuane

- **Buscas por matéria prima no exterior:**

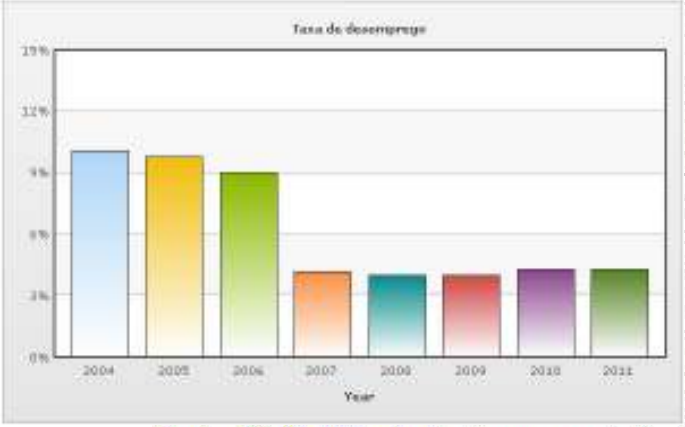
Para além da disputa direta com os Estados Unidos [22], a China tem estendido a mão aos seus vizinhos asiáticos e aos países africanos e latino-americanos. No Congo, em Angola, na Nigéria e em vários outros países africanos, a China opera basicamente com acordos de permuta: banca e faz obras de engenharia pesada (estradas, barragens) em troca de concessões de exploração de jazidas minerais. A Sinopec, estatal de petróleo, fechou um acordo com a Petrobras para financiar 10 bilhões de dólares em troca de fornecimento de petróleo. Tem estreitado também relações com Hugo Chávez, de olho no petróleo venezuelano, e com os russos, com quem a empresa firmou um compromisso de abastecimento de petróleo para as próximas duas décadas no valor de 25 bilhões de dólares.

- **Investimentos no exterior:**

A curva de crescimento de investimentos da China no exterior [22] não para de apontar para o alto. Em 2008, foram 52 bilhões de dólares em aquisições. Menos que os 186 bilhões de dólares dos EUA e os 74 bilhões de dólares do Japão. Mas 63% a mais do que no ano anterior. A previsão para 2009 era chegar aos 100 bilhões de dólares (mas só atingiu U$56.5 bilhões em investimento direto, mas posicionou a China no 5º lugar mundial e no 1º lugar entre os países em desenvolvimento). A China quer comprar o que puder na baixa – e não há por que não fazê-lo. Tudo o que for matéria-prima, recursos minerais e fonte de energia interessa ao país: a China é o maior consumidor mundial de cobre, zinco, alumínio e aço; o segundo maior de petróleo. Para que se tenha uma idéia do tamanho do mega-consumo chinês, o Brasil consome 24 milhões de toneladas por ano de aço; a China, quase vinte vezes mais: 450 milhões de toneladas por ano.

- **Combate à pobreza e desemprego:**

A China tem 900 milhões de pobres ainda à espera para entrar no fabuloso trem de prosperidade que tirou quase 400 milhões de pessoas da miséria [22]. A China convive ainda com a humilhação de ter 116 milhões de analfabetos, um número que vem crescendo, aliás. E esses são problemas que nem os EUA (donos de uma economia ainda o triplo da chinesa) nem a Europa nem o Japão têm. O próprio governo chinês diz que abaixo de 8% não conseguirá produzir empregos para os 15 milhões de chineses que deixam o campo todos os anos e para os 7 milhões de jovens que se graduam nas universidades, anualmente. Segundo o economista americano Nouriel Roubini [22], o número de desempregados foi de 40 milhões em 2008. A taxa de desemprego para áreas urbanas está mostrada na Tabela 13. Incluindo migrantes (das áreas rurais) pode atingir cerca de 9%. Há substancial desemprego e subemprego nas áreas rurais.



Ano	Taxa de desemprego	Posição	Mudança Percentual	Data da Informação
2004	10,10 %	93		2003 est.
2005	9,80 %	88	-2,97%	2004 est.
2006	9,00 %	92	-8,16%	2005 est.
2007	4,20 %	50	-53,33%	2005
2008	4,00 %	49	-4,76%	2007 est.
2009	4,00 %	45	0,00%	2008 est.
2010	4,30 %	39	7,50%	September 2009 est.
2011	4,30 %	40	0,00%	September 2009 est.

Fonte: CIA World Factbook - A menos que indicado de outra maneira, toda a informação en esta página es correta até Março 11, 2011

Tabela 13. Desemprego.

- **População urbana x população rural:**

Razão entre população urbana e rural:

a) Urbana: 42,3% (2007) - 562 milhões; 45,7% (2008) – 607 milhões; 46,6% (2009) – 609 milhões;
b) Rural: 57,7% (2007) - 767 milhões; 54,3% (2008) – 710 milhões; 53,4% (2009) - 720 milhões.

A renda dos camponeses cresceu 8% ante 8,4% do aumento de ganhos daqueles que trabalham nas zonas urbanas [22]. Na China, a remuneração média de um empregado nas cidades é quase o quádruplo dos 50 dólares mensais ganhos pelos camponeses.

- **Superprodução:**

Alguns perigos espreitam a economia chinesa [23]. Um deles é a superprodução, que pode ser o corolário de um erro de cálculo nos investimentos para a reativação da economia. Em 2009, o total de capacidade de produção da China excede a capacidade de consumo em 10% do PIB. Em 2008, isso nunca foi problema: o excedente era disputado pelos EUA, pela Europa e pelo Japão. Agora, a partir da última crise global, não mais. O que aconteceu nas siderúrgicas chinesas, que aumentaram a produção em fevereiro de 2009, é um exemplo desse risco. Pelo ritmo daquele mês, a China fabricaria 517 milhões de toneladas em 2009. Em 2008, o maior fabricante de aço do mundo produziu 500 milhões de toneladas. Sobrou aço. O preço caiu. Sob esse ponto de vista, não são só os EUA que precisam de ajustes – a China também. Se os EUA tiveram crédito abundante para torrar em consumo, os chineses tiveram crédito farto para produzir. Se continuasse a oferta de crédito, haveria superprodução. "Essa é uma preocupação do governo", admite o diretor adjunto do Ministério do Comércio, Shen Danyang.

- **Inflação:**

A primeira conseqüência da superprodução em alguns setores é a queda de preços [23]. Ela compensa o aumento da cotação do barril de petróleo, para as outras economias. Para cada US$ 1 de poder de compra perdido com o aumento da gasolina, US$ 1,50 voltou para os consumidores americanos na forma de produtos chineses mais baratos e competitivos [24]. Não pode fazer qualquer coisa para exportar mais, pois tal atitude levantaria a bandeira do protecionismo do resto do mundo. Segundo o americano Michael Pettis[42], professor de finanças da Universidade de Pequim "O protecionismo seria desastroso para a China, pois forçaria o país a absorver toda essa produção internamente." É uma substituição que, apesar dos esforços do governo, é impossível de ser feita a médio prazo [23]. No entanto, se estimula o consumo interno - os chineses ficaram mais ricos (apesar da alta da inflação), pois a taxa de poupança só aumenta: era de 37% do PIB em 1998 e em 2007 subiu para 59% (a dos EUA é de apenas 14% do PIB), a mais elevada de todos os tempos em qualquer economia. Há um fator cultural (o confucionismo não estimula a extravagância consumista) e um estrutural (não há assistência médica gratuita, nem aposentadoria garantida do estado).

[42] Apud Jardim [20].

O salto inflacionário chinês deve-se, sobretudo, ao maior consumo de alimentos, cujos preços acumulam um aumento de 18% em 2008 (a carne ficou 50% mais cara) [24]. É o tipo de efeito que ocorre quando uma nação com 1,3 bilhões de pessoas se urbaniza, passa a freqüentar restaurantes (como o da foto acima, decorado sob a inspiração da tenebrosa revolução cultural maoísta) e comprar comidas mais caras. Outra inevitabilidade da riqueza chinesa é que os salários, até recentemente irrisórios nas comparações internacionais, também estão em trajetória de alta. A nova geração de trabalhadores não se submete à baixa remuneração que era a norma desde que a China se abriu ao mundo, há duas décadas [24]. Até recentemente, um salário entre 105 a 145 dólares era considerado razoável para um operário. Hoje, um trabalhador com experiência exige pelo menos 200 dólares ao mês (o equivalente ao salário mínimo brasileiro). Tudo isso contribuiu para despertar a dinâmica inflacionária na China, imediatamente embutida no preço dos produtos exportados pelo país.

3.2 – Indústria de TI: [25]

O setor de TI da China é devia ser visualizado como uma indústria de civil com vínculos com a indústria de defesa chinesa e o PLA. Certas empresas de TI fornecem equipamentos terminados de comando, controle, comunicações, computadores, e inteligência (C4I) e produtos relacionados para o PLA, contribuindo para uma modernização importante da infra-estrutura de C4I do exército da China. Enquanto sistemas de defesa/industriais da China sofrem há muito tempo com um conjunto de problemas de grande abrangência e com problemas estruturais que impediram desenvolvimento de equipamento militar moderno, o setor de TI comercial não suporta este fardo. A indústria é marcada por novas instalações em lugares dinâmicos, uma mão-de-obra de alta tecnologia, e infusões de tecnologia estrangeira. Não tem que se preocupar em manter a rede de proteção social para milhares de trabalhadores desempregados e suas famílias em áreas rurais, mas ao invés atrai pessoal usando incentivos baseados em mercado, incluindo opções de ações, e os demite quando necessário.

Usando a canção de sereia do mercado chinês como uma isca para adquirir tecnologia de ponta de estrangeira, as empresas de TI da China, institutos de Pesquisa e Desenvolvimento e fundos estatais de Pesquisa e Desenvolvimento formaram um "triângulo digital" potente que combina os recursos significativos do estado com o dinamismo do setor comercial orientado ao mercado. O triângulo digital é facilitado por uma combinação de uma estratégia de desenvolvimento nacional focada em tecnologia, coordenação burocrática de alto nível, e incentivos fiscais significantes oriundos de planos nacionais de 5 anos de duração e programas orçamentários de ciência e tecnologia como recente Programa 863. Por causa da rápida obsolescência da tecnologia, o setor de TI está orientado para explorar estas tendências comercializando porções base estatal de Pesquisa e Desenvolvimento com benefício da economia de civil e das aquisições militar. Este modo "civil" de pesquisa envolvendo tecnologias militares é a real mudança de paradigma no coração do triângulo digital: introduzindo motivações comerciais e orientadas ao lucro e aumento da eficiência aperfeiçoam o nível tecnológico global da China e assim beneficiam a capacidade militar em TI.

A eficiência do triângulo digital em obter inovações de ruptura pode ser vista em quatro áreas: equipamentos de telecomunicações, supercomputadores, roteadores e ótica de fibra. As empresas estrangeiras ajudaram os esforços do triângulo digital infundindo tecnologia, equipamento, capital, e "expertise" nas empresas comerciais importantes ligadas ao sistema, principalmente em uma tentativa em obter acesso seguro ao mercado chinês, porque a natureza de regulação e do ambiente comercial na China colocam pressão enorme nas empresas estrangeiras para transferir tecnologia. As transferências de tecnologia estrangeira fizeram os ministérios e empresas menos dependentes em moeda estrangeira e de tecnologia com o passar do tempo. Esta dinâmica é o que os chineses se referem como o “novo modelo” ou caminho para o desenvolvimento da China: cooperação, aprendizado, desenvolvimento independente, substituição, inovação produzida no país e, principalmente, competitividade global.

A experiência de aquisição de equipamentos militares de TI a partir de empresas chinesas mostrou ao Departamento de Armamento Geral uma grande oportunidade de negócio em relação a contratos, competição e licitações, e incentivou oficiais de obtenção a aplicar lições aprendidas neste setor aos setores tradicionais da indústria de defesa. Os oficiais chineses também são rápidos para apontar os

limites ou restrições de transferência por atacado destas lições para os setores de defesa mais tradicionais, levando em conta as características e vantagens sem iguais do setor de TI, que são a base da manutenção da estabilidade social à custa de eficiência econômica.

Para o PLA, o triângulo digital abriu uma janela de acesso a tecnologias de informação avançadas, abastecendo uma revolução de C4I nas forças armadas. Como resultado, o PLA tem reportado melhorias significantes alcançadas em suas comunicações e segurança operacionais, como também na sua capacidade para transmitir informação, mas não está claro se avanço crescente em tecnologia da informação no exército somente melhorará a manipulação de informação, ou terá uma função muito maior nos próprios meios do PLA, no que se refere à sua modernização, transformando forças convencionais que se apresentavam como primitivas, muito menos informatizadas que uma força moderna.

O emergente setor de TI, embora não faça parte, oficialmente, do complexo industrial de defesa, é o setor mais inovador organizacionalmente e o mais dinâmico economicamente entre os fabricantes de equipamentos militares chineses. Enquanto a indústria é orientada principalmente para o mercado, chinês, o PLA tem sido capaz de balancear a capacidade de produção industrial para facilitar melhorias na capacidade militar de C4I. O setor de TI continuará a seguir os padrões mundiais em equipamentos de telecomunicações, supercomputadores, roteadores e outras tecnologias. Os militares chineses terão acesso a estas tecnologias para aplicações críticas de C4I.

3.3 – Percepção de ameaças: [26]

A percepção de ameaças por parte do exército chinês e pelo governo[43] e o desejo de usar a capacidade militar para influenciar as relações políticas regionais terão grande efeito decisório sobre os gastos militares. Estas percepções fornecem indicadores para o estabelecimento de prioridades para os gastos militares, de acordo com o governo chinês. Estas percepções também norteiam o planejamento e a modernização da força. Assim, podem-se identificar os aspectos prioritários da obtenção de material militar, pois se apresentam diretamente relacionados às suas necessidades de defesa.

Há três condicionantes para o pensamento estratégico chinês: ***unidade nacional, estabilidade e soberania***. A percepção de ameaças e o planejamento estratégico são orientados a manter estes três condicionantes. Estes condicionantes englobam salvaguardas à soberania do estado, unidade, integridade territorial e segurança, apoio ao desenvolvimento econômico como tarefa principal e incessante para realçar a força nacional, adesão ao sistema socialista e seu aperfeiçoamento, manutenção e promoção da estabilidade e harmonia nacionais, esforço para a obtenção e manutenção de um ambiente internacional de paz duradoura e de um clima regional favorável à China.

As mais importantes ameaças percebidas são:

a) ***política externa americana e sua política de emprego de forças militares*** (especialmente as relacionadas a Taiwan): é a ameaça considerada mais importante. Esta ameaça tem por base o relacionamento dos EUA com seus aliados e aspectos relacionados à defesa na Ásia, além da estratégia de segurança nacional americana. Desde o final da década de 90 do século passado, as atividades do exército chinês em relação as atividades de reforma, modernização, aquisição e treinamento têm sido pesadas e orientadas à preparação do conflito com Taiwan, incluindo o desenvolvimento de "capacidades assimétricas"[44] (a fim de dissuadir ou degradar a capacidade militar superior americana em impossível conflito). O temor tem como cerne a idéia de que os EUA procuram afastar Taiwan da integração com a China como um ponto estratégico na Ásia, a fim de conter o crescimento da influência chinesa na região (militar e econômica)[45]. Os estrategistas chineses percebem a venda de armas a Taiwan e interações militares bilaterais, como parte de um esforço de manutenção da China dividida permanentemente, impactando sobre os objetivos chineses de unidade e soberania;

---

43 não possuem pontos de vista exatamente iguais, visto que os líderes políticos não possuem experiência militar expressiva e vêem o exército como uma entre muitas organizações constituintes da burocracia chinesa. As diferenças residem no escopo e na intensidade das ameaças percebidas.

44 Incluindo Guerra Cibernética.

45 que, segundo os estrategistas chineses fica claro pela intensificação das alianças, ajuda militar e relações de cooperação em defesa anti-míssil, com os EUA, na região.

b) ***emergência do Japão como potência militar regional***: os chineses vêem mudanças na doutrina militar japonesa, na estrutura de força e desenvolvimento militar nos últimos anos como uma evidência do esforço japonês em aumentar sua capacidade militar e assumir um papel mais influente na Ásia. Pode-se perceber um sentimento anti-japonês em todos os níveis do exército chinês. A aliança EUA-Japão é vista pelos estrategistas chineses como a parte central da estratégia de limitação da influência da China na Ásia;
c) ***crescimento do poder militar da Índia e sua influência regional***: A Índia é uma preocupação relativamente nova para a China. China e Índia já travaram uma guerra de fronteiras em 1962 e posiciona, desde então, grande quantidade de tropas na fronteira com a Índia, para evitar a recuperação de territórios perdidos pela Índia. Mas, por muitas décadas, as fronteiras têm se mantido estáveis e a Índia não se configura como a maior ameaça à China. Já se envolveu, também, com conflitos fronteiriços com várias nações[46]. A justificativa indiana para seu primeiro teste nuclear (1968) foi considerá-lo uma resposta ao crescimento da ameaça imposta pela China. Estrategistas chineses refletem preocupação crescente com a capacidade nuclear e a capacidade em mísseis indiana, que são vistas como capacidades de coerção à China. Esta percepção é agravada pela intensificação das relações militares EUA-Índia;
d) ***defesa de litoral e de fronteiras***: a proteção de fronteiras têm se tornado uma preocupação crescente, em virtude dos inúmeros conflitos e disputas travadas ao longo das fronteiras. Tem estado fortemente envolvida com a Rússia e países da Ásia Central através da Organização de Cooperação de Xangai (principalmente, no que concerne ao terrorismo na região);
e) ***defesa de águas territoriais e do espaço aéreo***: incluem a proteção das pretensões chinesas no sul do Mar da China (que vêm sido reclamadas desde 1988). É uma das principais preocupações dos estrategistas chineses. A China tem despendido um grande esforço no aperfeiçoamento de sua capacidade de defesa aérea.

Como avaliação principal desta percepção de ameaças, pode-se estabelecer que as avaliações do exército chinês refletem o reconhecimento de novos desafios impostos por aspectos não tradicionais sobre segurança e defesa, tais como: terrorismo, controle de armas, proliferação de armas de destruição em massa, tráfico de drogas, aspectos ambientais, entre outros.

A percepção de ameaças descrita aponta para uma busca de modernização da estrutura da força para dotá-la de capacidades necessárias para fazer frente a estas ameaças. O exército chinês busca quatro categorias de capacidades:
a) ***capacidade de resposta a ameaças*** externas e internas pela tomada de iniciativa rápida, obtenção de superioridade e resolução de conflitos nos termos chineses;
b) ***desenvolvimento eventual de capacidade de projeção limitada de poder*** que sustentaria a presença no mar e negação de área, embora o controle de áreas não seja uma prioridade alta do exército chinês;
c) ***habilidade de condução de ataques preventivos de curto alcance*** usando mísseis convencionais e força aérea;
d) ***desenvolvimento de capacidade nuclear estratégica confiável*** a fim de dissuadir outras potências nucleares do uso de ameaças nucleares com o objetivo de exercer coerção sobre a China, ou limitar suas opções estratégicas em um contexto de crise.

Para cumprir estas missões, tornou-se necessário desenvolver um conjunto capacidades militares que tornem o exército mais moderno, diverso, versátil. Esta estrutura de força consistiria de dois componentes: forças convencionais e forças nucleares. A distância entre o estado atual e o estado desejado é percebido como fraqueza do exército chinês em cumprir suas missões. O exército chinês vem efetuando uma transição entre uma força militar continental que requer grandes forças terrestres para defesa em profundidade para uma força marítima-continental consistindo de forças militares menores, mais sofisticadas e com deslocamento mais veloz (principalmente capacidade para executar missões de

[46] **Conflitos de baixa intensidade com**: Nepal, Sikkim, Myamar, Tailândia, Malásia, Indonésia, Filipinas, Brunei, Laos, Kazaquistão e Quirguistão (desde 1990);
Guerra de fronteiras: Índia, Rússia e Vietnam.
Disputas territoriais: Laos, Rússia, Kazaquistão, Quirguistão, Vietnam e Tajiquistão.

negação de área às forças americanas, que teriam seus esforços dificultados ou impedidos para deslocar força militar para Taiwan, em caso de conflito – esta capacidade é muitas vezes referida como capacidade de "anti-acesso").

Capacidades convencionais desejadas:

a) ***uma força terrestre menor***, mais flexível, altamente treinada e bem equipada centrada em unidades de reação rápida, sendo grande parte do tipo aerotransportada, e com substancialmente maior capacidade anfíbia;

b) ***capacidade naval robusta*** para águas verdes para azuis, centrada em uma nova geração de navios de superfície com defesa aérea aperfeiçoada, com melhor capacidade em guerra anti-submarino e em guerra de superfície, submarinos mais silenciosos com torpedos mais avançados e dotados de mísseis de cruzeiro, capacidade significantemente fortalecida para reabastecimento no mar e maior e melhor aviação naval;

c) ***força aérea mais moderna e mais versátil*** com capacidade de ataque a longas distâncias e de aeronaves de ataque ao solo, alarme aéreo antecipado melhor, melhor apoio aéreo aproximado e estendido, capacidade de transporte a longas distâncias e capacidade de reabastecimento com melhor performance;

d) doutrina de operacional para operações combinadas utilizando melhores sistemas de C4ISR[47], alarme antecipado, sistemas de gerenciamento de combate, com equipamentos espaciais e embarcados em aeronaves para melhorar detecção, acompanhamento, designação de alvos e capacidade de ataque para melhorar a coordenação entre as forças armadas;

Outras características buscadas em relação a capacidades convencionais diretamente relacionadas a Taiwan:

a) desenvolvimento e produção em número significante de ***mísseis convencionais de curto e médio alcance e mísseis de cruzeiro*** está diretamente associada à percepção de ameaças relacionadas a Taiwan;

b) ***mísseis de cruzeiro anti-navio de longo alcance*** e mísseis de cruzeiro ***para ataque terrestre***;

c) capacidade para realização de ***operações de informação***[48] ***e de GE*** sofisticadas e complexas;

d) ***caças de quarta geração***;

e) ***submarinos a diesel*** avançados;

f) ***contra-torpedeiros de emprego geral*** dotados de mísseis de cruzeiro anti-navio de longo alcance;

g) capacidade de ***comunicação*** melhorada;

h) ***capacidade anti-satélite*** limitada;

Em termos de ***capacidade nuclear estratégica***, a China está efetuando uma transição de uma força nuclear pequena não sofisticada e altamente vulnerável (de dissuasão nuclear limitada – visando alvos militares como parte de estratégia de produção de danos limitados) para uma ***força moderna com maior capacidade de sobrevivência e confiável (capaz de efetuar um segundo ataque eficiente).*** Isto está sendo obtido pelo desenvolvimento e fornecimento de sistemas móveis com mísseis de propelente sólido. Outras capacidades buscadas:

a) ***maior número de mísseis balísticos baseados em terra e no mar***, com alcance estendido, mais precisos e com capacidade de sobrevivência;

b) tecnologias mais avançadas para cabeças de combate nucleares, com capacidade de penetração nas defesas anti-mísseis americanas;

c) cabeças de combate nucleares menores e mais potentes com designação de alvos independente (MIRV) ou com múltiplos veículos de re-entrada (MRV);

d) sistema de alerta antecipado moderno com componentes de C4ISR terrestres, aerotransportados, e espaciais.

---

47 Comando, Controle, Comunicações, Computação, Busca e Reconhecimento.

48 incluindo aqui operações de informação associadas à GC.

3.4 – Resultados da análise:

- **elementos motivadores de conflito:**

a) declaração de independência de Taiwan: pouco provável;
b) interrupção de fornecimento de petróleo e gás das fontes atuais: pouco provável;
c) impossibilidade ou redução significativa na previsão de expansão do fornecimento de óleo e gás a partir de novas fontes[49]: probabilidade média, mas com impacto contornável para os chineses;
d) chineses assumem prejuízo de 1,4 trilhão de dólares e se livram dos papéis da dívida interna dos EUA e, em seguida lideram movimento para substituir o dólar como moeda de referência pela moeda contábil usada internamente pelo FMI (a SDR), regida por uma cesta de moedas que reúne o euro, a libra, o dólar e o iene: improvável a curto prazo. Mesmo que haja reposição gradativa destes papéis, passa a ser pouco provável[50].
e) exploração de vulnerabilidades operacionais: Nenhum dos dois lados está completamente preparado para um envolvimento neste nível. As vulnerabilidades já descobertas vão sendo imediatamente corrigidas. Não se pode afirmar nada quanto à capacidade de enfrentamento de inúmeras reações não previstas que podem ocorrer durante um conflito deste tipo (GC). Pouco provável.

- **elementos que afastam a idéia de conflito:**

a) estrutura da dívida interna americana: elemento muito forte.
Os EUA inverteram uma premissa fundamental: ao invés de financiarem-se a partir da tributação, fazem-no tomando empréstimos às grandes corporações e aos cidadãos mais ricos e a credores soberanos (outros países). Em setembro de 2010, segundo dados da Secretaria do Tesouro dos EUA, 42% da dívida pública de 14 trilhões de dólares era frente a grandes corporações, fundos de pensão dos militares e civis e de cidadãos extremamente ricos. Para os restantes 58% são tomados à China, Japão, exportadores de petróleo (Arábia Saudita, etc.), Reino Unido e ao Brasil. Uma situação como esta dificilmente se sustentaria (condição de Ponzi), apenas se mantendo porque o governo dos EUA conseguem manter sua credibilidade de maior economia do planeta (a economia americana possui 25% da economia mundial). A estrutura da dívida interna americana está mostrada na Figura 11.

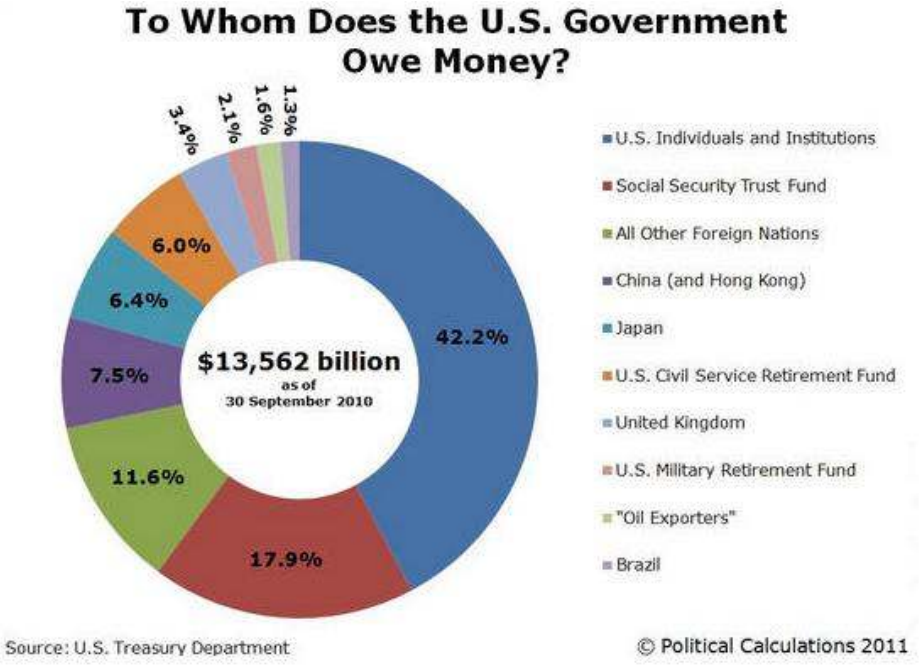


Figura 11. Estrutura da dívida interna americana.

49 principalmente em decorrência dos atuais acontecimentos no Oriente Médio e na implementação de novos gasodutos que podem beneficiar os a Europa (principalmente) e os EUA (indiretamente), com impactos negativos conseqüentes à Rússia (diretamente) e à China (indiretamente).
50 Chama a atenção o fato do presidente americano ter proposto uma redução da dívida no mesmo valor que está de poder dos chineses, mas em 10 anos. A reposição agiria contra os interesses chineses, pois poderia permitir maiores pressões por parte dos americanos em crises internacionais.

O presidente do Banco Central da China, Zhou Xiaochuan, publicou um artigo propondo a substituição do dólar como moeda internacional de referência para as reservas [19]. Em seu lugar, entraria uma moeda contábil usada internamente pelo FMI (a SDR), regida por uma cesta de moedas que reúne o euro, a libra, o dólar e o iene. Por enquanto, não se sabe exatamente, qual seria esta moeda. Não poderia ser o iuan (como gostariam os chineses - na imprensa oficial chinesa, cada um desses entendimentos é saudado como "mais um passo para tornar o iuane uma moeda global"). A China teria que fazer reformas importantes, como a liberação das operações cambiais, antes de poder emitir uma moeda plenamente conversível e utilizável como reserva internacional. Esta hipótese da SRD é sempre lembrada, mas não é exeqüível em curto prazo. Os economistas que prevêem o fim do dólar como moeda de referência acham que isso só acontecerá a longo prazo.

No entanto, a China, num movimento paralelo, fechou alguns acordos, com países como Argentina, Indonésia e Brasil, para que nas transações de comércio exterior se utilize o iuane, jogando o dólar para escanteio [22].

Uma pergunta importante que pode ser feita é o que acontecerá se os chineses resolverem se livrar destes papéis. A resposta esperada seria que os EUA sofreriam um forte aperto de crédito, o dólar seria muito desvalorizado (mais do que já é) e os EUA teriam que realizar um ajuste econômico muito severo, comparável àqueles enfrentados em crises de insolvência, pelas economias pobres ou em desenvolvimento. Mas a hipótese de um aperto externo jamais foi tratada com muita seriedade em Washington, apesar das pressões chinesas. Este aparente desprezo pelo risco foi sempre sustentado numa crença otimista: o mundo nunca deixará de aceitar o dólar como reserva e meio preferencial de pagamento. Como essa crença tem sido seguida até o momento, os EUA têm conseguido financiar seu déficit fiscal e o seu desajuste nas contas externas.

Por muitos anos o arranjo foi confortável para a China: os EUA importam enorme volume de produtos chineses e em troca recebem o financiamento para fechar suas contas.

b) solução para desequilíbrios mundiais: elemento muito forte.

O articulista Martin Wolf [22] no livro *A Reconstrução do Sistema Financeiro Global,* "a China, como o maior país superavitário do mundo, tornou-se fundamental em qualquer solução para os desequilíbrios globais. O país desempenha um duplo papel na economia mundial: é, ao mesmo tempo, o maior exportador de capital (como o Reino Unido do fim do século XIX) e o gigante emergente em mais rápido crescimento (como os EUA da mesma época)".

c) confiança da população no modelo produzido pelo governo chinês x integração nacional: elemento frágil.

A China possui um ativo em quantidade inexistente no mundo, além de escasso no mercado: confiança no futuro [23]. Enquanto a *economia se mostrar favorável*, o risco de desintegração de uma população formada por várias etnias[51] muito afastadas culturalmente fica afastado.

4 – Histórico da GI na China [27]

4.1 – Aspectos conceituais:

A China tem um programa de GI estratégica ofensiva bastante ativo e dota recursos significativos ao estuda do GI. A China vê, na GI, uma arma assimétrica poderosa, que poderia dar ao seu exército capacidade de projeção de poder de longo alcance contra forças americanas convencionais, considerando como alvos potenciais a serem explorados os sistemas de informação, especialmente aqueles relacionados ao comando e controle e ao transporte. Assim esperam retardar ou degradar a mobilização

[51] A China reconhece oficialmente 56 grupos étnicos diferentes. Composição: chineses han 92%, grupos étnicos minoritários 7,5% (chuans, manchus, uigures, huis, yis, duias, tibetanos, mongóis, miaos, puyis, dongues, iaos, coreanos, bais, hanis, cazaques, dais, lis), outros 0,5% (1990). As minorias étnicas têm crescido mais acentuadamente do que a maioria han, passando de 6,1% do total em 1953 para 8,04% em 1990, 8, 41% em 2000 e 9,44% em 2005. Pesquisas recentes indicam que a taxa de crescimento das minorias é cerca de sete vezes a da etnia han.
Divisão administrativa na China: 22 províncias, 5 regiões autônomas (inclui Tibete), 2 regiões administrativas especiais (Hong Kong e Macau) e 4 municipalidades.

de forças americanas em um cenário dependente do tempo (como o que envolve a resposta a uma anexação de Taiwan), configurando uma medida de negação ao uso de força.

Artigos publicados por chineses sobre GI sugerem que GI é um assunto exclusivamente militar, com forte inspiração em aspectos doutrinários americanos.[52] No entanto, considera-se que a China é capaz de desenvolver uma estratégia própria de GI (o que feitos recentes que utilizam técnicas de GC são capazes de corroborar). Percebe-se foco em:

a) sistemas logísticos e de comunicações;

b) compreensão da ameaça americana e admissão se suas próprias fraquezas técnicas que incluem baixa confiabilidade, pouca capacidade de sobrevivência e segurança pobre;

c) identificação de lições importantes decorrentes de observações do conflito "Tempestade no Deserto";

d) tentativa de obter capacidade de desenvolvimento de contramedidas defensivas.

4.2 – Evolução do conceito:

Shen Weiguang[53], um militar de uma unidade de campo escreveu o primeiro artigo[54] conhecido sobre GI em 1995, após ter publicado um livro em 1985[55]. A liderança militar chinesa, impressionada com a performance americana na "Tempestade no Deserto", especialmente sobre a facilidade de destruição de equipamentos militares russos e chineses, acreditam que a GI teve um papel significante na vitória americana. Acreditam, por exemplo, que o uso de vírus de informática tiveram papel importante na destruição ou colocação em estado de não utilização de sistemas de informação americanos.[56] Nestes artigos, são apontados operações e tecnologias aliadas como exemplos de GI. **Wang Pufeng**[57] chamou a "Tempestade no Deserto" de GI e apontou o reconhecimento estratégico superior e os ataques aos centros de C2 iraquianos. como elementos chave para a vitória aliada[58]. Liu Yichang[59] destaca a perfeita execução dos ataques. Li Zhisun e Sun Dafeng[60] descrevem a "Tempestade no Deserto" como a grande transformação e sugere que estratégias de defesa e ataque a computadores podem ser significantes em guerras futuras.

Outros pesquisadores importantes: **Wang Baocun** (Academia de Ciências Militares), **Wang Xusheng**, **Su Jinhai** e **Zhang Hong** (Academia de Tecnologia Eletrônica do Exército).

Centros de excelência em pesquisa de GI:

a) Academia de Ciências Militares (principal centro de pesquisa em GI);

b) Centro de Pesquisa Estratégica (desenvolvimento de estratégias de GI, integração de GI como doutrina militar);

c) Academia de Tecnologia Eletrônica do Exército;

---

52 Pode-se citar as definições de encontradas nas publicações americanas:

a) ***Joint Pub 3-13 Joint Doctrine for Information Operations (IO)*** 1989: "Operações de Informação conduzidas em tempo de crise para obter ou promover a obtenção de objetivos específicos sobre adversário(s) específico(s)";

b) ***Joint Pub 3-13.1 Joint Doutrine for Command and Control Warfare (C2W)*** 1996: "Ações executadas para obtenção de SI ao se afetar as informações adversárias, os processos baseados em informação sistemas de informação e redes de computadores, enquanto se defende as próprias informações, os processos baseados em informação sistemas de informação e as redes de computadores";

c) ***FM-100-6 Information Operations*** (1996) define Operações de Informação como "*Operações militares contínuas dentro do ambiente militar para habilitar, enaltecer e proteger a capacidade das forças aliadas para coletar, processar a lidar com informação a fim de obter uma vantagem ao longo das operações militares. Operações de Informação incluem interação com o ambiente de informações mundial e exploração ou negação de uso da informação ao adversário e sua capacidade de tomar decisões*";

d) ***FM-100-6 Information Operations*** (1996) estabelece que o objetivo das Operações de Informação é estabelecer a Superioridade de Informação (SI) – também definida como Dominância da Informação: "o grau de SI que permite ao seu detentor o uso de sistemas de informação e de suas capacidades associadas para estabelecer vantagem operacional em um conflito ou para controlar a situação em operações de guerra curtas, enquanto nega-se estas capacidades ao adversário".

53 do Escritório de Regiões Econômicas do Conselho Especial do Estado.

54 Foco da Revolução Militar Mundial – Introdução à Guerra de Informação". Diário do Exército de Libertação (Jiefangjun bao, 7 de novembro de 1995. p.6.

55 Guerra de Informação. Sem data de publicação.

56 "Papel do Exército na Guerra de Informação". Jiefangjun bao. 25 de junho de 1996. p.6.

57 considerado pai da disciplina GI.

58 também se considera que a Primeira Guerra do Iraque foi um campo de teste para armas avançadas tecnologicamente e de uma nova estratégia a ser usada no futuro (no caso da Tempestade no Deserto, a estratégia da Rápida Dominância. Na Liberdade para o Iraque, a estratégia do Choque e Pavor).

59 "Sobre a Guerra de Alta Tecnologia" – Gaojishu zhanzheng lun. Pequim: Universidade de Defesa. 1993, p 272.

60 "A Estratégia da Guerra de Alta Tecnologia" **-** Gaojishu zhanzheng molü. Pequim: Universidade de Defesa. 1993. p 3 – 9, 184 0- 201.

d) Departamento de Estado Maior Terceira Sub-seção (GI desenvolvida no Instituto de Pesquisa 61 e na Academia de Engenharia da Informação);
e) Centro de Pesquisa Nacional para Inteligência de Sistemas de Computação;
f) Universidade de Ciências Eletrônicas e Tecnologia (Comissão de Ciência, Tecnologia e Industria para a Defesa Nacional).

O ponto alto de definição de GI foi alcançado em dezembro de 1995, na Conferência de Diretores Nacionais da Comissão de Ciência, Tecnologia e Industria para a Defesa Nacional, com a declaração de **Liu Huaqing**[61]:

> *"GI e GE são de importância capital, enquanto que lutar no terreno pode somente servir para explorar a vitória. Portanto, a China e seu exército estão mais convencidos que uma revolução militar utilizando GI como núcleo principal alcançou estágio onde esforços devem ser feitos para acompanhar de maneira próxima ou ultrapassar adversários".*

Atualmente, pesquisadores desenvolvem conceitos em GI, tais como: natureza, posição, princípios, modos, métodos e meios.

4.3 – Definições:

A China definiu GI[62] como:

> *"GI é um produto da era da informação onde se utiliza extensamente tecnologia da informação equipamentos que manipulam de informação em batalha. Ela é constituída a partir da informatização do campo de batalha pela utilização de redes de computadores, e um novo modelo para o contexto de tempo e espaço. Nela, se situa a luta pelo controle da informação no campo de batalha e, portanto a capacidade de influenciar ou decidir a vitória ou a derrota".*
>
> *...*
>
> *"GI é um estágio crucial na guerra de alta tecnologia. No seu coração estão as tecnologias de informação, fundindo guerra de inteligência, GE, guerra de mísseis guiados, mecanização, guerra total. É um novo tipo de guerra".*

Wang Pufeng distingue este novo tipo de guerra do paradigma anterior:

> *"Informação e a capacidade de empregá-la liberam uma nova energia na batalha; informação fluindo através de topologias de rede de computadores abre um novo campo de batalha de computadores. Com a informatização do exército, agilidade e velocidade, mobilidade e ataques em profundidade, em uma batalha sem linha de frente, gera uma salto à frente, na concepção de métodos tradicionais de guerra. A área do campo de batalha se expande, as velocidades aumentam, a precisão do ataque aumenta consideravelmente, alterando as concepções passadas de espaço e tempo".*

4.4 – Princípios:

O objetivo da GI na China é a obtenção da SI, que é definida como a habilidade de defender a própria informação enquanto se explora ou se ataca a estrutura de informação do oponente. Entende que esta SI possui dois componentes: tecnológico e estratégico. Requer habilidade para interferir na habilidade do adversário em obter, processar, transmitir e usar informação a fim de paralisar todo o seu sistema operacional. Afirmam que a SI não é determinada por superioridade tecnológica, mas por novas táticas e pela criatividade dos comandantes em campo, colocando mais ênfase nos componentes pessoas e organizações, no conflito. Aparecem conceitos novos como campo de batalha espacial multidimensional, integrando ar, terra, mar, espaço e espectro eletromagnético[63]. Dentro deste teatro de operações, unidades militares conduzem operações furtivas integrando sensores e sistemas de amas. Neste contexto, sensores são utilizados para garantir a "consciência dominante no teatro de operações" (Consciência

---

61 "Últimas tendências na Revolução de Assuntos Militares na China". Hsin Pao. Hong Kong Economic Journal.

62 **Wang Pufeng**. "GI e RAM".

63 **Wang Jianghuai** e **Lin Dong**. "Visões de Crescimento da Qualidade de nosso Exército sob a Perspectiva de Demandas da GI". Jiefangjun bao. 3 de março de 1998. p.6.

Situacional), que permite ataques em profundidade contra "hubs" de unidades de comando e controle, redes de comunicação e sistemas logísticos, não permitindo ao adversário uma visão completa da situação (Visão Combinada – *Joint Vision*). Coloca-se ênfase no ataque em profundidade e guerra além do horizonte contra instalações de comando e controle que são percebidas como centros de gravidade. Os objetivos de uma operação não são mais cercar e matar inimigos, mas destruir a disposição do adversário em resistir. A vitória no campo de batalha da informação[64] seria o foco das operações. Como conseqüência, conduzem os militares para se organizarem com a utilização de redes de computadores, exigindo unidades menores e modulares. Também são muito citados pelos pesquisadores chineses de GI os conceitos emanados por Alvin Tofler (A terceira Onda e Guerra e Anti-Guerra).

Comparando-se com a doutrina americana de GI, os chineses[65] também incluem na sua doutrina, elementos de GE, dissuasão estratégica, guerra de propaganda, guerra psicológica, guerra de computadores (*netwar*) e guerra de comando e controle. No entanto, vão além dos estrategistas americanos ao afirmar ser necessário novas estratégias e novas formas organizacionais.

Consideram a GI como arma de guerra não convencional e não um multiplicador de força (como consideram os estrategistas americanos). Seria uma arma utilizada para redução de assimetria, uma arma de uso preventivo. Consideram a derrota iraquiana na Primeira Guerra do Iraque devido à incapacidade iraquiana de lançar um ataque preventivo, durante a fase de deslocamento de forças americanas para a Arábia Saudita, onde consideram que o adversário poderia ser mais vulnerável.

5 – Termos técnicos [27]

a) xinxi zhanzheng — GI;
b) junshi geming — Revolução de Assuntos Militares (RAM);
c) zhixinxiquan — Dominância da informação (Superioridade da informação – SI);
d) yitihua — integração;
e) feixianxing zuozhan — operações furtivas / operações especiais;
f) zongshen zuozhan — ataque em profundidade;
g) turanxing yu kuaisuxing zuozhan — ataques súbitos e rápidos;
h) dianxue — pontos vitais (Centros de Gravidade);
i) yuanzhan — Guerra Além do Horizonte;
j) bingdu — viroses;
k) wangluohua — desenvolvimento em redes;
l) xinxihua — informatização;
m) feixianxing zuozhan — "uma Guerra sem linha de frente";
n) zhiming daji — ataques mortais;
o) xinxi gaosu gonglu — "super-via de Informação (info-via)";
p) ruan shashang — destruição branda;
q) kuayue — salto tecnológico (em relação à introdução de ciclos de vida de inovações, se refere à utilização de certo tipo de inovação tecnológica, evitando-se inovações intermediárias, em relação a que é utilizada atualmente. Ação comum em TIC);
l) *zhongda biange* – grande transformação;
m) *gaojishu zhanzheng molü* – Estratégia de guerra de alta tecnologia;
n) *jidong zhan* – mecanização;
o) *huoli* – guerra total;
p) *wanshan* – execução perfeita de um ataque.

64 ou Teatro de Operações Virtual.
65 Su Enze. "Conceitos Lógicos em GI". Jiefangjun bao. 11 de junho de 1996. p.6.

6 – Cenários escolhidos para análise

Os cenários descritos a seguir foram propostos por **Lu Linzhi** [27], de emprego de GI como arma de ataque preventivo para derrotar os EUA (um inimigo tecnologicamente superior) durante as fases de mobilização e deslocamento, após a tomada de Taiwan pelos chineses. Para o exército chinês, utilizar GI contra os sistemas de informação dos EUA para degradar ou mesmo retardar o deslocamento de força para Taiwan se constitui em uma estratégia assimétrica interessante. As forças americanas são extremamente dependentes de informação e necessitam grandemente de redes logísticas bem coordenadas. s chineses poderiam retardar a chegada da força tarefa americana ao teatro de operações, enquanto se desenvolve e se consolida a campanha para a tomada da ilha pelos chineses.

Nestes cenários Taiwan proclama a sua independência e a China decide tomar a ilha. Acredita-se que os americanos socorrerão Taiwan, mas seriam pressionados para não deslocarem uma força tarefa neste sentido.

6.1 - Ataque Cibernético de grande escala aos EUA anterior à mobilização dos EUA (invasão de Taiwan) - Nível estratégico: [28]

Enunciado*:* A China lançaria um ataque cibernético estratégico em larga escala contra a rede de energia americana, colocando a rede do meio-oeste fora de operação. A intenção seria passar a mensagem de que os custos de intervenção não ocorreriam somente no solo chinês. Portanto, a força tarefa não deveria partir.

Análise: Este objetivo seria atingido? Um ataque cibernético teria um efeito de coerção (dissuasório) somente se pudesse ser atribuído à China. Esta atribuição não seria uma atividade simples (geralmente é uma atividade extremamente difícil descobrir a origem de um ataque cibernético). Supondo-se que se consiga êxito nesta identificação, seguindo-se ao ataque, a China invade Taiwan. Pode-se afirmar que os EUA não interviriam no conflito após o ataque cibernético? Considerando-se as reações americanas a Pearl Harbour e aos ataques de 11 de setembro de 2001, provavelmente não. Considerando que os chineses levam em conta seriamente a história, não considerariam este cenário, a não ser que este ataque pudesse alterar a narrativa do conflito. Para tal deveriam acreditar que os americanos temeriam ser duramente atingidos durante o conflito, no qual teriam que participar para manter a coerência com a estratégia americana de contenção da China (segundo a visão chinesa).

No entanto, um ataque cibernético levaria transformaria a percepção do conflito que passaria de um conflito regional para um conflito global (com o envolvimento das alianças militares produzidas pelos americanos na Ásia).

Portanto, um ataque cibernético estratégico teria um fraco poder dissuasório (de coerção) e seria improvável.

6.2 - Ataque Cibernético aos EUA (sistemas logísticos, de transporte, centros de comando e controle) anterior à mobilização dos EUA (invasão de Taiwan) - Nível operacional: [28]

Enunciado*:* A China lançaria um ataque cibernético operacional aos sistemas militares americanos (utilizando-se armas de efeito de semântica sobre nas bases de dados existentes). Seria considerado uso legítimo de poder. A intenção seria retardar o deslocamento de forças americanas pelo Pacífico de tal forma que a situação na ilha já estaria consolidada quando a força tarefa americana chegasse ao teatro de operações.

Análise: A avaliação da extensão dos danos causados por este ataque seria praticamente impossível para os chineses, que não teriam a certeza em atingir seu objetivo. Como fator adicional, os efeitos seriam temporários e a janela de retardo de deslocamento seria da ordem de alguns dias (considerando um efeito devastador). É uma janela muito pequena para se traduzir em vantagem operacional explorável. Restaria a realização de ataques cibernéticos que degradariam a habilidade de operação das forças americanas. Mas ataque dificilmente seria eficiente: medidas de segurança são continuamente aperfeiçoadas e a possibilidade de sucesso cai a cada dia. Também haveria a preocupação, por parte dos chineses, da resposta americana a este ataque cibernético (na forma de um

ataque cibernético), que poderia prejudicar suas operações em Taiwan (teriam que operar simultaneamente em dois domínios: físico - invasão e virtual – espaço cibernético).

Para obter sucesso neste ataque preventivo, os chineses teriam que gastar muito tempo planejando, fazendo varreduras redes de computadores dos sistemas logísticos e de defesa (que podem ser detectadas) e pesquisando vulnerabilidades para exploração futura. As vulnerabilidades encontradas ainda precisariam ser monitoradas continuamente a fim de evitar surpresas na hora de lançar o ataque cibernético.

Resta ainda analisar a habilidade das forças armadas dos dois países de efetuarem operações militares com sucesso sob ataque cibernético intenso (simultaneamente operacional e estratégico). Isto exigiria tempo e condições de simulação e avaliação extremamente difíceis.

Portanto, um ataque cibernético operacional teria um fraco efeito sobre as operações em andamento no teatro de operações e seria pouco provável, no momento.

O framework relativo aos Cenários 2 e 3 está mostrado na Figura 12. [29]

6.3 - Ataques Cibernéticos esporádicos para demonstração de capacidade – Dissuasão cibernética – Nível estratégico:

Enunciado*:* Este cenário se desenvolveria quando a China se envolvesse em uma crise internacional após o corte (ou percepção de ameaça de corte) de linhas de fornecimento de óleo ou gás, como estratégia de contenção de seu desenvolvimento econômico.

Análise: A China promoveria ataques cibernéticos nos países considerados seus adversários nesta crise, sem permitir identificação explícita da origem dos ataques ou sem admitir sua realização, como forma de dissuasão (coerção).

Pode produzir algum efeito positivo, mas será uma iniciativa secundária (apoiaria negociações diplomáticas, etc.). Pode ser considerada muito provável.

7 - Conclusões

No nível estratégico de condução da guerra, a China poderá realizar (já realiza) operações cuja finalidade é a dissuasão estratégica, em um contexto de GEI.

No nível de condução operacional, não demonstra suficiente agilidade ou flexibilidade organizacional (cultura organizacional de grande distância ao poder – em relação à concentração de autoridade, proteção de paradigma, baixa redução de incerteza na estruturação de atividades) para tratar a informação com eficácia, de forma a desenvolver uma GM com flexibilidade, agilidade e velocidade necessárias para reduzir a assimetria do conflito com os EUA, em uma GI. A obtenção de SI pode até ser obtida, mas se mostrará momentânea.

Apresenta problemas infinitamente maiores com manutenção de integridade nacional (também não deve ter sucesso nisso), para os próximos 50 anos, onde deve manter o seu foco.

Segundo Libicki [28] há três estágios que devem ser superados por EUA e China para que haja possibilidade de utilização de operações de GC:

a) determinar a extensão da habilidade de executar missões sob risco de ataques cibernéticos;
b) assegurar que haverá resiliência para lutar em um ambiente onde ocorrerão ataques cibernéticos;
c) determinar quão bem pode-se resistir a um ataque cibernético.

Segundo o mesmo autor os EUA já teriam ultrapassado os dois primeiros estágios e estariam se preparando em relação ao terceiro.

Quanto aos chineses não há, obviamente, discussões sobre o assunto, mas percebe-se que, pelos ataques realizados a organizações militares de defesa americanas que o primeiro estágio já foi ultrapassado. Quanto ao segundo e terceiro estágios as autoridades chinesas nunca comentariam, em público, seu desempenho em uma situação dessas. Portanto não há avaliação disponível.

Portanto um ataque cibernético aos EUA só seria possível se os chineses terminassem, antes dos americanos, o terceiro estágio.

7.1 – Lições que poderiam ser seguidas pelas Forças Armadas brasileiras:

A China possui muitas similaridades com o Brasil, na implementação de doutrinas militares:

a) são países em desenvolvimento;
b) possuem mão de obra barata;
c) produzem taxas de crescimento igual ou superior à média mundial;
d) têm controle firme da inflação;
e) são países de dimensões continentais;
f) possuem grande diversidade demográfica;
g) possuem grande extensão de litoral a defender;
h) possuem grande extensão de fronteiras a controlar;
i) tem grande necessidade de recursos energéticos para sustentar seu crescimento;
j) possuem necessidade (com graus diferentes de intensidade e tempo de prontificação) de modernização de suas forças armadas;
k) podem enfrentar, no futuro, forças muito superiores tecnologicamente (mantidas as devidas proporções e intensidade de envolvimento em crises).

Portanto, há aspectos doutrinários, organizacionais, de pesquisa e desenvolvimento de tecnologia militar, de gestão de inovação e conhecimento, de formação de parcerias com empresas internacionais para a produção de tecnologia dual (de uso militar e civil) que poderiam ser vistos com mais interesse pelas Forças Armadas brasileiras.

REFERÊNCIAS:

[1] McNEILLY, Mark. **Sun Tzu e a arte da guerra moderna.** 1. ed. Rio de Janeiro: Record, 2003. p.130;
[2] HILDRETH, Steven A. **Cyberwarfare - CRS Report for Congress.** Received through the CRS Web. Order Code RL30735. Disponível em: <http://www.faz.org/irp/crs/RL30735.pdf>. Acesso em: 08 de julho de2003. p.16.
[3] ibid. p.1.
[4] SARAIVA. (Ed). Minidicionário**: informática.** São Paulo: Saraiva. 2001. p.70.
[5] CORTES, Camilo. **O Ataque ao Iraque no Contexto do Pós-Modernismo Militar.** Rio de Janeiro: [s.n.], 2003. Palestra proferida na Escola de Guerra Naval em 02 de julho de 2003.
[6] ARQUILLA, John, RONFELT, David. **Swarming & the future of conflict.** Santa Monica: RAND Corporation - National Defense Research Institute, 2003. p.1.
[7] ARQUILLA, John, RONFELT, David. **Swarming & the future of conflict.** Santa Monica: RAND Corporation - National Defense Research Institute, 2003. p.vii.
[8] ALBERTS, David, GARSTKA, John J.; HAYES, Richard E., SIGNORI, David A. **Understanding information age warfare**. 1. ed. Washington: CCRP (DoD Command and Control Research Program), 2001. p.88.
[9] ALVES, José Ricardo Rodrigues Teixeira, CMG (EN). **A guerra de informação**. Revista Marítima Brasileira, Rio de Janeiro, v. 122, n. 10/12, p. 143 - 153, out./dez. 2002.
[10] NUNES, Paulo Fernando Viegas, CT. **Impacto das novas tecnologias no meio militar: a guerra de informação.** Aerospace Power Journal (em português). Alabama, v. s.n., n. s.n., p. 39 - 53, abr./maio/jun. 2000.
[11] HILDRETH, Steven A. **Cyberwarfare - CRS Report for Congress.** Received through the CRS Web. Order Code RL30735. Disponível em: <http://www.faz.org/irp/crs/RL30735.pdf>. Acesso em: 08 de julho de 2003. p.16.
[12] SMITH, Edward Allen. **Effects based operations - applying network centric warfare in peace, crisis and war.** 1. ed. Washington: Center for Advanced Concepts and Technology (ACT) - CCRP, 2002. p. xiv.
[13] ibid. p.111-119.

[14] DUTRA, A. M. C. **Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto**. IX Simpósio de Guerra Eletrônica. Disponível em http://161.24.2.250/sige/sige_old/IXSIGE/Artigos/GE_39.pdf. Acesso em 6 de junho de 2011.
[15] LIBICKI, Martin C. **Cyberdeterrence and Cyberwar**. 1. ed. Santa Monica: RAND Corporation, 2009.
[16] Waltz, Edward. **Information warfare principles and operations.** 1 ed. Norwood: Artech House, Inc., 1998.
[17] BOISOT, Max. **Information, space, and the information-space: a conceptual framework.** Disponível em: <http://www.uoc.edu/in3/gnike/eng/docs/dp_02_boisot.doc>. Acesso em: 08 de setembro de 2003.
[18] BOISOT, Max. **Information space - a framework for learning in organizations, institutions and culture.** Disponível em: <http://www.iscc.edu/site/publications.html>. Acesso em 08 de setembro de2003.
[19] JORDAN, Ernest. **National and organizational culture: their use in information systems design.** Disponível em: <http://www.is.cityu.edu.hk/Research/workingpapers/working_paper94.htm>. Acesso em: 08 de setembro de 2003.
[20] DAVISON, Robert, JORDAN, Ernest. **Cultural Factors in the Adoption and Use of Group Support Systems.** Disponível em: <http://www.is.cityu.edu.hk/Research/workingpapers/paper9604.htm>. Acesso em: 08 de setembro de 2003.
[21] SCHERMERHORN Jr., John R., HUNT, James G., OSBORN, Richard N. **Fundamentos de comportamento organizacional.** 2 ed. Porto Alegre: Bookman, 1999. p.262-263.
[22] JARDIM, L. **2009, o ano do G-2.** Revista Veja. Disponível em http://veja.abril.com.br/060509/p_074.shtml. Edição de 06 de maio de 2009. Edição 2111. Acesso em 20/05/2011.
[23] JARDIM, L. **A prova de fogo do dragão.** Revista Veja. Disponível em http://veja.abril.com.br/060509/p_088.shtml. Edição de 06 de maio de 2009. Edição 2111. Acesso em 20/05/2011.
[24] BORSATO, C. **Inflação *made in* China**. Revista Veja. Disponível em http://veja.abril.com.br/241007/p_098.shtml. Edição de 24/10/2007. Edição 2031. acesso em 20/05/2011.
[25] Crane, K., Cliff, R., Medeiros, E., Mulvenon, J., Overholt, W. **Modernizing China's Military. Opportunities and Constraints**. MG-260. 1 ed. Santa Monica: RAND Corporation, 2005. p. 183-184; p. 187-190.
[26] ibid. p. 191-203.
[27] MULVENON, J., Yang, R. H. **The People's Liberation Army in the Information Age**. Conference Proceedings. CF-145. 1 ed. Santa Monica: Rand Corporation, 1999. p. 183-184; p. 175-186.
[28] LIBICKI, Martin C. **Chinese Use of Cyberwar as an Anti-Access Strategy – Two Scenarios**. Testimony before the U.S. Economic and Security Review Commission. RAND Corporation, 27 de Janeiro de 2011.
[29] MOLANDER, R. C., WILSON, P. A., MUSINGTON, D. A., MESIC, R. F. **Strategic Information Warfare Rising**. 1 ed. Santa Monica: RAND Corporation, 1998.

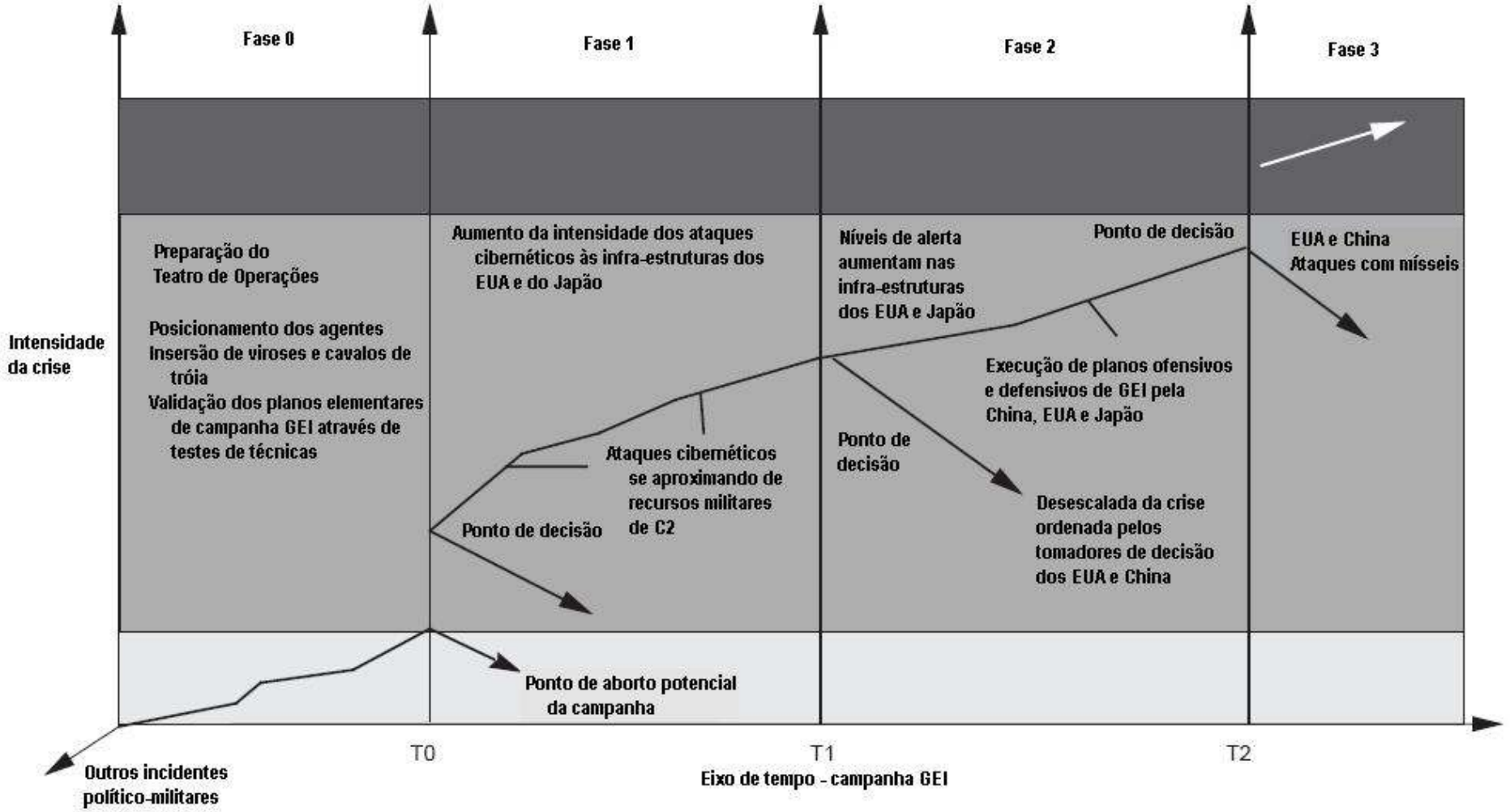


Figura 12 – Framework relativo aos Cenários 1 e 2. [29]