A Guerra de Informação

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

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

Sun Tzu

1 - Histórico

O propósito deste artigo é situar a Guerra de Informação (GI) num contexto de evolução histórica da Arte da Guerra. Como será descrito abaixo, esta evolução foi marcada por fatos extremamente relevantes que deram início a verdadeiras eras. Estes fatos revolucionários não distorcem, de forma alguma, os princípios da guerra, como foram enunciados por Clausewitz, mas otimizam a utilização dos recursos disponíveis de forma que esses princípios são assegurados de forma tão eficaz, que se traduzem em vitória [1].

[2] Presencia-se, hoje, uma revolução na arte da guerra. Afirma-se também que não é a única ocorrida, nem será a última. Essas transformações ocorrem quando um fato marcante de natureza tecnológica, política, ou uma inovação social fundamental ocorre, alterando o caráter e a condução de um conflito. No entanto, novas tecnologias ou armas não serão verdadeiramente eficazes se não se desenvolver a adaptação da doutrina que permita a maximização do potencial inerente a tais desenvolvimentos.

Nos últimos duzentos anos, foram experimentados seis revoluções na arte da guerra. A primeira foi a Revolução Francesa em 1789. Com a instituição do serviço militar obrigatório, a França conseguiu montar grandes exércitos, permitindo a Napoleão se contrapor a seus adversários por vinte anos.

O marco importante seguinte foi a Revolução Industrial na metade do século dezenove. Esta revolução permitiu a uma nação em desenvolvimento equipar, armar e transportar grandes exércitos de conscritos. Novas armas aumentaram a letalidade e o escopo do teatro de operações. O telégrafo e as ferrovias aumentaram dramaticamente a velocidade e a agressividade das operações.

A terceira revolução foi uma revolução gerencial, no final do século dezenove, que permitiu a rápida formação e utilização de grandes unidades militares. As nações criaram "staffs" formados por pessoal técnico qualificado, para integrar seus recursos industriais e civis. Infelizmente, o período compreendido entre a Revolução Industrial e a Revolução Gerencial resultou na Primeira Guerra Mundial, onde esses conceitos pareceram pouco assimilados, tendo-se perdido quase uma geração nos teatros de operações da Europa.

A quarta revolução foi a Revolução Mecanizada, ocorrida entre 1919 e 1939. O uso do inovador motor de combustão interna mudou drasticamente as guerras terrestre e aérea. Ela substituiu a guerra de trincheiras por operações rápidas, caracterizadas por grandes penetrações e envolvimentos de forças. Na Segunda Guerra Mundial esses conceitos foram bastante explorados.

A Segunda Guerra Mundial terminou com o aparecimento da quinta revolução, a Revolução Científica. Esta revolução passou a utilizar o intelecto do cientista, do engenheiro e do técnico especialista para vencer a guerra. Como exemplo, temos o projeto, a construção e o emprego da bomba atômica.

Após o despertar da era nuclear, as características da guerra permaneceram virtualmente inalteradas por trinta anos. Então, com a introdu-

[1] O autor exerce a função de Superintendente de Apoio aos Sistemas, na Diretoria de Telecomunicações da Marinha. Subordinado a esta superintendência, foi criado, recentemente, o Departamento de Segurança das Comunicações. Este departamento desenvolve Normas de Segurança para Redes Locais, realiza auditorias em redes, efetua pesquisa de vulnerabilidades e detecção de intrusos a nível de RECIM, estuda e implementa técnicas de ataque a redes pela Internet, e gerencia os recursos criptológicos em vigor na MB. Atualmente está sendo preparada uma equipe de auditores que atuarão como "hackers éticos" para auditar redes e testar vulnerabilidades nas comunicações da MB.

ção de computadores e armas de alta precisão, iniciou-se uma nova era. A Revolução da Informação centra no conceito de que a habilidade para coletar, analisar, disseminar e agir no teatro de operações é um fator dominante na arte da guerra.

Na atual Era da Informação, tempo e tecnologia confundem a linha divisória entre planejamento e execução (6ª revolução). As Forças Armadas do século XXI devem estar preparadas para enfrentar oponentes num espectro muito mais amplo. Elas devem estar equipadas para enfrentar inimigos das Eras Agrária e Industrial (dentro do conceito desenvolvido por Alvin Toffler, em "A Terceira Onda" e "Guerra e Antiguerra"), assim como deve estar pronta para se contrapor a adversários da Era da Informação. Como no passado, o primeiro desafio é a adoção de tecnologias emergentes para maximizar as capacidades inerentes do combatente. Mas a interface entre a tecnologia e o combatente individual deve ser o coração de um projeto dentro de uma força armada de adaptação às necessidades do século atual.

De acordo com Nunes [3], esta nova era, em que a ciência e a indústria desempenham um papel determinante na potência destrutiva das Forças Armadas, é caracterizada pela existência de três grandes tipos de armamento que se sucederam em importância ao longo dos tempos, dentro do duelo milenar entre ofensiva e defensiva:

- ***armas de obstrução***: fossos, rampas, bastiões, couraças e fortificações de todos os gêneros;
- ***armas de destruição***: lanças, arcos, peças de artilharia, mísseis, etc.; e
- ***armas de comunicação***: sinais, vetores de informação, telegrafia, rádio, radares, satélites, etc.

Cada um desses tipos de arma dominou um tipo de confrontação, e um tipo de guerra:

- ***guerra de cerco***: armas de obstrução;
- ***guerra de movimento:*** armas de destruição; e
- ***guerra relâmpago:*** armas de comunicação.

Também pode-se definir o objetivo das guerras impostas pelas estruturas socioeconômicas predominantes em cada época (primeira onda – era agrária, segunda onda – era industrial, e terceira onda – era da informação). A era agrária impôs uma guerra de conquista e/ou controle de recursos territoriais. A era industrial caracterizou-se por uma guerra de redução dos recursos de produção de um oponente. A era da informação serão travadas para assegurar o controle de dados, da informação e do conhecimento.

A Figura 1 [4] ilustra as características das guerras da segunda e terceira ondas. A "força de batalha" será extremamente móvel e preparada para operar num ambiente independente, que será mais vertical (no sentido espacial, de terceira dimensão, pelo emprego crescente do Poder Aerospacial – Iniciativa de Defesa Estratégica/Guerra nas Estrelas) que linear (terrestre, primeira dimensão), além de virtual (quarta dimensão – ciberguerra).

2 – Cenário

Neste novo contexto, [5] o mundo está prestes a entrar numa nova etapa na qual não haverá muito derramamento de sangue nessas guerras. Por um único motivo: as armas inimigas, principalmente, nem chegarão a ser sequer disparadas porque os seus mecanismos de ignição serão simplesmente desativados. Isso será feito de forma sutil, remotamente, a milhares de quilômetros de distância. Além disso, com a globalização dos meios de comunicação (mídia internacional), dentro de um conceito de "aldeia global", o impacto provocado por muitas baixas poderá influenciar a opinião pública e retirar o apoio da população (que elege os governantes) ao conflito em andamento (perda da vontade de lutar – derrota, segundo Clausewitz).

O século XXI começa nesta terceira onda do campo de batalha. Este campo passará a ser, principalmente, o espaço virtual: define-se assim a era da GI, também chamada de Guerra Cibernética ("Cyberwar").

Neste cenário virtual, a maior ameaça estrangeira passa a ser, então, a invasão de redes de computadores e demais meios de comunicação. Os ataques virão diretamente de outros governos, e poderão causar danos de longo prazo à economia – alertou Lawrence

Gershwin, o principal conselheiro em assuntos tecnológicos da CIA. A própria CIA informou que os EUA estão mais vulneráveis a esses tipos de ataque. Em depoimento à Comissão Conjunta de Economia, da Câmara e do Senado, há uma semana, Gershwin previu que as guerras de informação serão uma realidade num período de cinco a dez anos.

Os combates eletrônicos visarão a infra-estrutura funcional: a destruição das redes que controlam as comunicações, a distribuição de energia, os transportes, a movimentação eletrônica de dinheiro.

Os terroristas ainda preferem bombas. Mas essa prioridade logo deverá mudar. As ameaças cibernéticas aumentarão substancialmente à medida em que uma geração tecnicamente mais competente comece a fazer parte das células terroristas. A perícia de incapacitar um país a partir da segurança de uma casa, é, segundo o especialista em computação da Hewlett-Packard Co, Gary Sevounts [6], uma das supremas ferramentas do terrorismo. Assim, o "ciberterrorismo" poderá ficar cada vez mais destrutivo e inatingível.

Segundo Gershwin, já existem vinte países investindo pesadamente no desenvolvimento de armas e estratégias de ataque cibernético - entre eles a China, a Coréia do Norte, o Iraque, Israel, França, Grã-Bretanha, Líbia e Cuba.

A mudança [5] de conceito bélico começou, segundo a CIA, na Guerra do Golfo Pérsico, em 1991. Ao observar o conflito, o governo da China percebeu que seria muito difícil, se não impossível, derrotar os EUA numa guerra convencional. Por isso, o país reuniu um batalhão de especialistas em computação com o fim específico de desenvolver vírus ofensivos, além de um sistema de defesa eletrônico que o Pentágono apelidou de "Grande Muralha Virtual da China".

De acordo com Geewax [6], vermes ("worms") do "Code Red" (Código Vermelho) podem ter tido como objetivo anunciar ao mundo que a China é agora capaz de prejudicar os EUA à vontade. O verme teria sido criado para atacar o Web site da Casa Branca e deixar uma mensagem: "Piratea-do por chineses"[2]. De acordo com relatório divulgado pelo NIPC, órgão investigativo do FBI para assuntos de proteção à infra-estrutura nacional, a praga infectou mais de 250 mil sistemas em apenas nove horas de atividade, causando prejuízos de 2 bilhões e meio de dólares, pode ter sido gerada na universidade chinesa da província de Guangdong [8].

A Agência de Sistemas de Informação de Defesa (DISA, na sigla em inglês), do Pentágono, tem uma vasta equipe de especialistas cuidando da proteção do sistema que interliga os seus 2,5 milhões de computadores. Eles têm sido atacados constantemente por "hackers". Mas uma boa parte do seu orçamento passou a ser destinada a um programa específico de defesa contra sistemas cibernéticos de outros governos. Os militares americanos sabem que esse tipo de guerra deixou de ser assunto da ficção científica: afinal, o Pentágono já utilizou, em passado recente, computadores como armas.

CIA e Pentágono não revelam as armas eletrônicas que vêm desenvolvendo. Especialistas, no entanto, mencionam uma série de vírus conhecidos como "Cavalo de Tróia", com funções diversas. Eles seriam instalados de forma inofensiva em sistemas de outros países, para serem deflagrados quando isso for necessário - ou de interesse dos EUA.

O que mais impressiona neste novo enfoque é o conceito empregado a nível estratégico, pois a guerra de informação transcende o ambiente militar, envolvendo outros segmentos da sociedade, vitais para a soberania e segurança nacional. Considerando a globalização de mercados e de economia, dos meios de comunicação de massa, e o uso cada vez mais intenso da Internet, o extremismo religioso que obtém mais adeptos a cada dia, as "limpezas étnicas" mais freqüentes, a explosão de focos de nacionalismo regionais, o

[2] Para se enfrentar forças muito mais poderosas, precisa-se de alguma arma, ferramenta, método ou sistema que multiplique a eficiência de forças consideradas menos poderosas.
Como vêm dizendo os chineses, desde há dois mil anos e quatrocentos anos (Sun Tzu) e agora ("Code Red"), tal arma se configuraria como sendo a definida pela Guerra de Informação, pois sabemos que desde os primórdios da história do homem neste planeta, o homem primitivo podia não dispor de muita tecnologia, mas necessitava de muita informação, e sempre a utilizou (e ainda a utiliza).

aparecimento do narco-terrorismo (que já chega a obter o domínio regional em vastas áreas em alguns países), do terrorismo anti-globalização, nos aproximamos e nos afastamos simultaneamente do conceito de "aldeia global" conforme definiu Mac Luhan, na década de 60 (movimento de pulsação). A ameaça de uma guerra estratégica de informação, nesta nova realidade, elimina por completo (por diluição) a distinção entre sistemas militares e civis, assim como a definição precisa de quem é o inimigo, ou onde ele está.

3 - Enquadramento conceitual

Conforme demonstrado por Nunes [3], ainda não se chegou a uma definição exata do termo "guerra de informação", embora seja objeto de vários estudos na área de Defesa. Mas concorda-se que, na era digital, a informação e sua disseminação alcançaram o estado de recurso estratégico vital.

O que a expressão significa é realizar tarefas que antes eram realizadas, mas de forma mais rápida, utilizando eventualmente equipamentos resultantes da evolução tecnológica da nossa sociedade. Constata-se pois, que as idéias básicas do conceito da guerra de informação já existem há vários séculos.

Pode-se defini-la, mesmo de maneira rude, como tudo o que se possa efetuar para preservar os próprios sistemas de informação da exploração, corrupção ou destruição causadas pelo inimigo, enquanto, simultaneamente se explora, corrompe e destrói os seus sistemas, visando obter assim, a necessária vantagem de informação se houver necessidade de enfrentar um conflito armado.

Ainda que se torne fundamental em caso de se verificar a ocorrência de um combate, a utilização da força não constitui a seqüência natural da guerra de informação. Muitas vezes, a guerra de informação não é mais do que obter a informação mais rapidamente que o inimigo e examiná-la de modo mais cuidadoso e eficiente.

O verdadeiro problema reside no fato de termos antigos conceitos numa nova roupagem. Ela se materializa através de suas envolventes, descritas abaixo, que são:

- combate aos sistemas de comando e controle;
- segurança operacional;
- ciberguerra;
- guerra eletrônica;
- pirataria eletrônica ("hacking");
- bloqueio de informação;
- guerra baseada na informação; e
- guerra psicológica.

4 – Envolventes

4.1 - Combate aos sistemas de Comando e Controle:

Desenvolve-se através de ações que neguem ou dificultem ao inimigo o controle de suas forças e a faculdade de comunicar-se com elas.

É um dos mais antigos princípios da guerra, e é provavelmente o mais importante. A chave do problema é a capacidade de tomar decisões de uma forma mais rápida que o adversário e passar em seguida à ação com base nessas decisões.

Todos os nossos atos se baseiam em ciclos de decisão. Cada ciclo pode ser definido como "OODA" (Observar, Orientar a atenção para o que acabou de acontecer, Decidir como atuar e Agir). A guerra de informação pode evitar a nossa observação. A falta desta informação compromete a maneira de como orientamos a nossa atenção, atingindo a nossa decisão e a ação conseqüente.

4.2 – Segurança operacional:

É a preservação dos assuntos sigilosos e do local onde são guardados.

4.3 – Guerra eletrônica:

É a negação do uso do espectro eletromagnético ao inimigo, especialmente para neutralizar centros de comando e controle e comunicações.

4.4 – Ciberguerra:

Pode ser considerada como parte integrante do conceito de guerra eletrônica. Envolve a utilização de todas as ferramentas disponíveis ao nível de eletrônica e informática para derrubar sistemas eletrônicos e de comunicações inimigos e manter os sistemas operacionais amigos. Muitas das ações nessa

área se encontram ainda pouco definidas, devido ao aparecimento contínuo de novos equipamentos, e pelo fato de ser uma área nova de interesse militar, como forma de guerra.

Os "ciberguerreiros" ("cyberwarriors") operam a partir de Centros de Informação de Combate, e tem a missão de informar o comandante sobre a situação do Teatro de Operações Militar, com dados confiáveis.

4.5 – Pirataria eletrônica:

Também conhecida por "hacking", consiste numa "guerra de guerrilha eletrônica" da qual qualquer pessoa, em qualquer lugar do mundo, pode participar. Basta um microcomputador, um modem conectado à linha telefônica, bons conhecimentos de redes LAN ("Local Area Network" – Redes Locais), WAN ("Wide Area Network" – Redes de Grande Área) e MAN ("Metropolitan Area Network" – Redes de Área Metropolitana), e muita determinação para obter conhecimento sobre técnicas de invasão de redes no submundo dos sites "hackers" da Internet (onde esta informação se encontra sob a forma dispersa, ou seja, não didática, e muitas vezes deve ser negociada, isto é, só é fornecida em troca de outra informação de mesma importância).

É um fenômeno recente (tem cerca de dez anos de existência), disponibilizado pela explosão de uso da Internet. Uma quantidade assustadora de programadores, técnicos de informática e curiosos autodidatas com tempo disponível e intenções maliciosas, navegam pela rede à procura de falhas de segurança dos sistemas de informação (inclusive os sistemas militares). É claro que se pode transformar "hackers" em armas militares, isto permitira a vantagem de se penetrar nos sistemas do inimigo em tempo de guerra.

Por outro lado, também é uma ação atrativa para o terrorismo internacional.

4.6 – Bloqueio de informação:

É uma variação da prática de bloqueio do território inimigo, com a finalidade de impedir que ele receba recursos e bens.

É obtido pela inoperância provocada de satélites, enlaces-rádio de comunicação, cabos de fibras ópticas, impedindo a canalização de informação para o território inimigo.

4.7 – Guerra baseada na informação:

Tem o seu peso, pela importância que os meios de comunicação de massa possuem sobre a opinião pública e sobre o processo de tomada de decisão política.

4.8 – Guerra psicológica:

Constitui na divulgação de informação enganosa, com o fim de desmoralizar o inimigo. Este aspecto vem sendo utilizado com sucesso assinalável, mas existe outro aspecto a ressaltar. Dentro do contexto da guerra psicológica, pode-se atuar sobre a informação que circula nos sistemas inimigos vedando-lhe a utilização, ou pode-se efetuar defesas contra este tipo de ação por parte do inimigo, tentando eliminar a informação manipulada pelo inimigo e que este fez chegar às forças amigas, via computador, telefone, ou outra forma camuflada.

5 – Armas utilizadas

[3] As armas empregadas na Guerra de Informação podem ser classificadas quanto ao efeito que produzem, em três classes:

- armas de efeito físico;
- armas de efeito de sintaxe; e
- armas de efeito de semântica.

A discussão da forma de utilização dessas armas (em termos ofensivos ou defensivos), vem se tornando acalorada ultimamente. Muito esforço vem se desenvolvendo a nível defensivo, obviamente. Um critério de verificação de eficiência, neste novo contexto, é a análise de vulnerabilidades (principalmente de redes de computador, mas não esquecendo dos sistemas de informação suportados por essas redes, e até mesmo dos protocolos que "rodam" nelas – "Network Centric Warfare" – Guerra Centrada em Redes). A segurança começa com uma mentalidade preventiva, acima de tudo.

5.1 – Armas de efeito físico:

A utilização de uma arma física resultará na destruição permanente de componentes físicos da estrutura da informação, tendo como conseqüência direta, a correspondente negação de serviço. Faz eco no conceito de supressão da

ameaça, segundo a nova doutrina de guerra eletrônica nos EUA.

A complexidade deste tipo de arma é baixa, e seu emprego é linear.

Como exemplos, podemos citar: mísseis, explosivos, ações de sabotagem, armas de energia direcionada ("DEW – Directed Energy Weapons" – grandes canhões de laser de raios X, laser de elétrons ou canhões eletromagnéticos, geralmente para serem colocados em órbita terrestre, componentes da SDI, com o objetivo de destruição de mísseis nucleares, ou causadores de forte interferência eletromagnética, se utilizadas no solo).

5.2 – Armas de efeito de sintaxe:

Uma arma 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 ("worms") e cavalos-de-tróia ("trojans").

Assim, controlando o sistema de informação do inimigo, se controlará o seu processo de decisão e a sua capacidade de percepção e compreensão dos acontecimentos.

5.3 – Armas de efeito de semântica:

O objetivo de tais armas é 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.

A complexidade associada é elevada, pois não visam afetar os sistemas de informação, mas o comportamento das pessoas que os utilizam, influenciando as suas decisões.

6 - Conclusão

Por isso, é cada vez mais importante, a capacitação pessoal (inteligência individual) numa situação de conflito armado que, a partir da evolução do conceito de guerra atual para um conceito de guerra de informação, leva grande parte dos combates para um enfoque mais "cerebral". A história tem demonstrado que a superioridade tecnológica não é, sozinha, um fator decisivo para o sucesso. Isso ficou demonstrado pela dificuldade que as forças armadas americanas encontraram na Coréia e no Vietnã. Mesmo considerando forças vencedoras, estas podem ser surpreendidas com perdas inesperadas e importantes durante a condução do conflito, como foi a perda do HMS Sheffield para os ingleses, durante a guerra das Malvinas. Um equilíbrio deve ser estabelecido entre qualidade de pessoal, treinamento, liderança, doutrina e equipamento. Ao redor do mundo as forças armadas vêm sendo reformuladas drasticamente, tendo esse preceito por base, mas sempre mantendo suas características de prontificação e treinamento, a fim de se adequar às necessidade de um mundo ainda em construção. O preceito anterior que validava o sacrifício da juventude de uma nação num envolvimento em um conflito já está descartado.

A Força Armada do século XXI deve ser dotada de qualidade em termos de pessoal, uma doutrina revista, organização eficiente, treinamento adequado na paz e na guerra e o melhor equipamento e sistemas de armas prontos, dadas as fontes disponíveis.

Assim, o poder da informação permitirá que a arma principal - o combatente individual - enfrente os desafios do próximo século e que obtenha a vitória decisiva.

Assim, numa perspectiva de GI, combatentes devem continuamente melhorar sua habilidade no uso da tecnologia, para combater o inimigo. Devem ser capazes de assimilar um fluxo rápido de informações e desempenhar missões num ambiente multinacional, e até mesmo "virtual".

Além do uso confortável da tecnologia, devem possuir outras características, tais como bom nível cultural, boa capacidade de processar informações, adaptabilidade, tenacidade sob "stress" e sólidos critérios de julgamento. Ainda

assim, devem ser capazes de enfrentar inimigos que "não jogam pelas regras", tais como terroristas, traficantes de drogas, grupos que perfazem limpeza étnica e genocídio. Mesmo assim, a GI será conduzida, principalmente, numa forma geral, num ambiente sem muito derramamento de sangue, mais parecido com um vídeo game, do que as sangrentas batalhas do passado. Espera-se um envolvimento mais acelerado, e tomadas de decisão mais rápidas e com mais qualidade, assim como uma maior disposição para envolvimento em conflitos.

Mesmo assim, pode-se afirmar que a Arte da Guerra pode mudar, mas não mudará o impacto sobre nações, exércitos e soldados.

REFERÊNCIAS

[1] – Reimer, Dennis J. – War in the Information Age: New Challenges for U.S. Security. Ed Brassey's, 1997;

[2] - Pfaltzgraff, R. L. e Shultz Jr, R. H. e- "War in Information Age". Ed. Brassey's, 1997;

[3] – Nunes, P. F. V. Cap. – Impacto das Novas Tecnologias no Meio Militar – A Guerra de Informação. Aerospace Power Journal;

[4] – Scales Jr., R. H., Maj. Gen. – Cycles of War – Armed Forces Journal - Intenational. Jul/97;

[5} – Passos, José Meirelles – A ameaça de guerra sem sangue. O Mundo - O Globo – 29/07/01 – 2ª Ed.;

[6] – Geewax, M. – Defesas não livram EUA do Ciberterrorismo. O Estado de São Paulo;

[7] – Denning, D. E. – Information Warfare and Security. Ed. Addison-Wesley. 1999.

[8] – Equipe Securenet. "Code Red" pode Ter mesmo origem chinesa. 31/08/01. http://www.securenet.com.br.

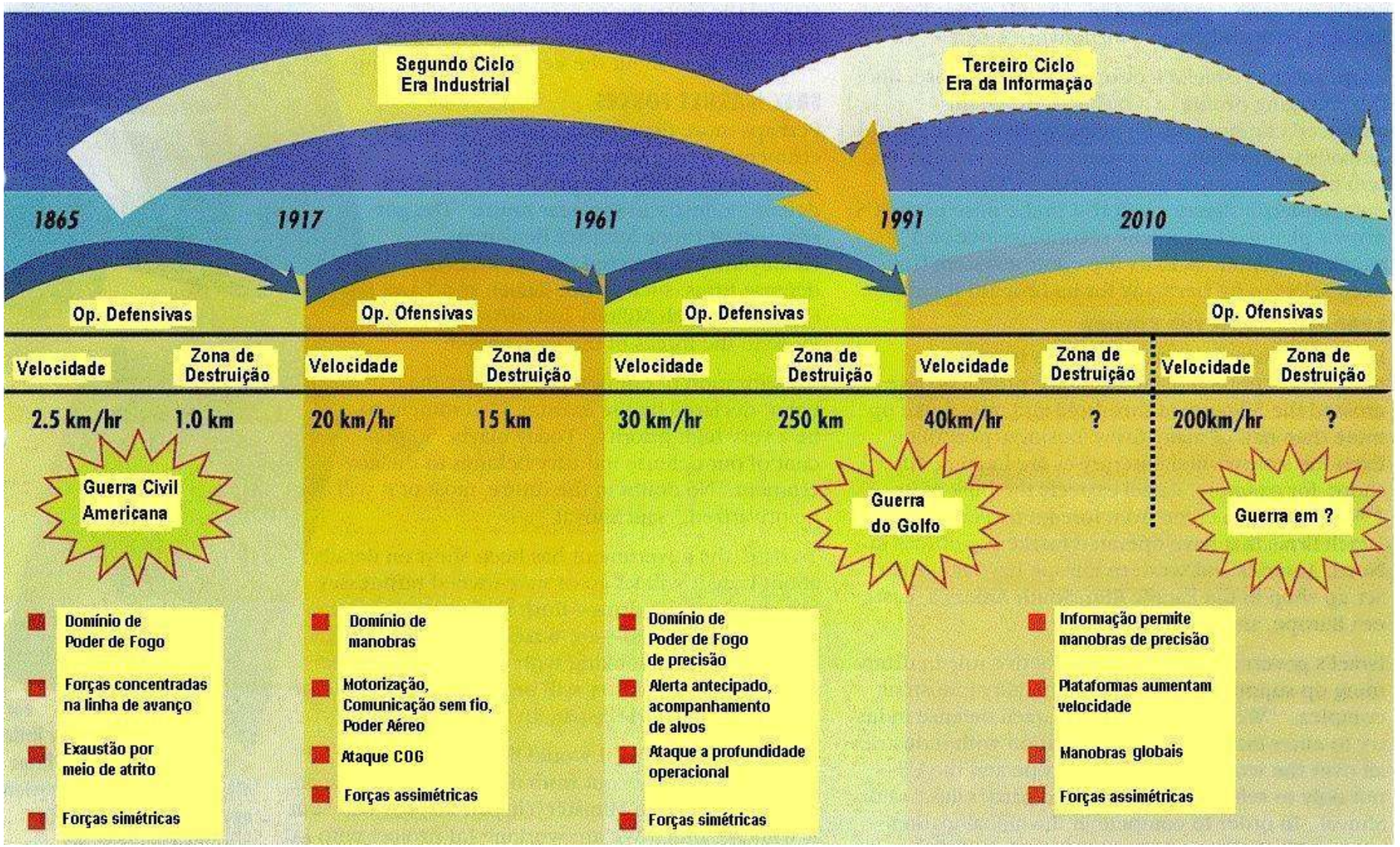

Figura 1 – Os ciclos de eras mostram com clareza como a tecnologia altera o equilíbrio entre operações ofensivas e defensivas. Mostra também a influência da era da informação sobre essas operações.