

INFORMAÇÕES: UM ANTIGO CONCEITO SOB UM NOVO PARADIGMA

Tenente Coronel Alexandre José Corrêa

O Ten Cel Corrêa é o atual Comandante do 25º Batalhão de Infantaria Paraquedista, no Rio de Janeiro. Ao longo dos 12 anos em que serviu na Brigada de Infantaria Paraquedista, atuou como Elemento de Inteligência e coordenador de Informações em várias operações Singulares e Conjuntas. É Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras, Mestre em Operações de Informação pela Universidade de Toronto e Canadian Forces College, no Canadá, e Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército. Possui, ainda, o Curso Superior de Inteligência Estratégica, na Escola Superior de Guerra, no Rio de Janeiro.



é cada vez mais descontínuo, assimétrico e multidimensional. No ambiente de hoje – essencialmente conjunto e interagências – as Forças Armadas estão cada vez mais envolvidas em assuntos que não os exclusivos da esfera militar, mas que são igualmente essenciais para o êxito na condução das operações.

É crescente a necessidade de captação e gestão de informações advindas de todas as áreas do conhecimento. A participação em operações conjuntas e multinacionais contribui ainda mais para a necessidade de expandir o ambiente de informação situado na tradicional área de interesse das Forças, além de destacar a imperiosa necessidade de proteção de dados e informações essenciais para a tomada de decisão em momentos de crise.

Por outro lado, a interconexão global das informações – uma das vertentes da “globalização” – impõe que os países disponham da capacidade de preservar e proteger sua liberdade de ação interna e externamente, informando e exercendo influência sobre determinados públicos-alvo, afetados diretamente ou não pelas ações desse país.

A partir da caracterização da Era da Informação, na obra de Heide e Alvin Toffler, “Guerra e Anti-Guerra: Sobrevivência na Aurora do Terceiro Milênio”¹, consolidou-se o entendimento de que a gestão das informações na Segurança e Defesa tornou-se algo vital para a própria existência e soberania dos Estados.

O ambiente do moderno campo de batalha



O presente artigo pretende discutir essa imperiosa necessidade de obtenção do domínio das Informações pelos Comandantes nos diversos escalões, em qualquer situação de emprego da Força Terrestre, e destacar as Operações de Informação (Op Info) – basicamente as ações voltadas para informar e influenciar públicos – como um “atuador” essencial no espaço de batalha atual, analisando, por consequência, implicações que essa nova realidade possa ter para o Exército Brasileiro (EB).

A SUPERIORIDADE DE INFORMAÇÕES

Primeiramente, é preciso que nivelemos o entendimento sobre dois conceitos importantes relativos ao emprego das informações pelos comandantes e seus estados-maiores. Conceitos que podemos afirmar serem complementares, mas que, em essência, são bastante distintos.

O primeiro refere-se à superioridade de informações. Tal como a superioridade de meios – ou a superioridade relativa de poder de combate – a superioridade no campo das informações é determinante no espaço de batalha moderno.

Comandantes que dispõem de mais e melhores dados decidem melhor do que seus oponentes e, conseqüentemente, têm maiores chances de vitória.

É fácil inferir que, como consequência direta do atual ambiente complexo descrito por vários autores e Instituições internacionais², o processo de tomada de decisão deverá ser calcado no máximo de informações possíveis, advindas das mais diversas áreas de interesse, incluindo aquelas em que as Forças Armadas já possuem elevado grau de expertise.

Apesar de muitos considerarem que a complexidade sempre foi uma característica presente no ambiente operacional e nos espaços de batalha, o incremento da facilidade de interconexão entre a grande gama de riscos enfrentados pelas sociedades nacionais, na atualidade, é um dos principais aspectos que diferencia e torna único o ambiente operacional

de hoje. Um exemplo bem próximo da realidade brasileira é o risco de corrupção que interliga-se de forma marcante aos riscos de crime organizado, à falha de governança global, ao comércio ilícito e à disparidade econômica. Por outro lado, esses riscos podem estar relacionados, ainda que com menor grau de interdependência, aos riscos decorrentes do terrorismo, da fragilidade da infraestrutura e dos aspectos relacionados à segurança das informações e dos dados em redes informatizadas³. Dessa forma, fica fácil entender que serão bem sucedidas as nações que dispuserem de um eficiente sistema de gestão das informações, de forma que o processo decisório de seus líderes possa contar com a sinergia derivada da superioridade de informação adquirida sobre potenciais adversários.

Em muitos países essa é uma visão nacional, sobretudo quando se trata da condução de operações conjuntas. Esses países tendem a adotar uma visão orientada para o emprego de capacidades operativas específicas, de acordo com a qual explorar a superioridade do conhecimento na área de operações – e fora dela – assume um papel determinante para o sucesso.

Em operações militares, portanto, a superioridade de informações seria traduzida pela vantagem que uma Força tem sobre seu adversário, em função de sua maior capacidade para coletar, processar e disseminar informações em caráter permanente e contínuo, ao mesmo tempo em que nega essa capacidade ao oponente.

O nível de planejamento conjunto abrange, entre outras, a necessidade de interligação de sistemas de comando e controle (C2) táticos aos sistemas operacionais e estratégicos que lhes são correlatos.

AS OPERAÇÕES DE INFORMAÇÃO

O segundo conceito a destacar é o de Operações de Informação (Op Info). Nele, o vernáculo “informação” tem sentido diverso daquele que utilizamos até agora, neste artigo.

“Comandantes que dispõem de mais e melhores dados decidem melhor do que seus oponentes e, conseqüentemente, têm maiores chances de vitória”.

Refere-se ao ato de informar, ou seja, comunicar, fazer saber ou dar conhecimento de algo a alguém.

Um conceito empregado há alguns anos pela maioria dos países integrantes da Organização do Tratado do Atlântico Norte (OTAN), as Op Info representam a forma encontrada para integrar as atividades e tarefas executadas em apoio às operações que se destinam a informar o público amigo e a comunidade internacional e influenciar públicos neutros, adversários ou hostis.

Em outras palavras, Op Info seriam, basicamente, o emprego de capacidades específicas que permitam a uma Força Militar afetar o espaço de batalha por meio da informação intencionalmente dirigida aos públicos que podem influenciar seu desfecho. Adicionalmente, as Op Info incluem as tarefas relacionadas à proteção das informações vitais para o processo decisório e à degradação do processo decisório adversário.

Para que seja possível caracterizar e entender toda gama de capacidades que abrangem as Op Info, é interessante realizar uma breve análise da perspectiva que orientou a adoção desse conceito pela OTAN e pelo Exército dos Estados Unidos da América (EUA), que já testaram em combate suas doutrinas sobre o assunto.

INFORMAÇÕES E OPERAÇÕES DE INFORMAÇÃO NA OTAN

Ao constatar que suas estruturas orgânicas dependiam, de forma significativa, das informações e dos seus processos associados, a OTAN começou a desenvolver sua doutrina para esta área específica. A finalidade foi “reduzir as vulnerabilidades e aproveitar as oportunidades da Aliança, no que se refere ao controle da informação necessária ao processo de tomada de decisão”⁴. Assim, o documento MC 422/1 (2002) definiu que as Op Info teriam caráter ofensivo e defensivo, coordenadas pelo mais alto escalão, de forma que a sua condução refletisse a orientação político-estratégica decidida pelos países-membros.

Pela definição da OTAN, as Operações de Informação Defensivas procuram “assegurar o acesso permanente e a utilização efetiva da informação e dos sistemas de informação, durante uma situação de paz, crise ou conflito e proteger a informação crítica da Aliança, de forma a atingir determinados objetivos”. Percebe-se

certa semelhança entre esta definição e a que utilizamos para a Superioridade de Informações. Aparentemente, esses conceitos também se confundem na Aliança Atlântica.

Já as Operações de Informação Ofensivas da OTAN objetivariam “influenciar a informação e os sistemas de informação de potenciais adversários, durante uma situação de paz, crise ou conflito, na consecução de determinados objetivos, ou em resposta a uma ameaça específica”. Percebe-se, aqui, o emprego do verbo “influenciar” – que nos remete mais diretamente às tarefas a serem executadas pelas Op Info.

O primeiro manual da Doutrina Aliada Conjunta, de 2005 (*Allied Joint Doctrine - AJP-01/2005*) apresenta o conjunto das diversas atividades associadas à área das Op Info. O documento define Operações de Informação como aquelas que “incluem e envolvem a Guerra de Comando e Controle (C2W, na sigla em inglês)⁵, com as atividades políticas, diplomáticas, a Cooperação Civil-Militar (CIMIC, na sigla em inglês) e a Informação Pública, assim como quaisquer outras que possam afetar a percepção de um adversário e de outras partes envolvidas”⁶. É uma definição que enfatiza a intenção de informar e influenciar públicos.

Percebe-se que, para a OTAN, as Op Info incluem dois grupos de atividades distintas: um com aplicação civil e outro com aplicação militar. O primeiro inclui componentes das atividades política, diplomática, de CIMIC e de relações públicas que estão, ou poderão vir a estar, relacionadas com a condução das operações militares. O segundo grupo, por sua vez, compreende a condução de atividades de C2W e das Comunicações e Sistemas de Informação, com a finalidade de negar informação, influenciar, degradar ou destruir as capacidades de C2 de um adversário, enquanto os próprios sistemas são protegidos⁷.

Em novembro de 2009, a Organização publicou o manual “Doutrina Aliada Conjunta para Operações de Informação” (*Allied Joint Doctrine for Information Operations - AJP-3.10*). Apesar de focado no nível operacional, o *AJP-3.10* deixa bem clara a sua subordinação ao nível político-estratégico, do qual emanam as orientações para as ações militares⁸. Segundo o manual:



Figura 1: A abordagem da OTAN para afetar a vontade, as percepções e as capacidades de potenciais adversários⁹.

“Ações militares isoladas não podem resolver crises, mas podem estabelecer condições para que outros atores a resolvam, incluindo, para tanto, o uso de todas as capacidades do poder nacional, oferecidas pelos estados membros da OTAN.”

Ainda, segundo o AJP-3.10, uma Op Info

“(...) oferece tanto o assessoramento, quanto a coordenação das atividades de informação militar, com a finalidade de criar o efeito desejado na vontade, no entendimento e nas capacidades dos adversários, potenciais adversários e outras partes, após aprovadas pelo Conselho do Atlântico Norte, em apoio aos objetivos militares estabelecidos (...)”.

As Op Info possuem os seguintes focos específicos:

- mudar, influenciar ou reforçar percepções e atitudes de adversários;
- preservar e proteger a liberdade de manobra da Aliança no ambiente das informações, por meio da defesa de dados e informações que apoiem o processo e a tomada de decisão; e
- atingir a capacidade de comando do adversário, afetando as informações que servem de dados de suporte para o C2, inteligência, vigilância e aquisição de alvos, além daqueles dos quais se valem os sistemas de armas inteligentes.

A figura 1 apresenta uma visualização de como as Operações de Informação conduzidas

pela Aliança Atlântica, constituem um grande guarda-chuva sob o qual várias outras operações são desenvolvidas.

INFORMAÇÕES E OPERAÇÕES DE INFORMAÇÃO NOS EUA

Os EUA foram o país que primeiro decidiu desenvolver doutrina específica, buscando sistematizar a utilização da informação no ambiente operacional. Inicialmente, as Op Info empregavam capacidades da C2W, por meio do ataque aos meios de Comando e Controle inimigos e da proteção dos próprios meios de C2. Posteriormente, o Manual de Campanha 100-6 “Operações de Informação” (*FM 100-6, Information Operations*), de 1996, incluiu duas outras atividades: Assuntos Cíveis e a Informação Pública. Ao conjunto integrado dessas tarefas e atividades foi atribuída a designação de Operações de Informação¹⁰.

O entendimento de que as Op Info estavam inseridas em um contexto mais abrangente (civil e militar) levou ao desenvolvimento de Doutrina Conjunta específica, consolidada na Publicação Conjunta 3-13 “Publicação de Doutrina Conjunta para Operações de Informação” (*Joint Publication 3-13 “Joint Doctrine for Information Operations Publication”*), de 1998. Essa publicação destacou a interdependência estrutural e funcional entre agências civis e forças militares, o que condiciona o processo de planejamento e execução das Op Info. A “guerra de Informação” foi definida



Militares brasileiros afixam cartaz em *créole*, Porto Príncipe/Haiti.

como “o conjunto das Operações de Informação conduzidas durante um período de crise ou conflito com a finalidade de atingir ou promover a consecução de objetivos específicos sobre um ou mais adversários.” As Op Info deveriam ser planejadas além do nível estratégico-militar: no nível político-estratégico¹¹.

Em outubro de 2003, o documento *Information Operations Roadmap*¹² tornou as Op Info uma competência militar fundamental, estabelecendo diretrizes e metas para todos os atores envolvidos com a Defesa, desde o nível político-estratégico até o nível tático de atuação. A publicação destacou três objetivos das Op Info, desenvolvidos desde o tempo de paz:

- deter, desencorajar, dissuadir e direcionar um adversário por meio da desintegração da sua unidade de comando e intenção de combater, enquanto preserva a sua própria;
- proteger seus planos e desorientar os dos adversários, permitindo, dessa forma, maximizar o efeito das suas forças, obtendo exorbitante vantagem, enquanto o adversário gasta seus recursos para obter efeitos reduzidos ou limitados; e
- controlar as comunicações e redes do adversário e proteger as suas, incapacitando, dessa forma, a habilidade do inimigo organizar-se e defender-se, enquanto preserva o efetivo C2 das suas forças.

Em fevereiro de 2006 foi publicada uma atualização do *JP 3-13*, agora um compêndio detalhado da doutrina de Op Info. As Op Info são descritas como o

“emprego integrado de capacidades fundamentais da Guerra Eletrônica, da Guerra Centrada em Redes, das Operações

Psicológicas, da Dissimulação e das Operações de Segurança, em concerto com capacidades que as apoiam e a elas são relacionadas, para influenciar, romper, corromper ou usurpar o processo de decisão humano ou automatizado de um adversário, enquanto protege o processo aliado”.

As capacidades de apoio das Op Info são a Garantia das Info, a Segurança Física, o Ataque Físico, a Contrainteligência e a Transmissão do Combate por Câmeras (tradução livre de *Combat Camera - COMCAM*). As capacidades relacionadas são as Relações Públicas, a Cooperação Civil-Militar e a Diplomacia Pública.

O *JP 3-13* ainda definiu que as Op Info devem receber prioridade da comunidade de Inteligência, uma vez que as fontes serão sempre limitadas e que, normalmente, o prazo para obtenção dos produtos necessários será longo, considerando as restrições legais e as especificidades de cada público-alvo.

De todas as publicações sobre Op Info, a última versão do *JP 3-13* foi a que melhor caracterizou o ambiente da informação, descrevendo-o como um agregado de indivíduos, organizações e sistemas que coletam, processam, disseminam ou agem sobre a informação¹³.

CONCEITOS POSSIVELMENTE APLICÁVEIS À DOCTRINA BRASILEIRA

O desenvolvimento de uma doutrina autóctone sobre o assunto pode partir de conceitos bem estabelecidos e consolidados na F Ter, empregando-se a expertise desenvolvida em trabalhos e pesquisas junto a Exércitos que já avançaram nessa área. Toda discussão e a evolução conceitual em torno da necessidade de dominar as informações pode ser explorada por aqueles que estudam sua implantação no Exército Brasileiro (EB).

Para facilitar a análise das capacidades requeridas para que a Força Terrestre tenha condições de obter essa vantagem, o primeiro passo é levantar as tarefas operativas relacionadas, agrupando-as segundo suas finalidades. Como referência inicial, sugerimos os grupos de tarefas a seguir:

- obter dados para desenvolver um completo entendimento do espaço de batalha – São as

atividades e tarefas que permitem ao comandante saber mais sobre o ambiente operacional no qual está operando. Aí estão incluídas as tarefas direcionadas à obtenção de dados sobre o adversário – como as executadas pela Inteligência, a vigilância e as missões de reconhecimento, por exemplo – e as tarefas para obtenção de dados sobre aspectos culturais e sociais das populações afetadas pelo conflito;

- gerenciar as informações e o conhecimento – As muitas informações que devem apoiar o decisor são produzidas por elementos distintos dentro da F Ter e muitas vezes não são adequadamente processadas – ou sequer chegam ao conhecimento do decisor. Gerenciar o conhecimento é garantir que os comandantes possam fazer uso de todas as informações necessárias para apoiar seu entendimento situacional. Gerenciar as informações, por seu turno, implica no emprego de meios e métodos para continuamente processar, integrar e transmitir essas informações aos decisores, com eficiência e eficácia;

- proteger as informações e os ambientes por onde elas transitam – A importância das informações, por si só, torna clara a necessidade de adotar medidas ativas e passivas para defendê-las e negar que os adversários tenham oportunidade de explorá-las a seu favor. Também inclui a proteção de instalações e dos ambientes (físicos e virtuais) por onde elas transitam e onde são armazenadas. A Contraineligência e as rotinas de segurança de rede e de instalações executam as tarefas deste grupo;

- moldar o ambiente, informando o público nacional e influenciando públicos externos – Neste grupo estão as tarefas que nos permitem atuar para modificar o espaço de batalha, conformando-o e alinhando-o aos objetivos estratégicos da campanha. É possível perceber que o emprego integrado das capacidades da Comunicação Social (informar público amigo) e das Operações Psicológicas (influenciar público estrangeiro) são fundamentais para a execução dessas tarefas;

- degradar, desabilitar ou destruir os sistemas de informações do adversário – Inclui, além de ataques centrados nas redes cibernéticas, as tarefas que permitem interromper a capacidade

de Comando e Controle do adversário, ou negar seu acesso às informações; e

- confundir e iludir o adversário – Este grupo inclui toda e qualquer ação conduzida para deliberadamente iludir os adversários quanto às nossas capacidades, intenções e ações. Podemos citar a dissimulação como exemplo de capacidade empregada com essa finalidade.

É fácil perceber que as tarefas incluídas nos dois primeiros grupos são aquelas empregadas em apoio ao processo decisório dos comandantes e estados-maiores, na busca pela vantagem (ou superioridade) de informações. Os quatro grupos de tarefas seguintes indicam o emprego de atuadores específicos no espaço de batalha, com caráter tanto ofensivo quanto defensivo – ou seja, as operações de informação.

No ambiente operacional de hoje, as potencialidades da utilização sinérgica dessas capacidades não podem ser negligenciadas. A dependência do funcionamento dos modernos sistemas, relativamente à informação (ex: SIVAM, DAAe, CINDACTA, bem como o Programa SISFROM, após a sua conclusão), ilustram bem sua importância no âmbito das Forças Armadas brasileiras.

Note-se que praticamente todas as capacidades citadas já existem no EB. Por essa razão não se visualiza a necessidade de criar um novo sistema. Basta apenas integrar as capacidades dos sistemas já existentes na Força, empregando-as sistemicamente. Os estados-maiores, a partir do escalão brigada, devem estar organizados e treinados para coordenar o emprego dessas capacidades.

Cabe ressaltar que, por sua natureza, as tarefas empregadas para moldar o espaço de batalha ficam, normalmente, restritas ao nível Força-Tarefa Conjunta, ou ao próprio Comando Conjunto. Nestes escalões, será preciso prever um elemento coordenador, que integre essas capacidades operativas para a obtenção dos resultados desejados em todo o Teatro de Operações – e além dele, muitas vezes.

Uma análise sumária dos diversos escalões da F Ter permite-nos afirmar que o EB necessitará investir mais fortemente em meios e métodos para a gestão eficiente das informações que devem chegar aos estados-maiores¹⁴.



A Comunicação Social é uma valiosa ferramenta para informar o público.

Além disso, o desenvolvimento de dispositivos de proteção para os modernos sistemas que lidam com informações encontra-se muito aquém do desenvolvimento dos próprios sistemas de armas. Tanto por razões técnicas como econômicas, considera-se que não será razoável pensar que, hoje ou num futuro próximo, o Brasil poderá vir a dispor de um sistema 100% seguro. No entanto, julga-se importante a adoção de contramedidas e de mecanismos capazes de reduzir o risco¹⁵.

Esse cenário eleva a demanda pelas medidas de proteção das informações dentro do paradigma da Guerra de Informação, refletindo-se na necessidade imperiosa do desenvolvimento da capacidade de Op Info, não só no âmbito do Exército e das Forças Armadas, mas no nível nacional¹⁶.

CONSIDERAÇÕES FINAIS

O ambiente estratégico internacional evidencia o fato de que a prevenção e a resolução de conflitos envolverão, cada vez mais, uma

coordenação estreita de todos os campos do poder, que vai além do campo de batalha clássico. Nesse contexto, informar e influenciar a vontade e o comportamento de adversários ou das partes em conflito, e afetar sua capacidade de comando e controle – negando-lhe o acesso às informações e degradando suas estruturas físicas – assume uma relevância estratégica sem precedentes.

Óbvio dizer, a vulnerabilidade a ataques aos meios de gestão da informação é diretamente proporcional ao desenvolvimento tecnológico de uma Nação ou Força Armada, uma vez que estas, geralmente, empregam e dependem de sistemas complexos.

Doutrinas estrangeiras mais recentes mostram claramente a distinção e um entendimento comum do que seja o emprego de Informações em proveito dos Comandantes Operacionais e as Op Info propriamente ditas, bem como do seu papel nos conflitos atuais e emergentes.

A plena integração das Informações, no contexto global das operações militares, começa a se constituir como um desafio para o Brasil, quer no nível político nacional, quer no desenvolvimento de competências específicas neste domínio, no âmbito da Defesa. Essas necessidades acabam tendo reflexos na Força Terrestre, demandando ajustes nas estruturas existentes. É possível que a solução adotada pelo EB determine a necessidade de quebrar alguns paradigmas quanto à organização dos estados-maiores e a integração de dados de Inteligência, entre outros aspectos. É preciso começar a implantá-las.

NOTAS

1. Uma caracterização da chamada Era da Informação se apresenta nesta obra de Heide e Alvin Toffler. Utilizamos a versão original, em inglês do livro. Vide TOFFLER, Alvin e TOFFLER, Heidi (1995). *War and anti-War: Survival at the Dawn of the 21 Century*, New York, Warner Books.
2. Uma análise com razoável grau de credibilidade está no Relatório de Riscos Globais 2011 (*Global Risks Report 2011*), do Fórum Econômico Mundial (WEF, sigla em inglês). O Relatório apresenta um diagnóstico dos riscos mais marcantes que envolvem a atual conjuntura global, dentro de cinco grandes áreas de interesse: economia, geopolítica, meio-ambiente, social e tecnologia. Segundo Klaus Schwab, fundador e Presidente Executivo do WEF, o relatório de 2011 destaca que o mundo de hoje se encontra em um nível sem precedentes de riscos interconectados entre todas as áreas de interesse. O assunto destaque no corrente ano foi o processo de decisão nesse mundo interconectado e a necessidade de incrementar a consciência sobre os impactos globais dos riscos advindos dessa situação. Disponível em www.weforum.org.
3. A argumentação foi baseada no mapa de interconexão de riscos apresentado por Klaus Schwab, disponível em: www.weforum.org
4. Cf. MC 422/1 – OTAN Military Policy on Information Operations.

5. *C2W- Command and Control Warfare – essa designação é empregada até os dias de hoje, pelas Forças Armadas dos EUA.*
6. *Cf. Allied Joint Doctrine AJP-01(B) (2000).*
7. *Nem o AJP-01, nem o MC 422/1 abordam aspectos táticos relativos à condução das Operações de Informação. Isto coube a outra publicação, o MC 348, de 1998, que se concentrou em descrever as atividades de C2W 10, que se apoia nos mesmos cinco pilares da doutrina norte-americana. As “fundações” sobre as quais se assentam estes pilares são constituídas pelas informações (todos os aspectos) e pelas Comunicações e Sistemas de Informação.*
8. *É importante observar que a OTAN visualiza as Op Info sendo desenvolvidas ao longo de todo o espectro do conflito (paz, crise, guerra e pós-guerra) e nos três níveis de condução das operações (estratégico, operacional e tático). No entanto, sua condução sempre irá requerer uma orientação político-estratégica. Esta situação faz com que, normalmente, o planejamento das Op Info esteja restrito aos níveis estratégico e operacional.*
9. *Fonte: AJP 3-10, 2009. Tradução Livre.*
10. *No que diz respeito aos Sistemas de Informação, o FM 100-6 já apresentava uma descrição das suas funções e do seu papel na condução das operações, distinguindo os sistemas militares dos sistemas civis e expondo alguns aspectos relacionados com a sua gestão e segurança.*
11. *A primeira Revisão Quadrienal de Defesa pós-atentados de 11 de setembro de 2001 identificou as Op Info como um dos seis objetivos operacionais críticos para a transformação das Forças Armadas dos EUA, refletindo a visão de o Estado é o responsável pela definição da política de Op Info, durante as crises e conflitos armados. Este documento apontava para a necessidade de as Op Info serem tratadas não apenas como facilitadoras das atividades conduzidas mas, essencialmente, como uma capacidade fundamental, ao lado das operações aéreas, terrestres, marítimas e das operações especiais, condicionadoras do sucesso operacional das futuras Forças Armadas.*
12. *O então Secretário de Defesa, Donald H. Rumsfeld, aprovou a Information Operations Roadmap (Diretriz para o Desenvolvimento das Op Info, em tradução livre), publicada pelo Departamento de Defesa dos EUA, disponível em <http://www.iwar.org.uk/iwar/resources/io/io-roadmap.pdf>.*
13. *A publicação conjunta JP 3-13 segue detalhando atribuições e formas de atuação para cada uma das capacidades fundamentais, de apoio e relacionadas das Op Info, que foram anteriormente citadas, o que foge ao objetivo do presente artigo. Porém, é interessante destacar o perfeito alinhamento de pensamento entre os níveis político, estratégico, operacional e tático, que embora tenha demorado mais de duas décadas para ser atingido, hoje pode servir de modelo como consciência de defesa para o estamento político de qualquer nação do planeta.*
14. *Integrar e sistematizar a gestão de informações advindas de órgãos e sistemas distintos como o os Centros de Inteligência, de Defesa Cibernética, de Comunicações e Guerra Eletrônica do e de Comunicação Social do Exército é parte do desafio. Será preciso adotar meios de gestão das informações que façam esses dados chegarem aos estados-maiores com oportunidade, para que sejam filtrados, analisados e integrados, produzindo o conhecimento necessário ao decisor. Integrar as Informações das diversas fontes é, portanto, uma forma de gestão de dados que vai além do simples acesso e do somatório das informações gerados por qualquer um dos órgãos citados, individualmente. É, de fato, uma questão de gestão do conhecimento, no seu sentido mais amplo.*
15. *O emprego de alguns atuadores próprios das operações de informação pode contribuir para reduzir a destruição física associada ao fenômeno da guerra, mas não podem alterar as consequências legais e diplomáticas a ela associadas.*
16. *Hoje, atores estatais e não estatais podem empregar uma equipe de “hackers” e desenvolver ataques contra as redes de computadores que suportam as infraestruturas críticas nacionais. Estes sistemas poderão ter um potencial destrutivo semelhante ao obtido com a utilização de sistemas de armas dispendiosos e, eventualmente, com uma probabilidade de sucesso mais elevada associada ao seu emprego. Nesse âmbito, existe também uma elevada probabilidade de que um ataque de informação possa ser conduzido fora do ambiente militar tradicional, sem que seja necessária a condução de ataques convencionais por parte de um Estado ou de atores não estatais.*