

# O Sistema Operacional “Informações”, no Exército Brasileiro

Tenente-Coronel Sérgio Luiz Gomes de Melo, Exército Brasileiro

**A** NOVA DIRETRIZ GERAL do Comandante do Exército (Dtz Ge Cmt Ex) determina a realização de estudos para “a concepção de um Sistema Operacional ‘Informações’” (SOI). Esse sistema “absorveria o atual de Inteligência e incorporaria as áreas de Guerra Eletrônica, Defesa Cibernética, Operações Psicológicas, Comunicação Social, Assuntos Cíveis e Operações de Dissimulação, dentre outras”. Assim, e independentemente do grau de familiaridade que se tenha sobre o tema, é difícil não reconhecer que essa prescrição guarda o potencial de desencadear debates inéditos no âmbito da Força, a ponto de, inclusive, contribuir com o nosso atual processo de transformação.

Por outro lado, parece lógico que essa mesma prescrição decorre de necessidades visualizadas pelo Exército, seja em razão de experiências próprias ou em consequência da observação dos acontecimentos e tendências mundiais. Nesse sentido, desperta a atenção o fato de o “Sistema Operacional Informações” ter muita afinidade com a compreensão básica que as Operações de Informações (Op Info) vêm assumindo nos âmbitos nacional e internacional. Portanto e não obstante a existência de diferentes conceitos para essas operações<sup>1</sup>, tem-se que esses compartilham a premissa de integração de capacidades envolvidas no trato das informações. A finalidade dessa integração seria assegurar melhores condições para o cumprimento da missão, o que, grosso modo, configuraria uma “superioridade de informação”<sup>2</sup>.

A partir desses entendimentos, os argumentos a seguir abordam possíveis condicionantes dos estudos para a concepção do “Sistema

Operacional Informações”, o que ocorre por meio da articulação de aspectos relacionados ao papel das informações nos conflitos recentes, à integração de capacidades no contexto das Operações de Informações e, ainda, à concepção sistêmica da Força.

## As Informações nos Conflitos Recentes

Em função das peculiaridades deste ensaio, cabe enfatizar que a expressão “conflitos recentes” está implicada com a compreensão de “Era do Conhecimento”. Essa assertiva é importante não só porque pressupõe que a efetividade dos empreendimentos humanos nunca esteve tão dependente das tecnologias da informação (TI), como também porque se baseia na constatação de que as inovações tecnológicas ocorrem de forma conexas a significativas mudanças nos campos social, político, econômico e militar.

Em termos de Defesa, tais reflexões demandam quatro entendimentos complementares. O primeiro é que a utilização de modernos sistemas de informação potencializa as capacidades bélicas e oferece vantagens substanciais em relação a oponentes que não disponham ou que sejam impedidos de usufruir desses recursos. Nesse sentido, tão importante quanto as consequências que tal condição pode trazer para as ações de combate é o fato de as vantagens em questão terem também efeitos dissuasórios ponderáveis, uma vez que forças acentuadamente desfavorecidas buscariam evitar um quadro conflituoso como o vivido, por exemplo, na Guerra do Golfo (1990-1991).

Naquele conflito, que pode ser considerado um ícone da transformação das guerras convencionais

---

*O Tenente-Coronel Sérgio Luiz Gomes de Melo, do Exército Brasileiro, serve atualmente como instrutor convidado na Escola de Operações Psicológicas do Exército do Peru, onde ministra a matéria “Operações de Informações”. É Doutor em Ciências Militares, sendo também especialista em Guerra*

*Eletrônica, Operações Psicológicas e em Comunicação Social. Exerceu funções nas áreas de Comando e Controle, Operações Psicológicas e Comunicação Social e foi assessor para assuntos de Operações de Informações do Gabinete do Comandante do Exército.*

modernas, as disparidades tecnológicas ficaram patentes e se manifestaram, dentre outras formas, na superior consciência situacional oferecida pelo sistema de comando e controle (C2) das tropas da coalizão e, também, no ganho de efetividade de diversos sistemas de armas, o que em boa medida deveu-se à incorporação de modernas TI aplicadas à busca, identificação, monitoramento e neutralização de alvos em toda a sua diversidade.

Em termos sintéticos, a Guerra do Golfo não só ratificou o imperativo mundial de que os exércitos devem desenvolver, aplicar e integrar tecnologias da informação, como também demonstrou que a superioridade tecnológica pode contribuir sobremaneira para a abreviação dos conflitos convencionais, além de reduzir as perdas e os efeitos colaterais da atuação de forças amigas. Portanto, não é por menos que aquele conflito recebeu por parte de alguns a adjetivação propagandística de “guerra cirúrgica”, a qual vai ao encontro da baixa tolerância da opinião pública mundial aos conflitos violentos, demorados e de grande escala destrutiva.

O segundo entendimento complementar constitui-se em ressalva ao anterior e serve para agregar maior complexidade ao tema. Assim, cabe reconhecer que as vantagens tecnológicas não podem ser tomadas como suficientemente decisivas e absolutas, embora sejam uma meta irrenunciável para qualquer força armada. Em outras palavras, isso significa que as variáveis de um conflito vão além do campo tecnológico e que o domínio da tecnologia admite brechas.

A esse respeito, tem-se que os embates modernos, como os mais recentemente vividos no Iraque e no Afeganistão, evidenciam que forças dotadas de meios convencionais inferiores tanto podem se manter em luta durante um longo tempo, como também seguem atualizando seus procedimentos e encontrando espaço para fazer uso de modernas tecnologias da informação. Note-se que a telefonia celular, as câmeras digitais e a internet são recursos amplamente disseminados, cada vez mais acessíveis e têm se prestado, por exemplo, às atividades clandestinas de C2, ao acionamento remoto de dispositivos explosivos, à Inteligência, à agitação e à propaganda eletrônica em escala mundial.

Por um lado, é certo que os conflitos assimétricos de hoje continuam validando posicionamentos

consagrados em longa data, como é o caso da propaganda pela aceitação, apoio e adesão populares aos posicionamentos de cada uma das partes em confronto<sup>3</sup>. Por outro lado, no entanto, as TI atuais exigem adaptações e permitem evoluções que, vale ressaltar, não recaem somente sobre os menos favorecidos em poder bélico convencional, mas também justificam o fato de forças mais poderosas aperfeiçoarem suas formas de atuação, o que se comprova pelas recentes modificações nas práticas estadunidenses de contrainsurgência.

O terceiro entendimento complementar diz respeito ao fato de as novas tecnologias da informação seguirem diversificando as possibilidades de engajamento nos conflitos. No tocante à Guerra Eletrônica, essa afirmação encontra um exemplo notável, especialmente quando são considerados os avanços das últimas décadas, o que inclui possibilidades de emprego envolvendo enlaces “*wireless*” próprios à telefonia móvel e às redes de computadores<sup>4</sup>.

Por sua vez e além das modernas formas de utilização do espectro eletromagnético — cuja relação com a Guerra Eletrônica é bastante evidente — cabe destacar que a própria expressão “redes de computadores” já conforma em si outro exemplo de nova possibilidade de engajamento nos conflitos. Neste caso, em um ambiente definido como cibernético.

Os consideráveis impactos vividos pela República da Geórgia, em 2008, após os ataques cibernéticos simultâneos à ofensiva militar russa naquele país<sup>5</sup>, assim como os efeitos do *worm STUXNET* sobre o Programa Nuclear Iraniano, em 2010<sup>6</sup>, são dois exemplos que ilustram com muita clareza a exploração da dependência das sociedades modernas pelas tecnologias da informação. Assim, não é difícil concluir sobre os perigos de eventuais deficiências em segurança das redes de informática que suportam setores críticos da grande maioria dos países, tais como energia, finanças, transportes e telecomunicações.

Ademais e compartilhando as características das ações cobertas<sup>7</sup> tradicionais, os ataques cibernéticos citados atestam que atos hostis podem ser preparados e/ou desencadeados em períodos que antecedem o reconhecimento de beligerâncias ou conflitos armados, ou seja, em períodos anteriores à declaração formal de eventuais teatros de operações (TO). Consequentemente, também



*Uma patrulha acompanha a viatura que faz a disseminação de mensagens por alto-falante em Cité Soleil, 1º semestre de 2011.*

não é difícil reconhecer a validade das iniciativas assumidas por alguns países — incluindo o Brasil — para o desenvolvimento de técnicas, regulamentações e estruturas militares dedicadas à Defesa Cibernética desde o tempo de paz.

O último e não menos importante entendimento complementar corresponde ao fato de as atuais tecnologias da informação sustentarem cada vez mais a compreensão macluhiana<sup>8</sup> de “aldeia global”, ou seja, as TI seguem contribuindo para a ampliação das interações em termos planetários e, obviamente, seguem contribuindo para a maior consciência dessas interações.

Na prática, essa afirmação tem como dois de seus principais desdobramentos: o aumento da importância da opinião pública no contexto dos conflitos modernos e a articulação de pequenos grupos que, operando em redes, chegam a conformar organizações capazes de interferir sobremaneira em dinâmicas conflituosas. Vale notar que algumas dessas organizações alcançam uma visibilidade comparável à de outros

importantes atores internacionais, tais como governos e grandes corporações econômico-financeiras.

Especificamente em termos de formação de opinião, é certo que os posicionamentos assumidos pelo público são consequência da qualidade e da quantidade das informações por ele acessadas<sup>9</sup>. Assim, não se pode deixar de reconhecer o papel dos veículos de comunicação de massa nesse processo, o qual já foi evidenciado nas guerras do Vietnã e do Golfo, mas que agora encontra exemplo na atenção frequente da mídia sobre as divergências internacionais quanto ao Programa Nuclear Iraniano. Neste caso, a cobertura ampla e diversificada dos órgãos da imprensa mundial tem contribuído para a conscientização pública sobre a controvérsia em tela, para a conformação das imagens dos atores envolvidos e, ainda, para o respaldo ou a rejeição das ações e intenções desses atores, sejam essas presumidas ou afirmadas.

Note-se que, uma vez configurada uma tendência geral de posicionamento da mídia

sobre questões conflituosas, é fácil identificar os potenciais reflexos desses posicionamentos na liberdade de ação de cada uma das partes divergentes. Não obstante e ao passo que a mídia pode ser mesmo considerada um “quarto poder”<sup>10</sup>, há que se ponderar que os veículos de comunicação nem sempre obedecem a regras de conduta que garantam níveis sensatos de imparcialidade e precisão. Como exemplo, convém destacar o ataque destrutivo da OTAN à TV estatal líbia, em julho de 2011, a fim de impedir a transmissão de discursos intimidadores e de estímulo à violência civil naquele país<sup>11</sup>.

Já no tocante à constituição de redes de afinidades, é certo que as TI oferecem oportunidades de interação entre pessoas motivadas por questões ideológicas, afetivas e econômicas. Também é certo que tal condição favorece o incremento do ativismo social e político, inclusive em termos transnacionais. Portanto, seria imprudente desconsiderar os reflexos das TI nos engajamentos

populares em questões conflituosas. Note-se que tais engajamentos podem ocorrer dentro e fora dos limites de áreas conflagradas e que, ainda, esses engajamentos podem ou não ser pacíficos, colaborativos, diretos, organizados, patrocinados ou focados em questões precisas e claras. Existem vários exemplos que melhor contextualizam e facilitam a compreensão da presente assertiva. Dois serão destacados neste ensaio.

O primeiro diz respeito à conformação de redes internacionais de *hackers* em apoio à causa palestina<sup>12</sup>, o que sugere que tais *hackers* não somente tiveram acesso a informações e formularam opiniões sobre o conflito em tela, como também sugere que eles puderam ser “recrutados” e coordenados “virtualmente” até o ponto de desfecharem ataques que, partindo de diversos países, chegaram a afetar redes estadunidenses e de Israel.

Como segundo exemplo, as redes sociais, sustentadas pelos modernos recursos de telefonia



Autor: Dst Op Psc BRABAT 1/14

Mulher observa um cartaz produzido pelo BRABAT, durante distribuição de alimentos à população. O cartaz concita a população a denunciar os criminosos, 1º Semestre de 2011.

celular e pela internet, tiveram um papel central tanto na “Primavera Árabe” quanto nos distúrbios civis de agosto de 2011, na Inglaterra. Quanto à “Primavera Árabe” e de acordo com pesquisa realizada pela Universidade de Washington<sup>13</sup>, governos não só foram surpreendidos como caíram ante o ímpeto de ações incitadas, organizadas e divulgadas por meio de redes operadas eletronicamente. No segundo caso e conforme publicou o jornal *Estado de São Paulo*<sup>14</sup>, o Governo britânico não só apresentou ao Parlamento uma proposta para regularizar o emprego das Forças Armadas em caso de distúrbios internos, como também estuda “a possibilidade de o Estado ter autoridade para derrubar redes sociais e bloquear mensagens de celular”.

Portanto, conclui-se que, em nossos dias e de forma incomparável aos acontecimentos passados, as forças militares que atuam na solução de conflitos tanto usufruem das modernas TI, como também são afetadas e afetam outros atores em função do tratamento dispensado às informações em amplo espectro. Nesse contexto, as possibilidades e os riscos são grandes, diversificados e notadamente impõem desafios de evolução em circunstâncias nas quais o papel das informações se mostra cada vez mais importante.

## A Integração de Capacidades

A visualização expressa pelo Comandante do Exército acerca do SOI apresenta um ponto claramente comum em relação à essência das Op Info, ou seja, o destaque atribuído à integração de capacidades distintas, tais como Guerra Eletrônica, Operações Psicológicas, Defesa Cibernética e Assuntos Cívicos, dentre outras. Nesse contexto, duas premissas básicas podem ser adotadas como fundamentos para o referido destaque.

A primeira corresponde ao fato de a produção e o processamento das informações facultarem o reconhecimento de um “ambiente informacional”, o qual congrega três dimensões interdependentes: física, lógica e psicológica<sup>15</sup>. Sinteticamente, a dimensão física — e não necessariamente material — comporta elementos tais como: instalações de apoio, sensores, torres de transmissão, dispositivos de memória, documentos em papel, telas de projeção de imagens, ondas de rádio, etc. Por sua vez, a dimensão lógica não só sustenta as

relações de significação inerentes às informações, como também se expressa por meio das rotinas e dos processos de fluxo das informações. Finalmente, a dimensão psicológica enquadra a atividade mental relacionada aos processos perceptivos, motivacionais e de formação de atitudes, a qual faz com que decisores, atuadores e o público em geral se comportem de uma forma coerente à realidade percebida.

A segunda premissa básica é um desdobramento da primeira e corresponde ao entendimento de que, havendo mudanças em qualquer uma das dimensões que compõem o “ambiente informacional”, diferentes serão os efeitos produzidos na realidade dos conflitos. Em outras palavras, distintas combinações de emprego das capacidades envolvidas pelas Op Info podem afetar de maneira diferenciada uma ou mais dimensões do ambiente informacional e, assim, produzir efeitos desejáveis em circunstâncias conflituosas.

Como ilustração, cabe considerar um exemplo hipotético, mas que apropria relatos de experiências vividas em Sirte, na Líbia<sup>16</sup>, e em Najaf e Fallujah, no Iraque<sup>17</sup>. Trata-se de uma cidade ALFA, a qual se acha compreendida pelos limites de um teatro de operações ativado.

De imediato e considerando apenas uma pequena parcela das implicações possíveis, são facilmente identificáveis as demandas de controle da população civil e de satisfação de suas necessidades humanitárias. Essas demandas seriam naturalmente agravadas à medida que: elementos hostis operassem clandestinamente em meio à população; as instituições sociais de ALFA entrassem em colapso; os habitantes locais fossem afligidos por rumores decorrentes da carência de informações confiáveis; ou, ainda, que a população fosse submetida à agitação adversa por meio da mídia eletrônica ou irradiada.

Nesse contexto, as consequências para o campo militar não seriam difíceis de visualizar e poderiam, por exemplo, se manifestar em maiores esforços operacionais, logísticos e de preparo em ações de controle de distúrbios, como também poderiam se materializar em fluxos desordenados de deslocados ou em protestos civis que, ocorrendo sobre eixos de progressão, acarretariam o atraso de forças em aproveitamento do êxito, implicariam maiores desgastes físicos, psicológicos e de imagem às tropas amigas e,

ainda, comprometeriam a segurança e a eficiência das atividades de apoio logístico a essas tropas.

Assim e tendo em conta as premissas básicas anteriormente expostas, é possível considerar que os indesejados efeitos do pânico civil ou da “agitação” no teatro de operações poderiam ser minorados de diversas formas. Uma das possibilidades seria a difusão de esclarecimentos e orientações à população, ao mesmo tempo em que esforços seriam executados para desacreditar as fontes adversas de informações falsas. Para tanto, poder-se-ia contar com ações integradas de Operações Psicológicas, de Comunicação Social ou mesmo de Inteligência, ao passo que esta atividade recebesse encargos correspondentes, a exemplo dos relatos envolvendo práticas dos Estados Unidos<sup>18</sup> e da extinta União Soviética<sup>19</sup>.

No entanto e caso tais esforços não fossem suficientes, a capacidade de agitação adversa por meios irradiados (rádio, TV e redes de telefonia celular) poderia ser afetada pela destruição física de antenas transmissoras, tal como fez a OTAN na Líbia, ou por meio do bloqueio de sinais realizado pela Guerra Eletrônica, respeitando-se obviamente as capacidades técnicas e operacionais dos equipamentos correspondentes. Indo mais além, é evidente que quanto mais efetiva a atuação das estruturas de Assuntos Civis maior seria a atenuação das circunstâncias exploradas pela agitação adversa.

Embora complexo, o quadro de integração de capacidades aqui apreciado nem de longe esgota os desdobramentos das circunstâncias do TO, ou mesmo de ALFA, o que evidencia que as coordenações e as combinações possíveis vão muito além das capacidades e dos efeitos aqui exemplificados. Neste caso, conforma-se uma situação intrincada, cujo equacionamento não só implica a consideração de riscos e ameaças, como também deve respeitar as possibilidades dos meios disponíveis, além de ter em conta a multiplicidade e a mudança de prioridades ao longo da manobra. Em especial, tal condição aumenta de importância, à medida que são consideradas eventuais limitações das capacidades à disposição.

Em termos práticos e ilustrativos, isso significa dizer que as ações de contra-agitação em ALFA poderiam contar inicialmente com os esforços preponderantes das Operações Psicológicas e

da Inteligência, visto que as demais capacidades estariam prioritariamente empregadas no atendimento de outras demandas do teatro de operações. É o que se pode exemplificar por meio da Guerra Eletrônica que, durante uma ofensiva militar, estaria mais dedicada a afetar os sistemas de armas e de comando e controle das forças convencionais inimigas. Seja como for, fica caracterizada a necessidade de medidas de C2 que, em função das prioridades dos efeitos desejados, dimensionem adequadamente e melhor combinem as capacidades disponíveis e que, ainda, coordenem as necessárias sincronias e transições de esforços de forma oportuna e sem transtornos.

Note-se que a grande complexidade por ora visualizada ajuda a explicar iniciativas como as adotadas pelos Estados Unidos no que se refere às Op Info<sup>20</sup>. Assim e não desconsiderando que existem relatos sugerindo possibilidades de aperfeiçoamentos<sup>21,22</sup>, cabe destacar a existência de manuais específicos (“JP 3-13” e “FM 3-13”), os quais buscam regular a sistemática de emprego dessas operações. Igualmente, deve-se salientar o estabelecimento de estruturas dedicadas às Op Info, tal como ocorre em relação ao 1º Comando de Operações de Informações do Exército<sup>23</sup> e às “células” de Operações de Informações dos estados-maiores conjuntos, as quais recebem a designação de “J39” (Figura 1).

Também em termos estruturais e de um modo especial, a criação de uma instituição subordinada ao Comando Estratégico dos Estados Unidos (USSTRATCOM) — o Centro de Operações de Informações Conjuntas — faculta o destaque de que as Op Info não são um empreendimento que corresponda apenas a elementos de forças terrestres. Em adição, a existência desse Centro também favorece o destaque de que as Op Info podem ser desencadeadas visando a efeitos fora de eventuais TO e, mais ainda, que tais operações podem ser executadas em períodos que extrapolam o tempo de ativação desses teatros, o que gera a possibilidade de apoio à consecução de objetivos não necessariamente militares. Nesse caso, considerações acerca das Operações Psicológicas nos Estados Unidos ilustram muito bem a presente assertiva:

As Operações Psicológicas (Op Psc) são empregadas tanto durante as operações militares, como também por ocasião de

atividades conduzidas por agências civis. As Op Psc podem ser um recurso vital para as agências de governo em muitas situações em que o Departamento de Defesa não é o órgão coordenador[...] Quando conduzidas no nível estratégico, as Op Psc são designadas para apoiar os departamentos e agências governamentais, os Comandos Combatentes Geográficos ou, ainda, parceiros multinacionais. Tipicamente, as Op Psc conduzidas neste nível são concentradas

no alcance de objetivos estadunidenses ou multinacionais amplos, nas diversas regiões do globo, as quais contam com diferentes públicos. Entretanto, um indivíduo ou líder adversário também podem ser um objetivo estratégico das Operações Psicológicas. No nível estratégico, as forças de Op Psc constituem uma capacidade do Departamento de Defesa empregada como parte de um amplo esforço governamental dos Estados Unidos<sup>24</sup>. (Em tradução livre)

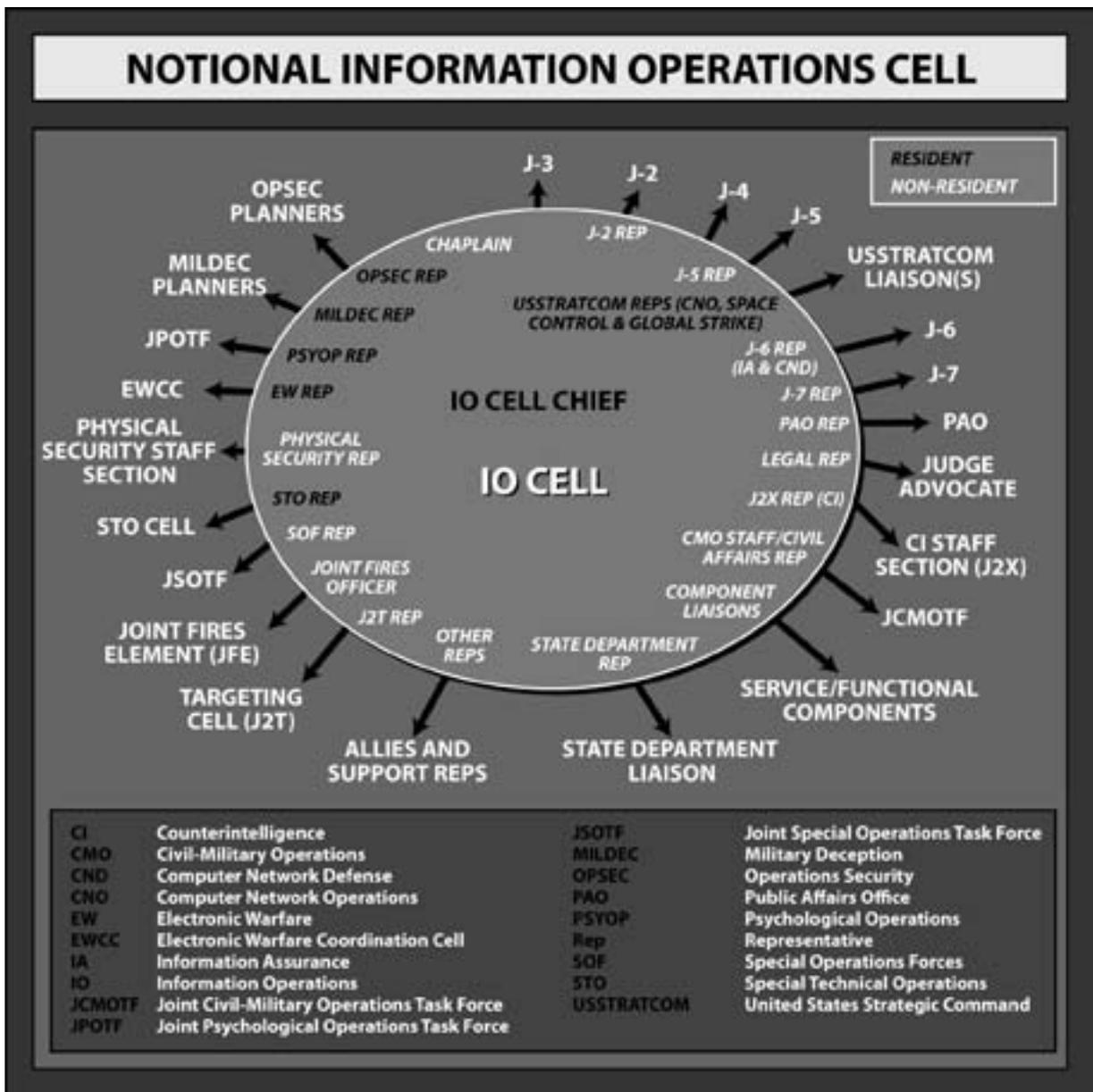


Figura 1 — Concepção Genérica de uma Subseção de “Operações de Informações”

Em resumo, se observa que a integração de capacidades obedece a uma lógica que enfatiza os efeitos pretendidos e que, com base na compreensão de ambiente informacional, busca uma premeditada sinergia de esforços, com vistas à consecução de objetivos comuns estabelecidos pelo nível de decisão considerado. Assim e por exemplo, não se trata tanto de mencionar o apoio da Guerra Eletrônica às Operações Psicológicas, ou vice-versa, mas sim de coordenação de esforços para a obtenção de efeitos prioritários.

## **A Concepção Sistêmica do Exército**

A abordagem da concepção sistêmica do Exército e, em particular, das implicações relacionadas à criação de um “Sistema Operacional Informações” é um desafio considerável. Para tanto, logrou-se o estabelecimento de duas perspectivas com a pretensão de sinteticamente esclarecer as questões suscitadas neste ensaio.

A primeira dessas perspectivas destaca o grau de inovação que o “Sistema Operacional Informações” representaria para a Força, o que impõe a abordagem de posicionamentos praticados nos últimos anos pela Instituição. Assim, deve-se inicialmente ressaltar que a ideia de integração de esforços relacionados às informações (e que ora é enfatizada pelo SOI) não pode ser tomada como absolutamente inédita. A compreensão do Sistema de Informações do Exército (SINFOEx) é um exemplo cabal dessa assertiva, a ponto de sua última atualização oferecer referências imprescindíveis para os estudos em tela<sup>25</sup>. Nesse sentido, a concepção do SOI configuraria uma espécie de reforço a um impulso inovador que já vem sendo maturado no âmbito da Força.

Sendo assim, duas considerações complementares devem ser feitas. Uma delas é que há mais de 10 anos e por meio do SINFOEx, a Força vem preconizando a integração de subsistemas correspondentes a muitas das atividades assinaladas na última Dtz Ge Cmt Ex, tais como Inteligência, Comunicação Social, Guerra Eletrônica e Operações Psicológicas. Desde então, já se reconhecia que

a gestão dos recursos informacionais deve ser realizada de forma sistêmica

por um conjunto de recursos de pessoal, material, instalações, doutrina, normas e procedimentos. As atividades desenvolvidas em cada sistema, embora diferenciadas por suas características e produtos finais específicos, são interdependentes e contribuem, de forma integrada, para a consecução dos objetivos estabelecidos<sup>26</sup>.

A outra consideração complementar é que a nova concepção do SINFOEx (Figura 2) explicita o Sistema de Informações Operacionais Terrestres (SINFOTER) como sistema que produz, integra e disponibiliza as informações operacionais necessárias ao preparo e emprego da Força Terrestre e, mais ainda, que esse sistema interage com o Sistema de Informações Organizacionais do Exército (SINFORGEEx) na

produção do conhecimento necessário ao processo decisório nas situações de paz, crise ou conflito armado/guerra, respeitadas as normas de acesso e segurança da informação, e desdobram-se nos níveis de planejamento estratégico, operacional e tático<sup>27</sup>.

Consequentemente e tomando também como referência a definição doutrinária de sistemas operacionais<sup>28</sup>, o desencadeamento de estudos sobre o SOI permite a visualização de que:

- seriam apresentados os eventuais relacionamentos entre o SOI e o SINFOTER, assim como seria equacionado o fato de o SOI enquadrar interações entre sistemas de primeira ordem na Força, notadamente, os sistemas de Inteligência e de Comunicação Social. Decerto, tudo isso remete a questões de modelagem de processos e de arquitetura sistêmica no âmbito institucional;

- os estudos acerca do SOI, por definição, tenderiam a destacar a integração de atividades em suporte aos níveis de decisão tático e operacional, o que deixaria para outras instâncias sistêmicas o tratamento específico de questões relacionadas ao nível estratégico. Nesse caso, não deixa de ser instigante a determinação de estudos para a criação de um órgão de direção setorial “Informações”<sup>29</sup>;

- seria equacionado o fato de o SOI envolver atividades com níveis variados de consolidação sistêmica. Condição essa que é suscitada, por

Fonte: Portaria do Comandante do Exército Nº 445, de 14 de junho de 2010

<b>ÁREAS DE ATIVIDADES DO EB</b>		<b>OPERACIONAL</b>	<b>PESSOAL</b>	<b>EDUCAÇÃO E CULTURA</b>	<b>ECONOMIA E FINANÇAS</b>	<b>CIÊNCIA E TECNOLOGIA</b>	<b>LOGÍSTICA</b>	<b>MOBILIZAÇÃO</b>	<b>CONSTRUÇÃO</b>	<b>INTELIGÊNCIA</b>	<b>COMUNICAÇÃO SOCIAL</b>		
<b>ÓRGÃOS GESTORES</b>		<b>COTER</b>	<b>DGP</b>	<b>DECEX</b>	<b>SEF</b>	<b>DCT</b>	<b>COLOG</b>	<b>DGP/COLOG</b>	<b>DEC</b>	<b>CIE</b>	<b>CCOMSEX</b>		
<b>NÍVEIS DE PLANEJAMENTO</b>	<b>ESTRATÉGICO</b>	<b>S</b>	<b>S I N F O E X</b>										
	<b>OPERACIONAL</b>											<b>SINFOTER</b>	<b>SINFORGE<sub>x</sub></b>
	<b>TÁTICO</b>												
<b>INFRAESTRUTURA</b>		<b>SISTEMA DE COMUNICAÇÕES DO EXÉRCITO (SICOME<sub>x</sub>)</b>											
<b>GESTÃO</b>		<b>SISTEMA DE TECNOLOGIA DA INFORMAÇÃO DO EXÉRCITO (SITIE<sub>x</sub>)</b>											
		<b>SISTEMA DE EXCELÊNCIA GERENCIAL DO EB (SE-EB)</b>											

**Figura 2 — SINFOEX**

exemplo, pelas recentes modificações vividas pela Força em termos de Defesa Cibernética e de Operações Psicológicas;

- tais estudos poderiam identificar eventuais necessidades de inovações ou aprofundamentos das prescrições já estabelecidas no âmbito da Força, o que levaria a uma descrição ainda mais clara e precisa das medidas relativas ao “como” operar a integração pretendida. Essa visualização assume especial importância, uma vez que as ações correspondentes deverão envolver os já citados: “recursos de pessoal, material, instalações, doutrina, normas e procedimentos”;

- em função da assertiva anterior e com base na Teoria Geral dos Sistemas (TGS)<sup>30</sup>, a concepção do SOI não traria reflexos apenas para o Sistema Operacional Inteligência, mas também teria efeitos em outros sistemas operacionais.

- em complemento ao que já foi estabelecido em relação ao SINFOTER e segundo o significado de “superioridade de informação”, os estudos sobre o SOI poderiam enfatizar os limites e as possibilidades de adoção de medidas ativas para negar ao adversário o efetivo uso de suas capacidades relacionadas ao ambiente informacional;



Fonte: Arquivo do CCOMGEX

*Um militar do Exército Brasileiro opera equipamentos do terminal rebocado do Sistema de Comunicações Militares por Satélite (SISCOMIS).*

- poderia levar ao enquadramento de novos subsistemas pelo SINFOEx, como, por exemplo, o de Defesa Cibernética.

Avançando um pouco mais na primeira perspectiva de abordagem da concepção sistêmica da Instituição e levando em conta as atividades de preparo e emprego da Força, não se pode deixar de considerar a recente atuação do Exército em operações no Complexo do Alemão (Rio de Janeiro-RJ) como uma evidência de integração de capacidades envolvidas com o ambiente informacional. A esse respeito, convém citar a matéria publicada pelo portal de notícias UOL<sup>31</sup>, a qual identifica ações de emprego coordenado da Inteligência, de alto-falantes para orientação da população e de medidas de relacionamento com a mídia, além do registro audiovisual das ações militares, a fim de “preservar a tropa” de denúncias infundadas.

Sendo então possível identificar que experiências exitosas já ocorrem antes da concepção do SOI, três questões cruciais se

apresentam: o modelo de integração aplicado pela Força em suas recentes atuações — o que também inclui sua participação no Haiti antes e depois do terremoto — pode ser suficientemente reproduzido em outras circunstâncias de emprego visualizadas? Se aperfeiçoamentos ou inovações são necessários, existiriam, além do SOI, outros caminhos para melhor alcançar a integração pretendida? Em que medida esses caminhos seriam complementares, redundantes ou mutuamente excludentes?

Muito provavelmente as questões aqui suscitadas serão exploradas, de uma forma ou outra, nos estudos determinados pelo Comandante do Exército. Por ora e em razão da complexidade que o assunto envolve, é muito difícil imaginar que alguém possa dispor de respostas prontas. Em essência, o que está em jogo são o dimensionamento e os procedimentos de articulação de capacidades, de modo que a Força esteja em condições de superar oportunamente suas exigências de emprego. Exigências essas que podem

evoluir, em especial, à medida que avanços tecnológicos se processem ou que se confirmem as expectativas de que o Brasil assumirá novos papéis no contexto internacional.

Passando agora à segunda perspectiva de abordagem da concepção sistêmica da Força, temos como certo que essa corresponde a uma noção básica de limites aplicáveis ao SOI. Nesse sentido, é evidente que a Instituição tem certa liberdade para promover modificações de ordem interna e que muitas medidas podem ser aplicadas em curto prazo. A questão decorrente é que eventuais mudanças, motivadas ou reforçadas pelo SOI, poderiam produzir impactos diversificados e com isso abranger diversas áreas, tais como recursos humanos, estrutura, gestão e doutrina<sup>32</sup>. Assim, é possível que eventuais modificações demandem tempo para serem processadas, o que faz ressaltar a importância dos “contratos de estratégias” preconizados pela nova Dtz Ge Cmt Ex, além de outros instrumentos de gestão estratégica institucional.

Por outro lado, a questão de limites também tem a ver com o ambiente externo à Força. Em outras palavras, o “Sistema Exército” também deve ser percebido como um subsistema, cujas ações devem ser coerentes com as condicionantes estabelecidas pelos suprasistemas institucionais. Em termos ilustrativos, considera-se que os estudos sobre a concepção do SOI certamente levarão em conta as prescrições do MD (“Suprasistema Defesa”) acerca das Operações de Informações, assim como as políticas daquele ministério para a Guerra Eletrônica e a Comunicação Social, por exemplo. De igual modo e constatando que algumas atividades envolvidas pelo SOI compreenderiam possíveis ações de natureza sensível, há que se considerar o balizamento legal que respalde tais ações. Como último exemplo, aspectos de ordem orçamentária provenientes do ambiente externo também poderão compor o rol de condicionantes dos estudos acerca da concepção do SOI, especialmente, no que se refere ao escalonamento de eventuais metas onerosas de longo prazo.

Cabe enfatizar, no entanto, que a existência de limites como os assinalados não impõe à Força um papel meramente reativo em seus

relacionamentos externos. Decerto, existe uma dimensão pró-ativa e que seguramente já vem sendo conformada pela Força, a exemplo do que segue ocorrendo no contexto do Setor Cibernético de Defesa. Nesse sentido, não é difícil visualizar que o SOI, ou qualquer outra solução apresentada, assumiria a condição de “sistema emergente” e levaria os suprasistemas da Força a adotarem medidas compatíveis com as demandas fundamentadamente suscitadas pela Instituição. Naturalmente, tudo isso envolveria um esforço de “comunicação estratégica” criterioso, não desprezível e bastante objetivo.

Em resumo, a integração de capacidades previstas para o SOI ao mesmo tempo em que encontra no SINFOEx um importante precedente institucional, apresenta um inequívoco potencial de transformação da Força. Ademais, é possível visualizar que a implementação desse sistema estaria condicionada a uma concepção consistente, econômica e suficiente para a superação de importantes desafios da Força e, em termos mais amplos, do País.

### Conclusões

Este ensaio evidenciou que os estudos acerca do SOI encontram respaldos em imperativos da Era do Conhecimento, em tendências internacionais e em precedentes relacionados ao SINFOEx. Igualmente, constatou-se que tais estudos podem levar a relevantes impactos no plano institucional, especialmente, à medida que esses corroborem a imprescindibilidade da integração de capacidades relacionadas ao trato das informações.

Além da possível incorporação do “Sistema Operacional Inteligência”, antecipada na própria Dtz Ge Cmt Ex que determinou os estudos acerca do SOI, a eventual implementação deste sistema permite a visualização de outros efeitos concretos para o Exército, os quais certamente vão demandar maior familiarização e capacitação dos quadros da Força. Como desdobramentos específicos, é possível estabelecer a revisão e a elaboração de manuais, a adequação dos temas aplicados em nossas escolas e em nossos exercícios de adestramento e, por fim, mudanças na própria sistemática de organização, planejamento e emprego real da Força Terrestre. Neste caso, cabe

ressaltar que as mudanças presumidas vão estar relacionadas, por definição, aos níveis operacional e tático, o que provavelmente deixará em aberto um estudo específico quanto ao nível estratégico.

Por outro lado, os estudos sobre o SOI têm o claro potencial de atrair a atenção para um conjunto de atividades, todas inegavelmente importantes, mas que, por ora, possuem níveis distintos de consolidação no plano institucional. O eventual refinamento do equilíbrio entre as capacidades pertinentes poderá demandar tempo para ser alcançado e, muito possivelmente, terá reflexos nos planejamentos de articulação e de equipamento da Força.

Também será árduo o trabalho de composição de prioridades visando ao aprimoramento das

capacidades envolvidas pelo SOI, especialmente, à medida que se considere o quadro de limitações vivenciado. Tal constatação se torna ainda mais relevante, ao passo que a efetivação desse sistema impõe a abordagem de questões relacionadas a “recursos de pessoal, material, instalações, doutrina, normas e procedimentos”.

Assim, conclui-se que a tarefa definida pela Dtz Ge Cmt Ex é bastante complexa, reforça a posição de destaque do Exército em iniciativas de integração no ambiente informacional e, igualmente importante, pode levar a repercussões práticas de transformação da Força, o que, por fim, levaria a melhores condições de cumprimento de sua missão constitucional. **MR**

## REFERÊNCIAS

1. OTAN. RESEARCH AND TECHNOLOGY ORGANISATION. *Information Operations – Analysis Support and Capability Requirements*. 2006. Disponível em: <<http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-SAS-057//SSTR-SAS-057-TOC.pdf>>. Acesso em: 17 mai. 2009.
2. Como adaptação do Manual JP 1 – 02 (*Department of Defense Dictionary of Military and Associated Terms*), considerar-se-á como superioridade de informação a conquista de uma vantagem relativa — permanente ou episódica, total ou limitada — tanto em termos de coleta, processamento e difusão de um fluxo contínuo de informação, quanto em termos de exploração ou negação das capacidades de eventuais adversários em fazer o mesmo.
3. HEYDTE, Friedrich A. Von Der. *A Guerra Irregular Moderna*. Rio de Janeiro: Biblioteca do Exército Editora, 1990.
4. Conf. <[http://www.darpa.mil/Our\\_Work/STO/Focus\\_Areas/Communications\\_Networks\\_and\\_Electronic\\_Warfare.aspx](http://www.darpa.mil/Our_Work/STO/Focus_Areas/Communications_Networks_and_Electronic_Warfare.aspx)>. Acesso em: 15 nov. 2011.
5. SHAKARIAN, Paulo. “The 2008 Russian Cyber Campaign Against Georgia”, *Military Review*. p. 63-68, nov./dez. 2011 (também publicado na Edição brasileira da *Military Review* de nov./dez. 2011, sob o título “Análise da Campanha Cibernética da Rússia Contra a Geórgia”, em 2008, p. 67-73).
6. Como sugestão de leitura complementar, tem-se a matéria “O desafio mundial da cibersegurança”, publicada pelo jornal *Estado de São Paulo*. Disponível em: <<http://www.estadao.com.br/noticias/impresso,o-desafio-mundial-da-ciberseguranca,685882,0.htm>>. Acesso em: 01 mar. 2011.
7. Ações “cobertas” serão aqui entendidas como atividades que demandam medidas para a negação de conhecimentos que despertem a atenção sobre a ação em si ou que permitam a identificação de seus verdadeiros propósitos e/ou autoridades. Para o caso dessas ações serem reconhecidas pelo adversário, os dados produzidos poderiam, no máximo, levar a suposições e não a comprovações de seus executores, patrocinadores ou intentos.
8. McLUHAM, Marshall. *O meio é a Mensagem*. Rio de Janeiro: Record, 1969.
9. WOLF, M. *Teorias da Comunicação*. Lisboa: Editorial Presença, 1999.
10. HUNT, Frederick K. *The Fourth State: Contributions towards a History of Newspapers and of the Liberty of the Press*. London. 1850. Vol. 1. Disponível em: <<http://books.google.com>>. Acesso em 22 nov. 2010.
11. Disponível em: <[http://www.nato.int/cps/en/natolive/news\\_76776.htm](http://www.nato.int/cps/en/natolive/news_76776.htm)>. Acesso em 10 out. 2011.
12. ALLEN, Patrick D.; DEMCHAK, Cris. “A Guerra Cibernética Entre Palestina e Israel”, *Military Review* – Edição Brasileira. p. 51-58, 1º Trim. 2004.
13. Conf. Relatório do *Project on Information Technology and Political Islam*. Disponível em: <<http://pitpi.org/index.php/2011/09/11/opening-closed-regimes-what-was-the-role-of-social-media-during-the-arab-spring/>>. Acesso em: 10 out. 2011.
14. Matéria com o Título “Pacote britânico prevê Exército contra gangues e controle sobre redes sociais”, edição de 12 de agosto de 2011.
15. A presente compreensão foi formulada pelo autor, a partir da análise de diversos entendimentos existentes acerca da expressão “ambiente informacional”.
16. Conf. <<http://g1.globo.com/revolta-arabe/noticia/2011/10/forças-do-governo-da-libia-preparam-ataque-final-cidade-natal-de-kadhafi.html>>. Acesso em 12 out. 2011.
17. Conf. matérias publicadas pelo jornal *Folha de São Paulo*, em 08 de abril de 2004, p. A2.
18. GOLDSTEIN, Cora Sol. “Um fracasso estratégico: A política Norte-Americana de Controle das Informações no Iraque Ocupado”, *Military Review* – Edição Brasileira. p. 52-61, jul./ago. 2008.
19. RADVANYI, Janos (org). *Psychological Operations and Political Warfare in Long-term Strategic Planning*. New York: Praeger Publishers. 1990.
20. Aliás, os Estados Unidos apresentam uma condição peculiar e tratam das Op Info de uma forma destacadamente mais aberta que outros países.
21. RICHTER, Walter E. “O Futuro das Operações de Informações”, *Military Review* – Edição Brasileira. p. 71-82, mai./jun. 2009.
22. FLOR, Leonardo J. “Como Explorar a Energia Potencial das Operações de Informações”, *Military Review* – Edição Brasileira. p. 49-56, set./out. 2010.
23. 1st Information Operations (IO) Command. <<http://www.1stiocmd.army.mil/>>. Acesso em: 04 nov. 2011.
24. JP 3-13.2. *Psychological Operations*. US Joint Publication. 2010. p. I-3 e I-4. Vale ressaltar que atualmente as Operações Psicológicas nos Estados Unidos recebem a designação de *Military Information Support Operations*.
25. A nova concepção do SINFOEx foi aprovada pela Portaria do Comandante do Exército Nº 445, de 14 de junho de 2010.
26. Portaria do Comandante do Exército Nº 459, de 13 de setembro de 2001.
27. Portaria do Comandante do Exército Nº 445, de 14 de junho de 2010.
28. Esses sistemas — que atualmente perfazem um total de sete (comando e controle; inteligência; manobra; apoio de fogo; defesa antiaérea; mobilidade, contramobilidade e proteção; e logístico) — “permitem ao comandante coordenar o emprego oportuno e sincronizado de seus meios no tempo, no espaço e na finalidade”. Tem-se, ainda, que “esses sistemas aplicam-se tanto ao nível tático quanto ao nível estratégico-operacional do combate e facilitam a integração, coordenação, preparação e execução de operações de armas combinadas bem sucedidas”. Conf. BRASIL. Exército. Estado-Maior. C 100 - 5: *Operações*. 3 ed. Brasília, DF, 1997.
29. Portaria do Comandante do Exército Nº 445, de 14 de junho de 2010.
30. BERTALANFY, L. V. *Teoria Geral dos Sistemas*. 2. ed. Petrópolis: Vozes, 1973.
31. Conf. Uol Notícias. Disponível em: <<http://noticias.uol.com.br/cotidiano/2011/10/27/exercito-realiza-nova-operacao-em-busca-de-armas-e-drogas-no-complexo-do-alemao-rj.jhtm>>. Acesso em: 28 out. 11.
32. Conforme sugere a concepção sistêmica do “efeito borboleta”. In: GLEICK, J. *Caos: a criação de uma nova ciência*. 2. ed. Rio de Janeiro: Campos, 1987.