Após transmitirem um anúncio pelo alto-falante, soldados da 213ª Companhia de Op Psc observam a reação ao redor da Estação de Segurança Combinada de Oubaidy, nas proximidades de Cidade Sadr, no Iraque, que havia sido alvo de uma série de ataques de foguetes e morteiros, 29 Mar 08. (Força Aérea dos EUA, Sgt Jason T. Bailey)

As Operações de Informações como um Elemento Dissuasório do Conflito Armado

Cel (Res) Blane R. Clark, Exército dos EUA

Precisamos manter nossas mentes alertas e receptivas à aplicação de métodos e armas não vislumbrados.

—General Douglas A. MacArthur

As Operações de Informações (Op Info) proporcionam ao comandante alternativas dissuasórias não letais e flexíveis. A aplicação das Op Info

dessa forma é viável tanto em relação a adversários estatais quanto a adversários não estatais. O grau de impacto dependerá da capacidade específica que o adversário possuir. As capacidades específicas de Op Info têm o efeito estratégico mais significativo como um dissuasor do conflito quando empregadas durante a "fase I" das operações combinadas. De fato, o objetivo estratégico central das Op Info é deter as ameaças de potenciais adversários[1]. A dissuasão induzida pelas operações de informações compele o adversário a adotar uma política ou tomar uma medida que obtenha ou mantenha a Segurança Nacional dos interesses dos EUA. Essencialmente, as aplicações das Op Info no nível estratégico têm consistido em apenas uma ou duas capacidades específicas como elementos habilitadores táticos, em vez de combinações sinérgicas para um efeito estratégico.

O Cel (Res) Blane R. Clark, Exército dos EUA, atuou como chefe da Divisão de Operações de Informações, Operações (J3), Comando Central dos EUA, de janeiro de 2005 a junho de 2008; como diretor de Operações de Comando, Controle, Comunicações e Computadores (C4) e Operações de Informações; e como instrutor do U.S. Army War College de julho de 2008 a dezembro de 2009. É mestre pela University of Southern California. Atuou em cargos de comando e estado-maior no território continental dos EUA, na Coreia, na Alemanha e no Iraque. O Coronel Clark é atualmente o subcomandante de Operações (J3) da Força-Tarefa Conjunta-Operações de Rede Global (JTF-GNO) e vice-adjunto de Operações Correntes (J33) do Comando Componente Funcional Combinado-Combate de Redes/JTF-GNO, no Forte Meade, Maryland.

As operações de informações planejadas, integradas e executadas como parte do plano de campanha de um comando unificado durante a "fase I" oferecem ao comandante alternativas não letais e "não cinéticas" [neste contexto, são aquelas que não envolvem o emprego de força — N. do T.] para a consecução de objetivos estratégicos. A probabilidade de sucesso durante a "fase I" aumenta quando os comandantes integram as Op Info em ciclos de planejamento deliberados e de ação em crise. Essa integração deve ocorrer desde o início e ser incluída em rigorosos processos combinados para a seleção de alvos. Devem ser desenvolvidas medidas de efetividade que sirvam de base para quaisquer decisões de reiniciar ou pôr fim a ações de Op Info.

A aplicação de Op Info concentradas, integradas e sincronizadas para dissuadir um adversário de seguir uma linha de ação e, com isso prevenir o início de um conflito armado, não constitui um ato de guerra[2]. Contudo, embora não seja um ato de guerra, ela inclui a seleção de alvos. Para que a aplicação das Op Info alcance o efeito dissuasório desejado, três componentes habilitadores devem estar alinhados: as capacidades de engajar e de acessar um alvo e a autoridade para atingi-lo.

Bases para as Operações de Informações

Entre as capacidades militares específicas das operações de informações estão a guerra eletrônica, as operações de redes de computadores, as operações psicológicas, a dissimulação militar e a segurança das operações. Quando devidamente coordenadas e bem focalizadas, elas podem impedir o conflito armado. A meta principal das Op Info no nível estratégico é coagir um líder-chave ou grupo de líderes a desistir de uma ação específica ou a adotar uma medida compatível com os interesses dos EUA[3].

As operações de informações não são a aplicação individual de qualquer uma das capacidades específicas. A integração sincronizada e coordenada de combinações dessas capacidades específicas caracteriza as operações de informações, e isso gera o componente ofensivo "não cinético" da força, que pode impedir o conflito armado.

Guerra eletrônica. Essa capacidade específica é composta de três subdivisões: ataque eletrônico, proteção eletrônica e apoio eletrônico. Todas elas representam ações militares nas quais armas eletromagnéticas ou de energia dirigida controlam o espectro eletromagnético ou atacam um inimigo[4]. Como o foco é na dissuasão, o ataque eletrônico tem a relevância mais direta.

O ataque eletrônico tem como alvo instalações, equipamentos ou efetivos do inimigo para degradar, neutralizar e, se necessário, destruir seus sistemas de apoio eletrônico[5]. Por exemplo, meios de ataque eletrônico aeroterrestres podem efetuar interferência de

comunicações à distância contra a rede integrada de comunicações do sistema de defesa antiaérea do inimigo, de modo que ele sofra uma degradação da capacidade de comando e controle do seu sistema.

> …a Estratégia de Segurança Nacional também aponta para a dissuasão "pelo convencimento" como uma prioridade…

Operações de redes de computadores. A última capacidade específica de Op Info inserida na Publicação Conjunta 3-13, "Operações de Redes de Computadores" (*Computer Network Operations*), conta com três subcomponentes: ataque a redes de computadores, defesa de redes de computadores e exploração de redes de computadores[6]. Mais uma vez, como o foco está em causar um efeito dissuasório, o ataque a redes de computadores representa o subcomponente "gerador de efeitos" mais viável.

O ataque a redes de computadores inclui o uso de redes de computadores para negar, prejudicar ou degradar computadores, redes de computadores ou informações neles contidas. Atualmente, os potenciais grupos adversários dependem cada vez mais de computadores e de redes de computadores para facilitar o comando e controle, possibilitar transações e coordenar ações[7].

O ataque a redes de computadores é uma potencial arma de "perturbação" em massa contra alvos de infraestrutura tanto militares quanto civis[8]. Por exemplo, um ataque de recusa de serviço de internet que consista na introdução de um grande fluxo de dados contra a rede de computadores do inimigo tem o potencial de consumir toda a largura de banda disponível naquela rede e de reduzir consideravelmente ou de impedir seu uso.

Operações psicológicas. Essa capacidade específica consiste em enviar informações que influenciem ou dissuadam as principais lideranças do inimigo e suas estruturas de apoio, para evitar ações adversas subsequentes. As operações psicológicas são mais bem empregadas como uma capacidade integrada de Op Info em apoio às operações da "fase I"[9]. As operações psicológicas influenciam as populações estrangeiras e neutralizam as mensagens do adversário[10]. As mensagens transmitidas por rádio de ondas curtas, alertando a população em geral que as ações de seus líderes podem resultar na ação militar, são um exemplo. Dentro do Departamento de Defesa, apenas as Forças de operações psicológicas têm autorização para influenciar públicos-alvo estrangeiros com o uso de diversos mecanismos de envio por rádio, mídia impressa e outros tipos de mídia[11].

Dissimulação militar. Essa capacidade específica visa, de forma deliberada, os principais decisores do adversário, para induzi-los a tomar decisões que apoiem objetivos favoráveis. Como uma arma de dissuasão, ela provoca dúvida, confusão e possivelmente o medo entre os principais alvos da liderança do adversário, ao interromper ou degradar seu ciclo de decisão normal de comando e controle enquanto ele busca avaliar a dissimulação[12]. Um exemplo seria uma mensagem destinada a explorar divergências entre um integrante-chave da liderança do adversário e outro importante decisor, com quem ele tenha uma relação conflituosa. Tal mensagem poderia causar disputas internas, que levassem o adversário a desistir de uma linha de ação planejada e a adotar uma posição mais favorável aos nossos interesses.

Segurança das operações. Na "fase I", a segurança das operações nega, ao adversário, informações essenciais que facilitariam uma avaliação precisa da nossa intenção e capacidades. Além disso, a efetividade na segurança das operações faz com que o adversário ou tome decisões erradas ou as atrase porque faltam informações confiáveis[13]. Negar ao decisor adversário informações essenciais sobre a nossa intenção e capacidades contribui para sua incerteza, atrapalha seu ciclo de decisões e aumenta sua sensação de dúvida, medo e confusão, o que torna a dissuasão uma possibilidade real[14].

Cinco outras capacidades apoiam as Op Info: contrainteligência, segurança física, qualidade das informações, câmera de combate e ataque físico. Com exceção

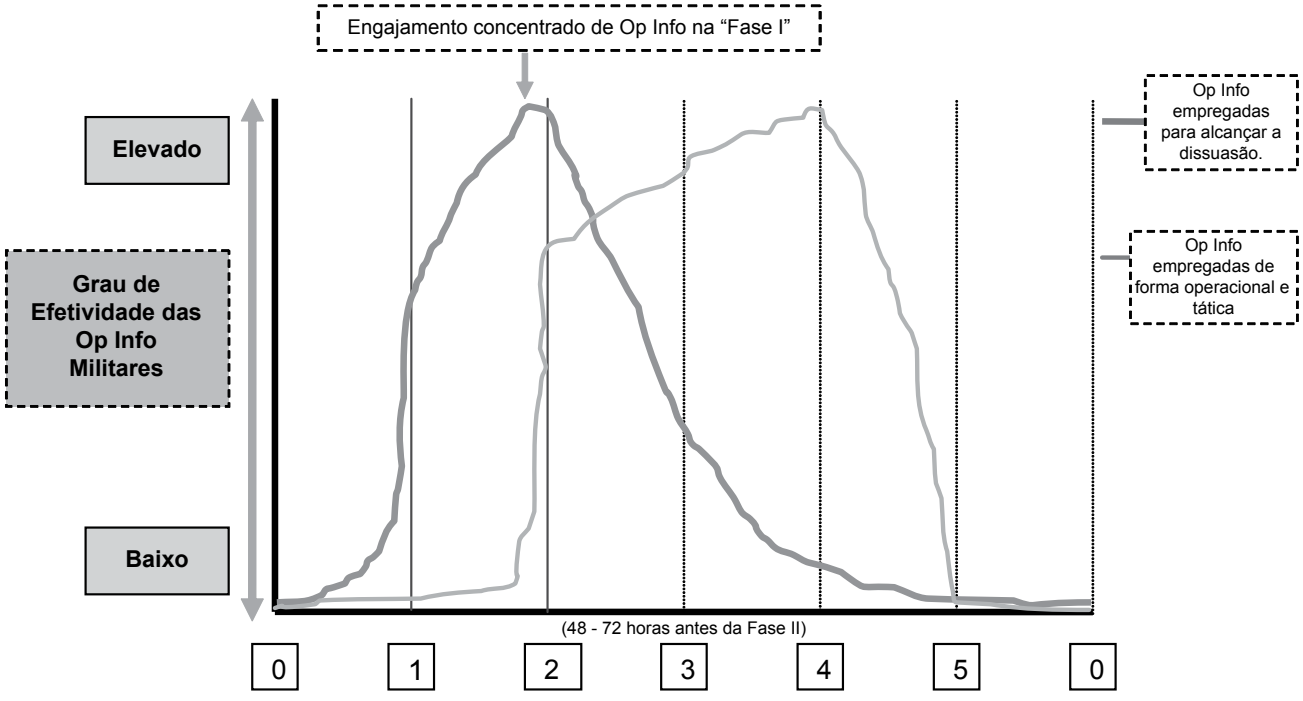

Figura 1. Operações de Informações na "Fase I": dissuasão

do ataque físico, essas medidas servem para defender infraestruturas amigas ou para a documentação de informações visuais e não são tão pertinentes como formas de dissuasão. O ataque físico envolve o uso de fogos "cinéticos" contra um alvo de Op Info para influenciar um público-alvo específico[15].

Embora a doutrina afirme que outras três capacidades relacionadas com Op Info — relações públicas, operações civil-militares e apoio de Defesa à diplomacia pública — contribuem para o ambiente geral de informações e precisam ser coordenadas com as Op Info, pode-se argumentar que sua aplicação para obter a dissuasão, em relação às operações de informações ofensivas, é indireta, na melhor das hipóteses. As Op Info militares visam o adversário e suas estruturas de apoio. As operações de relações públicas transmitem mensagens para públicos internos e estrangeiros. Operações civil-militares são mais efetivas nas fases "IV" (estabilizar) e "V" (capacitar a autoridade civil). O apoio de Defesa à diplomacia pública consiste no suporte dado por soldados treinados em Op Psc à disseminação de mensagens e temas, sob a autoridade de um embaixador. Essas capacidades relacionadas não são tão efetivas quanto as capacidades de Op Info em termos de alcançar a dissuasão na "fase I"[16].

Operações de Informações na "Fase I": Uma Posição Convincente

Sustentadas por uma vontade política comprometida, as Op Info oferecem aos Comandantes de comandos unificados uma alternativa não letal que pode impedir o conflito, quando empregada no contexto de um conjunto geral de objetivos estratégicos. De fato, a principal ênfase estratégica das Op Info deve ser a dissuasão e o emprego de capacidades específicas para tal fim[17]. Para que as Op Info sejam efetivas em dissuadir um potencial adversário, devemos empregá-las com a mesma força e rigor que caracterizam nossa aplicação da força letal. Devemos convencer o adversário que será inútil levar adiante uma linha de ação considerada ameaçadora aos interesses dos Estados Unidos e que insistir nela resultará em consequências terríveis. As operações de informações em apoio à dissuasão, empregadas com efetividade, deixam o adversário com uma sensação de dúvida, medo e confusão e o induzem a abandonar a linha de ação. Com Op Info organizadas para influenciar o ciclo "observar, orientar, decidir e agir" (OODA) do adversário, suas operações e percepção da possibilidade de sucesso diminuem. Isso cria a possibilidade real de que o adversário possa abandonar ou alterar a política questionada pelos Estados Unidos[18].

O valor da aplicação das Op Info para impedir o conflito tem um apelo amplamente reconhecido. Na Estratégia de Segurança Nacional dos Estados Unidos (*National Security Strategy of the United States*), dissuadir um adversário potencial é uma das prioridades para proteger os interesses nacionais dos EUA[19]. O documento aborda diretamente a necessidade de engajar um potencial adversário com as capacidades de Op Info antes do início de um conflito armado.

Curiosamente, a Estratégia de Segurança Nacional também aponta para a dissuasão "pelo convencimento" como uma prioridade para proteger os interesses dos EUA[20]. Dissuadir "pelo convencimento" consiste em atividades relacionadas com a "fase 0" (definição das operações). Na "fase 0", as Op Info militares devem desempenhar um papel apenas secundário. Outros elementos do Poder Nacional — diplomático, econômico e de informações — devem dominar os esforços dos EUA em dissuadir um adversário de executar uma política que ameace os interesses de segurança do país.

A distinção entre dissuadir [no sentido clássico – N. do T.] e dissuadir "pelo convencimento" está no foco do esforço. No caso de esforços de dissuasão "pelo convencimento", o foco é, muitas vezes, menos direto em relação ao adversário. Em comparação, a dissuasão clássica exige pressão direcionada contra um adversário potencial. Os alvos para a aplicação de Op Info dissuasórias devem corresponder diretamente aos essenciais componentes humano, de infraestrutura e de conteúdo que sustentem o potencial adversário e a política ou a linha de ação que ele esteja executando.

A Diretriz 3600.1, do Departamento de Defesa, aborda as Op Info e defende a necessidade de maximizar tais capacidades para obter a dissuasão. A diretriz afirma que as Op Info devem visar a impedir o conflito em que o potencial para neutralizar uma crise é seu aspecto mais promissor[21]. A "fase 0" consiste na definição das operações combinadas e a "fase II", "conquista da iniciativa", representa o início do conflito armado. As operações de informações rapidamente se convertem em aplicação tática, ao serem empregadas como

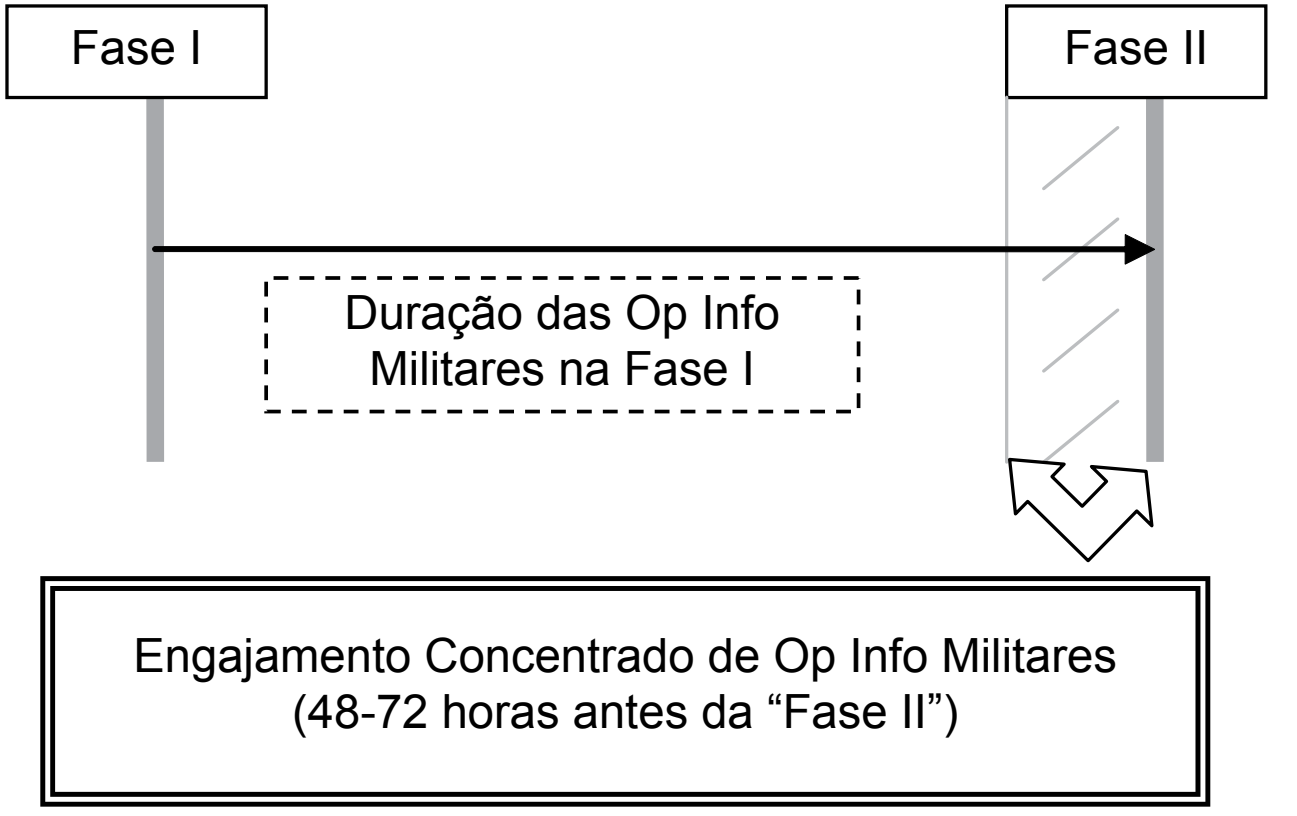

Figura 2. Operações de Informações ao longo da linha cronológica da "Fase I"

ofensiva na "fase II". "Na fase I", as Op Info preenchem a lacuna de dissuasão estratégica entre a dissuasão "pelo convencimento" da "fase 0" e o início da aplicação de força letal na "fase II". Quanto mais agressivo for o uso das Op Info na "fase I", mais provável será que o adversário perceba nossa disposição a empregar a força[22]. As operações de informações em apoio à dissuasão estratégica podem, assim, minimizar a necessidade de posicionar Forças perto da área do conflito[23]. As operações de informações influenciarão o processo decisório e as percepções de um potencial adversário ao mesmo tempo em que aumentam o impacto dissuasório das alternativas de projeção de poder[24].

> "…a aplicação das Op Info ofensivas pode neutralizar uma crise…"

A figura 1 descreve a efetividade dissuasória das operações de informações em todas as fases das operações conjuntas. A análise desse diagrama ajudará a esclarecer a argumentação em prol de Op Info ofensivas nas operações da "fase I", assim como de um engajamento concentrado de Op Info à medida que a "fase I" se aproximar da conclusão e a "fase II" estiver prestes a começar.

A linha à esquerda representa as Op Info empregadas para obter a dissuasão. O diagrama mostra que a efetividade das Op Info é mínima na "fase 0", mas acelera rapidamente com o início da "fase I", aumentando ao longo desta de forma cumulativa. Essa efetividade crescente reflete o fato de que o adversário potencial está reagindo à aplicação sincronizada das capacidades militares centrais de operações de informações. Na "fase I", as Op Info devem buscar afetar a liderança e as estruturas de apoio de um adversário, incluindo a população, de modo que os EUA alcancem sua meta de impedir o conflito ao induzir a mudança favorável de uma política do adversário[25]. O diagrama mostra que, conforme o início da "fase II" se aproximar, é preciso que ocorra um engajamento concentrado de Op Info que assegure, em primeiro lugar, uma dissuasão bem-sucedida e, em caso de insucesso, uma superioridade de informações das Forças amigas na preparação para o início do conflito armado, na "fase II". A característica central do engajamento concentrado de Op Info é redobrar esforços e concentrar "fogos" de Op Info. Caso a dissuasão não funcione, o engajamento concentrado de Op Info na "fase I" deve começar de 48 a 72 horas antes do início previsto da "fase II". A figura 2 mostra a linha cronológica para iniciar e executar o engajamento concentrado de Op Info na "fase I".

Quando a "fase II" começar, o impacto estratégico das Op Info como alternativa para obter a dissuasão rapidamente se tornará secundário à aplicação das Op Info em apoio às exigências operacionais e táticas.

Os mesmos meios utilizados para as Op Info na "fase I" também apoiam o combate operacional e tático, e seu emprego aumenta a partir do início da "fase II" até o final da "fase III", principais operações de combate. No início da "fase VI" — operações de estabilidade —, a efetividade das Op Info operacionais e táticas diminui.

Uma aplicação agressiva, sincronizada e coordenada das cinco capacidades específicas para impedir as ações de um potencial adversário estatal pode se dar da seguinte maneira:

- A guerra eletrônica pode visar uma rede de comando e controle de mísseis balísticos e radares do adversário para reduzir sua capacidade de lançamento. Pode causar interferência nas estações de rádio e televisão estatais para isolar a população da propaganda estatal.
- Um ataque, pela rede de computadores, contra a rede de telecomunicações estatal pode impedir, reduzir ou atrapalhar seu uso para comando e controle de Forças militares e para a liderança nacional dirigir uma resposta centralizada. Tal ataque, juntamente com as operações psicológicas, pode enviar mensagens discretas para os líderes importantes de facções nacionais, de modo a gerar atrito e a aumentar a pressão interna sobre a liderança estatal do adversário, no sentido de induzi-la a abandonar políticas desfavoráveis.
- As operações psicológicas podem transmitir mensagens para a população a fim de criar uma separação entre ela e a liderança estatal do adversário, gerando pressão interna adicional.

- As operações de dissimulação militar podem gerar dúvida, medo e confusão nos comandantes, interpretadas como as verdadeiras intenções das Forças militares americanas. Essas operações forçarão os líderes militares do Estado adversário a mostrar à liderança política que será inútil resistir.
- A segurança operacional pode envolver as operações das Forças amigas com uma "cobertura de proteção" e impedir a detecção das intenções dos EUA.

O Comandante do comando combatente unificado busca isolar os líderes de um potencial adversário do apoio físico e psicológico de que usufruem, particularmente do que recebem de suas Forças militares e da infraestrutura de apoio[26]. Se o ator é um Estado-Nação, a dependência em relação a uma burocracia mais formal e à tecnologia incorporada, como redes de telecomunicações e de radares, provavelmente será maior do que a de um ator não estatal. Portanto, a guerra eletrônica e os ataques às redes de computadores podem ter um maior efeito contra um ator estatal do que contra um ator não estatal. Em ambos os casos, a aplicação das Op Info ofensivas pode neutralizar uma crise e eliminar a necessidade de passar para o estágio de conflito armado, que começa com a "fase II" [27].

A falta de sofisticação tecnológica e o comando e controle menos estruturado dos típicos adversários não estatais potenciais, em comparação com adversários estatais, podem reduzir a efetividade direta da guerra eletrônica e dos ataques a redes de computadores. Contudo, como os adversários não estatais podem utilizar a infraestrutura de telecomunicações da nação anfitriã onde operem, o ataque a redes de computadores pode permitir o envio de mensagens de operações psicológicas diretas. Da mesma forma, os ataques a redes de computadores podem possibilitar mensagens de operações psicológicas a líderes-chave da nação anfitriã, incentivando ações mais arrojadas contra o adversário.

As operações de influência que utilizem as operações psicológicas e a dissimulação militar terão maior grau de impacto em um adversário que careça de sofisticação tecnológica para o comando e controle. A dissimulação militar pode fazer com que a liderança do adversário não estatal passe a desconfiar da tolerância às suas atividades pela nação anfitriã e gerar medo em relação às operações militares pendentes contra ele pelas Forças da coalizão lideradas pelos EUA. As operações psicológicas contra a população local podem minar seu apoio ao adversário. Por exemplo, oferecer uma recompensa por informações estimula a população local a denunciar as atividades do grupo adversário.

Ambos os cenários demonstram que, para que a aplicação das operações de informações militares contra qualquer potencial adversário tenha êxito, são necessárias as seguintes ações:

- Análise do ambiente, para garantir a devida sincronização das capacidades específicas;
- Avaliação dos interesses vitais do potencial adversário, para assegurar que o planejamento das operações de informações esteja correto;
- Avaliação dos pontos de pressão críticos de um potencial adversário, para que a força aplicada pelas operações de informações obtenha a máxima efetividade; e
- Uso da(s) adequada(s) capacidade(s) de operações de informações, no grau e na variedade de forças necessárias para a obtenção do efeito dissuasório almejado[28].

Planejamento, Seleção de Alvos e Efetividade

As operações de informações devem se integrar plenamente ao planejamento e à seleção de alvos e medidas de efetividade devem proporcionar o *feedback*, para assegurar que a efetividade seja atingida. O uso de todas as capacidades específicas sincronizadas e integradas é essencial para a efetividade[29]. A menos que as Op Info sejam integradas no planejamento e na seleção de alvos, a efetividade das operações na "fase I" será duvidosa. Os planejadores de operações de informações devem participar como integrantes ativos em equipes de planejamento de operações e estar prontos para defender o valor dos produtos das Op Info, tanto como um conjunto distinto de capacidades, quanto como um multiplicador da força em todas as fases das operações combinadas[30].

É necessário e adequado empregar procedimentos tradicionais de seleção de alvos porque as operações de informações oferecem alternativas que produzem efeitos, da mesma forma que opções letais. Uma matriz de sincronização que descreva a integração de alvos é tão aplicável às operações de informações quanto às capacidades letais[31]. Deve haver uma única matriz de sincronização de alvos que integre alvos letais e não

> …as operações de informações comportam esforços no sentido de obedecer a restrições morais e legais tradicionais…

letais. As medidas de efetividade devem ser ligadas de modo lógico à situação final almejada. Contudo, é preciso reconhecer que medidas de efetividade representam um enorme desafio. O efeito cumulativo das operações de informações necessárias à dissuasão torna difícil avaliar o impacto de cada uma das capacidades individualmente[32].

Pode-se dizer que é irrelevante ter uma medida de efetividade para cada uma das capacidades específicas, quando é necessário haver a sincronização de duas ou mais capacidades para se atingir o efeito desejado. Sem uma medida de efetividade baseada na análise dedutiva, para os efeitos de primeira ordem, e em uma análise indutiva racional, para os efeitos de segunda e terceira ordem, a aceitabilidade das operações de informações como um conjunto previsível de alternativas não letais para o comandante é ilusória.

Justificativa Legal e Moral

O conflito armado é regido pelo Direito Internacional[33]. As operações de informações não se enquadram nesse marco jurídico. O Direito Internacional não cita a utilização das operações de informações como um aspecto do conflito armado e, portanto, o uso das Op Info como um dissuasor da guerra não constitui um ato de guerra[34].

O artigo 41 da Carta da ONU é um exemplo da legislação vigente que não classifica o uso das operações de informações como um ato de guerra. Ela afirma que atos destinados a interromper as comunicações de um adversário não envolvem o emprego de força armada[35]. Portanto, a utilização das operações de informações em operações de dissuasão, como a guerra eletrônica e o ataque a redes de computadores, não constitui um ato de guerra.

Dentro do contexto das Leis do Conflito Armado, as condições de *jus in bello* [Direito na Guerra, N. do T.] — como uma força é empregada na guerra — incluem princípios de necessidade, proporcionalidade, distinção e humanidade. As convenções de Genebra e de Haia codificam as condições de *jus in bello*. Essas convenções não contêm acordos de controle específicos que restrinjam o uso das operações de informações[36]. Na verdade, as operações de informações comportam esforços no sentido de obedecer a restrições morais e legais tradicionais destinadas a incentivar o comedimento e a minimizar o uso da força[37]. Por exemplo, o princípio de proporcionalidade exige que o valor de um objetivo militar se compare à perda de vidas e aos danos provocados por uma ação militar[38]. As operações de informações ajudam a atender às demandas para satisfazer esse princípio. O princípio de distinção requer, igualmente, que os alvos atacados possuam um valor militar e que não sejam de caráter exclusivamente civil[39]. Como as capacidades das operações de informações não provocam diretamente a perda de vidas ou danos à infraestrutura — e, pode-se argumentar, tampouco o fazem os efeitos de segunda e de terceira delas resultantes —, o objetivo desse princípio é atendido. Do mesmo modo, "humanidade", como um princípio de *jus in bello*, requer a minimização do sofrimento humano na guerra[40]. Assim, mais uma vez, as operações de informações podem levar a resultados mais morais.

Conclusão

As capacidades militares básicas de Op Info podem impedir o conflito armado tanto com potenciais adversários estatais quanto não estatais. Os resultados das ações tomadas pelos EUA no sentido de dissuadir um adversário potencial de uma linha de ação ou de uma política indesejável — e não as armas utilizadas — determinarão como a comunidade internacional e o público interno julgará o país[41]. A capacidade de justificar o uso de Op Info ofensivas como sendo moralmente prudente contribuirá consideravelmente para a aceitação pela comunidade internacional de que o uso dessas operações não representa o emprego de força no sentido tradicional[42].

Atualmente, a política e os líderes militares norte-americanos costumam respeitar uma restrição operacional que visa a minimizar as baixas, especialmente entre as Forças dos EUA e a população civil

afetada[43]. Evidentemente, as Op Info com características não letais e "não cinéticas" atendem a essa restrição operacional e oferecem uma justificativa para as operações de informações ofensivas. Quanto mais se entender o uso de Op Info para fins de dissuasão, maior a probabilidade que líderes políticos e militares americanos concordem que as operações de informações militares aplicadas de forma ofensiva na "fase I" obterão a dissuasão com um mínimo de baixas e de danos à infraestrutura. Só então a nação acolherá as Op Info a ponto de permitir sua plena contribuição para a segurança nacional como um elemento dissuasório[44].

A aplicação das operações de informações como dissuasor do conflito armado é consideravelmente promissora tanto para os líderes militares quanto para os políticos. Contudo, o país carece, atualmente, da vontade política e de alguns fatores facilitadores que permitam que as operações de informações ofensivas sejam uma alternativa de força da "fase I", na busca por atingir um objetivo estratégico.

Os fatores facilitadores relacionados a seguir contribuirão para o êxito das Op Info ofensivas na "fase I". Aceitos e implantados conjuntamente, eles oferecem verdadeira esperança de progresso.

- Ampliar a doutrina nas Publicações Conjuntas 3-0 e 3-13 para especificar que a utilização de operações de informações ofensivas na "fase I" das operações combinadas representa a primeira alternativa para o Comandante dos comandos combatentes unificados. A doutrina poderia especificar um engajamento concentrado de operações de informações como uma aplicação final da "fase I" — um último esforço conjunto para forçar um adversário potencial a sujeitar-se à pressão dissuasória dos EUA —, ou como um precursor de operações favoráveis na "fase II".
- Estabelecer as Op Info como uma capacidade específica em todos os comandos combatentes unificados[45]. Para tanto, são necessárias armas de Op Info novas e tecnicamente superiores, assim como uma estrutura da força adequada para implantá-las. Existe um número insuficiente de meios, tanto em armas quanto em efetivos, para apoiar todos os comandos combatentes unificados em engajamentos simultâneos, ou para concentrar, de forma adequada, "fogos" de Op Info nas quantidades necessárias para obter a efetividade. É preciso estabelecer um gabinete conjunto de desenvolvimento e aquisições, autorizado a explorar, desenvolver e colocar em campo sistemas de armas de Op Info tecnicamente superiores em quantidades suficientes para o emprego em ambientes aéreos, terrestres e marítimos. Também há a necessidade de uma estrutura de força combinada, que forneça a cada comando combatente unificado geográfico, ao Comando de Operações Especiais e ao Comando Estratégico dos EUA uma organização de apoio direto. Cada uma dessas organizações poderia planejar e executar operações de informações com capacidades orgânicas destacadas ou em reforço.
- Tratar, em diretrizes, nas políticas e na doutrina, de questões básicas referentes à preparação do campo de batalha, para apoiar operações de informações ofensivas[46]. É imprescindível que haja uma diretriz presidencial à comunidade de Inteligência que determine a preparação de Inteligência dinâmica e proativa para o espaço de batalha contra todos os potenciais adversários, com o intuito de obter acesso aos seus nós críticos de informação para apoiar Op Info ofensivas. O processo para obter acesso a um alvo de Op Info sigiloso do adversário é bastante lento e desconfortável e extremamente politizado, privilegiando o processo da Inteligência em vez da necessidade operacional.
- Conferir autoridade aos Comandantes dos comandos combatentes unificados para executar operações de informações ofensivas essenciais, de modo a garantir que elas sejam uma alternativa de força para a dissuasão. Deve ser estabelecida uma política abrangente, que determine que todas as capacidades existentes de operações de informações e estruturas de força auxiliares estejam à disposição do Comandante de um comando combatente unificado em apoio às operações dissuasórias. Testes específicos devem estabelecer os critérios que definem as condições aceitáveis para a utilização de operações de informações na "fase I".
- Requerer que o governo dos EUA utilize as operações de informações para atingir objetivos nacionais estratégicos e proteger os interesses nacionais. A menos que exista vontade política para utilização das Op Info na "fase I" de modo a dissuadir um adversário potencial, é provável que ocorra o conflito armado, com as correspondentes baixas e dispêndio de recursos. ■

Referências

1. JOINT CHIEFS OF STAFF (JCS), Joint Publication (JP) 3-13, *Information Operations*, (Washington, DC: U.S. Government Printing Office [GPO], 13 fev. 2006), p. 1-12.

2. MILLER, Earl E. *Army Transformation and Information Operations: The International Legal Implications* (Strategy Research Project, Carlisle Barracks, PA: U.S. Army War College, 9 abr. 2002), p. 8-9.

3. ARMISTEAD, Leigh. (ed.) *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC: Brassey's Inc., 2004), p. 16.

4. JCS, Joint Publication 3-51, *Joint Doctrine for Electronic Warfare* (Washington, DC: GPO, 7 abr. 2000), p. vii.

5. Ibid, p. 1-2.

6. JCS, *Information Operations*, p. II-6.

7. Ibid.

8. WILLIAMSON, Jennie M. *Information Operations: Computer Network Attack in the 21st Century* (Strategy Research Project, Carlisle Barracks, PA: U.S. Army War College, 9 abr. 2002), p. 9.

9. JCS, JP 3-53, *Joint Doctrine for Psychological Warfare* (Washington, DC: GPO, 5 set. 2003), p. ix.

10. Ibid., p. x.

11. Ibid., p. xii.

12. JCS, JP 3-58, *Joint Doctrine for Military Deception* (Washington, DC: GPO, 31 maio 1996), p. v-vi.

13. JCS, JP 3-54, *Joint Doctrine for Operations Security* (Washington, DC: GPO, 24 jan. 1997), p. v-vi.

14. Ibid., p. I-4.

15. JCS, *Information Operations*, p. II-7–II-10.

16. JCS, *Information Operations*, p. II-10–II-13.

17. BARNETT, Roger W. "Information Operations, Deterrence, and the Use of Force", *Naval War College Review* (Spring 1998): p. 1.

18. GUEVIN, Paul R. "Information Operations", *Air and Space Power Journal* 18, no 2 (Summer 2004): p. 122.

19. DEPARTMENT OF DEFENSE (DOD), *The National Defense Strategy of the United States of America* (Washington, DC: GPO, March 2005), p. iv.

20. Ibid.

21. FREDERICKS, Brian E. "Information Warfare at the Crossroads", *Joint Force Quarterly* (Summer 1997): p. 100.

22. Ibid., p. 98.

23. DOD, *Joint Operations Concepts* (Washington, DC: GPO, nov. 2003), p. 19.

24. TULAK, Arthur N. "Information Operations in Support of Demonstrations and Shows of Force", *Military Intelligence Professional Bulletin* 29, no 3 (jul.-set. 2003): p. 10.

25. GRANGE, David L.; KELLEY, James A. "Information Operations for the Ground Commander", *Military Review* (mar.-abr. 1997): p. 9.

26. JCS, JP 3-0, *Doctrine for Joint Operations* (Washington, DC: GPO, 10 set. 2001), p. IV-2.

27. RHODES, J.E. "A Concept for Information Operations", *Marine Corps Gazette* 82, no 8 (ago. 1998): p. 48.

28. ARMISTEAD, Leigh (ed.), p. 21.

29. MURPHY, Dennis M. "Information Operations on the Non-traditional Battlefield", *Military Review* (nov. – dez. 1996): p. 18.

30. LAWLOR, Maryann. "Information Operations Specialists Move to the Mission Planners' Table", *Signal* (dez. 2005): p. 47.

31. GONZALES, Richard L.; ROMANYCH, Marc J. "Nonlethal Targeting Revisited", *Field Artillery Journal* (maio-jun. 2001): p. 6-8.

32. GROHOSKI, David C.; SEYBERT, Steven M.; ROMANYCH, Marc J. "Measures of Effectiveness in the Information Environment", *Military Intelligence Professional Bulletin* 29, no 3 (jul.-set. 2003): p. 12-14.

33. DICENSO, David J. "Information Operations: An Act of War?" *Law Technology* 33, no 2 (2nd Quarter 2002): p. 28.

34. MILLER, p. 14.

35. Ibid., p. 29.

36. BARNETT, p. 6.

37. DICENSO, p. 31.

38. Ibid.

39. Ibid.

40. Ibid.

41. MILLER, p. 11.

42. BARNETT, p. 7.

43. Ibid., p. 5.

44. Ibid., p. 1.

45. MYERS, Richard B. "Shift to a Global Perspective", *Naval War College Review* 56, no 4 (Autumn 2003): p. 11.

46. JAJKO, Walter. "A Critical Commentary on the Department of Defense Authorities for Information Operations", *Comparative Strategy* 21 (2002): p. 111.