Atacar ou Defender?
Como Explorar as Informações e Equilibrar os Riscos no Ciberespaço

Coronel Dennis M. Murphy (Reserva), Exército dos EUA

Quando da redação deste artigo, as políticas do Departamento de Defesa e os regulamentos militares restringiam consideravelmente o uso da internet para fins de comunicação estratégica em prol da segurança. Em 25 Fev 10, o Departamento de Defesa emitiu uma política que adota uma abordagem equilibrada nesse sentido, apoiando, portanto, a tese original do presente artigo. Assim sendo, o autor atualizou o trabalho para oferecer uma explicação mais aprofundada sobre a decisão de emitir a política e para promover a adoção de seus princípios.

A HISTÓRIA DAS FORÇAS militares dos Estados Unidos está repleta de exemplos de preparação para a guerra seguinte a partir do estudo da última (ou atual). Em consequência, travamos a guerra, muitas vezes, com uma doutrina e processos defasados em relação à realidade atual. O resultado pode ser um esforço de guerra prolongado, a um grande custo para o tesouro nacional tanto em termos fiscais quanto humanos. O desenvolvimento e implantação problemáticos da doutrina de contrainsurgência, resultando na chamada "escalada de tropas" no meio da campanha no Iraque, são apenas um de muitos exemplos[1].

A reflexão introspectiva sobre a guerra futura pelo Exército no final dos anos 70 e início dos anos 80 é uma exceção, porém. Utilizando a Guerra Árabe-Israelense de 1973 como um prenúncio da guerra em que as armas de precisão e os avanços tecnológicos mostrariam a importância da manobra, o Exército passou da doutrina de "Defesa Ativa" para a de "Batalha Ar-Terra". Contudo, essa mudança não foi universalmente aceita. Em um trabalho de 2006 sobre Poder Terrestre, o General Huba Wass de Czege relembrou:

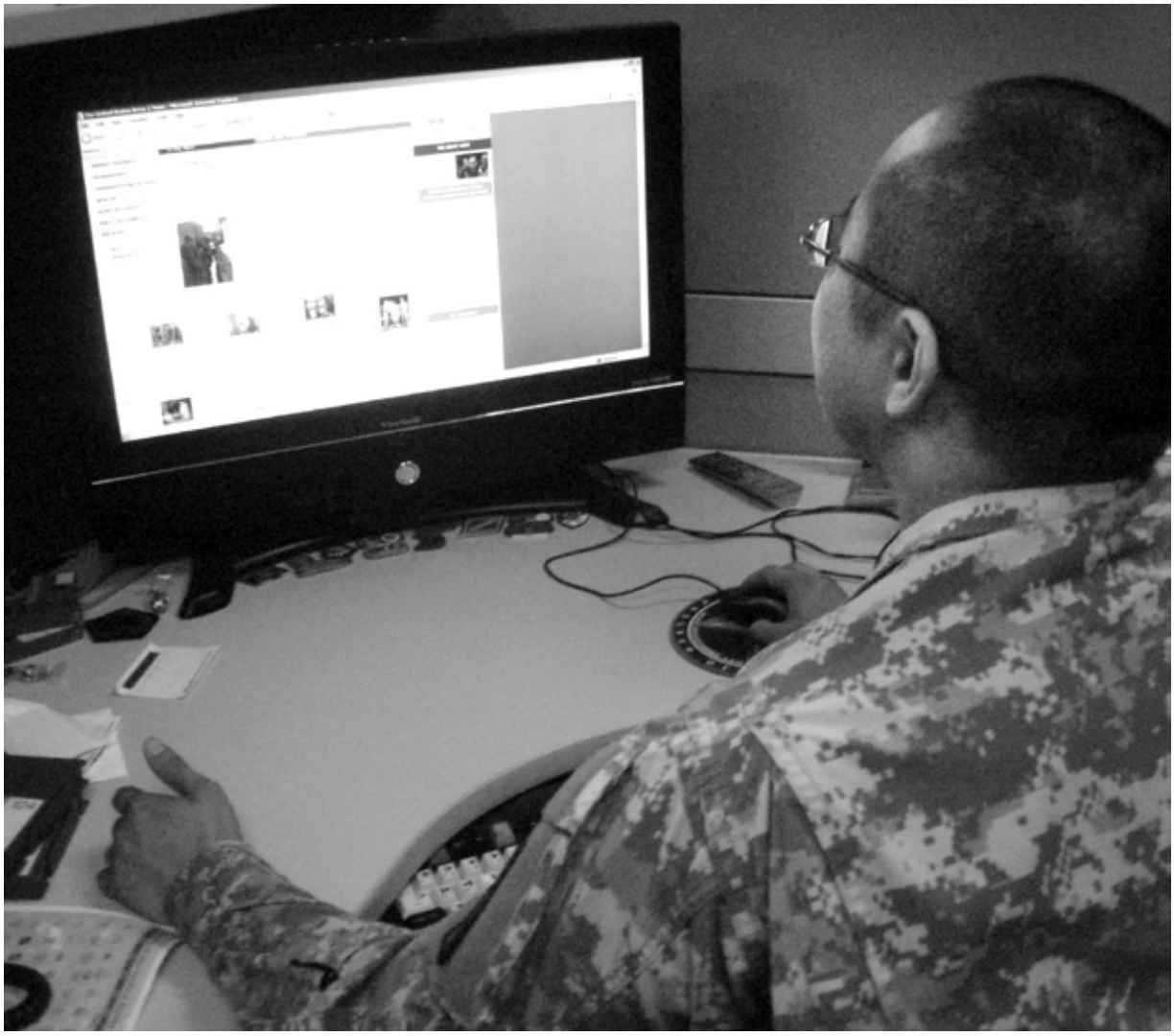
> No que se transformou em um diálogo saudável, [jovens oficiais] enxergavam a tática defensiva como uma abordagem de "recuo por fileiras", que confundia o retardamento com a defesa e que levaria os comandantes a evitar o engajamento decisivo... Eles a viam como sendo reativa, abrindo mão da iniciativa e resultando em um método arriscado de defesa[2].

A história oficial da Guerra do Golfo de 1991 descreve a mudança para a Doutrina de Batalha Ar-Terra como uma decisão visionária, que foi a base daquela vitória dramática para as Forças militares dos EUA[3].

Então, como será a próxima guerra? Ninguém tem uma bola de cristal infalível para prever o futuro, mas mesmo uma consideração superficial de possíveis futuros adversários revela a importância dada à informação como um meio assimétrico estratégico de conduzir a guerra. Segundo consta, as Forças militares chinesas penetraram as redes militares do Pentágono[4]. Alega-se que o governo russo conduziu um grande ataque cibernético contra a infraestrutura estoniana[5]. Contudo, embora ataques contra sistemas de informação tenham se mostrado como ameaças, a dependência em relação à internet para travar a "guerra de ideias" vem aumentando. Considere-se a chamada "Segunda Guerra do Líbano" entre Israel e o Hezbollah, no verão de

---

O Coronel Dennis M. Murphy (Reserva), Exército dos EUA é o Diretor do Grupo Informações na Guerra (Information in Warfare Group) na Escola de Guerra do Exército dos EUA. O Professor Murphy leciona disciplinas eletivas sobre Operações de Informações e Comunicação Estratégica e realiza oficinas sobre o Elemento da Informação do Poder Nacional.



Exército dos EUA, David Vergun

Soldado entra no ciberespaço.

2006. O Hezbollah utilizou informações para afetar as percepções como um meio de alcançar a vitória estratégica, a ponto de colocar *outdoors* sobre os escombros de edifícios no sul do Líbano com os dizeres: "Feito nos EUA" (em inglês)[6].

As Forças militares dos EUA certamente reconhecem essa ameaça, como demonstra a iniciativa de estabelecer o Comando Cibernético dos EUA (*U.S. Cyber Command*). Contudo, até recentemente, a doutrina estava defasada. As políticas anteriores davam preferência à "defesa ativa" em vez da "manobra" no ciberespaço. Embora uma recente alteração de política aponte para uma mudança potencialmente significativa nessa equação, questiona-se se as Forças militares acolherão a transformação organizacional necessária para equilibrar a necessidade de proteger as redes com a ofensiva ideológica, adotada por seus adversários.

No final das contas, os líderes devem avaliar os riscos envolvidos, a fim de obter equilíbrio para competir no espaço de combate das informações. Desenvolverão o equivalente à "Batalha Ar-Terra" para o ciberespaço ou esperarão até a próxima guerra para obter o equilíbrio, a um custo potencialmente alto para a nossa nação?

Como Definir o Problema

Permanecer atualizado com a definição de ciberespaço pode exigir dedicação constante. Desde 2004, o governo dos EUA apresentou quatro definições "oficiais" diferentes. Atualmente, o Departamento de Defesa define o ciberespaço da seguinte forma:

> domínio global, dentro do ambiente de informações, que consiste na rede interdependente de infraestruturas de tecnologia da informação, incluindo a internet, as redes de telecomunicações, os sistemas computacionais e os processadores e controladores que a integram[7].

Talvez mais importante, poder cibernético é "a capacidade de utilizar o ciberespaço para criar vantagens e influenciar eventos em todos os ambientes operacionais e nos instrumentos de poder"[8]. Assim, da mesma forma que os poderes terrestre, marítimo e aéreo, o poder cibernético é uma arma de guerra.

A definição de ciberespaço do Departamento de Defesa reconhece, acertadamente, a importância da internet como um habilitador desse domínio no atual ambiente de informações. A rede mundial de computadores (*web*), como um subconjunto da internet, é fundamentalmente sem governo, o que oferece liberdades e sugere cuidados óbvios. A *web* proporciona uma voz ao indivíduo — com frequência, anônima — e um público potencialmente amplo. Pode-se facilmente estabelecer, desfazer e restabelecer um *site*. Esse atributo torna os *sites* valiosos para os movimentos extremistas. Por outro lado, a mesma capacidade conferida aos nossos adversários pela *web* está à nossa disposição, se escolhermos utilizá-la. A "Estratégia Nacional para o Combate ao Terrorismo" (*The National Strategy for Combating Terrorism*) observa que a internet proporciona aos terroristas refúgios cibernéticos para "comunicar, recrutar, treinar, mobilizar apoio, converter e disseminar sua propaganda sem arriscar o contato pessoal". Também destaca a oportunidade que a internet oferece para desacreditar essa mesma propaganda[9].

O impacto das tecnologias da internet na Segurança Nacional e no combate não somente aumentará no futuro, mas o fará de forma exponencial[10]. Deve-se considerá-la como um importante meio de conduzir a "guerra de ideias". Os *blogs*, o *YouTube*, o *Google Earth* e o *Second Life* são todos "novas mídias": tecnologias facilitadoras que os nossos adversários empregam para ganhar uma vantagem assimétrica ao afetar percepções, posturas, comportamentos e, por fim, crenças. Os *sites* de mídia social, como o *Facebook* e o *Twitter*, explodiram recentemente e têm sido utilizados para fins muito além da interação social que tais veículos implicam. O *iPhone* poder parecer um telefone, mas possui todos os recursos de um computador de mesa (às vezes, mais) em um dispositivo do tamanho da palma da mão.

Não há dúvida de que a tecnologia continuará a ficar mais rápida, barata e capaz. Nesse contexto, as novas mídias logo se tornam "velhas" mídias. Por isso, uma definição mais durável considera as novas mídias como quaisquer capacidades que permitam que vários atores (de indivíduos a Estados-Nação) criem e disseminem informações em tempo real ou "quase-real" que possam afetar um amplo público (regional ou mundial). Embora fosse, anteriormente, da esfera exclusiva dos Estados-Nação e das grandes empresas multinacionais, os indivíduos hoje podem utilizar as informações como um meio estratégico, um desenvolvimento importante para os formuladores de políticas e para os combatentes.

Os futuros desafios do combate devem considerar o emprego quase certo da internet por qualquer adversário potencial. Os analistas não deveriam ganhar um falso sentimento de segurança com base na baixa penetração da internet em algumas das partes mais conflituosas do mundo. Por exemplo, embora, com base na sua população, a África tenha uma taxa de penetração da internet de apenas 6,8%, seu uso por lá cresceu em 1.392% de 2000 para 2009. Também há taxas de crescimento acentuadas na Ásia, no Oriente Médio e na América Latina[11].

Os combatentes reconhecem a necessidade de competir no ciberespaço.

Os combatentes reconhecem a necessidade de competir no ciberespaço. Cada vez mais, Comandantes e Unidades patrocinam páginas de *Facebook* e "tuitam" rotineiramente. O Comando Central dos EUA interage com vozes dissidentes ao participar de *blogs* que criticam a Guerra Contra o Terrorismo, observando que "com a proliferação das informações hoje em dia, se você não falar com esse fórum, não será ouvido por

ele"[12]. As Forças Armadas dos Estados Unidos também reconhecem a importância de competir na mídia de vídeos, utilizando o *YouTube* para exibir imagens correntes das operações americanas nos atuais teatros de operações[13].

Por outro lado, a considerável dependência das Forças militares dos EUA em relação à internet, para atividades e comunicações diárias, cria uma vulnerabilidade ao ataque cibernético. Há muitas pessoas e organizações sondando as redes americanas. Embora os EUA consigam rechaçar a maioria dos ataques, as falhas nos permitem vislumbrar seu impacto. O Exército Popular de Libertação da China atacou os computadores do Pentágono em junho de 2007, aparentemente depois de várias sondagens, fazendo com que a rede fosse tirada do ar por mais de uma semana[14]. Os chineses vêm se transformando de uma Força mecanizada em uma Força "informatizada" e afirmam que pretendem utilizar a guerra das informações "como uma ferramenta de guerra [ou] forma de conquistar a vitória sem a guerra"[15]. O General da Reserva Barry McCaffrey indica que essa não é uma anormalidade, mas pode, na verdade, ser a regra. Observa que todos os nossos adversários potenciais, assim como elementos criminosos, conduzem atividades diárias de reconhecimento do nosso espectro eletrônico em áreas essenciais à Segurança Nacional dos EUA[16]. De fato, os sistemas de computadores do governo dos EUA sofrem ataques a cada oito segundos, em média[17].

O caso da Estônia pode ser um precursor do que os Estados Unidos podem esperar à medida que aumentarem sua dependência em relação à internet para atividades governamentais ou militares. A Estônia utiliza alguns dos processos de "governo eletrônico" mais avançados do mundo. Os estonianos conduzem atividades bancárias, votam e pagam impostos *on-line*, e a Estônia colocou *chips* eletrônicos nas cédulas de identidade, tornando-as bastante eficientes, mas, como foi possível constatar, extremamente vulneráveis. Assim, foi relevante o ataque de *hackers* russos no início de 2007[18]. De fato, alguns observadores equipararam o ataque cibernético a um ato de guerra no sentido clausewitziano, com o objetivo de criar um pânico social generalizado[19].

Prudence Siebert/Jornal Fort Leavenworth Lamp

Alunos da ECEME dos EUA trabalham no posto de comando principal da Divisão durante o Exercício de Combate Digital, no Forte Leavenworth, Kansas, 14 Fev 08.

Não deve surpreender, então, que a necessidade de proteger a rede tenha assumido grande importância no Departamento de Defesa e que a utilização da mesma rede, para transmitir mensagens proativas e positivas dos EUA, seja algo cada vez mais importante. Uma recente mudança de política no Departamento de Defesa ampliou a abertura, permitindo oportunidades para utilizar a internet no combate à desinformação e para contar a história das Forças militares americanas. Contudo, só o tempo dirá se a cultura organizacional adotará tal abordagem.

Defesa: Como Proteger a Rede

São empregados grandes esforços e recursos para proteger os sistemas ligados à internet do Departamento de Defesa e de outras organizações governamentais. O Departamento de Segurança Nacional estabeleceu um Centro de Segurança Cibernética Nacional (*National Cybersecurity Center*), cuja missão é "coordenar e integrar as informações necessárias para ajudar a proteger as redes e sistemas cibernéticos dos EUA e ajudar a promover a cooperação entre grupos cibernéticos federais"[20]. O Departamento de Defesa codificou o processo para proteger suas redes em um conceito chamado garantia da informação. A garantia da informação inclui:

> medidas que protegem e defendem as informações e sistemas de informações ao garantir sua disponibilidade, integridade, autenticação, confidencialidade e não-rejeição. Isso inclui providenciar o restabelecimento de sistemas de informações com a incorporação de recursos de proteção, detecção e relação [...] A garantia da informação exige uma abordagem de *defesa em profundidade* [grifo do autor][21].

O Departamento de Defesa conduz operações computacionais ostensivas dentro de um subconjunto da internet conhecido como NIPRnet (originalmente a rede ostensiva de protocolos de roteamento de internet). A NIPRnet isola o acesso à internet mais ampla por meio da utilização de um número limitado de portais. Essa metodologia torna a "defesa em profundidade" necessária exequível do ponto de vista dos recursos, na medida em que reduz o número de rotas a serem monitoradas quanto a ataques. Permite o acesso à internet para facilitar a eficiência na condução de atividades e no comando e controle[22]. Contudo, os *firewalls* e filtros de conteúdo que bloqueiam a entrada em *sites* externos específicos muitas vezes restringem o acesso à *web*, a fim de promover a produtividade no trabalho, atender a requisitos de largura de banda, proteger a segurança das operações e impedir a intrusão e o comprometimento. Em um passado recente, parecia que esse acesso externo se tornaria ainda mais restrito. Em julho de 2008, o Subsecretário de Defesa Gordon England solicitou verbas ao Congresso para construir — na falta de um termo melhor — uma "DODnet", ou rede do Departamento de Defesa. "Os ataques recentes da China contra as redes e os sistemas do Departamento de Defesa aumentam a urgência de se construírem sistemas cibernéticos impenetráveis"[23]. A tendência apontava para o aumento da segurança por meio do confinamento do sistema, uma abordagem incompatível com a vitória na guerra de ideias.

Ataque: Como Transmitir a Mensagem

Os Chefes militares enfatizam cada vez mais a importância da "comunicação estratégica" para competir no ambiente de informações. O Departamento de Defesa define a comunicação estratégica como:

> processos e esforços concentrados do governo dos Estados Unidos para compreender e atrair públicos-chave de modo a criar, fortalecer ou preservar condições favoráveis à promoção dos interesses e objetivos nacionais por meio da utilização de informações, temas, planos, programas e ações coordenados e sincronizados com outros elementos do Poder Nacional[24].

Assim, a comunicação estratégica é a integração de ações, imagens e palavras para transmitir uma mensagem que afete percepções, posturas e comportamentos[25]. As ações transmitem as mensagens mais fortes, mas as imagens e palavras fornecem o contexto e têm, muitas vezes, efeitos significativos por si só. Embora se concentre na dimensão cognitiva do ambiente de informações, a comunicação estratégica depende do ambiente físico para a transmissão de suas mensagens. Com frequência, isso requer acesso fácil e rápido à internet.

Os líderes apontam cada vez mais para a importância de utilizar novas mídias e a internet para combater de forma proativa no ciberespaço. Contudo, constatações empíricas revelam o conflito entre defender as redes e utilizá-las para transmitir a mensagem ativamente. As operações americanas no Iraque exibidas no *YouTube* estavam entre os dez vídeos mais vistos semanas depois de sua publicação, mas o Exército só os publicou depois que generais mais antigos superaram consideráveis obstáculos burocráticos[26]. Considerações sobre a largura de banda podem ter sido um problema. Os *blogs* vêm se tornando rapidamente a mídia preferida, não só para atividades recreativas, como também para atividades militares e políticas mais sérias. Os *blogs* oferecem um fórum para contar a história das Forças militares, muitas vezes pelas fontes de maior credibilidade — os próprios soldados, marinheiros, aviadores e fuzileiros navais — mas a aversão a riscos, com frequência, impede a iniciativa. As políticas militares passadas no Iraque foram restritivas e muitas vezes desencorajaram os *blogs* em vez de incentivá-los[27]. Em maio de 2008, o *blog* "Kaboom", do Tenente Matthew Gallagher, do Exército, foi tirado do ar pelos seus Chefes, depois que ele relatou, sem mencionar nomes, uma conversa entre ele e seu Comandante sem buscar aprovação prévia. Antes de ser fechado, o site sobre o dia-a-dia de um pelotão do Exército na zona de guerra recebeu dezenas de milhares de acessos[28]. O *MySpace* e o *Facebook* recebem ampla cobertura da mídia sobre sua transparência e sobre o efeito prejudicial de revelações pessoais nas mãos erradas. Por outro lado, de uma perspectiva militar, esses *sites* de rede social oferecem uma oportunidade para contar uma história confiável e contextualizada da vida na caserna. Tanto os *blogs* quanto as redes sociais, porém, apresentam problemas de segurança das operações para os comandantes, que se preocupam, com razão, em manter o sigilo sobre as operações, os recursos e as vulnerabilidades militares.

Muitos comandantes mais antigos reconhecem a importância dessas novas ferramentas de mídia como recursos militares contemporâneos e incentivam a participação no diálogo que elas facilitam. Exemplos recentes apontam para um ambiente avesso a riscos nos escalões mais altos, o que, por sua vez, prejudica o aproveitamento do potencial da rede[29]. Por exemplo, em março de 2008, o Centro de Armas Combinadas do Exército (*Combined Arms Center — CAC*), no Forte Leavenworth, Estado do Kansas, apresentou um memorando que solicitava uma "exceção à política" para permitir que seus oficiais criassem *blogs* no domínio público[30]. O CAC é comandado por um General de três estrelas, que precisou solicitar tal autorização ao seu Comandante de quatro estrelas. O que é pior: o CAC é o responsável pelo treinamento e pela formação de líderes do Exército no uso desses recursos.

O Departamento de Defesa também restringiu a autoridade para conduzir atividades interativas na internet aos generais de quatro estrelas, só permitindo que oficiais de Relações Públicas participassem de atividades interativas com jornalistas, na internet[31]. Essas políticas não só se aplicavam ao NIPRnet, como também restringiam o uso doméstico da internet.

O que parece ser um avanço significativo, porém, ocorreu em fevereiro de 2010, com a publicação de um memorando do Departamento de Defesa intitulado "Uso Responsável e Eficaz de Recursos da Internet" (*"Responsible and Effective Use of Internet-based Capabilites"*). Essa política genérica ameniza consideravelmente as restrições anteriores ao direcionar explicitamente o acesso da NIPRnet a uma ampla gama de ferramentas de colaboração e fóruns de discussão disponíveis ao público. (A política cita, especificamente, o *YouTube*, o *Facebook* e o *Twitter*, entre outros). Por outro lado, os comandantes de todos os escalões são instruídos a defender-se contra atividades maliciosas e a tomar medidas para salvaguardar as missões[32].

Essa política recente parece fazer sentido com base em uma perspectiva de equilíbrio. Contudo, também apresenta um dilema aos comandantes. Eles são responsáveis por travar a guerra de ideias em uma época em que precisam gerar mensagens proativas e respostas com rapidez. Essa necessidade requer uma abordagem descentralizada quanto à comunicação estratégica e ao engajamento de informações[33]. O meio de alcançar essa velocidade, a internet, é indispensável para a condução das atividades diárias, mas está sob vigilância e ataques contínuos, levando alguns comandantes a

colocá-la sob controle centralizado. A questão tende para um extremo ou outro de acordo com o nível de risco que um comandante está disposto a correr no ambiente de informações e na cultura organizacional militar, com relação ao benefício de se competir em tal ambiente.

Como Resolver o Dilema: Gerenciar o Risco e Alcançar o Equilíbrio

Uma abordagem de comando com foco na "defesa em profundidade" para proteger a NIPRnet, bem como controlar o acesso externo à internet e seu uso, embora compreensível do ponto de vista da análise de ameaças, vai de encontro aos princípios do bom planejamento estratégico e militar:

> O pensamento estratégico [é] um processo intelectual sofisticado com vistas a criar uma síntese do consenso, dos esforços e das circunstâncias para influenciar favoravelmente o ambiente geral, ao mesmo tempo em que se gerenciam os riscos inerentes à busca de oportunidades e à reação a ameaças[34].

Portanto, uma estratégia relativa ao uso da internet para influenciar o ambiente de informações requer que se gerencie o risco de ataques ao mesmo tempo em que se buscam oportunidades para competir. A definição supracitada de poder cibernético como sendo a "capacidade de criar vantagens e influenciar eventos" no ciberespaço parece proporcionar um foco proativo e voltado à ofensiva em atividades cibernéticas. A "Estratégia Nacional para o Combate ao Terrorismo" observa a oportunidade que a internet oferece para desacreditar a propaganda do adversário. A Estratégia de Defesa Nacional (*National Defense Strategy*) de 2008 discutiu [Essa NDS foi substituída pela primeira NDS do governo Obama, em maio de 2010 – N. do T.] a exigência de minimizar o risco — mas em termos da habilidade para explorar oportunidades[35]. Contudo, só o tempo dirá se os comandantes adotarão uma abordagem avessa a riscos quanto à nova política do Departamento de Defesa, com o estabelecimento de um controle centralizado que enfatize a proteção da rede[36].

As operações militares se baseiam no planejamento centralizado e na execução descentralizada, com um abrangente plano sincronizado, ao qual as organizações subordinadas obedecem em seus planos para alcançar os objetivos almejados. A execução descentralizada promove a agilidade, a velocidade e a capacidade de reação em um ambiente fluido, em constante mutação. Portanto, se as informações são um componente-chave dos ambientes operacionais militares atuais e futuros, conclui-se que um plano centralizado com uma execução descentralizada se aplicaria ao ciberespaço. Mais uma vez, porém, a ênfase de alguns comandos em relação à internet pode restringir a execução descentralizada, prejudicando a capacidade de ação proativa, ágil e oportuna ao travar a guerra de ideias.

A questão é como explorar os recursos cibernéticos que surgem para influenciar percepções, posturas e comportamentos, ao mesmo tempo em que se gerencia o risco de vigilância e ataques da internet. Vale considerar os diversos motivos dados para se restringir o acesso a novas mídias, já que eles influenciam o raciocínio dos comandos propensos a fazer isso: promover a produtividade no trabalho, atender a requisitos de largura de banda, manter a segurança das operações e impedir a invasão e o comprometimento. Esses exemplos são claramente descritos na nova política do Departamento de Defesa. Mesmo assim, a explicação a seguir é necessária para fundamentar o raciocínio em favor de uma abordagem equilibrada determinada por tal política.

Produtividade. Um argumento para a utilização de filtros de conteúdo da NIPRnet que impedem o acesso a *sites* com *links* para vídeos (ex.: *YouTube*), *blogs* e *sites* de relacionamento social é a premissa de que os soldados os acessarão para uso pessoal durante o expediente, prejudicando, assim, a produtividade. Esse potencial, sem dúvida, existe. Contudo, a responsabilidade de administrar esse problema é uma questão de liderança, pura e simplesmente, e ele deve ser tratado na base da exceção. Os filtros de conteúdo estabelecidos em qualquer escalão de comando usurpam as responsabilidades dos Comandantes em organizações subordinadas.

Requisitos de largura de banda. Outro argumento para se restringir o acesso a *sites* de vídeos é a necessidade de administrar requisitos de largura de banda. A largura de banda é a

Prudence Siebert/Fort Leavenworth Lamp

Alunos da ECEME dos EUA, servindo como Comandantes de brigada, coordenam Inteligência e fogos durante um exercício, 25 Fev 10.

"capacidade de movimentar informações"[37]. É um item de baixa densidade e de alta demanda no fornecimento de recursos computacionais de comando e controle às Forças militares. Contudo, mais uma vez, os comandantes decidem como distribuir todos os recursos valiosos e limitados para atender às exigências da missão e cumprir a missão militar[38].

Segurança das operações. A segurança das operações "seleciona e executa medidas que eliminem ou reduzam, até um nível aceitável, as vulnerabilidades das ações amigas à exploração por adversários"[39]. Alguns líderes temem que a participação de militares em *blogs*, redes sociais e *sites* de vídeos possa revelar vulnerabilidades das Forças militares. Esse risco se aplica tanto à NIPRnet quanto à internet, já que os membros das Forças Armadas podem participar de mídias em suas casas. É, sem dúvida, um risco evidenciado por diversas violações significativas nos últimos anos. Contudo, a segurança das operações é, e sempre foi, um programa do Comandante. Os comandantes controlam o ambiente de segurança das operações por meio do treinamento, do ensino e de medidas disciplinares para os casos de violação intencional. Os filtros de conteúdo e as políticas do comando estabelecidos nos escalões superiores, com vistas a impedir violações da segurança das operações, são restrições que diminuem a capacidade do comandante subordinado de liderar e alcançar objetivos militares por meio da exploração de recursos da rede.

As invasões e a ameaça de comprometimento da própria rede são, por outro lado, preocupações válidas e importantes. Os sistemas do Departamento de Defesa, como mencionado anteriormente, sofrem ataques contínuos por Estados-Nação, atores não estatais, criminosos e *hackers*. Por isso, o Departamento acertou ao estabelecer um sistema que limita o acesso à internet e permite o monitoramento criterioso e contínuo — para impedir a instalação de *software* que possa conter código malicioso, com consequências desastrosas para a rede — e para continuar a avaliar formas de minimizar tais riscos. Tantos os adversários quanto os criminosos se adaptam continuamente a atualizações e a outras medidas de defesa.

Gerenciar riscos ao mesmo tempo em que se proporciona a chance de interagir com eficácia e de explorar as oportunidades oferecidas pela internet requer um realinhamento da filosofia de comando. Os líderes e comandantes têm a autoridade e os recursos para realizar comunicações estratégicas proativas e reativas rapidamente. As questões de produtividade, largura de banda e segurança das operações são claramente de competência da liderança, e os líderes devem monitorar os subordinados e responsabilizá-los por violações de suas diretrizes. Essa abordagem descentralizada implica risco. Os comandantes e líderes devem tomar medidas para minimizá-lo, mas de forma equilibrada.

O General-de-Divisão William Caldwell afirma (utilizando, curiosamente, um *blog* como mídia) que devemos incentivar os soldados a contar suas histórias, capacitá-los a tolerar erros não intencionais, ensinar-lhes as potenciais implicações estratégicas de tal participação e prepará-los para utilizar a nova mídia[40]. Embora Caldwell se refira especificamente aos equipamentos físicos, pode-se sustentar que é tão ou mais importante fornecer aos soldados a devida orientação de comando, que permita a interação por meio de novas mídias, ao mesmo tempo em que determine seus limites. A nova política do Departamento de Defesa, à medida que for alcançando os comandos subordinados, deve permitir a livre interação, contanto que os comandantes estejam abertos às oportunidades e atentos às ameaças.

Conclusão

Em agosto de 2008, a Rússia, segundo consta, realizou ataques cibernéticos de novo, dessa vez contra a Geórgia, em uma campanha coordenada e sincronizada, ao mesmo tempo cinética [que envolve o emprego de força — N. do T.] e não cinética[41]. É totalmente provável que isso se torne a regra em futuras guerras entre Estados-Nação capacitados a realizar esse tipo de excursão complexa. O caso do Hezbollah, no conflito com Israel, em 2006, sugere igualmente o futuro uso estratégico da internet e de novas mídias para atingir públicos internos e internacionais.

O ambiente de informações tem três dimensões: a física, o "meio" pelo qual se transmite a mensagem; a informativa, isto é, o conteúdo da mensagem; e a cognitiva, ou seja, o impacto da mensagem nas percepções, posturas e comportamentos dos públicos-alvo[42]. Pode-se dizer que a guerra do futuro incluirá cada vez mais o conflito no ciberespaço nas três dimensões.

Explorar as oportunidades ao mesmo tempo em que se gerencia o risco é o imperativo estratégico. Um bom plano militar, em terra, no mar ou no ar, "protege a Força" enquanto ataca o inimigo. Os líderes civis e os comandantes militares avaliam riscos, implantam políticas e atuam no sentido de minimizar os riscos, mas também se concentram em alcançar os objetivos militares e os traçados pelas políticas. No ciberespaço, isso significa proteger a internet e utilizá-la para interagir.

Também é importante considerar efeitos de segunda e terceira ordem ao tomar decisões. Dada a ameaça constante de um ataque cibernético bem-sucedido contra os sistemas do Governo dos EUA, os líderes podem recorrer à alternativa de baixo ou nenhum risco de reforçar as paredes virtuais em torno da NIPRnet, até um nível de impenetrabilidade. Mais ainda, para impedir a possível violação da segurança das operações, eles podem estabelecer políticas restritivas sobre o uso da internet. Contudo, o efeito de segunda ordem de tudo isso é reduzir, de forma considerável, a capacidade dos líderes e comandantes de interagir no ambiente de informações utilizando novas mídias.

Gerenciar riscos ao mesmo tempo em que se proporciona a chance de interagir com eficácia e de explorar as oportunidades oferecidas pela internet requer um realinhamento da filosofia de comando.

Atualmente, as estratégias do governo e das Forças Armadas dos EUA adotam um "discurso" nesse sentido, com evidências animadoras quanto à sua adoção da "prática". A orientação dos escalões mais altos, no sentido de interagir com os públicos utilizando novas mídias, anuncia o início da superação de um preconceito cultural de longa data contra a utilização da internet para importantes engajamentos de informações. A nova política do Departamento de Defesa oferece a oportunidade de se alcançar o equilíbrio necessário tanto para explorar quanto para proteger a internet. Os líderes e comandantes são responsáveis por conduzir as guerras. Uma NIPRnet mais restritiva não resolverá esse dilema e, na verdade, poderá ter consideráveis efeitos negativos de segunda ordem. Está na hora de modificar parte da cultura avessa a riscos, de modo a permitir espaço de "manobra" para que os líderes em todos os escalões possam fazer o seu trabalho.***MR***

REFERÊNCIAS

1. O Exército dos EUA publicou seu manual doutrinário sobre contrainsurgência, Manual de Campanha *FM 3-24* (Washington, DC: U.S. Government Printing Office [GPO], dez. 2006). O prefácio observa que o Exército não havia revisado sua doutrina de contrainsurgência havia mais de 20 anos e cita as operações em andamento no Iraque e no Afeganistão como sendo o ímpeto para essa iniciativa.

2. DE CZEGE, Huba Wass. "Lessons from the Past: Making the Army's Doctrine 'Right Enough' Today", *Landpower Essay*, Institute of Land Warfare, no. 06-2 (set. de 2006): p. 4, p. 5.

3. SCALES, Robert H. *Certain Victory: The U.S. Army in the Gulf War* (Washington, DC: Brassey's, 1997), p. 106-107.

4. SEVASTOPULO, Demitry; MCGREGOR, Richard. "Chinese Military Hacked into Pentagon", *Financial Times*, 4 set. 2007.

5. APPLEBAUM, Anne. "e-Stonia Under Attack", 22 de maio de 2007, disponível em: <www.slate.com/ id/2166716/> (18 ago. 2008).

6. PERAINO, Kevin. "Winning Hearts and Minds", *Newsweek International*, 2 out. 2006.

7. CHAIRMAN OF THE JOINT CHIEFS OF STAFF, "DOD Dictionary of Military Terms", conforme redação de 30 out. 2009.

8. KUEHL, Daniel. "From Cyberspace to Cyberpower, Defining the Problem", in *Cyberpower and National Security* (Washington: National Defense University Press, 2009), p. 38.

9. *National Strategy for Combating Terrorism* (Washington, DC: GPO, September, 2006), p. 4, p. 17.

10. COGAN, Kevin J.; DELUCIO, Raymond G. "Network Centric Warfare Case Study, vol. II" (Carlisle Barracks, PA: U.S. Army War College, 2006), p. 4.

11. DEIBERT, Ronald. Apresentação, U.S. Army War College, Carlisle Barracks, PA, 10 jan. 2008. Deibert cita <www.internetworldstats.com> como fonte desses dados estatísticos. Atualizado em 30 mar. 2009.

12. LEVESQUE, William R. "*Blogs* are CENTCOM's New Target", *Saint Petersburg Times*, 12 fev. 2007.

13. GLEASON, Carmen L. "Coalition Servicemembers Reach out to America via YouTube", *American Forces Press Service*, 14 mar. 2007.

14. SEVASTOPULO; MCGREGOR. "Chinese Military Hacked into Pentagon".

15. THOMAS, Timothy L. *DragonBytes: Chinese Information War Theory and Practice* (Foreign Military Studies Office: Fort Leavenworth, Kansas, 2004), p. 136.

16. GLEBOCKI, Joseph. "DOD Computer Network Operations: Time to Hit the Send Button" (Carlisle Barracks, Pensilvânia): U.S. Department of the Army, 15 mar. 2008), p. 4.

17. BLANK, Stephen. "Web War I: Is Europe's First Information War a New Kind of War", *Comparative Strategy 27*, no. 3 (maio 2008): p. 240.

18. APPLEBAUM, "e-Stonia Under Attack".

19. BLANK, p. 230.

20. CONDON, Stephanie. "DHS Stays Mum on New 'Cyber Security' Center", 31 jul. 2008, disponível em: <http://news.cnet.com/8301-13578_3-10004266-38.htm> (4 ago. 2008).

21. CHAIRMAN OF THE JOINT CHIEFS OF STAFF, Joint Publication 3-13, Information Operations" (Washington, DC: GPO, September, 2006, 13 fev. 2006), II-5, II-6.

22. O autor participou de um congresso sobre poder cibernético patrocinado pelo Center for Technology and National Security Policy na National Defense University, em Washington, D.C., em abril de 2008. Os comentários citados refletem as apresentações dos palestrantes. O congresso foi realizado segundo as regras da Chatham House, que permitem o diálogo livre e aberto, mantendo, ao mesmo tempo, o anonimato dos palestrantes.

23. CAPACCIO, Tony. "Cyber Attacks from China Show Computers Insecure, Pentagon Says", 6 ago. 2008, disponível em: <www.bloomberg.com/apps/news?pid=newsarchive&sid=aGqtPqPlSCt8> (18 ago. 2008).

24. U.S. DEPARTMENT OF DEFENSE, *QDR Execution Roadmap for Strategic Communication* (Washington DC: U.S. Department of Defense, set. 2006), p. 3.

25. OFFICE OF THE DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR JOINT COMMUNICATION (DASD(JC)), apresentação, jun. 2008. O DASD(JC) é responsável pelo ensino e treinamento do Planejamento de Comunicação Estratégica da Revisão Quadrienal da Defesa e Comunicação Estratégica no Departamento de Defesa.

26. CALDWELL, Gen Div William. "Changing the Organizational Culture", 30 jan. 2008, disponível em: <http://smallwarsjournal.com/blog/2008/01/changing-the-organizational-cu-1/> (18 ago. 2008).

27. ROBBINS, Elizabeth. "Muddy Boots IO: The Rise of Soldier Blogs", *Military Review*, no. 5 (set.-out. 2007), p. 116.

28. LONDONO, Ernesto. "Silent Posting", Washington Post, 24 jul. 2008.

29. O autor assistiu a diversas apresentações na Escola de Guerra do Exército dos EUA, nas quais os líderes superiores (oficiais-generais e líderes civis superiores do Exército) defendiam o uso agressivo de novas mídias para transmitir mensagens positivas sobre os integrantes da Força singular. Um memorando de abr. 2008, coassinado pelo Chefe do Estado-Maior do Exército e pelo Secretário do Exército, instava que se envidassem esforços significativos para contar a história de apoio às famílias do Exército por meio do uso de "novas mídias, como *blogs*, como meios eficazes para transmitir" a mensagem.

30. Comandante, Combined Arms Center, CALDWELL, Gen Div William. "Request for Exception to Policy for Publishing to a Publically Accessible Website", *memorandum for Commander*, U.S. Army Training and Doctrine Command et al., 27 mar. 2008.

31. ENGLAND, Gordon (Subsecretário de Defesa dos EUA), "Policy for Department of Defense (DOD) Interactive Internet Activities", *memorandum for Secretaries of the Military Departments et al.*, 8 jun. 2007.

32. LYNN, William (Subsecretário de Defesa dos EUA), "Responsible and Effective Use of Internet-based Capabilities", *memorandum for Secretaries of the Military Departments et al.*, 25 fev. 2010.

33. O Manual de Campanha do Exército sobre operações (fev. de 2008) dedica um capítulo ao tema da informação como um recurso de combate. Ele ressalta a necessidade do "engajamento de informações" no âmbito do soldado individual. Também discute a necessidade de superar uma cultura avessa a riscos para o engajamento eficaz. Consulte o capítulo 7.

34. YARGER, Harry R. *Strategic Theory for the 21st Century: The Little Book on Big Strategy* (Carlisle Barracks, Pensilvânia: Strategic Studies Institute, 2006), p. 36.

35. U.S. DEPARTMENT OF DEFENSE, *National Defense Strategy* (Washington, DC: U.S. Department of Defense, jun. 2008). Consulte "Strategic Framework".

36. O autor não pôde acessar o *Facebook* em uma visita recente ao Centro de Armas Combinadas no Forte Leavenworth, no Kansas, onde pretendia mostrar aos alunos militares seus efeitos facilitadores.

37. WU, Tim. "OPEC 2.0", *New York Times*, 30 jul. 2008.

38. TISSERAND, John B. "Network Centric Warfare Case Study, Volume I" (Carlisle Barracks, Pensilvânia: U.S. Army War College, 2006), p. 53.

39. CHAIRMAN OF THE JOINT CHIEFS OF STAFF, "DOD Dictionary of Military Terms", conforme redação de 30 out. 2009.

40. CALDWELL. "Changing the Organizational Culture."

41. MARKOFF, John. "Before the Gunfire, Cyberattacks," *New York Times*, 13 ago. 2008.

42. Joint Publication 3-13, *Information Operations*, I-1-I-2.