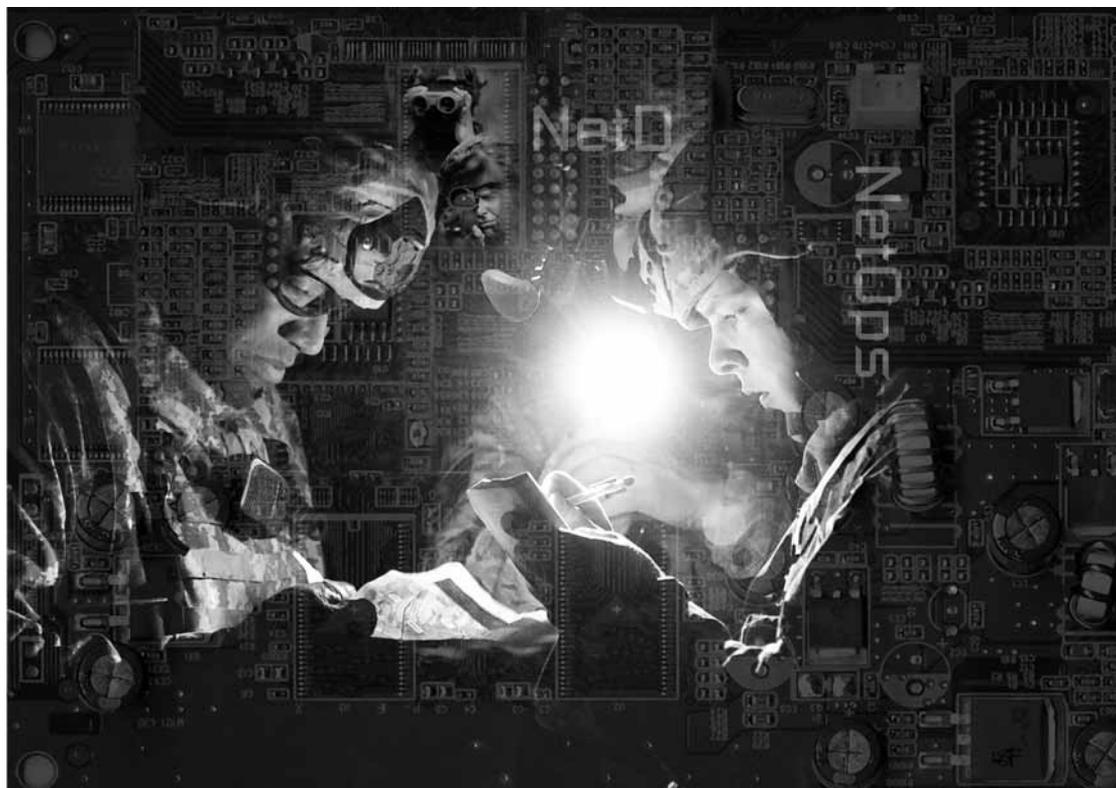


É Hora de Reagir: A “Operacionalização” da Rede de Defesa

NICOLAS ADAM FRASER*

TENENTE-CORONEL ROBERT J. KAUFMAN III, USAF, REFORMADO

TENENTE-CORONEL MARK R. RYDELL, USAF, REFORMADO



A DECISÃO DE estabelecer a 24ª Força Aérea subordinada ao Comando Espacial oferece a oportunidade de examinar os conceitos existentes referentes à guerra de rede, a fim de garantir que as operações levem avante a missão: “voar, combater e vencer no ar, espaço e ciberespaço.”¹ Essa revisão tão vasta compreenderia grande número de organizações, den-

tro e fora da Força Aérea, abrangendo discussões de normas, prioridades de alocação de verbas, pessoal e coordenação entre as Armas, entre outras. Este artigo não pretende abordar todas as questões complexas que dizem respeito às operações ciberespaciais. Ao contrário, examina o componente mais visível da guerra ciberespacial – a defesa da rede (*NetD*).

*Os três autores fazem parte da 688ª Ala de Operações de Informática na Base Aérea Lackland, Texas [688th Information Operations Wing]. O Sr. Fraser é Chefe de Seção de Engenharia de Acesso à Rede [Network Access Engineering Branch], o Tenente-Coronel Kaufman é Vice-Diretor do 318º Grupo de Operações de Informática [318th Information Operations Group]. O Tenente-Coronel Rydell é sócio líder da Booz, Allen, and Hamilton. Todos serviram anteriormente na Equipe de Reação à Emergência em Informática para a Força Aérea [Air Force Computer Emergency Response Team]

Desde 1992, a Força Aérea monitora as redes e reage, combatendo atividades maliciosas. À medida que a Força torna-se mais experiente, a capacidade de comandar e controlar as redes, alguns princípios operacionais mesclaram a *NetD* e as operações de rede [*Network Operations – NetOps*] inadvertidamente. O artigo propõe novos conceitos operacionais que obrigarão a distinção salutar entre a rede de guerra, em particular a *NetD* – e a *NetOps*. A seleção de alvos cibernéticos, o primeiro conceito proposto, destaca a necessidade de descobrir, localizar, rastrear e manter o adversário na mira, de forma proativa. As operações de seleção de alvos cibernéticos garantem que os sistemas críticos à missão ou mesmo as vias de acesso à rede permanecerão livres de adversários. O segundo conceito, o engajamento cibernético é uma coleta de reações especificamente projetadas para punir os invasores identificados. Os conceitos atuais de *NetD* e a seleção de alvos cibernéticos facilitam as operações de combate cibernético. Finalmente, devemos coordenar intimamente com os comandos combatentes (*COCOMs*) as operações de seleção de alvos e de combate, bem como aquelas de âmbito das agências nacionais. Ambos os conceitos cibernéticos mencionados acima provocam grande contraste entre manutenção e defesa de rede. O resultado dessa distinção e do emprego dos conceitos propostos é que as operações *NetD* tornam-se mais eficazes.

Como Preparar o Cenário para a Mudança

A Força Aérea é bem seleta em suas definições de *NetOps* e *NetD*. A primeira fornece “aplicativos rede-cêntricos de informática eficientes, eficientes, seguros e confiáveis utilizados em processos críticos de dados e comunicações para o Departamento de Defesa (*DoD*) e Força Aérea”. A segunda “emprega (...) a capacidade de rede na defesa de dados úteis, intrínsecos ou em trâmite pelas redes, contra as tentativas de adversários em destruir, interromper, corromper e usurpar os mesmos. A *NetD* é vista como o planejamento, direciona-

mento e execução de ações para prevenir atividades não autorizadas em defesa de sistemas e redes de informática da Força Aérea, bem como planejamento, direção e execução de reações para a recuperação de atividade não autorizada, caso ocorra.”² O fato da comunidade das Forças conjuntas não possuir um termo para descrever o que a Força Aérea denomina de *NetOps* significa que considera as *NetOps* um sub-elemento da *NetD* ou simplesmente uma função de manutenção que não merece discussão em documentos de doutrina conjunta.³ Devido às diferenças entre as doutrinas conjuntas e da Força Aérea, sugerimos versões simplificadas de *NetD* e *NetOps* para que o leitor possa reconhecer imediatamente os atributos e prioridades de cada operação:

- *operações de guerra de rede/NetD*: as operações que visam produzir efeitos táticos, operacionais e estratégicos desejáveis contra o adversário. Essas operações, que requerem apoio de planejamento e inteligência são reativas ou pró-ativas. O mais importante é que as operações *NetD* consideram a descoberta de um adversário, não apenas ameaça, mas a oportunidade de engajamento operacional.
- *NetOps*: as operações nas quais o provedor primariamente *age, prestando* serviços confiáveis e seguros. Na realidade, o adversário que interrompe as operações não é pior do que uma falha de equipamento, já que o objetivo é manter a disponibilidade e os requisitos de desempenho. Assim como podemos substituir o equipamento, podemos também reconstituir um computador corrompido.

Alegamos que a Força Aérea, na verdade, não realiza as operações *NetD* como definidas acima. Comprovamos essa declaração com a análise de dois princípios inerentes a atual abordagem de *NetD* da Força e que a mantêm reativa, debilitando sua capacidade de defender a rede de forma eficaz.

Princípio 1: é importantíssimo detectar o adversário

Este princípio, o fundamento sobre o qual erigimos a maioria das *NetD* tradicionais, consome grande parte dos recursos da Força Aérea destinados à *NetD*. A Força conta com o monitoramento em tempo real e destaca o fortalecimento do perímetro da rede para detectar atividade inimiga. A motivação é grande. A Força Aérea pretende detectar o intruso ou invasor, não para combatê-lo, mas para encontrar e corrigir um problema de segurança. A situação é similar à do membro das forças de segurança em patrulha de pista de pouso que reage à atividade suspeita. Ao ver um intruso entrar por uma ruptura na cerca, ilumina-a com a lanterna e começa a consertá-la, em vez de ir ao encalço e capturar o intruso. Atualmente, a Força Aérea não distingue entre invasões de sistema sofisticadas e não sofisticadas, tratando todas da mesma forma, reagindo de maneira a proteger e restabelecer a boa condição da rede. Tal monitoramento não se concentra em garantir a realização de missões necessárias e continuar as *NetOps*, apesar de ataques adversários.

Embora importante, a detecção de adversários não é a única maneira de proteger a rede. Mudar sua configuração rápida e regularmente também oferece proteção sem ser necessário descobrir o adversário para conseguir o resultado desejado.⁴ Além disso, não propomos eliminar a detecção, algo fundamental às operações *NetD*. O que deve mudar é a motivação que impulsiona as tentativas. Enfim, admitimos que a melhor defesa de perímetro e metodologia de gerenciamento de conserto de rede [*patch management*] não impedem ou dificultam os adversários sofisticados.⁵ Embora úteis, é preciso suplementar a abordagem atual com o objetivo de alcançar efeitos contra o adversário, garantindo o sucesso da missão.

Princípio 2: a reconstituição de computador corrompido significa o sucesso de operações *NetD*

Esse princípio relega as operações *NetD* à função de manutenção, destacando a situação salutar da rede, em detrimento à determinação do efeito causado pelo inimigo em mis-

sões futuras ou em curso. Além disso, raramente usamos um computador corrompido para engajar o adversário. Além de buscar, analisar e “curar” os computadores infectados, os operadores de *NetD* confrontam o adversário, mesmo em nossas próprias redes, concebendo e executando estratégias de defesa que os afetem, simultaneamente garantindo a integridade da prioridade das missões de combate de guerra.

Devido a esse princípio, provavelmente mais do que ao anterior, devemos definir a *NetD* como *NetOps* atuais. Quando ocorre a invasão e “abrimos um relatório de incidente, quando é que devemos fechá-lo? Após concluirmos a operação? Quando o computador estiver livre de intrusos e pronto para ser reintegrado à rede? Não. Devemos medir o sucesso pela eficácia em combate. Consequentemente, devemos tomar medidas estratégicas, operacionais e táticas para determinar se estamos atingindo os objetivos de *NetD*, tais como impedir o adversário de estabelecer ou utilizar capacidade ofensiva contra os interesses dos Estados Unidos”.⁶

O Novo Conceito

A fim de corrigir esses problemas propomos a criação de equipes operacionais (tamanho a ser determinado) encarregadas de realmente causar efeito adverso às operações aquele adversário que mantém as redes da Força Aérea e do *DoD* em sua mira. De fato, as equipes da 24^a *Air Force* (inclusive a 688^a Ala de Operações de Dados [*688th Information Operations Wing*] e a 67^a Ala de Guerra em Rede [*67th Network Warfare Wing*] são responsáveis pela execução da missão cibernética da Força Aérea. No entanto, equipe alguma da 24^a Força Aérea atualmente faz o que sugerimos a seguir. Os novos paradigmas exigirão a renovação das equipes já existentes e, possivelmente, a criação de outras.

A primeira organização proposta possuiria a missão com enfoque interno, buscando o adversário em redes da Força Aérea e do *DoD*. A segunda seria a missão com enfoque externo, combatendo-o nessas mesmas redes. Embora ambas operem em conjunto (e inti-

mamente, de forma contínua, juntamente com a missão de monitorar as redes), seriam distintas em seu compromisso para com as missões planejadas ou “*surtidas*” vinculadas às necessidades operacionais de comandantes e finalizadas após a conclusão da missão. As diretrizes adequadas devem apoiar as estratégias pró-ativas de *NetD*, tais como a seleção de alvo e engajamento. Em seguida, operacionalmente, devemos estabelecer planos para lidar com adversários específicos e prescrever cursos de ação aprovados que permitam aos defensores da rede efetuar no ciberespaço um empenho único, de massa, surpresa e no momento oportuno. Por fim, taticamente devemos treinar e certificar os operadores de armas de *NetD* que possam frustrar ataques ou impedir tentativas de acesso às redes da Força Aérea. Essas organizações e planos permitirão à Força Aérea realizar operações *NetD* que buscam combater e atuar contra adversários ciberespaciais.

A Seleção de Alvos Cibernéticos

Claramente, os inimigos – especialmente os mais aptos e persistentes – encontram-se dentro da rede da Força Aérea. Os ataques de surpresa, que persuadem os usuários a abrir ou clicar um arquivo anexo malicioso e *elos* de página da *Web* suspeitos, violam as defesas de perímetro, sem dificuldade. A facilidade com que o adversário obtém acesso às redes do *DoD* é superada apenas pela facilidade com que navega e manobra após estabelecer *cabeças-de-praia* dentro das redes, ambas permitindo acesso a sistemas de dados valiosos. Sendo abordagem pró-ativa, a seleção de alvos cibernéticos identifica intrusos, utilizando “armas” *NetD*, de ponta, localizadas permanentemente na rede, juntamente com ferramentas típicas de segurança de perímetro. Conduziríamos operações com objetivos específicos em mente: encontrar; persuadir; interromper as ações; combater o inimigo. A operação permanece *aberta* até conseguirmos identificar o adversário e verificar sua remoção. O fator que requer uma *conclusão*, aqui não entra em jogo. Essas operações também exigem execução e planejamento apropriados, devido a enorme quanti-

dade de dados ciberespaciais legítimos, o que oferece bom esconderijo ao adversário.

O Engajamento Cibernético

A defesa sempre exige retardar, interferir, dissuadir e negar objetivos ao inimigo. No entanto, ao admitirmos a impossibilidade de fazer com que o adversário cesse por completo, devemos então investigar meios para impedir, em grande parte, suas ações ou explorar suas atividades, (aqui o termo explorar significa causar efeitos de segunda e terceira ordens em sua capacidade de decisão). O adversário durante o engajamento cibernético toma a decisão consciente de utilizar as redes do *DoD* como via de acesso, o que permite alcançar as metas defensivas.⁷ Ao descobrir um computador ou rede corrompida, os operadores de *NetD* não mais simplesmente reconstituíram o sistema, mas usariam dados secretos e talvez outras armas de *NetD* para identificar o intruso. Em seguida, dependendo do nível de atribuição e planos operacionais (*OPLAN*) existentes, executariam operações táticas contra o adversário, utilizando o computador ou a rede infectada como ponto de partida.⁸ Por exemplo, durante dada operação o operador de *NetD* pode intencionalmente passar dados imprecisos ao inimigo ou manipular dados extraídos do mesmo, tornando-os não confiáveis. Independentemente da técnica utilizada, o operador deve sempre tentar introduzir insegurança, fazer com que as invasões custem caro ou causem efeitos adversos às ações do adversário. Por conseguinte, os operadores devem planejar e coordenar essas “reações” com o *COCOM* maior ou estratégias de alcance nacional.⁹ Além disso, devem evitar conflito com esses tipos de operações, monitorando diariamente os sensores da rede.

Como acima exposto, o engajamento cibernético abrange todo um espectro de operações e não simplesmente ataques à rede. Esse engajamento pressupõe a inabilidade de detecção e tentativas de proteção para defender a rede de forma adequada. Ao contrário, possui abordagem distinta não limitada à seleção de determinada tecnologia, mas que se preocupa com as ações necessárias para atingir as

metas de defesa. Para propósitos de ilustração, durante um jogo de futebol americano os jogadores na ofensiva tentam chegar à área de fundo, implantando forte linha defensiva, com o zagueiro, por exemplo, utilizando também esquemas diferentes para confundir o *capitão* do time (*quarterback*). Um defensor lateral arremessa-se contra o *capitão*, enquanto dois outros permanecem ao fundo para dar cobertura. Às vezes, o coordenador defensivo ordena um ataque total ao jogador que está prestes a passar a pelota. Independentemente do esquema, o bom treinador sabe que nem sempre pode evitar que a linha ofensiva marque um gol de campo, mas o que pode fazer é dificultar a tarefa, confundindo os jogadores adversários, principalmente o *capitão*.

Com a analogia acima em mente, somos obrigados a declarar que o *DoD* atualmente joga na defesa, sem jamais pensar em causar confusão na linha de ataque. Não contamos com diferentes esquemas defensivos, nem projetamos planos para afetar o planejamento, execução e, em última análise, o resultado de um encontro com o inimigo. Pelo contrário, a defesa permanece no perímetro e esperamos que ninguém passe despercebido.

O engajamento e a seleção de alvos cibernéticos constituem grande mudança de paradigma na forma como levamos a cabo as operações *NetD*. Ao incluirmos a *NetD* aos objetivos principais de *OPLAN*, podemos torná-la em forma de combate mais potente do que os ataques à rede.¹⁰ De fato, o Exército dos Estados Unidos já notou isso durante as operações defensivas mais tradicionais.¹¹ Além do mais, a *NetD* assume função mais ativa em guerra de rede, criando, ao mesmo tempo, a distinção tão necessária entre *NetD* e *NetOps*. Finalmente, esses novos conceitos apoiam a determinação do Presidente de ir além do processo penal na reação adequada a ataques cibernéticos.¹²

Uma Proposta Simples

O planejamento e o preparo para operações militares em grande escala, como a invasão do Iraque em 2003, exigem que os *OPLANs* do *COCOM* sejam encaminhados através das

organizações *NetD* de cada Força, permitindo assim que os defensores de rede programem as medidas contra os inimigos que mantêm as redes do *DoD* em mira, prevenindo qualquer interrupção da execução do plano operacional. Os requisitos fornecidos pelos *COCOMs* normalmente abordam ameaças genéricas. Ao início das operações, costumamos tomar medidas pró-ativas como bloquear endereços *hostis* dos protocolos da *Internet*.

Nessas situações tradicionais, tratamos as redes como elemento de apoio. Ou seja, devem funcionar sem interrupção para que a capacidade da guerra simétrica funcione. É o mesmo que dizer que os caminhões de combustível devem estar disponíveis para que os *F-16* possam decolar. É difícil contemplar o combate em redes, mas as operações *NetD* devem tomar vantagem do acesso às operações de rede do inimigo e reagir, diminuindo a credibilidade de dados surripiados, aumentando o custo de ataque às redes, ou permitindo que os Estados Unidos prejudiquem a percepção do adversário, antes e durante todas as fases do conflito.

O que propomos a seguir é uma maneira de destacar a utilidade desse novo conceito, que realmente trata a *NetD* como forma de guerra assimétrica. Atualmente, cada *OPLAN* possui um apêndice que trata dos requisitos de *NetD*. No entanto, além de fornecer proteção preventiva à rede, os futuros *OPLANs* devem identificar os sistemas críticos para a realização de operações de guerras tradicionais (por exemplo, redes de logística, nexos de comando e controle, etc.) Além disso, devemos identificar adversários que apresentem grande ameaça para que possamos começar a planejar e coordenar as operações cibernéticas de engajamento. Devemos planejar e executar as operações de seleção de alvos em sistemas críticos à missão identificados pelo *COCOM*.

Desta vez, no entanto, se encontrarmos o adversário devemos iniciar o engajamento com o fim de causar impacto ou influenciar suas operações.

Dois pontos importantes merecem ênfase. Em primeiro lugar, o adversário descoberto durante as operações de seleção de alvo pode

ser totalmente diferente do abordado pelo *OPLAN*, uma possibilidade que faz do ciberespaço um domínio a ser conquistado. Em segundo lugar, as operações de seleção de alvos e engajamento não precisam ser necessariamente vinculadas a um *OPLAN* específico do *COCOM*. Podemos realizar operações práticas de seleção de alvo, contanto que devidamente delineadas e sincronizadas com outras operações. Devemos considerar as operações de engajamento toda vez que descobrimos invasão de rede, seja através de técnicas tradicionais de detecção ou de operações de seleção de alvo.

Conclusão

De acordo com a 67ª Ala de Guerra em Rede [*67th Network Warfare Wing*], “o ponto decisivo é que a Força Aérea deve evoluir de orientação centrada em detecção à abordagem de cadeia de destruição de rede ativa que integra a prevenção, detecção, reação e engajamento.”¹³ Esse plano não pode ser posto em prática sem organizar e designar tarefas às equipes operacionais de *NetD* para mudar conceitos operacionais, de abordagem reativa (monitorar, detectar e reagir) a uma que, como recentemente descrito pelo Tenente-General William T. Lord, “busca ameaças (...) detectando-as e derrotando-as

instantaneamente.”¹⁴ Não podemos fazê-lo de forma isolada. Precisamos de planejamento com propósito determinado e coordenação com a inteligência e agências nacionais. Além disso, a criação do Comando Cibernético dos Estados Unidos ajudaria a garantir que as Forças atuem sob a autoridade e direção de um *COCOM*. Os conceitos de ciberalvo e ciberengajamento de fato “operacionalizam” a *NetD*, uma vez que se enfocam diretamente em agir e afetar o adversário. No futuro, devemos prestar a mesma atenção à garantia da missão (i.e., operações contínuas, apesar de ataques inimigos), área que impede a completa separação de *NetD* e *NetOps*. No entanto, não podemos abordá-la adequadamente sem planejamento e inteligência confiável. O *DoD* gasta \$100 milhões de dólares cada seis meses para defender a rede *.mil*.¹⁵ Em certo ponto, devemos nos perguntar se estamos atingindo os objetivos de defesa e dissuadindo os adversários. Atualmente, a resposta é não. Mas, com a operacionalização da *NetD* e a concentração em atingir o inimigo, podemos inverter essa tendência para que a Força Aérea consiga reagir.

Base Aérea Lackland, Texas

Notas

1. Air Force Program Action Directive 07-08, *Phase One of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces*, 19 December 2008, 8.

2. Air Force Instruction 33-115, vol. 1, *Network Operations (NETOPS)*, 24 May 2006, 3, <http://www.af.mil/shared/media/epubs/AFI33-115V1.pdf> (acessado em 13 de maio de 2010); e Air Force Doctrine Document 2-5, *Information Operations*, 11 January 2005, 20, http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_5.pdf (acessado em 13 de maio de 2010).

3. Joint Publication 3-13, *Information Operations*, 13 February 2006, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (acessado em 13 de maio de 2010).

4. Spyros Antonatos et al., “Defending against Hitlist Worms Using Network Address Space Randomization,” *Computer Networks* 51, no. 12 (22 August 2007): 3471–

3490; e Dorene Kewley et al., “Dynamic Approaches to Thwart Adversary Intelligence Gathering” in *Proceedings of the DARPA [Defense Advanced Research Projects Agency] Information Survivability Conference and Exposition*, vol. 1 (2001), 176.

5. “Engaging the Adversary on Air Force Networks,” Information Assurance Technology Analysis Center Report, TAT 04-25, DO 232, 5 March 2007, 1.

6. Chefe, Estado-Maior Conjunto à lista de distribuição, memorando, assunto: National Military Strategy for Cyberspace Operations (sem anexo), December 2006, 13, <http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf> (acessado em 14 de maio de 2010).

7. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1963), 87.

8. *Attribution* significa o grau de confiança com o qual podemos identificar o adversário.

9. John P. Stenbit, Secretário de Defesa Adjunto para comando, controle, comunicações e inteligência, aos secretários de departamentos militares, memorando, assunto: Guidance for Computer Network Defense Response Actions, 26 February 2003, <https://powhatan.iie.disa.mil/cnd/cnd-ra-matrixand-memo.pdf> (acessado em 14 de maio de 2010).

10. Carl von Clausewitz, *On War*, ed. e trans. Michael Howard e Peter Paret (Princeton, NJ: Princeton University Press, 1976), 84.

11. Field Manual 3-01.7, *Air Defense Artillery Brigade Operations*, 31 October 2000, 6-36, http://www.theblackvault.com/documents/fm3_01x7.pdf (acessado em 14 de maio de 2010).

12. White House, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003), http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (acessado em 14 de maio de 2010).

13. 26th Network Operations Group, "NetD Concept of Employment," versão final, 14 December 2007, 2.

14. Chuck Paone, "General Calls for New Thinking on Cyberspace," 12 de maio de 2009, <http://www.af.mil/news/story.asp?id=123148876> (acessado em 8 de abril de 2010).

15. William Jackson e Doug Beizer, "New DOD Cyber Command Will Focus on the Dot-Mil Domain," *Government Computer News*, 15 June 2009, <http://gcn.com/Articles/2009/06/15/Web-DOD-cyber-command.aspx?p=1> (acessado em 8 de abril de 2010).